Abstract

Autonomic functions need a control plane to communicate, which depends on some addressing and routing. This Autonomic Control Plane should ideally be self-managing, and as independent as possible of configuration. One application is a "virtual out of band channel" for communications over a network that is not configured or mis-configured. This document describes requirements and implementation options for an "Autonomic Control Plane".

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 1, 2016.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents.
1.  Introduction

Autonomic Networking is a concept of self-management: Autonomic functions self-configure, and negotiate parameters and settings across the network. [RFC7575] defines the fundamental ideas and design goals of Autonomic Networking. A gap analysis of Autonomic Networking is given in [RFC7576]. The reference architecture for
Autonomic Networking in the IETF is currently being defined in the document [I-D.behringer-anima-reference-model]

Autonomic functions need a stable and robust infrastructure to communicate on. This infrastructure should be as robust as possible, and it should be re-usable by all autonomic functions. [RFC7575] calls it the "Autonomic Control Plane". This document defines the requirements and implementation options of an Autonomic Control Plane.

Today, the management and control plane of networks typically runs in the global routing table, which is dependent on correct configuration and routing. Misconfigurations or routing problems can therefore disrupt management and control channels. Traditionally, an out of band network has been used to recover from such problems, or personnel is sent on site to access devices through console ports. However, both options are operationally expensive.

In increasingly automated networks either controllers or distributed autonomic service agents in the network require a control plane which is independent of the network they manage, to avoid impacting their own operations.

This document describes options for a self-forming, self-managing and self-protecting "Autonomic Control Plane" (ACP) which is inband on the network, yet as independent as possible of configuration, addressing and routing problems (for details how this achieved, see Section 5). It therefore remains operational even in the presence of configuration errors, addressing or routing issues, or where policy could inadvertently affect control plane connectivity. The Autonomic Control Plane serves several purposes at the same time:

- Autonomic functions communicate over the ACP.
- An operator can use it to log into remote devices, even if the data plane is misconfigured or unconfigured.
- A controller or network management system can use it to securely bootstrap network devices in remote locations, even if the network in between is not yet configured; no data-plane dependent bootstrap configuration is required. An example of such a secure bootstrap process is described in [I-D.pritikin-anima-bootstrapping-keyinfra]
- Devices can use the ACP for direct decentralised communications, such as negotiations or discovery. The ACP therefore supports directly Autonomic Networking functions, as described in
This document describes some use cases for the ACP in Section 2, it defines the requirements in Section 3, Section 4 gives an overview how an Autonomic Control Plane is constructed, and in Section 5 the detailed process is explained. The document "Autonomic Network Stable Connectivity" [I-D.eckert-anima-stable-connectivity] describes how the ACP can be used to provide stable connectivity for OAM applications. It also explains on how existing management solutions can leverage the ACP in parallel with traditional management models, when to use the ACP versus the data plane, how to integrate IPv4 based management, etc.

2. Use Cases for an Autonomic Control Plane

2.1. An Infrastructure for Autonomic Functions

Autonomic Functions need a stable infrastructure to run on, and all autonomic functions should use the same infrastructure to minimise the complexity of the network. This way, there is only need for a single discovery mechanism, a single security mechanism, and other process that distributed functions require.

2.2. Secure Bootstrap over an Unconfigured Network

Today, bootstrapping a new device typically requires all devices between a controlling node (such as an SDN controller) and the new device to be completely and correctly addressed, configured and secured. Therefore, bootstrapping a network happens in layers around the controller. Without console access (for example through an out of band network) it is not possible today to make devices securely reachable before having configured the entire network between.

With the ACP, secure bootstrap of new devices can happen without requiring any configuration on the network. A new device can automatically be bootstrapped in a secure fashion and be deployed with a domain certificate. This does not require any configuration on intermediate nodes, because they can communicate through the ACP.

2.3. Data Plane Independent Permanent Reachability

Today, most critical control plane protocols and network management protocols are running in the data plane (global routing table) of the network. This leads to undesirable dependencies between control and management plane on one side and the data plane on the other: Only if the data plane is operational, will the other planes work as expected.
Data plane connectivity can be affected by errors and faults, for example certain AAA misconfigurations can lock an administrator out of a device; routing or addressing issues can make a device unreachable; shutting down interfaces over which a current management session is running can lock an admin irreversibly out of the device. Traditionally only console access can help recover from such issues.

Data plane dependencies also affect NOC/SDN controller applications: Certain network changes are today hard to operate, because the change itself may affect reachability of the devices. Examples are address or mask changes, routing changes, or security policies. Today such changes require precise hop-by-hop planning.

The ACP provides reachability that is largely independent of the data plane, which allows control plane and management plane to operate more robustly:

- For management plane protocols, the ACP provides the functionality of a "Virtual-out-of-band (VooB) channel", by providing connectivity to all devices regardless of their configuration or global routing table.

- For control plane protocols, the ACP allows their operation even when the data plane is temporarily faulty, or during transitional events, such as routing changes, which may affect the control plane at least temporarily. This is specifically important for autonomic service agents, which could affect data plane connectivity.

The document "Autonomic Network Stable Connectivity" [I-D.eckert-anima-stable-connectivity] explains the use cases for the ACP in significantly more detail and explains how the ACP can be used in practical network operations.

3. Requirements

The Autonomic Control Plane has the following requirements:

1. The ACP SHOULD provide robust connectivity: As far as possible, it should be independent of configured addressing, configuration and routing. (2 and 3 build on this requirement, but also have value on their own)

2. The ACP MUST have a separate address space from the data plane. Reason: traceability, debug-ability, separation from data plane, security (can block at edge)
3. The ACP MUST use autonomically managed address space. Reason: easy bootstrap and setup ("autonomic"); robustness (admin can’t mess things up so easily). ULA seems like a good choice for 1 and 2.

4. The ACP MUST be generic. Usable by all the functions and protocols of the AN infrastructure. MUST NOT be tied to a particular protocol.

5. The ACP MUST provide security: Messages coming through the ACP MUST be authenticated to be from a trusted node, and SHOULD (very strong SHOULD) be encrypted.

The default mode of operation of the ACP is hop-by-hop, because this interaction can be built on IPv6 link local addressing, which is autonomic, and has no dependency on configuration (requirement 1). It may be necessary to have end-to-end connectivity in some cases, for example to provide an end-to-end security association for some protocols. This is possible, but then has a dependency on routable address space.

4. Overview

The Autonomic Control Plane is constructed in the following way (for details, see Section 5):

- Each autonomic node creates a virtual routing and forwarding (VRF) instance, or a similar virtual context.

- When an autonomic node discovers another autonomic node from the same domain, it authenticates that node and negotiates a secure tunnel to it. These tunnels are placed into the previously set up VRF. This creates an overlay network with hop-by-hop tunnels.

- Inside the ACP VRF, each node sets up a loopback interface with a ULA IPv6 address.

- Each node runs a lightweight routing protocol, to announce reachability of the loopback addresses inside the ACP.

- NMS systems or controllers have to be manually connected into the ACP.

- None of the above operations is reflected in the configuration of the device.

The following figure illustrates the ACP.
The resulting overlay network is normally based exclusively on hop-by-hop tunnels. This is because addressing used on links is IPv6 link local addressing, which does not require any prior set-up. This way the ACP can be built even if there is no configuration on the devices, or if the data plane has issues such as addressing or routing problems.

An alternative ACP design can be achieved without the VRFs. In this case, the autonomic virtual addresses are part of the data plane, and subject to routing, filtering, QoS, etc on the data plane. The secure tunnels are in this case used by traffic to and from the autonomic address space. They are still required to provide the authentication function for all autonomic packets.

5. Self-Creation of an Autonomic Control Plane

This section describes the steps to set up an Autonomic Control Plane, and highlights the key properties which make it "indestructible" against many inadvert changes to the data plane, for example caused by misconfigurations.

5.1. Preconditions

Each autonomic device has a globally unique domain certificate, with which it can cryptographically assert its membership of the domain. The document [I-D.pritikin-anima-bootstrapping-keyinfra] describes how a domain certificate can be automatically and securely derived from a vendor specific Unique Device Identifier (UDI) or IDevID certificate. (Note the UDI used in this document is NOT the UUID specified in [RFC4122].)
5.2. Adjacency Discovery

Adjacency discovery exchanges identity information about neighbors, either the UDI or, if present, the domain certificate (see Section 5.1. This document assumes the existence of a domain certificate.

Adjacency discovery provides a table of information of adjacent neighbors. Each neighbor is identified by a globally unique device identifier (UDI).

The adjacency table contains the following information about the adjacent neighbors.

- Globally valid Unique device identifier (UDI).
- Link Local IPv6 address with its scope.
- Trust information: The certificate chain, if available.
- Validity of the trust (once validated, see next section).

Adjacency discovery can populate this table by several means. One such mechanism is to discover using link local multicast probes, which has no dependency on configured addressing and is preferable in an autonomic network.

The "Generic Discovery and Negotiation Protocol" GDNP described in [I-D.carpenter-anima-gdn-protocol] is a possible candidate protocol to meet the requirements for Adjacency Discovery described here.

5.3. Authenticating Neighbors

Each neighbor in the adjacency table is authenticated. The result of the authentication of the neighbor information is stored in the adjacency table. We distinguish the following cases:

- Inside the domain: If the domain certificate presented is validated (including proof of possession of the corresponding private key) to be in the same domain as that of the autonomic entity then the neighbor is deemed to be inside the autonomic domain. Only entities inside the autonomic domain will by default be able to establish the autonomic control plane. Alternatively, policy can define whether to simply trust devices with the same trust anchor. An ACP channel will be established.

- Outside the domain: If there is no domain certificate presented by the neighbor, or if the domain certificate presented is invalid or
expired, then the neighbor is deemed to be outside the autonomic domain. No ACP channel will be established.

Certificate management questions such as enrolment, revocation, renewal, etc, are not discussed in this draft. Please refer to [I-D.pritikin-anima-bootstrapping-keyinfra] for more details.

5.4. Capability Negotiation

Autonomic devices have different capabilities based on the type of device and where it is deployed. To establish a trusted secure communication channel, devices must be able to negotiate with each neighbor a set of parameters for establishing the communication channel, most notably channel type and security type. The channel type could be any tunnel mechanism that is feasible between two adjacent neighbors, for example a GRE tunnel. The security type could be any of the channel protection mechanism that is available between two adjacent neighbors on a given channel type, for example TLS, DTLS or IPsec. The establishment of the autonomic control plane can happen after the channel type and security type is negotiated.

The "Generic Discovery and Negotiation Protocol GDNP described in [I-D.carpenter-anima-gdn-protocol] is a possible candidate protocol to meet the requirements for capability negotiation described here.

5.5. Channel Establishment

After authentication and capability negotiation autonomic nodes establish a secure channel towards their direct AN neighbors with the above negotiated parameters. In order to be independent of configured link addresses, these channels can be implemented in several ways:

- As a secure IP tunnel (e.g., IPsec, DTLS, TLS, etc.), using IPv6 link local addresses between two adjacent neighbors. This way, the ACP tunnels are independent of correct network wide routing. They also do not require larger than link local scope addresses, which would normally need to be configured or maintained. Each AN node MUST support this function.

- L2 separation, for example via a separate 802.1q tag for ACP traffic. This even further reduces dependency against the data plane (not even IPv6 link-local there required), but may be harder to implement.
Since channels are established between adjacent neighbors, the resulting overlay network does hop by hop encryption. Each node decrypts incoming traffic from the ACP, and encrypts outgoing traffic to its neighbors in the ACP. Routing is discussed in Section 5.8.

If two nodes are connected via several links, the ACP SHOULD be established on every link, but it is possible to establish the ACP only on a sub-set of links. Having an ACP channel on every link has a number of advantages, for example it allows for a faster failover in case of link failure, and it reflects the physical topology more closely. Using a subset of links (for example, a single link), reduces resource consumption on the devices, because state needs to be kept per ACP channel.

5.6. Context Separation

The ACP is in a separate context from the normal data plane of the device. This context includes the ACP channels IPv6 forwarding and routing as well as any required higher layer ACP functions.

In classical network device platforms, a dedicated so called "Virtual routing and forwarding instance" (VRF) is one logical implementation option for the ACP. If possible by the platform SW architecture, separation options that minimize shared components are preferred.

The context for the ACP needs to be established automatically during bootstrap of a device and - as necessitated by the implementation option be protected from being modified unintentional from data plane configuration.

In addition this provides for security, because the ACP is not reachable from the global routing table. Also, configuration errors from the data plane setup do not affect the ACP.

5.7. Addressing inside the ACP

The channels explained above only establish communication between two adjacent neighbors. In order for the communication to happen across multiple hops, the autonomic control plane requires internal network wide valid addresses and routing. Each autonomic node must create a loopback interface with a network wide unique address inside the ACP context mentioned in Section 5.6.

We suggest to create network wide Unique Local Addresses (ULA) in accordance with [RFC4193] with the following algorithm:

- Prefix FC01::/8
o Global ID: a hash of the domain ID; this way all devices in the same domain have the same /48 prefix. Conversely, global ID from different domains are unlikely to clash, such that two networks can be merged, as long as the policy allows that merge. See also Section 6 for a discussion on merging domains.

o Subnet ID and interface ID: These can be either derived deterministically from the name of the device, or assigned at registration time of the device.

Links inside the ACP only use link-local IPv6 addressing, such that each node only requires one routable loopback address.

5.8. Routing in the ACP

Once ULA address are set up all autonomic entities should run a routing protocol within the autonomic control plane context. This routing protocol distributes the ULA created in the previous section for reachability. The use of the autonomic control plane specific context eliminates the probable clash with the global routing table and also secures the ACP from interference from the configuration mismatch or incorrect routing updates.

The establishment of the routing plane and its parameters are automatic and strictly within the confines of the autonomic control plane. Therefore, no manual configuration is required.

All routing updates are automatically secured in transit as the channels of the autonomic control plane are by default secured.

The routing protocol inside the ACP should be light weight and highly scalable to ensure that the ACP does not become a limiting factor in network scalability. We suggest the use of RPL as one such protocol which is light weight and scales well for the control plane traffic.

5.9. Connecting a Controller / NMS system

The Autonomic Control Plane can be used by management systems, such as controllers or network management system (NMS) hosts (henceforth called simply "NMS hosts"), to connect to devices through it. For this, an NMS host must have access to the ACP. By default, the ACP is a self-protecting overlay network, which only allows access to trusted systems. Therefore, a traditional NMS system does not have access to the ACP by default, just like any other external device.

The preferred way for an NMS host to connect to the ACP of a network is to enrol that NMS host as a domain device, such that it shares a domain certificate with the same trust anchor as the network devices.
Then, the NMS host can automatically discover an adjacent network element, and join the ACP automatically, just like a network device would connect to a neighboring device. Alternatively, if there is no directly connected autonomic network element, a secure connection to a single remote network element can be established by configuration, authenticated using the domain certificates. There, the NMS host "enters" the ACP, from which point it can use the ACP to reach further nodes.

If the NMS host does not support autonomic negotiation of the ACP, then it can be brought into the ACP by configuration. On an adjacent autonomic node with ACP, the interface with the NMS host can be configured to be part of the ACP. In this case, the NMS host is with this interface entirely and exclusively inside the ACP. It would likely require a second interface for connections between the NMS host and administrators, or Internet based services. This mode of connecting an NMS host has security consequences: All systems and processes connected to this implicitly trusted interface have access to all autonomic nodes on the entire ACP, without further authentication. Thus, this connection must be physically controlled.

In both options, the NMS host must be routed in the ACP. This involves two parts: 1) the NMS host must point default to the AN device for all IPv6, or for the ULA prefix used inside the ACP, and 2) the prefix used between AN node and NMS host must be announced into the ACP, and distributed there.

The document "Autonomic Network Stable Connectivity" [I-D.eckert-anima-stable-connectivity] explains in more detail how the ACP can be integrated in a mixed NOC environment.

6. Self-Healing Properties

The ACP is self-healing:

- New neighbors will automatically join the ACP after successful validation and will become reachable using their unique ULA address across the ACP.

- When any changes happen in the topology, the routing protocol used in the ACP will automatically adapt to the changes and will continue to provide reachability to all devices.

- If an existing device gets revoked, it will automatically be denied access to the ACP as its domain certificate will be validated against a Certificate Revocation List during authentication. Since the revocation check is only done at the establishment of a new security association, existing ones are not
automatically torn down. If an immediate disconnect is required, existing sessions to a freshly revoked device can be re-set.

The ACP can also sustain network partitions and mergers. Practically all ACP operations are link local, where a network partition has no impact. Devices authenticate each other using the domain certificates to establish the ACP locally. Addressing inside the ACP remains unchanged, and the routing protocol inside both parts of the ACP will lead to two working (although partitioned) ACPs.

There are few central dependencies: A certificate revocation list (CRL) may not be available during a network partition; a suitable policy to not immediately disconnect neighbors when no CRL is available can address this issue. Also, a registrar or Certificate Authority might not be available during a partition. This may delay renewal of certificates that are to expire in the future, and it may prevent the enrolment of new devices during the partition.

After a network partition, a re-merge will just establish the previous status, certificates can be renewed, the CRL is available, and new devices can be enrolled everywhere. Since all devices use the same trust anchor, a re-merge will be smooth.

Merging two networks with different trust anchors requires the trust anchors to mutually trust each other (for example, by cross-signing). As long as the domain names are different, the addressing will not overlap (see Section 5.7).

7. Self-Protection Properties

As explained in Section 5, the ACP is based on channels being built between devices which have been previously authenticated based on their domain certificates. The channels themselves are protected using standard encryption technologies like DTLS or IPsec which provide additional authentication during channel establishment, data integrity and data confidentiality protection of data inside the ACP and in addition, provide replay protection.

An attacker will therefore not be able to join the ACP unless having a valid domain certificate, also packet injection and sniffing traffic will not be possible due to the security provided by the encryption protocol.

The remaining attack vector would be to attack the underlying AN protocols themselves, either via directed attacks or by denial-of-service attacks. However, as the ACP is built using link-local IPv6 address, remote attacks are impossible. The ULA addresses are only reachable inside the ACP context, therefore unreachable from the data.
plane. Also, the ACP protocols should be implemented to be attack resistant and not consume unnecessary resources even while under attack.

8. The Administrator View

An ACP is self-forming, self-managing and self-protecting, therefore has minimal dependencies on the administrator of the network. Specifically, it cannot be configured, there is therefore no scope for configuration errors on the ACP itself. The administrator may have the option to enable or disable the entire approach, but detailed configuration is not possible. This means that the ACP must not be reflected in the running configuration of devices, except a possible on/off switch.

While configuration is not possible, an administrator must have full visibility of the ACP and all its parameters, to be able to do trouble-shooting. Therefore, an ACP must support all show and debug options, as for any other network function. Specifically, a network management system or controller must be able to discover the ACP, and monitor its health. This visibility of ACP operations must clearly be separated from visibility of data plane so automated systems will never have to deal with ACP aspect unless they explicitly desire to do so.

Since an ACP is self-protecting, a device not supporting the ACP, or without a valid domain certificate cannot connect to it. This means that by default a traditional controller or network management system cannot connect to an ACP. See Section 5.9 for more details on how to connect an NMS host into the ACP.

9. Security Considerations

An ACP is self-protecting and there is no need to apply configuration to make it secure. Its security therefore does not depend on configuration.

However, the security of the ACP depends on a number of other factors:

- The usage of domain certificates depends on a valid supporting PKI infrastructure. If the chain of trust of this PKI infrastructure is compromised, the security of the ACP is also compromised. This is typically under the control of the network administrator.

- Security can be compromised by implementation errors (bugs), as in all products.
Fundamentally, security depends on correct operation, implementation and architecture. Autonomic approaches such as the ACP largely eliminate the dependency on correct operation; implementation and architectural mistakes are still possible, as in all networking technologies.

10. IANA Considerations

This document requests no action by IANA.

11. Acknowledgements

This work originated from an Autonomic Networking project at Cisco Systems, which started in early 2010. Many people contributed to this project and the idea of the Autonomic Control Plane, amongst which (in alphabetical order): Ignas Bagdonas, Parag Bhide, Alex Clemm, Toerless Eckert, Yves Hertoghs, Bruno Klauser, Max Pritikin, Ravi Kumar Vadapalli.

Further input and suggestions were received from: Rene Struik, Brian Carpenter, Benoit Claise.

12. Change log [RFC Editor: Please remove]

12.1. Initial version

First version of this document:
[I-D.behringer-autonomic-control-plane]

12.2. version 00

Initial version of the anima document; only minor edits.

12.3. version 01

- Clarified that the ACP should be based on, and support only IPv6.
- Clarified in intro that ACP is for both, between devices, as well as for access from a central entity, such as an NMS.
- Added a section on how to connect an NMS system.
- Clarified the hop-by-hop crypto nature of the ACP.
- Added several references to GDNP as a candidate protocol.
Added a discussion on network split and merge. Although, this should probably go into the certificate management story longer term.

12.4. version 02

Addresses (numerous) comments from Brian Carpenter. See mailing list for details. The most important changes are:

- Introduced a new section "overview", to ease the understanding of the approach.
- Merged the previous "problem statement" and "use case" sections into a mostly re-written "use cases" section, since they were overlapping.
- Clarified the relationship with draft-eckert-anima-stable-connectivity

12.5. version 03

- Took out requirement for IPv6 --> that’s in the reference doc.
- Added requirement section.
- Changed focus: more focus on autonomic functions, not only virtual out of band. This goes a bit throughout the document, starting with a changed abstract and intro.

13. References

[I-D.behringer-anima-reference-model]

[I-D.behringer-autonomic-control-plane]

[I-D.carpenter-anima-gdn-protocol]
[I-D.eckert-anima-stable-connectivity]  

[I-D.pritikin-anima-bootstrapping-keyinfra]  

[RFC4122]  

[RFC4193]  

[RFC7575]  

[RFC7576]  

Authors’ Addresses

Michael H. Behringer (editor)  
Cisco Systems  
Building D, 45 Allee des Ormes  
Mougins  06250  
France  
Email: mbehring@cisco.com

Steinthor Bjarnason  
Cisco  
Email: sbjarnas@cisco.com

Balaji BL  
Cisco  
Email: blbalaji@cisco.com
Abstract

The concept of fog computing has emerged driven by the Internet of Things (IoT) due to the need of handling the data generated from the end-user devices. The term fog is referred to any networked computational resource in the continuum between things and cloud. In fog computing, functions can be stitched together composing a service function chain. These functions might be hosted on resources that are inherently heterogeneous, volatile and mobile. This means that resources might appear and disappear, and the connectivity characteristics between these resources may also change dynamically. This calls for new orchestration solutions able to cope with dynamic changes to the resources in runtime or ahead of time (in anticipation through prediction) as opposed to today’s solutions which are inherently reactive and static or semi-static.

A fog monitoring solution can be used to help predicting events so an action can be taken before an event actually takes place. This solution is composed of agents running on the fog nodes plus a controller hosted at another device (running in the infrastructure or in another fog node). Since fog environments are inherently volatile and extremely dynamic, it is convenient to enable the use of autonomic technologies to autonomously set-up the fog monitoring platform. This document aims at presenting this use case as well as specifying how to use GRASP as needed in this scenario.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."
1. Introduction

The concept of fog computing has emerged driven by the Internet of Things (IoT) due to the need of handling the data generated from the end-user devices. The term fog is referred to any networked computational resource in the continuum between things and cloud. A fog node may therefore be an infrastructure network node such as an eNodeB or gNodeB, an edge server, a customer premises equipment (CPE), or even a user equipment (UE) terminal node such as a laptop, a smartphone, or a computing unit on-board a vehicle, robot or drone.

In fog computing, functions might be organized in service function chains (SFCs), hosted on resources that are inherently heterogeneous,
volatile and mobile. This means that resources might appear and disappear, and the connectivity characteristics between these resources may also change dynamically. This calls for new orchestration solutions able to cope with dynamic changes to the resources in runtime or ahead of time (in anticipation through prediction) as opposed to today’s solutions which are inherently reactive and static or semi-static.

1.1. Problem statement

Figure 1 shows an exemplary scenario of a (robot) network service. A robot device has its (navigation) control application running in the fog away from the robot, as a network service in the form of an SFC "F1-F2" (e.g., F1 might be in charge of identifying obstacles and F2 takes decisions on the robot navigation). Initially the function F1 is assumed to be hosted at a fog node A and F2 at fog node B. At a given point of time, fog node A becomes unavailable (e.g., due to low battery issues or the fog node A moving away from the coverage of the robot). There is therefore a need to predict the need of migrating/moving the function F1 to another node (e.g., fog node C in the figure), and this needs to be done prior to the fog/edge node becoming no longer capable/available. Such dynamic migration cannot be dealt with in today’s orchestration solutions, which are rather reactive and static or semi-static (e.g., resources may fail, but this is an exceptional event, happening with low frequency, and only scaling actions are supported to react to SLA-related events).

```
+-------+  +-------+
|      |  |      |
|      |  |      |
|      |  |      |
+-------+  +-------+
  |      |  |      |
  |      |  |      |
  |      |  |      |
  --------  --------
  |      |  |      |
  |      |  |      |
  |      |  |      |
+-------+  +-------+
  |      |  |      |
  |      |  |      |
  |      |  |      |
  --------  --------
    |      |  |      |
    |      |  |      |
    |      |  |      |
---0----0---
```

Figure 1: Example scenario
Existing frameworks rely on monitoring platforms that react to resource failure events and ensure that negotiated SLAs are met. However, these are not designed to predict events likely to happen in a volatile fog environment, such as resources moving away, resources becoming unavailable due to battery issues or just changes in availability of the resources because of variations of the use of the local resources on the nodes. Besides, it is not feasible in this kind of volatile and extremely mobile environment to perform a continuous monitoring and reporting of every possible parameter on all the nodes hosting resources, as this would not scale and would consume many resources and generate extra overhead.

In volatile and mobile environments, prediction (make-before-break) is needed, as pure reaction (break-before-make) is not enough. This prediction is not generic, and depends on the nature of the network service/SFC: the functions of the SFC, the connectivity between them, the service-specific requirements, etc. Monitoring has to be setup differently on the nodes, depending on the specifics of the network service. Besides, in order to act proactively and predict what might need to be done, monitoring in such a volatile and mobile environments does not only involve the nodes currently hosting the resources running the network service/service function chain (i.e., hosting a function), but also other nodes which are potential candidates to join either in addition or in substitution to current nodes for running the network service in accordance with the orchestration decisions.

In the example of Figure 1, the fog node initially hosting function F1 (fog node A) might be running out of battery and this should be detected before the node A actually becomes unavailable, so the function F1 can be effectively migrated in a time to a different fog node C, capable of meeting the requirements of F1 (compute, networking, location, expected availability, etc.). In order to be able to predict the need for such a migration and have already identified a target fog node where to move the function, it is needed to have a monitoring solution in place that instructs each node involved in the service (A and B), and also neighboring node candidate (C) to host function (F1), to monitor and report on metrics that are relevant for the specific network service "F1-F2" that is currently running.

1.2. Fog monitoring framework

Fog environments differ from data-center ones on three key aspects: heterogeneity, volatility and mobility. The fog monitoring framework is used to predict events triggering and orchestration event (e.g., migrating a function to a different resource).
The monitoring framework we propose for fog environments is composed of 2 logical components:

- Fog agents running on each fog node. An agent is responsible for sending information to a fog monitoring controller and to other fog agents. What to monitor and what information to send (including frequency) is configured per agent considering the specifics of the network service/SFC. A fog agent might also take some autonomous actions (such as request migration of a function to a neighbor node) in certain situations where connectivity with the fog monitoring controller is temporarily unavailable.

- A fog monitoring controller (e.g., running at the edge or at a fog node). This node obtains input from the orchestration logic (MANO stack) and autonomously decides what information to monitor, where and how, based on the requirements provided by the orchestration logic managing the network services instantiated in the fog. This configuration is network service/function specific.
  * It interacts with the orchestration logic to coordinate and trigger orchestration events, such as function migration, connectivity updates, etc. In some deployments, this entity might be co-located with the orchestration logic (e.g., the NFVO).
  * It interacts with the fog agents to instruct what information and parameters need to be monitored, as well as to obtain such information. This interaction is not limited to fog agents at nodes currently involved in a given network service/SFC, but also includes other nodes that are suitable for hosting a function that needs to be migrated. This allows to provide the orchestration logic with candidate nodes in a pro-active way.
  * It is capable of autonomously discover and set up fog agents.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The following terms are using in this document:

- fog: Fog goes to the Extreme Edge, that is the closest possible to the user including on the user device itself.
fog node: Any device that is capable of participating in the Fog. A Fog node might be volatile, mobile and constrained (in terms of computing resources). Fog nodes may be heterogeneous and may belong to different owners.

orchestrator: In this document we use orchestrator and NFVO terms interchangeably.

3. Autonomic setup of fog monitoring framework

Fog nodes autonomously start fog agents at the bootstrapping, then start looking for other agents and the fog monitoring controller. This autonomic setup can be performed using GRASP. The procedure is represented in Figure 2. The different steps are described next:
Figure 2: Autonomic setup of fog agents
The fog monitoring controller is regularly sending periodic multicast advertisement messages, which include its ID as well as the scope for the advertisement messages (i.e., the scope of where the messages have to be flooded).

M_DISCOVERY messages are used, with new objectives and objective options. GRASP specifies that "an objective option is used to identify objectives for the purposes of discovery, negotiation or synchronization". New objective options are defined for the purposes of discovering potential fog agents with certain characteristics. Non-limiting examples of these options are listed below (note that the names are just examples, and the ones used have to be registered by the IANA):

- FOGNODERADIO: used to specify a given type of radio technology, e.g., WiFi (version), D2D, LTE, 5G, Bluetooth (version), etc.
- FOGNODECONNECTIVITY: used to specify a given type of connectivity, e.g., layer-2, IPv4, IPv6.
- FOGNODEVIRTUALIZATION: used to specify a given type of virtualization supported by the node where the agent runs. Examples are: hypervisor (type), container, micro-kernel, bare-metal, etc.
- FOGNODEDOMAIN: used to specify the domain/owner of the node. This is useful to support operation of multiple domains/operators simultaneously on the same fog network.

An example of discovery message using GRASP would be the following (in this example, the fog monitoring controller is identified by its IPv6 address: 2001:DB8:1111:2222:3333:4444:5555:6666):

[M_DISCOVERY, 13948745, h'20010db8111122223333444455556666', "FOGDOMAIN", F_SYNCH_bits, 2, "operator1"]

GRASP is used to allow the fog agents and the controller discovery in an autonomic way. The extensions defined above, together with the use of properly scoped multicast addresses (as explained below), allow to precisely define which nodes participate in the monitoring and to gather their principal characteristics.

When a fog node bootstraps, such as nodes A and B in the figure, they start sending multicast discovery messages within a given scope, that is, the intended area that composes the fog. The definition of the scope depends on the scenario, and examples of possible scopes are:
* All-resources of a given manufacturer.
* All-resources of a given type.
* All-resources of a given administrative domain.
* All-resources of a given user.
* All-resources within a topological network distance (e.g., number of hops).
* All-resources within a geographical location.
* Etc.

Combination of previous scopes are also possible.

The discovery messages are multicast within the scope, reaching all the nodes that compose the specified fog resources. This can be done for example using well defined IPv6 multicast addresses, specified for each of the different scopes. This signaling is based on GRASP. Different IPv6 multicast addresses need to be defined to reach each different scope, using scopes equal or larger than Admin-Local according to [RFC7346].

- In response to multicast fog discovery messages, the fog monitoring controller replies with unicast information messages.

- Fog agents can then register with a controller. The registration message is unicast, and includes information on the capabilities of the fog node, such as:
  * Type of node.
  * Vendor.
  * Energy source: battery-powered or not.
  * Connectivity (number of network interfaces and information associated to them, such as radio technology type, layer-2 and layer-3 addresses, etc.).
  * Etc.

Note that registration to multiple fog monitoring controller instances could also be possible if a fog node wants to belong to several fog domains at the same time (but note that how the orchestration of the same resource is done by multiple
orchestrators is not covered by this invention). The defined mechanisms support this via the use of fog IDs and FOGNODEDOMAIN options.

- A fog node C bootstraps after nodes A and B are already registered. The same discovery process is followed by fog node C, but in addition to the regular advertisement, registration procedures described before, existing neighboring fog agents (such as A and B in this example), might also respond to discovery messages sent by bootstrapping nodes to provide required information. This makes the procedure faster, more efficient and reliable. In addition to helping the fog monitoring controller in the fog agent discovery process, fog agents learn themselves about the existence and associated capabilities of other fog agents. This can be used to allow autonomous monitoring by the fog agents without the involvement of the central controller.

4. IANA Considerations

TBD.

5. Security Considerations

TBD.

6. Acknowledgments

The work in this draft will be further developed and explored under the framework of the H2020 5G-CORAL project (Grant 761586).

7. References

7.1. Normative References


7.2. Informative References

Authors' Addresses

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/

Alain Mourad
InterDigital Europe

Email: Alain.Mourad@InterDigital.com
URI: http://www.InterDigital.com/
Guidelines for Autonomic Service Agents
draft-carpenter-anima-asa-guidelines-07

Abstract

This document proposes guidelines for the design of Autonomic Service Agents for autonomic networks. It is based on the Autonomic Network Infrastructure outlined in the ANIMA reference model, making use of the Autonomic Control Plane and the Generic Autonomic Signaling Protocol.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 8, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents.
carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.  Introduction ............................................. 2
2.  Logical Structure of an Autonomic Service Agent .......... 3
3.  Interaction with the Autonomic Networking Infrastructure .. 5
   3.1.  Interaction with the security mechanisms ............ 5
   3.2.  Interaction with the Autonomic Control Plane ........ 5
   3.3.  Interaction with GRASP and its API ................. 5
   3.4.  Interaction with policy mechanism .................. 6
4.  Interaction with Non-Autonomic Components ................ 7
5.  Design of GRASP Objectives .............................. 7
6.  Life Cycle ................................................. 8
   6.1.  Installation phase ..................................... 9
      6.1.1.  Installation phase inputs and outputs .......... 10
   6.2.  Instantiation phase .................................... 10
      6.2.1.  Operator’s goal ................................... 11
      6.2.2.  Instantiation phase inputs and outputs ........ 11
      6.2.3.  Instantiation phase requirements ............... 12
   6.3.  Operation phase ....................................... 12
7.  Coordination between Autonomic Functions .................. 13
8.  Coordination with Traditional Management Functions ........ 13
9.  Robustness ............................................... 14
10. Security Considerations .................................... 15
11. IANA Considerations ....................................... 15
12. Acknowledgements ......................................... 15
13. References ................................................. 15
   13.1.  Normative References ................................. 15
   13.2.  Informative References .............................. 16
Appendix A.  Change log [RFC Editor: Please remove] .......... 18
Appendix B.  Example Logic Flows ............................. 19
Authors’ Addresses ........................................... 24

1.  Introduction

This document proposes guidelines for the design of Autonomic Service Agents (ASAs) in the context of an Autonomic Network (AN) based on the Autonomic Network Infrastructure (ANI) outlined in the ANIMA reference model [I-D.ietf-anima-reference-model]. This infrastructure makes use of the Autonomic Control Plane (ACP) [I-D.ietf-anima-autonomic-control-plane] and the Generic Autonomic Signaling Protocol (GRASP) [I-D.ietf-anima-grasp].
There is a considerable literature about autonomic agents with a variety of proposals about how they should be characterized. Some examples are [DeMola06], [Huebscher08], [Movahedi12] and [GANA13]. However, for the present document, the basic definitions and goals for autonomic networking given in [RFC7575] apply. According to RFC 7575, an Autonomic Service Agent is "An agent implemented on an autonomic node that implements an autonomic function, either in part (in the case of a distributed function) or whole."

ASAs must be distinguished from other forms of software component. They are components of network or service management; they do not in themselves provide services. For example, the services envisaged for network function virtualisation [RFC8568] or for service function chaining [RFC7665] might be managed by an ASA rather than by traditional configuration tools.

The reference model [I-D.ietf-anima-reference-model] expands this by adding that an ASA is "a process that makes use of the features provided by the ANI to achieve its own goals, usually including interaction with other ASAs via the GRASP protocol [I-D.ietf-anima-grasp] or otherwise. Of course it also interacts with the specific targets of its function, using any suitable mechanism. Unless its function is very simple, the ASA will need to handle overlapping asynchronous operations. This will require either a multi-threaded implementation, or a logically equivalent event loop structure. It may therefore be a quite complex piece of software in its own right, forming part of the application layer above the ANI."

There will certainly be very simple ASAs that manage a single objective in a straightforward way and do not asynchronous operations. In such a case, many aspects of the current document do not apply. However, in general a basic property of an ASA is that it is a relatively complex software component that will in many cases control and monitor simpler entities in the same host or elsewhere. For example, a device controller that manages tens or hundreds of simple devices might contain a single ASA.

The remainder of this document offers guidance on the design of such ASAs.

2. Logical Structure of an Autonomic Service Agent

As mentioned above, all but the simplest ASAs will need to support asynchronous operations. Not all programming environments explicitly support multi-threading. In that case, an ‘event loop’ style of implementation should be adopted, in which case each thread would be implemented as an event handler called in turn by the main loop. For this, the GRASP API (Section 3.3) must provide non-blocking calls.
If necessary, the GRASP session identifier will be used to distinguish simultaneous operations.

A typical ASA will have a main thread that performs various initial housekeeping actions such as:

- Obtain authorization credentials.
- Register the ASA with GRASP.
- Acquire relevant policy parameters.
- Define data structures for relevant GRASP objectives.
- Register with GRASP those objectives that it will actively manage.
- Launch a self-monitoring thread.
- Enter its main loop.

The logic of the main loop will depend on the details of the autonomic function concerned. Whenever asynchronous operations are required, extra threads will be launched, or events added to the event loop. Examples include:

- Repeatedly flood an objective to the AN, so that any ASA can receive the objective’s latest value.
- Accept incoming synchronization requests for an objective managed by this ASA.
- Accept incoming negotiation requests for an objective managed by this ASA, and then conduct the resulting negotiation with the counterpart ASA.
- Manage subsidiary non-autonomic devices directly.

These threads or events should all either exit after their job is done, or enter a wait state for new work, to avoid blocking others unnecessarily.

According to the degree of parallelism needed by the application, some of these threads or events might be launched in multiple instances. In particular, if negotiation sessions with other ASAs are expected to be long or to involve wait states, the ASA designer might allow for multiple simultaneous negotiating threads, with appropriate use of queues and locks to maintain consistency.
The main loop itself could act as the initiator of synchronization requests or negotiation requests, when the ASA needs data or resources from other ASAs. In particular, the main loop should watch for changes in policy parameters that affect its operation. It should also do whatever is required to avoid unnecessary resource consumption, such as including an arbitrary wait time in each cycle of the main loop.

The self-monitoring thread is of considerable importance. Autonomic service agents must never fail. To a large extent this depends on careful coding and testing, with no unhandled error returns or exceptions, but if there is nevertheless some sort of failure, the self-monitoring thread should detect it, fix it if possible, and in the worst case restart the entire ASA.

Appendix B presents some example logic flows in informal pseudocode.

3. Interaction with the Autonomic Networking Infrastructure

3.1. Interaction with the security mechanisms

An ASA by definition runs in an autonomic node. Before any normal ASAs are started, such nodes must be bootstrapped into the autonomic network’s secure key infrastructure in accordance with [I-D.ietf-anima-bootstrapping-keyinfra]. This key infrastructure will be used to secure the ACP (next section) and may be used by ASAs to set up additional secure interactions with their peers, if needed.

Note that the secure bootstrap process itself may include special-purpose ASAs that run in a constrained insecure mode.

3.2. Interaction with the Autonomic Control Plane

In a normal autonomic network, ASAs will run as clients of the ACP. It will provide a fully secured network environment for all communication with other ASAs, in most cases mediated by GRASP (next section).

Note that the ACP formation process itself may include special-purpose ASAs that run in a constrained insecure mode.

3.3. Interaction with GRASP and its API

GRASP [I-D.ietf-anima-grasp] is expected to run as a separate process with its API [I-D.ietf-anima-grasp-api] available in user space. Thus ASAs may operate without special privilege, unless they need it for other reasons. The ASA’s view of GRASP is built around GRASP objectives (Section 5), defined as data structures containing
administrative information such as the objective’s unique name, and
its current value. The format and size of the value is not
restricted by the protocol, except that it must be possible to
serialise it for transmission in CBOR [RFC7049], which is no
restriction at all in practice.

The GRASP API should offer the following features:

o Registration functions, so that an ASA can register itself and the
  objectives that it manages.

o A discovery function, by which an ASA can discover other ASAs
  supporting a given objective.

o A negotiation request function, by which an ASA can start
  negotiation of an objective with a counterpart ASA. With this,
  there is a corresponding listening function for an ASA that wishes
  to respond to negotiation requests, and a set of functions to
  support negotiating steps.

o A synchronization function, by which an ASA can request the
  current value of an objective from a counterpart ASA. With this,
  there is a corresponding listening function for an ASA that wishes
  to respond to synchronization requests.

o A flood function, by which an ASA can cause the current value of
  an objective to be flooded throughout the AN so that any ASA can
  receive it.

For further details and some additional housekeeping functions, see
[I-D.ietf-anima-grasp-api].

This API is intended to support the various interactions expected
between most ASAs, such as the interactions outlined in Section 2. However, if ASAs require additional communication between themselves,
they can do so using any desired protocol. One option is to use
GRASP discovery and synchronization as a rendez-vous mechanism
between two ASAs, passing communication parameters such as a TCP port
number via GRASP. As noted above, either the ACP or in special cases
the autonomic key infrastructure will be used to secure such
communications.

3.4. Interaction with policy mechanism

At the time of writing, the policy (or "Intent") mechanism for the
ANI is undefined. It is expected to operate by an information
distribution mechanism that can reach all autonomic nodes, and
therefore every ASA. However, each ASA must be capable of operating
"out of the box" in the absence of locally defined policy, so every ASA implementation must include carefully chosen default values and settings for all policy parameters.

4. Interaction with Non-Autonomic Components

An ASA, to have any external effects, must also interact with non-autonomic components of the node where it is installed. For example, an ASA whose purpose is to manage a resource must interact with that resource. An ASA whose purpose is to manage an entity that is already managed by local software must interact with that software. This is stating the obvious, and the details are specific to each case, but it has an important security implication. The ASA might act as a loophole by which the managed entity could penetrate the security boundary of the ANI. The ASA must be designed to avoid such loopholes, and should if possible operate in an unprivileged mode.

In an environment where systems are virtualized and specialized using techniques such as network function virtualization or network slicing, there will be a design choice whether ASAs are deployed once per physical node or once per virtual context. A related issue is whether the ANI as a whole is deployed once on a physical network, or whether several virtual ANIs are deployed. This aspect needs to be considered by the ASA designer.

5. Design of GRASP Objectives

The general rules for the format of GRASP Objective options, their names, and IANA registration are given in [I-D.ietf-anima-grasp]. Additionally that document discusses various general considerations for the design of objectives, which are not repeated here. However, we emphasize that the GRASP protocol does not provide transactional integrity. In other words, if an ASA is capable of overlapping several negotiations for a given objective, then the ASA itself must use suitable locking techniques to avoid interference between these negotiations. For example, if an ASA is allocating part of a shared resource to other ASAs, it needs to ensure that the same part of the resource is not allocated twice. This might impact the design of the objective as well as the logic flow of the ASA.

In particular, if 'dry run' mode is defined for the objective, its specification, and every implementation, must consider what state needs to be saved following a dry run negotiation, such that a subsequent live negotiation can be expected to succeed. It must be clear how long this state is kept, and what happens if the live negotiation occurs after this state is deleted. An ASA that requests a dry run negotiation must take account of the possibility that a successful dry run is followed by a failed live negotiation. Because
of these complexities, the dry run mechanism should only be supported by objectives and ASAs where there is a significant benefit from it.

The actual value field of an objective is limited by the GRASP protocol definition to any data structure that can be expressed in Concise Binary Object Representation (CBOR) [RFC7049]. For some objectives, a single data item will suffice; for example an integer, a floating point number or a UTF-8 string. For more complex cases, a simple tuple structure such as [item1, item2, item3] could be used. Nothing prevents using other formats such as JSON, but this requires the ASA to be capable of parsing and generating JSON. The formats acceptable by the GRASP API will limit the options in practice. A fallback solution is for the API to accept and deliver the value field in raw CBOR, with the ASA itself encoding and decoding it via a CBOR library.

Note that a mapping from YANG to CBOR is defined by [I-D.ietf-core-yang-cbor]. Subject to the size limit defined for GRASP messages, nothing prevents objectives using YANG in this way.

6. Life Cycle

Autonomic functions could be permanent, in the sense that ASAs are shipped as part of a product and persist throughout the product’s life. However, a more likely situation is that ASAs need to be installed or updated dynamically, because of new requirements or bugs. Because continuity of service is fundamental to autonomic networking, the process of seamlessly replacing a running instance of an ASA with a new version needs to be part of the ASA’s design.

The implication of service continuity on the design of ASAs can be illustrated along the three main phases of the ASA life-cycle, namely Installation, Instantiation and Operation.
6.1. Installation phase

Before being able to instantiate and run ASAs, the operator must first provision the infrastructure with the sets of ASA software corresponding to its needs and objectives. The provisioning of the infrastructure is realized in the installation phase and consists in installing (or checking the availability of) the pieces of software of the different ASA classes in a set of Installation Hosts.

There are 3 properties applicable to the installation of ASAs:

The dynamic installation property allows installing an ASA on demand, on any hosts compatible with the ASA.

The decoupling property allows controlling resources of a NE from a remote ASA, i.e. an ASA installed on a host machine different from the resources’ NE.

The multiplicity property allows controlling multiple sets of resources from a single ASA.

These three properties are very important in the context of the installation phase as their variations condition how the ASA class could be installed on the infrastructure.
6.1.1. Installation phase inputs and outputs

Inputs are:

[ASA class of type_x] that specifies which classes ASAs to install,

[Installation_target_Infrastructure] that specifies the candidate Installation Hosts,

[ASA class placement function, e.g. under which criteria/constraints as defined by the operator] that specifies how the installation phase shall meet the operator’s needs and objectives for the provision of the infrastructure. In the coupled mode, the placement function is not necessary, whereas in the decoupled mode, the placement function is mandatory, even though it can be as simple as an explicit list of Installation hosts.

The main output of the installation phase is an up-to-date directory of installed ASAs which corresponds to [list of ASA classes] installed on [list of installation Hosts]. This output is also useful for the coordination function and corresponds to the static interaction map (see next section).

The condition to validate in order to pass to next phase is to ensure that [list of ASA classes] are well installed on [list of installation Hosts]. The state of the ASA at the end of the installation phase is: installed. (not instantiated). The following commands or messages are foreseen: install(list of ASA classes, Installation_target_Infrastructure, ASA class placement function), and un-install (list of ASA classes).

6.2. Instantiation phase

Once the ASAs are installed on the appropriate hosts in the network, these ASA may start to operate. From the operator viewpoint, an operating ASA means the ASA manages the network resources as per the objectives given. At the ASA local level, operating means executing their control loop/algorithm.

But right before that, there are two things to take into consideration. First, there is a difference between 1. having a piece of code available to run on a host and 2. having an agent based on this piece of code running inside the host. Second, in a coupled case, determining which resources are controlled by an ASA is straightforward (the determination is embedded), in a decoupled mode determining this is a bit more complex (hence a starting agent will have to either discover or be taught it).
The instantiation phase of an ASA covers both these aspects: starting the agent piece of code (when this does not start automatically) and determining which resources have to be controlled (when this is not obvious).

6.2.1. Operator’s goal

Through this phase, the operator wants to control its autonomic network in two things:

1. determine the scope of autonomic functions by instructing which of the network resources have to be managed by which autonomic function (and more precisely which class e.g. 1. version X or version Y or 2. provider A or provider B),

2. determine how the autonomic functions are organized by instructing which ASAs have to interact with which other ASAs (or more precisely which set of network resources have to be handled as an autonomous group by their managing ASAs).

Additionally in this phase, the operator may want to set objectives to autonomic functions, by configuring the ASAs technical objectives.

The operator’s goal can be summarized in an instruction to the ANIMA ecosystem matching the following pattern:

[ASA of type_x instances] ready to control [Instantiation_target_Infrastructure] with [Instantiation_target_parameters]

6.2.2. Instantiation phase inputs and outputs

Inputs are:

[ASA of type_x instances] that specifies which are the ASAs to be targeted (and more precisely which class e.g. 1. version X or version Y or 2. provider A or provider B),

[Instantiation_target_Infrastructure] that specifies which are the resources to be managed by the autonomic function, this can be the whole network or a subset of it like a domain a technology segment or even a specific list of resources,

[Instantiation_target_parameters] that specifies which are the technical objectives to be set to ASAs (e.g. an optimization target)

Outputs are:
[Set of ASAs - Resources relations] describing which resources are managed by which ASA instances, this is not a formal message, but a resulting configuration of a set of ASAs.

6.2.3. Instantiation phase requirements

The instructions described in section 4.2 could be either:

- sent to a targeted ASA In which case, the receiving Agent will have to manage the specified list of [Instantiation_target_Infrastructure], with the [Instantiation_target_parameters].

- broadcast to all ASAs In which case, the ASAs would collectively determine from the list which Agent(s) would handle which [Instantiation_target_Infrastructure], with the [Instantiation_target_parameters].

This set of instructions can be materialized through a message that is named an Instance Mandate (description TBD).

The conclusion of this instantiation phase is a ready to operate ASA (or interacting set of ASAs), then this (or those) ASA(s) can describe themselves by depicting which are the resources they manage and what this means in terms of metrics being monitored and in terms of actions that can be executed (like modifying the parameters values). A message conveying such a self description is named an Instance Manifest (description TBD).

Though the operator may well use such a self-description "per se", the final goal of such a description is to be shared with other ANIMA entities like:

- the coordination entities (see [I-D.ciavaglia-anima-coordination] - Autonomic Functions Coordination)
- collaborative entities in the purpose of establishing knowledge exchanges (some ASAs may produce knowledge or even monitor metrics that other ASAs cannot make by themselves why those would be useful for their execution)

6.3. Operation phase

Note: This section is to be further developed in future revisions of the document, especially the implications on the design of ASAs.

During the Operation phase, the operator can:
Activate/Deactivate ASA: meaning enabling those to execute their autonomic loop or not.

Modify ASAs targets: meaning setting them different objectives.

Modify ASAs managed resources: by updating the instance mandate which would specify different set of resources to manage (only applicable to decouples ASAs).

During the Operation phase, running ASAs can interact the one with the other:

in order to exchange knowledge (e.g. an ASA providing traffic predictions to load balancing ASA)

in order to collaboratively reach an objective (e.g. ASAs pertaining to the same autonomic function targeted to manage a network domain, these ASA will collaborate - in the case of a load balancing one, by modifying the links metrics according to the neighboring resources loads)

During the Operation phase, running ASAs are expected to apply coordination schemes

then execute their control loop under coordination supervision/instructions

The ASA life-cycle is discussed in more detail in "A Day in the Life of an Autonomic Function" [I-D.peloso-anima-autonomic-function].

7. Coordination between Autonomic Functions

Some autonomic functions will be completely independent of each other. However, others are at risk of interfering with each other - for example, two different optimization functions might both attempt to modify the same underlying parameter in different ways. In a complete system, a method is needed of identifying ASAs that might interfere with each other and coordinating their actions when necessary. This issue is considered in "Autonomic Functions Coordination" [I-D.ciavaglia-anima-coordination].

8. Coordination with Traditional Management Functions

Some ASAs will have functions that overlap with existing configuration tools and network management mechanisms such as command line interfaces, DHCP, DHCPv6, SNMP, NETCONF, RESTCONF and YANG-based solutions. Each ASA designer will need to consider this issue and how to avoid clashes and inconsistencies. Some specific
considerations for interaction with OAM tools are given in [RFC8368].
As another example, [I-D.ietf-anima-prefix-management] describes how
autonomic management of IPv6 prefixes can interact with prefix
delegation via DHCPv6. The description of a GRASP objective and of
an ASA using it should include a discussion of any such interactions.

A related aspect is that management functions often include a data
model, quite likely to be expressed in a formal notation such as
YANG. This aspect should not be an afterthought in the design of an
ASA. To the contrary, the design of the ASA and of its GRASP
objectives should match the data model; as noted above, YANG
serialized as CBOR may be used directly as the value of a GRASP
objective.

9. Robustness

   It is of great importance that all components of an autonomic system
   are highly robust. In principle they must never fail. This section
   lists various aspects of robustness that ASA designers should
   consider.

1. If despite all precautions, an ASA does encounter a fatal error,
   it should in any case restart automatically and try again. To
   mitigate a hard loop in case of persistent failure, a suitable
   pause should be inserted before such a restart. The length of
   the pause depends on the use case.

2. If a newly received or calculated value for a parameter falls out
   of bounds, the corresponding parameter should be either left
   unchanged or restored to a safe value.

3. If a GRASP synchronization or negotiation session fails for any
   reason, it may be repeated after a suitable pause. The length of
   the pause depends on the use case.

4. If a session fails repeatedly, the ASA should consider that its
   peer has failed, and cause GRASP to flush its discovery cache and
   repeat peer discovery.

5. Any received GRASP message should be checked. If it is wrongly
   formatted, it should be ignored. Within a unicast session, an
   Invalid message (M_INVALID) may be sent. This function may be
   provided by the GRASP implementation itself.

6. Any received GRASP objective should be checked. If it is wrongly
   formatted, it should be ignored. Within a negotiation session, a
   Negotiation End message (M_END) with a Decline option (O_DECLINE)
should be sent. An ASA may log such events for diagnostic purposes.

7. If an ASA receives either an Invalid message (M_INVALID) or a Negotiation End message (M_END) with a Decline option (O_DECLINE), one possible reason is that the peer ASA does not support a new feature of either GRASP or of the objective in question. In such a case the ASA may choose to repeat the operation concerned without using that new feature.

8. All other possible exceptions should be handled in an orderly way. There should be no such thing as an unhandled exception (but see point 1 above).

10. Security Considerations

ASAs are intended to run in an environment that is protected by the Autonomic Control Plane [I-D.ietf-anima-autonomic-control-plane], admission to which depends on an initial secure bootstrap process [I-D.ietf-anima-bootstrapping-keyinfra]. In some deployments, a secure partition of the link layer might be used instead [I-D.carpenter-anima-l2acp-scenarios]. However, this does not relieve ASAs of responsibility for security. In particular, when ASAs configure or manage network elements outside the ACP, they must use secure techniques and carefully validate any incoming information. As appropriate to their specific functions, ASAs should take account of relevant privacy considerations [RFC6973].

Authorization of ASAs is a subject for future study. At present, ASAs are trusted by virtue of being installed on a node that has successfully joined the ACP.

11. IANA Considerations

This document makes no request of the IANA.

12. Acknowledgements

Useful comments were received from Toerless Eckert, Alex Galis, Bing Liu, and other members of the ANIMA WG.

13. References

13.1. Normative References
[I-D.ietf-anima-autonomic-control-plane]

[I-D.ietf-anima-bootstrapping-keyinfra]

[I-D.ietf-anima-grasp]


13.2. Informative References

[DeMola06]

[GANA13]

[Huebscher08]

[I-D.carpenter-anima-l2acp-scenarios]
Carpenter, B. and B. Liu, "Scenarios and Requirements for Layer 2 Autonomic Control Planes", draft-carpenter-anima-l2acp-scenarios-00 (work in progress), February 2019.


Appendix A. Change log [RFC Editor: Please remove]

draft-carpenter-anima-asa-guidelines-07, 2019-07-17:
Improved explanation of threading vs event-loop
Other editorial improvements.
draft-carpenter-anima-asa-guidelines-06, 2018-01-07:
Expanded and improved example logic flow.
Editorial corrections.
draft-carpenter-anima-asa-guidelines-05, 2018-06-30:
Added section on relationship with non-autonomic components.
Editorial corrections.
draft-carpenter-anima-asa-guidelines-04, 2018-03-03:
Added note about simple ASAs.
Added note about NFV/SFC services.
Improved text about threading v event loop model
Added section about coordination with traditional tools.
Added appendix with example logic flow.
draft-carpenter-anima-asa-guidelines-03, 2017-10-25:
Added details on life cycle.
Added details on robustness.
Added co-authors.
draft-carpenter-anima-asa-guidelines-02, 2017-07-01:
Expanded description of event-loop case.
Added note about ‘dry run’ mode.
draft-carpenter-anima-asa-guidelines-01, 2017-01-06:
More sections filled in
draft-carpenter-anima-asa-guidelines-00, 2016-09-30:
Initial version

Appendix B. Example Logic Flows

This appendix describes generic logic flows for an Autonomic Service Agent (ASA) for resource management. Note that these are illustrative examples, and in no sense requirements. As long as the rules of GRASP are followed, a real implementation could be different. The reader is assumed to be familiar with GRASP [I-D.ietf-anima-grasp] and its conceptual API [I-D.ietf-anima-grasp-api].

A complete autonomic function for a resource would consist of a number of instances of the ASA placed at relevant points in a network. Specific details will of course depend on the resource concerned. One example is IP address prefix management, as specified in [I-D.ietf-anima-prefix-management]. In this case, an instance of the ASA would exist in each delegating router.

An underlying assumption is that there is an initial source of the resource in question, referred to here as a master ASA. The other ASAs, known as delegators, obtain supplies of the resource from the
master, and then delegate quantities of the resource to consumers that request it, and recover it when no longer needed.

Another assumption is there is a set of network wide policy parameters, which the master will provide to the delegators. These parameters will control how the delegators decide how much resource to provide to consumers. Thus the ASA logic has two operating modes: master and delegator. When running as a master, it starts by obtaining a quantity of the resource from the NOC, and it acts as a source of policy parameters, via both GRASP flooding and GRASP synchronization. (In some scenarios, flooding or synchronization alone might be sufficient, but this example includes both.)

When running as a delegator, it starts with an empty resource pool, it acquires the policy parameters by GRASP synchronization, and it delegates quantities of the resource to consumers that request it. Both as a master and as a delegator, when its pool is low it seeks quantities of the resource by requesting GRASP negotiation with peer ASAs. When its pool is sufficient, it hands out resource to peer ASAs in response to negotiation requests. Thus, over time, the initial resource pool held by the master will be shared among all the delegators according to demand.

In theory a network could include any number of masters and any number of delegators, with the only condition being that each master's initial resource pool is unique. A realistic scenario is to have exactly one master and as many delegators as you like. A scenario with no master is useless.

An implementation requirement is that resource pools are kept in stable storage. Otherwise, if a delegator exits for any reason, all the resources it has obtained or delegated are lost. If a master exits, its entire spare pool is lost. The logic for using stable storage and for crash recovery is not included below.

The description below does not implement GRASP’s 'dry run' function. That would require temporarily marking any resource handed out in a dry run negotiation as reserved, until either the peer obtains it in a live run, or a suitable timeout expires.

The main data structures used in each instance of the ASA are:

- The resource_pool, for example an ordered list of available resources. Depending on the nature of the resource, units of resource are split when appropriate, and a background garbage collector recombines split resources if they are returned to the pool.
o The delegated_list, where a delegator stores the resources it has given to consumers routers.

Possible main logic flows are below, using a threaded implementation model. The transformation to an event loop model should be apparent - each thread would correspond to one event in the event loop.

The GRASP objectives are as follows:

["EX1.Resource", flags, loop_count, value] where the value depends on the resource concerned, but will typically include its size and identification.

["EX1.Params", flags, loop_count, value] where the value will be, for example, a JSON object defining the applicable parameters.

In the outline logic flows below, these objectives are represented simply by their names.
MAIN PROGRAM:

Create empty resource_pool (and an associated lock)
Create empty delegated_list
Determine whether to act as master
if master:
   Obtain initial resource_pool contents from NOC
   Obtain value of EX1.Params from NOC
Register ASA with GRASP
Register GRASP objectives EX1.Resource and EX1.Params
if master:
   Start FLOODER thread to flood EX1.Params
   Start SYNCHRONIZER listener for EX1.Params
Start MAIN_NEGOTIATOR thread for EX1.Resource
if not master:
   Obtain value of EX1.Params from GRASP flood or synchronization
Start DELEGATOR thread
Start GARBAGE_COLLECTOR thread

do forever:
   good_peer = none
   if resource_pool is low:
      Calculate amount A of resource needed
      Discover peers using GRASP M_DISCOVER / M_RESPONSE
      if good_peer in peers:
         peer = good_peer
      else:
         peer = #any choice among peers
         grasp.request_negotiate("EX1.Resource", peer)
         i.e., send M_REQ_NEG
         Wait for response (M_NEGOTIATE, M_END or M_WAIT)
         if OK:
            if offered amount of resource sufficient:
               Send M_END + O_ACCEPT #negotiation succeeded
               Add resource to pool
               good_peer = peer
            else:
               Send M_END + O_DECLINE #negotiation failed
               sleep() #sleep time depends on application scenario
   MAIN_NEGOTIATOR thread:

do forever:
   grasp.listen_negotiate("EX1.Resource")
   i.e., wait for M_REQ_NEG
   Start a separate new NEGOTIATOR thread for requested amount A
NEGOTIATOR thread:

Request resource amount A from resource_pool
if not OK:
    while not OK and A > Amin:
        A = A - 1
        Request resource amount A from resource_pool
if OK:
    Offer resource amount A to peer by GRASP M_NEGOTIATE
    if received M_END + O_ACCEPT:
        #negotiation succeeded
    elif received M_END + O_DECLINE or other error:
        #negotiation failed
else:
    Send M_END + O_DECLINE #negotiation failed

DELEGATOR thread:

do forever:
    Wait for request or release for resource amount A
    if request:
        Get resource amount A from resource_pool
        if OK:
            Delegate resource to consumer
            Record in delegated_list
        else:
            Signal failure to consumer
            Signal main thread that resource_pool is low
    else:
        Delete resource from delegated_list
        Return resource amount A to resource_pool

SYNCHRONIZER thread:

do forever:
    Wait for M_REQ_SYN message for EX1.Params
    Reply with M_SYNCH message for EX1.Params

FLOODER thread:

do forever:
    Send M_FLOOD message for EX1.Params
    sleep() #sleep time depends on application scenario
GARBAGE_COLLECTOR thread:

do forever:
    Search resource_pool for adjacent resources
    Merge adjacent resources
    sleep()  #sleep time depends on application scenario

Authors’ Addresses

Brian Carpenter
School of Computer Science
University of Auckland
PB 92019
Auckland 1142
New Zealand

Email: brian.e.carpenter@gmail.com

Laurent Ciavaglia
Nokia
Villarceaux
Nozay 91460
FR

Email: laurent.ciavaglia@nokia.com

Sheng Jiang
Huawei Technologies Co., Ltd
Q14, Huawei Campus, No.156 Beiqing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: jiangsheng@huawei.com

Pierre Peloso
Nokia
Villarceaux
Nozay 91460
FR

Email: pierre.peloso@nokia.com
Transferring Bulk Data over the GeneRic Autonomic Signaling Protocol (GRASP)
draft-carpenter-anima-grasp-bulk-04

Abstract

This document describes how bulk data may be transferred between Autonomic Service Agents via the GeneRic Autonomic Signaling Protocol (GRASP). Although not an equivalent of a file transfer protocol, such a technique may be used for non-urgent transfer of data too large to fit into a normal GRASP message.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 4, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1.  Introduction .......................... 2
2.  General Method for Bulk Transfer ......... 3
3.  Example for File Transfer ................ 4
4.  Loss Detection ........................ 7
5.  Maximum Transmission Unit ............... 8
6.  Pipelining ................................ 8
7.  Other Considerations ..................... 8
8.  Possible Future Work ...................... 9
9.  Implementation Status [RFC Editor: please remove] .... 9
10. Security Considerations .................. 9
11. IANA Considerations ...................... 9
12. Acknowledgements ........................ 9
13. References ............................. 10
13.1. Normative References ................. 10
13.2. Informative References ............... 10
Appendix A. Change log [RFC Editor: Please remove] ........ 11
Authors’ Addresses ........................ 11

1. Introduction

The document [I-D.liu-anima-grasp-distribution] discusses how
information may be distributed within the secure Autonomic Networking
Infrastructure (ANI) [I-D.ietf-anima-reference-model]. Specifically,
it describes using the Synchronization and Flood Synchronization
mechanisms of the GeneRic Autonomic Signaling Protocol (GRASP)
[I-D.ietf-anima-grasp] for this purpose. However, those mechanisms
are limited to distributing GRASP Objective Options contained in
messages that cannot exceed the GRASP maximum message size of 2048
bytes. This places a limit on the size of data that can be
transferred in a Synchronization or Flood operation.

There are scenarios in autonomic networks where this restriction is a
problem. One example is the distribution of network policy in
lengthy formats such as YANG or JSON. Another case might be an
Autonomic Service Agent (ASA) uploading a log file to the Network
Operations Center (NOC). A third case might be a supervisory system
downloading a software upgrade to an autonomic node. A related case
might be installing the code of a new or updated ASA to a target node
(see the discussion of ASA life cycles in
[I-D.carpenter-anima-asa-guidelines]).
Naturally, an existing solution such as a secure file transfer protocol or secure HTTP might be used for this. Other management protocols such as syslog [RFC5424] or NETCONF [RFC6241] might also be used for related purposes, or might be mapped directly over GRASP. The present document, however, applies to any scenario where it is preferable to re-use the autonomic networking infrastructure itself to transfer a significant amount of data, rather than install and configure an additional mechanism. The basic model is to use the GRASP Negotiation process to transfer and acknowledge multiple blocks of data in successive negotiation steps, thereby overcoming the GRASP message size limitation.

The emphasis is placed on simplicity rather than efficiency, high throughput, or advanced functionality. For example, if a transfer gets out of step or data packets are lost, the strategy is to abort the transfer and try again. In an enterprise network with low bit error rates, and with GRASP running over TCP, this is not considered a serious issue. Clearly, a more sophisticated approach could be designed but if the application requires that, existing protocols could be used, as indicated in the preceding paragraph.

This is an informational description of a class of solutions. Standards track solutions could be published as detailed specifications of the corresponding GRASP objectives.

2. General Method for Bulk Transfer

As for any GRASP operation, the two participants are considered to be Autonomic Service Agents (ASAs) and they communicate using a specific GRASP Objective Option, containing its own name, some flag bits, a loop count, and a value. In bulk transfer, we can model the ASA acting as the source of the transfer as a download server, and the destination as a download client. No changes or extensions are required to GRASP itself, but compared to a normal GRASP negotiation, the communication pattern is slightly asymmetric:

1. The client first discovers the server by the GRASP discovery mechanism (M_DISCOVERY and M_RESPONSE messages).

2. The client then sends a GRASP negotiation request (M_REQ_NEG message). The value of the objective expresses the requested item (e.g., a file name - see the next section for a detailed example).

3. The server replies with a negotiation step (M_NEGOTIATE message). The value of the objective is the first section of the requested item (e.g., the first block of the requested file as a raw byte string).
4. The client replies with a negotiation step (M_NEGOTIATE message). The value of the objective is a simple acknowledgement (e.g., the text string ‘ACK’).

The last two steps repeat until the transfer is complete. The server signals the end by transferring an empty byte string as the final value. In this case the client responds with a normal end to the negotiation (M_END message with an O_ACCEPT option).

Errors of any kind are handled with the normal GRASP mechanisms, in particular by an M_END message with an O_DECLINE option in either direction.

The block size must be chosen such that each step does not exceed the GRASP message size limit of 2048 bits.

This approach is safe since each block must be positively acknowledged, and data transfer errors will be detected by TCP. If a future variant of GRASP runs over UDP, the mandatory UDP checksum for IPv6 will detect such errors. The method does not specify retransmission for failed blocks, so a failed transfer will need to be restarted.

An observant reader will notice that the GRASP loop count mechanism, intended to terminate endless negotiations, will cause a problem for large transfers. For this reason, both the client and server must artificially increment the loop count by 1 before each negotiation step, cancelling out the normal decrement at each step.

If network load is a concern, the data rate can be limited by inserting a delay before each negotiation step, with the GRASP timeout set accordingly. Either the server or the client, or both, could insert such a delay. Also, either side could use the GRASP Confirm Waiting (M_WAIT) message to slow the other side down.

The description above concerns bulk download from a server (responding ASA) to a client (requesting ASA). The data transfer could also be in the opposite (upload) direction with minor modifications to the procedure: the client would send the file name and the data blocks, and the server would send acknowledgements.

3. Example for File Transfer

This example describes a client ASA requesting a file download from a server ASA.

Firstly we define a GRASP objective informally:
The formal CDDL definition [RFC8610] is:

```
mvfile-objective = ["411:mvFile", objective-flags, loop-count, value]
objective-flags = ; as in the GRASP specification
loop-count = ; as in the GRASP specification
value = any
```

The objective-flags field is set to indicate negotiation.

Dry run mode must not be used.

The loop-count is set to a suitable value to limit the scope of discovery. A suggested default value is 6.

The value takes the following forms:

- In the initial request from the client, a UTF-8 string containing the requested file name (with file path if appropriate).

- In negotiation steps from the server, a byte string containing at most 1024 bytes. However:
  - If the file does not exist, the first negotiation step will return an M_END, O_DECLINE response.
  - After sending the last block, the next and final negotiation step will send an empty byte string as the value.

- In negotiation steps from the client, the value is the UTF-8 string 'ACK'.

Note that the block size of 1024 is chosen to guarantee not only that each GRASP message is below the size limit, but also that only one TCP data packet will be needed, even on an IPv6 network with a minimum link MTU.

We now present outline pseudocode for the client and the server ASA. The API documented in [I-D.ietf-anima-grasp-api] is used in a simplified way, and error handling is not shown in detail.
Pseudo code for client ASA (request and receive a file):

requested_obj = objective('411:mvFile')
locator = discover(requested_obj)
requested_obj.value = 'etc/test.pdf'
received_obj = request_negotiate(requested_obj, locator)
if error_code == declined:
    #no such file
    exit

file = open(requested_obj.value)
file.write(received_obj.value)  #write to file
eof = False
while not eof:
    received_obj.value = 'ACK'
    received_obj.loop_count = received_obj.loop_count + 1
    received_obj = negotiate_step(received_obj)
    if received_obj.value == null:
        end_negotiate(True)
        file.close()
        eof = True
    else:
        file.write(received_obj.value)  #write to file

#file received
exit
Pseudo code for server ASA (await request and send a file):

supported_obj = objective('411:mvFile')
requested_obj = listen_negotiate(supported_obj)
file = open(requested_obj.value) #open the source file
if no such file:
    end_negotiate(False) #decline negotiation
    exit

eof = False
while not eof:
    chunk = file.read(1024) #next block of file
    requested_obj.value = chunk
    requested_obj.loop_count = requested_obj.loop_count + 1
    requested_obj = negotiate_step(requested_obj)
    if chunk == null:
        file.close()
        eof = True
        end_negotiate(True)
        exit
        if requested_obj.value != 'ACK':
            #unexpected reply...

4. Loss Detection

The above description and example assume that GRASP is implemented over a reliable transport layer such as TCP, such that lost or corrupted messages are not likely. Rarely, an error might be detected via a missing ACK, in which case the transfer would be aborted and restarted. In the event that GRASP is implemented over an unreliable transport layer such as UDP, it would be possible to add a block number to both the data block and acknowledgement objectives, so that missing blocks can be retransmitted, or duplicate blocks can be ignored. For example, the objective in Section 3 would become:

mvfile-objective = ["411:mvFile", objective-flags, loop-count, value]

objective-flags = ; as in the GRASP specification
loop-count = ; as in the GRASP specification
value = [block-number, any]
block-number = uint

It would also be necessary for the transport layer to detect data errors, for example by enabling UDP checksums.
5. Maximum Transmission Unit

In an IPv6 environment, a minimal MTU of 1280 bytes can be assumed, and assuming that high throughput is not a requirement, bulk transfers can be designed to match that MTU. However, there are environments where the underlying physical MTU is much smaller. For example, on an IEEE 802.15.4 network it may be less than 100 bytes [RFC4944]. Even in a 5G network, the Transport Block Size may be quite small, depending on the radio parameters. In such a case, a bulk transfer solution has several choices:

1. Accept the overhead of fragmentation in an adaptation layer, and therefore assume a network-layer MTU of 1280 bytes. Indeed, the presence of such an adaptation layer may be impossible to detect.

2. Attempt to determine the actual MTU available without lower-layer fragmentation. This however will be impossible without using low-level functions of the socket interface.

3. Attempt to determine a message size that provides optimum performance, by some sort of trial-and-error solution.

These complexities suggest that using a GRASP-based mechanism is unlikely to be optimal in environments with a very small physical MTU.

6. Pipelining

The above description and example describe a simple handshake model where each block is acknowledged before the next block is sent. For the scenarios discussed in Section 1, this should be acceptable. Therefore we do not suggest adding a pipelining or windowing mechanism. If high throughput is required, a conventional file transfer protocol should be used.

7. Other Considerations

If multiple transfers are requested simultaneously, each one will proceed as a separate GRASP negotiation session. The ASA acting as the server must be coded accordingly, like any ASA that needs to handle simultaneous sessions [I-D.carpenter-anima-asa-guidelines].

Bulk transfer might become a utility function for use by various ASAs, such as those supporting YANG or JSON distribution, log file uploads, or code downloads. In this case some form of user space API for bulk transfer will be required. This could be in the form of an inter-process communication call between the ASA in question and the...
ASA implementing the bulk transfer mechanism. The details are out of scope for this document.

8. Possible Future Work

The simple file transfer mechanism described above is only an example. Other application scenarios should be developed.

The mechanism described in this document is suitable for simple unicast scenarios where GRASP runs over TCP and can be treated as a reliable protocol. A more sophisticated approach would be needed in at least two cases:

1. A scenario where GRASP runs over UDP, where error detection and retransmission would be essential.

2. A scenario where multicast data distribution is required, so that a mechanism such as Trickle [RFC6206] would be appropriate.

These solutions might also require extensions to the GRASP protocol itself.

9. Implementation Status [RFC Editor: please remove]

A prototype open source Python implementation of simple file transfer has been used to verify the mechanism described above. It may be found at https://github.com/becarpenter/graspy/blob/master/getter.py and https://github.com/becarpenter/graspy/blob/master/pusher.py.

10. Security Considerations

All GRASP transactions are secured by the mandatory security substrate required by [I-D.ietf-anima-grasp]. No additional security issues are created by the application of GRASP described in this document.

11. IANA Considerations

This document makes no request of the IANA.

12. Acknowledgements

Thanks to Joel Halpern and other members of the ANIMA WG.
13. References

13.1. Normative References

[I-D.ietf-anima-grasp]


13.2. Informative References

[I-D.carpenter-anima-asa-guidelines]

[I-D.ietf-anima-grasp-api]

[I-D.ietf-anima-reference-model]

[I-D.liu-anima-grasp-distribution]

Appendix A. Change log [RFC Editor: Please remove]

draft-carpenter-anima-grasp-bulk-04, 2019-07-03:
Updated description of very small link-layer MTU issue.
Clarified informational status, updated reference.
draft-carpenter-anima-grasp-bulk-03, 2019-01-07:
Added future work section, implementation status.
draft-carpenter-anima-grasp-bulk-02, 2018-06-30:
Update reference, fix TBDs.
draft-carpenter-anima-grasp-bulk-01, 2018-03-03:
Updates after IETF100 discussion.
draft-carpenter-anima-grasp-bulk-00, 2017-09-12:
Initial version.

Authors’ Addresses

Brian Carpenter
School of Computer Science
University of Auckland
PB 92019
Auckland 1142
New Zealand

Email: brian.e.carpenter@gmail.com
Sheng Jiang  
Huawei Technologies Co., Ltd  
Q14, Huawei Campus, No.156 Beiqing Road  
Hai-Dian District, Beijing, 100095  
P.R. China  
Email: jiangsheng@huawei.com

Bing Liu  
Huawei Technologies Co., Ltd  
Q14, Huawei Campus  
No.156 Beiqing Road  
Hai-Dian District, Beijing 100095  
P.R. China  
Email: leo.liubing@huawei.com
Abstract

This document discusses scenarios and requirements for Autonomic Control Planes (ACPs) constructed and secured at Layer 2. These would be alternatives to an ACP constructed and secured at the network layer. A secure ACP is required as the substrate for the Generic Autonomic Signaling Protocol (GRASP) used by Autonomic Service Agents.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 1, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

Carpenter & Liu Expires September 1, 2019 [Page 1]
1. Introduction

As defined in [I-D.ietf-anima-reference-model], the Autonomic Service Agent (ASA) is the atomic entity of an autonomic function, and it is instantiated on autonomic nodes. When ASAs communicate with each other, they should use the Generic Autonomic Signaling Protocol (GRASP) [I-D.ietf-anima-grasp]. It is essential that such communication is strongly secured to avoid malicious interference with the Autonomic Infrastructure (ANI).

For this reason, GRASP must run over a secure substrate that is isolated from regular data plane traffic. This substrate is known as the Autonomic Control Plane (ACP). A method for constructing an ACP at the network layer is described in [I-D.ietf-anima-autonomic-control-plane]. The present document discusses scenarios and requirements for constructing an ACP at layer 2.

2. Network Scenarios Suitable for a Layer 2 ACP

The ANI design is aimed at managed networks, as explained in the reference model [I-D.ietf-anima-reference-model]. For a wide area network (such as a large campus, a multi-site enterprise network, or a carrier network considered as a whole) it is appropriate to construct the ACP using network layer techniques and network layer security, and that is the model described in [I-D.ietf-anima-autonomic-control-plane]. However, in at least two cases an ACP covering a smaller geographical area may be appropriate:
1. A small enterprise that is completely within one building or several adjacent buildings, but is large enough to require autonomic network management.

2. An enterprise that prefers in any case to segment its network into smaller units for management purposes.

In either case, we assume that the L2 ACP may extend into the Network Operations Centre (NOC) so that it can be interfaced to traditional tools for Operations, Administration and Maintenance, as described in [RFC8368]. In the terminology of that document, an L2 ACP is an instance of a Generalized ACP.

3. Requirements for a Layer 2 Technology

1. The technology must support transmission of IPv6 packets according to [RFC8200]. Since GRASP can run on a single network segment using link-local addresses, there is not required to be an IPv6 router or DHCPv6 server.

2. The technology must support multicast. If the switches are not completely transparent to layer 2 multicast, they must support Multicast Listener Discovery Version 2 (MLDv2) for IPv6 [RFC3810].

3. The technology should have a minimum MTU of 1500 bytes.

4. The technology must support isolation of a given set of nodes (the "ACP VLAN").

5. The technology must support secure authorization for access to the ACP VLAN. If the VLAN technology in use does not support password protection, a VLAN access control list could be used.

6. The technology should support both the normal dataplane VLAN and the ACP VLAN on the same physical sockets. (Possibly the dataplane may be the native VLAN, i.e. frames with no VLAN tag.)

7. The technology should support line speed encryption of the ACP VLAN.

8. The technology should support wired/wireless bridging if relevant.

9. The technology should require minimal manual configuration of ACP nodes. However, it is expected that the nodes will need to be preconfigured before deployment with the VLAN ID, and a password or encryption key if necessary. A solution which is both secure
and self-configuring at Layer 2 is out of scope for this document.

A small ACP software module will be needed in each autonomic node, whose job is to provide the GRASP core with the following information about the L2 ACP:

1. A signal that the L2 ACP is available and secure.

2. The current global scope IPv6 address that GRASP should use as its primary locator, preferably a ULA, if available. As mentioned, if no such address is available, GRASP will simply operate with link-local addresses.

3. A list of [interface_index, link_local_address] pairs for all valid IPv6 interfaces attached to the L2 ACP. The interface index is an integer for maximum portability between operating systems.

4. Multiple Segments

   This section is for further study.

   The L2 ACP could in principle be extended across multiple segments or even multiple sites by use of secure L2VPN technology.

5. Implementation Status [RFC Editor: please remove]

   A simple ACP software module emulating that needed for a secure L2 ACP has been implemented, but it does not in fact verify security. It may be found at <https://github.com/becarpenter/graspy/blob/master/acp.py> and is briefly documented in <https://github.com/becarpenter/graspy/blob/master/graspy.pdf>.

6. Security Considerations

   The assumption of this document is that any Layer 2 solution chosen must have adequate security against interlopers and eavesdroppers. It should be noted that (at least in a wired network) this also requires adequate physical security to prevent access by unauthorized persons, including physical intrusion detection.

   The fact that an IPv6 router is not required in an L2 ACP excludes many Layer 3 vulnerabilities by construction. No outside entity can generate link-local IPv6 packets, and no outside entity can send global scope packets to any autonomic node.
7. IANA Considerations

This document makes no request of the IANA.

8. Acknowledgements

Excellent suggestions were made by TBD and other participants in the ANIMA WG.

9. References

9.1. Normative References


9.2. Informative References

[I-D.ietf-anima-autonomic-control-plane]

[I-D.ietf-anima-grasp]

[I-D.ietf-anima-reference-model]

Appendix A. Change log [RFC Editor: Please remove]

draft-carpenter-anima-l2acp-scenarios-00, 2019-02-28:

Initial version

Authors’ Addresses

Brian Carpenter
The University of Auckland
School of Computer Science
University of Auckland
PB 92019
Auckland  1142
New Zealand

Email: brian.e.carpenter@gmail.com

Bing Liu (editor)
Huawei Technologies
Q14, Huawei Campus
No.156 Beiqing Road
Hai-Dian District, Beijing  100095
P.R. China

Email: leo.liubing@huawei.com
Abstract

This document outlines multiple advanced use cases and integrations that ACME facilitates without any modifications or enhancements required to the base ACME specification. These use cases are not immediately obvious from reading the ACME specification and thus are explicitly documented here. The use cases include ACME issuance of subdomain certificates, and ACME integration with EST and TEAP.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 3, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ....................................................... 2
2. Terminology ....................................................... 2
3. ACME Issuance of Subdomain Certificates .......................... 3
4. ACME Integration with EST ......................................... 5
5. ACME Integration with BRSKI ....................................... 8
6. ACME Integration with TEAP ........................................ 10
7. ACME Integration with TEAP-BRSKI ................................. 13
8. IANA Considerations .............................................. 15
9. Security Considerations ......................................... 16
10. Informative References ........................................... 16
Appendix A. Comments .................................................. 16
Authors’ Addresses ..................................................... 16

1. Introduction

ACME [RFC8555] defines a protocol that a certificate authority (CA) and an applicant can use to automate the process of domain name ownership validation and X.509 (PKIX) certificate issuance. The protocol is rich and flexible and enables multiple use cases that are not immediately obvious from reading the specification. This document explicitly outlines multiple advanced ACME use cases including:

- ACME issuance of subdomain certificates
- ACME integration with EST [RFC7030]
- ACME integration with BRSKI [I-D.ietf-anima-bootstrapping-keyinfra]
- ACME integration with TEAP [RFC7170]
- ACME integration with TEAP-BRSKI draft-lear-eap-teap-brski

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The following terms are used in this document:
3. ACME Issuance of Subdomain Certificates

A typical ACME workflow for issuance of certificates is as follows:

1. client POSTs a newOrder request that contains a set of "identifiers"

2. server replies with a set of "authorizations" and a "finalize" URI

3. client sends POST-as-GET requests to retrieve the "authorizations", with the downloaded "authorization" object(s) containing the "identifier" that the client must prove control of

4. client proves control over the "identifier" in the "authorization" object by completing the specified challenge, for example, by publishing a DNS TXT record

5. client POSTs a CSR to the "finalize" API

ACME places the following restrictions on "identifiers":

- section 7.1.4: the only type of "identifier" defined by the ACME specification is a fully qualified domain name: "The only type of identifier defined by this specification is a fully qualified domain name (type: "dns"). The domain name MUST be encoded in the form in which it would appear in a certificate."

- Section 7.4: the "identifier" in the CSR request must match the "identifier" in the newOrder request: "The CSR MUST indicate the
exact same set of requested identifiers as the initial newOrder request."

- Sections 8.3: the "identifier", or FQDN, in the "authorization" object must be used when fulfilling challenges via HTTP: "Construct a URL by populating the URL template ... where the domain field is set to the domain name being verified"

- Section 8.4: the "identifier", or FQDN, in the "authorization" object must be used when fulfilling challenges via DNS: "The client constructs the validation domain name by prepending the label "_acme-challenge" to the domain name being validated."

ACME does not mandate that the "identifier" in a newOrder request matches the "identifier" in "authorization" objects. This means that the ACME specification does not preclude an ACME server processing newOrder requests and issuing certificates for a subdomain without requiring a challenge to be fulfilled against that explicit subdomain. ACME server policy could allow issuance of certificates for a subdomain to a client where the client only has to fulfill an authorization challenge for the parent domain.

This allows a flow where a client proves ownership of "domain.com" and then successfully obtains a certificate for "sub.domain.com". The ACME pre-authorization flow makes most sense for this use case, and that is what is illustrated in the following call flow.

The client could pre-authorize for the parent domain once, and then issue multiple newOrder requests for certificates for multiple subdomains. This call flow illustrates the client only placing one newOrder request.

```
+--------+             +------+     +-----+
| Client |             | ACME |     | DNS |
+--------+             +------+     +-----+
STEP 1: Pre-Authorization of parent domain
          |               |
POST /newAuthz
"domain.com"
------------------->
201 authorizations
<-------------------
Publish DNS TXT
"domain.com"
------------------->
```
4. ACME Integration with EST

EST [RFC7030] defines a mechanism for clients to enroll with a PKI Registration Authority by sending CMC messages over HTTP. EST section 1 states:

"Architecturally, the EST service is located between a Certification Authority (CA) and a client. It performs several functions traditionally allocated to the Registration Authority (RA) role in a PKI."

EST section 1.1 states that:
"For certificate issuing services, the EST CA is reached through the EST server; the CA could be logically "behind" the EST server or embedded within it."

When the CA is logically "behind" the EST RA, EST does not specify how the RA communicates with the CA. EST section 1 states:

"The nature of communication between an EST server and a CA is not described in this document."

This section outlines how ACME could be used for communication between the EST RA and the CA. The example call flow shows the RA proving ownership of a parent domain, with individual client certificates being subdomains under that parent domain. This is an optimisation that reduces DNS and ACME traffic overhead. The RA could of course prove ownership of every explicit client certificate identifier.

The call flow also illustrates how the Pledge inserts relevant domain information into the CSR Subject and Subject Alternative Name fields.

[todo: The details of how the pledge determines what information to include in the CSR are TBD. For example, the pledge could discover the DNS domain via DHCP Option 15, and prepend the identifier from the IDevID to this.

Note also that EST https://tools.ietf.org/html/rfc7030#section-4.2.1 states that the ChangeSubjectName attribute MAY be used, for example, if the Pledge uses its IDevID when requesting a CSR/LDevID with a different Subject, however this field does not appear to have widespread support across CAs.]

```
+--------+             +--------+             +------+     +-----+
| Pledge |             | EST RA |             | ACME |     | DNS |
+--------+             +--------+             +------+     +-----+
|                      |                      |           |
STEP 1: Pre-Authorization of parent domain
|                      | POST /newAuthz       |           |
|                      | "domain.com"         |           |
|                      |----------------------|-----------|
|                      | 201 authorizations   |           |
|                      |<----------------------|
|                      | Publish DNS TXT      |           |
|                      | "domain.com"         |-----------|
|                      |----------------------|-----------|
```
POST /challenge

--------------------->  Verify

200 status=valid

Delete DNS TXT
"domain.com"

------------------------>

STEP 2: Pledge enrolls against RA

POST /simpleenroll
PCSK#10 CSR
"pledgeid.domain.com"

--------------------->

202 Retry-After

------------------------>

STEP 3: RA places ACME order

POST /newOrder
"pledgeid.domain.com"

--------------------->

201 status=ready

POST /finalize
PKCS#10 CSR
"pledgeid.domain.com"

--------------------->

200 OK status=valid

POST /certificate

--------------------->

200 OK
PEM

"pledgeid.domain.com"

------------------------>

STEP 4: Pledge retries enroll
5. ACME Integration with BRSKI

BRSKI [I-D.ietf-anima-bootstrapping-keyinfra] is based upon EST [RFC7030] and defines how to autonomically bootstrap PKI trust anchors into devices via means of signed vouchers. EST certificate enrollment may then optionally take place after trust has been established. BRKSI voucher exchange and trust establishment are based on EST extensions and the certificate enrollment part of BRKSI is fully based on EST. Similar to EST, BRKSI does not define how the EST RA communicates with the CA. Therefore, the mechanisms outlined in the previous section for using ACME as the communications protocol between the EST RA and the CA are equally applicable to BRKSI.

The following call flow shows how ACME may be integrated into a full BRKSI voucher plus EST enrollment workflow. For brevity, it assumes that the EST RA has previously proven ownership of a parent domain and that pledge certificate identifiers are a subdomain of that parent domain. The domain ownership exchanges between the RA, ACME and DNS are not shown. Similarly, not all BRKSI interactions are shown and only the key protocol flows involving voucher exchange and EST enrollment are shown.

[todo: similar to the EST section above, it is TBD exactly how the pledge determines what domain information to insert in the CSR. A possibility is that the Voucher response includes domain information and explicitly instructs the pledge what information to insert in the CSR. The RA could also instruct the Pledge to include a guid or a new unique random identifier in place of its MAC address, serial number, or whatever other identifying information is included in the IDevID.

+--------+             +--------+             +------+     +------+
|  Pledge |             |  EST RA |             |  ACME |     |  MASA |
+--------+             +--------+             +------+     +------+
     |                   |             |                   |        |
NOTE: Pre-Authorization of "domain.com" is complete
STEP 1: Pledge requests Voucher

POST /requestvoucher  
--------------------->  
200 OK Voucher  
<---------------------

STEP 2: Pledge enrolls against RA

POST /simpleenroll  
PCSK#10 CSR  
"pledgeid.domain.com"  
--------------------->  
202 Retry-After  
<---------------------

STEP 3: RA places ACME order

POST /newOrder  
"pledgeid.domain.com"  
--------------------->  
201 status=ready  
<---------------------

POST /finalize  
PKCS#10 CSR  
"pledgeid.domain.com"  
--------------------->  
200 OK status=valid  
<---------------------

POST /certificate  
--------------------->  
200 OK  
PDM  
"pledgeid.domain.com"  
<---------------------

STEP 4: Pledge retries enroll
6. ACME Integration with TEAP

TEAP [RFC7170] define a tunnel-based EAP method that enables secure communication between a peer and a server by using TLS to establish a mutually authenticated tunnel. TEAP enables certificate provisioning within the tunnel. TEAP does not define how the TEAP server communicates with the CA.

This section outlines how ACME could be used for communication between the TEAP server and the CA. The example call flow shows the TEAP server proving ownership of a parent domain, with individual client certificates being subdomains under that parent domain. This is an optimisation that reduces DNS and ACME traffic overhead. The TEAP server could of course prove ownership of every explicit client certificate identifier.

[todo: Similar to the previous section, it is TBD exactly how the Pledge determines what Subject/SAN to put in the CSR request.]
STEP 2: Establish EAP Outer Tunnel

EAP-Request/
Type=Identity

EAP-Response/
Type=Identity

EAP-Request/
Type=TEAP,
TEAP Start,
Authority-ID TLV

EAP-Response/
Type=TEAP,
TLS(ClientHello)

EAP-Request/
Type=TEAP,
TLS(ServerHello,
Certificate,
ServerKeyExchange,
CertificateRequest,
ServerHelloDone)

EAP-Response/
Type=TEAP,
TLS(Certificate,
ClientKeyExchange,
CertificateVerify,
ChangeCipherSpec,
Finished)
STEP 3: Enroll for certificate

EAP-Request/
Type=TEAP,
{Request-Action TLV: Status=Failure,
Action=Process-TLV,
TLV=PKCS#10}
7. ACME Integration with TEAP-BRSKI

TEAP-BRSKI [I-D.lear-eap-teap-brski] defines how to execute BRSKI at layer 2 inside a TEAP tunnel. Similar to the TEAP proposal in the previous section, BRSKI-TEAP leverages the existing TEAP PKXS#10 and PKCS#7 mechanisms for certificate enrollment, and does not define how the TEAP server communicates with the CA.

This section outlines how ACME could be used for communication between the TEAP server and the CA, and how this fits in with the TEAP-BRSKI proposal.

[TODO: Similar to the previous section, it is TBD exactly how the Pledge determines what Subject/SAN to put in the CSR request.]

+--------+                +-------------+         +------+   +------+
| Pledge |                | TEAP-Server |         | ACME |   | MASA |
+--------+                +-------------+         +------+   +------+

NOTE: Pre-Authorization of "domain.com" is complete and EAP outer tunnel is established as outlined in the previous section

STEP 1: Perform BRSKI Flow

EAP-Request/
Type=TEAP,
STEP 2: Retrieve CA Configuration

EAP-Response/  
Type=TEAP,  
{Trusted-Server-Root TLV}
------------------------>

EAP-Request/  
Type=TEAP,  
{Trusted-Server-Root TLV}
<------------------------

EAP-Response/  
Type=TEAP,  
{CSR-Attributes TLV}
------------------------>

EAP-Request/  
Type=TEAP,  
{CSR-Attributes TLV}
<------------------------

STEP 3: Enroll for certificate

EAP-Response/  
Type=TEAP,  
{PKCS#10 TLV:  
TLV=Request-Voucher,  
TLV=Trusted-Server-Root,  
TLV=CSR-Attributes,  
TLV=PKCS#10}  
<------------------------

EAP-Response/  
Type=TEAP,  
{Request-Voucher TLV}  
------------------------>

EAP-Request/  
Type=TEAP,  
{Request-Voucher TLV}  
<------------------------

EAP-Request/  
Type=TEAP,  
{Voucher TLV}  
<------------------------

EAP-Response/  
Type=TEAP,  
{Trusted-Server-Root TLV}  
------------------------>

EAP-Request/  
Type=TEAP,  
{Trusted-Server-Root TLV}  
<------------------------
<table>
<thead>
<tr>
<th>&quot;pledgeid.domain.com&quot;</th>
<th>POST /newOrder</th>
<th>&quot;pledgeid.domain.com&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>201 status=ready</td>
<td></td>
</tr>
<tr>
<td></td>
<td>POST /finalize</td>
<td>PKCS#10 CSR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;pledgeid.domain.com&quot;</td>
</tr>
<tr>
<td></td>
<td>200 OK status=valid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>POST /certificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>200 OK</td>
<td>PEM</td>
</tr>
<tr>
<td></td>
<td>&quot;pledgeid.domain.com&quot;</td>
<td></td>
</tr>
</tbody>
</table>

EAP-Request/  
Type=TEAP,  
{PKCS#7 TLV,  
Result TLV=Success}  
EAP-Response/  
Type=TEAP,  
{Result TLV=Success}  
EAP-Success

8. IANA Considerations

[todo]
9. Security Considerations

[todo]

10. Informative References

[I-D.ietf-anima-bootstrapping-keyinfra]

[I-D.lear-eap-teap-brski]
Lear, E., Friel, O., and N. Cam-Winget, "Bootstrapping Key Infrastructure over EAP", draft-lear-eap-teap-brski-02 (work in progress), February 2019.


Appendix A. Comments

Authors’ Addresses

Friel & Barnes Expires January 3, 2020
Abstract

This document discusses an enhancement of automated bootstrapping of a remote secure key infrastructure (BRSKI) to operate in domains featuring no or only timely limited connectivity to backend services offering enrollment functionality, specifically a Public Key Infrastructure (PKI). In the context of deploying new devices the design of BRSKI allows for online (synchronous object exchange) and offline interactions (asynchronous object exchange) with a manufacturer’s authorization service. For this it utilizes a self-contained voucher to transport the domain credentials as a signed object to establish an initial trust between the pledge and the deployment domain. The currently supported enrollment protocol for request and distribution of deployment domain specific device certificates provides only limited support for asynchronous PKI interactions. This memo motivates the enhancement of supporting self-contained objects for certificate management by using an abstract notation. This allows off-site operation of PKI services outside the deployment domain of the pledge. This addresses specifically scenarios, in which the final authorization of certification request of a pledge cannot be made in the deployment domain and is therefore delegated to a operator backend. The goal is to enable the usage of existing and potentially new PKI protocols supporting self-containment for certificate management.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."
time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 9, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction .............................................. 3
2. History of changes ....................................... 5
3. Terminology .............................................. 6
4. Scope of solution ......................................... 6
   4.1. Supported environment ................................. 6
   4.2. Application Examples ................................. 7
      4.2.1. Rolling stock .................................. 7
      4.2.2. Building automation ............................. 7
      4.2.3. Substation automation ............................ 8
      4.2.4. Electric vehicle charging infrastructure ....... 8
      4.2.5. Infrastructure isolation policy ................ 8
      4.2.6. Less operational security in the deployment domain 9
   4.3. Requirement discussion and mapping to solution elements 9
5. Architectural Overview .................................... 11
   5.1. Behavior of a pledge ................................. 14
   5.2. Secure Imprinting using Vouchers ........................ 14
   5.3. Addressing ........................................... 15
6. Protocol Flows ............................................ 15
   6.1. Pledge - Registrar discovery and voucher exchange ...... 15
   6.2. Registrar - MASA voucher exchange .................... 16
   6.3. Pledge - Registrar - RA/CA certificate enrollment ...... 17
7. Mapping to existing enrollment protocols .................... 19
   7.1. EST Handling ........................................ 19
   7.2. CMP Handling ........................................ 20
8. IANA Considerations ....................................... 20
9. Privacy Considerations .................................... 20
1. Introduction

BRSKI as defined in [I-D.ietf-anima-bootstrapping-keyinfra] specifies a solution for secure zero-touch (automated) bootstrapping of devices (pledges) in a target deployment domain. This includes the discovery of network elements in the deployment domain, time synchronization, and the exchange of security information necessary to establish trust between a pledge and the domain and to adopt a pledge as new network and application element. Security information about the deployment domain, specifically the deployment domain certificate (domain root certificate), is exchanged utilizing vouchers as defined in [RFC8366]. These vouchers are self-contained objects, which may be provided online (synchronous) or offline (asynchronous) via the domain registrar to the pledge and originate from a manufacturer’s authorization service (MASA). The manufacturer signed voucher contains the target domain certificate and can be verified by the pledge due to the possession of a manufacturer root certificate. It facilitates the enrollment of the pledge in the deployment domain and is used to establish trust.

For the enrollment of devices BRSKI relies on EST [RFC7030] to request and distribute deployment domain specific device certificates. EST in turn relies on a binding of the certification request to an underlying TLS connection between the EST client and the EST server. According to BRSKI the domain registrar acts as EST server and is also acting as registration authority (RA) or local registration authority (LRA). The binding to TLS is used to protect the exchange of a certification request (for an LDevID certificate) and to provide data origin authentication to support the authorization decision for processing the certification request. The TLS connection is mutually authenticated and the client side authentication bases on the pledge’s manufacturer issued device certificate (IDevID certificate). This approach requires an on-site availability of the RA as PKI component and/or a local asset or inventory management system performing the authorization decision based on the certification request to issue a domain specific certificate to the pledge. This is due to the EST server terminating the security association with the pledge and thus the binding between the certification request and the authentication of the pledge. This type of enrollment utilizing an online connection to the PKI is considered as synchronous enrollment.
For certain use cases on-site support of a RA/CA component and/or an asset management is not available and rather provided by an operators backend and may be provided timely limited or completely through offline interactions. This may be due to higher security requirements for operating the certification authority. The authorization of a certification request based on an asset management in this case will not / can not be performed on-site at enrollment time. Enrollment, which cannot be performed in a (timely) consistent fashion is considered as asynchronous enrollment in this document. It requires the support of a store and forward functionality of certification request together with the requester authentication information. This enables processing of the request at a later point in time. A similar situation may occur through network segmentation, which is utilized in industrial systems to separate domains with different security needs. Here, a similar requirement arises if the communication channel carrying the requester authentication is terminated before the RA/CA. If a second communication channel is opened to forward the certification request to the issuing CA, the requester authentication information needs to be bound to the certification request. For both cases, it is assumed that the requester authentication information is utilized in the process of authorization of a certification request. There are different options to perform store and forward of certification requests including the requester authentication information:

- Providing a trusted component (e.g., an LRA) in the deployment domain, which stores the certification request combined with the requester authentication information (the 
  IDevID) and potentially the information about a successful proof of possession (of the corresponding private key) in a way prohibiting changes to the combined information. Note that the assumption is that the information elements may not be cryptographically bound together. Once connectivity to the backend is available, the trusted component forwards the certification request together with the requester information (authentication and proof of possession) to the off-site PKI for further processing. It is assumed that the off-site PKI in this case relies on the local authentication result and thus performs the authorization and issues the requested certificate. In BRSKI the trusted component may be the EST server residing co-located with the registrar in the deployment domain.

- Utilization of self-contained objects binding the certification request and the requester authentication in a cryptographic way. This approach reduces the necessary trust in a domain component to storage and delivery. Unauthorized modifications of the requestor information (request and authentication) can be detected during
the verification of the cryptographic binding of the self-contained object in the off-site PKI.

This document targets environments, in which connectivity to the PKI functionality is only temporary or not directly available by specifying support for handling self-contained objects supporting asynchronous enrollment. As it is intended to enhance BRSKI it is named BRSKI-AE, where AE stands for asynchronous enrollment. As BRSKI, BRSKI-AE results in the pledge storing a X.509 root certificate sufficient for verifying the domain registrar / proxy identity as well as an domain specific X.509 device certificate (LDevID certificate).

The goal is to enhance BRSKI to either allow other existing certificate management protocols supporting self-contained objects to be applied or to allow other types of encoding for the certificate management information exchange.

Note that in contrast to BRSKI, BRSKI-AE assumes support of multiple enrollment protocols on the infrastructure side, allowing the pledge manufacturer to select the most appropriate. Thus, BRSKI-AE can be applied for both, asynchronous and synchronous enrollment.

2. History of changes

From version 00 -> 01:

- Update of examples, specifically for building automation as well as two new application use cases in Section 4.2.
- Deletion of asynchronous interaction with MASA to not complicate the use case. Note that the voucher exchange can already be handled in an asynchronous manner and is therefore not considered further. This resulted in removal of the alternative path the MASA in Figure 1 and the associated description in Section 5.
- Enhancement of description of architecture elements and changes to BRSKI in Section 5.
- Consideration of existing enrollment protocols in the context of mapping the requirements to existing solutions in Section 4.3.
- New section starting Section 7 with the mapping to existing enrollment protocols by collecting boundary conditions.
3. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

This document relies on the terminology defined in [I-D.ietf-anima-bootstrapping-keyinfra]. The following terms are defined additionally:

CA: Certification authority, issues certificates.

RA: Registration authority, an optional system component to which a CA delegates certificate management functions such as authorization checks.

LRA: Local registration authority, an optional RA system component with proximity to end entities.

IED: Intelligent Electronic Device (in essence a pledge).

on-site: Describes a component or service or functionality available in the target deployment domain.

off-site: Describes a component or service or functionality available in an operator domain different from the target deployment domain. This may be a central side, to which only a temporarily connection is available or which is in a different administrative domain.

asynchronous communication: Describes a timely interrupted communication between an end entity and a PKI component.

synchronous communication: Describes a timely uninterrupted communication between an end entity and a PKI component.

4. Scope of solution

4.1. Supported environment

This solution is intended to be used in domains with limited support of on-site PKI services and comprises use cases in which:

- there is no registration authority available in the deployment domain. The connectivity to the backend RA may only be temporarily available. A local store and forward device is used for the communication with the backend services.
 authoritative actions of a LRA are limited and may not comprise authorization of certification requests of pledges. Final authorization is done at the RA residing in the backend operator domain.

- the target deployment domain already uses a certificate management approach that shall be reused to be consistent throughout the lifecycle.

4.2. Application Examples

The following examples are intended to motivate the support of different enrollment approaches in general and asynchronous enrollment specifically, by introducing industrial applications cases, which could leverage BRSKI as such but also require support of asynchronous operation as intended with BRSKI-AE.

4.2.1. Rolling stock

Rolling stock or railroad cars contain a variety of sensors, actuators, and controller, which communicate within the railroad car but also exchange information between railroad cars building a train or with a backend. These devices are typically unaware of backend connectivity. Managing certificates may be done during maintenance cycles of the railroad car, but can already be prepared during operation. The preparation may comprise the generation of certification requests by the components which are collected and forwarded for processing once the railroad car is connected to the operator backend. The authorization of the certification request is then done based on the operators asset/inventory information.

4.2.2. Building automation

In building automation a use case can be described by a detached building or the basement of a building equipped with sensor, actuators, and controllers connected, but with only limited or no connection to the centralized building management system. This limited connectivity may be during the installation time but also during operation time. During the installation in the basement, a service technician collects the necessary information from the basement network and provides them to the central building management system, e.g., using a laptop or even a mobile phone to transport the information. This information may comprise parameters and settings required in the operational phase of the sensors/actuators, like a certificate issued by the operator to authenticate against other components and services.
4.2.3. Substation automation

In substation automation a control center typically hosts PKI services to issue certificates for Intelligent Electronic Devices (IED)s in a substation. Communication between the substation and control center is done through a proxy/gateway/DMZ, which terminates protocol flows. Note that NERC CIP-005-5 [NERC-CIP-005-5] requires inspection of protocols at the boundary of a security perimeter (the substation in this case). In addition, security management in substation automation assumes central support of different enrollment protocols to facilitate the capabilities of IEDs from different vendors. The IEC standard IEC62351-9 [IEC-62351-9] specifies the mandatory support of two enrollment protocols, SCEP [I-D.gutmann-scep] and EST [RFC7030] for the infrastructure side, while the IED must only support one of the two.

4.2.4. Electric vehicle charging infrastructure

For the electric vehicle charging infrastructure protocols have been defined for the interaction between the electric vehicle (EV) and the charging point (e.g., ISO 15118-2 [ISO-IEC-15118-2]) as well as between the charging point and the charging point operator (e.g. OCPP [OCPP]). Depending on the authentication model, unilateral or mutual authentication is required. In both cases the charging point authenticates uses an X.509 certificate to authenticate in the context of a TLS connection between the EV and the charging point. The management of this certificate depends (beyond others) on the selected backend connectivity protocol. Specifically in case of OCPP it is intended as single communication protocol between the charging point and the backend carrying all information to control the charging operations and maintain the charging point itself. This means that the certificate management is intended to be handled in-band of OCPP. This requires to be able to encapsulate the certificate management exchanges in a transport independent way. Self-containment will ease this by allowing the transport without a separate communication protocol. For the purpose of certificate management CMP [RFC4210] is intended to be used.

4.2.5. Infrastructure isolation policy

This refers to any case in which network infrastructure is normally isolated from the Internet as a matter of policy, most likely for security reasons. In such a case, limited access to external PKI resources will be allowed in carefully controlled short periods of time, for example when a batch of new devices are deployed, but impossible at other times.
4.2.6. Less operational security in the deployment domain

The registration point performing the authorization of a certificate request is a critical PKI component and therefore implicates higher operational security than other components utilizing the issued certificates for their security features. CAs may also demand higher security in the registration procedures. Especially the CA/Browser forum currently increases the security requirements in the certificate issuance procedures for publicly trusted certificates. There may be the situation that the deployment domain does not offer enough security to operate a registration point and therefore wants to transfer this service to a backend.

4.3. Requirement discussion and mapping to solution elements

For the requirements discussion it is assumed that the entity receiving the self-contained object in the deployment domain is not the authorization point for the certification request contained in the object. If the entity is the authorization point, BRSKI can be used directly. Note that BRSKI-AE could address both cases.

Based on the supported deployment environment described in Section 4.1 and the motivated application examples described in Section 4.2 the following base requirements are derived to support self-contained objects as container carrying the certification request and further information to support asynchronous operation. Moreover, potential solution examples (not complete) based on existing technology are provided with the focus on existing IETF standards track documents:

- Certification requests are structures protecting at least integrity of the contained data combined with a proof-of-private-key-possession for locally generated key pairs. Examples for certification requests
  
  * PKCS#10 [RFC2986]: Defines a structure for a certification request. The structure must be signed to ensure integrity protection and proof-of-private-key-possession. Hence, the signature is performed by using the private key of the requestor (corresponding to the contained public key).
  
  * CRMF [RFC4211]: Defines a structure for the certification request. The structure also typically contains an integrity protection and a proof of possession, in which a signature value is generated by using the corresponding private key to the contained public key. This self-signature can also be replaced by the RA after verification, if the RA intends to update or alter the request message.
Note that the integrity is bound to the public key contained in the certification request. In the considered application examples, this is not sufficient and needs to be bound to the data origin authentication (IDevID). This binding also supports the authorization decision for the certification request. The binding of data origin authentication to the certification request is delegated to the management protocol.

1. The container carrying the certification request should support a binding to an existing credential known to the peer performing the authorization of the certification request as proof of identity. The binding may be transport dependent if the endpoint at the next communication hop is authorizing the certification request. This requirement is addressed by existing enrollment protocols in different ways, for instance:

   * EST [RFC7030]: Utilizes PKCS#10 to encode the certification request. The Certificate Signing Request (CSR) contains a binding to the underlying TLS by including the tls-unique value in the self-signed CSR structure. The tls-unique value is one result of the TLS handshake. As the TLS handshake is performed mutually authenticated and the pledge utilized its IDevID for it, the proof of identity can be provided by the binding to the TLS session.

   * SCEP [I-D.gutmann-scep]: Provides the option to utilize either an existing secret (password) or an existing certificate to protect the CSR based on SCEP Secure Message Objects using CMS ([RFC5652]). Note that the wrapping using an existing IDevID credential is not specified directly in SCEP.

   * CMP [RFC4210] Provides the option to utilize either an existing secret (password) or an existing certificate to protect the PKIMessage containing the certification request. The certification request is encoded utilizing CRMF. PKCS#10 is optionally supported. The proof of identity of the PKIMessage containing the certification request can be achieved by using IDevID credentials to calculate a signature over the header and the body of the PKIMessage utilizing the protectionAlg signaled in the PKIMessage header and the PKIProtection carrying the actual signature value.

   * CMC [RFC5272] Provides the option to utilize either an existing secret (password) or an existing certificate to protect the certification request (either in CRMF or PKCS#10) based on CMS ([RFC5652]). Here a FullCMCRequest would be used, which allows signing with an existing IDevID credential to provide a proof of identity.
The container carrying the certification request should support transport independent protection using an existing credential of the pledge verifiable at the authorization point of the certification request (typically the RA in conjunction with an inventory). This requirements is addressed by existing enrollment protocols in different ways, for instance:

* EST [RFC7030]: Not supported.
* SCEP [I-D.gutmann-scep]: Not specified in SCEP, could be done using message wrapping with signature (based on CMS).
* CMP [RFC4210]: Message wrapping with signature.
* CMC [RFC5272]: Message wrapping with signature.

5. Architectural Overview

To support asynchronous enrollment, the base system architecture defined in BRSKI [I-D.ietf-anima-bootstrapping-keyinfra] is changed to allow for off-site operation of the PKI components. The assumption for BRSKI-AE is that the authorization for a certification request is performed using an inventory or asset management system residing in the backend of the domain operator as described in Section 4.1. This leads to changes in the placement or enhancements of the logical elements as shown in Figure 1.
The architecture overview in Figure 1 utilizes the same logical elements as BRSKI but with a different placement in the architecture for some of the elements. The main difference is the placement of the PKI RA/CA component, which is actually performing the authorization decision for the certification request message. Also shown is the connectivity of the RA/CA with an inventory management system, which is expected to be utilized in the authorization.
decision. Note that this may also be an integrated functionality of the RA. Both components are placed in the off-site domain of the operator (not the deployment site directly), which may have no or only temporary connectivity to the deployment domain of the pledge. This is to underline the authorization decision for the certification request in the backend rather than in the deployment domain itself. The following list describes the components in the deployment domain:

- Join Proxy: same functionality as described in BRSKI

- Domain Registrar / Proxy: In general the domain registrar / proxy has a similar functionality regarding the imprinting of the pledge in the deployment domain to facilitate the communication of the pledge with the MASA and the PKI. Different is the authorization of the certification request. BRSKI-AE allows to perform this in the operators backend (off-site), even if the deployment domain has only temporary or no connectivity to an operator domain.

  * Voucher exchange: The voucher exchange with the MASA via the domain registrar is performed as described in BRSKI [I-D.ietf-anima-bootstrapping-keyinfra] .

  * Certificate enrollment: For the pledge enrollment the domain registrar in the deployment domain support the authorization of the pledge to be part of the domain, but not necessarily to authorize the certification request provided during enrollment. This may be due to lack of authorization information in the deployment domain. If the authorization is done in the operator domain, the domain registrar is used to forward the certification request to the RA. Thus it basically works as a proxy. In the case of no connectivity, the domain registrar stores the certification request and forwards it to the RA upon connectivity. As this requires the certification request to be self-contained, the domain registrar needs functionality enhancements with respect to the support of alternative enrollment approaches supporting self-containment. To support alternative enrollment approaches (protocols, encodings), it is necessary to enhance the addressing scheme at the domain registrar. The communication channel between the pledge and the domain registrar may be similarly described as in BRSKI within the same "/.well-known" tree and may result in "/.well-known/enrollment-variant/request".

The following list describes the vendor related components/service outside the deployment domain:

- MASA: general functionality as described in BRSKI. Assumption that the interaction with the MASA may be synchronous (voucher
request with nonce) or asynchronous (voucher request without nonce).

- Ownership tracker: as defined in BRSKI.

The following list describes the operator related components/service operated in the backend:

- PKI RA: Performs certificate management functions (validation of certification requests, interaction with inventory/asset management for authorization of certification requests, etc.) for issuing, updating, and revoking certificates for a domain as a centralized infrastructure for the operator.

- PKI CA: Performs certificate generation by signing the certificate structure provided in the certification request.

- Inventory (asset) management: contains information about the known devices belonging to the operator. Specifically, the inventory is used to provide the information to authorize issuing a certificate based on the certification request of the pledge. Note: the communication between the inventory (asset) management and the PKI components (RA/CA) are out of scope of this document.

- (Domain) registrar: Optional component if the deployment domain does not feature a domain registrar but only a proxy. In this case it is involved in the certification request processing and is assumed to be co-located with the PKI RA.

5.1. Behavior of a pledge

The behavior of a pledge as described in [I-D.ietf-anima-bootstrapping-keyinfra] is kept with one exception. After finishing the imprinting phase (4) the enrollment phase (5) is performed with a method supporting self-contained objects. Using simpleenroll with EST as taken in BRSKI cannot be applied here, as it binds the pledge authentication with the existing IDevID using the transport channel. This authentication is not visible / verifiable at the authorization point in the off-site domain. /* mapping to existing protocols based on the outcome of the discussion */

5.2. Secure Imprinting using Vouchers

The described approach in [I-D.ietf-anima-bootstrapping-keyinfra] is kept as is.
5.3. Addressing

For the provisioning of different enrollment options at the domain registrar, the addressing approach of BRSKI using a "/.well-known" tree from [RFC5785] is enhanced.

/* to be done: Description of "/.well-known/enrollment-protocol/request" in which enrollment-protocol may be an already existing protocol like "est" or "scep" or "cmp" or "cms" or a newly defined protocol. */

6. Protocol Flows

Based on BRSKI and the architectural changes the original protocol flow is divided into three phases showing commonalities and differences to the original approach as depicted in the following.

- Discovery phase (same as BRSKI)
- Voucher exchange with deployment domain registrar (same as BRSKI).
- Enrollment phase (changed to accompany the application of self-contained objects for the enrollment).

6.1. Pledge - Registrar discovery and voucher exchange

The discovery phase is applied as specified in [I-D.ietf-anima-bootstrapping-keyinfra]. /* for discussion: is a reference to BRSKI sufficient here or is it helpful to provide additional information and the figure? */
Figure 2: Pledge discovery of domain registrar discovery and voucher exchange

6.2. Registrar - MASA voucher exchange

The voucher exchange is performed as specified in [I-D.ietf-anima-bootstrapping-keyinfra]. /* for discussion: is a reference to BRSKI sufficient here or is it helpful to provide additional information and the figure? */
6.3. Pledge - Registrar - RA/CA certificate enrollment

The enrollment for BRSKI-AE will be performed using a self-contained object. According to the abstract requirements from [I-D.ietf-anima-bootstrapping-keyinfra]. This object shall at least contain the following information:

- Proof of Possession: utilizing the private key corresponding to the public key contained in the certification request.
- Proof of Identity: utilizing the existing IDevID credential to generate a signature of the certification request.
- /* further parameter to be specified */.
Figure 4: Certificate enrollment

The following list provides an abstract description of the flow depicted in Figure 4.

- **CA Cert Request:** The pledge SHOULD request the full distribution of CA Certificates message. This ensures that the pledge has the complete set of current CA certificates beyond the pinned-domain-cert.
Attribute Request: Typically, the automated bootstrapping occurs without local administrative configuration of the pledge. Nevertheless, there are cases, in which the pledge should also include additional attributes specific to the deployment domain into the certification request. To get these attributes in advance, the attribute request SHOULD be used.

Cert Request: certification request message (to be done: reference to PKCS#10 or CRMF, proof of possession, pledge authentication)

Cert Response: certification response message containing the requested certificate and potentially further information like certificates of intermediary CAs on the certification path.

Cert Waiting: waiting indication for the pledge to retry after a given time. For this a request identifier is necessary. This request identifier may be either part of the enrollment protocol or build based on the certification request.

Cert Poling: querying the registrar, if the certificate request was already processed; can be answered either with another Cert Waiting, or a Cert Response.

Cert Confirm: confirmation message from pledge after receiving and verifying the certificate.

PKI/Registrar Confirm: confirmation message from PKI/registrar about reception of the pledge’s certificate confirmation.

7. Mapping to existing enrollment protocols

This sections maps the requirements and the approach described in Section 6.3 to already existing enrollment protocols.

7.1. EST Handling

When using the EST protocol [RFC7030], the following constrains should be observed:

- Proof of possession is provided by using the specified PKCS #10 structure in the request method.

- For proof of identity only the /fullcmc endpoint should be used with a fullcmc request. This contains sufficient information for
the RA/CA to make an authorization decision on the received certification request. Note that EST references CMC [RFC5272] for the definition of the full PKI request. For proof of identity, the signature of the SignedData of the Full PKI Request would be calculated using the IDEVID credential of the pledge. /*TBD: in this case the binding to the underlying TLS connection may not be necessary */

- When the CA/CA is not available, as per [RFC7030] Section 4.2.3, a 202 return code should be returned by the Join Registrar. The pledge in this case would retry with the same PKCS#10 request as in the initial simple enroll run. Note that if the TLS connection is teared down for the waiting time, the PKCS#10 request would need to be rebuild as it contains the unique identifier (tls_unique) from the underlying TLS connection for the binding.

7.2. CMP Handling

When using the CMP protocol [RFC4210], the following constrains should be observed:

- For proof of possession, the defined approach in CMP [RFC4210] section 4.3 should be supported. This can be achieved by using either CRMF or PKCS#10 to specify the certification request.

- Proof of identity can be provided by using the MSG_SIG_ALG to protect the certificate request message with signatures as outlined in section D.5.

- When the CA/CA is not available, as per [RFC4210] Section 5.2.3, a waiting indication should be returned in the PKIStatus by the Join Registrar. The pledge in this case would retry using the PollReqContent with a request identifier certReqId provided in the initial CertRequest message as specified in section 5.3.22.

8. IANA Considerations

This document requires the following IANA actions:

/* to be done: clarification necessary */

9. Privacy Considerations

/* to be done: clarification necessary */
10. Security Considerations

/* to be done: clarification necessary */

11. Acknowledgements

We would like to thank the various reviewers for their input, in particular Brian E. Carpenter, Giorgio Romanenghi, Oskar Camenzind for their input and discussion on use cases and call flows.

12. References

12.1. Normative References

[I-D.ietf-anima-bootstrapping-keyinfra]


12.2. Informative References


[ISO-IEC-15118-2]

[NERC-CIP-005-5]


Authors' Addresses
Abstract

Autonomic functions need a control plane to communicate, which depends on some addressing and routing. This Autonomic Management and Control Plane should ideally be self-managing, and as independent as possible of configuration. This document defines such a plane and calls it the "Autonomic Control Plane", with the primary use as a control plane for autonomic functions. It also serves as a "virtual out-of-band channel" for Operations Administration and Management (OAM) communications over a network that provides automatically configured hop-by-hop authenticated and encrypted communications via automatically configured IPv6 even when the network is not configured, or misconfigured.
This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction (Informative) ....................................... 6
   1.1. Applicability and Scope ..................................... 8
2. Acronyms and Terminology (Informative) .......................... 10
3. Use Cases for an Autonomic Control Plane (Informative) ....... 16
   3.1. An Infrastructure for Autonomic Functions ................. 16
   3.2. Secure Bootstrap over a not configured Network ........... 16
   3.3. Data-Plane Independent Permanent Reachability ............ 16
4. Requirements (Informative) ..................................... 18
5. Overview (Informative) ........................................ 19
6. Self-Creation of an Autonomic Control Plane (ACP) (Normative) 20
   6.1. ACP Domain, Certificate and Network ....................... 20
       6.1.1. ACP Certificates ..................................... 21
       6.1.2. ACP Certificate ACP Domain Information Field ........ 22
       6.1.3. ACP domain membership check .......................... 26
       6.1.4. Trust Points and Trust Anchors ....................... 28
       6.1.5. Certificate and Trust Point Maintenance .............. 29
           6.1.5.1. GRASP objective for EST server .................. 30
           6.1.5.2. Renewal ......................................... 31
           6.1.5.3. Certificate Revocation Lists (CRLs) .............. 31
           6.1.5.4. Lifetimes ....................................... 32
           6.1.5.5. Re-enrollment ................................... 32
           6.1.5.6. Failing Certificates ............................. 34
       6.2. ACP Adjacency Table ...................................... 34
       6.3. Neighbor Discovery with DULL GRASP ...................... 35
       6.4. Candidate ACP Neighbor Selection ......................... 38
       6.5. Channel Selection ....................................... 39
       6.6. Candidate ACP Neighbor verification ...................... 42
       6.7. Security Association protocols ........................... 42
           6.7.1. ACP via IKEv2 .................................... 43
               6.7.1.1. Native IPsec .................................. 43
               6.7.1.2. IPsec with GRE encapsulation .................. 44
           6.7.2. ACP via DTLS ...................................... 45
           6.7.3. ACP Secure Channel Requirements ..................... 45
       6.8. GRASP in the ACP ........................................ 46
           6.8.1. GRASP as a core service of the ACP ................. 46
           6.8.2. ACP as the Security and Transport substrate for GRASP 46
6.8.2.1. Discussion .............................................. 49
6.9. Context Separation ........................................... 50
6.10. Addressing inside the ACP .................................... 51
  6.10.1. Fundamental Concepts of Autonomic Addressing ............ 51
  6.10.2. The ACP Addressing Base Scheme .......................... 52
  6.10.3. ACP Zone Addressing Sub-Scheme .......................... 54
  6.10.3.1. Usage of the Zone-ID Field ............................. 55
  6.10.4. ACP Manual Addressing Sub-Scheme ........................ 56
  6.10.5. ACP Vlong Addressing Sub-Scheme ........................ 58
  6.10.6. Other ACP Addressing Sub-Schemes ........................ 59
  6.10.7. ACP Registrars ........................................... 59
    6.10.7.1. Use of BRSKI or other Mechanism/Protocols .......... 60
    6.10.7.2. Unique Address/Prefix allocation ..................... 60
    6.10.7.3. Addressing Sub-Scheme Policies ....................... 61
    6.10.7.4. Address/Prefix Persistence ........................... 62
    6.10.7.5. Further Details ....................................... 62
  6.11. Routing in the ACP .......................................... 62
    6.11.1. RPL Profile ........................................... 63
      6.11.1.1. Overview ........................................... 63
      6.11.1.2. RPL Instances ....................................... 65
      6.11.1.3. Storing vs. Non-Storing Mode .......................... 65
      6.11.1.4. DAO Policy .......................................... 65
      6.11.1.5. Path Metric .......................................... 65
      6.11.1.6. Objective Function ................................... 65
      6.11.1.7. DODAG Repair ........................................ 65
      6.11.1.8. Multicast ............................................ 66
      6.11.1.9. Security ............................................. 66
      6.11.1.10. P2P communications .................................. 66
      6.11.1.11. IPv6 address configuration ........................... 66
      6.11.1.12. Administrative parameters ............................ 66
      6.11.1.13. RPL Data-Plane artifacts ............................. 67
      6.11.1.14. Unknown Destinations ................................. 67
  6.12. General ACP Considerations .................................. 67
    6.12.1. Performance ............................................ 67
    6.12.2. Addressing of Secure Channels ............................ 68
    6.12.3. MTU .................................................... 68
    6.12.4. Multiple links between nodes ............................. 69
    6.12.5. ACP interfaces .......................................... 69
  7. ACP support on L2 switches/ports (Normative) .................... 72
    7.1. Why (Benefits of ACP on L2 switches) ........................ 72
    7.2. How (per L2 port DULL GRASP) ................................ 73
  8. Support for Non-ACP Components (Normative) ...................... 75
    8.1. ACP Connect ................................................. 75
      8.1.1. Non-ACP Controller / NMS system ........................ 75
      8.1.2. Software Components ..................................... 77
      8.1.3. Auto Configuration ...................................... 78
      8.1.4. Combined ACP/Data-Plane Interface (VRF Select) ........ 79
      8.1.5. Use of GRASP ............................................ 80
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2</td>
<td>ACP through Non-ACP L3 Clouds (Remote ACP neighbors)</td>
</tr>
<tr>
<td>8.2.1</td>
<td>Configured Remote ACP neighbor</td>
</tr>
<tr>
<td>8.2.2</td>
<td>Tunneled Remote ACP Neighbor</td>
</tr>
<tr>
<td>8.2.3</td>
<td>Summary</td>
</tr>
<tr>
<td>9</td>
<td>Benefits (Informative)</td>
</tr>
<tr>
<td>9.1</td>
<td>Self-Healing Properties</td>
</tr>
<tr>
<td>9.2</td>
<td>Self-Protection Properties</td>
</tr>
<tr>
<td>9.2.1</td>
<td>From the outside</td>
</tr>
<tr>
<td>9.2.2</td>
<td>From the inside</td>
</tr>
<tr>
<td>9.3</td>
<td>The Administrator View</td>
</tr>
<tr>
<td>10</td>
<td>ACP Operations (Informative)</td>
</tr>
<tr>
<td>10.1</td>
<td>ACP (and BRSKI) Diagnostics</td>
</tr>
<tr>
<td>10.2</td>
<td>ACP Registrars</td>
</tr>
<tr>
<td>10.2.1</td>
<td>Registrar interactions</td>
</tr>
<tr>
<td>10.2.2</td>
<td>Registrar Parameter</td>
</tr>
<tr>
<td>10.2.3</td>
<td>Certificate renewal and limitations</td>
</tr>
<tr>
<td>10.2.4</td>
<td>ACP Registrars with sub-CA</td>
</tr>
<tr>
<td>10.2.5</td>
<td>Centralized Policy Control</td>
</tr>
<tr>
<td>10.3</td>
<td>Enabling and disabling ACP/ANI</td>
</tr>
<tr>
<td>10.3.1</td>
<td>Filtering for non-ACP/ANI packets</td>
</tr>
<tr>
<td>10.3.2</td>
<td>Admin Down State</td>
</tr>
<tr>
<td>10.3.2.1</td>
<td>Security</td>
</tr>
<tr>
<td>10.3.2.2</td>
<td>Fast state propagation and Diagnostics</td>
</tr>
<tr>
<td>10.3.2.3</td>
<td>Low Level Link Diagnostics</td>
</tr>
<tr>
<td>10.3.2.4</td>
<td>Power Consumption Issues</td>
</tr>
<tr>
<td>10.3.3</td>
<td>Interface level ACP/ANI enable</td>
</tr>
<tr>
<td>10.3.4</td>
<td>Which interfaces to auto-enable?</td>
</tr>
<tr>
<td>10.3.5</td>
<td>Node Level ACP/ANI enable</td>
</tr>
<tr>
<td>10.3.5.1</td>
<td>Brownfield nodes</td>
</tr>
<tr>
<td>10.3.5.2</td>
<td>Greenfield nodes</td>
</tr>
<tr>
<td>10.3.6</td>
<td>Undoing ANI/ACP enable</td>
</tr>
<tr>
<td>10.3.7</td>
<td>Summary</td>
</tr>
<tr>
<td>10.4</td>
<td>Configuration and the ACP (summary)</td>
</tr>
<tr>
<td>11</td>
<td>Security Considerations</td>
</tr>
<tr>
<td>12</td>
<td>IANA Considerations</td>
</tr>
<tr>
<td>13</td>
<td>Acknowledgements</td>
</tr>
<tr>
<td>14</td>
<td>Change log [RFC Editor: Please remove]</td>
</tr>
<tr>
<td>14.1</td>
<td>Initial version</td>
</tr>
<tr>
<td>14.2</td>
<td>draft-behringer-anima-autonomic-control-plane-00</td>
</tr>
<tr>
<td>14.3</td>
<td>draft-behringer-anima-autonomic-control-plane-01</td>
</tr>
<tr>
<td>14.4</td>
<td>draft-behringer-anima-autonomic-control-plane-02</td>
</tr>
<tr>
<td>14.5</td>
<td>draft-behringer-anima-autonomic-control-plane-03</td>
</tr>
<tr>
<td>14.6</td>
<td>draft-ietf-anima-autonomic-control-plane-00</td>
</tr>
<tr>
<td>14.7</td>
<td>draft-ietf-anima-autonomic-control-plane-01</td>
</tr>
<tr>
<td>14.8</td>
<td>draft-ietf-anima-autonomic-control-plane-02</td>
</tr>
<tr>
<td>14.9</td>
<td>draft-ietf-anima-autonomic-control-plane-03</td>
</tr>
<tr>
<td>14.10</td>
<td>draft-ietf-anima-autonomic-control-plane-04</td>
</tr>
<tr>
<td>14.11</td>
<td>draft-ietf-anima-autonomic-control-plane-05</td>
</tr>
</tbody>
</table>
1. Introduction (Informative)

Autonomic Networking is a concept of self-management: Autonomic functions self-configure, and negotiate parameters and settings across the network. [RFC7575] defines the fundamental ideas and design goals of Autonomic Networking. A gap analysis of Autonomic Networking is given in [RFC7576]. The reference architecture for Autonomic Networking in the IETF is specified in the document [I-D.ietf-anima-reference-model].

Autonomic functions need an autonomically built communications infrastructure. This infrastructure needs to be secure, resilient and re-usable by all autonomic functions. Section 5 of [RFC7575] introduces that infrastructure and calls it the Autonomic Control Plane (ACP). More descriptively it would be the "Autonomic communications infrastructure for Management and Control". For naming consistency with that prior document, this document continues to use the name ACP though.

Today, the management and control plane of networks typically uses a routing and forwarding table which is dependent on correct configuration and routing. Misconfigurations or routing problems can disrupt management and control channels. Traditionally, an out-of-band network has been used to avoid or allow recovery from such problems, or personnel are sent on site to access devices through out-of-band management ports (also called craft ports, serial console, management ethernet port). However, both options are expensive.

In increasingly automated networks either centralized management systems or distributed autonomic service agents in the network require a control plane which is independent of the configuration of the network they manage, to avoid impacting their own operations through the configuration actions they take.

This document describes a modular design for a self-forming, self-managing and self-protecting Autonomic Control Plane (ACP), which is a virtual in-band network designed to be as independent as possible of configuration, addressing and routing problems. The details how this is achieved are described in Section 6. The ACP is designed to remain operational even in the presence of configuration errors, addressing or routing issues, or where policy could inadvertently affect connectivity of both data packets or control packets.

This document uses the term "Data-Plane" to refer to anything in the network nodes that is not the ACP, and therefore considered to be dependent on (mis-)configuration. This Data-Plane includes both the traditional forwarding-plane, as well as any pre-existing control-
plane, such as routing protocols that establish routing tables for the forwarding plane.

The Autonomic Control Plane serves several purposes at the same time:

1. Autonomic functions communicate over the ACP. The ACP therefore directly supports Autonomic Networking functions, as described in [I-D.ietf-anima-reference-model]. For example, Generic Autonomic Signaling Protocol (GRASP - [I-D.ietf-anima-grasp]) runs securely inside the ACP and depends on the ACP as its "security and transport substrate".

2. A controller or network management system can use it to securely bootstrap network devices in remote locations, even if the (Data-Plane) network in between is not yet configured; no Data-Plane dependent bootstrap configuration is required. An example of such a secure bootstrap process is described in [I-D.ietf-anima-bootstrapping-keyinfra].

3. An operator can use it to log into remote devices, even if the network is misconfigured or not configured.

This document describes these purposes as use cases for the ACP in Section 3, it defines the requirements in Section 4. Section 5 gives an overview how the ACP is constructed.

The normative part of this document starts with Section 6, where the ACP is specified. Section 7 defines normative how to support ACP on L2 switches. Section 8 explains normative how non-ACP nodes and networks can be integrated.

The remaining sections are non-normative: Section 9 reviews benefits of the ACP (after all the details have been defined), Section 10 provides operational recommendations, Appendix A provides additional explanations and describes additional details or future standard or propriety extensions that were considered not to be appropriate for standardization in this document but were considered important to document. There are no dependencies against Appendix A to build a complete working and interoperable ACP according to this document.

The ACP provides secure IPv6 connectivity, therefore it can be used not only as the secure connectivity for self-management as required for the ACP in [RFC7575], but it can also be used as the secure connectivity for traditional (centralized) management. The ACP can be implemented and operated without any other components of autonomic networks, except for the GRASP protocol. ACP relies on per-link DULL GRASP (see Section 6.3) to autodiscover ACP neighbors, and includes the ACP GRASP instance to provide service discovery for clients of...
the ACP (see Section 6.8) including for its own maintenance of ACP
certificates.

The document "Using Autonomic Control Plane for Stable Connectivity
of Network OAM" [RFC8368] describes how the ACP alone can be used to
provide secure and stable connectivity for autonomic and non-
autonomic Operations Administration and Management (OAM)
applications. That document also explains how existing management
solutions can leverage the ACP in parallel with traditional
management models, when to use the ACP and how to integrate with
potentially IPv4 only OAM backends.

Combining ACP with Bootstrapping Remote Secure Key Infrastructures
(BRSKI), see [I-D.ietf-anima-bootstrapping-keyinfra]) results in the
"Autonomic Network Infrastructure" as defined in
[I-D.ietf-anima-reference-model], which provides autonomic
connectivity (from ACP) with secure zero-touch (automated) bootstrap
from BRSKI. The ANI itself does not constitute an Autonomic Network,
but it allows the building of more or less autonomic networks on top
of it - using either centralized, Software Defined Networking-
(SDN-)style (see [RFC7426]) automation or distributed automation via
Autonomic Service Agents (ASA) / Autonomic Functions (AF) - or a
mixture of both. See [I-D.ietf-anima-reference-model] for more
information.

1.1. Applicability and Scope

Please see the following Terminology section (Section 2) for
explanations of terms used in this section.

The design of the ACP as defined in this document is considered to be
applicable to all types of "professionally managed" networks: Service
Provider, Local Area Network (LAN), Metro(politan networks), Wide
Area Network (WAN), Enterprise Information Technology (IT) and
->"Operational Technology" (OT) networks. The ACP can operate
equally on layer 3 equipment and on layer 2 equipment such as bridges
(see Section 7). The hop-by-hop authentication and confidentiality
mechanism used by the ACP is defined to be negotiable, therefore it
can be extended to environments with different protocol preferences.
The minimum implementation requirements in this document attempt
to achieve maximum interoperability by requiring support for multiple
options depending on the type of device: IPsec, see [RFC4301], and
datagram Transport Layer Security version 1.2 (DTLS), see [RFC6347]).

The implementation footprint of the ACP consists of Public Key
Infrastructure (PKI) code for the ACP certificate, the GRASP
protocol, UDP, TCP and TLS (for security and reliability of GRASP),
the ACP secure channel protocol used (such as IPsec or DTLS), and an
instance of IPv6 packet forwarding and routing via the Routing Protocol for Low-power and Lossy Networks (RPL), see [RFC6550], that is separate from routing and forwarding for the Data-Plane (user traffic).

The ACP uses only IPv6 to avoid complexity of dual-stack ACP operations (IPv6/IPv4). Nevertheless, it can without any changes be integrated into even otherwise IPv4-only network devices. The Data-Plane itself would not need to change, it could continue to be IPv4 only. For such IPv4 only devices, the IPv6 protocol itself would be additional implementation footprint only used for the ACP.

The protocol choices of the ACP are primarily based on wide use and support in networks and devices, well understood security properties and required scalability. The ACP design is an attempt to produce the lowest risk combination of existing technologies and protocols to build a widely applicable operational network management solution:

RPL was chosen because it requires a smaller routing table footprint in large networks compared to other routing protocols with an autonomically configured single area. The deployment experience of large scale Internet of Things (IoT) networks serves as the basis for wide deployment experience with RPL. The profile chosen for RPL in the ACP does not leverage any RPL specific forwarding plane features (IPv6 extension headers), making its implementation a pure control plane software requirement.

GRASP is the only completely novel protocol used in the ACP, and this choice was necessary because there is no existing suitable protocol to provide the necessary functions to the ACP, so GRASP was developed to fill that gap.

The ACP design can be applicable to (cpu, memory) constrained devices and (bitrate, reliability) constrained networks, but this document does not attempt to define the most constrained type of devices or networks to which the ACP is applicable. RPL and DTLS for ACP secure channels are two protocol choices already making ACP more applicable to constrained environments. Support for constrained devices in this specification is opportunistic, but not complete, because the reliable transport for GRASP (see Section 6.8.2) only specifies TCP/TLS. See Appendix A.9 for discussions about how future standards or proprietary extensions/variations of the ACP could better meet different expectations from those on which the current design is based including supporting constrained devices better.
2. Acronyms and Terminology (Informative)

[RFCEditor: WG/IETF/IESG review of the terms below asked for references between these terms when they refer to each other. The only option I could find RFC/XML to point to a hanging text acronym definition that also displays the actual term is the format="title" version, which leads to references such as ‘->"ACP domain certificate" ()’. I found no reasonable way to eliminate the trailing ‘()’ generated by this type of cross references. Can you please take care of removing these artefacts during editing (after conversion to nroff?). I also created a ticket to ask for an xml2rfc enhancement to avoid this in the future: https://trac.tools.ietf.org/tools/xml2rfc/trac/ticket/347.

[RFCEditor: Question: Is it possible to change the first occurrences of [RFCxxxx] references to "rfcxxx title" [RFCxxxx]? the XML2RFC format does not seem to offer such a format, but I did not want to duplicate 50 first references - one reference for title mentioning and one for RFC number.]

In the rest of the document we will refer to systems using the ACP as "nodes". Typically such a node is a physical (network equipment) device, but it can equally be some virtualized system. Therefore, we do not refer to them as devices unless the context specifically calls for a physical system.

This document introduces or uses the following terms (sorted alphabetically). Terms introduced are explained on first use, so this list is for reference only.

ACP: "Autonomic Control Plane". The Autonomic Function as defined in this document. It provides secure zero-touch (automated) transitive (network wide) IPv6 connectivity for all nodes in the same ACP domain as well as a GRASP instance running across this ACP IPv6 connectivity. The ACP is primarily meant to be used as a component of the ANI to enable Autonomic Networks but it can equally be used in simple ANI networks (with no other Autonomic Functions) or completely by itself.

ACP address: An IPv6 address assigned to the ACP node. It is stored in the domain information field of the "ACP domain certificate" ()

ACP address range/set: The ACP address may imply a range or set of addresses that the node can assign for different purposes. This address range/set is derived by the node from the format of the ACP address called the "addressing sub-scheme".
ACP connect interface: An interface on an ACP node providing access to the ACP for non ACP capable nodes without using an ACP secure channel. See Section 8.1.1.

ACP domain: The ACP domain is the set of nodes with "ACP domain certificates" that allow them to authenticate each other as members of the ACP domain. See also Section 6.1.3.

ACP (ANI/AN) Domain Certificate: A [RFC5280] certificate (LDevID) carrying the domain information field which is used by the ACP to learn its address in the ACP and to derive and cryptographically assert its membership in the ACP domain.

domain information (field): An rfc822Name information element (e.g., field) in the domain certificate in which the ACP relevant information is encoded: the domain name and the ACP address.

ACP Loopback interface: The Loopback interface in the ACP Virtual Routing and Forwarding (VRF) that has the ACP address assigned to it.

ACP network: The ACP network constitutes all the nodes that have access to the ACP. It is the set of active and transitively connected nodes of an ACP domain plus all nodes that get access to the ACP of that domain via ACP edge nodes.

ACP (ULA) prefix(es): The /48 IPv6 address prefixes used across the ACP. In the normal/simple case, the ACP has one ULA prefix, see Section 6.10. The ACP routing table may include multiple ULA prefixes if the "rsub" option is used to create addresses from more than one ULA prefix. See Section 6.1.2. The ACP may also include non-ULA prefixes if those are configured on ACP connect interfaces. See Section 8.1.1.

ACP secure channel: A cryptographically authenticated and encrypted data connection established between (normally) adjacent ACP nodes to carry traffic of the ACP VRF securely and isolated from Data-Plane traffic in-band over the same link/path as the Data-Plane.

ACP secure channel protocol: The protocol used to build an ACP secure channel, e.g., Internet Key Exchange Protocol version 2 (IKEv2) with IPsec or Datagram Transport Layer Security (DTLS).

ACP virtual interface: An interface in the ACP VRF mapped to one or more ACP secure channels. See Section 6.12.5.
AN "Autonomic Network": A network according to [I-D.ietf-anima-reference-model]. Its main components are ANI, Autonomic Functions and Intent.

(AN) Domain Name: An FQDN (Fully Qualified Domain Name) in the domain information field of the Domain Certificate. See Section 6.1.2.

ANI (nodes/network): "Autonomic Network Infrastructure". The ANI is the infrastructure to enable Autonomic Networks. It includes ACP, BRSKI and GRASP. Every Autonomic Network includes the ANI, but not every ANI network needs to include autonomic functions beyond the ANI (nor Intent). An ANI network without further autonomic functions can for example support secure zero-touch (automated) bootstrap and stable connectivity for SDN networks - see [RFC8368].

ANIMA: "Autonomic Networking Integrated Model and Approach". ACP, BRSKI and GRASP are products of the IETF ANIMA working group.

ASA: "Autonomic Service Agent". Autonomic software modules running on an ANI device. The components making up the ANI (BRSKI, ACP, GRASP) are also described as ASAs.

Autonomic Function: A function/service in an Autonomic Network (AN) composed of one or more ASA across one or more ANI nodes.

BRSKI: "Bootstrapping Remote Secure Key Infrastructures" ([I-D.ietf-anima-bootstrapping-keyinfra]. A protocol extending EST to enable secure zero-touch bootstrap in conjunction with ACP. ANI nodes use ACP, BRSKI and GRASP.

Data-Plane: The counterpoint to the ACP VRF in an ACP node: all routing and forwarding in the node other than the ACP VRF. In a simple ACP or ANI node, the Data-Plane is typically provisioned by means other than autonomically, for example manually (including across the ACP) or via SDN controllers. In a fully Autonomic Network node, the Data-Plane is managed autonomically via Autonomic Functions and Intent. Note that other (non-ANIMA) RFCs use the Data-Plane to refer to what is better called the forwarding plane. This is not the way the term is used in this document!

device: A physical system, or physical node.

Enrollment: The process where a node presents identification (for example through keying material such as the private key of an IDevID) to a network and acquires a network specific identity uch
as an LDevID and trust anchors such as Certificate Authority (CA) certificates.

EST: "Enrollment over Secure Transport" ([RFC7030]). IETF standard-track protocol for enrollment of a node with an LDevID. BRSKI is based on EST.

GRASP: "Generic Autonomic Signaling Protocol". An extensible signaling protocol required by the ACP for ACP neighbor discovery. The ACP also provides the "security and transport substrate" for the "ACP instance of GRASP". This instance of GRASP runs across the ACP secure channels to support BRSKI and other NOC/OAM or Autonomic Functions. See [I-D.ietf-anima-grasp].

IDevID: An "Initial Device IDentity" X.509 certificate installed by the vendor on new equipment. Contains information that establishes the identity of the node in the context of its vendor/manufacturer such as device model/type and serial number. See [AR8021]. IDevID cannot be used for the ACP because they are not provisioned by the owner of the network, so they can not directly indicate an ACP domain they belong to.

in-band (management): The type of management used predominantly in IP based networks, not leveraging an ->"out-of-band network" (). In in-band management, access to the managed equipment depends on the configuration of this equipment itself: interface, addressing, forwarding, routing, policy, security, management. This dependency makes in-band management fragile because the configuration actions performed may break in-band management connectivity. Breakage can not only be unintentional, it can simply be an unavoidable side effect of being unable to create configuration schemes where in-band management connectivity configuration is unaffected by Data-Plane configuration. See also ->"(virtual) out-of-band network" ()

Intent: Policy language of an autonomic network according to [I-D.ietf-anima-reference-model].

Loopback interface: The conventional name for an internal IP interface to which addresses may be assigned, but which transmits no external traffic.

LDevID: A "Local Device IDentity" is an X.509 certificate installed during "enrollment". The Domain Certificate used by the ACP is an LDevID. See [AR8021].
MIC: "Manufacturer Installed Certificate". This is another word to describe an IDevID in referenced materials. This term is not used in this document.

native interface: Interfaces existing on a node without configuration of the already running node. On physical nodes these are usually physical interfaces. On virtual nodes their equivalent.

node: A system, e.g., supporting the ACP according to this document. Can be virtual or physical. Physical nodes are called devices.

Node-ID: The identifier of an ACP node inside that ACP. It is the last 64 (see Section 6.10.3) or 78-bits (see Section 6.10.5) of the ACP address.

Operational Technology (OT): "https://en.wikipedia.org/wiki/Operational_Technology" [1]: "The hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, etc.". OT networks are today in most cases well separated from Information Technology (IT) networks.

(virtual) out-of-band network: An out-of-band network is a secondary network used to manage a primary network. The equipment of the primary network is connected to the out-of-band network via dedicated management ports on the primary network equipment. Serial (console) management ports were historically most common, higher end network equipment now also has ethernet ports dedicated only for management. An out-of-band network provides management access to the primary network independent of the configuration state of the primary network. One of the goals of the ACP is to provide this benefit of out-of-band networks virtually on the primary network equipment. The ACP VRF acts as a virtual out of band network device providing configuration independent management access. The ACP secure channels are the virtual links of the ACP virtual out-of-band network, meant to be operating independent of the configuration of the primary network. See also ->"in-band (management)" ()..

RPL: "IPv6 Routing Protocol for Low-Power and Lossy Networks". The routing protocol used in the ACP. See [RFC6550].

MASA (service): "Manufacturer Authorized Signing Authority". A vendor/manufacturer or delegated cloud service on the Internet used as part of the BRSKI protocol.
(ACP/ANI/BRSKI) Registrar: An ACP registrar is an entity (software and/or person) that is orchestrating the enrollment of ACP nodes with the ACP domain certificate. ANI nodes use BRSKI, so ANI registrars are also called BRSKI registrars. For non-ANI ACP nodes, the registrar mechanisms are undefined by this document. See Section 6.10.7. Renewal and other maintenance (such as revocation) of ACP domain certificates may be performed by other entities than registrars. EST must be supported for ACP domain certificate renewal (see Section 6.1.5). BRSKI is an extension of EST, so ANI/BRSKI registrars can easily support ACP domain certificate renewal in addition to initial enrollment.

sUDI: "secured Unique Device Identifier". This is another word to describe an IDevID in referenced material. This term is not used in this document.

UDI: "Unique Device Identifier". In the context of this document unsecured identity information of a node typically consisting of at least device model/type and serial number, often in a vendor specific format. See sUDI and LDevID.

ULA: (Global ID prefix) A "Unique Local Address" (ULA) is an IPv6 address in the block fc00::/7, defined in [RFC4193]. It is the approximate IPv6 counterpart of the IPv4 private address ([RFC1918]). The ULA Global ID prefix are the first 48-bits of a ULA address. In this document it is abbreviated as "ULA prefix".

(ACP) VRF: The ACP is modeled in this document as a "Virtual Routing and Forwarding" instance (VRF). This means that it is based on a "virtual router" consisting of a separate IPv6 forwarding table to which the ACP virtual interfaces are attached and an associated IPv6 routing table separate from the Data-Plane. Unlike the VRFs on MPLS/VPN-PE ([RFC4364]) or LISP XTR ([RFC6830]), the ACP VRF does not have any special "core facing" functionality or routing/mapping protocols shared across multiple VRFs. In vendor products a VRF such as the ACP-VRF may also be referred to as a so called VRF-lite.

(ACP) Zone: An ACP zone is a set of ACP nodes using the same zone field value in their ACP address according to Section 6.10.3. Zones are a mechanism to support structured addressing of ACP addresses within the same /48-bit ULA prefix.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119],[RFC8174] when, and only when, they appear in all capitals, as shown here.
3. Use Cases for an Autonomic Control Plane (Informative)

3.1. An Infrastructure for Autonomic Functions

Autonomic Functions need a stable infrastructure to run on, and all autonomic functions should use the same infrastructure to minimize the complexity of the network. In this way, there is only need for a single discovery mechanism, a single security mechanism, and single instances of other processes that distributed functions require.

3.2. Secure Bootstrap over a not configured Network

Today, bootstrapping a new node typically requires all nodes between a controlling node such as an SDN controller ("Software Defined Networking", see [RFC7426]) and the new node to be completely and correctly addressed, configured and secured. Bootstrapping and configuration of a network happens in rings around the controller - configuring each ring of devices before the next one can be bootstrapped. Without console access (for example through an out-of-band network) it is not possible today to make devices securely reachable before having configured the entire network leading up to them.

With the ACP, secure bootstrap of new devices and whole new networks can happen without requiring any configuration of unconfigured devices along the path: As long as all devices along the path support ACP and a zero-touch bootstrap mechanism such as BRSKI, the ACP across a whole network of unconfigured devices can be brought up without operator/provisioning intervention. The ACP also provides additional security for any bootstrap mechanism, because it can provide encrypted discovery (via ACP GRASP) of registrars or other bootstrap servers by bootstrap proxies connecting to nodes that are to be bootstrapped and the ACP encryption hides the identities of the communicating entities (pledge and registrar), making it more difficult to learn which network node might be attackable. The ACP domain certificate can also be used to end-to-end encrypt the bootstrap communication between such proxies and server. Note that bootstrapping here includes not only the first step that can be provided by BRSKI (secure keys), but also later stages where configuration is bootstrapped.

3.3. Data-Plane Independent Permanent Reachability

Today, most critical control plane protocols and network management protocols are using the Data-Plane of the network. This leads to often undesirable dependencies between control and management plane on one side and the Data-Plane on the other: Only if the forwarding
and control plane of the Data-Plane are configured correctly, will the Data-Plane and the management plane work as expected.

Data-Plane connectivity can be affected by errors and faults, for example misconfigurations that make AAA (Authentication, Authorization and Accounting) servers unreachable or can lock an administrator out of a device; routing or addressing issues can make a device unreachable; shutting down interfaces over which a current management session is running can lock an admin irreversibly out of the device. Traditionally only out-of-band access can help recover from such issues (such as serial console or ethernet management port).

Data-Plane dependencies also affect applications in a Network Operations Center (NOC) such as SDN controller applications: Certain network changes are today hard to implement, because the change itself may affect reachability of the devices. Examples are address or mask changes, routing changes, or security policies. Today such changes require precise hop-by-hop planning.

Note that specific control plane functions for the Data-Plane often want to depend on forwarding of their packets via the Data-Plane: Aliveness and routing protocol signaling packets across the Data-Plane to verify reachability across the Data-Plane, using IPv4 signaling packets for IPv4 routing vs. IPv6 signaling packets for IPv6 routing.

Assuming appropriate implementation (see Section 6.12.2 for more details), the ACP provides reachability that is independent of the Data-Plane. This allows the control plane and management plane to operate more robustly:

- For management plane protocols, the ACP provides the functionality of a Virtual out-of-band (VooB) channel, by providing connectivity to all nodes regardless of their Data-Plane configuration, routing and forwarding tables.

- For control plane protocols, the ACP allows their operation even when the Data-Plane is temporarily faulty, or during transitional events, such as routing changes, which may affect the control plane at least temporarily. This is specifically important for autonomic service agents, which could affect Data-Plane connectivity.

The document "Using Autonomic Control Plane for Stable Connectivity of Network OAM" [RFC8368] explains this use case for the ACP in significantly more detail and explains how the ACP can be used in practical network operations.
4. Requirements (Informative)

The following requirements were identified for the design of the ACP based on the above use-cases (Section 3). These requirements are informative. The ACP as specified in the normative parts of this document is meeting or exceeding these use-case requirements:

ACP1: The ACP should provide robust connectivity: As far as possible, it should be independent of configured addressing, configuration and routing. Requirements 2 and 3 build on this requirement, but also have value on their own.

ACP2: The ACP must have a separate address space from the Data-Plane. Reason: traceability, debug-ability, separation from Data-Plane, infrastructure security (filtering based on known address space).

ACP3: The ACP must use autonomically managed address space. Reason: easy bootstrap and setup ("autonomic"); robustness (admin cannot break network easily). This document suggests using ULA addressing for this purpose ("Unique Local Address", see [RFC4193]).

ACP4: The ACP must be generic, that is it must be usable by all the functions and protocols of the ANI. Clients of the ACP must not be tied to a particular application or transport protocol.

ACP5: The ACP must provide security: Messages coming through the ACP must be authenticated to be from a trusted node, and should (very strong should) be encrypted.

Explanation for ACP4: In a fully autonomic network (AN), newly written ASA could potentially all communicate exclusively via GRASP with each other, and if that was assumed to be the only requirement against the ACP, it would not need to provide IPv6 layer connectivity between nodes, but only GRASP connectivity. Nevertheless, because ACP also intends to support non-AN networks, it is crucial to support IPv6 layer connectivity across the ACP to support any transport and application layer protocols.

The ACP operates hop-by-hop, because this interaction can be built on IPv6 link local addressing, which is autonomic, and has no dependency on configuration (requirement 1). It may be necessary to have ACP connectivity across non-ACP nodes, for example to link ACP nodes over the general Internet. This is possible, but introduces a dependency against stable/resilient routing over the non-ACP hops (see Section 8.2).
5. Overview (Informative)

The Autonomic Control Plane is constructed in the following way (for details, see Section 6):

1. An ACP node creates a Virtual Routing and Forwarding (VRF) instance, or a similar virtual context.

2. It determines, following a policy, a candidate peer list. This is the list of nodes to which it should establish an Autonomic Control Plane. Default policy is: To all link-layer adjacent nodes supporting ACP.

3. For each node in the candidate peer list, it authenticates that node (according to Section 6.1.3) and negotiates a mutually acceptable channel type.

4. For each node in the candidate peer list, it then establishes a secure tunnel of the negotiated channel type. The resulting tunnels are then placed into the previously set up VRF. This creates an overlay network with hop-by-hop tunnels.

5. Inside the ACP VRF, each node assigns its ULA IPv6 address to a Loopback interface assigned to the ACP VRF.

6. Each node runs a lightweight routing protocol, to announce reachability of the virtual addresses inside the ACP (see Section 6.12.5).

Note:

- Non-ACP NMS ("Network Management Systems") or SDN controllers have to be explicitly configured for connection into the ACP.

- Connecting over non-ACP Layer-3 clouds requires explicit configuration. See Section 8.2.

- None of the above operations (except explicit configured ones) are reflected in the configuration of the node.

The following figure illustrates the ACP.
The resulting overlay network is normally based exclusively on hop-by-hop tunnels. This is because addressing used on links is IPv6 link local addressing, which does not require any prior set-up. In this way the ACP can be built even if there is no configuration on the node, or if the Data-Plane has issues such as addressing or routing problems.

6. Self-Creation of an Autonomic Control Plane (ACP) (Normative)

This section describes the components and steps to set up an Autonomic Control Plane (ACP), and highlights the key properties which make it "indestructible" against many inadvertent changes to the Data-Plane, for example caused by misconfigurations.

An ACP node can be a router, switch, controller, NMS host, or any other IP capable node. Initially, it must have its ACP domain certificate, as well as an (empty) ACP Adjacency Table (described in Section 6.2). It then can start to discover ACP neighbors and build the ACP. This is described step by step in the following sections:

6.1. ACP Domain, Certificate and Network

The ACP relies on group security. An ACP domain is a group of nodes that trust each other to participate in ACP operations. To establish trust, each ACP member requires keying material: An ACP node MUST have a certificate (LDevID) and a Trust Anchor (TA) consisting of a certificate (chain) used to sign the LDevID of all ACP domain members. The LDevID is used to cryptographically authenticate the membership of its owner node in the ACP domain to other ACP domain members. The TA is used to authenticate the ACP domain membership of other nodes (see Section 6.1.3).
The LDevID is called the ACP domain certificate, the TA is the Certificate Authority (CA) of the ACP domain.

The ACP does not mandate specific mechanisms by which this keying material is provisioned into the ACP node. It only requires the Domain information field as specified in Section 6.1.2 in its domain certificate as well as those of candidate ACP peers. See Appendix A.2 for more information about enrollment or provisioning options.

This document uses the term ACP in many places where the Autonomic Networking reference documents [RFC7575] and [I-D.ietf-anima-reference-model] use the word autonomic. This is done because those reference documents consider (only) fully autonomic networks and nodes, but support of ACP does not require support for other components of autonomic networks except for relying on GRASP and providing security and transport for GRASP. Therefore the word autonomic might be misleading to operators interested in only the ACP.

[RFC7575] defines the term "Autonomic Domain" as a collection of autonomic nodes. ACP nodes do not need to be fully autonomic, but when they are, then the ACP domain is an autonomic domain. Likewise, [I-D.ietf-anima-reference-model] defines the term "Domain Certificate" as the certificate used in an autonomic domain. The ACP domain certificate is that domain certificate when ACP nodes are (fully) autonomic nodes. Finally, this document uses the term ACP network to refer to the network created by active ACP nodes in an ACP domain. The ACP network itself can extend beyond ACP nodes through the mechanisms described in Section 8.1.

6.1.1. ACP Certificates

ACP domain certificates are [RFC5280] compliant X.509 certificates.

An ACP domain certificate MUST have an Elliptic Curve Diffie-Hellman (ECDH) public key. It SHOULD be signed with an ECDH public key. Otherwise it MUST be signed with an RSA key. Any secure channel protocols used for the ACP as specified in this document or extensions MUST therefore support authentication (e.g.:signing) starting with these type of certificates. See [RFC4492] for more information.

The ACP domain certificate SHOULD be used for any authentication between nodes with ACP domain certificates (ACP nodes and NOC nodes) where the required authorization condition is ACP domain membership, such as ACP node to NOC/OAM end-to-end security and ASA to ASA end-to-end security. Section 6.1.3 defines this "ACP domain membership
The uses of this check that are standardized in this document are for the establishment of hop-by-hop ACP secure channels (Section 6.6) and for ACP GRASP (Section 6.8.2) end-to-end via TLS ([RFC5246]).

The ACP domain membership check requires a minimum amount of elements in a certificate as described in Section 6.1.3. All elements are [RFC5280] compliant. The identity of a node in the ACP is carried via the ACP Domain Information Field as defined in Section 6.1.2 which is encoded as an rfc822Name field.

Any other field of the ACP domain certificate is to be populated as required by [RFC5280] or desired by the operator of the ACP domain ACP registrars/CA and required by other purposes that the ACP domain certificate is intended to be used for.

For diagnostic and other operational purposes, it is beneficial to copy the device identifying fields of the node’s IDevID into the ACP domain certificate, such as the "serialNumber" (see [I-D.ietf-anima-bootstrapping-keyinfra] section 2.3.1). Inclusion of this information makes it easier to potentially attack the node though, for example by learning the device model, which may help to select a fitting subset of attacks. Neighboring attackers can retrieve the certificate through an otherwise unsuccessful initiation of a secure channel association.

Note that there is no intention to constrain authorization within the ACP or autonomic networks using the ACP to just the ACP domain membership check as defined in this document. It can be extended or modified with future requirements. Such future authorizations can use and require additional elements in certificates or policies or even additional certificates. For an example, see Appendix A.10.5.

6.1.2. ACP Certificate ACP Domain Information Field

Information about the domain MUST be encoded in the domain certificate in a subjectAltName / rfc822Name field according to the following ABNF ([RFC5234]) definition:

[RFC Editor: Please substitute SELF in all occurrences of rfcSELF in this document with the RFC number assigned to this document and remove this comment line]
domain-information = local-part "@" acp-domain-name
local-part = key [ "." local-info ]
key = "rfcSELF"
local-info = [ acp-address ] [ "+" rsup extensions ]
acp-address = 32HEXDIG | 0 ; HEXDIG as of RFC5234 section B.1
rsup = [ <subdomain> ] ; <subdomain> as of RFC1034, section 3.5
acp-domain-name = ; <domain> ; as of RFC 1034, section 3.5
extensions = *( "+" extension )
extension = ; future standard definition.
               ; Must fit RFC5322 simple dot-atom format.

routing-subdomain = [ rsup "." ] acp-domain-name

Example:
   given an ACP address of fd89:b714:f3db:0:200:0:6400:0000
   and an ACP domain-name of acp.example.com
   and an rsub extension of area51.research
then this results in:
domain-information = rfcSELF+fd89b714f3db0000020000064000000
                  +area51.research@acp.example.com
acp-domain-name = acp.example.com
routing-subdomain = area51.research.acp.example.com

Figure 2: ACP Domain Information Field ABNF

domain-information is the encoded information that is put into the
ACP domain certificates subjectAltName / rfc822Name field. routing-
subdomain is a string that can be constructed from the domain-
information, and it is used in the hash-creation of the ULA (see
below). The requirements and semantics of the parts of this
information are explained in the following paragraphs:

Nodes complying with this specification MUST be able to receive their
ACP address through the domain certificate, in which case their own
ACP domain certificate MUST have the 32HEXDIG "acp-address" field.
Nodes complying with this specification MUST also be able to
authenticate nodes as ACP domain members / ACP secure channel peers
when they have an empty or 0-value acp-address field. See
Section 6.1.3.

"acp-domain-name" is used to indicate the ACP Domain across which all
ACP nodes trust each other and are willing to build ACP channels to
each other. See Section 6.1.3. Acp-domain-name SHOULD be the FQDN
of a DNS domain owned by the operator assigning the certificate.
This is a simple method to ensure that the domain is globally unique
and collision of ACP addresses would therefore only happen due to ULA
hash collisions (see Section 6.10.2). If the operator does not own

any FQDN, it should choose a string (in FQDN format) that it intends to be equally unique.

To keep the encoding simple, there is no consideration for internationalized acp-domain-names. The ACP domain information is not intended for enduser consumption, and there is no protection against someone not owning a domain name to simply choose it. Instead, it only serves as a hash seed for the ULA and for diagnostics to the operator. Therefore, any operator owning only an internationalized domain name should be able to pick an equivalently unique 7-bit ASCII acp-domain-name string representing the internationalized domain name.

"routing-subdomain" is a heuristic that allows a Registrar to consistently generate a unique 48-bit ULA prefix for ACP addresses. The presence of the "rsub" component allows to a single ACP domain to employ multiple /48 ULA prefixes. See Appendix A.7 for example use-cases.

The optional "extensions" field is used for future standardized extensions to this specification. It MUST be ignored if present and not understood.

Formatting notes:

- "rsub" needs to be in the "local-part": If the format just had routing-subdomain as the domain part of the domain-information, rsub and acp-domain-name could not be separated from each other. It also makes domain-information a valid e-mail target across all routing-subdomains.

- "acp-address" cannot use standard IPv6 address formats because it must match the simple dot-atom format of [RFC5322]. The character ":" is not allowed in that format.

- If "acp-address" is empty, and "rsub" is empty too, the "local-part" will have the format "rfcSELF++extension(s)". The two plus characters are necessary so the node can unambiguously parse that both "acp-address" and "rsub" are empty.

- The maximum size of "domain-information" is 254 characters and the maximum size of local-part is 64 characters according to [RFC5280] that is referring to [RFC2821] (superseded by [RFC5321]).

The subjectAltName / rfc822Name encoding of the ACP domain name and ACP address is used for the following reasons:
It should be possible to use the ACP domain certificate as an LDevID on the system for other uses beside the ACP. Therefore, the information element required for the ACP should be encoded so that it minimizes the possibility of creating incompatibilities with such other uses.

The information for the ACP should not cause incompatibilities with any pre-existing ASN.1 software. This eliminates the introduction of a novel information element because that could require extensions to such pre-existing ASN.1 parsers.

subjectAltName / rfc822Name is a pre-existing element that must be supported by all existing ASN.1 parsers for LDevID.

The element required for the ACP should not be misinterpreted by any other uses of the LDevID. If the element used for the ACP is interpreted by other uses, the impact should be benign.

The element should not require additional ASN.1 en/decoding, because it is unclear if all, especially embedded devices certificate libraries would support extensible ASN.1 functionality.

Using an IP address format encoding could result in non-benign misinterpretation of the domain information field; other uses unaware of the ACP could try to do something with the ACP address that would fail to work correctly. For example, the address could be interpreted to be an address of the node which does not belong to the ACP VRF.

At minimum, both the AN domain name and the non-domain name derived part of the ACP address need to be encoded in one or more appropriate fields of the certificate, so there are not many alternatives with pre-existing fields where the only possible conflicts would likely be beneficial.

rfc822Name encoding is very flexible. It allows to encode all the different fields of information required for the ACP.

The format of the rfc822Name is chosen so that an operator can set up a mailbox called rfcSELF@<domain> that would receive emails sent towards the rfc822Name of any node inside a domain. This is possible because in many modern mail systems, components behind a "+" character are considered part of a single mailbox. In other words, it is not necessary to set up a separate mailbox for every ACP node, but only one for the whole domain.
In result, if any unexpected use of the ACP addressing information in a certificate happens, it is benign and detectable: it would be mail to that mailbox.

See section 4.2.1.6 of [RFC5280] for details on the subjectAltName field.

6.1.3. ACP domain membership check

The following points constitute the ACP domain membership check of a candidate peer via its certificate:

1: The peer certificate is valid (lifetime).

2: The peer has proved ownership of the private key associated with the certificate’s public key. This check is performed by the security association protocol used, for example [RFC7296], section 2.15.

3: The peer’s certificate passes certificate path validation as defined in [RFC5280], section 6 against one of the Trust Anchors associated with the ACP node’s ACP domain certificate (see Section 6.1.4 below).

4: If the node certificate indicates a Certificate Revocation List (CRL) Distribution Point (CDP) ([RFC5280], section 4.2.1.13) or Online Certificate Status Protocol (OCSP) responder ([RFC5280], section 4.2.2.1), then the peer’s certificate must be valid according to those criteria: An OCSP check for the peer’s certificate across the ACP must succeed or the peer certificate must not be listed in the CRL retrieved from the CDP. This rule has to be skipped for ACP secure channel peer authentication when the node has no ACP or non-ACP connectivity to retrieve current CRL or access an OCSP responder (and the security association protocol itself has also no way to communicate CRL or OCSP check).

5: The peer’s certificate has a syntactically valid ACP domain information field (encoded as subjectAltName / rfc822Name) and the acp-domain-name in that peer’s domain information field is the same as in this ACP node’s certificate (lowercase normalized).

Note: When an ACP node learns later via OCSP/CRL that an ACP peer’s certificate for which rule 4 had to be skipped during ACP secure channel establishment is invalid, then the ACP secure channel to that peer SHOULD be closed even if this peer is the only connectivity to access CRL/OCSP. The ACP secure channel connection MUST be retried periodically to support the case that the neighbor acquires a new, valid certificate.
When checking a candidate peer’s certificate for the purpose of establishing an ACP secure channel, one additional check is performed:

6: The candidate peer certificate’s ACP domain information field has a non-empty acp-address field (either 32HEXDIG or 0, according to Figure 2).

Technically, ACP secure channels can only be built with nodes that have an acp-address. Rule 6 ensures that this is taken into account during ACP domain membership check.

Nodes with an empty acp-address field can only use their ACP domain certificate for non-ACP-secure channel authentication purposes. This includes for example NMS type nodes permitted to communicate into the ACP via ACP connect (Section 8.1).

The special value 0 in an ACP certificates acp-address field is used for nodes that can and should determine their ACP address through other mechanisms than learning it through the acp-address field in their ACP domain certificate. These ACP nodes are permitted to establish ACP secure channels. Mechanisms for those nodes to determine their ACP address are outside the scope of this specification, but this option is defined here so that any ACP nodes can build ACP secure channels to them according to Rule 6.

In summary:

Steps 1...4 constitute standard certificate validity verification and private key authentication as defined by [RFC5280] and security association protocols (such as IKEv2 [RFC7296] when leveraging certificates.

Steps 1...4 do not include verification of any pre-existing form of non-public-key-only based identity elements of a certificate such as a web servers domain name prefix often encoded in certificate common name. Steps 5 and 6 are the equivalent steps.

Step 4 Constitutes standard CRL/OCSP checks refined for the case of missing connectivity and limited functionality security association protocols.

Step 5 Checks for the presence of an ACP identity for the peer.

Steps 1...5 authorize to build any secure connection between members of the same ACP domain except for ACP secure channels.
Step 6 is the additional verification of the presence of an ACP address.

Steps 1...6 authorize to build an ACP secure channel.

For brevity, the remainder of this document refers to this process only as authentication instead of as authentication and authorization.

6.1.4. Trust Points and Trust Anchors

ACP nodes need Trust Point (TP) certificates to perform certificate path validation as required by Section 6.1.3, rule 3. Trust Point(s) must be provisioned to an ACP node (together with its ACP domain certificate) by an ACP Registrar during initial enrolment of a candidate ACP node. ACP nodes MUST also support renewal of TPs via EST as described below in Section 6.1.5.

Trust Point is the term used in this document for a certificate authority (CA) and its associated set of certificates. Multiple certificates are required for a CA to deal with CA certificate renewals as explained in Section 4.4 of CMP ([RFC4210]).

A certificate path is a chain of certificates starting at the ACP certificate (leaf/end-entity) followed by zero or more intermediate Trust Point or sub-CA certificates and ending with a self-signed certificate of a so called root-CA or Trust Anchor. Certificate path validation authenticates that the ACP certificate is signed by a Trust Anchor, directly or indirectly via one or more intermediate Trust Points.

Note that different ACP nodes may have different Trust Points and even different Trust Anchors in their certificate path, as long as the set of Trust Points for all ACP node includes the same set of Trust Anchors (usually 1), and each ACP nodes set of Trust Anchors includes the intermediate Trust Points for its own ACP domain certificate. The protocols through which ACP domain membership check rules 1-4 are performed therefore need to support the exchange not only of the ACP nodes certificates, but also their intermediate Trust Points.

ACP nodes MUST support for the ACP domain membership check the certificate path validation with 0 or 1 intermediate Trust Points. They SHOULD support 2 intermediate Trust Points and two Trust Anchors (to permit migration to different root-CAs).

Trust Points for ACP domain certificates must be trusted to sign certificates with valid ACP domain information fields only for
trusted ACP registrars of that domain. This can be achieved by using Trust Anchors private to the owner of the ACP domain or potentially through appropriate contractual agreements between the involved parties. Public CA without such obligations and guarantees can not be used.

A single owner can operate multiple independent ACP domains from the same set of private trust anchors (CAs) when the ACP Registrars are trusted not to permit certificates with incorrect ACP information fields to be signed, such as ACP information with a wrong acp-domain field. In this case, CAs can be completely unaware of ACP specifics, so that it should be possible to use any existing CA software. When ACP Registrars are not to be trusted, the correctness of the ACP domain information field for the candidate ACP node has to be verified by the CA signing the ACP domain certificate.

6.1.5. Certificate and Trust Point Maintenance

ACP nodes MUST support renewal of their Certificate and Trust Points (TP) via EST ("Enrollment over Secure Transport", see [RFC7030]) and MAY support other mechanisms. An ACP network MUST have at least one ACP node supporting EST server functionality across the ACP so that EST renewal is useable.

ACP nodes SHOULD be able to remember the EST server from which they last renewed their ACP domain certificate and SHOULD provide the ability for this remembered EST server to also be set by the ACP Registrar (see Section 6.10.7) that initially enrolled the ACP device with its ACP domain certificate. When BRSKI (see [I-D.ietf-anima-bootstrapping-keyinfra]) is used, the ACP address of the BRSKI registrar from the BRSKI TLS connection SHOULD be remembered and used for the next renewal via EST if that registrar also announces itself as an EST server via GRASP (see next section) on its ACP address.

The EST server MUST present a certificate that is passing ACP domain membership check in its TLS connection setup (Section 6.1.3, rules 1..5, not rule 6 as this is not for an ACP secure channel setup). The EST server certificate MUST also contain the id-kp-cmcRA [RFC6402] extended key usage extension and the EST client must check its presence.

The additional check against the id-kp-cmcRA extended key usage extension field ensures that clients do not fall prey to an illicit EST server. While such illicit EST servers should not be able to support certificate signing requests (as they are not able to elicit a signing response from a valid CA), such an illicit EST server would
be able to provide faked CA certificates to EST clients that need to renew their CA certificates when they expire.

Note that EST servers supporting multiple ACP domains will need to have for each of these ACP domains a separate certificate and respond on a different transport address (IPv6 address and/or TCP port), but this is easily automated on the EST server as long as the CA does not restrict registrars to request certificates with the id-kp-cmcRA extended usage extension for themselves.

6.1.5.1. GRASP objective for EST server

ACP nodes that are EST servers MUST announce their service via GRASP in the ACP through M_FLOOD messages. See [I-D.ietf-anima-grasp], section 2.8.11 for the definition of this message type:

Example:

```plaintext
[M_FLOOD, 12340815, h'fd89b714f3db0000200000064000001', 210000,
 ["SRV.est", 4, 255 ],
 [O_IPv6_LOCATOR,
  h'fd89b714f3db0000200000064000001', TCP, 443]
]
```

Figure 3: GRASP SRV.est example

The formal definition of the objective in Concise data definition language (CDDL) (see [I-D.ietf-cbor-cddl]) is as follows:

```
flood-message = [M_FLOOD, session-id, initiator, ttl,
  +[objective, (locator-option / [])]]
  ; see example above and explanation below for initiator and ttl

objective = ["SRV.est", objective-flags, loop-count, objective-value]

objective-flags = sync-only  ; as in GRASP spec
  sync-only       = 4          ; M_FLOOD only requires synchronization
  loop-count      = 255        ; recommended as there is no mechanism;
  objective-value = any        ; reserved for future extensions

```

Figure 4: GRASP SRV.est definition

The objective name "SRV.est" indicates that the objective is an [RFC7030] compliant EST server because "est" is an [RFC6335]
registered service name for [RFC7030]. Objective-value MUST be ignored if present. Backward compatible extensions to [RFC7030] MAY be indicated through objective-value. Non [RFC7030] compatible certificate renewal options MUST use a different objective-name. Non-recognized objective-values (or parts thereof if it is a structure partially understood) MUST be ignored.

The M_FLOOD message MUST be sent periodically. The default SHOULD be 60 seconds, the value SHOULD be operator configurable but SHOULD be not smaller than 60 seconds. The frequency of sending MUST be such that the aggregate amount of periodic M_FLOODs from all flooding sources cause only negligible traffic across the ACP. The time-to-live (ttl) parameter SHOULD be 3.5 times the period so that up to three consecutive messages can be dropped before considering an announcement expired. In the example above, the ttl is 210000 msec, 3.5 times 60 seconds. When a service announcer using these parameters unexpectedly dies immediately after sending the M_FLOOD, receivers would consider it expired 210 seconds later. When a receiver tries to connect to this dead service before this timeout, it will experience a failing connection and use that as an indication that the service instance is dead and select another instance of the same service instead (from another GRASP announcement).

6.1.5.2. Renewal

When performing renewal, the node SHOULD attempt to connect to the remembered EST server. If that fails, it SHOULD attempt to connect to an EST server learned via GRASP. The server with which certificate renewal succeeds SHOULD be remembered for the next renewal.

Remembering the last renewal server and preferring it provides stickiness which can help diagnostics. It also provides some protection against off-path compromised ACP members announcing bogus information into GRASP.

Renewal of certificates SHOULD start after less than 50% of the domain certificate lifetime so that network operations has ample time to investigate and resolve any problems that causes a node to not renew its domain certificate in time - and to allow prolonged periods of running parts of a network disconnected from any CA.

6.1.5.3. Certificate Revocation Lists (CRLs)

The ACP node SHOULD support Certificate Revocation Lists (CRL) via HTTP from one or more CRL Distribution Points (CDPs). The CDP(s) MUST be indicated in the Domain Certificate when used. If the CDP URL uses an IPv6 address (ULA address when using the addressing rules
specified in this document), the ACP node will connect to the CDP via the ACP. If the CDP uses a domain name, the ACP node will connect to the CDP via the Data-Plane.

It is common to use domain names for CDP(s), but there is no requirement for the ACP to support DNS. Any DNS lookup in the Data-Plane is not only a possible security issue, but it would also not indicate whether the resolved address is meant to be reachable across the ACP. Therefore, the use of an IPv6 address versus the use of a DNS name doubles as an indicator whether or not to reach the CDP via the ACP.

A CDP can be reachable across the ACP either by running it on a node with ACP or by connecting its node via an ACP connect interface (see Section 8.1). The CDP SHOULD use an ACP domain certificate for its HTTPs connections. The connecting ACP node SHOULD verify that the CDP certificate used during the HTTPs connection has the same ACP address as indicated in the CDP URL of the node’s ACP domain certificate if the CDP URL uses an IPv6 address.

6.1.5.4. Lifetimes

Certificate lifetime may be set to shorter lifetimes than customary (1 year) because certificate renewal is fully automated via ACP and EST. The primary limiting factor for shorter certificate lifetimes is load on the EST server(s) and CA. It is therefore recommended that ACP domain certificates are managed via a CA chain where the assigning CA has enough performance to manage short lived certificates. See also Section 10.2.4 for discussion about an example setup achieving this. See also [I-D.ietf-acme-star].

When certificate lifetimes are sufficiently short, such as few hours, certificate revocation may not be necessary, allowing to simplify the overall certificate maintenance infrastructure.

See Appendix A.2 for further optimizations of certificate maintenance when BRSKI can be used ("Bootstrapping Remote Secure Key Infrastructures", see [I-D.ietf-anima-bootstrapping-keyinfra]).

6.1.5.5. Re-enrollment

An ACP node may determine that its ACP domain certificate has expired, for example because the ACP node was powered down or disconnected longer than its certificate lifetime. In this case, the ACP node SHOULD convert to a role of a re-enrolling candidate ACP node.
In this role, the node does maintain the trust anchor and certificate chain associated with its ACP domain certificate exclusively for the purpose of re-enrollment, and attempts (or waits) to get re-enrolled with a new ACP certificate. The details depend on the mechanisms/protocols used by the ACP registrars.

Please refer to Section 6.10.7 and [I-D.ietf-anima-bootstrapping-keyinfra] for explanations about ACP registrars and vouchers as used in the following text. When ACP is intended to be used without BRSKI, the details about BRSKI and vouchers in the following text can be skipped.

When BRSKI is used (i.e.: on ACP nodes that are ANI nodes), the re-enrolling candidate ACP node would attempt to enroll like a candidate ACP node (BRSKI pledge), but instead of using the ACP nodes IDevID, it SHOULD first attempt to use its ACP domain certificate in the BRSKI TLS authentication. The BRSKI registrar MAY honor this certificate beyond its expiration date purely for the purpose of re-enrollment. Using the ACP node’s domain certificate allows the BRSKI registrar to learn that node’s ACP domain information field, so that the BRSKI registrar can re-assign the same ACP address information to the ACP node in the new ACP domain certificate.

If the BRSKI registrar denies the use of the old ACP domain certificate, the re-enrolling candidate ACP node MUST re-attempt re-enrollment using its IDevID as defined in BRSKI during the TLS connection setup.

Both when the BRSKI connection is attempted with the old ACP domain certificate or the IDevID, the re-enrolling candidate ACP node SHOULD authenticate the BRSKI registrar during TLS connection setup based on its existing trust anchor/certificate chain information associated with its old ACP certificate. The re-enrolling candidate ACP node SHOULD only fall back to requesting a voucher from the BRSKI registrar when this authentication fails during TLS connection setup.

When other mechanisms than BRSKI are used for ACP domain certificate enrollment, the principles of the re-enrolling candidate ACP node are the same. The re-enrolling candidate ACP node attempts to authenticate any ACP registrar peers during re-enrollment protocol/mechanisms via its existing certificate chain/trust anchor and provides its existing ACP domain certificate and other identification (such as the IDevID) as necessary to the registrar.

Maintaining existing trust anchor information is especially important when enrollment mechanisms are used that unlike BRSKI do not leverage a voucher mechanism to authenticate the ACP registrar and where
therefore the injection of certificate failures could otherwise make the ACP node easily attackable remotely.

When using BRSKI or other protocol/mechanisms supporting vouchers, maintaining existing trust anchor information allows for re-enrollment of expired ACP certificates to be more lightweight, especially in environments where repeated acquisition of vouchers during the lifetime of ACP nodes may be operationally expensive or otherwise undesirable.

6.1.5.6. Failing Certificates

An ACP domain certificate is called failing in this document, if/when the ACP node to which the certificate was issued can determine that it was revoked (or explicitly not renewed), or in the absence of such explicit local diagnostics, when the ACP node fails to connect to other ACP nodes in the same ACP domain using its ACP certificate. For connection failures to determine the ACP domain certificate as the culprit, the peer should pass the domain membership check (Section 6.1.3) and other reasons for the connection failure can be excluded because of the connection error diagnostics.

This type of failure can happen during setup/refresh of a secure ACP channel connections or any other use of the ACP domain certificate, such as for the TLS connection to an EST server for the renewal of the ACP domain certificate.

Example reasons for failing certificates that the ACP node can only discover through connection failure are that the domain certificate or any of its signing certificates could have been revoked or may have expired, but the ACP node cannot self-diagnose this condition directly. Revocation information or clock synchronization may only be available across the ACP, but the ACP node cannot build ACP secure channels because ACP peers reject the ACP node’s domain certificate.

ACP nodes SHOULD support the option to determines whether its ACP certificate is failing, and when it does, put itself into the role of a re-enrolling candidate ACP node as explained above (Section 6.1.5.5).

6.2. ACP Adjacency Table

To know to which nodes to establish an ACP channel, every ACP node maintains an adjacency table. The adjacency table contains information about adjacent ACP nodes, at a minimum: Node-ID (identifier of the node inside the ACP, see Section 6.10.3 and Section 6.10.5), interface on which neighbor was discovered (by GRASP as explained below), link-local IPv6 address of neighbor on that
interface, certificate (including domain information field). An ACP node MUST maintain this adjacency table. This table is used to determine to which neighbor an ACP connection is established.

Where the next ACP node is not directly adjacent (i.e., not on a link connected to this node), the information in the adjacency table can be supplemented by configuration. For example, the Node-ID and IP address could be configured. See Section 8.2.

The adjacency table MAY contain information about the validity and trust of the adjacent ACP node’s certificate. However, subsequent steps MUST always start with the ACP domain membership check against the peer (see Section 6.1.3).

The adjacency table contains information about adjacent ACP nodes in general, independently of their domain and trust status. The next step determines to which of those ACP nodes an ACP connection should be established.

6.3. Neighbor Discovery with DULL GRASP

[RFCEditor: GRASP draft is in RFC editor queue, waiting for dependencies, including ACP. Please ensure that references to I-D.ietf-anima-grasp that include section number references (throughout this document) will be updated in case any last-minute changes in GRASP would make those section references change.]

Discovery Unsolicited Link-Local (DULL) GRASP is a limited subset of GRASP intended to operate across an insecure link-local scope. See section 2.5.2 of [I-D.ietf-anima-grasp] for its formal definition. The ACP uses one instance of DULL GRASP for every L2 interface of the ACP node to discover link level adjacent candidate ACP neighbors. Unless modified by policy as noted earlier (Section 5 bullet point 2.), native interfaces (e.g., physical interfaces on physical nodes) SHOULD be initialized automatically to a state in which ACP discovery can be performed and any native interfaces with ACP neighbors can then be brought into the ACP even if the interface is otherwise not configured. Reception of packets on such otherwise not configured interfaces MUST be limited so that at first only IPv6 StateLess Address Auto Configuration (SLAAC - [RFC4862]) and DULL GRASP work and then only the following ACP secure channel setup packets – but not any other unnecessary traffic (e.g., no other link-local IPv6 transport stack responders for example).

Note that the use of the IPv6 link-local multicast address (ALL_GRASP_NEIGHBORS) implies the need to use Multicast Listener Discovery Version 2 (MLDv2, see [RFC3810]) to announce the desire to receive packets for that address. Otherwise DULL GRASP could fail to
operate correctly in the presence of MLD snooping, non-ACP enabled L2 switches - because those would stop forwarding DULL GRASP packets. Switches not supporting MLD snooping simply need to operate as pure L2 bridges for IPv6 multicast packets for DULL GRASP to work.

ACP discovery SHOULD NOT be enabled by default on non-native interfaces. In particular, ACP discovery MUST NOT run inside the ACP across ACP virtual interfaces. See Section 10.3 for further, non-normative suggestions on how to enable/disable ACP at node and interface level. See Section 8.2.2 for more details about tunnels (typical non-native interfaces). See Section 7 for how ACP should be extended on devices operating (also) as L2 bridges.

Note: If an ACP node also implements BRSKI to enroll its ACP domain certificate (see Appendix A.2 for a summary), then the above considerations also apply to GRASP discovery for BRSKI. Each DULL instance of GRASP set up for ACP is then also used for the discovery of a bootstrap proxy via BRSKI when the node does not have a domain certificate. Discovery of ACP neighbors happens only when the node does have the certificate. The node therefore never needs to discover both a bootstrap proxy and ACP neighbor at the same time.

An ACP node announces itself to potential ACP peers by use of the "AN_ACP" objective. This is a synchronization objective intended to be flooded on a single link using the GRASP Flood Synchronization (M_FLOOD) message. In accordance with the design of the Flood message, a locator consisting of a specific link-local IP address, IP protocol number and port number will be distributed with the flooded objective. An example of the message is informally:

```
[M_FLOOD, 12340815, h'fe80000000000000c0011001FEEF0000, 210000, 
["AN_ACP", 4, 1, "IKEv2" ],
[O_IPv6_LOCATOR, 
  h'fe80000000000000c0011001FEEF0000, UDP, 15000] 
["AN_ACP", 4, 1, "DTLS" ],
[O_IPv6_LOCATOR, 
  h'fe80000000000000c0011001FEEF0000, UDP, 17000] ]
```

Figure 5: GRASP AN_ACP example

The formal CDDL definition is:
flood-message = [M_FLOOD, session-id, initiator, ttl, 
+objective, (locator-option / [])]]

objective = ['AN_ACP', objective-flags, loop-count, 
objective-value]

objective-flags = sync-only ; as in the GRASP specification
sync-only = 4    ; M_FLOOD only requires synchronization
loop-count = 1    ; limit to link-local operation
objective-value = method
method = "IKEv2" / "DTLS" ; or future standard methods

Figure 6: GRASP AN_ACP definition

The objective-flags field is set to indicate synchronization.
The loop-count is fixed at 1 since this is a link-local operation.
In the above example the RECOMMENDED period of sending of the 
objective is 60 seconds. The indicated ttl of 210000 msec means that 
the objective would be cached by ACP nodes even when two out of three 
messages are dropped in transit.
The session-id is a random number used for loop prevention 
(distinguishing a message from a prior instance of the same message). 
In DULL this field is irrelevant but must still be set according to the 
GRASP specification.
The originator MUST be the IPv6 link local address of the originating 
ACP node on the sending interface.
The ‘objective-value’ parameter is a string indicating the secure 
channel protocol available at the specified or implied locator.
The locator-option is optional and only required when the secure 
channel protocol is not offered at a well-defined port number, or if 
there is no well-defined port number.

"IKEv2" is the abbreviation for "Internet Key Exchange protocol 
version 2". It is the main protocol used by the Internet IP security 
arquitectures (IPsec). We therefore use the term "IKEv2" and not 
"IPsec" in the GRASP definitions and example above. "IKEv2" has a 
well-defined port number 500, but in the above example, the candidate 
ACP neighbor is offering ACP secure channel negotiation via IKEv2 on 
port 15000 (for the sake of creating a non-standard example).
"DTLS" indicates datagram Transport Layer Security version 1.2. There is no default UDP port, it must always be locally assigned by the node. See Section 6.7.2.

If a locator is included, it MUST be an O_IPV6_LOCATOR, and the IPv6 address MUST be the same as the initiator address (these are DULL requirements to minimize third party DoS attacks).

The secure channel methods defined in this document use the objective-values of "IKEv2" and "DTLS". There is no distinction between IKEv2 native and GRE-IKEv2 because this is purely negotiated via IKEv2.

A node that supports more than one secure channel protocol method needs to flood multiple versions of the "AN_ACP" objective so that each method can be accompanied by its own locator-option. This can use a single GRASP M_FLOOD message as shown in Figure 5.

Note that a node serving both as an ACP node and BRSKI Join Proxy may choose to distribute the "AN_ACP" objective and the respective BRSKI in the same M_FLOOD message, since GRASP allows multiple objectives in one message. This may be impractical though if ACP and BRSKI operations are implemented via separate software modules / ASAs.

The result of the discovery is the IPv6 link-local address of the neighbor as well as its supported secure channel protocols (and non-standard port they are running on). It is stored in the ACP Adjacency Table (see Section 6.2), which then drives the further building of the ACP to that neighbor.

Note that the DULL GRASP objective described does intentionally not include ACP nodes ACP domain certificate even though this would be useful for diagnostics and to simplify the security exchange in ACP secure channel security association protocols (see Section 6.7). The reason is that DULL GRASP messages are periodically multicasted across IPv6 subnets and full certificates could easily lead to fragmented IPv6 DULL GRASP multicast packets due to the size of a certificate. This would be highly undesirable.

6.4. Candidate ACP Neighbor Selection

An ACP node must determine to which other ACP nodes in the adjacency table it should build an ACP connection. This is based on the information in the ACP Adjacency table.

The ACP is established exclusively between nodes in the same domain. This includes all routing subdomains. Appendix A.7 explains how ACP connections across multiple routing subdomains are special.
The result of the candidate ACP neighbor selection process is a list of adjacent or configured autonomic neighbors to which an ACP channel should be established. The next step begins that channel establishment.

6.5. Channel Selection

To avoid attacks, initial discovery of candidate ACP peers cannot include any non-protected negotiation. To avoid re-inventing and validating security association mechanisms, the next step after discovering the address of a candidate neighbor can only be to try first to establish a security association with that neighbor using a well-known security association method.

From the use-cases it seems clear that not all type of ACP nodes can or need to connect directly to each other or are able to support or prefer all possible mechanisms. For example, code space limited IoT devices may only support DTLS because that code exists already on them for end-to-end security, but low-end in-ceiling L2 switches may only want to support Media Access Control Security (MacSec, see 802.1AE ([MACSEC])) because that is also supported in their chips. Only a flexible gateway device may need to support both of these mechanisms and potentially more. Note that MacSec is not required by any profiles of the ACP in this specification but just mentioned as a likely next interesting secure channel protocol.

To support extensible secure channel protocol selection without a single common MTI protocol, ACP nodes must try all the ACP secure channel protocols it supports and that are feasible because the candidate ACP neighbor also announced them via its AN_ACP GRASP parameters (these are called the "feasible" ACP secure channel protocols).

To ensure that the selection of the secure channel protocols always succeeds in a predictable fashion without blocking, the following rules apply:

- An ACP node may choose to attempt to initiate the different feasible ACP secure channel protocols it supports according to its local policies sequentially or in parallel, but it MUST support acting as a responder to all of them in parallel.

- Once the first secure channel protocol succeeds, the two peers know each other’s certificates because they must be used by all secure channel protocols for mutual authentication. The node with the lower Node-ID in the ACP address of its ACP domain certificate becomes Bob, the one with the higher Node-ID in the certificate Alice. A peer with an empty ACP address field in its ACP domain
certificate becomes Bob (this specification does not define such peers, only the interoperability with them).

- Bob becomes passive, he does not attempt to further initiate ACP secure channel protocols with Alice and does not consider it to be an error when Alice closes secure channels. Alice becomes the active party, continues to attempt setting up secure channel protocols with Bob until she arrives at the best one from her view that also works with Bob.

For example, originally Bob could have been the initiator of one ACP secure channel protocol that Bob prefers and the security association succeeded. The roles of Bob and Alice are then assigned and the connection setup is completed. The protocol could for example be IPsec via IKEv2 ("IP security", see [RFC4301] and "Internet Key Exchange protocol version 2", see [RFC7296]). It is now up to Alice to decide how to proceed. Even if the IPsec connection from Bob succeeded, Alice might prefer another secure protocol over IPsec (e.g., FOOBAR), and try to set that up with Bob. If that preference of Alice succeeds, she would close the IPsec connection. If no better protocol attempt succeeds, she would keep the IPsec connection.
The following sequence of steps show this example in more detail:

[1] Node 1 sends GRASP AN_ACP message to announce itself

[2] Node 2 sends GRASP AN_ACP message to announce itself


[4:C1] Because of [3], Node 2 starts as initiator on its preferred secure channel protocol towards Node 1. Connection C1.


[6:C2] Because of [5], Node 1 starts as initiator on its preferred secure channel protocol towards Node 2. Connection C2.

[7:C1] Node1 and Node2 have authenticated each others certificate on connection C1 as valid ACP peers.

[8:C1] Node 1 certificate has lower ACP Node-ID than Node2, therefore Node 1 considers itself Bob and Node 2 Alice on connection C1. Connection setup C1 is completed.

[9] Node 1 (Bob) refrains from attempting any further secure channel connections to Node 2 (Alice) as learned from [2] because it knows from [8:C1] that it is Bob relative to Node 1.

[10:C2] Node1 and Node2 have authenticated each others certificate on connection C2 (like [7:C1]).

[11:C2] Node 1 certificate has lower ACP Node-ID than Node2, therefore Node 1 considers itself Bob and Node 2 Alice on connection C1, but they also identify that C2 is to the same mutual peer as their C1, so this has no further impact.

[12:C2] Node 1 (Alice) closes C1. Because of [8:C1], Node 2 (Bob) expected this.

[13] Node 1 (Alice) and Node 2 (Bob) start data transfer across C2, which makes it become a secure channel for the ACP.

Figure 7: Secure Channel sequence of steps

All this negotiation is in the context of an "L2 interface". Alice and Bob will build ACP connections to each other on every "L2
interface" that they both connect to. An autonomic node MUST NOT assume that neighbors with the same L2 or link-local IPv6 addresses on different L2 interfaces are the same node. This can only be determined after examining the certificate after a successful security association attempt.

6.6. Candidate ACP Neighbor verification

Independent of the security association protocol chosen, candidate ACP neighbors need to be authenticated based on their domain certificate. This implies that any secure channel protocol MUST support certificate based authentication that can support the ACP domain membership check as defined in Section 6.1.3. If it fails, the connection attempt is aborted and an error logged. Attempts to reconnect MUST be throttled. The RECOMMENDED default is exponential base 2 backoff with a minimum delay of 10 seconds and a maximum delay of 640 seconds.

6.7. Security Association protocols

Due to Channel Selection (Section 6.5), ACP can support an evolving set of security association protocols. These protocols only need to be used to establish secure channels with L2 adjacent ACP neighbors and only optionally (where needed) across non-ACP capable L3 network (see Section 8.2). Therefore, there is architecturally no need for any network wide mandatory to implement (MTI) security association protocols. Instead, ACP nodes only need to implement those protocols required to be supported by their neighbors. See Section 6.7.3 for an example of this.

The authentication of peers in any security association protocol MUST use the ACP domain certificate according to Section 6.1.3. Because auto-discovery of candidate ACP neighbors via GRASP (see Section 6.3) as specified in this document does not communicate the neighbors ACP domain certificate, and ACP nodes may not (yet) have any other network connectivity to retrieve certificates, any security association protocol MUST use a mechanism to communicate the certificate directly instead of relying on a referential mechanism such as communicating only a hash and/or URL for the certificate.

The degree of security required on every hop of an ACP network needs to be consistent across the network so that there is no designated "weakest link" because it is that "weakest link" that would otherwise become the designated point of attack. When the secure channel protection on one link is compromised, it can be used to send/receive packets across the whole ACP network. This principle does not imply that the requirements against ACP security association protocols have to be the same across all subnets in an ACP network:
o Underlying L2 mechanisms such as strong encrypted radio technologies or [MACSEC] may offer equivalent encryption and the ACP security association protocol may only be required to authenticate ACP domain membership of a peer. Mechanisms to auto-discover and associate ACP peers leveraging such underlying L2 security are possible and desirable to avoid duplication of encryption, but none are specified in this document.

o Strong physical security of a link may stand in where cryptographic security is infeasible. As there is no secure mechanism to automatically discover strong physical security solely between two peers, it can only be used with explicit configuration and that configuration too could become an attack vector. This document therefore only specifies with ACP connect (Figure 15) one explicitly configured mechanism without any secure channel association protocol - for the case where both the link and the nodes attached to it have strong physical security.

The following sub-sections define the security association protocols that are considered to be important and feasible to specify in this document.

6.7.1. ACP via IKEv2

An ACP node announces its ability to support IKEv2 as the ACP secure channel protocol in GRASP as "IKEv2".

6.7.1.1. Native IPsec

To run ACP via IPsec natively, no further IANA assignments/definitions are required.

An ACP node that is supporting native IPsec MUST use IPsec security setup via IKEv2 for tunnel mode and IPsec/IKE signaling accordingly for IPv6 payload (e.g.: ESP next header of 41). It MUST use local and peer link-local IPv6 addresses for encapsulation.

Authentication MUST use the ACP domain certificates. Certificate Encoding MUST support "PKCS #7 wrapped X.509 certificate" (0) (see [IKEV2IANA] for this and other IANA IKEv2 parameter names used in this text). If certificate chains are used, all intermediate certificates up to, but not including the locally provisioned trust anchor certificate must be signaled.

IPsec tunnel mode is required because the ACP will route/forward packets received from any other ACP node across the ACP secure channels, and not only its own generated ACP packets. With IPsec
transport mode, it would only be possible to send packets originated by the ACP node itself.

IPsec MUST use ESP with ENCR_AES_GCM_16 ([RFC4106]) due to its higher performance over ENCR_AES_CBC. ACP MUST NOT use any NULL encryption option due to the confidentiality of ACP payload that may not be encrypted by itself (when carrying legacy management protocol traffics as well as hop-by-hop GRASP).

These IPsec requirements are based on [RFC8221] but limited to the minimum necessary options because ACP is not a general purpose use case today with a wide range of interoperability requirements against legacy devices originally developed against older profile recommendations. Once there are updates to [RFC8221], these should accordingly be reflected in updates to these ACP requirements (for example if ENCR_AES_GCM_16 was to be superceded in the future).

Additional requirements from [RFC8221] MAY be used for ACP channels as long as they do not result in a reduction of security over the above MTI requirements. For example, ESP compression MAY be used.

IKEv2 MUST follow [RFC8247] as necessary to support the above listed IPsec requirements.

6.7.1.2. IPsec with GRE encapsulation

In network devices it is often more common to implement high performance virtual interfaces on top of GRE encapsulation than on top of a "native" IPsec association (without any other encapsulation than those defined by IPsec). On those devices it may be beneficial to run the ACP secure channel on top of GRE protected by the IPsec association.

To run ACP via GRE/IPsec, no further IANA assignments/definitions are required.

The requirements for ESP/IPsec/IKEv2 are the same as for native IPsec (see Section 6.7.1.1) except that IPsec transport mode and next protocol GRE (47) are to be negotiated. Tunnel mode is not required because of GRE.

If IKEv2 initiator and responder support IPsec over GRE, it has to be preferred over native IPsec. The ACP IPv6 traffic has to be carried across GRE according to [RFC7676].
6.7.2. ACP via DTLS

We define the use of ACP via DTLS in the assumption that it is likely the first transport encryption supported in some classes of constrained devices.

To run ACP via UDP and DTLS v1.2 [RFC6347] a locally assigned UDP port is used that is announced as a parameter in the GRASP AN_ACP objective to candidate neighbors.

All ACP nodes supporting DTLS as a secure channel protocol MUST adhere to the DTLS implementation recommendations and security considerations of BCP 195 [RFC7525] except with respect to the DTLS version. ACP nodes supporting DTLS MUST implement only DTLS 1.2 or later. For example, implementing DTLS-1.3 ([I-D.ietf-tls-dtls13]) is also an option.

There is no additional session setup or other security association besides this simple DTLS setup. As soon as the DTLS session is functional, the ACP peers will exchange ACP IPv6 packets as the payload of the DTLS transport connection. Any DTLS defined security association mechanisms such as re-keying are used as they would be for any transport application relying solely on DTLS.

6.7.3. ACP Secure Channel Requirements

As explained in the beginning of Section 6.5, there is no single secure channel mechanism mandated for all ACP nodes. Instead, this section defines two ACP profiles (baseline and constrained) for ACP nodes that do introduce such requirements.

A baseline ACP node MUST support IPsec natively and MAY support IPsec via GRE. A constrained ACP node that cannot support IPsec MUST support DTLS. An ACP node connecting an area of constrained ACP nodes with an area of baseline ACP nodes must therefore support IPsec and DTLS and supports therefore the baseline and constrained profile.

Explanation: Not all type of ACP nodes can or need to connect directly to each other or are able to support or prefer all possible secure channel mechanisms. For example, code space limited IoT devices may only support DTLS because that code exists already on them for end-to-end security, but high-end core routers may not want to support DTLS because they can perform IPsec in accelerated hardware but would need to support DTLS in an underpowered CPU forwarding path shared with critical control plane operations. This is not a deployment issue for a single ACP across these type of nodes as long as there are also appropriate gateway ACP nodes that support sufficiently many secure channel mechanisms to allow interconnecting...
areas of ACP nodes with a more constrained set of secure channel protocols. On the edge between IoT areas and high-end core networks, general-purpose routers that act as those gateways and that can support a variety of secure channel protocols is the norm already.

ACP nodes need to specify in documentation the set of secure ACP mechanisms they support and should declare which profile they support according to above requirements.

An ACP secure channel MUST immediately be terminated when the lifetime of any certificate in the chain used to authenticate the neighbor expires or becomes revoked. Note that this is not standard behavior in secure channel protocols such as IPsec because the certificate authentication only influences the setup of the secure channel in these protocols.

6.8. GRASP in the ACP

6.8.1. GRASP as a core service of the ACP

The ACP MUST run an instance of GRASP inside of it. It is a key part of the ACP services. The function in GRASP that makes it fundamental as a service of the ACP is the ability to provide ACP wide service discovery (using objectives in GRASP).

ACP provides IP unicast routing via the RPL routing protocol (see Section 6.11).

The ACP does not use IP multicast routing nor does it provide generic IP multicast services (the handling of GRASP link-local multicast messages is explained in Section 6.8.2). Instead, the ACP provides service discovery via the objective discovery/announcement and negotiation mechanisms of the ACP GRASP instance (services are a form of objectives). These mechanisms use hop-by-hop reliable flooding of GRASP messages for both service discovery (GRASP M_DISCOVERY messages) and service announcement (GRASP M_FLOOD messages).

See Appendix A.5 for discussion about this design choice of the ACP.

6.8.2. ACP as the Security and Transport substrate for GRASP

In the terminology of GRASP ([I-D.ietf-anima-grasp]), the ACP is the security and transport substrate for the GRASP instance run inside the ACP ("ACP GRASP").

This means that the ACP is responsible for ensuring that this instance of GRASP is only sending messages across the ACP GRASP virtual interfaces. Whenever the ACP adds or deletes such an
interface because of new ACP secure channels or loss thereof, the ACP needs to indicate this to the ACP instance of GRASP. The ACP exists also in the absence of any active ACP neighbors. It is created when the node has a domain certificate, and continues to exist even if all of its neighbors cease operation.

In this case ASAs using GRASP running on the same node would still need to be able to discover each other’s objectives. When the ACP does not exist, ASAs leveraging the ACP instance of GRASP via APIs MUST still be able to operate, and MUST be able to understand that there is no ACP and that therefore the ACP instance of GRASP cannot operate.

The way ACP acts as the security and transport substrate for GRASP is visualized in the following picture:
Figure 8: ACP as security and transport substrate for GRASP
GRASP unicast messages inside the ACP always use the ACP address. Link-local addresses from the ACP VRF must not be used inside objectives. GRASP unicast messages inside the ACP are transported via TLS according to [RFC7525] except that only TLS version 1.2 ([RFC5246]) or higher MUST be used - because there is no need for backward compatibility in the new use-case of ACP. Mutual authentication MUST use the ACP domain membership check defined in (Section 6.1.3).

GRASP link-local multicast messages are targeted for a specific ACP virtual interface (as defined Section 6.12.5) but are sent by the ACP into an ACP GRASP virtual interface that is constructed from the TCP connection(s) to the IPv6 link-local neighbor address(es) on the underlying ACP virtual interface. If the ACP GRASP virtual interface has two or more neighbors, the GRASP link-local multicast messages are replicated to all neighbor TCP connections.

TCP and TLS connections for GRASP in the ACP use the IANA assigned TCP port for GRASP (7107). Effectively the transport stack is expected to be TLS for connections from/to the ACP address (e.g., global scope address(es)) and TCP for connections from/to link-local addresses on the ACP virtual interfaces. The latter ones are only used for flooding of GRASP messages.

6.8.2.1. Discussion

TCP encapsulation for GRASP M_DISCOVERY and M_FLOOD link local messages is used because these messages are flooded across potentially many hops to all ACP nodes and a single link with even temporary packet loss issues (e.g., WiFi/Powerline link) can reduce the probability for loss free transmission so much that applications would want to increase the frequency with which they send these messages. Such shorter periodic retransmission of datagrams would result in more traffic and processing overhead in the ACP than the hop-by-hop reliable retransmission mechanism by TCP and duplicate elimination by GRASP.

TLS is mandated for GRASP non-link-local unicast because the ACP secure channel mandatory authentication and encryption protects only against attacks from the outside but not against attacks from the inside: Compromised ACP members that have (not yet) been detected and removed (e.g., via domain certificate revocation / expiry).

If GRASP peer connections were to use just TCP, compromised ACP members could simply eavesdrop passively on GRASP peer connections for whom they are on-path ("Man In The Middle" - MITM) or intercept and modify them. With TLS, it is not possible to completely
eliminate problems with compromised ACP members, but attacks are a lot more complex:

Eavesdropping/spoofing by a compromised ACP node is still possible because in the model of the ACP and GRASP, the provider and consumer of an objective have initially no unique information (such as an identity) about the other side which would allow them to distinguish a benevolent from a compromised peer. The compromised ACP node would simply announce the objective as well, potentially filter the original objective in GRASP when it is a MITM and act as an application level proxy. This of course requires that the compromised ACP node understand the semantics of the GRASP negotiation to an extent that allows it to proxy it without being detected, but in an ACP environment this is quite likely public knowledge or even standardized.

The GRASP TLS connections are run the same as any other ACP traffic through the ACP secure channels. This leads to double authentication/encryption, which has the following benefits:

- Secure channel methods such as IPsec may provide protection against additional attacks, for example reset-attacks.
- The secure channel method may leverage hardware acceleration and there may be little or no gain in eliminating it.
- There is no different security model for ACP GRASP from other ACP traffic. Instead, there is just another layer of protection against certain attacks from the inside which is important due to the role of GRASP in the ACP.

6.9. Context Separation

The ACP is in a separate context from the normal Data-Plane of the node. This context includes the ACP channels’ IPv6 forwarding and routing as well as any required higher layer ACP functions.

In classical network system, a dedicated so called Virtual routing and forwarding instance (VRF) is one logical implementation option for the ACP. If possible by the systems software architecture, separation options that minimize shared components are preferred, such as a logical container or virtual machine instance. The context for the ACP needs to be established automatically during bootstrap of a node. As much as possible it should be protected from being modified unintentionally by (“Data-Plane”) configuration.
Context separation improves security, because the ACP is not reachable from the Data-Plane routing or forwarding table(s). Also, configuration errors from the Data-Plane setup do not affect the ACP.

6.10. Addressing inside the ACP

The channels explained above typically only establish communication between two adjacent nodes. In order for communication to happen across multiple hops, the autonomic control plane requires ACP network wide valid addresses and routing. Each ACP node must create a Loopback interface with an ACP network wide unique address inside the ACP context (as explained in in Section 6.9). This address may be used also in other virtual contexts.

With the algorithm introduced here, all ACP nodes in the same routing subdomain have the same /48 ULA prefix. Conversely, ULA global IDs from different domains are unlikely to clash, such that two ACP networks can be merged, as long as the policy allows that merge. See also Section 9.1 for a discussion on merging domains.

Links inside the ACP only use link-local IPv6 addressing, such that each node’s ACP only requires one routable virtual address.

6.10.1. Fundamental Concepts of Autonomic Addressing

- **Usage**: Autonomic addresses are exclusively used for self-management functions inside a trusted domain. They are not used for user traffic. Communications with entities outside the trusted domain use another address space, for example normally managed routable address space (called "Data-Plane" in this document).

- **Separation**: Autonomic address space is used separately from user address space and other address realms. This supports the robustness requirement.

- **Loopback-only**: Only ACP Loopback interfaces (and potentially those configured for "ACP connect", see Section 8.1) carry routable address(es); all other interfaces (called ACP virtual interfaces) only use IPv6 link local addresses. The usage of IPv6 link local addressing is discussed in [RFC7404].

- **Use-ULA**: For Loopback interfaces of ACP nodes, we use Unique Local Addresses (ULA), as defined in [RFC4193] with L=1 (as defined in section 3.1 of [RFC4193]). Note that the random hash for ACP Loopback addresses uses the definition in Section 6.10.2 and not the one of [RFC4193] section 3.2.2.
No external connectivity: They do not provide access to the Internet. If a node requires further reaching connectivity, it should use another, traditionally managed address scheme in parallel.

Addresses in the ACP are permanent, and do not support temporary addresses as defined in [RFC4941].

Addresses in the ACP are not considered sensitive on privacy grounds because ACP nodes are not expected to be end-user host. All ACP nodes are in one (potentially federated) administrative domain. They are assumed to be to be candidate hosts of ACP traffic amongst each other or transit thereof. There are no transit nodes less privileged to know about the identity of other hosts in the ACP. Therefore, ACP addresses do not need to be pseudo-random as discussed in [RFC7721]. Because they are not propagated to untrusted (non ACP) nodes and stay within a domain (of trust), we also consider them not to be subject to scanning attacks.

The ACP is based exclusively on IPv6 addressing, for a variety of reasons:

- Simplicity, reliability and scale: If other network layer protocols were supported, each would have to have its own set of security associations, routing table and process, etc.
- Autonomic functions do not require IPv4: Autonomic functions and autonomic service agents are new concepts. They can be exclusively built on IPv6 from day one. There is no need for backward compatibility.
- OAM protocols do not require IPv4: The ACP may carry OAM protocols. All relevant protocols (SNMP, TFTP, SSH, SCP, Radius, Diameter, ...) are available in IPv6. See also [RFC8368] for how ACP could be made to interoperate with IPv4 only OAM.

6.10.2. The ACP Addressing Base Scheme

The Base ULA addressing scheme for ACP nodes has the following format:

```
+-------------------------------+---------------+------------------+
<table>
<thead>
<tr>
<th>fd</th>
<th>hash(routing-subdomain)</th>
<th>Type</th>
<th>(sub-scheme)</th>
</tr>
</thead>
</table>
```

Figure 9: ACP Addressing Base Scheme
The first 48-bits follow the ULA scheme, as defined in [RFC4193], to which a type field is added:

- "fd" identifies a locally defined ULA address.

- The 40-bits ULA "global ID" (term from [RFC4193]) for ACP addresses carried in the domain information field of domain certificates are the first 40-bits of the SHA256 hash of the routing subdomain from the same domain information field. In the example of Section 6.1.2, the routing subdomain is "area51.research.acp.example.com" and the 40-bits ULA "global ID" 89b714f3db.

- When creating a new routing-subdomain for an existing autonomic network, it MUST be ensured, that rsub is selected so the resulting hash of the routing-subdomain does not collide with the hash of any pre-existing routing-subdomains of the autonomic network. This ensures that ACP addresses created by registrars for different routing subdomains do not collide with each others.

- To allow for extensibility, the fact that the ULA "global ID" is a hash of the routing subdomain SHOULD NOT be assumed by any ACP node during normal operations. The hash function is only executed during the creation of the certificate. If BRSKI is used then the BRSKI registrar will create the domain information field in response to the EST Certificate Signing Request (CSR) Attribute Request message by the pledge.

- Establishing connectivity between different ACP (different acp-domain-name) is outside the scope of this specification. If it is being done through future extensions, then the rsub of all routing-subdomains across those autonomic networks need to be selected so the resulting routing-subdomain hashes do not collide. For example a large cooperation with its own private Trust Anchor may want to create different autonomic networks that initially should not be able to connect but where the option to do so should be kept open. When taking this future possibility into account, it is easy to always select rsub so that no collisions happen.

- Type: This field allows different address sub-schemes. This addresses the "upgradability" requirement. Assignment of types for this field will be maintained by IANA.

The sub-scheme may imply a range or set of addresses assigned to the node, this is called the ACP address range/set and explained in each sub-scheme.
Please refer to Section 6.10.7 and Appendix A.1 for further explanations why the following Sub-Addressing schemes are used and why multiple are necessary.

The following summarizes the addressing schemes:

<table>
<thead>
<tr>
<th>type</th>
<th>Z</th>
<th>name</th>
<th>F-bit</th>
<th>V-bit size</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>0</td>
<td>ACP Zone</td>
<td>N/A</td>
<td>1 bit</td>
</tr>
<tr>
<td>0x00</td>
<td>1</td>
<td>ACP Manual</td>
<td>N/A</td>
<td>1 bit</td>
</tr>
<tr>
<td>0x01</td>
<td>N/A</td>
<td>VLong-ASA</td>
<td>0</td>
<td>8-bits</td>
</tr>
<tr>
<td>0x01</td>
<td>N/A</td>
<td>VLong-ACP-edge</td>
<td>1</td>
<td>16-bits</td>
</tr>
</tbody>
</table>

Figure 10: Addressing schemes

6.10.3. ACP Zone Addressing Sub-Scheme

The sub-scheme defined here is defined by the Type value 00b (zero) in the base scheme and 0 in the Z bit.

<table>
<thead>
<tr>
<th>64</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>(base scheme)</td>
<td>Z</td>
</tr>
<tr>
<td>Zone-ID</td>
<td></td>
</tr>
<tr>
<td>Registrar-ID</td>
<td>Node-ID</td>
</tr>
<tr>
<td>50</td>
<td>13</td>
</tr>
<tr>
<td>48</td>
<td>15</td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Figure 11: ACP Zone Addressing Sub-Scheme

The fields are defined as follows:

- Zone-ID: If set to all zero bits: The Node-ID bits are used as an identifier (as opposed to a locator). This results in a non-hierarchical, flat addressing scheme. Any other value indicates a zone. See Section 6.10.3.1 on how this field is used in detail.
- Z: MUST be 0.
- Node-ID: A unique value for each node.

The 64-bit Node-ID is derived and composed as follows:
o Registrar-ID (48-bit): A number unique inside the domain that identifies the ACP registrar which assigned the Node-ID to the node. A MAC address of the ACP registrar can be used for this purpose.

o Node-Number: A number which is unique for a given ACP registrar, to identify the node. This can be a sequentially assigned number.

o V (1-bit): Virtualization bit: 0: Indicates the ACP itself ("ACP node base system"); 1: Indicates the optional "host" context on the ACP node (see below).

In the ACP Zone Addressing Sub-Scheme, the ACP address in the certificate has Zone-ID and V fields as all zero bits. The ACP address set includes addresses with any Zone-ID value and any V value.

The "Node-ID" itself is unique in a domain (i.e., the Zone-ID is not required for uniqueness). Therefore, a node can be addressed either as part of a flat hierarchy (Zone-ID = 0), or with an aggregation scheme (any other Zone-ID). An address with Zone-ID = 0 is an identifier, with a Zone-ID !=0 it is a locator. See Section 6.10.3.1 for more details.

The Virtual bit in this sub-scheme allows the easy addition of the ACP as a component to existing systems without causing problems in the port number space between the services in the ACP and the existing system. V:0 is the ACP router (autonomic node base system), V:1 is the host with pre-existing transport endpoints on it that could collide with the transport endpoints used by the ACP router. The ACP host could for example have a p2p virtual interface with the V:0 address as its router into the ACP. Depending on the software design of ASAs, which is outside the scope of this specification, they may use the V:0 or V:1 address.

The location of the V bit(s) at the end of the address allows the announcement of a single prefix for each ACP node. For example, in a network with 20,000 ACP nodes, this avoid 20,000 additional routes in the routing table.

6.10.3.1. Usage of the Zone-ID Field

The Zone-ID allows for the introduction of route prefixes in the addressing scheme.

Zone-ID = 0 is the default addressing scheme in an ACP domain. Every ACP node with a Zone Addressing Sub-Scheme address MUST respond to its ACP address with Zone-ID = 0. Used on its own this leads to a
non-hierarchical address scheme, which is suitable for networks up to a certain size. Zone-ID = 0 addresses act as identifiers for the nodes, and aggregation of these address in the ACP routing table is not possible.

If aggregation is required, the 13-bit Zone-ID value allows for up to 8191 zones. The allocation of Zone-ID’s may either happen automatically through a to-be-defined algorithm; or it could be configured and maintained explicitly.

If a node learns (see Appendix A.10.1) that it is part of a zone, it MUST also respond to its ACP address with that Zone-ID. In this case the ACP Loopback is configured with two ACP addresses: One for Zone-ID = 0 and one for the assigned Zone-ID. This method allows for a smooth transition between a flat addressing scheme and a hierarchical one.

A node knowing it is in a zone MUST use that Zone-ID != 0 address in GRASP locator fields. This eliminates the use of the identifier address (Zone-ID = 0) in forwarding and the need for network wide reachability of those non-aggregable identifier addresses. Zone-ID != 0 addresses are assumed to be aggregable in routing/forwarding based on how they are allocated in the ACP topology.

Note: The Zone-ID is one method to introduce structure or hierarchy into the ACP. Another way is the use of the routing subdomain field in the ACP that leads to multiple /48 Global IDs within an ACP domain.

Note: Zones and Zone-ID as defined here are not related to [RFC4007] zones or zone_id. ACP zone addresses are not scoped (reachable only from within an RFC4007 zone) but reachable across the whole ACP. An RFC4007 zone_id is a zone index that has only local significance on a node, whereas an ACP Zone-ID is an identifier for an ACP zone that is unique across that ACP.

6.10.4. ACP Manual Addressing Sub-Scheme

The sub-scheme defined here is defined by the Type value 00b (zero) in the base scheme and 1 in the Z bit.
The fields are defined as follows:

- **Subnet-ID**: Configured subnet identifier.
- **Z**: MUST be 1.
- **Interface Identifier**.

This sub-scheme is meant for "manual" allocation to subnets where the other addressing schemes cannot be used. The primary use case is for assignment to ACP connect subnets (see Section 8.1.1).

"Manual" means that allocations of the Subnet-ID need to be done today with pre-existing, non-autonomic mechanisms. Every subnet that uses this addressing sub-scheme needs to use a unique Subnet-ID (unless some anycast setup is done).

The Z bit field was added to distinguish Zone addressing and manual addressing sub-schemes without requiring one more bit in the base scheme and therefore allowing for the Vlong scheme (described below) to have one more bit available.

Manual addressing sub-scheme addresses SHOULD NOT be used in ACP domain certificates. Any node capable to build ACP secure channels and permitted by Registrar policy to participate in building ACP secure channels SHOULD receive an ACP address (prefix) from one of the other ACP addressing sub-schemes. Nodes not capable (or permitted) to participate in ACP secure channels can connect to the ACP via ACP connect interfaces of ACP edge nodes (see Section 8.1), without setting up an ACP secure channel. Their ACP domain certificate MUST include an empty acp-address to indicate that their ACP domain certificate is only usable for non-ACP secure channel authentication, such as end-to-end transport connections across the ACP or Data-Plane.

Address management of ACP connect subnets is done using traditional assignment methods and existing IPv6 protocols. See Section 8.1.3 for details.
6.10.5. ACP Vlong Addressing Sub-Scheme

The sub-scheme defined here is defined by the Type value 01b (one) in the base scheme.

```
+---------------------++-----------------------------+----------+
|    (base scheme)    ||           Node-ID                      |
|                     || Registrar-ID |F| Node-Number|        V |
+---------------------++--------------+--------------+----------+
```

Figure 13: ACP Vlong Addressing Sub-Scheme

This addressing scheme foregoes the Zone-ID field to allow for larger, flatter routed networks (e.g., as in IoT) with $2^{23}+2^{15}$ Node-Numbers. It also allows for up to $2^{16}$ (i.e. 65536) different virtualized addresses within a node, which could be used to address individual software components in an ACP node.

The fields are the same as in the Zone-ID sub-scheme with the following refinements:

- F: format bit. This bit determines the format of the subsequent bits.

- V: Virtualization bit: this is a field that is either 8 or 16 bits. For F=0, it is 8 bits, for F=1 it is 16 bits. The V bits are assigned by the ACP node. In the ACP certificate’s ACP address Section 6.1.2, the V-bits are always set to 0.

- Registrar-ID: To maximize Node-Number and V, the Registrar-ID is reduced to 46-bits. This still permits the use of the MAC address of an ACP registrar by removing the V and U bits from the 48-bits of a MAC address (those two bits are never unique, so they cannot be used to distinguish MAC addresses).

- The Node-Number is unique to each ACP node. There are two formats for the Node-Number. When F=0, the node-number is 23 bits, for F=1 it is 15 bits. Each format of node-number is considered to be in a unique number space.

The F=0 bit format addresses are intended to be used for "general purpose" ACP nodes that would potentially have a limited number (< 256) of clients (ASA/Autonomic Functions or legacy services) of the ACP that require separate V(irtual) addresses.
The F=1 bit Node-Numbers are intended for ACP nodes that are ACP edge nodes (see Section 8.1.1) or that have a large number of clients requiring separate V(irtual) addresses. For example large SDN controllers with container modular software architecture (see Section 8.1.2).

In the Vlong addressing sub-scheme, the ACP address in the certificate has all V field bits as zero. The ACP address set for the node includes any V value.

6.10.6. Other ACP Addressing Sub-Schemes

Before further addressing sub-schemes are defined, experience with the schemes defined here should be collected. The schemes defined in this document have been devised to allow hopefully sufficiently flexible setup of ACPs for a variety of situation. These reasons also lead to the fairly liberal use of address space: The Zone Addressing Sub-Scheme is intended to enable optimized routing in large networks by reserving bits for Zone-ID’s. The Vlong addressing sub-scheme enables the allocation of 8/16-bit of addresses inside individual ACP nodes. Both address spaces allow distributed, uncoordinated allocation of node addresses by reserving bits for the registrar-ID field in the address.

IANA is asked need to assign a new "type" for each new addressing sub-scheme. With the current allocations, only 2 more schemes are possible, so the last addressing scheme MUST provide further extensions (e.g., by reserving bits from it for further extensions).

6.10.7. ACP Registrars

ACP registrars are responsible to enroll candidate ACP nodes with ACP domain certificates and associated trust point(s). They are also responsible that an ACP domain information field is included in the ACP domain certificate carrying the ACP domain name and the ACP nodes ACP address prefix. This address prefix is intended to persist unchanged through the lifetime of the ACP node.

Because of the ACP addressing sub-schemes, an ACP domain can have multiple distributed ACP registrars that do not need to coordinate for address assignment. ACP registrars can also be sub-CAs, in which case they can also assign ACP domain certificates without dependencies against a (shared) root-CA (except during renewals of their own certificates).

ACP registrars are PKI registration authorities (RA) enhanced with the handling of the ACP domain certificate specific fields. They request certificates for ACP nodes from a Certificate Authority
through any appropriate mechanism (out of scope in this document, but required to be BRSKI for ANI registrars). Only nodes that are trusted to be compliant with the requirements against registrar described in this section must be given the necessary credentials to perform this RA function, such as credentials for the BRSKI connection to the CA for ANI registrars.

6.10.7.1. Use of BRSKI or other Mechanism/Protocols

Any protocols or mechanisms may be used as ACP registrars, as long as the resulting ACP certificate and trust anchors allow to perform the ACP domain membership described in Section 6.1.3 with other ACP domain members, and meet the ACP addressing requirements for its ACP domain information field as described further below in this section.

An ACP registrar could be a person deciding whether to enroll a candidate ACP node and then orchestrating the enrollment of the ACP certificate and associated trust anchor, using command line or web based commands on the candidate ACP node and trust anchor to generate and sign the ACP domain certificate and configure certificate and trust anchors onto the node.

The only currently defined protocol for ACP registrars is BRSKI ([I-D.ietf-anima-bootstrapping-keyinfra]). When BRSKI is used, the ACP nodes are called ANI nodes, and the ACP registrars are called BRSKI or ANI registrars. The BRSKI specification does not define the handling of the ACP domain information field because the rules do not depend on BRSKI but apply equally to any protocols/mechanisms an ACP registrar may use.

6.10.7.2. Unique Address/Prefix allocation

ACP registrars MUST NOT allocate ACP address prefixes to ACP nodes via the ACP domain information field that would collide with the ACP address prefixes of other ACP nodes in the same ACP domain. This includes both prefixes allocated by the same ACP registrar to different ACP nodes as well as prefixes allocated by other ACP registrars for the same ACP domain.

For this purpose, an ACP registrar MUST have one or more unique 46-bit identifiers called Registrar-IDs used to allocate ACP address prefixes. The lower 46-bits of a EUI-48 MAC addresses are globally unique 46 bit identifiers, so ACP registrars with known unique EUI-48 MAC addresses can use these as Registrar-IDs. Registrar-IDs do not need to be globally unique but only unique across the set of ACP registrars for an ACP domain, so other means to assign unique Registrar-IDs to ACP registrars can be used, such as configuration on the ACP registrars.
When the candidate ACP device (called Pledge in BRSKI) is to be enrolled into an ACP domain, the ACP registrar needs to allocate a unique ACP address to the node and ensure that the ACP certificate gets a domain information field (Section 6.1.2) with the appropriate information - ACP domain-name, ACP-address, and so on. If the ACP registrar uses BRSKI, it signals the ACP domain information field to the Pledge via the EST /csrattrs command (see [I-D.ietf-anima-bootstrapping-keyinfra], section 5.9.2 - "EST CSR Attributes").

[RFC Editor: please update reference to section 5.9.2 accordingly with latest BRSKI draft at time of publishing, or RFC]

6.10.7.3. Addressing Sub-Scheme Policies

The ACP registrar selects for the candidate ACP node a unique address prefix from an appropriate ACP addressing sub-scheme, either a zone addressing sub-scheme prefix (see Section 6.10.3), or a Vlong addressing sub-scheme prefix (see Section 6.10.5). The assigned ACP address prefix encoded in the domain information field of the ACP domain certificate indicates to the ACP node its ACP address information. The sub-addressing scheme indicates the prefix length: /127 for zone address sub-scheme, /120 or /112 for Vlong address sub-scheme. The first address of the prefix is the ACP address. All other addresses in the prefix are for other uses by the ACP node as described in the zone and Vlong addressing sub scheme sections. The ACP address prefix itself is then signaled by the ACP node into the ACP routing protocol (see Section 6.11) to establish IPv6 reachability across the ACP.

The choice of addressing sub-scheme and prefix-length in the Vlong address sub-scheme is subject to ACP registrar policy. It could be an ACP domain wide policy, or a per ACP node or per ACP node type policy. For example, in BRSKI, the ACP registrar is aware of the IDevID of the candidate ACP node, which contains a "serialNumber" that is typically indicating the node’s vendor and device type and can be used to drive a policy selecting an appropriate addressing sub-scheme for the (class of) node(s).

ACP registrars SHOULD default to allocate ACP zone sub-address scheme addresses with Zone-ID 0. Allocation and use of zone sub-addresses with Zone-ID != 0 is outside the scope of this specification because it would need to go along with rules for extending ACP routing to multiple zones, which is outside the scope of this specification.

ACP registrars that can use the IDevID of a candidate ACP device SHOULD be able to choose the zone vs. Vlong sub-address scheme for ACP nodes based on the "serialNumber" of the IDevID, for example by
the PID (Product Identifier) part which identifies the product type, or the complete "serialNumber".

In a simple allocation scheme, an ACP registrar remembers persistently across reboots its currently used Registrar-ID and for each addressing scheme (zone with Zone-ID 0, Vlong with /112, Vlong with /120), the next Node-Number available for allocation and increases it during successful enrollment to an ACP node. In this simple allocation scheme, the ACP registrar would not recycle ACP address prefixes from no longer used ACP nodes.

6.10.7.4. Address/Prefix Persistence

When an ACP domain certificate is renewed or rekeyed via EST or other mechanisms, the ACP address/prefix in the ACP domain information field MUST be maintained unless security issues or violations of the unique address assignment requirements exist or are suspected by the ACP registrar.

ACP address information SHOULD be maintained even when the renewing/rekeying ACP registrar is not the same as the one that enrolled the prior ACP certificate. See Section 10.2.4 for an example.

ACP address information SHOULD also be maintained even after an ACP certificate did expire or failed. See Section 6.1.5.5 and Section 6.1.5.6.

6.10.7.5. Further Details

Section 10.2 discusses further informative details of ACP registrars: What interactions registrars need, what parameters they require, certificate renewal and limitations, use of sub-CAs on registrars and centralized policy control.

6.11. Routing in the ACP

Once ULA address are set up all autonomic entities should run a routing protocol within the autonomic control plane context. This routing protocol distributes the ULA created in the previous section for reachability. The use of the autonomic control plane specific context eliminates the probable clash with Data-Plane routing tables and also secures the ACP from interference from the configuration mismatch or incorrect routing updates.

The establishment of the routing plane and its parameters are automatic and strictly within the confines of the autonomic control plane. Therefore, no explicit configuration is required.
All routing updates are automatically secured in transit as the channels of the ACP are encrypted, and this routing runs only inside the ACP.

The routing protocol inside the ACP is RPL ([RFC6550]). See Appendix A.4 for more details on the choice of RPL.

RPL adjacencies are set up across all ACP channels in the same domain including all its routing subdomains. See Appendix A.7 for more details.

6.11.1. RPL Profile

The following is a description of the RPL profile that ACP nodes need to support by default. The format of this section is derived from draft-ietf-roll-applicability-template.

6.11.1.1. Overview

The chosen RPL profile is one that expects a fairly reliable network with reasonably fast links so that RPL convergence will be triggered immediately upon recognition of link failure/recovery.

The profile is also designed to not require any RPL Data-Plane artifacts (such as defined in [RFC6553]). This is largely driven by the desire to avoid introducing the required Hop-by-Hop headers into the ACP forwarding plane, especially to support devices with silicon forwarding planes that cannot support insertion/removal of these headers in silicon or hop-by-hop forwarding based on them. Note: Insertion/removal of headers by a (potentially silicon based) ACP node would be be necessary when senders/receivers of ACP packets are legacy NOC devices connected via ACP connect (see Section 8.1.1 to the ACP. Their connectivity can be handled in RPL as non-RPL-aware leafs (or "Internet") according to the Data-Plane architecture explained in [I-D.ietf-roll-useofrplinfo].

To avoid Data-Plane artefacts, the profile uses a simple destination prefix based routing/forwarding table. To achieve this, the profiles uses only one RPL instanceID. This single instanceID can contain only one Destination Oriented Directed Acyclic Graph (DODAG), and the routing/forwarding table can therefore only calculate a single class of service ("best effort towards the primary NOC/root") and cannot create optimized routing paths to accomplish latency or energy goals between any two nodes.

Consider a network that has multiple NOCs in different locations. Only one NOC will become the DODAG root. Traffic to and from other NOCs has to be sent through the DODAG (shortest path tree) rooted in
the primary NOC. Depending on topology, this can be an annoyance from a latency point of view or from minimizing network path resources, but this is deemed to be acceptable given how ACP traffic is "only" network management/control traffic.

Using a single instanceID/DODAG does not introduce a single point of failure, as the DODAG will reconfigure itself when it detects data-plane forwarding failures including choosing a different root when the primary one fails. See Appendix A.10.4 for more details.

The benefit of this profile, especially compared to other IGPs is that it does not calculate routes for node reachable through the same interface as the DODAG root. This RPL profile can therefore scale to much larger number of ACP nodes in the same amount of compute and memory than other routing protocols. Especially on nodes that are leafs of the topology or those close to those leafs.

The lack of RPL Packet Information (RPI, the IPv6 header for RPL defined by [RFC6553]), means that the Data-Plane will have no rank value that can be used to detect loops. As a result, traffic may loop until the time-to-live (TTL) of the packet reaches zero. This is the same behavior as that of other IGPs that do not have the Data-Plane options of RPL.

Since links in the ACP are assumed to be mostly reliable (or have link layer protection against loss) and because there is no stretch according to Section 6.11.1.7, loops caused by RPL routing packet loss should be exceedingly rare.

There are a variety of mechanisms possible in RPL to further avoid temporary loops: DODAG Information Objects (DIOs) SHOULD be sent 2...3 times to inform children when losing the last parent. The technique in [RFC6550] section 8.2.2.6. (Detaching) SHOULD be favored over that in section 8.2.2.5., (Poisoning) because it allows local connectivity. Nodes SHOULD select more than one parent, at least 3 if possible, and send Destination Advertisement Objects (DAO)s to all of them in parallel.

Additionally, failed ACP tunnels can be quickly discovered through the secure channel protocol mechanisms such as IKEv2 Dead Peer Detection. This can function as a replacement for a Low-power and Lossy Networks’ (LLN’s) Expected Transmission Count (ETX) feature that is not used in this profile. A failure of an ACP tunnel should immediately signal the RPL control plane to pick a different parent.
6.11.1.2. RPL Instances

Single RPL instance. Default RPLInstanceID = 0.

6.11.1.3. Storing vs. Non-Storing Mode

RPL Mode of Operations (MOP): MUST support mode 2 - "Storing Mode of Operations with no multicast support". Implementations MAY support mode 3 ("... with multicast support" as that is a superset of mode 2). Note: Root indicates mode in DIO flow.

6.11.1.4. DAO Policy

Proactive, aggressive DAO state maintenance:

o Use K-flag in unsolicited DAO indicating change from previous information (to require DAO-ACK).

o Retry such DAO DAO-RETRIES(3) times with DAO-ACK_TIME_OUT(256ms) in between.

6.11.1.5. Path Metric

Hopcount.

6.11.1.6. Objective Function

Objective Function (OF): Use OF0 [RFC6552]. No use of metric containers.

rank_factor: Derived from link speed: <= 100Mbps:
LOW_SPEED_FACTOR(5), else HIGH_SPEED_FACTOR(1)

6.11.1.7. DODAG Repair

Global Repair: we assume stable links and ranks (metrics), so no need to periodically rebuild DODAG. DODAG version only incremented under catastrophic events (e.g., administrative action).

Local Repair: As soon as link breakage is detected, send No-Path DAO for all the targets that were reachable only via this link. As soon as link repair is detected, validate if this link provides you a better parent. If so, compute your new rank, and send new DIO that advertises your new rank. Then send a DAO with a new path sequence about yourself.

stretch_rank: none provided ("not stretched").
Data Path Validation: Not used.

Trickle: Not used.

6.11.1.8. Multicast

Not used yet but possible because of the selected mode of operations.

6.11.1.9. Security

[RFC6550] security not used, substituted by ACP security.

Because the ACP links already include provisions for confidentiality and integrity protection, their usage at the RPL layer would be redundant, and so RPL security is not used.

6.11.1.10. P2P communications

Not used.

6.11.1.11. IPv6 address configuration

Every ACP node (RPL node) announces an IPv6 prefix covering the address(es) used in the ACP node. The prefix length depends on the chosen addressing sub-scheme of the ACP address provisioned into the certificate of the ACP node, e.g., /127 for Zone Addressing Sub-Scheme or /112 or /120 for Vlong addressing sub-scheme. See Section 6.10 for more details.

Every ACP node MUST install a black hole (aka null) route for whatever ACP address space that it advertises (i.e.: the /96 or /127). This is avoid routing loops for addresses that an ACP node has not (yet) used.

6.11.1.12. Administrative parameters

Administrative Preference ([RFC6550], 3.2.6 - to become root):
Indicated in DODAGPreference field of DIO message.

- Explicit configured "root": 0b100
- ACP registrar (Default): 0b011
- ACP-connect (non-registrar): 0b010
- Default: 0b001.
6.11.1.13. RPL Data-Plane artifacts

RPI (RPL Packet Information [RFC6553]): Not used as there is only a single instance, and data path validation is not being used.

SRH (RPL Source Routing - RFC6552): Not used. Storing mode is being used.

6.11.1.14. Unknown Destinations

Because RPL minimizes the size of the routing and forwarding table, prefixes reachable through the same interface as the RPL root are not known on every ACP node. Therefore traffic to unknown destination addresses can only be discovered at the RPL root. The RPL root SHOULD have attach safe mechanisms to operationally discover and log such packets.

As this requirement raises additional data plane requirements, it does not apply to nodes where the administrative parameter to become root (Section 6.11.1.12) can always only be 0b001, e.g.: the node does not support explicit configuration to be root, or to be ACP registrar or to have ACP-connect functionality. If an ACP network is degraded to the point where there are no nodes that could be configured roots, ACP registrars or ACP-connect nodes, traffic to unknown destinations could not be diagnosed, but in the absence of any intelligent nodes supporting other than 0b001 administrative preference, there is likely also no diagnostic function possible.

6.12. General ACP Considerations

Since channels are by default established between adjacent neighbors, the resulting overlay network does hop-by-hop encryption. Each node decrypts incoming traffic from the ACP, and encrypts outgoing traffic to its neighbors in the ACP. Routing is discussed in Section 6.11.

6.12.1. Performance

There are no performance requirements against ACP implementations defined in this document because the performance requirements depend on the intended use case. It is expected that full autonomic node with a wide range of ASA can require high forwarding plane performance in the ACP, for example for telemetry. Implementations of ACP to solely support traditional/SDN style use cases can benefit from ACP at lower performance, especially if the ACP is used only for critical operations, e.g., when the Data-Plane is not available. The design of the ACP as specified in this document is intended to support a wide range of performance options: It is intended to allow software-only implementations at potentially low performance, but can
also support high performance options. See [RFC8368] for more details.

6.12.2. Addressing of Secure Channels

In order to be independent of the Data-Plane (routing and addressing) the GRASP discovered (autonomic) ACP secure channels use IPv6 link local addresses between adjacent neighbors. Note: Section 8.2 specifies extensions in which secure channels are configured tunnels operating over the Data-Plane, so those secure channels cannot be independent of the Data-Plane.

To avoid that Data-Plane configuration can impact the operations of the IPv6 (link-local) interface/address used for ACP channels, appropriate implementation considerations are required. If the IPv6 interface/link-local address is shared with the Data-Plane it needs to be impossible to unconfigure/disable it through configuration. Instead of sharing the IPv6 interface/link-local address, a separate (virtual) interface with a separate IPv6 link-local address can be used. For example, the ACP interface could be run over a separate MAC address of an underlying L2 (Ethernet) interface. For more details and options, see Appendix A.10.2.

Note that other (non-ideal) implementation choices may introduce additional undesired dependencies against the Data-Plane. For example shared code and configuration of the secure channel protocols (IPsec / DTLS).

6.12.3. MTU

The MTU for ACP secure channels must be derived locally from the underlying link MTU minus the secure channel encapsulation overhead.

ACP secure Channel protocols do not need to perform MTU discovery because they are built across L2 adjacencies - the MTU on both sides connecting to the L2 connection are assumed to be consistent. Extensions to ACP where the ACP is for example tunneled need to consider how to guarantee MTU consistency. This is an issue of tunnels, not an issue of running the ACP across a tunnel. Transport stacks running across ACP can perform normal PMTUD (Path MTU Discovery). Because the ACP is meant to be prioritize reliability over performance, they MAY opt to only expect IPv6 minimum MTU (1280) to avoid running into PMTUD implementation bugs or underlying link MTU mismatch problems.
6.12.4. Multiple links between nodes

If two nodes are connected via several links, the ACP SHOULD be established across every link, but it is possible to establish the ACP only on a sub-set of links. Having an ACP channel on every link has a number of advantages, for example it allows for a faster failover in case of link failure, and it reflects the physical topology more closely. Using a subset of links (for example, a single link), reduces resource consumption on the node, because state needs to be kept per ACP channel. The negotiation scheme explained in Section 6.5 allows Alice (the node with the higher ACP address) to drop all but the desired ACP channels to Bob - and Bob will not re-try to build these secure channels from his side unless Alice shows up with a previously unknown GRASP announcement (e.g., on a different link or with a different address announced in GRASP).

6.12.5. ACP interfaces

The ACP VRF has conceptually two type of interfaces: The "ACP Loopback interface(s)" to which the ACP ULA address(es) are assigned and the "ACP virtual interfaces" that are mapped to the ACP secure channels.

The term "Loopback interface" was introduced initially to refer to an internal interface on a node that would allow IP traffic between transport endpoints on the node in the absence or failure of any or all external interfaces, see [RFC4291] section 2.5.3.

Even though Loopback interfaces were originally designed to hold only Loopback addresses not reachable from outside the node, these interfaces are also commonly used today to hold addresses reachable from the outside. They are meant to be reachable independent of any external interface being operational, and therefore to be more resilient. These addresses on Loopback interfaces can be thought of as "node addresses" instead of "interface addresses", and that is what ACP address(es) are. This construct makes it therefore possible to address ACP nodes with a well-defined set of addresses independent of the number of external interfaces.

For these reason, the ACP (ULA) address(es) are assigned to Loopback interface(s).

Any type of ACP secure channels to another ACP node can be mapped to ACP virtual interfaces in following ways. This is independent of the chosen secure channel protocol (IPsec, DTLS or other future protocol - standards or non-standards):

ACP point-to-point virtual interface:
Each ACP secure channel is mapped into a separate point-to-point ACP virtual interface. If a physical subnet has more than two ACP capable nodes (in the same domain), this implementation approach will lead to a full mesh of ACP virtual interfaces between them.

ACP multi-access virtual interface:

In a more advanced implementation approach, the ACP will construct a single multi-access ACP virtual interface for all ACP secure channels to ACP capable nodes reachable across the same underlying (physical) subnet. IPv6 link-local multicast packets sent into an ACP multi-access virtual interface are replicated to every ACP secure channel mapped into the ACP multicast-access virtual interface. IPv6 unicast packets sent into an ACP multi-access virtual interface are sent to the ACP secure channel that belongs to the ACP neighbor that is the next-hop in the ACP forwarding table entry used to reach the packets destination address.

There is no requirement for all ACP nodes on the same multi-access subnet to use the same type of ACP virtual interface. This is purely a node local decision.

ACP nodes MUST perform standard IPv6 operations across ACP virtual interfaces including SLAAC (Stateless Address Auto-Configuration) - [RFC4862]) to assign their IPv6 link local address on the ACP virtual interface and ND (Neighbor Discovery - [RFC4861]) to discover which IPv6 link-local neighbor address belongs to which ACP secure channel mapped to the ACP virtual interface. This is independent of whether the ACP virtual interface is point-to-point or multi-access.

"Optimistic Duplicate Address Detection (DAD)" according to [RFC4429] is RECOMMENDED because the likelihood for duplicates between ACP nodes is highly improbable as long as the address can be formed from a globally unique local assigned identifier (e.g., EUI-48/EUI-64, see below).

ACP nodes MAY reduce the amount of link-local IPv6 multicast packets from ND by learning the IPv6 link-local neighbor address to ACP secure channel mapping from other messages such as the source address of IPv6 link-local multicast RPL messages - and therefore forego the need to send Neighbor Solicitation messages.

The ACP virtual interface IPv6 link local address can be derived from any appropriate local mechanism such as node local EUI-48 or EUI-64 ("EUI" stands for "Extended Unique Identifier"). It MUST NOT depend on something that is attackable from the Data-Plane such as the IPv6 link-local address of the underlying physical interface, which can be
attacked by SLAAC, or parameters of the secure channel encapsulation header that may not be protected by the secure channel mechanism.

The link-layer address of an ACP virtual interface is the address used for the underlying interface across which the secure tunnels are built, typically Ethernet addresses. Because unicast IPv6 packets sent to an ACP virtual interface are not sent to a link-layer destination address but rather an ACP secure channel, the link-layer address fields SHOULD be ignored on reception and instead the ACP secure channel from which the message was received should be remembered.

Multi-access ACP virtual interfaces are preferable implementations when the underlying interface is a (broadcast) multi-access subnet because they do reflect the presence of the underlying multi-access subnet into the virtual interfaces of the ACP. This makes it for example simpler to build services with topology awareness inside the ACP VRF in the same way as they could have been built running natively on the multi-access interfaces.

Consider also the impact of point-to-point vs. multi-access virtual interface on the efficiency of flooding via link local multicasted messages:

Assume a LAN with three ACP neighbors, Alice, Bob and Carol. Alice’s ACP GRASP wants to send a link-local GRASP multicast message to Bob and Carol. If Alice’s ACP emulates the LAN as one point-to-point virtual interface to Bob and one to Carol, The sending application itself will send two copies, if Alice’s ACP emulates a LAN, GRASP will send one packet and the ACP will replicate it. The result is the same. The difference happens when Bob and Carol receive their packet. If they use ACP point-to-point virtual interfaces, their GRASP instance would forward the packet from Alice to each other as part of the GRASP flooding procedure. These packets are unnecessary and would be discarded by GRASP on receipt as duplicates (by use of the GRASP Session ID). If Bob and Carol’s ACP would emulate a multi-access virtual interface, then this would not happen, because GRASPs flooding procedure does not replicate back packets to the interface that they were received from.

Note that link-local GRASP multicast messages are not sent directly as IPv6 link-local multicast UDP messages into ACP virtual interfaces, but instead into ACP GRASP virtual interfaces, that are layered on top of ACP virtual interfaces to add TCP reliability to link-local multicast GRASP messages. Nevertheless, these ACP GRASP virtual interfaces perform the same replication of message and, therefore, result in the same impact on flooding. See Section 6.8.2 for more details.
RPL does support operations and correct routing table construction across non-broadcast multi-access (NBMA) subnets. This is common when using many radio technologies. When such NBMA subnets are used, they MUST NOT be represented as ACP multi-access virtual interfaces because the replication of IPv6 link-local multicast messages will not reach all NBMA subnet neighbors. In result, GRASP message flooding would fail. Instead, each ACP secure channel across such an interface MUST be represented as a ACP point-to-point virtual interface. See also Appendix A.10.4.

Care must also be taken when creating multi-access ACP virtual interfaces across ACP secure channels between ACP nodes in different domains or routing subdomains. If for example future inter-domain ACP policies are defined as "peer-to-peer" policies, it is easier to create ACP point-to-point virtual interfaces for these inter-domain secure channels.

7. ACP support on L2 switches/ports (Normative)

7.1. Why (Benefits of ACP on L2 switches)

Consider a large L2 LAN with ANrtr1...ANrtrN connected via some topology of L2 switches. Examples include large enterprise campus networks with an L2 core, IoT networks or broadband aggregation networks which often have even a multi-level L2 switched topology.

If the discovery protocol used for the ACP is operating at the subnet level, every ACP router will see all other ACP routers on the LAN as neighbors and a full mesh of ACP channels will be built. If some or all of the AN switches are autonomic with the same discovery protocol, then the full mesh would include those switches as well.

A full mesh of ACP connections can create fundamental scale challenges. The number of security associations of the secure channel protocols will likely not scale arbitrarily, especially when they leverage platform accelerated encryption/decryption. Likewise, any other ACP operations (such as routing) needs to scale to the number of direct ACP neighbors. An ACP router with just 4 physical interfaces might be deployed into a LAN with hundreds of neighbors connected via switches. Introducing such a new unpredictable scaling
factor requirement makes it harder to support the ACP on arbitrary platforms and in arbitrary deployments.

Predictable scaling requirements for ACP neighbors can most easily be achieved if in topologies such as these, ACP capable L2 switches can ensure that discovery messages terminate on them so that neighboring ACP routers and switches will only find the physically connected ACP L2 switches as their candidate ACP neighbors. With such a discovery mechanism in place, the ACP and its security associations will only need to scale to the number of physical interfaces instead of a potentially much larger number of "LAN-connected" neighbors. And the ACP topology will follow directly the physical topology, something which can then also be leveraged in management operations or by ASAs.

In the example above, consider ANswitch1 and ANswitchM are ACP capable, and ANswitch2 is not ACP capable. The desired ACP topology is that ANrtr1 and ANrtrM only have an ACP connection to ANswitch1, and that ANswitch1, ANrtr2, ANrtrN have a full mesh of ACP connection amongst each other. ANswitch1 also has an ACP connection with ANswitchM and ANswitchM has ACP connections to anything else behind it.

7.2. How (per L2 port DULL GRASP)

To support ACP on L2 switches or L2 switched ports of an L3 device, it is necessary to make those L2 ports look like L3 interfaces for the ACP implementation. This primarily involves the creation of a separate DULL GRASP instance/domain on every such L2 port. Because GRASP has a dedicated link-local IPv6 multicast address (ALL_GRASP_NEIGHBORS), it is sufficient that all packets for this address are being extracted at the port level and passed to that DULL GRASP instance. Likewise the IPv6 link-local multicast packets sent by that DULL GRASP instance need to be sent only towards the L2 port for this DULL GRASP instance.

If the device with L2 ports is supporting per L2 port ACP DULL GRASP as well as MLD snooping ([RFC4541]), then MLD snooping must be changed to never forward packets for ALL_GRASP_NEIGHBORS because that would cause the problem that per L2 port ACP DULL GRASP is meant to overcome (forwarding DULL GRASP packets across L2 ports).

The rest of ACP operations can operate in the same way as in L3 devices: Assume for example that the device is an L3/L2 hybrid device where L3 interfaces are assigned to VLANs and each VLAN has potentially multiple ports. DULL GRASP is run as described individually on each L2 port. When it discovers a candidate ACP neighbor, it passes its IPv6 link-local address and supported secure channel protocols to the ACP secure channel negotiation that can be
bound to the L3 (VLAN) interface. It will simply use link-local IPv6 multicast packets to the candidate ACP neighbor. Once a secure channel is established to such a neighbor, the virtual interface to which this secure channel is mapped should then actually be the L2 port and not the L3 interface to best map the actual physical topology into the ACP virtual interfaces. See Section 6.12.5 for more details about how to map secure channels into ACP virtual interfaces. Note that a single L2 port can still have multiple ACP neighbors if it connect for example to multiple ACP neighbors via a non-ACP enabled switch. The per L2 port ACP virtual interface can therefore still be a multi-access virtual LAN.

For example, in the above picture, ANswitch1 would run separate DULL GRASP instances on its ports to ANrtr1, ANswitch2 and ANswitchI, even though all those three ports may be in the data plane in the same (V)LAN and perform L2 switching between these ports, ANswitch1 would perform ACP L3 routing between them.

The description in the previous paragraph was specifically meant to illustrate that on hybrid L3/L2 devices that are common in enterprise, IoT and broadband aggregation, there is only the GRASP packet extraction (by Ethernet address) and GRASP link-local multicast per L2-port packet injection that has to consider L2 ports at the hardware forwarding level. The remaining operations are purely ACP control plane and setup of secure channels across the L3 interface. This hopefully makes support for per-L2 port ACP on those hybrid devices easy.

This L2/L3 optimized approach is subject to "address stealing", e.g., where a device on one port uses addresses of a device on another port. This is a generic issue in L2 LANs and switches often already have some form of "port security" to prohibit this. They rely on NDP or DHCP learning of which port/MAC-address and IPv6 address belong together and block duplicates. This type of function needs to be enabled to prohibit DoS attacks. Likewise the GRASP DULL instance needs to ensure that the IPv6 address in the locator-option matches the source IPv6 address of the DULL GRASP packet.

In devices without such a mix of L2 port/interfaces and L3 interfaces (to terminate any transport layer connections), implementation details will differ. Logically most simply every L2 port is considered and used as a separate L3 subnet for all ACP operations. The fact that the ACP only requires IPv6 link-local unicast and multicast should make support for it on any type of L2 devices as simple as possible.

A generic issue with ACP in L2 switched networks is the interaction with the Spanning Tree Protocol. Without further L2 enhancements,
the ACP would run only across the active STP topology and the ACP would be interrupted and re-converge with STP changes. Ideally, ACP peering should be built also across ports that are blocked in STP so that the ACP does not depend on STP and can continue to run unaffected across STP topology changes, where re-convergence can be quite slow. The above described simple implementation options are not sufficient to achieve this.

8. Support for Non-ACP Components (Normative)

8.1. ACP Connect

8.1.1. Non-ACP Controller / NMS system

The Autonomic Control Plane can be used by management systems, such as controllers or network management system (NMS) hosts (henceforth called simply "NMS hosts"), to connect to devices (or other type of nodes) through it. For this, an NMS host must have access to the ACP. The ACP is a self-protecting overlay network, which allows by default access only to trusted, autonomic systems. Therefore, a traditional, non-ACP NMS system does not have access to the ACP by default, such as any other external node.

If the NMS host is not autonomic, i.e., it does not support autonomic negotiation of the ACP, then it can be brought into the ACP by explicit configuration. To support connections to adjacent non-ACP nodes, an ACP node must support "ACP connect" (sometimes also called "autonomic connect"): "ACP connect" is an interface level configured workaround for connection of trusted non-ACP nodes to the ACP. The ACP node on which ACP connect is configured is called an "ACP edge node". With ACP connect, the ACP is accessible from those non-ACP nodes (such as NOC systems) on such an interface without those non-ACP nodes having to support any ACP discovery or ACP channel setup. This is also called "native" access to the ACP because to those (NOC) systems the interface looks like a normal network interface (without any encryption/novel-signaling).
ACP connect has security consequences: All systems and processes connected via ACP connect have access to all ACP nodes on the entire ACP, without further authentication. Thus, the ACP connect interface and (NOC) systems connected to it must be physically controlled/secured. For this reason the mechanisms described here do explicitly not include options to allow for a non-ACP router to be connected across an ACP connect interface and addresses behind such a router routed inside the ACP.

An ACP connect interface provides exclusively access to only the ACP. This is likely insufficient for many NMS hosts. Instead, they would require a second "Data-Plane" interface outside the ACP for connections between the NMS host and administrators, or Internet based services, or for direct access to the Data-Plane. The document "Using Autonomic Control Plane for Stable Connectivity of Network OAM" [RFC8368] explains in more detail how the ACP can be integrated in a mixed NOC environment.

An ACP connect interface SHOULD use an IPv6 address/prefix from the ACP Manual Addressing Sub-Scheme (Section 6.10.4), letting the operator configure for example only the Subnet-ID and having the node automatically assign the remaining part of the prefix/address. It SHOULD NOT use a prefix that is also routed outside the ACP so that the addresses clearly indicate whether it is used inside the ACP or not.
The prefix of ACP connect subnets MUST be distributed by the ACP edge node into the ACP routing protocol (RPL). The NMS hosts MUST connect to prefixes in the ACP routing table via its ACP connect interface. In the simple case where the ACP uses only one ULA prefix and all ACP connect subnets have prefixes covered by that ULA prefix, NMS hosts can rely on [RFC6724] to determine longest match prefix routes towards its different interfaces, ACP and data-plane. With RFC6724, the NMS host will select the ACP connect interface for all addresses in the ACP because any ACP destination address is longest matched by the address on the ACP connect interface. If the NMS hosts ACP connect interface uses another prefix or if the ACP uses multiple ULA prefixes, then the NMS hosts require (static) routes towards the ACP interface for these prefixes.

When an ACP Edge node receives a packet from an ACP connect interface, the ACP Edge node MUST only forward the packet into the ACP if the packet has an IPv6 source address from that interface. This is sometimes called "RPF filtering". This MAY be changed through administrative measures.

To limit the security impact of ACP connect, nodes supporting it SHOULD implement a security mechanism to allow configuration/use of ACP connect interfaces only on nodes explicitly targeted to be deployed with it (those in physically secure locations such as a NOC). For example, the registrar could disable the ability to enable ACP connect on devices during enrollment and that property could only be changed through re-enrollment. See also Appendix A.10.5.

8.1.2. Software Components

The ACP connect mechanism be only be used to connect physically external systems (NMS hosts) to the ACP but also other applications, containers or virtual machines. In fact, one possible way to eliminate the security issue of the external ACP connect interface is to collocate an ACP edge node and an NMS host by making one a virtual machine or container inside the other; and therefore converting the unprotected external ACP subnet into an internal virtual subnet in a single device. This would ultimately result in a fully ACP enabled NMS host with minimum impact to the NMS hosts software architecture. This approach is not limited to NMS hosts but could equally be applied to devices consisting of one or more VNF (virtual network functions): An internal virtual subnet connecting out-of-band management interfaces of the VNFs to an ACP edge router VNF.

The core requirement is that the software components need to have a network stack that permits access to the ACP and optionally also the Data-Plane. Like in the physical setup for NMS hosts this can be realized via two internal virtual subnets. One that is connecting to
the ACP (which could be a container or virtual machine by itself), and one (or more) connecting into the Data-Plane.

This "internal" use of ACP connect approach should not considered to be a "workaround" because in this case it is possible to build a correct security model: It is not necessary to rely on unprovable external physical security mechanisms as in the case of external NMS hosts. Instead, the orchestration of the ACP, the virtual subnets and the software components can be done by trusted software that could be considered to be part of the ANI (or even an extended ACP). This software component is responsible for ensuring that only trusted software components will get access to that virtual subnet and that only even more trusted software components will get access to both the ACP virtual subnet and the Data-Plane (because those ACP users could leak traffic between ACP and Data-Plane). This trust could be established for example through cryptographic means such as signed software packages.

8.1.3. Auto Configuration

ACP edge nodes, NMS hosts and software components that as described in the previous section are meant to be composed via virtual interfaces SHOULD support on the ACP connect subnet StateLess Address Autoconfiguration (SLAAC - [RFC4862]) and route auto configuration according to [RFC4191].

The ACP edge node acts as the router on the ACP connect subnet, providing the (auto-)configured prefix for the ACP connect subnet to NMS hosts and/or software components. The ACP edge node uses route prefix option of RFC4191 to announce the default route (::/) with a lifetime of 0 and aggregated prefixes for routes in the ACP routing table with normal lifetimes. This will ensure that the ACP edge node does not become a default router, but that the NMS hosts and software components will route the prefixes used in the ACP to the ACP edge node.

Aggregated prefix means that the ACP edge node needs to only announce the /48 ULA prefixes used in the ACP but none of the actual /64 (Manual Addressing Sub-Scheme), /127 (ACP Zone Addressing Sub-Scheme), /112 or /120 (Vlong Addressing Sub-Scheme) routes of actual ACP nodes. If ACP interfaces are configured with non ULA prefixes, then those prefixes cannot be aggregated without further configured policy on the ACP edge node. This explains the above recommendation to use ACP ULA prefix covered prefixes for ACP connect interfaces: They allow for a shorter list of prefixes to be signaled via RFC4191 to NMS hosts and software components.
The ACP edge nodes that have a Vlong ACP address MAY allocate a subset of their /112 or /120 address prefix to ACP connect interface(s) to eliminate the need to non-autonomically configure/provision the address prefixes for such ACP connect interfaces.

8.1.4. Combined ACP/Data-Plane Interface (VRF Select)

Using two physical and/or virtual subnets (and therefore interfaces) into NMS Hosts (as per Section 8.1.1) or Software (as per Section 8.1.2) may be seen as additional complexity, for example with legacy NMS Hosts that support only one IP interface.

To provide a single subnet into both ACP and Data-Plane, the ACP Edge node needs to de-multiplex packets from NMS hosts into ACP VRF and Data-Plane. This is sometimes called "VRF select". If the ACP VRF has no overlapping IPv6 addresses with the Data-Plane (it should have no overlapping addresses), then this function can use the IPv6 Destination address. The problem is Source Address Selection on the NMS Host(s) according to RFC6724.

Consider the simple case: The ACP uses only one ULA prefix, the ACP IPv6 prefix for the Combined ACP and Data-Plane interface is covered by that ULA prefix. The ACP edge node announces both the ACP IPv6 prefix and one (or more) prefixes for the Data-Plane. Without further policy configurations on the NMS Host(s), it may select its ACP address as a source address for Data-Plane ULA destinations because of Rule 8 of RFC6724. The ACP edge node can pass on the packet to the Data-Plane, but the ACP source address should not be used for Data-Plane traffic, and return traffic may fail.
If the ACP carries multiple ULA prefixes or non-ULA ACP connect prefixes, then the correct source address selection becomes even more problematic.

With separate ACP connect and Data-Plane subnets and RFC4191 prefix announcements that are to be routed across the ACP connect interface, RFC6724 source address selection Rule 5 (use address of outgoing interface) will be used, so that above problems do not occur, even in more complex cases of multiple ULA and non-ULA prefixes in the ACP routing table.

To achieve the same behavior with a Combined ACP and Data-Plane interface, the ACP Edge Node needs to behave as two separate routers on the interface: One link-local IPv6 address/router for its ACP reachability, and one link-local IPv6 address/router for its Data-Plane reachability. The Router Advertisements for both are as described above (Section 8.1.3): For the ACP, the ACP prefix is announced together with RFC4191 option for the prefixes routed across the ACP and lifetime=0 to disqualify this next-hop as a default router. For the Data-Plane, the Data-Plane prefix(es) are announced together with whatever default router parameters are used for the Data-Plane.

In result, RFC6724 source address selection Rule 5.5 may result in the same correct source address selection behavior of NMS hosts without further configuration on it as the separate ACP connect and Data-Plane interfaces. As described in the text for Rule 5.5, this is only a MAY, because IPv6 hosts are not required to track next-hop information. If an NMS Host does not do this, then separate ACP connect and Data-Plane interfaces are the preferable method of attachment. Hosts implementing [RFC8028] should (instead of may) implement [RFC6724] Rule 5.5, so it is preferred for hosts to support [RFC8028].

ACP edge nodes MAY support the Combined ACP and Data-Plane interface.

8.1.5. Use of GRASP

GRASP can and should be possible to use across ACP connect interfaces, especially in the architectural correct solution when it is used as a mechanism to connect Software (e.g., ASA or legacy NMS applications) to the ACP.

Given how the ACP is the security and transport substrate for GRASP, the requirements for devices connected via ACP connect is that those are equivalently (if not better) secured against attacks and run only software that is equally (if not better) protected, known (or
trusted) not to be malicious and accordingly designed to isolate access to the ACP against external equipment.

The difference in security is that cryptographic security of the ACP secure channel is replaced by required physical security of the network connection between an ACP edge node and the NMS or other host reachable via the ACP connect interface. Node integrity too is expected to be easier because the ACP connect node, the ACP connect link and the nodes connecting to it must be in a contiguous secure location, hence assuming there can be no physical attack against the devices.

When using "Combined ACP and Data-Plane Interfaces", care must be taken that only GRASP messages intended for the ACP GRASP domain received from Software or NMS Hosts are forwarded by ACP edge nodes. Currently there is no definition for a GRASP security and transport substrate beside the ACP, so there is no definition how such Software/NMS Host could participate in two separate GRASP Domains across the same subnet (ACP and Data-Plane domains). At current it is assumed that all GRASP packets on a Combined ACP and Data-Plane interface belong to the GRASP ACP Domain. They must all use the ACP IPv6 addresses of the Software/NMS Hosts. The link-local IPv6 addresses of Software/NMS Hosts (used for GRASP M_DISCOVERY and M_FLOOD messages) are also assumed to belong to the ACP address space.

8.2. ACP through Non-ACP L3 Clouds (Remote ACP neighbors)

Not all nodes in a network may support the ACP. If non-ACP Layer-2 devices are between ACP nodes, the ACP will work across it since it is IP based. However, the autonomic discovery of ACP neighbors via DULL GRASP is only intended to work across L2 connections, so it is not sufficient to autonomically create ACP connections across non-ACP Layer-3 devices.

8.2.1. Configured Remote ACP neighbor

On the ACP node, remote ACP neighbors are configured explicitly. The parameters of such a "connection" are described in the following ABNF.
connection = [ method , local-addr, remote-addr, ?pmtu ]
method   = [ "IKEv2" , ?port ]
method //= [ "DTLS",    port ]
local-addr = [ address , ?vrf ]
remote-addr = [ address ]
address = ("any" | ipv4-address | ipv6-address )
vrf = tstr ; Name of a VRF on this node with local-address

Figure 17: Parameters for remote ACP neighbors

Explicit configuration of a remote-peer according to this ABNF provides all the information to build a secure channel without requiring a tunnel to that peer and running DULL GRASP inside of it.

The configuration includes the parameters otherwise signaled via DULL GRASP: local address, remote (peer) locator and method. The differences over DULL GRASP local neighbor discovery and secure channel creation are as follows:

- The local and remote address can be IPv4 or IPv6 and are typically global scope addresses.

- The VRF across which the connection is built (and in which local-addr exists) can to be specified. If vrf is not specified, it is the default VRF on the node. In DULL GRASP the VRF is implied by the interface across which DULL GRASP operates.

- If local address is "any", the local address used when initiating a secure channel connection is decided by source address selection ([RFC6724] for IPv6). As a responder, the connection listens on all addresses of the node in the selected VRF.

- Configuration of port is only required for methods where no defaults exist (e.g., "DTLS").

- If remote address is "any", the connection is only a responder. It is a "hub" that can be used by multiple remote peers to connect simultaneously - without having to know or configure their addresses. Example: Hub site for remote "spoke" sites reachable over the Internet.

- Pmtu should be configurable to overcome issues/limitations of Path MTU Discovery (PMTUD).

- IKEv2/IPsec to remote peers should support the optional NAT Traversal (NAT-T) procedures.
8.2.2. Tunneled Remote ACP Neighbor

An IPinIP, GRE or other form of pre-existing tunnel is configured between two remote ACP peers and the virtual interfaces representing the tunnel are configured for "ACP enable". This will enable IPv6 link local addresses and DULL on this tunnel. In result, the tunnel is used for normal "L2 adjacent" candidate ACP neighbor discovery with DULL and secure channel setup procedures described in this document.

Tunneled Remote ACP Neighbor requires two encapsulations: the configured tunnel and the secure channel inside of that tunnel. This makes it in general less desirable than Configured Remote ACP Neighbor. Benefits of tunnels are that it may be easier to implement because there is no change to the ACP functionality - just running it over a virtual (tunnel) interface instead of only native interfaces. The tunnel itself may also provide PMTUD while the secure channel method may not. Or the tunnel mechanism is permitted/possible through some firewall while the secure channel method may not.

8.2.3. Summary

Configured/Tunneled Remote ACP neighbors are less "indestructible" than L2 adjacent ACP neighbors based on link local addressing, since they depend on more correct Data-Plane operations, such as routing and global addressing.

Nevertheless, these options may be crucial to incrementally deploy the ACP, especially if it is meant to connect islands across the Internet. Implementations SHOULD support at least Tunneled Remote ACP Neighbors via GRE tunnels - which is likely the most common router-to-router tunneling protocol in use today.

9. Benefits (Informative)

9.1. Self-Healing Properties

The ACP is self-healing:

- New neighbors will automatically join the ACP after successful validation and will become reachable using their unique ULA address across the ACP.

- When any changes happen in the topology, the routing protocol used in the ACP will automatically adapt to the changes and will continue to provide reachability to all nodes.
The ACP tracks the validity of peer certificates and tears down ACP secure channels when a peer certificate has expired. When short-lived certificates with lifetimes in the order of OCSP/CRL refresh times are used, then this allows for removal of invalid peers (whose certificate was not renewed) at similar speeds as when using OCSP/CRL. The same benefit can be achieved when using CRL/OCSP, periodically refreshing the revocation information and also tearing down ACP secure channels when the peer’s (long-lived) certificate is revoked. There is no requirement against ACP implementations to require this enhancement though to keep the mandatory implementations simpler.

The ACP can also sustain network partitions and mergers. Practically all ACP operations are link local, where a network partition has no impact. Nodes authenticate each other using the domain certificates to establish the ACP locally. Addressing inside the ACP remains unchanged, and the routing protocol inside both parts of the ACP will lead to two working (although partitioned) ACPs.

There are few central dependencies: A certificate revocation list (CRL) may not be available during a network partition; a suitable policy to not immediately disconnect neighbors when no CRL is available can address this issue. Also, an ACP registrar or Certificate Authority might not be available during a partition. This may delay renewal of certificates that are to expire in the future, and it may prevent the enrollment of new nodes during the partition.

Highly resilient ACP designs can be built by using ACP registrars with embedded sub-CA, as outlined in Section 10.2.4. As long as a partition is left with one or more of such ACP registrars, it can continue to enroll new candidate ACP nodes as long as the ACP registrar’s sub-CA certificate does not expire. Because the ACP addressing relies on unique Registrar-IDs, a later re-merge of partitions will also not cause problems with ACP addresses assigned during partitioning.

After a network partition, a re-merge will just establish the previous status, certificates can be renewed, the CRL is available, and new nodes can be enrolled everywhere. Since all nodes use the same trust anchor(s), a re-merge will be smooth.

Merging two networks with different trust anchors requires the ACP nodes to trust the union of Trust Anchors. As long as the routing-subdomain hashes are different, the addressing will not overlap, which only happens in the unlikely event of a 40-bit hash collision in SHA256 (see Section 6.10). Note that the complete mechanisms to merge networks is out of scope of this specification.
It is also highly desirable for implementation of the ACP to be able to run it over interfaces that are administratively down. If this is not feasible, then it might instead be possible to request explicit operator override upon administrative actions that would administratively bring down an interface across which the ACP is running. Especially if bringing down the ACP is known to disconnect the operator from the node. For example any such down administrative action could perform a dependency check to see if the transport connection across which this action is performed is affected by the down action (with default RPL routing used, packet forwarding will be symmetric, so this is actually possible to check).

9.2. Self-Protection Properties

9.2.1. From the outside

As explained in Section 6, the ACP is based on secure channels built between nodes that have mutually authenticated each other with their domain certificates. The channels themselves are protected using standard encryption technologies such as DTLS or IPsec which provide additional authentication during channel establishment, data integrity and data confidentiality protection of data inside the ACP and in addition, provide replay protection.

An attacker will not be able to join the ACP unless having a valid domain certificate, also packet injection and sniffing traffic will not be possible due to the security provided by the encryption protocol.

The ACP also serves as protection (through authentication and encryption) for protocols relevant to OAM that may not have secured protocol stack options or where implementation or deployment of those options fall on some vendor/product/customer limitations. This includes protocols such as SNMP ([RFC3411]), NTP ([RFC5905]), PTP ([IEEE-1588-2008]), DNS ([RFC1886]), DHCPv6 ([RFC3315]), syslog ([RFC3164]), Radius ([RFC2865]), Diameter ([RFC6733]), TACACS ([RFC1492]), IPFIX ([RFC7011]), Netflow ([RFC3954]) - just to name a few. Protection via the ACP secure hop-by-hop channels for these protocols is meant to be only a stopgap though: The ultimate goal is for these and other protocols to use end-to-end encryption utilizing the domain certificate and rely on the ACP secure channels primarily for zero-touch reliable connectivity, but not primarily for security.

The remaining attack vector would be to attack the underlying ACP protocols themselves, either via directed attacks or by denial-of-service attacks. However, as the ACP is built using link-local IPv6 addresses, remote attacks from the data-plane are impossible as long as the data-plane has no facilities to remotely sent IPv6 link-local
The only exception are ACP connected interfaces which require higher physical protection. The ULA addresses are only reachable inside the ACP context, therefore, unreachable from the Data-Plane. Also, the ACP protocols should be implemented to be attack resistant and not consume unnecessary resources even while under attack.

9.2.2. From the inside

The security model of the ACP is based on trusting all members of the group of nodes that receive an ACP domain certificate for the same domain. Attacks from the inside by a compromised group member are therefore the biggest challenge.

Group members must be protected against attackers so that there is no easy way to compromise them, or use them as a proxy for attacking other devices across the ACP. For example, management plane functions (transport ports) should only be reachable from the ACP but not the Data-Plane. Especially for those management plane functions that have no good protection by themselves because they do not have secure end-to-end transport and to whom ACP not only provides automatic reliable connectivity but also protection against attacks. Protection across all potential attack vectors is typically easier to do in devices whose software is designed from the ground up with security in mind than with legacy software based systems where the ACP is added on as another feature.

As explained above, traffic across the ACP SHOULD still be end-to-end encrypted whenever possible. This includes traffic such as GRASP, EST and BRSKI inside the ACP. This minimizes man in the middle attacks by compromised ACP group members. Such attackers cannot eavesdrop or modify communications, they can just filter them (which is unavoidable by any means).

See Appendix A.10.8 for further considerations how to avoid and deal with compromised nodes.

9.3. The Administrator View

An ACP is self-forming, self-managing and self-protecting, therefore has minimal dependencies on the administrator of the network. Specifically, since it is (intended to be) independent of configuration, there is only limited scope for configuration errors on the ACP itself. The administrator may have the option to enable or disable the entire approach, but detailed configuration is not possible. This means that the ACP must not be reflected in the running configuration of nodes, except a possible on/off switch (and even that is undesirable).
While configuration (except for Section 8 and Section 10.2) is not possible, an administrator must have full visibility of the ACP and all its parameters, to be able to do trouble-shooting. Therefore, an ACP must support all show and debug options, as for any other network function. Specifically, a network management system or controller must be able to discover the ACP, and monitor its health. This visibility of ACP operations must clearly be separated from visibility of Data-Plane so automated systems will never have to deal with ACP aspects unless they explicitly desire to do so.

Since an ACP is self-protecting, a node not supporting the ACP, or without a valid domain certificate cannot connect to it. This means that by default a traditional controller or network management system cannot connect to an ACP. See Section 8.1.1 for more details on how to connect an NMS host into the ACP.

10. ACP Operations (Informative)

The following sections document important operational aspects of the ACP. They are not normative because they do not impact the interoperability between components of the ACP, but they include recommendations/requirements for the internal operational model beneficial or necessary to achieve the desired use-case benefits of the ACP (see Section 3).

- Section 10.1 describes recommended operator diagnostics capabilities of ACP nodes. The have been derived from diagnostic of a commercially available ACP implementation.

- Section 10.2 describes high level how an ACP registrar needs to work, what its configuration parameters are and specific issues impacting the choices of deployment design due to renewal and revocation issues. It describes a model where ACP Registrars have their own sub-CA to provide the most distributed deployment option for ACP Registrars, and it describes considerations for centralized policy control of ACP Registrar operations.

- Section 10.3 describes suggested ACP node behavior and operational interfaces (configuration options) to manage the ACP in so-called greenfield devices (previously unconfigured) and brownfield devices (preconfigured).

The recommendations and suggestions of this chapter were derived from operational experience gained with a commercially available pre-standard ACP implementation.
10.1. ACP (and BRSKI) Diagnostics

Even though ACP and ANI in general are taking out many manual configuration mistakes through their automation, it is important to provide good diagnostics for them.

The basic diagnostics is support of (yang) data models representing the complete (auto-)configuration and operational state of all components: BRSKI, GRASP, ACP and the infrastructure used by them: TLS/DTLS, IPsec, certificates, trust anchors, time, VRF and so on. While necessary, this is not sufficient:

Simply representing the state of components does not allow operators to quickly take action - unless they do understand how to interpret the data, and that can mean a requirement for deep understanding of all components and how they interact in the ACP/ANI.

Diagnostic supports should help to quickly answer the questions operators are expected to ask, such as "is the ACP working correctly?", or "why is there no ACP connection to a known neighboring node?"

In current network management approaches, the logic to answer these questions is most often built as centralized diagnostics software that leverages the above mentioned data models. While this approach is feasible for components utilizing the ANI, it is not sufficient to diagnose the ANI itself:

- Developing the logic to identify common issues requires operational experience with the components of the ANI. Letting each management system define its own analysis is inefficient.
- When the ANI is not operating correctly, it may not be possible to run diagnostics from remote because of missing connectivity. The ANI should therefore have diagnostic capabilities available locally on the nodes themselves.
- Certain operations are difficult or impossible to monitor in real-time, such as initial bootstrap issues in a network location where no capabilities exist to attach local diagnostics. Therefore it is important to also define means of capturing (logging) diagnostics locally for later retrieval. Ideally, these captures are also non-volatile so that they can survive extended power-off conditions - for example when a device that fails to be brought up zero-touch is being sent back for diagnostics at a more appropriate location.
The most simple form of diagnostics answering questions such as the above is to represent the relevant information sequentially in dependency order, so that the first non-expected/non-operational item is the most likely root cause. Or just log/highlight that item. For example:

Q: Is ACP operational to accept neighbor connections:

- Check if any potentially necessary configuration to make ACP/ANI operational are correct (see Section 10.3 for a discussion of such commands).
- Does the system time look reasonable, or could it be the default system time after clock chip battery failure (certificate checks depend on reasonable notion of time).
- Does the node have keying material - domain certificate, trust anchors.
- If no keying material and ANI is supported/enabled, check the state of BRSKI (not detailed in this example).
- Check the validity of the domain certificate:
  * Does the certificate validate against the trust anchor?
  * Has it been revoked?
  * Was the last scheduled attempt to retrieve a CRL successful (e.g., do we know that our CRL information is up to date).
  * Is the certificate valid: validity start time in the past, expiration time in the future?
  * Does the certificate have a correctly formatted ACP domain information field?
- Was the ACP VRF successfully created?
- Is ACP enabled on one or more interfaces that are up and running?

If all this looks good, the ACP should be running locally "fine" - but we did not check any ACP neighbor relationships.

Question: why does the node not create a working ACP connection to a neighbor on an interface?
o Is the interface physically up? Does it have an IPv6 link-local address?

o Is it enabled for ACP?

o Do we successfully send DULL GRASP messages to the interface (link layer errors)?

o Do we receive DULL GRASP messages on the interface? If not, some intervening L2 equipment performing bad MLD snooping could have caused problems. Provide e.g., diagnostics of the MLD querier IPv6 and MAC address.

o Do we see the ACP objective in any DULL GRASP message from that interface? Diagnose the supported secure channel methods.

o Do we know the MAC address of the neighbor with the ACP objective? If not, diagnose SLAAC/ND state.

o When did we last attempt to build an ACP secure channel to the neighbor?

o If it failed, why:
  * Did the neighbor close the connection on us or did we close the connection on it because the domain certificate membership failed?
  * If the neighbor closed the connection on us, provide any error diagnostics from the secure channel protocol.
  * If we failed the attempt, display our local reason:
    + There was no common secure channel protocol supported by the two neighbors (this could not happen on nodes supporting this specification because it mandates common support for IPsec).
    + The ACP domain certificate membership check (Section 6.1.3) fails:
      - The neighbor’s certificate does not have the required trust anchor. Provide diagnostics which trust anchor it has (can identify whom the device belongs to).
      - The neighbor’s certificate does not have the same domain (or no domain at all). Diagnose domain-name and potentially other cert info.
- The neighbor’s certificate has been revoked or could not be authenticated by OCSP.
- The neighbor’s certificate has expired - or is not yet valid.

* Any other connection issues in e.g., IKEv2 / IPsec, DTLS?.

Question: Is the ACP operating correctly across its secure channels?
- Are there one or more active ACP neighbors with secure channels?
- Is the RPL routing protocol for the ACP running?
- Is there a default route to the root in the ACP routing table?
- Is there for each direct ACP neighbor not reachable over the ACP virtual interface to the root a route in the ACP routing table?
- Is ACP GRASP running?
- Is at least one SRV.est objective cached (to support certificate renewal)?
- Is there at least one BRSKI registrar objective cached (in case BRSKI is supported)
- Is BRSKI proxy operating normally on all interfaces where ACP is operating?
- ...

These lists are not necessarily complete, but illustrate the principle and show that there are variety of issues ranging from normal operational causes (a neighbor in another ACP domain) over problems in the credentials management (certificate lifetimes), explicit security actions (revocation) or unexpected connectivity issues (intervening L2 equipment).

The items so far are illustrating how the ANI operations can be diagnosed with passive observation of the operational state of its components including historic/cached/counted events. This is not necessary sufficient to provide good enough diagnostics overall:

The components of ACP and BRSKI are designed with security in mind but they do not attempt to provide diagnostics for building the network itself. Consider two examples:
1. BRSKI does not allow for a neighboring device to identify the pledges certificate (IDevID). Only the selected BRSKI registrar can do this, but it may be difficult to disseminate information about undesired pledges from those BRSKI registrars to locations/nodes where information about those pledges is desired.

2. The Link Layer Discovery Protocol (LLDP, [LLDP]) disseminates information about nodes to their immediate neighbors, such as node model/type/software and interface name/number of the connection. This information is often helpful or even necessary in network diagnostics. It can equally considered to be too insecure to make this information available unprotected to all possible neighbors.

An "interested adjacent party" can always determine the IDevID of a BRSKI pledge by behaving like a BRSKI proxy/registrar. Therefore the IDevID of a BRSKI pledge is not meant to be protected - it just has to be queried and is not signaled unsolicited (as it would be in LLDP) so that other observers on the same subnet can determine who is an "interested adjacent party".

10.2. ACP Registrars

As described in Section 6.10.7, the ACP addressing mechanism is designed to enable lightweight, distributed and uncoordinated ACP registrars that are providing ACP address prefixes to candidate ACP nodes by enrolling them with an ACP domain certificate into an ACP domain via any appropriate mechanism/protocol, automated or not.

This section discusses informatively more details and options for ACP registrars.

10.2.1. Registrar interactions

This section summarizes and discusses the interactions with other entities required by an ACP registrar.

In a simple instance of an ACP network, no central NOC component beside a trust anchor (root CA) is required. One or more uncoordinated acting ACP registrar can be set up, performing the following interactions:

To orchestrate enrolling a candidate ACP node autonomically, the ACP registrar can rely on the ACP and use Proxies to reach the candidate ACP node, therefore allowing minimum pre-existing (auto-)configured network services on the candidate ACP node. BRSKI defines the BRSKI proxy, a design that can be adopted for various protocols that
Pledges/candidate ACP nodes could want to use, for example BRSKI over CoAP (Constrained Application Protocol), or proxying of Netconf.

To reach a trust anchor unaware of the ACP, the ACP registrar would use the Data-Plane. ACP and Data-Plane in an ACP registrar could (and by default should be) completely isolated from each other at the network level. Only applications such as the ACP registrar would need the ability for their transport stacks to access both.

In non-autonomic enrollment options, the Data-Plane between a ACP registrar and the candidate ACP node needs to be configured first. This includes the ACP registrar and the candidate ACP node. Then any appropriate set of protocols can be used between ACP registrar and candidate ACP node to discover the other side, and then connect and enroll (configure) the candidate ACP node with an ACP domain certificate. Netconf ZeroTouch ([I-D.ietf-netconf-zerotouch]) is an example protocol that could be used for this. BRSKI using optional discovery mechanisms is equally a possibility for candidate ACP nodes attempting to be enrolled across non-ACP networks, such as the Internet.

When candidate ACP nodes have secure bootstrap, such as BRSKI Pledges, they will not trust to be configured/enrolled across the network, unless being presented with a voucher (see [RFC8366]) authorizing the network to take possession of the node. An ACP registrar will then need a method to retrieve such a voucher, either offline, or online from a MASA (Manufacturer Authorized Signing Authority). BRSKI and Netconf ZeroTouch are two protocols that include capabilities to present the voucher to the candidate ACP node.

An ACP registrar could operate EST for ACP certificate renewal and/or act as a CRL Distribution point. A node performing these services does not need to support performing (initial) enrollment, but it does require the same above described connectivity as an ACP registrar: via the ACP to ACP nodes and via the Data-Plane to the trust anchor and other sources of CRL information.

10.2.2. Registrar Parameter

The interactions of an ACP registrar outlined Section 6.10.7 and Section 10.2.1 above depend on the following parameters:

- A URL to the trust anchor (root CA) and credentials so that the ACP registrar can let the trust anchor sign candidate ACP member certificates.

- The ACP domain-name.
The Registrar-ID to use. This could default to a MAC address of the ACP registrar.

For recovery, the next-useable Node-IDs for zone (Zone-ID=0) sub-addressing scheme, for Vlong /112 and for Vlong /1120 sub-addressing scheme. These IDs would only need to be provisioned after recovering from a crash. Some other mechanism would be required to remember these IDs in a backup location or to recover them from the set of currently known ACP nodes.

Policies if candidate ACP nodes should receive a domain certificate or not, for example based on the devices IDevID as in BRSKI. The ACP registrar may have a whitelist or blacklist of devices "serialNumbers" from their IDevID.

Policies what type of address prefix to assign to a candidate ACP devices, based on likely the same information.

For BRSKI or other mechanisms using vouchers: Parameters to determine how to retrieve vouchers for specific type of secure bootstrap candidate ACP nodes (such as MASA URLs), unless this information is automatically learned such as from the IDevID of candidate ACP nodes (as defined in BRSKI).

10.2.3. Certificate renewal and limitations

When an ACP node renews/rekeys its certificate, it may end up doing so via a different registrar (e.g., EST server) than the one it originally received its ACP domain certificate from, for example because that original ACP registrar is gone. The ACP registrar through which the renewal/rekeying is performed would by default trust the ACP domain information from the ACP nodes current ACP domain certificate and maintain this information so that the ACP node maintains its ACP address prefix. In EST renewal/rekeying, the ACP nodes current ACP domain certificate is signaled during the TLS handshake.

This simple scenario has two limitations:

1. The ACP registrars cannot directly assign certificates to nodes and therefore needs an "online" connection to the trust anchor (root CA).

2. Recovery from a compromised ACP registrar is difficult. When an ACP registrar is compromised, it can insert for example conflicting ACP domain information and create thereby an attack against other ACP nodes through the ACP routing protocol.
Even when such a malicious ACP registrar is detected, resolving the problem may be difficult because it would require identifying all the wrong ACP domain certificates assigned via the ACP registrar after it was compromised. And without additional centralized tracking of assigned certificates there is no way to do this.

10.2.4. ACP Registrars with sub-CA

In situations, where either of the above two limitations are an issue, ACP registrars could also be sub-CAs. This removes the need for connectivity to a root-CA whenever an ACP node is enrolled, and reduces the need for connectivity of such an ACP registrar to a root-CA to only those times when it needs to renew its own certificate. The ACP registrar would also now use its own (sub-CA) certificate to enroll and sign the ACP nodes certificates, and therefore it is only necessary to revoke a compromised ACP registrars sub-CA certificate. Alternatively one can let it expire and not renew it, when the certificate of the sub-CA is appropriately short-lived.

As the ACP domain membership check verifies a peer ACP node’s ACP domain certificate trust chain, it will also verify the signing certificate which is the compromised/revoked sub-CA certificate. Therefore ACP domain membership for an ACP node enrolled from a compromised and discovered ACP registrar will fail.

ACP nodes enrolled by a compromised ACP registrar would automatically fail to establish ACP channels and ACP domain certificate renewal via EST and therefore revert to their role as a candidate ACP members and attempt to get a new ACP domain certificate from an ACP registrar – for example, via BRSKI. In result, ACP registrars that have an associated sub-CA makes isolating and resolving issues with compromised registrars easier.

Note that ACP registrars with sub-CA functionality also can control the lifetime of ACP domain certificates easier and therefore also be used as a tool to introduce short lived certificates and not rely on CRL, whereas the certificates for the sub-CAs themselves could be longer lived and subject to CRL.

10.2.5. Centralized Policy Control

When using multiple, uncoordinated ACP registrars, several advanced operations are potentially more complex than with a single, resilient policy control backend, for example including but not limited to:

Which candidate ACP node is permitted or not permitted into an ACP domain. This may not be a decision to be taken upfront, so that a per-"serialNumber" policy can be loaded into every ACP registrar.
Instead, it may better be decided in real-time including potentially a human decision in a NOC.

Tracking of all enrolled ACP nodes and their certificate information. For example in support of revoking individual ACP nodes certificates.

More flexible policies what type of address prefix or even what specific address prefix to assign to a candidate ACP node.

These and other operations could be introduced more easily by introducing a centralized Policy Management System (PMS) and modifying ACP registrar behavior so that it queries the PMS for any policy decision occurring during the candidate ACP node enrollment process and/or the ACP node certificate renewal process. For example, which ACP address prefix to assign. Likewise the ACP registrar would report any relevant state change information to the PMS as well, for example when a certificate was successfully enrolled onto a candidate ACP node.

10.3. Enabling and disabling ACP/ANI

Both ACP and BRSKI require interfaces to be operational enough to support sending/receiving their packets. In node types where interfaces are by default (e.g., without operator configuration) enabled, such as most L2 switches, this would be less of a change in behavior than in most L3 devices (e.g.: routers), where interfaces are by default disabled. In almost all network devices it is common though for configuration to change interfaces to a physically disabled state and that would break the ACP.

In this section, we discuss a suggested operational model to enable/disable interfaces and nodes for ACP/ANI in a way that minimizes the risk of operator action to break the ACP in this way, and that also minimizes operator surprise when ACP/ANI becomes supported in node software.

10.3.1. Filtering for non-ACP/ANI packets

Whenever this document refers to enabling an interface for ACP (or BRSKI), it only requires to permit the interface to send/receive packets necessary to operate ACP (or BRSKI) - but not any other Data-Plane packets. Unless the Data-Plane is explicitly configured/enabled, all packets not required for ACP/BRSKI should be filtered on input and output:

Both BRSKI and ACP require link-local only IPv6 operations on interfaces and DULL GRASP. IPv6 link-local operations means the
minimum signaling to auto-assign an IPv6 link-local address and talk to neighbors via their link-local address: SLAAC (Stateless Address Auto-Configuration - [RFC4862]) and ND (Neighbor Discovery - [RFC4861]). When the device is a BRSKI pledge, it may also require TCP/TLS connections to BRSKI proxies on the interface. When the device has keying material, and the ACP is running, it requires DULL GRASP packets and packets necessary for the secure-channel mechanism it supports, e.g., IKEv2 and IPsec ESP packets or DTLS packets to the IPv6 link-local address of an ACP neighbor on the interface. It also requires TCP/TLS packets for its BRSKI proxy functionality, if it does support BRSKI.

10.3.2. Admin Down State

Interfaces on most network equipment have at least two states: "up" and "down". These may have product specific names. "down" for example could be called "shutdown" and "up" could be called "no shutdown". The "down" state disables all interface operations down to the physical level. The "up" state enables the interface enough for all possible L2/L3 services to operate on top of it and it may also auto-enable some subset of them. More commonly, the operations of various L2/L3 services is controlled via additional node-wide or interface level options, but they all become only active when the interface is not "down". Therefore an easy way to ensure that all L2/L3 operations on an interface are inactive is to put the interface into "down" state. The fact that this also physically shuts down the interface is in many cases just a side effect, but it may be important in other cases (see below, Section 10.3.2.2).

To provide ACP/ANI resilience against operators configuring interfaces to "down" state, this document recommends to separate the "down" state of interfaces into an "admin down" state where the physical layer is kept running and ACP/ANI can use the interface and a "physical down" state. Any existing "down" configurations would map to "admin down". In "admin down", any existing L2/L3 services of the Data-Plane should see no difference to "physical down" state. To ensure that no Data-Plane packets could be sent/received, packet filtering could be established automatically as described above in Section 10.3.1.

As necessary (see discussion below) new configuration options could be introduced to issue "physical down". The options should be provided with additional checks to minimize the risk of issuing them in a way that breaks the ACP without automatic restoration. For example they could be denied to be issued from a control connection (netconf/ssh) that goes across the interface itself ("do not disconnect yourself"). Or they could be performed only temporary and only be made permanent with additional later reconfirmation.
In the following sub-sections important aspects to the introduction of "admin down" state are discussed.

10.3.2.1. Security

Interfaces are physically brought down (or left in default down state) as a form of security. "Admin down" state as described above provides also a high level of security because it only permits ACP/ANI operations which are both well secured. Ultimately, it is subject to security review for the deployment whether "admin down" is a feasible replacement for "physical down".

The need to trust the security of ACP/ANI operations needs to be weighed against the operational benefits of permitting this: Consider the typical example of a CPE (customer premises equipment) with no on-site network expert. User ports are in physical down state unless explicitly configured not to be. In a misconfiguration situation, the uplink connection is incorrectly plugged into such as user port. The device is disconnected from the network and therefore no diagnostics from the network side is possible anymore. Alternatively, all ports default to "admin down". The ACP (but not the Data-Plane) would still automatically form. Diagnostics from the network side is possible and operator reaction could include to either make this port the operational uplink port or to instruct re-cabling. Security wise, only ACP/ANI could be attacked, all other functions are filtered on interfaces in "admin down" state.

10.3.2.2. Fast state propagation and Diagnostics

"Physical down" state propagates on many interface types (e.g., Ethernet) to the other side. This can trigger fast L2/L3 protocol reaction on the other side and "admin down" would not have the same (fast) result.

Bringing interfaces to "physical down" state is to the best of our knowledge always a result of operator action, but today, never the result of (autonomic) L2/L3 services running on the nodes. Therefore one option is to change the operator action to not rely on link-state propagation anymore. This may not be possible when both sides are under different operator control, but in that case it is unlikely that the ACP is running across the link and actually putting the interface into "physical down" state may still be a good option.

Ideally, fast physical state propagation is replaced by fast software driven state propagation. For example a DULL GRASP "admin-state" objective could be used to auto configure a Bidirectional Forwarding Protocol (BFD, [RFC5880]) session between the two sides of the link that would be used to propagate the "up" vs. admin down state.
Triggering physical down state may also be used as a mean of diagnosing cabling in the absence of easier methods. It is more complex than automated neighbor diagnostics because it requires coordinated remote access to both (likely) sides of a link to determine whether up/down toggling will cause the same reaction on the remote side.

See Section 10.1 for a discussion about how LLDP and/or diagnostics via GRASP could be used to provide neighbor diagnostics, and therefore hopefully eliminating the need for "physical down" for neighbor diagnostics - as long as both neighbors support ACP/ANI.

10.3.2.3. Low Level Link Diagnostics

"Physical down" is performed to diagnose low-level interface behavior when higher layer services (e.g., IPv6) are not working. Especially Ethernet links are subject to a wide variety of possible wrong configuration/cablings if they do not support automatic selection of variable parameters such as speed (10/100/1000 Mbps), crossover (Auto-MDIX) and connector (fiber, copper - when interfaces have multiple but can only enable one at a time). The need for low level link diagnostic can therefore be minimized by using fully auto configuring links.

In addition to "Physical down", low level diagnostics of Ethernet or other interfaces also involve the creation of other states on interfaces, such as physical Loopback (internal and/or external) or bringing down all packet transmissions for reflection/cable-length measurements. Any of these options would disrupt ACP as well.

In cases where such low-level diagnostics of an operational link is desired but where the link could be a single point of failure for the ACP, ASA on both nodes of the link could perform a negotiated diagnostics that automatically terminates in a predetermined manner without dependence on external input ensuring the link will become operational again.

10.3.2.4. Power Consumption Issues

Power consumption of "physical down" interfaces, may be significantly lower than those in "admin down" state, for example on long-range fiber interfaces. Bringing up interfaces, for example to probe reachability, may also consume additional power. This can make these type of interfaces inappropriate to operate purely for the ACP when they are not currently needed for the Data-Plane.
10.3.3. Interface level ACP/ANI enable

The interface level configuration option "ACP enable" enables ACP operations on an interface, starting with ACP neighbor discovery via DULL GRAP. The interface level configuration option "ANI enable" on nodes supporting BRSKI and ACP starts with BRSKI pledge operations when there is no domain certificate on the node. On ACP/BRSKI nodes, "ACP enable" may not need to be supported, but only "ANI enable". Unless overridden by global configuration options (see later), "ACP/ANI enable" will result in "down" state on an interface to behave as "admin down".

10.3.4. Which interfaces to auto-enable?

(Section 6.3) requires that "ACP enable" is automatically set on native interfaces, but not on non-native interfaces (reminder: a native interface is one that exists without operator configuration action such as physical interfaces in physical devices).

Ideally, ACP enable is set automatically on all interfaces that provide access to additional connectivity that allows to reach more nodes of the ACP domain. The best set of interfaces necessary to achieve this is not possible to determine automatically. Native interfaces are the best automatic approximation.

Consider an ACP domain of ACP nodes transitively connected via native interfaces. A Data-Plane tunnel between two of these nodes that are non-adjacent is created and "ACP enable" is set for that tunnel. ACP RPL sees this tunnel as just as a single hop. Routes in the ACP would use this hop as an attractive path element to connect regions adjacent to the tunnel nodes. In result, the actual hop-by-hop paths used by traffic in the ACP can become worse. In addition, correct forwarding in the ACP now depends on correct Data-Plane forwarding config including QoS, filtering and other security on the Data-Plane path across which this tunnel runs. This is the main issue why "ACP/ANI enable" should not be set automatically on non-native interfaces.

If the tunnel would connect two previously disjoint ACP regions, then it likely would be useful for the ACP. A Data-Plane tunnel could also run across nodes without ACP and provide additional connectivity for an already connected ACP network. The benefit of this additional ACP redundancy has to be weighed against the problems of relying on the Data-Plane. If a tunnel connects two separate ACP regions: how many tunnels should be created to connect these ACP regions reliably enough? Between which nodes? These are all standard tunneled network design questions not specific to the ACP, and there are no generic fully automated answers.
Instead of automatically setting "ACP enable" on these type of interfaces, the decision needs to be based on the use purpose of the non-native interface and "ACP enable" needs to be set in conjunction with the mechanism through which the non-native interface is created/configured.

In addition to explicit setting of "ACP/ANI enable", non-native interfaces also need to support configuration of the ACP RPL cost of the link - to avoid the problems of attracting too much traffic to the link as described above.

Even native interfaces may not be able to automatically perform BRSKI or ACP because they may require additional operator input to become operational. Example include DSL interfaces requiring PPPoE credentials or mobile interfaces requiring credentials from a SIM card. Whatever mechanism is used to provide the necessary config to the device to enable the interface can also be expanded to decide on whether or not to set "ACP/ANI enable".

The goal of automatically setting "ACP/ANI enable" on interfaces (native or not) is to eliminate unnecessary "touches" to the node to make its operation as much as possible "zero-touch" with respect to ACP/ANI. If there are "unavoidable touches" such a creating/configuring a non-native interface or provisioning credentials for a native interface, then "ACP/ANI enable" should be added as an option to that "touch". If a wrong "touch" is easily fixed (not creating another high-cost touch), then the default should be not to enable ANI/ACP, and if it is potentially expensive or slow to fix (e.g., parameters on SIM card shipped to remote location), then the default should be to enable ACP/ANI.

10.3.5. Node Level ACP/ANI enable

A node level command "ACP/ANI enable [up-if-only]" enables ACP or ANI on the node (ANI = ACP + BRSKI). Without this command set, any interface level "ACP/ANI enable" is ignored. Once set, ACP/ANI will operate an interface where "ACP/ANI enable" is set. Setting of interface level "ACP/ANI enable" is either automatic (default) or explicit through operator action as described in the previous section.

If the option "up-if-only" is selected, the behavior of "down" interfaces is unchanged, and ACP/ANI will only operate on interfaces where "ACP/ANI enable" is set and that are "up". When it is not set, then "down" state of interfaces with "ACP/ANI enable" is modified to behave as "admin down".
10.3.5.1. Brownfield nodes

A "brownfield" node is one that already has a configured Data-Plane. Executing global "ACP/ANI enable [up-if-only]" on each node is the only command necessary to create an ACP across a network of brownfield nodes once all the nodes have a domain certificate. When BRSKI is used ("ANI enable"), provisioning of the certificates only requires set-up of a single BRSKI registrar node which could also implement a CA for the network. This is the most simple way to introduce ACP/ANI into existing (== brownfield) networks.

The need to explicitly enable ACP/ANI is especially important in brownfield nodes because otherwise software updates may introduce support for ACP/ANI: Automatic enablement of ACP/ANI in networks where the operator does not only not want ACP/ANI but where the operator likely never even heard of it could be quite irritating to the operator. Especially when "down" behavior is changed to "admin down".

Automatically setting "ANI enable" on brownfield nodes where the operator is unaware of BRSKI and MASA operations could also be an unlikely but then critical security issue. If an attacker could impersonate the operator and register as the operator at the MASA or otherwise get hold of vouchers and can get enough physical access to the network so pledges would register to an attacking registrar, then the attacker could gain access to the network through the ACP that the attacker then has access to.

In networks where the operator explicitly wants to enable the ANI this could not happen, because the operator would create a BRSKI registrar that would discover attack attempts, and the operator would be setting up his registrar with the MASA. Nodes requiring "ownership vouchers" would not be subject to that attack. See [I-D.ietf-anima-bootstrapping-keyinfra] for more details. Note that a global "ACP enable" alone is not subject to these type of attacks, because it always depends on some other mechanism first to provision domain certificates into the device.

10.3.5.2. Greenfield nodes

A "greenfield" node is one that did not have any prior configuration.

For greenfield nodes, only "ANI enable" is relevant. If another mechanism than BRSKI is used to (zero-touch) bootstrap a node, then it is up to that mechanism to provision domain certificates and to set global "ACP enable" as desired.
Nodes supporting full ANI functionality set "ANI enable" automatically when they decide that they are greenfield, e.g., that they are powering on from factory condition. They will then put all native interfaces into "admin down" state and start to perform BRSKI pledge functionality - and once a domain certificate is enrolled they automatically enable ACP.

Attempts for BRSKI pledge operations in greenfield state should terminate automatically when another method of configuring the node is used. Methods that indicate some form of physical possession of the device such as configuration via the serial console port could lead to immediate termination of BRSKI, while other parallel auto configuration methods subject to remote attacks might lead to BRSKI termination only after they were successful. Details of this may vary widely over different type of nodes. When BRSKI pledge operation terminates, this will automatically unset "ANI enable" and should terminate any temporarily needed state on the device to perform BRSKI - DULL GRASP, BRSKI pledge and any IPv6 configuration on interfaces.

10.3.6. Undoing ANI/ACP enable

Disabling ANI/ACP by undoing "ACP/ANI enable" is a risk for the reliable operations of the ACP if it can be executed by mistake or unauthorized. This behavior could be influenced through some additional (future) property in the certificate (e.g., in the domain information extension field): In an ANI deployment intended for convenience, disabling it could be allowed without further constraints. In an ANI deployment considered to be critical more checks would be required. One very controlled option would be to not permit these commands unless the domain certificate has been revoked or is denied renewal. Configuring this option would be a parameter on the BRSKI registrar(s). As long as the node did not receive a domain certificate, undoing "ANI/ACP enable" should not have any additional constraints.

10.3.7. Summary

Node-wide "ACP/ANI enable [up-if-only]" commands enable the operation of ACP/ANI. This is only auto-enabled on ANI greenfield devices, otherwise it must be configured explicitly.

If the option "up-if-only" is not selected, interfaces enabled for ACP/ANI interpret "down" state as "admin down" and not "physical down". In "admin-down" all non-ACP/ANI packets are filtered, but the physical layer is kept running to permit ACP/ANI to operate.
(New) commands that result in physical interruption ("physical down", "loopback") of ACP/ANI enabled interfaces should be built to protect continuance or reestablishment of ACP as much as possible.

Interface level "ACP/ANI enable" control per-interface operations. It is enabled by default on native interfaces and has to be configured explicitly on other interfaces.

Disabling "ACP/ANI enable" global and per-interface should have additional checks to minimize undesired breakage of ACP. The degree of control could be a domain wide parameter in the domain certificates.

10.4. Configuration and the ACP (summary)

There is no desirable configuration for the ACP. Instead, all parameters that need to be configured in support of the ACP are limitations of the solution, but they are only needed in cases where not all components are made autonomic. Wherever this is necessary, it relies on pre-existing mechanisms for configuration such as CLI or YANG ([RFC7950]) data models.

The most important examples of such configuration include:

- When ACP nodes do not support an autonomic way to receive an ACP domain certificate, for example BRSKI, then such certificate needs to be configured via some pre-existing mechanisms outside the scope of this specification. Today, router have typically a variety of mechanisms to do this.

- Certificate maintenance requires PKI functions. Discovery of these functions across the ACP is automated (see Section 6.1.5), but their configuration is not.

- When non-ACP capable nodes such as pre-existing NMS need to be physically connected to the ACP, the ACP node to which they attach needs to be configured with ACP-connect according to Section 8.1. It is also possible to use that single physical connection to connect both to ACP and the data-plane of the network as explained in Section 8.1.4.

- When devices are not autonomically bootstrapped, explicit configuration to enable the ACP needs to be applied. See Section 10.3.

- When the ACP needs to be extended across interfaces other than L2, the ACP as defined in this document can not autodiscover...
candidate neighbors automatically. Remote neighbors need to be configured, see Section 8.2.

Once the ACP is operating, any further configuration for the data-plane can be configured more reliably across the ACP itself because the ACP provides addressing and connectivity (routing) independent of the data-plane itself. For this, the configuration methods simply need to also allow to operate across the ACP VRF - netconf, ssh or any other method.

The ACP also provides additional security through its hop-by-hop encryption for any such configuration operations: Some legacy configuration methods (SNMP, TFTP, HTTP) may not use end-to-end encryption, and most of the end-to-end secured configuration methods still allow for easy passive observation along the path about configuration taking place (transport flows, port numbers, IP addresses).

The ACP can and should equally be used as the transport to configure any of the aforementioned non-autonomic components of the ACP, but in that case, the same caution needs to be exercised as with data-plane configuration without ACP: Misconfiguration may cause the configuring entity to be disconnected from the node it configures - for example when incorrectly unconfiguring a remote ACP neighbor through which the configured ACP node is reached.

11. Security Considerations

After seeding an ACP by configuring at least one ACP registrar with routing-subdomain and a CA, an ACP is self-protecting and there is no need to apply configuration to make it secure (typically the ACP Registrar doubles as EST server for certificate renewal). Its security therefore does not depend on configuration. This does not include workarounds for non-autonomic components as explained in Section 8. See Section 9.2 for details of how the ACP protects itself against attacks from the outside and to a more limited degree from the inside as well.

However, the security of the ACP depends on a number of other factors:

- The usage of domain certificates depends on a valid supporting PKI infrastructure. If the chain of trust of this PKI infrastructure is compromised, the security of the ACP is also compromised. This is typically under the control of the network administrator.

- Every ACP registrar is critical infrastructure that needs to be hardened against attacks, similar to a CA. A malicious registrar
can enroll enemy pledges to an ACP network or break ACP routing by
duplicate ACP address assignment to pledges via their ACP domain
certificates.

- Security can be compromised by implementation errors (bugs), as in
certain products.

There is no prevention of source-address spoofing inside the ACP.
This implies that if an attacker gains access to the ACP, it can
spoof all addresses inside the ACP and fake messages from any other
node.

The ACP is designed to enable automation of current network
management and future autonomic peer-to-peer/distributed network
automation. Any ACP member can send ACP IPv6 packet to other ACP
members and announce via ACP GRASP services to all ACP members
without dependency against centralized components.

The ACP relies on peer-to-peer authentication and authorization using
ACP certificates. This security model is necessary to enable the
autonomic ad-hoc any-to-any connectivity between ACP nodes. It
provides infrastructure protection through hop by hop authentication
and encryption - without relying on third parties. For any services
where this complete autonomic peer-to-peer group security model is
appropriate, the ACP domain certificate can also be used unchanged.
For example for any type of data-plane routing protocol security.

This ACP security model is designed primarily to protect against
attack from the outside, but not against attacks from the inside. To
protect against spoofing attacks from compromised on-path ACP nodes,
end-to-end encryption inside the ACP is used by new ACP signaling:
GRASP across the ACP using TLS. The same is expected from any non-
legacy services/protocols using the ACP. Because no group-keys are
used, there is no risk for impacted nodes to access end-to-end
encrypted traffic from other ACP nodes.

Attacks from impacted ACP nodes against the ACP are more difficult
than against the data-plane because of the autoconfiguration of the
ACP and the absence of configuration options that could be abused
that allow to change/break ACP behavior. This is excluding
configuration for workaround in support of non-autonomic components.

Mitigation against compromised ACP members is possible through
standard automated certificate management mechanisms including
revocation and non-renewal of short-lived certificates. In this
version of the specification, there are no further optimization of
these mechanisms defined for the ACP (but see Appendix A.10.8).
Higher layer service built using ACP domain certificates should not solely rely on undifferentiated group security when another model is more appropriate/more secure. For example central network configuration relies on a security model where only few especially trusted nodes are allowed to configure the data-plane of network nodes (CLIL, Netconf). This can be done through ACP domain certificates by differentiating them and introduce roles. See Appendix A.10.5.

Fundamentally, security depends on avoiding operator and network operations automation mistakes, implementation and architecture. Autonomic approaches such as the ACP largely eliminate operator mistakes and make it easier to recover from network operations mistakes. Implementation and architectural mistakes are still possible, as in all networking technologies.

Many details of ACP are designed with security in mind and discussed elsewhere in the document:

IPv6 addresses used by nodes in the ACP are covered as part of the node's domain certificate as described in Section 6.1.2. This allows even verification of ownership of a peer’s IPv6 address when using a connection authenticated with the domain certificate.

The ACP acts as a security (and transport) substrate for GRASP inside the ACP such that GRASP is not only protected by attacks from the outside, but also by attacks from compromised inside attackers - by relying not only on hop-by-hop security of ACP secure channels, but adding end-to-end security for those GRASP messages. See Section 6.8.2.

ACP provides for secure, resilient zero-touch discovery of EST servers for certificate renewal. See Section 6.1.5.

ACP provides extensible, auto-configuring hop-by-hop protection of the ACP infrastructure via the negotiation of hop-by-hop secure channel protocols. See Section 6.5.

The ACP is designed to minimize attacks from the outside by minimizing its dependency against any non-ACP (Data-Plane) operations/configuration on a node. See also Section 6.12.2.

In combination with BRSKI, ACP enables a resilient, fully zero-touch network solution for short-lived certificates that can be renewed or re-enrolled even after unintentional expiry (e.g., because of interrupted connectivity). See Appendix A.2.
Because ACP secure channels can be long lived, but certificates used may be short lived, secure channels, for example built via IPsec need to be terminated when peer certificates expire. See Section 6.7.3.

The ACP is designed to minimize attacks from the outside by minimizing its dependency against any non-ACP (Data-Plane) operations/configuration on a node. See also Section 6.12.2.

12. IANA Considerations

This document defines the "Autonomic Control Plane".

The IANA is requested to register the value "AN_ACP" (without quotes) to the GRASP Objectives Names Table in the GRASP Parameter Registry. The specification for this value is this document, Section 6.3.

The IANA is requested to register the value "SRV.est" (without quotes) to the GRASP Objectives Names Table in the GRASP Parameter Registry. The specification for this value is this document, Section 6.1.5.

Explanation: This document chooses the initially strange looking format "SRV.<service-name>" because these objective names would be in line with potential future simplification of the GRASP objective registry. Today, every name in the GRASP objective registry needs to be explicitly allocated with IANA. In the future, this type of objective names could considered to be automatically registered in that registry for the same service for which <service-name> is registered according to [RFC6335]. This explanation is solely informational and has no impact on the requested registration.

The IANA is requested to create an ACP Parameter Registry with currently one registry table - the "ACP Address Type" table.

"ACP Address Type" Table. The value in this table are numeric values 0...3 paired with a name (string). Future values MUST be assigned using the Standards Action policy defined by [RFC8126]. The following initial values are assigned by this document:

0: ACP Zone Addressing Sub-Scheme (ACP RFC Figure 11) / ACP Manual Addressing Sub-Scheme (ACP RFC Section 6.10.4)
1: ACP Vlong Addressing Sub-Scheme (ACP RFC Section 6.10.5)

13. Acknowledgements

This work originated from an Autonomic Networking project at Cisco Systems, which started in early 2010. Many people contributed to this project and the idea of the Autonomic Control Plane, amongst
which (in alphabetical order): Ignas Bagdonas, Parag Bhide, Balaji BL, Alex Clemm, Yves Hertoghs, Bruno Klauser, Max Pritikin, Michael Richardson, Ravi Kumar Vadapalli.

Special thanks to Brian Carpenter, Elwyn Davies, Joel Halpern and Sheng Jiang for their thorough reviews and to Pascal Thubert and Michael Richardson to provide the details for the recommendations of the use of RPL in the ACP.

Further input, review or suggestions were received from: Rene Struik, Brian Carpenter, Benoit Claise, William Atwood and Yongkang Zhang.

14. Change log [RFC Editor: Please remove]

14.1. Initial version

First version of this document: draft-behringer-autonomic-control-plane

14.2. draft-behringer-anima-autonomic-control-plane-00

Initial version of the anima document; only minor edits.

14.3. draft-behringer-anima-autonomic-control-plane-01

- Clarified that the ACP should be based on, and support only IPv6.
- Clarified in intro that ACP is for both, between devices, as well as for access from a central entity, such as an NMS.
- Added a section on how to connect an NMS system.
- Clarified the hop-by-hop crypto nature of the ACP.
- Added several references to GDNP as a candidate protocol.
- Added a discussion on network split and merge. Although, this should probably go into the certificate management story longer term.

14.4. draft-behringer-anima-autonomic-control-plane-02

Addresses (numerous) comments from Brian Carpenter. See mailing list for details. The most important changes are:

- Introduced a new section "overview", to ease the understanding of the approach.
Merged the previous "problem statement" and "use case" sections into a mostly re-written "use cases" section, since they were overlapping.

Clarified the relationship with draft-ietf-anima-stable-connectivity

14.5. draft-behringer-anima-autonomic-control-plane-03

Took out requirement for IPv6 --> that’s in the reference doc.

Added requirement section.

Changed focus: more focus on autonomic functions, not only virtual out-of-band. This goes a bit throughout the document, starting with a changed abstract and intro.

14.6. draft-ietf-anima-autonomic-control-plane-00

No changes; re-submitted as WG document.

14.7. draft-ietf-anima-autonomic-control-plane-01

Added some paragraphs in addressing section on "why IPv6 only", to reflect the discussion on the list.

Moved the Data-Plane ACP out of the main document, into an appendix. The focus is now the virtually separated ACP, since it has significant advantages, and isn’t much harder to do.

Changed the self-creation algorithm: Part of the initial steps go into the reference document. This document now assumes an adjacency table, and domain certificate. How those get onto the device is outside scope for this document.

Created a new section 6 "workarounds for non-autonomic nodes", and put the previous controller section (5.9) into this new section. Now, section 5 is "autonomic only", and section 6 explains what to do with non-autonomic stuff. Much cleaner now.

Added an appendix explaining the choice of RPL as a routing protocol.

Formalized the creation process a bit more. Now, we create a "candidate peer list" from the adjacency table, and form the ACP with those candidates. Also it explains now better that policy (Intent) can influence the peer selection. (section 4 and 5)
o Introduce a section for the capability negotiation protocol (section 7). This needs to be worked out in more detail. This will likely be based on GRASP.

o Introduce a new parameter: ACP tunnel type. And defines it in the IANA considerations section. Suggest GRE protected with IPSec transport mode as the default tunnel type.

o Updated links, lots of small edits.

14.8. draft-ietf-anima-autonomic-control-plane-02

o Added explicitly text for the ACP channel negotiation.

o Merged draft-behringer-anima-autonomic-addressing-02 into this document, as suggested by WG chairs.

14.9. draft-ietf-anima-autonomic-control-plane-03

o Changed Neighbor discovery protocol from GRASP to mDNS. Bootstrap protocol team decided to go with mDNS to discover bootstrap proxy, and ACP should be consistent with this. Reasons to go with mDNS in bootstrap were a) Bootstrap should be reuseable also outside of full anima solutions and introduce as few as possible new elements. mDNS was considered well-known and very-likely even pre-existing in low-end devices (IoT). b) Using GRASP both for the insecure neighbor discovery and secure ACP operations raises the risk of introducing security issues through implementation issues/non-isolation between those two instances of GRASP.

o Shortened the section on GRASP instances, because with mDNS being used for discovery, there is no insecure GRASP session any longer, simplifying the GRASP considerations.

o Added certificate requirements for ANIMA in section 5.1.1, specifically how the ANIMA information is encoded in subjectAltName.

o Deleted the appendix on "ACP without separation", as originally planned, and the paragraph in the main text referring to it.

o Deleted one sub-addressing scheme, focusing on a single scheme now.

o Included information on how ANIMA information must be encoded in the domain certificate in section "preconditions".

o Editorial changes, updated draft references, etc.
14.10. draft-ietf-anima-autonomic-control-plane-04

Changed discovery of ACP neighbor back from mDNS to GRASP after revisiting the L2 problem. Described problem in discovery section itself to justify. Added text to explain how ACP discovery relates to BRSKY (bootstrap) discovery and pointed to Michael Richardson's draft detailing it. Removed appendix section that contained the original explanations why GRASP would be useful (current text is meant to be better).

14.11. draft-ietf-anima-autonomic-control-plane-05

- Section 5.3 (candidate ACP neighbor selection): Add that Intent can override only AFTER an initial default ACP establishment.
- Section 6.10.1 (addressing): State that addresses in the ACP are permanent, and do not support temporary addresses as defined in RFC4941.
- Modified Section 6.3 to point to the GRASP objective defined in draft-carpenter-anima-ani-objectives. (and added that reference)
- Section 6.10.2: changed from MD5 for calculating the first 40-bits to SHA256; reason is MD5 should not be used any more.
- Added address sub-scheme to the IANA section.
- Made the routing section more prescriptive.
- Clarified in Section 8.1.1 the ACP Connect port, and defined that term "ACP Connect".
- Section 8.2: Added some thoughts (from mcr) on how traversing a L3 cloud could be automated.
- Added a CRL check in Section 6.7.
- Added a note on the possibility of source-address spoofing into the security considerations section.
- Other editorial changes, including those proposed by Michael Richardson on 30 Nov 2016 (see ANIMA list).

14.12. draft-ietf-anima-autonomic-control-plane-06

- Added proposed RPL profile.
detailed DTLS profile - DTLS with any additional negotiation/signaling channel.

Fixed up text for ACP/GRE encap. Removed text claiming its incompatible with non-GRE IPsec and detailed it.

Added text to suggest admin down interfaces should still run ACP.

14.13. draft-ietf-anima-autonomic-control-plane-07

Changed author association.

Improved ACP connect section (after confusion about term came up in the stable connectivity draft review). Added picture, defined complete terminology.

Moved ACP channel negotiation from normative section to appendix because it can in the timeline of this document not be fully specified to be implementable. Aka: work for future document. That work would also need to include analysing IKEv2 and desribing the difference of a proposed GRASP/TLS solution to it.

Removed IANA request to allocate registry for GRASP/TLS. This would come with future draft (see above).

Gave the name "ACP domain information field" to the field in the certificate carrying the ACP address and domain name.

Changed the rules for mutual authentication of certificates to rely on the domain in the ACP information field of the certificate instead of the OU in the certificate. Also renewed the text pointing out that the ACP information field in the certificate is meant to be in a form that it does not disturb other uses of the certificate. As long as the ACP expected to rely on a common OU across all certificates in a domain, this was not really true: Other uses of the certificates might require different OUs for different areas/type of devices. With the rules in this draft version, the ACP authentication does not rely on any other fields in the certificate.

Added an extension field to the ACP information field so that in the future additional fields like a subdomain could be inserted. An example using such a subdomain field was added to the pre-existing text suggesting sub-domains. This approach is necessary so that there can be a single (main) domain in the ACP information field, because that is used for mutual authentication of the certificate. Also clarified that only the register(s) SHOULD/MUST
use that the ACP address was generated from the domain name - so that we can easier extend change this in extensions.

- Took the text for the GRASP discovery of ACP neighbors from Brian's grasp-ani-objectives draft. Alas, that draft was behind the latest GRASP draft, so I had to overhaul. The major change is to describe in the ACP draft the whole format of the M_FLOOD message (and not only the actual objective). This should make it a lot easier to read (without having to go back and forth to the GRASP RFC/draft). It was also necessary because the locator in the M_FLOOD messages has an important role and isn't coded inside the objective. The specification of how to format the M_FLOOD message should now be complete, the text may be some duplicate with the DULL specification in GRASP, but no contradiction.

- One of the main outcomes of reworking the GRASP section was the notion that GRASP announces both the candidate peer's IPv6 link local address but also the support ACP security protocol including the port it is running on. In the past we shied away from using this information because it is not secured, but I think the additional attack vectors possible by using this information are negligible: If an attacker on an L2 subnet can fake another devices GRASP message then it can already provide a similar amount of attack by purely faking the link-local address.

- Removed the section on discovery and BRSKI. This can be revived in the BRSKI document, but it seems mood given how we did remove mDNS from the latest BRSKI document (aka: this section discussed discrepancies between GRASP and mDNS discovery which should not exist anymore with latest BRSKI.

- Tried to resolve the EDNOTE about CRL vs. OCSP by pointing out we do not specify which one is to be used but that the ACP should be used to reach the URL included in the certificate to get to the CRL storage or OCSP server.

- Changed ACP via IPsec to ACP via IKEv2 and restructured the sections to make IPsec native and IPsec via GRE subsections.

- No need for any assigned DTLS port if ACP is run across DTLS because it is signaled via GRASP.

14.14. draft-ietf-anima-autonomic-control-plane-08

Modified mentioning of BRSKI to make it consistent with current (07/2017) target for BRSKI: MASA and IDevID are mandatory. Devices with only insecure UDI would need a security reduced variant of BRSKI. Also added mentioning of Netconf Zero-Touch. Made BRSKI non-
normative for ACP because wrt. ACP it is just one option how the domain certificate can be provisioned. Instead, BRSKI is mandatory when a device implements ANI which is ACP+BRSKI.

Enhanced text for ACP across tunnels to describe two options: one across configured tunnels (GRE, IPinIP etc) a more efficient one via directed DULL.

Moved description of BRSKI to appendix to emphasize that BRSKI is not a (normative) dependency of GRASP, enhanced text to indicate other options how Domain Certificates can be provisioned.

Added terminology section.

Separated references into normative and non-normative.

Enhanced section about ACP via "tunnels". Defined an option to run ACP secure channel without an outer tunnel, discussed PMTU, benefits of tunneling, potential of using this with BRSKI, made ACP via GREP a SHOULD requirement.

Moved appendix sections up before IANA section because there where concerns about appendices to be too far on the bottom to be read. Added (Informative) / (Normative) to section titles to clarify which sections are informative and which are normative.

Moved explanation of ACP with L2 from precondition to separate section before workarounds, made it instructive enough to explain how to implement ACP on L2 ports for L3/L2 switches and made this part of normative requirement (L2/L3 switches SHOULD support this).

Rewrote section "GRASP in the ACP" to define GRASP in ACP as mandatory (and why), and define the ACP as security and transport substrate to GRASP in ACP. And how it works.

Enhanced "self-protection" properties section: protect legacy management protocols. Security in ACP is for protection from outside and those legacy protocols. Otherwise need end-to-end encryption also inside ACP, e.g., with domain certificate.

Enhanced initial domain certificate section to include requirements for maintenance (renewal/revocation) of certificates. Added explanation to BRSKI informative section how to handle very short lived certificates (renewal via BRSKI with expired cert).

Modified the encoding of the ACP address to better fit RFC822 simple local-parts (":" as required by RFC5952 are not permitted in simple
dot-atoms according to RFC5322. Removed reference to RFC5952 as it is no longer needed.

Introduced a sub-domain field in the ACP information in the certificate to allow defining such subdomains with depending on future Intent definitions. It also makes it clear what the "main domain" is. Scheme is called "routing subdomain" to have a unique name.

Added V8 (now called Vlong) addressing sub-scheme according to suggestion from mcr in his mail from 30 Nov 2016 (https://mailarchive.ietf.org/arch/msg/anima/nZpEphrTqDCBdzsKMsaIh2gsIzI). Also modified the explanation of the single V bit in the first sub-scheme now renamed to Zone sub-scheme to distinguish it.

14.15. draft-ietf-anima-autonomic-control-plane-09

Added reference to RFC4191 and explained how it should be used on ACP edge routers to allow auto configuration of routing by NMS hosts. This came after review of stable connectivity draft where ACP connect is being referred to.

V8 addressing Sub-Scheme was modified to allow not only /8 device-local address space but also /16. This was in response to the possible need to have maybe as much as 2^12 local addresses for future encaps in BRSKI like IPinIP. It also would allow full autonomic address assignment for ACP connect interfaces from this local address space (on an ACP edge device), subject to approval of the implied update to rfc4291/rfc4193 (IID length). Changed name to Vlong addressing sub-scheme.


- The stable connectivity draft was vaguely describing ACP connect behavior that is better standardized in this ACP draft.
- Added new ACP "Manual" addressing sub-scheme with /64 subnets for use with ACP connect interfaces. Being covered by the ACP ULA prefix, these subnets do not require additional routing entries for NMS hosts. They also are fully 64-bit IID length compliant and therefore not subject to 4191bis considerations. And they avoid that operators manually assign prefixes from the ACP ULA prefixes that might later be assigned autonomically.
- ACP connect auto-configuration: Defined that ACP edge devices, NMS hosts should use RFC4191 to automatically learn ACP prefixes.
This is especially necessary when the ACP uses multiple ULA prefixes (via e.g., the rsub domain certificate option), or if ACP connect sub-interfaces use manually configured prefixes NOT covered by the ACP ULA prefixes.

- Explained how rfc6724 is (only) sufficient when the NMS host has a separate ACP connect and Data-Plane interface. But not when there is a single interface.

- Added a separate subsection to talk about "software" instead of "NMS hosts" connecting to the ACP via the "ACP connect" method. The reason is to point out that the "ACP connect" method is not only a workaround (for NMS hosts), but an actual desirable long term architectural component to modularly build software (e.g., ASA or OAM for VNF) into ACP devices.

- Added a section to define how to run ACP connect across the same interface as the Data-Plane. This turns out to be quite challenging because we only want to rely on existing standards for the network stack in the NMS host/software and only define what features the ACP edge device needs.

- Added section about use of GRASP over ACP connect.

- Added text to indicate packet processing/filtering for security: filter incorrect packets arriving on ACP connect interfaces, diagnose on RPL root packets to incorrect destination address (not in ACP connect section, but because of it).

- Reaffirm security goal of ACP: Do not permit non-ACP routers into ACP routing domain.

Made this ACP document be an update to RFC4291 and RFC4193. At the core, some of the ACP addressing sub-schemes do effectively not use 64-bit IIDs as required by RFC4191 and debated in rfc4191bis. During 6man in Prague, it was suggested that all documents that do not do this should be classified as such updates. Add a rather long section that summarizes the relevant parts of ACP addressing and usage and. Aka: This section is meant to be the primary review section for readers interested in these changes (e.g., 6man WG.).

Added changes from Michael Richardson's review https://github.com/anima-wg/autonomic-control-plane/pull/3/commits, textual and:

- ACP discovery inside ACP is bad *doh*!.

- Better CA trust and revocation sentences.
o More details about RPL behavior in ACP.

o black hole route to avoid loops in RPL.

Added requirement to terminate ACP channels upon cert expiry/revocation.

Added fixes from 08-mcr-review-reply.txt (on github):

o AN Domain Names are FQDNs.

o Fixed bit length of schemes, numerical writing of bits (00b/01b).

o Lets use US american english.

14.16. draft-ietf-anima-autonomic-control-plane-10

Used the term routing subdomain more consistently where previously only subdomain was used. Clarified use of routing subdomain in creation of ULA "global ID" addressing prefix.

6.7.1. Changed native IPsec encapsulation to tunnel mode (necessary), explained why. Added notion that ESP is used, added explanations why tunnel/transport mode in native vs. GRE cases.

6.10.3/6.10.5 Added term "ACP address range/set" to be able to better explain how the address in the ACP certificate is actually the base address (lowest address) of a range/set that is available to the device.

6.10.4 Added note that manual address sub-scheme addresses must not be used within domain certificates (only for explicit configuration).

6.12.5 Refined explanation of how ACP virtual interfaces work (p2p and multipoint). Did seek for pre-existing RFCs that explain how to build a multi-access interface on top of a full mesh of p2p connections (6man WG, anima WG mailing lists), but could not find any prior work that had a succinct explanation. So wrote up an explanation here. Added hopefully all necessary and sufficient details how to map ACP unicast packets to ACP secure channel, how to deal with ND packet details. Added verbiage for ACP not to assign the virtual interface link-local address from the underlying interface. Added note that GRAP link-local messages are treated specially but logically the same. Added paragraph about NBMA interfaces.
remaining changes from Brian Carpenters review. See Github file draft-ietf-anima-autonomic-control-plane/08-carpenter-review-reply.txt for more details:

Added multiple new RFC references for terms/technologies used.

Fixed verbage in several places.

2. (terminology) Added 802.1AR as reference.

2. Fixed up definition of ULA.

6.1.1 Changed definition of ACP information in cert into ABNF format. Added warning about maximum size of ACP address field due to domain-name limitations.

6.2 Mentioned API requirement between ACP and clients leveraging adjacency table.

6.3 Fixed TTL in GRASP example: msec, not hop-count!.

6.8.2 MAYOR: expanded security/transport substrate text:

Introduced term ACP GRASP virtual interface to explain how GRASP link-local multicast messages are encapsulated and replicated to neighbors. Explain how ACP knows when to use TLS vs. TCP (TCP only for link-local address (sockets). Introduced "ladder" picture to visualize stack.

6.8.2.1 Expanded discussion/explanation of security model. TLS for GRASP unicast connections across ACP is double encryption (plus underlying ACP secure channel), but highly necessary to avoid very simple man-in-the-middle attacks by compromised ACP members on-path. Ultimately, this is done to ensure that any apps using GRASP can get full end-to-end secrecy for information sent across GRASP. But for publically known ASA services, even this will not provide 100% security (this is discussed). Also why double encryption is the better/easier solution than trying to optimize this.

6.10.1 Added discussion about pseudo-random addressing, scanning-attacks (not an issue for ACP).

6.12.2 New performance requirements section added.

6.10.1 Added notion to first experiment with existing addressing schemes before defining new ones - we should be flexible enough.
6.3/7.2 clarified the interactions between MLD and DULL GRASP and specified what needs to be done (e.g., in 2 switches doing ACP per L2 port).

12. Added explanations and cross-references to various security aspects of ACP discussed elsewhere in the document.

13. Added IANA requirements.

Added RFC2119 boilerplate.

14.17. draft-ietf-anima-autonomic-control-plane-11

Same text as -10. Unfortunately when uploading -10.xml/.txt to datatracker, a wrong version of .txt got uploaded, only the.xml was correct. This impacts the -10.html version on datatracker and the PDF versions as well. Because rfc2119 also compares the .txt version, this -11 version was created so that one can compare changes from -09 and changes to the next version (-12).

14.18. draft-ietf-anima-autonomic-control-plane-12

Sheng Jiang's extensive review. Thanks! See Github file draft-ietf-anima-autonomic-control-plane/09-sheng-review-reply.txt for more details. Many of the larger changes listed below where inspired by the review.

Removed the claim that the document is updating RFC4291, RFC4193 and the section detailing it. Done on suggestion of Michael Richardson - just try to describe use of addressing in a way that would not suggest a need claim update to architecture.

Terminology cleanup:

- Replaced "device" with "node" in text. Kept "device" only when referring to "physical node". Added definitions for those words. Includes changes of derived terms, especially in addressing: "Node-ID" and "Node-Number" in the addressing details.

- Replaced term "autonomic FOOBAR" with "ACP FOOBAR" as wherever appropriate: "autonomic" would imply that the node would need to support more than the ACP, but that is not correct in most of the cases. Wanted to make sure that implementers know they only need to support/implement ACP - unless stated otherwise. Includes "AN->ACP node", "AN->ACP adjacency table" and so on.

1 Added explanation in the introduction about relationship between ACP, BR Skinner, ANI and Autonomic Networks.
6.1.1 Improved terminology and features of the certificate information field. Now called domain information field instead of ACP information field. The acp-address field in the domain information field is now optional, enabling easier introduction of various future options.

6.1.2 Moved ACP domain membership check from section 6.6 to (ACP secure channels setup) here because it is not only used for ACP secure channel setup.

6.1.3 Fix text about certificate renewal after discussion with Max Filitkin/Michael Richardson/Brian Carpenter:

- Version 10 erroneously assumed that the certificate itself could store a URL for renewal, but that is only possible for CRL URLs. Text now only refers to "remembered EST server" without implying that this is stored in the certificate.

- Objective for RFC7030/EST domain certificate renewal was changed to "SRV.est" See also IANA section for explanation.

- Removed detail of distance based service selection. This can be better done in future work because it would require a lot more detail for a good DNS-SD compatible approach.

- Removed detail about trying to create more security by using ACP address from certificate of peer. After rethinking, this does not seem to buy additional security.

6.10 Added reference to 6.12.5 in initial use of "loopback interface" in section 6.10 in result of email discussion michaelR/michaelB.

10.2 Introduced informational section (diagnostics) because of operational experience - ACP/ANI undeployable without at least diagnostics like this.

10.3 Introduced informational section (enabling/disabling) ACP. Important to discuss this for security reasons (e.g., why to never auto-enable ANI on brownfield devices), for implementers and to answer ongoing questions during WG meetings about how to deal with shutdown interface.

10.8 Added informational section discussing possible future variations of the ACP for potential adopters that cannot directly use the complete solution described in this document unmodified.
14.19.  draft-ietf-anima-autonomic-control-plane-13

Swap author list (with permission).

6.1.1.  Eliminate blank lines in definition by making it a picture (reformatting only).

6.10.3.1 New paragraph: Explained how nodes using Zone-ID != 0 need to use Zone-ID != 0 in GRASP so that we can avoid routing/forwarding of Zone-ID = 0 prefixes.

Rest of feedback from review of -12, see https://raw.githubusercontent.com/anima-wg/autonomic-control-plane/master/draft-ietf-anima-autonomic-control-plane/12-feedback-reply.txt

Review from Brian Carpenter:

various: Autonomous -> autonomic(ally) in all remaining occurrences.

various: changed "manual (configured)" to "explicitly (configured)" to not exclude the option of (SDN controller) automatic configuration (no humans involved).


2.  Added definition of loopback interface == internal interface. After discus on WG mailing lists, including 6man.

6.1.2 Defined CDP/OCSP and pointed to RFC5280 for them.

6.1.3 Removed "EST-TLS", no objective value needed or beneficial, added explanation paragraph why.

6.2 Added to adjacency table the interface that a neighbor is discovered on.

6.3 Simplified CDDL syntax: Only one method per AN_ACP objective (because of locators). Example with two objectives in GRASP message.

6.8.1 Added note about link-local GRASP multicast message to avoid confusion.

8.1.4 Added RFC8028 as recommended on hosts to better support VRF-select with ACP.
8.2.1 Rewrote and Simplified CDDL for configured remote peer and explanations. Removed pattern option for remote peer. Not important enough to be mandated.

Review thread started by William Atwood:

2. Refined definition of VRF (vs. MPLS/VPN, LISP, VRF-LITE).

2. Refined definition of ACP (ACP includes ACP GRASP instance).

2. Added explanation for "zones" to terminology section and into Zone Addressing Sub Scheme section, relating it to RFC4007 zones (from Brian Carpenter).

4. Fixed text for ACP4 requirement (Clients of the ACP must not be tied to specific protocol.).

5. Fixed step 4. with proposed text.

6.1.1 Included suggested explanation for rsub semantics.

6.1.3 must->MUST for at least one EST server in ACP network to autonomically renew certs.

6.7.2 normative: AND MUST NOT (permit weaker crypto options.

6.7.1.1 also included text denying weaker IPsec profile options.

6.8.2 Fixed description how to build ACP GRASP virtual interfaces. Added text that ACP continues to exist in absence of ACP neighbors.

various: Make sure all "zone" words are used consistently.

6.10.2/various: fixed 40-bit RFC4193 ULA prefix in all examples to 89b714f3db (thanks MichaelR).

6.10.1 Removed comment about assigned ULA addressing. Decision not to use it now ancient history of WG decision making process, not worth nothing anymore in the RFC.

Review from Yongkang Zhang:

6.10.5 Fixed length of Node-Numbers in ACP Vlong Addressing Sub-Scheme.
Disclaimer: All new text introduced by this revision provides only additional explanations/details based on received reviews and analysis by the authors. No changes to behavior already specified in prior revisions.

Joel Halpern, review part 3:

Define/explain "ACP registrar" in reply to Joel Halpern review part 3, resolving primarily 2 documentation issues:

1. Unclear how much ACP depends on BRSKI. ACP document was referring unqualified to registrars and Registrar-ID in the addressing section without explaining what a registrar is, leading to the assumption it must be a BRSKI Registrar.

2. Unclear how the ACP addresses in ACP domain certificates are assigned because the BRSKI document does not defines this, but refers to this ACP document.

Wrt. 1: ACP does NOT depend on BRSKI registrars, instead ANY appropriate automated or manual mechanism can be used to enroll ACP nodes with ACP domain certificates. This revision calls defines such mechanisms the "ACP registrar" and defines requirements. this is non-normative, because it does not define specific mechanisms that need to be support. In ANI devices, ACP Registrars are BRSKI Registrars. In non-ANI ACP networks, the registrar may simply be a person using CLI/web-interfaces to provision domain certificates and set the ACP address correctly in the ACP domain certificate.

Wrt. 2.: The BRSKI document does rightfully not define how the ACP address assignment and creation of the ACP domain information field has to work because this is independent of BRSKI and needs to follow the same rules whatever protocol/mechanisms are used to implement an ACP Registrar. Another set of protocols that could be used instead of BRSKI is Netconf/Netconf-Call-Home, but such an alternative ACP Registrar solution would need to be specified in its own document.

Additional text/sections had to be added to detail important conditions so that automatic certificate maintenance for ACP nodes (with BRSKI or other mechanisms) can be done in a way that as good as possible maintains ACP address information of ACP nodes across the nodes lifetime because that ACP address is intended as an identifier of the ACP node.

Summary of sections added:
6.1.3.5/6.1.3.6 (normative): re-enrollment of ACP nodes after certificate expiry/failure in a way that allows to maintain as much as possible ACP address information.

6.10.7 (normative): defines "ACP Registrar" including requirements and how it can perform ACP address assignment.

10.3 (informative): details / examples about registrars to help implementers and operators understand easier how they operate, and provide suggestion of models that are likely very useful (sub-CA and/or centralized policy management).

10.4 (informative): Explains the need for the multiple address sub-spaces defined in response to discuss with Joel.

Other changes:

Updated references (RFC8366, RFC8368).

Introduced sub-section headings for 6.1.3 (certificate maintenance) because section became too long with newly added sub-sections. Also some small text fixups/remove of duplicate text.

Gen-ART review, Elwyn Davies:

[ RFC Editor: how can I raise the issue of problematic cross references of terms in the terminology section - rendering is problematic.

4. added explanation for ACP4 (finally).

6.1.1 Simplified text in bullet list explaining rfc822 encoding.

6.1.3 refined second paragraph defining remembering of previous EST server and explaining how to do this with BRSKI.

9.1 Added paragraph outlining the benefit of the sub-CA Registrar option for supporting partitioned networks.

Roughly 100 more nits/minor fixes throughout the document. See: https://raw.githubusercontent.com/anima-wg/autonomic-control-plane/master/draft-ietf-anima-autonomic-control-plane/13-elwynd-reply.txt

Joel Halpern, review part 2:

6.1.1: added note about "+ +" format in address field when acp-address and rsub are empty.
6.5.10 - clarified text about V bit in Vlong addressing scheme.

6.10.3/6.10.4 - moved the Z bit field up front (directly after base scheme) and indicated more explicitly Z is part of selecting of the sub-addressing scheme.

Refined text about reaching CRL Distribution Point, explain why address as indicator to use ACP.

Note from Brian Carpenter: RFC Editor note for section reference into GRASP.

IOT directorate review from Pascal Thubert:

Various Nits/typos.

TBD: Punted wish for mentioning RFC reference titles to RFC editor for now.

1. Added section 1.1 - applicability, discussing protocol choices re. applicability to constrained devices (or not). Added notion of TCP/TLS via CoAP/DTLS to section 10.4 in support of this.


5. Referenced section 8.2 for remote ACP channel configuration.

6.3 made M_FLOOD periods RECOMMENDED (less guesswork)

6.7.x Clarified conditional nature of MUST for the profile details of IPsec parameters (aka: only 6.7.3 defines actual MUST for nodes, prior notions only define the requirements for IPsec profiles IF IPsec is supported.

6.8.1 Moved discussion about IP multicast, IGP, RPL for GRASP into a new subsection in the informative part (section 10) to tighten up text in normative part.

6.10.1 added another reference to stable-connectivity for interop with IPv4 management.

6.10.1 removed mentioning of ULA-Random, term was used in email discus of ULA with L=1, but term actually not defined in rfc4193, so mentioning it is just confusing/redundant. Also added note about the random hash being defined in this document, not using SHA1 from rfc4193.
6.11.1.1 added suggested text about mechanisms to further reduce opportunities for loop during reconvergence (active signaling options from RFC6550).

6.11.1.3 made mode 2 MUST and mode 2 MAY (RPL MOP - mode of operations). Removes ambiguity.

6.12.5 Added recommendation for RFC4429 (optimistic DAD).

Nits from Benjamin Kaduk: dTLS -> DTLS:

Review from Joel Halpern:

1. swapped order of "purposes" for ACP to match order in section 3.

2. Added notion about manageability of ACP going beyond RFC7575 (before discussion of stable connectivity).

2. Changed definition of Intent to be same as reference model (policy language instead of API).

6.1.1 changed BNF specification so that a local-part without acp-address (for future extensions) would not be rfcSELF+rsub but simpler rfcSELF+rsub. Added explanation why rsub is in local-part.

Tried to eliminate unnecessary references to VRF to minimize assumption how system is designed.

6.1.3 Explained how to make CDP reachable via ACP.

6.7.2 Made it clearer that constrained devices MUST support DTLS if they cannot support IPsec.

6.8.2.1 clarified first paragraph (TCP retransmissions lightweight).

6.11.1 fixed up RPL profile text - to remove "VRF". Text was also buggy. mentioned control plane, but it’s a forwarding/silicon issue to have these header.

6.12.5 Clarified how link-local ACP channel address can be derived, and how not.

8.2.1 Fixed up text to distinguish between configuration and model describing parameters of the configuration (spec only provides parameter model).

Various Nits.
14.21. draft-ietf-anima-autonomic-control-plane-15

Only reshuffling and formatting changes, but wanted to allow reviewers later to easily compare -13 with -14, and these changes in -15 mess that up too much.

increased TOC depth to 4.

Separated and reordered section 10 into an operational and a background and futures section. The background and futures could also become appendices if the layout of appendices in RFC format wasn’t so horrible that you really only want to avoid using them (all the way after a lot of text like references that stop most readers from proceeding any further).

14.22. draft-ietf-anima-autonomic-control-plane-16

Mirja Kuehlewind:

Tightened requirements for ACP related GRASP objective timers.

Better text to introduce/explains baseline and constrained ACP profiles.

IANA guideline: MUST only accept extensible last allocation for address sub-scheme.

Moved section 11 into appendix.

Warren Kumari:

Removed "global routing table", replaced with "Data-Plane routing (and forwarding) tables.

added text to indicate how routing protocols do like to have data-plane dependencies.

Changed power consumption section re. admin-down state. Power needed to bring up such interfaces make t inappropriate to probe. Need to think more about beat suggests -> beyond scope.

Replaced "console" with out-of-band... (console/management ethernet).

Various nits.

Joel Halpern:
Fixed up domain information field ABNF to eliminate confusion that rsub is not an FQDN but only a prefix to routing-subdomain.

Corrected certcheck to separate out cert verification into lifetime validity and proof of ownership of private key.

Fixed pagination for "ACP as security and transport substrate for GRASP" picture.

14.23. draft-ietf-anima-autonomic-control-plane-17

Review Alissa Cooper:

Main discuss point fixed by untangling two specific node type cases:

NOC nodes have ACP domain cert without acp-address field. Are ACP domain members, but cannot build ACP secure channels (just end-to-end or nay other authentications.

ACP nodes may have other methods to assign ACP address than getting it through the cert. This is indicated through new value 0 for acp-address in certificate.

Accordingly modified texts in ABNF/explanation and Cert-Check section.

Other:

Better separation of normative text and considerations for "future" work:

- Marked missing chapters as Informative. Reworded requirements section to indicate its informative nature, changed requirements to _MUST/_SHOULD_ to indicate these are not RFC2119 requirements but that this requirements section is really just in place of a separate solutions requirements document (that ANIMA was not allowed to produce).

- removed ca. 20 instances of "futures" in normative part of document.

- moved important instances of "futures" into new section A.10 (last section of appendix). These serve as reminder of work discussed during WG but not able to finish specifying it.

Eliminated perception that "rsub" (routing subdomain) is only beneficial with future work. Example in A.7.
Added RFC-editor note re formatting of references to terms defined in terminology section.

Using now correct RFC 8174 boilerplate.

Clarified semantic and use of manual ACP sub-scheme. Not used in certificates, only assigned via traditional methods. Use for ACP-connect subnets or the like.

Corrected text about Data-Plane dependencies of ACP. Appropriate implementations can be fully data-plane independent (without more spec work) if not sharing link-local address with Data-Plane. 6.12.2 text updated to discuss those (MAC address), A.10.2 discusses options that would require new standards work.

Moved all text about Intent into A.8 to clearly mark it as futures.

Changed suggestion of future insecure ACP option to future "end-to-end-security-only" option.

Various textual fixes.

Gen-ART review by Elwyn Davies:

Some fixes also mentioned by Alissa.

Added reference for OT.

Fixed notion that secure channel is not only a security association.

>20 good textual fixes. Thanks!

Other:

Added picture requested by Pascal Thubert about Dual-NOC (A.10.4).

Moved RFC-editor request for better first RFC reference closer to the top of the document.

Fixed typo /126 -> 127 for prefix length with zone address scheme.

Overlooked early SecDir review from frank.xialiang@huawei.com:

most issues fixed through other review in -16. Added reference to self-protection section 9.2 into security considerations section.
14.24.  draft-ietf-anima-autonomic-control-plane-18

Too many word/grammar mistakes in -17.

14.25.  draft-ietf-anima-autonomic-control-plane-19

Review Eric Rescola:

6.1.2 - clarified that we do certificate path validation against potentially multiple trust anchors.

6.1.3 - Added more comprehensive explanation of Trust Points via new section 6.1.3.

6.5 - added figure with sequential steps of ACP channel establishment and Alice and Bob finding their role in the setup.

6.7.x - detailed crypto profiles: AES-256-GCM, ECDHE.

6.7.2 - Referring to RFC7525 as the required crypto profile for DTLS (taking text from RFC8310 as previously discussed with Eric).

6.7.3 - Added explanation that ACP needs no single MTI secure channel protocol with example.

6.10.2 - Added requirement that rsup must be chosen so that they don’t create SHA256 collisions. Added explanation how the same could be done for different ACP networks with same trust anchors but that this outside the scope of this specification.

6.7.10 - Explains security expectations against ACP registrars: Must be trusted and then given credentials to act as PKI RA to help pledges to enroll with an ACP certificate.

9.1 - Added explanations about merging ACP domains requiring both domains to trust union of Trust Anchors and need to avoid ULA hash collisions.

11 - Added that ACP registrars are critical infrastructure requiring hardening like CA, mentioning attack impact examples.

11 - Mentioning that ACP requires initial setup of CA and registrar.

11 - long rewrite/extension of group security model and its implication shared with review from Ben (below).

Many nits fixed.
Review Benjamin Kaduk:

Fixed various nits.

Changed style of MUST/SHOULD in Requirements section to all lower case to avoid any RFC2119 confusion.

1. clarified support for constrained devices/DTLS: Opportunistic.

1. Clarified ACPs use of two variants of GRASP DULL for neighbor discovery and ACP grasp for service discovery/clients.

3.2 - amended text explaining what additional security ACP provides for bootstrap protocols.

6.1.1 - Added note about ASN.1 encoding in the justification for use of rfc822address.

6.1.2 - Added details how to handle ACP connection when node via which OCSP/CRL-server is reached fails certificate verification.

12. Rewrote explanation why objective names requested for ACP use SRV.name.

10.4 - added summary section about ACP and configuration.

Review Eric Rescorla:

6.1.2 - changed peer certificate verification to be certificate path verification, added lowercase normalization comparison to domain name check.

6.1.2 - explained how domain membership check is authentication and authorization.

6.1.4.1 - Fixed "objective value" to "objective name".

6.1.4.3 - check IPv6 address of CDP against CDP ACP certificate IPv6 address only if URL uses IPv6 address.

6.10.1 - added more justification why there is no need for privacy protection of ACP addresses.

6.11.1.1 - thorough fixup of sentences/structure of this RPL overview section to make it more logical and easier to digest. Also added a paragraph about the second key benefit of this profile (scalability).
6.11.1.9 - Added explanation about not using RPL security from Benjamin.

8.1.1 - Fixed up text for address assignment of ACP connect interfaces. Only recommending manual addressing scheme.

9.1 - changed self-healing benefit text to describe immediate channel reset for short-lived certificates and describing how the same with CRL/OCSP is optional.

11. - added note about immediate termination of secure channels after certificate expiry as this is uncommon today.

11. - rewrote section of security model, attacks and mitigation of compromised ACP members.

A.24 - clarified the process in which expired certificates are used for certificate renewal to avoid higher overhead of re-enrolment.

A.4 - removed mentioning of RPL trickle because not used by ACP RPL profile.

A.10.8 - added section discussing how to minimize risk of compromised nodes, recovering them or kicking them out.


Need to find good reference for TLS profile for ACP GRASP TLS connections.

TBD: Add DTLS choice to GRASP secure channel.

14.27. draft-ietf-anima-autonomic-control-plane-20

(1) In reply to review of -16 by Ben Kaduk:

Diff:


6.1.1 - Changed ABNF to use HEXDIG (to simplify ABNF) and changed example to resulting uppercase hex characters. There was no specific
reason to pick lower vs. upper-case left, and predefined HEXDIG is uppercase.

- Added explanation why internationalized domain-names are not supported/required.

6.1.4.1 - better hint/formal text to explain grasp objective encoding parameters.

6.7.1.1 - rewrote IPsec/IKEv2 requirements after discovering the appropriate references RFC8221/8247 and ben asking to use IANA registry code-point words correctly. Fully relying on RFC recommendation parameters, just stripping down required options to minimum for IPsec to simplify any HW dependencies. Not stripped down IKEv2 (SW) requirements though - unclear if that would be useful.

6.7.1.2 - stripped down IPsec/GRE requirements by referring to the new text in 6.7.1.1 (reducing duplication that existed up to -19.

Referring to RFC7525 also as BCP as requested by Benj. Q: Do BCPs keep numbers even if RFCs for them change ?? Otherwise i am not sure what difference it makes to mention the BCP (maybe just to emphasize on the operationall character..).

6.8.2 - Also referring now to RFC7525 for TLS requirements. Authors had overlooked that it was not only covering DTLS, but also TLS.

6.11.1.14 - added paragraph about "simple" nodes not having to become RPL roots (and therefore have less forwarding plane requirements. Logic is that when there are only "simple" nodes, the requested forwarding plane feature (diagnostcs) wouldn’t be useful immediately anyhow because no operator could connect to the network (all access to ACP assumed to be via more intelligent nodes.

10.3.7 - Refined/amended explanation of ACP-connect configuration case and how it can also be simple.

various - fixed places where LDevID was used instead of IDevID. Some other smaller textual fixes

(2)In reply to review of -16 by Eric Rescorla (by Ben Kaduk):

Diff:

http://tools.ietf.org/tools/rfcdiff/

6.1.1. - new subsection to cover generic ACP certificate requirements. Must be rfc5280 complaint. Asks for what is understood to be hopefully best current practices: Certificate with ECDH public key, preferably signed by ECDH key, describes how ACP domain information field is effectively non cryptographic identity/name of entity owning certificate.

6.1.3 (was 6.1.2) - ACP domain membership text refinement:

emphasises how this includes action of a security association protocol (example IKEv2 proof of ownership of cert), reines relevant parts of rfc5280, refines that CRL/OCSP are skipped only in absence of doing them via secure association protocol).

created new summary at the end restating the purpose of the different steps.

6.1.5 (was 6.1.4) - added requirement for EST server certificate to have extended key use id-kp-cmcRA so clients can trust them when requesting refreshed CA certificates. Also explains how to set up EST server for multiple ACP domains.

6.3 - DULL GRASP, explains why certs are not signalled in DULL grasp.

6.7 - explains generic requirements against security association protocols: be able to authenticate with ACP certificates, have appropriate security level (weakest link). Be able to directly signal ACP certificates due to absence of other option to learn peer cert. Discusses cases (L2 security, physical security) where security association protocol security can be relaxed/removed).

8.1.5 - GRASP via ACP connect: removed suggestion for policy filtering of GRASP messages. Better restatement of security model of ACP connect to argue that GRASP is to be run equally run across it as across the rest of ACP.

few smaller textual improvements.

In reply to 2nd review email (new ballot position) by Ben Kaduk:

Diff:

http://tools.ietf.org/tools/rfcdiff/
rfcdiff.pyht?url1=https://raw.githubusercontent.com/anima-wg/
large number of textual nits (thanks a lot!).

6.1.1 - Attempted to further complete what’s required in certificate: take from rfc5280 and if feasible by operator policy copy attributes from IDevID for easier diagnostics. Added note that authorization mechanisms for ACP can extend over time leveraging other fields of certificate.

6.1.2 - Added paragraph stating ABNF domain-information field is what becomes the rfc822address and other ABNF terminal nodes are used just in the text (and hash creation).

6.1.5.1 - added note about unknown GRASP objective values MUST be ignored.

6.1.5.3 - CDP distribution uses HTTP, not HTTP (to avoid circular authentication requirements and because payload is self signed/authenticated).

6.5 (Channel selection) - Alice/Bob uses ACP address as tiebreakers, empty ACP address just means "lowest tie-breaker" (become Bob).

10.3.5.1 - Better justification why ANI MUST be explicitly configured on brownfield nodes - customer not bothering about registering company with MASA etc.

A.6 - added RFC editor note to remove this section before publication (as I think we agreed on earlier in WG).

A.7 - added note about possible security wise undesirability to make IDevID information of nodes available even easier through unprotected protocols.

In reply to Michael Richardson:

Diff:

http://tools.ietf.org/tools/rfcdiff/
Terminology text improvements, sUDI, routing-subdomain.

6.10.2 - new table showing the different address formats as a summary.

6.10.5 - Vlong address format, cleaned up representation by introducing F-bit to distinguish 23/15 Vlong address prefixes. Adjusted explanatory text accordingly.

6.1.5.1 - Changed TCP port for SRV.est from 80 to 443 (EST is using TLS).

Other:

Change author association: Toerless Eckert, Huawei -> Futurewei USA.

15. References

15.1. Normative References

[I-D.ietf-anima-grasp]

[I-D.ietf-cbor-cddl]

[IKEV2IANA]

[RFC1034]


15.2. Informative References


[I-D.ietf-anima-prefix-management]
Jiang, S., Du, Z., Carpenter, B., and Q. Sun, "Autonomic IPv6 Edge Prefix Management in Large-scale Networks",
draft-ietf-anima-prefix-management-07 (work in progress), December 2017.

[I-D.ietf-anima-reference-model]
Behringer, M., Carpenter, B., Eckert, T., Ciavaglia, L.,
and J. Nobre, "A Reference Model for Autonomic Networking",
draft-ietf-anima-reference-model-10 (work in progress), November 2018.

[I-D.ietf-netconf-zero-touch]
Watsen, K., Abrahamsson, M., and I. Farrer, "Secure Zero Touch Provisioning (SZTP)"

[I-D.ietf-roll-applicability-template]
Richardson, M., "ROLL Applicability Statement Template",
draft-ietf-roll-applicability-template-09 (work in progress), May 2016.

[I-D.ietf-roll-use-of-rpl-info]
Robles, I., Richardson, M., and P. Thubert, "Using RPL Option Type, Routing Header for Source Routes and IPv6-in-IPv6 encapsulation in the RPL Data Plane",
draft-ietf-roll-useofrplinfo-31 (work in progress), July 2019.

[I-D.ietf-tls-dtls13]

[IEEE-1588-2008]

[IEEE-802.1X]
Group, W. -. H. L. L. P. W., "IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control", February 2010,


15.3. URIs


Appendix A. Background and Futures (Informative)

The following sections discuss additional background information about aspects of the normative parts of this document or associated mechanisms such as BRsKI (such as why specific choices were made by the ACP) and they provide discussion about possible future variations of the ACP.

A.1. ACP Address Space Schemes

This document defines the Zone, Vlong and Manual sub address schemes primarily to support address prefix assignment via distributed, potentially uncoordinated ACP registrars as defined in Section 6.10.7. This costs 48/46-bit identifier so that these ACP registrar can assign non-conflicting address prefixes. This design does not leave enough bits to simultaneously support a large number of nodes (Node-ID) plus a large prefix of local addresses for every node plus a large enough set of bits to identify a routing Zone. In result, Zone, Vlong 8/16 attempt to support all features, but in via separate prefixes.

In networks that always expect to rely on a centralized PMS as described above (Section 10.2.5), the 48/46-bits for the Registrar-ID could be saved. Such variations of the ACP addressing mechanisms could be introduced through future work in different ways. If the prefix rfcSELF in the ACP information field was changed, incompatible ACP variations could be created where every design aspect of the ACP could be changed. Including all addressing choices. If instead a new addressing sub-type would be defined, it could be a backward compatible extension of this ACP specification. Information such as the size of a zone-prefix and the length of the prefix assigned to the ACP node itself could be encoded via the extension field of the ACP domain information.
Note that an explicitly defined "Manual" addressing sub-scheme is always beneficial to provide an easy way for ACP nodes to prohibit incorrect manual configuration of any non-"Manual" ACP address spaces and therefore ensure that "Manual" operations will never impact correct routing for any non-"Manual" ACP addresses assigned via ACP domain certificates.

A.2. BRSKI Bootstrap (ANI)

[I-D.ietf-anima-bootstrapping-keyinfra] (BRSKI) describes how nodes with an IDevID certificate can securely and zero-touch enroll with a domain certificate (LDevID) to support the ACP. BRSKI also leverages the ACP to enable zero-touch bootstrap of new nodes across networks without any configuration requirements across the transit nodes (e.g., no DHCP/DNS forwarding/server setup). This includes otherwise not configured networks as described in Section 3.2. Therefore BRSKI in conjunction with ACP provides for a secure and zero-touch management solution for complete networks. Nodes supporting such an infrastructure (BRSKI and ACP) are called ANI nodes (Autonomic Networking Infrastructure), see [I-D.ietf-anima-reference-model]. Nodes that do not support an IDevID but only an (insecure) vendor specific Unique Device Identifier (UDI) or nodes whose manufacturer does not support a MASA could use some future security reduced version of BRSKI.

When BRSKI is used to provision a domain certificate (which is called enrollment), the BRSKI registrar (acting as an enhanced EST server) must include the subjectAltName / rfc822Name encoded ACP address and domain name to the enrolling node (called pledge) via its response to the pledges EST CSR Attribute request that is mandatory in BRSKI.

The Certificate Authority in an ACP network must not change the subjectAltName / rfc822Name in the certificate. The ACP nodes can therefore find their ACP address and domain using this field in the domain certificate, both for themselves, as well as for other nodes.

The use of BRSKI in conjunction with the ACP can also help to further simplify maintenance and renewal of domain certificates. Instead of relying on CRL, the lifetime of certificates can be made extremely small, for example in the order of hours. When a node fails to connect to the ACP within its certificate lifetime, it cannot connect to the ACP to renew its certificate across it (using just EST), but it can still renew its certificate as an "enrolled/expired pledge" via the BRSKI bootstrap proxy. This requires only that the BRSKI registrar honors expired domain certificates and that the pledge attempts to perform TLS authentication for BRSKI bootstrap using its expired domain certificate before falling back to attempting to use its IDevID for BRSKI. This mechanism could also render CRLs
unnecessary because the BRSKI registrar in conjunction with the CA would not renew revoked certificates – only a "Do-not-renew" list would be necessary on BRSKI registrars/CA.

In the absence of BRSKI or less secure variants thereof, provisioning of certificates may involve one or more touches or non-standardized automation. Node vendors usually support provisioning of certificates into nodes via PKCS#7 (see [RFC2315]) and may support this provisioning through vendor specific models via Netconf ([RFC6241]). If such nodes also support Netconf Zero-Touch ([I-D.ietf-netconf-zerotouch]) then this can be combined to zero-touch provisioning of domain certificates into nodes. Unless there are equivalent integration of Netconf connections across the ACP as there is in BRSKI, this combination would not support zero-touch bootstrap across a not configured network though.

A.3. ACP Neighbor discovery protocol selection

This section discusses why GRASP DULL was chosen as the discovery protocol for L2 adjacent candidate ACP neighbors. The contenders considered where GRASP, mDNS or LLDP.

A.3.1. LLDP

LLDP and Cisco’s earlier Cisco Discovery Protocol (CDP) are example of L2 discovery protocols that terminate their messages on L2 ports. If those protocols would be chosen for ACP neighbor discovery, ACP neighbor discovery would therefore also terminate on L2 ports. This would prevent ACP construction over non-ACP capable but LLDP or CDP enabled L2 switches. LLDP has extensions using different MAC addresses and this could have been an option for ACP discovery as well, but the additional required IEEE standardization and definition of a profile for such a modified instance of LLDP seemed to be more work than the benefit of "reusing the existing protocol" LLDP for this very simple purpose.

A.3.2. mDNS and L2 support

Multicast DNNS (mDNS) [RFC6762] with DNS Service Discovery (DNS-SD) Resource Records (RRs) as defined in [RFC6763] is a key contender as an ACP discovery protocol. Because it relies on link-local IP multicast, it does operate at the subnet level, and is also found in L2 switches. The authors of this document are not aware of mDNS implementation that terminate their mDNS messages on L2 ports instead of the subnet level. If mDNS was used as the ACP discovery mechanism on an ACP capable (L3)/L2 switch as outlined in Section 7, then this would be necessary to implement. It is likely that termination of mDNS messages could only be applied to all mDNS messages from such a
port, which would then make it necessary to software forward any non-ACP related mDNS messages to maintain prior non-ACP mDNS functionality. Adding support for ACP into such L2 switches with mDNS could therefore create regression problems for prior mDNS functionality on those nodes. With low performance of software forwarding in many L2 switches, this could also make the ACP risky to support on such L2 switches.

A.3.3. Why DULL GRASP

LLDP was not considered because of the above mentioned issues. mDNS was not selected because of the above L2 mDNS considerations and because of the following additional points:

If mDNS was not already existing in a node, it would be more work to implement than DULL GRASP, and if an existing implementation of mDNS was used, it would likely be more code space than a separate implementation of DULL GRASP or a shared implementation of DULL GRASP and GRASP in the ACP.

A.4. Choice of routing protocol (RPL)

This section motivates why RPL - "IPv6 Routing Protocol for Low-Power and Lossy Networks ([RFC6550] was chosen as the default (and in this specification only) routing protocol for the ACP. The choice and above explained profile was derived from a pre-standard implementation of ACP that was successfully deployed in operational networks.

Requirements for routing in the ACP are:

- Self-management: The ACP must build automatically, without human intervention. Therefore routing protocol must also work completely automatically. RPL is a simple, self-managing protocol, which does not require zones or areas; it is also self-configuring, since configuration is carried as part of the protocol (see Section 6.7.6 of [RFC6550]).

- Scale: The ACP builds over an entire domain, which could be a large enterprise or service provider network. The routing protocol must therefore support domains of 100,000 nodes or more, ideally without the need for zoning or separation into areas. RPL has this scale property. This is based on extensive use of default routing.

- Low resource consumption: The ACP supports traditional network infrastructure, thus runs in addition to traditional protocols. The ACP, and specifically the routing protocol must have low
resource consumption both in terms of memory and CPU requirements. Specifically, at edge nodes, where memory and CPU are scarce, consumption should be minimal. RPL builds a destination-oriented directed acyclic graph (DODAG), where the main resource consumption is at the root of the DODAG. The closer to the edge of the network, the less state needs to be maintained. This adapts nicely to the typical network design. Also, all changes below a common parent node are kept below that parent node.

- Support for unstructured address space: In the Autonomic Networking Infrastructure, node addresses are identifiers, and may not be assigned in a topological way. Also, nodes may move topologically, without changing their address. Therefore, the routing protocol must support completely unstructured address space. RPL is specifically made for mobile ad-hoc networks, with no assumptions on topologically aligned addressing.

- Modularity: To keep the initial implementation small, yet allow for complex methods, it is highly desirable that the routing protocol has a simple base functionality, but can import new functional modules if needed. RPL has this property with the concept of "objective function", which is a plugin to modify routing behavior.

- Extensibility: Since the Autonomic Networking Infrastructure is a new concept, it is likely that changes in the way of operation will happen over time. RPL allows for new objective functions to be introduced later, which allow changes to the way the routing protocol creates the DAGs.

- Multi-topology support: It may become necessary in the future to support more than one DODAG for different purposes, using different objective functions. RPL allow for the creation of several parallel DODAGs, should this be required. This could be used to create different topologies to reach different roots.

- No need for path optimization: RPL does not necessarily compute the optimal path between any two nodes. However, the ACP does not require this today, since it carries mainly non-delay-sensitive feedback loops. It is possible that different optimization schemes become necessary in the future, but RPL can be expanded (see point "Extensibility" above).

A.5. ACP Information Distribution and multicast

IP multicast is not used by the ACP because the ANI (Autonomic Networking Infrastructure) itself does not require IP multicast but only service announcement/discovery. Using IP multicast for that
would have made it necessary to develop a zero-touch auto configuring solution for ASM (Any Source Multicast - the original form of IP multicast defined in [RFC1112]), which would be quite complex and difficult to justify. One aspect of complexity where no attempt at a solution has been described in IETF documents is the automatic-selection of routers that should be PIM Sparse Mode (PIM-SM) Rendezvous Points (RPs) (see [RFC7761]). The other aspects of complexity are the implementation of MLD ([RFC4604]), PIM-SM and Anycast-RP (see [RFC4610]). If those implementations already exist in a product, then they would be very likely tied to accelerated forwarding which consumes hardware resources, and that in return is difficult to justify as a cost of performing only service discovery.

Some future ASA may need high performance in-network data replication. That is the case when the use of IP multicast is justified. Such an ASA can then use service discovery from ACP GRASP, and then they do not need ASM but only SSM (Source Specific Multicast, see [RFC4607]) for the IP multicast replication. SSM itself can simply be enabled in the Data-Plane (or even in an update to the ACP) without any other configuration than just enabling it on all nodes and only requires a simpler version of MLD (see [RFC5790]).

LSP (Link State Protocol) based IGP routing protocols typically have a mechanism to flood information, and such a mechanism could be used to flood GRASP objectives by defining them to be information of that IGP. This would be a possible optimization in future variations of the ACP that do use an LSP routing protocol. Note though that such a mechanism would not work easily for GRASP M_DISCOVERY messages which are intelligently (constrained) flooded not across the whole ACP, but only up to a node where a responder is found. We do expect that many future services in ASA will have only few consuming ASA, and for those cases, M_DISCOVERY is the more efficient method than flooding across the whole domain.

Because the ACP uses RPL, one desirable future extension is to use RPLs existing notion of loop-free distribution trees (DODAG) to make GRASPs flooding more efficient both for M_FLOOD and M_DISCOVERY) See Section 6.12.5 how this will be specifically beneficial when using NBMA interfaces. This is not currently specified in this document because it is not quite clear yet what exactly the implications are to make GRASP flooding depend on RPL DODAG convergence and how difficult it would be to let GRASP flooding access the DODAG information.
A.6. Extending ACP channel negotiation (via GRASP)

[RFC Editor: This section to be removed before RFC.

[This section kept for informational purposes up until the last draft version as that would be the version that readers interested in the changelog would also go to to revisit it.]

The mechanism described in the normative part of this document to support multiple different ACP secure channel protocols without a single network wide MTI protocol is important to allow extending secure ACP channel protocols beyond what is specified in this document, but it will run into problem if it would be used for multiple protocols:

The need to potentially have multiple of these security associations even temporarily run in parallel to determine which of them works best does not support the most lightweight implementation options.

The simple policy of letting one side (Alice) decide what is best may not lead to the mutual best result.

The two limitations can easier be solved if the solution was more modular and as few as possible initial secure channel negotiation protocols would be used, and these protocols would then take on the responsibility to support more flexible objectives to negotiate the mutually preferred ACP security channel protocol.

IKEv2 is the IETF standard protocol to negotiate network security associations. It is meant to be extensible, but it is unclear whether it would be feasible to extend IKEv2 to support possible future requirements for ACP secure channel negotiation:

Consider the simple case where the use of native IPsec vs. IPsec via GRE is to be negotiated and the objective is the maximum throughput. Both sides would indicate some agreed upon performance metric and the preferred encapsulation is the one with the higher performance of the slower side. IKEv2 does not support negotiation with this objective.

Consider DTLS and some form of MacSec are to be added as negotiation options - and the performance objective should work across all IPsec, DTLS and MacSec options. In the case of MacSEC, the negotiation would also need to determine a key for the peering. It is unclear if it would be even appropriate to consider extending the scope of negotiation in IKEv2 to those cases. Even if feasible to define, it is unclear if implementations of IKEv2 would be eager to adopt those type of extension given the long cycles of security testing that...
necessarily goes along with core security protocols such as IKEv2 implementations.

A more modular alternative to extending IKEv2 could be to layer a modular negotiation mechanism on top of the multitude of existing or possible future secure channel protocols. For this, GRASP over TLS could be considered as a first ACP secure channel negotiation protocol. The following are initial considerations for such an approach. A full specification is subject to a separate document:

To explicitly allow negotiation of the ACP channel protocol, GRASP over a TLS connection using the GRASP_LISTEN_PORT and the node’s and peer’s link-local IPv6 address is used. When Alice and Bob support GRASP negotiation, they do prefer it over any other non-explicitly negotiated security association protocol and should wait trying any non-negotiated ACP channel protocol until after it is clear that GRASP/TLS will not work to the peer.

When Alice and Bob successfully establish the GRASP/TLS session, they will negotiate the channel mechanism to use using objectives such as performance and perceived quality of the security. After agreeing on a channel mechanism, Alice and Bob start the selected Channel protocol. Once the secure channel protocol is successfully running, the GRASP/TLS connection can be kept alive or timed out as long as the selected channel protocol has a secure association between Alice and Bob. When it terminates, it needs to be re-negotiated via GRASP/TLS.

Notes:

- Negotiation of a channel type may require IANA assignments of code points.

- TLS is subject to reset attacks, which IKEv2 is not. Normally, ACP connections (as specified in this document) will be over link-local addresses so the attack surface for this one issue in TCP should be reduced (note that this may not be true when ACP is tunneled as described in Section 8.2.2.

- GRASP packets received inside a TLS connection established for GRASP/TLS ACP negotiation are assigned to a separate GRASP domain unique to that TLS connection.

A.7. CAs, domains and routing subdomains

There is a wide range of setting up different ACP solution by appropriately using CAs and the domain and rsub elements in the domain information field of the domain certificate. We summarize
these options here as they have been explained in different parts of
the document in before and discuss possible and desirable extensions:

An ACP domain is the set of all ACP nodes using certificates from one
or more Trust Anchors (TA) (typically one CA) using the same domain
field. GRASP inside the ACP is run across all transitively connected
ACP nodes in a domain.

The rsub element in the domain information field permits the use of
addresses from different ULA prefixes. One use case is to create
multiple physical networks that initially may be separated with one
ACP domain but different routing subdomains, so that all nodes can
mutual trust their ACP domain certificates (not depending on rsub)
and so that they could connect later together into a contiguous ACP
network.

One instance of such a use case is an ACP for regions interconnected
via a non-ACP enabled core, for example due to the absence of product
support for ACP on the core nodes. ACP connect configurations as
defined in this document can be used to extend and interconnect those
ACP islands to the NOC and merge them into a single ACP when later
that product support gap is closed.

Note that RPL scales very well. It is not necessary to use multiple
routing subdomains to scale ACP domains in a way it would be possible
if other routing protocols where used. They exist only as options
for the above mentioned reasons.

If different ACP domains are to be created that should not allow to
connect to each other by default, these ACP domains simply need to
have different domain elements in the domain information field.
These domain elements can be arbitrary, including subdomains of one
another: Domains "example.com" and "research.example.com" are
separate domains if both are domain elements in the domain
information element of certificates.

It is not necessary to have a separate CA for different ACP domains:
an operator can use a single CA to sign certificates for multiple ACP
domains that are not allowed to connect to each other because the
checks for ACP adjacencies includes comparison of the domain part.

If multiple independent networks choose the same domain name but had
their own CA, these would not form a single ACP domain because of CA
mismatch. Therefore there is no problem in choosing domain names
that are potentially also used by others. Nevertheless it is highly
recommended to use domain names that one can have high probability to
be unique. It is recommended to use domain names that start with a
DNS domain names owned by the assigning organization and unique within it. For example "acp.example.com" if you own "example.com".

A.8. Intent for the ACP

Intent is the architecture component of autonomic networks according to [I-D.ietf-anima-reference-model] that allows operators to issue policies to the network. Its applicability for use is quite flexible and freeform, with potential applications including policies flooded across ACP GRASP and interpreted on every ACP node.

One concern for future definitions of Intent solutions is the problem of circular dependencies when expressing Intent policies about the ACP itself.

For example, Intent could indicate the desire to build an ACP across all domains that have a common parent domain (without relying on the rsub/routing-subdomain solution defined in this document). For example ACP nodes with domain "example.com", "access.example.com", "core.example.com" and "city.core.example.com" should all establish one single ACP.

If each domain has its own source of Intent, then the Intent would simply have to allow adding the peer domains trust anchors (CA) and domain names to the ACP domain membership check (Section 6.1.3) so that nodes from those other domains are accepted as ACP peers.

If this Intent was to be originated only from one domain, it could likely not be made to work because the other domains will not build any ACP connection amongst each other, whether they use the same or different CA due to the ACP domain membership check.

If the domains use the same CA one could change the ACP setup to permit for the ACP to be established between two ACP nodes with different acp-domain-names, but only for the purpose of disseminating limited information, such as Intent, but not to set up full ACP connectivity, specifically not RPL routing and passing of arbitrary GRASP information. Unless the Intent policies permit this to happen across domain boundaries.

This type of approach where the ACP first allows Intent to operate and only then sets up the rest of ACP connectivity based on Intent policy could also be used to enable Intent policies that would limit functionality across the ACP inside a domain, as long as no policy would disturb the distribution of Intent. For example to limit reachability across the ACP to certain type of nodes or locations of nodes.
A.9. Adopting ACP concepts for other environments

The ACP as specified in this document is very explicit about the choice of options to allow interoperable implementations. The choices made may not be the best for all environments, but the concepts used by the ACP can be used to build derived solutions:

The ACP specifies the use of ULA and deriving its prefix from the domain name so that no address allocation is required to deploy the ACP. The ACP will equally work not using ULA but any other /48 IPv6 prefix. This prefix could simply be a configuration of the ACP registrars (for example when using BRSKI) to enroll the domain certificates – instead of the ACP registrar deriving the /48 ULA prefix from the AN domain name.

Some solutions may already have an auto-addressing scheme, for example derived from existing unique device identifiers (e.g., MAC addresses). In those cases it may not be desirable to assign addresses to devices via the ACP address information field in the way described in this document. The certificate may simply serve to identify the ACP domain, and the address field could be empty/unused. The only fix required in the remaining way the ACP operate is to define another element in the domain certificate for the two peers to decide who is Alice and who is Bob during secure channel building. Note though that future work may leverage the acp address to authenticate "ownership" of the address by the device. If the address used by a device is derived from some pre-existing permanent local ID (such as MAC address), then it would be useful to store that address in the certificate using the format of the access address information field or in a similar way.

The ACP is defined as a separate VRF because it intends to support well managed networks with a wide variety of configurations. Therefore, reliable, configuration-indestructible connectivity cannot be achieved from the Data-Plane itself. In solutions where all transit connectivity impacting functions are fully automated (including security), indestructible and resilient, it would be possible to eliminate the need for the ACP to be a separate VRF. Consider the most simple example system in which there is no separate Data-Plane, but the ACP is the Data-Plane. Add BRSKI, and it becomes a fully autonomic network – except that it does not support automatic addressing for user equipment. This gap can then be closed for example by adding a solution derived from [I-D.ietf-anima-prefix-management].

TCP/TLS as the protocols to provide reliability and security to GRASP in the ACP may not be the preferred choice in constrained networks. For example, CoAP/DTLS (Constrained Application Protocol) may be
preferred where they are already used, allowing to reduce the
additional code space footprint for the ACP on those devices. Hop-
by-hop reliability for ACP GRASP messages could be made to support
protocols like DTLS by adding the same type of negotiation as defined
in this document for ACP secure channel protocol negotiation. End-
to-end GRASP connections can be made to select their transport
protocol in future extensions of the ACP meant to better support
constrained devices by indicating the supported transport protocols
(e.g.: TLS/DTLS) via GRASP parameters of the GRASP objective through
which the transport endpoint is discovered.

The routing protocol chosen by the ACP design (RPL) does explicitly
not optimize for shortest paths and fastest convergence. Variations
of the ACP may want to use a different routing protocol or introduce
more advanced RPL profiles.

Variations such as what routing protocol to use, or whether to
instantiate an ACP in a VRF or (as suggested above) as the actual
Data-Plane, can be automatically chosen in implementations built to
support multiple options by deriving them from future parameters in
the certificate. Parameters in certificates should be limited to
those that would not need to be changed more often than certificates
would need to be updated anyhow; Or by ensuring that these parameters
can be provisioned before the variation of an ACP is activated in a
node. Using BRSKI, this could be done for example as additional
follow-up signaling directly after the certificate enrollment, still
leveraging the BRSKI TLS connection and therefore not introducing any
additional connectivity requirements.

Last but not least, secure channel protocols including their
encapsulations are easily added to ACP solutions. ACP hop-by-hop
network layer secure channels could also be replaced by end-to-end
security plus other means for infrastructure protection. Any future
network OAM should always use end-to-end security anyhow and can
leverage the domain certificates and is therefore not dependent on
security to be provided for by ACP secure channels.

A.10. Further (future) options

A.10.1. Auto-aggregation of routes

Routing in the ACP according to this specification only leverages the
standard RPL mechanism of route optimization, e.g. keeping only
routes that are not towards the RPL root. This is known to scale to
networks with 20,000 or more nodes. There is no auto-aggregation of
routes for /48 ULA prefixes (when using rsub in the domain
information field) and/or Zone-ID based prefixes.
Automatic assignment of Zone-ID and auto-aggregation of routes could be achieved for example by configuring zone-boundaries, announcing via GRASP into the zones the zone parameters (zone-ID and /48 ULA prefix) and auto-aggregating routes on the zone-boundaries. Nodes would assign their Zone-ID and potentially even /48 prefix based on the GRASP announcements.

A.10.2. More options for avoiding IPv6 Data-Plane dependency

As described in Section 6.12.2, the ACP depends on the Data-Plane to establish IPv6 link-local addressing on interfaces. Using a separate MAC address for the ACP allows to fully isolate the ACP from the data-plane in a way that is compatible with this specification. It is also an ideal option when using Single-root input/output virtualization (SR-IOV - see https://en.wikipedia.org/wiki/Single-root_input/output_virtualization [2]) in an implementation to isolate the ACP because different SR-IOV interfaces use different MAC addresses.

When additional MAC address(es) are not available, separation of the ACP could be done at different demux points. The same subnet interface could have a separate IPv6 interface for the ACP and Data-Plane and therefore separate link-local addresses for both, where the ACP interface is non-configurable on the Data-Plane. This too would be compatible with this specification and not impact interoperability.

An option that would require additional specification is to use a different Ethertype from 0x86DD (IPv6) to encapsulate IPv6 packets for the ACP. This would be a similar approach as used for IP authentication packets in [IEEE-802.1X] which use the Extensible Authentication Protocol over Local Area Network (EAPoL) ethertype (0x88A2).

Note that in the case of ANI nodes, all the above considerations equally apply to the encapsulation of BRSKI packets including GRASP used for BRSKI.

A.10.3. ACP APIs and operational models (YANG)

Future work should define YANG ([RFC7950]) data model and/or node internal APIs to monitor and manage the ACP.

Support for the ACP Adjacency Table (Section 6.2) and ACP GRASP need to be included into such model/API.
A.10.4. RPL enhancements

Figure 18: Dual NOC

The profile for RPL specified in this document builds only one spanning-tree path set to a root (NOC). In the presence of multiple NOCs, routing toward the non-root NOCs may be suboptimal. Figure 18 shows an extreme example. Assuming that node ACP1 becomes the RPL root, traffic between ACP11 and NOC2 will pass through ACP4-ACP3-ACP1-ACP2 instead of ACP4-ACP2 because the RPL calculated DODAG/routes are shortest paths towards the RPL root.

To overcome these limitations, extensions/modifications to the RPL profile can provide optimality for multiple NOCs. This requires utilizing Data-Plane artifact including IPinIP encap/decap on ACP routers and processing of IPv6 RPI headers. Alternatively, (Src,Dst) routing table entries could be used.

Flooding of ACP GRASP messages can be further constrained and therefore optimized by flooding only via links that are part of the RPL DODAG.

A.10.5. Role assignments

ACP connect is an explicit mechanism to "leak" ACP traffic explicitly (for example in a NOC). It is therefore also a possible security gap when it is easy to enable ACP connect on arbitrary compromised ACP nodes.

One simple solution is to define an extension in the ACP certificates ACP information field indicating the permission for ACP connect to be
configured on that ACP node. This could similarly be done to decide whether a node is permitted to be a registrar or not.

Tying the permitted "roles" of an ACP node to the ACP domain certificate provides fairly strong protection against misconfiguration, but is still subject to code modifications.

Another interesting role to assign to certificates is that of a NOC node. This would allow to limit certain type of connections such as OAM TLS connections to only NOC initiator or responders.

A.10.6. Autonomic L3 transit

In this specification, the ACP can only establish autonomic connectivity across L2 hops and only explicitly configured options to tunnel across L3. Future work should specify mechanisms to automatically tunnel ACP across L3 networks. A hub&spoke option would allow to tunnel across the Internet to a cloud or central instance of the ACP, a peer-to-peer tunneling mechanism could tunnel ACP islands across an L3VPN infrastructure.

A.10.7. Diagnostics

Section 10.1 describes diagnostics options that can be done without changing the external, interoperability affecting characteristics of ACP implementations.

Even better diagnostics of ACP operations is possible with additional signaling extensions, such as:

1. Consider if LLDP should be a recommended functionality for ANI devices to improve diagnostics, and if so, which information elements it should signal (noting that such information is conveyed in an insecure manner). Includes potentially new information elements.

2. In alternative to LLDP, A DULL GRASP diagnostics objective could be defined to carry these information elements.

3. The IDevID of BRSKI pledges should be included in the selected insecure diagnostics option. This may be undesirable when exposure of device information is seen as too much of a security issue (ability to deduce possible attack vectors from device model for example).

4. A richer set of diagnostics information should be made available via the secured ACP channels, using either single-hop GRASP or network wide "topology discovery" mechanisms.
A.10.8. Avoiding and dealing with compromised ACP nodes

Compromised ACP nodes pose the biggest risk to the operations of the network. The most common type of compromise is leakage of credentials to manage/configure the device and the application of malicious configuration including the change of access credentials, but not the change of software. Most of today's networking equipment should have secure boot/software infrastructure anyhow, so attacks that introduce malicious software should be a lot harder.

The most important aspect of security design against these type of attacks is to eliminate password based configuration access methods and instead rely on certificate based credentials handed out only to nodes where it is clear that the private keys can not leak. This limits unexpected propagation of credentials.

If password based credentials to configure devices still need to be supported, they must not be locally configurable, but only be remotely provisioned or verified (through protocols like Radius or Diameter), and there must be no local configuration permitting to change these authentication mechanisms, but ideally they should be autoconfiguring across the ACP. See [I-D.eckert-anima-noc-autoconfig].

Without physical access to the compromised device, attackers with access to configuration should not be able to break the ACP connectivity, even when they can break or otherwise manipulate (spoof) the data-plane connectivity through configuration. To achieve this, it is necessary to avoid providing configuration options for the ACP, such as enabling/disabling it on interfaces. For example there could be an ACP configuration that locks down the current ACP config unless factory reset is done.

With such means, the valid administration has the best chances to maintain access to ACP nodes, discover malicious configuration through ongoing configuration tracking from central locations for example, and to react accordingly.

The primary reaction is withdrawal/change of credentials, terminate malicious existing management sessions and fixing the configuration. Ensuring that management sessions using invalidated credentials are terminated automatically without recourse will likely require new work.

Only when these steps are not feasible would it be necessary to revoke or expire the ACP domain certificate credentials and consider the node kicked off the network - until the situation can be further rectified, likely requiring direct physical access to the node.
Without extensions, compromised ACP nodes can only be removed from the ACP at the speed of CRL/OCSP information refresh or expiry (and non-removal) of short lived certificates. Future extensions to the ACP could for example use GRASP flooding distribution of triggered updates of CRL/OCSP or explicit removal indication of the compromised nodes domain certificate.

Authors’ Addresses

Toerless Eckert (editor)
Futurewei Technologies Inc. USA
2330 Central Expy
Santa Clara  95050
USA

Email: tte+ietf@cs.fau.de

Michael H. Behringer (editor)

Email: michael.h.behringer@gmail.com

Steinthor Bjarnason
Arbor Networks
2727 South State Street, Suite 200
Ann Arbor  MI 48104
United States

Email: sbjarnason@arbor.net
Abstract

This document specifies automated bootstrapping of an Autonomic Control Plane. To do this a Remote Secure Key Infrastructure (BRSKI) is created using manufacturer installed X.509 certificates, in combination with a manufacturer’s authorizing service, both online and offline. Bootstrapping a new device can occur using a routable address and a cloud service, or using only link-local connectivity, or on limited/disconnected networks. Support for lower security models, including devices with minimal identity, is described for legacy reasons but not encouraged. Bootstrapping to is complete when the cryptographic identity of the new key infrastructure is successfully deployed to the device. The established secure connection can be used to deploy a locally issued certificate to the device as well.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 15, 2020.
Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ..................................................... 5
  1.1. Prior Bootstrapping Approaches .......................... 6
  1.2. Terminology .................................................. 7
  1.3. Scope of solution .............................................. 10
    1.3.1. Support environment .................................... 10
    1.3.2. Constrained environments .............................. 11
    1.3.3. Network Access Controls ............................... 12
    1.3.4. Bootstrapping is not Booting ......................... 12
  1.4. Leveraging the new key infrastructure / next steps ... 12
  1.5. Requirements for Autonomic Network Infrastructure (ANI) devices ........................................... 12

2. Architectural Overview .......................................... 13
  2.1. Behavior of a Pledge ....................................... 15
  2.2. Secure Imprinting using Vouchers ........................ 16
  2.3. Initial Device Identifier ................................. 17
    2.3.1. Identification of the Pledge ......................... 17
    2.3.2. MASA URI extension .................................... 18
  2.4. Protocol Flow ................................................. 20
  2.5. Architectural Components .................................. 23
    2.5.1. Pledge .................................................. 23
    2.5.2. Join Proxy .............................................. 23
    2.5.3. Domain Registrar ....................................... 23
    2.5.4. Manufacturer Service .................................. 23
    2.5.5. Public Key Infrastructure (PKI) ...................... 23
  2.6. Certificate Time Validation ................................ 24
    2.6.1. Lack of realtime clock ............................... 24
    2.6.2. Infinite Lifetime of IDevID .......................... 24
  2.7. Cloud Registrar ............................................. 24
  2.8. Determining the MASA to contact ......................... 25

3. Voucher-Request artifact ....................................... 26
  3.1. Nonceless Voucher Requests ............................... 26
3.2. Tree Diagram ........................................... 26
3.3. Examples ............................................... 27
3.4. YANG Module ........................................... 28
4. Proxying details (Pledge - Proxy - Registrar) .......................... 32
  4.1. Pledge discovery of Proxy ................................ 33
    4.1.1. Proxy GRASP announcements ............................ 34
  4.2. CoAP connection to Registrar .............................. 35
  4.3. Proxy discovery and communication of Registrar ............... 36
5. Protocol Details (Pledge - Registrar - MASA) ......................... 37
  5.1. BRSKI-EST TLS establishment details ........................ 39
  5.2. Pledge Requests Voucher from the Registrar .................. 40
  5.3. Registrar Authorization of Pledge .......................... 41
  5.4. BRSKI-MASA TLS establishment details ....................... 41
    5.4.1. MASA authentication of customer Registrar ............. 42
  5.5. Registrar Requests Voucher from MASA ......................... 43
    5.5.1. MASA renewal of expired vouchers ....................... 45
    5.5.2. MASA pinning of registrar ............................. 45
    5.5.3. MASA checking of voucher request signature .......... 45
    5.5.4. MASA verification of domain registrar ................ 46
    5.5.5. MASA verification of pledge prior-signed-voucher-request .......... 46
    5.5.6. MASA nonce handling .................................. 47
  5.6. MASA and Registrar Voucher Response ........................ 47
    5.6.1. Pledge voucher verification ............................ 50
    5.6.2. Pledge authentication of provisional TLS connection ...... 50
  5.7. Pledge BRSKI Status Telemetry ............................ 51
  5.8. Registrar audit-log request ................................ 52
    5.8.1. MASA audit log response ................................ 54
    5.8.2. Calculation of domainID ............................... 55
    5.8.3. Registrar audit log verification ....................... 56
  5.9. EST Integration for PKI bootstrapping ....................... 57
    5.9.1. EST Distribution of CA Certificates .................... 57
    5.9.2. EST CSR Attributes ................................... 58
    5.9.3. EST Client Certificate Request ........................ 59
    5.9.4. Enrollment Status Telemetry ........................... 59
    5.9.5. Multiple certificates ................................. 60
    5.9.6. EST over CoAP ......................................... 60
  6. Clarification of transfer-encoding .............................. 60
  7. Reduced security operational modes ............................. 60
    7.1. Trust Model ............................................ 61
    7.2. Pledge security reductions ............................... 61
    7.3. Registrar security reductions ............................ 62
    7.4. MASA security reductions ............................... 63
      7.4.1. Issuing Nonceless vouchers ........................... 63
      7.4.2. Trusting Owners on First Use ....................... 64
1. Introduction

BRSKI provides a solution for secure zero-touch (automated) bootstrap of new (unconfigured) devices that are called pledges in this document.

This document primarily provides for the needs of the ISP and Enterprise focused ANIMA Autonomic Control Plane (ACP) [I-D.ietf-anima-autonomic-control-plane]. This bootstrap process satisfies the [RFC7575] section 3.3 of making all operations secure by default. Other users of the BRSKI protocol will need to provide separate applicability statements that include privacy and security considerations appropriate to that deployment. Section 9 explains the details applicability for this the ACP usage.

The BRSKI protocol requires a significant amount of communication between manufacturer and owner: in it’s default modes it provides a cryptographic transfer of control to the initial owner. In it’s strongest modes, it leverages sales channel information to identify the owner in advance. Resale of devices is possible, provided that the manufacturer is willing to authorize the transfer. Mechanisms to enable transfers of ownership without manufacturer authorization are not included in this version of the protocol, but could be designed into future versions.

This document describes how pledges discover (or are discovered by) an element of the network domain to which the pledge belongs that will perform the bootstrap. This element (device) is called the registrar. Before any other operation, pledge and registrar need to establish mutual trust:

1. Registrar authenticating the pledge: "Who is this device? What is its identity?"
2. Registrar authorizing the pledge: "Is it mine? Do I want it? What are the chances it has been compromised?"
3. Pledge authenticating the registrar: "What is this registrar’s identity?"
4. Pledge authorizing the registrar: "Should I join this network?"

This document details protocols and messages to answer the above questions. It uses a TLS connection and an PKIX-shaped (X.509v3) certificate (an IEEE 802.1AR [IDevID] IDDevID) of the pledge to answer points 1 and 2. It uses a new artifact called a "voucher" that the registrar receives from a "Manufacturer Authorized Signing Authority" (MASA) and passes to the pledge to answer points 3 and 4.
A proxy provides very limited connectivity between the pledge and the registrar.

The syntactic details of vouchers are described in detail in [RFC8366]. This document details automated protocol mechanisms to obtain vouchers, including the definition of a ‘voucher-request’ message that is a minor extension to the voucher format (see Section 3) defined by [RFC8366].

BRSKI results in the pledge storing an X.509 root certificate sufficient for verifying the registrar identity. In the process a TLS connection is established that can be directly used for Enrollment over Secure Transport (EST). In effect BRSKI provides an automated mechanism for the "Bootstrap Distribution of CA Certificates" described in [RFC7030] Section 4.1.1 wherein the pledge "MUST [...] engage a human user to authorize the CA certificate using out-of-band information". With BRSKI the pledge now can automate this process using the voucher. Integration with a complete EST enrollment is optional but trivial.

BRSKI is agile enough to support bootstrapping alternative key infrastructures, such as a symmetric key solutions, but no such system is described in this document.

1.1. Prior Bootstrapping Approaches

To literally "pull yourself up by the bootstraps" is an impossible action. Similarly the secure establishment of a key infrastructure without external help is also an impossibility. Today it is commonly accepted that the initial connections between nodes are insecure, until key distribution is complete, or that domain-specific keying material (often pre-shared keys, including mechanisms like SIM cards) is pre-provisioned on each new device in a costly and non-scalable manner. Existing automated mechanisms are known as non-secured 'Trust on First Use' (TOFU) [RFC7435], ‘resurrecting duckling’ [Stajano99theresurrecting] or ‘pre-staging’.

Another prior approach has been to try and minimize user actions during bootstrapping, but not eliminate all user-actions. The original EST protocol [RFC7030] does reduce user actions during bootstrap but does not provide solutions for how the following protocol steps can be made autonomic (not involving user actions):

- using the Implicit Trust Anchor [RFC7030] database to authenticate an owner specific service (not an autonomic solution because the URL must be securely distributed),
o engaging a human user to authorize the CA certificate using out-of-band data (not an autonomic solution because the human user is involved),

o using a configured Explicit TA database (not an autonomic solution because the distribution of an explicit TA database is not autonomic),

o and using a Certificate-Less TLS mutual authentication method (not an autonomic solution because the distribution of symmetric key material is not autonomic).

These "touch" methods do not meet the requirements for zero-touch.

There are "call home" technologies where the pledge first establishes a connection to a well known manufacturer service using a common client-server authentication model. After mutual authentication, appropriate credentials to authenticate the target domain are transferred to the pledge. This creates several problems and limitations:

o the pledge requires realtime connectivity to the manufacturer service,

o the domain identity is exposed to the manufacturer service (this is a privacy concern),

o the manufacturer is responsible for making the authorization decisions (this is a liability concern),

BRSKI addresses these issues by defining extensions to the EST protocol for the automated distribution of vouchers.

1.2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The following terms are defined for clarity:

domainID: The domain IDentity is a unique hash based upon the Registrar CA's certificate. Section 5.8.2 specifies how it is calculated.
drop-ship: The physical distribution of equipment containing the "factory default" configuration to a final destination. In zero-touch scenarios there is no staging or pre-configuration during drop-ship.

imprint: The process where a device obtains the cryptographic key material to identify and trust future interactions with a network. This term is taken from Konrad Lorenz’s work in biology with new ducklings: during a critical period, the duckling would assume that anything that looks like a mother duck is in fact their mother. An equivalent for a device is to obtain the fingerprint of the network’s root certification authority certificate. A device that imprints on an attacker suffers a similar fate to a duckling that imprints on a hungry wolf. Securely imprinting is a primary focus of this document [imprinting]. The analogy to Lorenz’s work was first noted in [Stajano99theresurrecting].

enrollment: The process where a device presents key material to a network and acquires a network-specific identity. For example when a certificate signing request is presented to a certification authority and a certificate is obtained in response.

Pledge: The prospective device, which has an identity installed at the factory.

Voucher: A signed artifact from the MASA that indicates to a pledge the cryptographic identity of the registrar it should trust. There are different types of vouchers depending on how that trust is asserted. Multiple voucher types are defined in [RFC8366]

Domain: The set of entities that share a common local trust anchor. This includes the proxy, registrar, Domain Certificate Authority, Management components and any existing entity that is already a member of the domain.

Domain CA: The domain Certification Authority (CA) provides certification functionalities to the domain. At a minimum it provides certification functionalities to a registrar and manages the private key that defines the domain. Optionally, it certifies all elements.

Join Registrar (and Coordinator): A representative of the domain that is configured, perhaps autonomically, to decide whether a new device is allowed to join the domain. The administrator of the domain interfaces with a "join registrar (and coordinator)" to control this process. Typically a join registrar is "inside" its domain. For simplicity this document often refers to this as just "registrar". Within [I-D.ietf-anima-reference-model] this is
referred to as the "join registrar autonomic service agent". Other communities use the abbreviation "JRC".

(Public) Key Infrastructure: The collection of systems and processes that sustain the activities of a public key system. The registrar acts as an [RFC5280] and [RFC5272] (see section 7) "Registration Authority".

Join Proxy: A domain entity that helps the pledge join the domain. A join proxy facilitates communication for devices that find themselves in an environment where they are not provided connectivity until after they are validated as members of the domain. For simplicity this document sometimes uses the term of 'proxy' to indicate the join proxy. The pledge is unaware that they are communicating with a proxy rather than directly with a registrar.

Circuit Proxy: A stateful implementation of the join proxy. This is the assumed type of proxy.

IPiP Proxy: A stateless proxy alternative.

MASA Service: A third-party Manufacturer Authorized Signing Authority (MASA) service on the global Internet. The MASA signs vouchers. It also provides a repository for audit-log information of privacy protected bootstrapping events. It does not track ownership.

MASA Audit-Log: A list of previous owners maintained by the MASA on a per device (per pledge) basis. Described in Section 5.8.1.

Ownership Tracker: An Ownership Tracker service on the global Internet. The Ownership Tracker uses business processes to accurately track ownership of all devices shipped against domains that have purchased them. Although optional, this component allows vendors to provide additional value in cases where their sales and distribution channels allow for accurately tracking of such ownership. Ownership tracking information is indicated in vouchers as described in [RFC8366]

IDevID: An Initial Device Identity X.509 certificate installed by the vendor on new equipment.

TOFU: Trust on First Use. Used similarly to [RFC7435]. This is where a pledge device makes no security decisions but rather simply trusts the first registrar it is contacted by. This is also known as the "resurrecting duckling" model.
nonce: a voucher (or request) that contains a nonce (the normal case).

onceless: a voucher (or request) that does not contain a nonce, relying upon accurate clocks for expiration, or which does not expire.

manufacturer: the term manufacturer is used throughout this document to be the entity that created the device. This is typically the "original equipment manufacturer" or OEM, but in more complex situations it could be a "value added retailer" (VAR), or possibly even a systems integrator. In general, it a goal of BRSKI to eliminate small distinctions between different sales channels. The reason for this is that it permits a single device, with a uniform firmware load, to be shipped directly to all customers. This eliminates costs for the manufacturer. This also reduces the number of products supported in the field increasing the chance that firmware will be more up to date.

ANI: The Autonomic Network Infrastructure as defined by [I-D.ietf-anima-reference-model]. This document details specific requirements for pledges, proxies and registrars when they are part of an ANI.

offline: When an architectural component cannot perform realtime communications with a peer, either due to network connectivity or because the peer is turned off, the operation is said to be occurring offline.

1.3. Scope of solution

1.3.1. Support environment

This solution (BRSKI) can support large router platforms with multi-gigabit inter-connections, mounted in controlled access data centers. But this solution is not exclusive to large equipment: it is intended to scale to thousands of devices located in hostile environments, such as ISP provided CPE devices which are drop-shipped to the end user. The situation where an order is fulfilled from distributed warehouse from a common stock and shipped directly to the target location at the request of a domain owner is explicitly supported. That stock ("SKU") could be provided to a number of potential domain owners, and the eventual domain owner will not know a-priori which device will go to which location.

The bootstrapping process can take minutes to complete depending on the network infrastructure and device processing speed. The network communication itself is not optimized for speed; for privacy reasons,
the discovery process allows for the pledge to avoid announcing its presence through broadcasting.

Nomadic or mobile devices often need to acquire credentials to access the network at the new location. An example of this is mobile phone roaming among network operators, or even between cell towers. This is usually called handoff. BRSKI does not provide a low-latency handoff which is usually a requirement in such situations. For these solutions BRSKI can be used to create a relationship (an LDevID) with the "home" domain owner. The resulting credentials are then used to provide credentials more appropriate for a low-latency handoff.

1.3.2. Constrained environments

Questions have been posed as to whether this solution is suitable in general for Internet of Things (IoT) networks. This depends on the capabilities of the devices in question. The terminology of [RFC7228] is best used to describe the boundaries.

The solution described in this document is aimed in general at non-constrained (i.e., class 2+ [RFC7228]) devices operating on a non-Challenged network. The entire solution as described here is not intended to be useable as-is by constrained devices operating on challenged networks (such as 802.15.4 LLNs).

Specifically, there are protocol aspects described here that might result in congestion collapse or energy-exhaustion of intermediate battery powered routers in an LLN. Those types of networks SHOULD NOT use this solution. These limitations are predominately related to the large credential and key sizes required for device authentication. Defining symmetric key techniques that meet the operational requirements is out-of-scope but the underlying protocol operations (TLS handshake and signing structures) have sufficient algorithm agility to support such techniques when defined.

The imprint protocol described here could, however, be used by non-energy constrained devices joining a non-constrained network (for instance, smart light bulbs are usually mains powered, and speak 802.11i). It could also be used by non-constrained devices across a non-energy constrained, but challenged network (such as 802.15.4). The certificate contents, and the process by which the four questions above are resolved do apply to constrained devices. It is simply the actual on-the-wire imprint protocol that could be inappropriate.
1.3.3. Network Access Controls

This document presumes that network access control has either already occurred, is not required, or is integrated by the proxy and registrar in such a way that the device itself does not need to be aware of the details. Although the use of an X.509 Initial Device Identity is consistent with IEEE 802.1AR [IDevID], and allows for alignment with 802.1X network access control methods, its use here is for pledge authentication rather than network access control. Integrating this protocol with network access control, perhaps as an Extensible Authentication Protocol (EAP) method (see [RFC3748]), is out-of-scope.

1.3.4. Bootstrapping is not Booting

This document describes "bootstrapping" as the protocol used to obtain a local trust anchor. It is expected that this trust anchor, along with any additional configuration information subsequently installed, is persisted on the device across system restarts ("booting"). Bootstrapping occurs only infrequently such as when a device is transferred to a new owner or has been reset to factory default settings.

1.4. Leveraging the new key infrastructure / next steps

As a result of the protocol described herein, the bootstrapped devices have the Domain CA trust anchor in common. An end entity certificate has optionally been issued from the Domain CA. This makes it possible to securely deploy functionalities across the domain, e.g:

- Device management.
- Routing authentication.
- Service discovery.

The major intended beneficiary is that it possible to use the credentials deployed by this protocol to secure the Autonomic Control Plane (ACP) ([I-D.ietf-anima-autonomic-control-plane]).

1.5. Requirements for Autonomic Network Infrastructure (ANI) devices

The BRSKI protocol can be used in a number of environments. Some of the options in this document are the result of requirements that are out of the ANI scope. This section defines the base requirements for ANI devices.
For devices that intend to become part of an Autonomic Network Infrastructure (ANI) ([I-D.ietf-anima-reference-model]) that includes an Autonomic Control Plane ([I-D.ietf-anima-autonomic-control-plane]), the BRSKI protocol MUST be implemented.

The pledge must perform discovery of the proxy as described in Section 4.1 using GRASP DULL [I-D.ietf-anima-grasp] M_FLOOD announcements.

Upon successfully validating a voucher artifact, a status telemetry MUST be returned. See Section 5.7.

An ANIMA ANI pledge MUST implement the EST automation extensions described in Section 5.9. They supplement the [RFC7030] EST to better support automated devices that do not have an end user.

The ANI Join Registrar Autonomic Service Agent (ASA) MUST support all the BRSKI and above listed EST operations.

All ANI devices SHOULD support the BRSKI proxy function, using circuit proxies over the ACP. (See Section 4.3)

2. Architectural Overview

The logical elements of the bootstrapping framework are described in this section. Figure 1 provides a simplified overview of the components.
We assume a multi-vendor network. In such an environment there could be a Manufacturer Service for each manufacturer that supports devices following this document’s specification, or an integrator could provide a generic service authorized by multiple manufacturers. It is unlikely that an integrator could provide Ownership Tracking services for multiple manufacturers due to the required sales channel integrations necessary to track ownership.

The domain is the managed network infrastructure with a Key Infrastructure the pledge is joining. The domain provides initial device connectivity sufficient for bootstrapping through a proxy. The domain registrar authenticates the pledge, makes authorization decisions, and distributes vouchers obtained from the Manufacturer Service. Optionally the registrar also acts as a PKI Certification Authority.

Figure 1: Architecture Overview
2.1. Behavior of a Pledge

The pledge goes through a series of steps, which are outlined here at a high level.

```
+-----------------+ (1) Discover
| rejected         |
+-----------------+ (2) Identity
| Request          |
| Join             |
+-----------------+ (3) Request
| Imprint          |
+-----------------+ (4) Imprint
| Enroll          |
| Failure          |
| Enrolled        |
+-----------------+ (5) Enroll
| Enrolled        |
+-----------------+ (non-error HTTP codes) (e.g. 202 'Retry-After')
|
```

Figure 2: Pledge State Diagram

State descriptions for the pledge are as follows:

1. Discover a communication channel to a registrar.
2. Identify itself. This is done by presenting an X.509 IDevID credential to the discovered registrar (via the proxy) in a TLS handshake. (The registrar credentials are only provisionally accepted at this time).

3. Request to join the discovered registrar. A unique nonce is included ensuring that any responses can be associated with this particular bootstrapping attempt.

4. Imprint on the registrar. This requires verification of the manufacturer service provided voucher. A voucher contains sufficient information for the pledge to complete authentication of a registrar. This document details this step in depth.

5. Enroll. After imprint an authenticated TLS (HTTPS) connection exists between pledge and registrar. Enrollment over Secure Transport (EST) [RFC7030] can then used to obtain a domain certificate from a registrar.

The pledge is now a member of, and can be managed by, the domain and will only repeat the discovery aspects of bootstrapping if it is returned to factory default settings.

This specification details integration with EST enrollment so that pledges can optionally obtain a locally issued certificate, although any REST interface could be integrated in future work.

2.2. Secure Imprinting using Vouchers

A voucher is a cryptographically protected artifact (using a digital signature) to the pledge device authorizing a zero-touch imprint on the registrar domain.

The format and cryptographic mechanism of vouchers is described in detail in [RFC8366].

Vouchers provide a flexible mechanism to secure imprinting: the pledge device only imprints when a voucher can be validated. At the lowest security levels the MASA can indiscriminately issue vouchers and log claims of ownership by domains. At the highest security levels issuance of vouchers can be integrated with complex sales channel integrations that are beyond the scope of this document. The sales channel integration would verify actual (legal) ownership of the pledge by the domain. This provides the flexibility for a number of use cases via a single common protocol mechanism on the pledge and registrar devices that are to be widely deployed in the field. The MASA services have the flexibility to leverage either the currently
defined claim mechanisms or to experiment with higher or lower security levels.

Vouchers provide a signed but non-encrypted communication channel among the pledge, the MASA, and the registrar. The registrar maintains control over the transport and policy decisions, allowing the local security policy of the domain network to be enforced.

2.3. Initial Device Identifier

Pledge authentication and pledge voucher-request signing is via a PKIX-shaped certificate installed during the manufacturing process. This is the 802.1AR Initial Device Identifier (IDevID), and it provides a basis for authenticating the pledge during the protocol exchanges described here. There is no requirement for a common root PKI hierarchy. Each device manufacturer can generate its own root certificate. Specifically, the IDevID enables:

1. Uniquely identifying the pledge by the Distinguished Name (DN) and subjectAltName (SAN) parameters in the IDevID. The unique identification of a pledge in the voucher objects are derived from those parameters as described below. Section 10.3 discussed privacy implications.

2. Provides a cryptographic authentication of the pledge to the Registrar (see Section 5.3).

3. Secure auto-discovery of the pledge’s MASA by the registrar (see Section 2.8).

4. Signing of voucher-request by the pledge’s IDevID (see Section 3).

5. Provides a cryptographic authentication of the pledge to the MASA (see Section 5.5.5).

Section 7.2.13 (2009 edition) and section 8.10.3 (2018 edition) of [IDevID] discusses keyUsage and extendedKeyUsage extensions in the IDevID certificate. Any restrictions included reduce the utility of the IDevID and so this specification RECOMMENDS that no key usage restrictions be included. Additionally, [RFC5280] section 4.2.1.3 does not require key usage restrictions for end entity certificates.

2.3.1. Identification of the Pledge

In the context of BRSKI, pledges have a 1:1 relationship with a "serial-number". This serial-number is used both in the "serial-
number" field of voucher or voucher-requests (see Section 3) and in local policies on registrar or MASA (see Section 5).

The serialNumber fields is defined in [RFC5280], and is a SHOULD field in [IDevID]. IDevID certificates for use with this protocol MUST include the "serialNumber" attribute with the device's unique serial number (from [IDevID] section 7.2.8, and [RFC5280] section 4.1.2.4's list of standard attributes).

The serialNumber field is used as follows by the pledge to build the "serial-number" that is placed in the voucher-request. In order to build it, the fields need to be converted into a serial-number of "type string".

An example of a printable form of the "serialNumber" field is provided in [RFC4519] section 2.31 ("WI-3005"). That section further provides equality and syntax attributes.

Due to the reality of existing device identity provisioning processes, some manufacturers have stored serial-numbers in other fields. Registrar’s SHOULD be configurable, on a per-manufacturer basis, to look for serial-number equivalents in other fields.

As explained in Section 5.5 the Registrar MUST extract the serial-number again itself from the pledge’s TLS certificate. It can consult the serial-number in the pledge-request if there are any possible confusion about the source of the serial-number.

2.3.2. MASA URI extension

This document defines a new PKIX non-critical certificate extension to carry the MASA URI. This extension is intended to be used in the IDevID certificate. The URI is represented as described in Section 7.4 of [RFC5280].

The URI provides the authority information. The BRSKI "/.well-known" tree ([RFC5785]) is described in Section 5.

A complete URI MAY be in this extension, including the ‘scheme’, ‘authority’, and ‘path’. The complete URI will typically be used in diagnostic or experimental situations. Typically, (and in consideration to constrained systems), this SHOULD be reduced to only the ‘authority’, in which case a scheme of "https://" ([RFC7230] section 2.7.3) and ‘path’ of "/.well-known/est" is to be assumed, as explained in Section 5.

The registrar can assume that only the ‘authority’ is present in the extension, if there are no slash ("/") characters in the extension.
Section 7.4 of [RFC5280] calls out various schemes that MUST be supported, including LDAP, HTTP and FTP. However, the registrar MUST use HTTPS for the BRSKI-MASA connection.

The new extension is identified as follows:

<CODE BEGINS>

MASAURLExtnModule-2016 { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-MASAURLExtn2016(TBD) }

DEFINITIONS IMPLICIT TAGS ::= BEGIN

-- EXPORTS ALL --

IMPORTS
EXTENSION
FROM PKIX-CommonTypes-2009
{ iso(1) identified-organization(3) dod(6) internet(1)
security(5) mechanisms(5) pkix(7) id-mod(0)
id-mod-pkixCommon-02(57) }

id-pe FROM PKIX1Explicit-2009
{ iso(1) identified-organization(3) dod(6) internet(1)
security(5) mechanisms(5) pkix(7) id-mod(0)
id-mod-pkix1-explicit-02(51) };

MASACertExtensions EXTENSION ::= { ext-MASAURL, ... }
ext-MASAURL EXTENSION ::= { SYNTAX MASAURLSyntax
IDENTIFIED BY id-pe-masa-url }

id-pe-masa-url OBJECT IDENTIFIER ::= { id-pe TBD }

MASAURLSyntax ::= IA5String

END

<CODE ENDS>

Figure 3: MASAURL ASN.1 Module

The choice of id-pe is based on guidance found in Section 4.2.2 of [RFC5280], "These extensions may be used to direct applications to on-line information about the issuer or the subject". The MASA URL is precisely that: online information about the particular subject.
2.4. Protocol Flow

A representative flow is shown in Figure 4
Figure 4: Protocol Time Sequence Diagram
On initial bootstrap, a new device (the pledge) uses a local service autodiscovery (GRASP or mDNS) to locate a join proxy. The join proxy connects the pledge to a local registrar (the JRC).

Having found a candidate registrar, the fledgling pledge sends some information about itself to the registrar, including its serial number in the form of a voucher request and its device identity certificate (IDevID) as part of the TLS session.

The registrar can determine whether it expected such a device to appear, and locates a MASA. The location of the MASA is usually found in an extension in the IDevID. Having determined that the MASA is suitable, the entire information from the initial voucher request (including device serial number) is transmitted over the internet in a TLS protected channel to the manufacturer, along with information about the registrar/owner.

The manufacturer can then apply policy based on the provided information, as well as other sources of information (such as sales records), to decide whether to approve the claim by the registrar to own the device; if the claim is accepted, a voucher is issued that directs the device to accept its new owner.

The voucher is returned to the registrar, but not immediately to the device -- the registrar has an opportunity to examine the voucher, the MASA’s audit-logs, and other sources of information to determine whether the device has been tampered with, and whether the bootstrap should be accepted.

No filtering of information is possible in the signed voucher, so this is a binary yes-or-no decision. If the registrar accepts the voucher as a proper one for its device, the voucher is returned to the pledge for imprinting.

The voucher also includes a trust anchor that the pledge uses as representing the owner. This is used to successfully bootstrap from an environment where only the manufacturer has built-in trust by the device into an environment where the owner now has a PKI footprint on the device.

When BRSKI is followed with EST this single footprint is further leveraged into the full owner’s PKI and a LDevID for the device. Subsequent reporting steps provide flows of information to indicate success/failure of the process.
2.5. Architectural Components

2.5.1. Pledge

The pledge is the device that is attempting to join. Until the pledge completes the enrollment process, it has link-local network connectivity only to the proxy.

2.5.2. Join Proxy

The join proxy provides HTTPS connectivity between the pledge and the registrar. A circuit proxy mechanism is described in Section 4. Additional mechanisms, including a CoAP mechanism and a stateless IP/IP mechanism are the subject of future work.

2.5.3. Domain Registrar

The domain's registrar operates as the BRSKI-MASA client when requesting vouchers from the MASA (see Section 5.4). The registrar operates as the BRSKI-EST server when pledges request vouchers (see Section 5.1). The registrar operates as the BRSKI-EST server "Registration Authority" if the pledge requests an end entity certificate over the BRSKI-EST connection (see Section 5.9).

The registrar uses an Implicit Trust Anchor database for authenticating the BRSKI-MASA TLS connection MASA certificate. The registrar uses a different Implicit Trust Anchor database for authenticating the BRSKI-EST TLS connection pledge client certificate. Configuration or distribution of these trust anchor databases is out-of-scope of this specification.

2.5.4. Manufacturer Service

The Manufacturer Service provides two logically separate functions: the Manufacturer Authorized Signing Authority (MASA) described in Section 5.5 and Section 5.6, and an ownership tracking/auditing function described in Section 5.7 and Section 5.8.

2.5.5. Public Key Infrastructure (PKI)

The Public Key Infrastructure (PKI) administers certificates for the domain of concern, providing the trust anchor(s) for it and allowing enrollment of pledges with domain certificates.

The voucher provides a method for the distribution of a single PKI trust anchor (as the "pinned-domain-cert"). A distribution of the full set of current trust anchors is possible using the optional EST integration.
The domain’s registrar acts as an [RFC5272] Registration Authority, requesting certificates for pledges from the Key Infrastructure.

The expectations of the PKI are unchanged from EST [RFC7030]. This document does not place any additional architectural requirements on the Public Key Infrastructure.

2.6. Certificate Time Validation

2.6.1. Lack of realtime clock

Many devices when bootstrapping do not have knowledge of the current time. Mechanisms such as Network Time Protocols cannot be secured until bootstrapping is complete. Therefore bootstrapping is defined with a framework that does not require knowledge of the current time. A pledge MAY ignore all time stamps in the voucher and in the certificate validity periods if it does not know the current time.

The pledge is exposed to dates in the following five places: registrar certificate notBefore, registrar certificate notAfter, voucher created-on, and voucher expires-on. Additionally, CMS signatures contain a signingTime.

A pledge with a real time clock in which it has confidence in, MUST check the above time fields in all certificates and signatures that it processes.

If the voucher contains a nonce then the pledge MUST confirm the nonce matches the original pledge voucher-request. This ensures the voucher is fresh. See Section 5.2.

2.6.2. Infinite Lifetime of IDevID

[RFC5280] explains that long lived pledge certificates "SHOULD be assigned the GeneralizedTime value of 99991231235959Z" for the notAfter field.

Some deployed IDevID management systems are not compliant with the 802.1AR requirement for infinite lifetimes, and put in typical <= 3 year certificate lifetimes. Registrars SHOULD be configurable on a per-manufacturer basis to ignore pledge lifetimes when they did not follow the RFC5280 recommendations.

2.7. Cloud Registrar

There exist operationally open networks wherein devices gain unauthenticated access to the Internet at large. In these use cases the management domain for the device needs to be discovered within
the larger Internet. The case where a device can boot and get access to larger Internet are less likely within the ANIMA ACP scope but may be more important in the future. In the ANIMA ACP scope, new devices will be quarantined behind a Join Proxy.

There are additionally some greenfield situations involving an entirely new installation where a device may have some kind of management uplink that it can use (such as via 3G network for instance). In such a future situation, the device might use this management interface to learn that it should configure itself to become the local registrar.

In order to support these scenarios, the pledge MAY contact a well known URI of a cloud registrar if a local registrar cannot be discovered or if the pledge’s target use cases do not include a local registrar.

If the pledge uses a well known URI for contacting a cloud registrar a manufacturer-assigned Implicit Trust Anchor database (see [RFC7030]) MUST be used to authenticate that service as described in [RFC6125]. This is consistent with the human user configuration of an EST server URI in [RFC7030] which also depends on RFC6125.

2.8. Determining the MASA to contact

The registrar needs to be able to contact a MASA that is trusted by the pledge in order to obtain vouchers. There are three mechanisms described:

The device’s Initial Device Identifier (IDevID) will normally contain the MASA URL as detailed in Section 2.3. This is the RECOMMENDED mechanism.

If the registrar is integrated with [RFC8520] and the pledge IDevID contains the id-pe-mud-url then the registrar MAY attempt to obtain the MASA URL from the MUD file. The MUD file extension for the MASA URL is defined in Appendix C.

It can be operationally difficult to ensure the necessary X.509 extensions are in the pledge’s IDevID due to the difficulty of aligning current pledge manufacturing with software releases and development. As a final fallback the registrar MAY be manually configured or distributed with a MASA URL for each manufacturer. Note that the registrar can only select the configured MASA URL based on the trust anchor -- so manufacturers can only leverage this approach if they ensure a single MASA URL works for all pledge’s associated with each trust anchor.
3. Voucher-Request artifact

Voucher-requests are how vouchers are requested. The semantics of the vouchers are described below, in the YANG model.

A pledge forms the "pledge voucher-request", signs it with it’s IDevID and submits it to the registrar.

The registrar in turn forms the "registrar voucher-request", signs it with it’s Registrar keypair and submits it to the MASA.

The "proximity-registrar-cert" leaf is used in the pledge voucher-requests. This provides a method for the pledge to assert the registrar’s proximity.

The "prior-signed-voucher-request" leaf is used in registrar voucher-requests. If present, it is the signed pledge voucher-request artifact. This provides a method for the registrar to forward the pledge’s signed request to the MASA. This completes transmission of the signed "proximity-registrar-cert" leaf.

Unless otherwise signaled (outside the voucher-request artifact), the signing structure is as defined for vouchers, see [RFC8366].

3.1. Nonceless Voucher Requests

A registrar MAY also retrieve nonceless vouchers by sending nonceless voucher-requests to the MASA in order to obtain vouchers for use when the registrar does not have connectivity to the MASA. No "prior-signed-voucher-request" leaf would be included. The registrar will also need to know the serial number of the pledge. This document does not provide a mechanism for the registrar to learn that in an automated fashion. Typically this will be done via scanning of barcode or QR-code on packaging, or via some sales channel integration.

3.2. Tree Diagram

The following tree diagram illustrates a high-level view of a voucher-request document. The voucher-request builds upon the voucher artifact described in [RFC8366]. The tree diagram is described in [RFC8340]. Each node in the diagram is fully described by the YANG module in Section 3.4. Please review the YANG module for a detailed description of the voucher-request format.
module: ietf-voucher-request

grouping voucher-request-grouping
  +---- voucher
    +---- created-on?                     yang:date-and-time
    +---- expires-on?                     yang:date-and-time
    +---- assertion?                     enumeration
    +---- serial-number                  string
    +---- idevid-issuer?                  binary
    +---- pinned-domain-cert?            binary
    +---- domain-cert-revocation-checks?  boolean
    +---- nonce?                         binary
    +---- last-renewal-date?              yang:date-and-time
    +---- prior-signed-voucher-request?   binary
    +---- proximity-registrar-cert?       binary

Figure 5: YANG Tree diagram for Voucher-Request

3.3. Examples

This section provides voucher-request examples for illustration purposes. The contents of the certificate have been elided to save space. For detailed examples, see Appendix D.2. These examples conform to the encoding rules defined in [RFC7951].

Example (1) The following example illustrates a pledge voucher-request. The assertion leaf is indicated as ‘proximity’ and the registrar’s TLS server certificate is included in the ‘proximity-registrar-cert’ leaf. See Section 5.2.

```json
{  "ietf-voucher-request:voucher": {    "assertion": "proximity",    "nonce": "62a2e7693d82fcda2624de58fb6722e5",    "serial-number": "JADA123456789",    "created-on": "2017-01-01T00:00:00.000Z",    "proximity-registrar-cert": "base64encodedvalue="  }
}
```

Figure 6: JSON representation of example Voucher-Request

Example (2) The following example illustrates a registrar voucher-request. The ‘prior-signed-voucher-request’ leaf is populated with the pledge’s voucher-request (such as the prior example). The pledge’s voucher-request is a binary CMS signed object. In the JSON encoding used...
here it must be base64 encoded. The nonce and assertion MAY be carried forward from the pledge request to the registrar request. The serial-number is extracted from the pledge’s Client Certificate from the TLS connection. See Section 5.5.

```

{
    "ietf-voucher-request:voucher": {
        "assertion": "proximity",
        "nonce": "62a2e7693d82fcda2624de58fb6722e5",
        "created-on": "2017-01-01T00:00:02.000Z",
        "idevid-issuer": "base64encodedvalue==
        "serial-number": "JADA123456789"
    }
}
```

Figure 7: JSON representation of example Prior-Signed Voucher-Request

Example (3) The following example illustrates a registrar voucher-request. The ‘prior-signed-voucher-request’ leaf is not populated with the pledge’s voucher-request nor is the nonce leaf. This form might be used by a registrar requesting a voucher when the pledge can not communicate with the registrar (such as when it is powered down, or still in packaging), and therefore could not submit a nonce. This scenario is most useful when the registrar is aware that it will not be able to reach the MASA during deployment. See Section 5.5.

```

{
    "ietf-voucher-request:voucher": {
        "created-on": "2017-01-01T00:00:02.000Z",
        "idevid-issuer": "base64encodedvalue==
        "serial-number": "JADA123456789"
    }
}
```

Figure 8: JSON representation of Offline Voucher-Request

3.4. YANG Module

Following is a YANG [RFC7950] module formally extending the [RFC8366] voucher into a voucher-request.

```
<CODE BEGINS> file "ietf-voucher-request@2018-02-14.yang"
module ietf-voucher-request {
  yang-version 1.1;


```
namespace
prefix "vch";

import ietf-restconf {
  prefix rc;
  description "This import statement is only present to access the yang-data extension defined in RFC 8040.";
  reference "RFC 8040: RESTCONF Protocol";
}

import ietf-voucher {
  prefix v;
  description "This module defines the format for a voucher, which is produced by a pledge’s manufacturer or delegate (MASA) to securely assign a pledge to an 'owner', so that the pledge may establish a secure connection to the owner’s network infrastructure";
  reference "RFC 8366: Voucher Profile for Bootstrapping Protocols";
}

organization "IETF ANIMA Working Group";

contact
"WG Web: <http://tools.ietf.org/wg/anima/>
WG List: <mailto:anima@ietf.org>
Author: Kent Watsen <mailto:kwatsen@juniper.net>
Author: Michael H. Behringer <mailto:Michael.H.Behringer@gmail.com>
Author: Toerless Eckert <mailto:ttef@cs.fau.de>
Author: Max Pritikin <mailto:pritikin@cisco.com>
Author: Michael Richardson <mailto:mcr+ietf@sandelman.ca>";

description
"This module defines the format for a voucher request. It is a superset of the voucher itself. It provides content to the MASA for consideration during a voucher request.

The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'NOT RECOMMENDED', 'MAY', and 'OPTIONAL' in this document are to be interpreted as
described in BCP 14 RFC2119 RFC8174 when, and only when, they appear in all capitals, as shown here.

Copyright (c) 2019 IETF Trust and the persons identified as authors of the code. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted pursuant to, and subject to the license terms contained in, the Simplified BSD License set forth in Section 4.c of the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info).

This version of this YANG module is part of RFC XXXX; see the RFC itself for full legal notices.

revision "2018-02-14" {
  description
  "Initial version";
  reference
  "RFC XXXX: Voucher Profile for Bootstrapping Protocols";
}

// Top-level statement
rc:yang-data voucher-request-artifact {
  uses voucher-request-grouping;
}

// Grouping defined for future usage
grouping voucher-request-grouping {
  description
  "Grouping to allow reuse/extensions in future work.";
  uses v:voucher-artifact-grouping {
    refine "voucher/created-on" {
      mandatory false;
    }
    refine "voucher/pinned-domain-cert" {
      mandatory false;
    }
    refine "voucher/domain-cert-revocation-checks" {
      description "The domain-cert-revocation-checks field is not valid in a voucher request, and any occurrence MUST be ignored";
    }
    refine "voucher/assertion" {

mandatory false;
description "Any assertion included in voucher requests SHOULD be ignored by the MASA."
};

augment "voucher" {
  description "Adds leaf nodes appropriate for requesting vouchers.";

  leaf prior-signed-voucher-request {
    type binary;
    description "If it is necessary to change a voucher, or re-sign and forward a voucher that was previously provided along a protocol path, then the previously signed voucher SHOULD be included in this field.

    For example, a pledge might sign a voucher request with a proximity-registrar-cert, and the registrar then includes it as the prior-signed-voucher-request field. This is a simple mechanism for a chain of trusted parties to change a voucher request, while maintaining the prior signature information.

    The Registrar and MASA MAY examine the prior signed voucher information for the purposes of policy decisions. For example this information could be useful to a MASA to determine that both pledge and registrar agree on proximity assertions. The MASA SHOULD remove all prior-signed-voucher-request information when signing a voucher for imprinting so as to minimize the final voucher size.";
  }

  leaf proximity-registrar-cert {
    type binary;
    description "An X.509 v3 certificate structure as specified by RFC 5280, Section 4 encoded using the ASN.1 distinguished encoding rules (DER), as specified in ITU-T X.690.

    The first certificate in the Registrar TLS server certificate_list sequence (the end-entity TLS certificate, see [RFC8446]) presented by the Registrar to the Pledge. This MUST be populated in a Pledge's voucher request when a proximity assertion is requested.";
  }
}
4. Proxying details (Pledge - Proxy - Registrar)

This section applies is normative for uses with an ANIMA ACP. The use of GRASP mechanism part of the ACP. Other users of BRSKI will need to define an equivalent proxy mechanism, and an equivalent mechanism to configure the proxy.

The role of the proxy is to facilitate communications. The proxy forwards packets between the pledge and a registrar that has been provisioned to the proxy via full GRASP ACP discovery.

This section defines a stateful proxy mechanism which is referred to as a "circuit" proxy. This is a form of Application Level Gateway ([RFC2663] section 2.9).

The proxy does not terminate the TLS handshake: it passes streams of bytes onward without examination. A proxy MUST NOT assume any specific TLS version. Please see ([RFC8446]) section 9.3 for details on TLS invariants.

A Registrar can directly provide the proxy announcements described below, in which case the announced port can point directly to the Registrar itself. In this scenario the pledge is unaware that there is no proxing occurring. This is useful for Registrars which are servicing pledges on directly connected networks.

As a result of the proxy Discovery process in Section 4.1.1, the port number exposed by the proxy does not need to be well known, or require an IANA allocation.

During the discovery of the Registrar by the Join Proxy, the Join Proxy will also learn which kinds of proxy mechanisms are available. This will allow the Join Proxy to use the lowest impact mechanism which the Join Proxy and Registrar have in common.

In order to permit the proxy functionality to be implemented on the maximum variety of devices the chosen mechanism should use the minimum amount of state on the proxy device. While many devices in the ANIMA target space will be rather large routers, the proxy...
The function is likely to be implemented in the control plane CPU of such a device, with available capabilities for the proxy function similar to many class 2 IoT devices.

The document [I-D.richardson-anima-state-for-joinrouter] provides a more extensive analysis and background of the alternative proxy methods.

4.1. Pledge discovery of Proxy

The result of discovery is a logical communication with a registrar, through a proxy. The proxy is transparent to the pledge. The communication between the pledge and Join Proxy is over IPv6 Link-Local addresses.

To discover the proxy the pledge performs the following actions:

1. MUST: Obtains a local address using IPv6 methods as described in [RFC4862] IPv6 Stateless Address AutoConfiguration. Use of [RFC4941] temporary addresses is encouraged. To limit pervasive monitoring ([RFC7258]), a new temporary address MAY use a short lifetime (that is, set TEMP_PREFERRED_LIFETIME to be short). Pledges will generally prefer use of IPv6 Link-Local addresses, and discovery of proxy will be by Link-Local mechanisms. IPv4 methods are described in Appendix A

2. MUST: Listen for GRASP M_FLOOD ([I-D.ietf-anima-grasp]) announcements of the objective: "AN_Proxy". See section Section 4.1.1 for the details of the objective. The pledge MAY listen concurrently for other sources of information, see Appendix B.

Once a proxy is discovered the pledge communicates with a registrar through the proxy using the bootstrapping protocol defined in Section 5.

While the GRASP M_FLOOD mechanism is passive for the pledge, the optional other methods (mDNS, and IPv4 methods) are active. The pledge SHOULD run those methods in parallel with listening to for the M_FLOOD. The active methods SHOULD back-off by doubling to a maximum of one hour to avoid overloading the network with discovery attempts. Detection of change of physical link status (Ethernet carrier for instance) SHOULD reset the back off timers.

The pledge could discover more than one proxy on a given physical interface. The pledge can have a multitude of physical interfaces as well; a layer-2/3 Ethernet switch may have hundreds of physical ports.
Each possible proxy offer SHOULD be attempted up to the point where a voucher is received: while there are many ways in which the attempt may fail, it does not succeed until the voucher has been validated.

The connection attempts via a single proxy SHOULD exponentially back-off to a maximum of one hour to avoid overloading the network infrastructure. The back-off timer for each MUST be independent of other connection attempts.

Connection attempts SHOULD be run in parallel to avoid head of queue problems wherein an attacker running a fake proxy or registrar could perform protocol actions intentionally slowly. Connection attempts to different proxies SHOULD be sent with an interval of 3 to 5s. The pledge SHOULD continue to listen to for additional GRASP M_FLOOD messages during the connection attempts.

Each connection attempt through a distinct Join Proxy MUST have a unique nonce in the voucher-request.

Once a connection to a registrar is established (e.g. establishment of a TLS session key) there are expectations of more timely responses, see Section 5.2.

Once all discovered services are attempted (assuming that none succeeded) the device MUST return to listening for GRASP M_FLOOD. It SHOULD periodically retry any manufacturer-specific mechanisms. The pledge MAY prioritize selection order as appropriate for the anticipated environment.

4.1.1. Proxy GRASP announcements

A proxy uses the DULL GRASP M_FLOOD mechanism to announce itself. This announcement can be within the same message as the ACP announcement detailed in [I-D.ietf-anima-autonomic-control-plane].

The formal CDDL [RFC8610] definition is:
flood-message = [M_FLOOD, session-id, initiator, ttl, 
+[objective, (locator-option / [])]]

objective = ["AN_Proxy", objective-flags, loop-count, 
objective-value]

ttl = 180000 ; 180,000 ms (3 minutes)
initiator = ACP address to contact Registrar
objective-flags = sync-only ; as in GRASP spec
sync-only = 4 ; M_FLOOD only requires synchronization
loop-count = 1 ; one hop only
objective-value = any ; none

locator-option = [0.IPv6_LOCATOR, ipv6-address, 
transport-proto, port-number]
ipv6-address = the v6 LL of the Proxy
$transport-proto /= IPPROTO_TCP ; note this can be any value from the
; IANA protocol registry, as per 
; [GRASP] section 2.9.5.1, note 3.
port-number = selected by Proxy

Figure 10: CDDL definition of Proxy Discovery message

Here is an example M_FLOOD announcing a proxy at fe80::1, on TCP port 4443.

[M_FLOOD, 12340815, h'fe800000000000000000000000000001', 180000, 
["AN_Proxy", 4, 1, "]
[O.IPv6_LOCATOR, 
h'fe800000000000000000000000000001', IPPROTO_TCP, 4443]]

Figure 11: Example of Proxy Discovery message

On a small network the Registrar MAY include the GRASP M_FLOOD 
announcements to locally connected networks.

The $transport-proto above indicates the method that the pledge-
proxy-registrar will use. The TCP method described here is 
mandatory, and other proxy methods, such as CoAP methods not defined 
in this document are optional. Other methods MUST NOT be enabled
unless the Join Registrar ASA indicates support for them in it’s own 
announcement.

4.2. CoAP connection to Registrar

The use of CoAP to connect from pledge to registrar is out of scope 
for this document, and is described in future work. See 
[I-D.ietf-anima-constrained-voucher].
4.3. Proxy discovery and communication of Registrar

The registrar SHOULD announce itself so that proxies can find it and determine what kind of connections can be terminated.

The registrar announces itself using ACP instance of GRASP using M_FLOOD messages. A registrar may announce any convenient port number, including using a stock port 443. ANI proxies MUST support GRASP discovery of registrars.

The M_FLOOD is formatted as follows:

```
[M_FLOOD, 12340815, h’fda379a6f6ee0000020000064000001’, 180000,
  ["AN_join_registrar", 4, 255, "EST-TLS"],
  [O_IPv6_LOCATOR,
    h’fda379a6f6ee0000020000064000001’, IPPROTO_TCP, 8443]]
```

Figure 12: An example of a Registrar announcement message

The formal CDDL definition is:

```
flood-message = [M_FLOOD, session-id, initiator, ttl,
  +[objective, (locator-option / [])]]
```

```
objective = ["AN_join_registrar", objective-flags, loop-count,
  objective-value]
```

```
initiator = ACP address to contact Registrar
objective-flags = sync-only ; as in GRASP spec
sync-only = 4 ; M_FLOOD only requires synchronization
loop-count = 255 ; mandatory maximum
objective-value = text ; name of the (list of) of supported
  protocols: "EST-TLS" for RFC7030.
```

Figure 13: CDDL definition for Registrar announcement message

The M_FLOOD message MUST be sent periodically. The default SHOULD be 60 seconds, the value SHOULD be operator configurable but SHOULD be not smaller than 60 seconds. The frequency of sending MUST be such that the aggregate amount of periodic M_FLOODs from all flooding sources cause only negligible traffic across the ACP.

Here are some examples of locators for illustrative purposes. Only the first one (\$transport-protocol = 6, TCP) is defined in this document and is mandatory to implement.

---

locator1 = [O_IPv6_LOCATOR, fd45:1345::6789, 6, 443]
locator2 = [O_IPv6_LOCATOR, fd45:1345::6789, 17, 5683]
locator3 = [O_IPv6_LOCATOR, fe80::1234, 41, nil]

A protocol of 6 indicates that TCP proxying on the indicated port is desired.

Registrars MUST announce the set of protocols that they support. They MUST support TCP traffic.

Registrars MUST accept HTTPS/EST traffic on the TCP ports indicated.

Registrars MUST support ANI TLS circuit proxy and therefore BRSKI across HTTPS/TLS native across the ACP.

In the ANI, the Autonomic Control Plane (ACP) secured instance of GRASP ([I-D.ietf-anima-grasp]) MUST be used for discovery of ANI registrar ACP addresses and ports by ANI proxies. The TCP leg of the proxy connection between ANI proxy and ANI registrar therefore also runs across the ACP.

5. Protocol Details (Pledge - Registrar - MASA)

The pledge MUST initiate BRSKI after boot if it is unconfigured. The pledge MUST NOT automatically initiate BRSKI if it has been configured or is in the process of being configured.

BRSKI is described as extensions to EST [RFC7030]. The goal of these extensions is to reduce the number of TLS connections and crypto operations required on the pledge. The registrar implements the BRSKI REST interface within the same "/.well-known" URI tree as the existing EST URIs as described in EST [RFC7030] section 3.2.2. The communication channel between the pledge and the registrar is referred to as "BRSKI-EST" (see Figure 1).

The communication channel between the registrar and MASA is similarly described as extensions to EST within the same "/.well-known" tree. For clarity this channel is referred to as "BRSKI-MASA". (See Figure 1).

The MASA URI is "https://" authority "/.well-known/est".

BRSKI uses existing CMS message formats for existing EST operations. BRSKI uses JSON [RFC8259] for all new operations defined here, and voucher formats.

While EST section 3.2 does not insist upon use of HTTP persistent connections, ([RFC7230] section 6.3) BRSKI-EST connections SHOULD use...
persistent connections. The intention of this guidance is to ensure the provisional TLS state occurs only once, and that the subsequent resolution of the provision state is not subject to a MITM attack during a critical phase.

If non-persistent connections are used, then both the pledge and the registrar MUST remember the certificates seen, and also sent for the first connection. They MUST check each subsequent connections for the same certificates, and each end MUST use the same certificates as well. This places a difficult restriction on rolling certificates on the Registrar.

Summarized automation extensions for the BRSKI-EST flow are:

- The pledge either attempts concurrent connections via each discovered proxy, or it times out quickly and tries connections in series, as explained at the end of Section 5.1.

- The pledge provisionally accepts the registrar certificate during the TLS handshake as detailed in Section 5.1.

- The pledge requests and validates a voucher using the new REST calls described below.

- The pledge completes authentication of the server certificate as detailed in Section 5.6.1. This moves the BRSKI-EST TLS connection out of the provisional state.

- Mandatory bootstrap steps conclude with voucher status telemetry (see Section 5.7).

The BRSKI-EST TLS connection can now be used for EST enrollment.

The extensions for a registrar (equivalent to EST server) are:

- Client authentication is automated using Initial Device Identity (IDevID) as per the EST certificate based client authentication. The subject field’s DN encoding MUST include the "serialNumber" attribute with the device’s unique serial number as explained in Section 2.3.1

- The registrar requests and validates the voucher from the MASA.

- The registrar forwards the voucher to the pledge when requested.

- The registrar performs log verifications in addition to local authorization checks before accepting optional pledge device enrollment requests.
5.1. BRSKI-EST TLS establishment details

The pledge establishes the TLS connection with the registrar through the circuit proxy (see Section 4) but the TLS handshake is with the registrar. The BRSKI-EST pledge is the TLS client and the BRSKI-EST registrar is the TLS server. All security associations established are between the pledge and the registrar regardless of proxy operations.

Establishment of the BRSKI-EST TLS connection is as specified in EST [RFC7030] section 4.1.1 "Bootstrap Distribution of CA Certificates" [RFC7030] wherein the client is authenticated with the IDevID certificate, and the EST server (the registrar) is provisionally authenticated with an unverified server certificate. Configuration or distribution of the trust anchor database used for validating the IDevID certificate is out-of-scope of this specification. Note that the trust anchors in/excluded from the database will affect which manufacturers’ devices are acceptable to the registrar as pledges, and can also be used to limit the set of MASAs that are trusted for enrollment.

The signatures in the certificate MUST be validated even if a signing key can not (yet) be validated. The certificate (or chain) MUST be retained for later validation.

A self-signed certificate for the Registrar is acceptable as the voucher will validate it.

The pledge performs input validation of all data received until a voucher is verified as specified in Section 5.6.1 and the TLS connection leaves the provisional state. Until these operations are complete the pledge could be communicating with an attacker.

The pledge code needs to be written with the assumption that all data is being transmitted at this point to an unauthenticated peer, and that received data, while inside a TLS connection, MUST be considered untrusted. This particularly applies to HTTP headers and CMS structures that make up the voucher.

A pledge that can connect to multiple registries concurrently SHOULD do so. Some devices may be unable to do so for lack of threading, or resource issues. Concurrent connections defeat attempts by a malicious proxy from causing a TCP Slowloris-like attack (see [slowloris]).

A pledge that can not maintain as many connections as there are eligible proxies will need to rotate among the various choices, terminating connections that do not appear to be making progress. If
no connection is making progress after 5 seconds then the pledge
SHOULD drop the oldest connection and go on to a different proxy: the
proxy that has been communicated with least recently. If there were
no other proxies discovered, the pledge MAY continue to wait, as long
as it is concurrently listening for new proxy announcements.

5.2. Pledge Requests Voucher from the Registrar

When the pledge bootstraps it makes a request for a voucher from a
registrar.

This is done with an HTTPS POST using the operation path value of
"/.well-known/est/requestvoucher".

The pledge voucher-request Content-Type is:

application/voucher-cms+json  [RFC8366] defines a "YANG-defined JSON
document that has been signed using a CMS structure", and the
voucher-request described in Section 3 is created in the same way.
The media type is the same as defined in [RFC8366]. and is also
used for the pledge voucher-request. The pledge MUST sign the
request using the Section 2.3 credential.

Registrar implementations SHOULD anticipate future media types but of
course will simply fail the request if those types are not yet known.

The pledge SHOULD include an [RFC7231] section 5.3.2 "Accept" header
field indicating the acceptable media type for the voucher response.
The "application/voucher-cms+json" media type is defined in [RFC8366]
but constrained voucher formats are expected in the future.
Registrars and MASA are expected to be flexible in what they accept.

The pledge populates the voucher-request fields as follows:

created-on:  Pledges that have a realtime clock are RECOMMENDED to
populate this field with the current date and time in yang:date-
and-time format. This provides additional information to the
MASA. Pledges that have no real-time clocks MAY omit this field.

nonce: The pledge voucher-request MUST contain a cryptographically
strong random or pseudo-random number nonce. (see [RFC4086]) Doing
so ensures Section 2.6.1 functionality. The nonce MUST NOT be
reused for multiple bootstrapping attempts. (The registrar
voucher-request MAY omit the nonce as per Section 3.1)

proximity-registrar-cert: In a pledge voucher-request this is the
first certificate in the TLS server ‘certificate_list’ sequence
(see [RFC5246]) presented by the registrar to the pledge. That
is, it is the end-entity certificate. This MUST be populated in a pledge voucher-request if the "proximity" assertion is populated.

All other fields MAY be omitted in the pledge voucher-request.

An example JSON payload of a pledge voucher-request is in Section 3.3 Example 1.

The registrar confirms that the assertion is 'proximity' and that pinned 'proximity-registrar-cert' is the Registrar’s certificate. If this validation fails, then there a On-Path Attacker (MITM), and the connection MUST be closed after the returning an HTTP 401 error code.

5.3. Registrar Authorization of Pledge

In a fully automated network all devices must be securely identified and authorized to join the domain.

A Registrar accepts or declines a request to join the domain, based on the authenticated identity presented. For different networks, examples of Automated acceptance may include:

- allow any device of a specific type (as determined by the X.509 IDevID),
- allow any device from a specific vendor (as determined by the X.509 IDevID),
- allow a specific device from a vendor (as determined by the X.509 IDevID) against a domain white list. (The mechanism for checking a shared white list potentially used by multiple Registrars is out of scope).

If validation fails the registrar SHOULD respond with the HTTP 404 error code. If the voucher-request is in an unknown format, then an HTTP 406 error code is more appropriate. A situation that could be resolved with administrative action (such as adding a vendor to a whitelist) MAY be responded with an 403 HTTP error code.

If authorization is successful the registrar obtains a voucher from the MASA service (see Section 5.5) and returns that MASA signed voucher to the pledge as described in Section 5.6.

5.4. BRSKI-MASA TLS establishment details

The BRSKI-MASA TLS connection is a 'normal' TLS connection appropriate for HTTPS REST interfaces. The registrar initiates the connection and uses the MASA URL obtained as described in
Section 2.8. The mechanisms in [RFC6125] SHOULD be used for authentication of the MASA. Some vendors will establish explicit (or private) trust anchors for validating their MASA; this will typically be done as part of a sales channel integration.

As described in [RFC7030], the MASA and the registrars SHOULD be prepared to support TLS client certificate authentication and/or HTTP Basic or Digest authentication. This connection MAY also have no client authentication at all.

Registrars SHOULD permit trust anchors to be pre-configured on a per-vendor(MASA) basis. Registrars SHOULD include the ability to configure a TLS ClientCertificate on a per-MASA basis, or to use no client certificate. Registrars SHOULD also permit an HTTP Basic and Digest authentication to be configured.

The authentication of the BRSKI-MASA connection does not change the voucher-request process, as voucher-requests are already signed by the registrar. Instead, this authentication provides access control to the audit-log as described in Section 5.8.

Implementors are advised that contacting the MASA is to establish a secured REST connection with a web service and that there are a number of authentication models being explored within the industry. Registrars are RECOMMENDED to fail gracefully and generate useful administrative notifications or logs in the advent of unexpected HTTP 401 (Unauthorized) responses from the MASA.

5.4.1. MASA authentication of customer Registrar

Providing per-customer options requires that the customer’s registrar be uniquely identified. This can be done by any stateless method that HTTPS supports: such as with HTTP Basic or Digest authentication (that is using a password), but the use of TLS Client Certificate authentication is RECOMMENDED.

Stateful methods involving API tokens, or HTTP Cookies are not recommended.

It is expected that the setup and configuration of per-customer Client Certificates is done as part of a sales ordering process.

The use of public PKI (i.e. WebPKI) End-Entity Certificates to identify the Registrar is reasonable, and if done universally this would permit a MASA to identify a customers’ Registrar simply by a FQDN.
The use of DANE records in DNSSEC signed zones would also permit use of a FQDN to identify customer Registrars.

A third (and simplest, but least flexible) mechanism would be for the MASA to simply store the Registrar’s certificate pinned in a database.

A MASA without any supply chain integration can simply accept Registrars without any authentication, or can accept them on a blind Trust-on-First-Use basis as described in Section 7.4.2.

This document does not make a specific recommendation as there is likely different tradeoffs in different environments and product values. Even within the ANIMA ACP applicability, there is a significant difference between supply chain logistics for $100 CPE devices and $100,000 core routers.

### 5.5. Registrar Requests Voucher from MASA

When a registrar receives a pledge voucher-request it in turn submits a registrar voucher-request to the MASA service via an HTTPS interface ([RFC7231]).

This is done with an HTTP POST using the operation path value of "/.well-known/est/requestvoucher".

The voucher media type "application/voucher-cms+json" is defined in [RFC8366] and is also used for the registrar voucher-request. It is a JSON document that has been signed using a CMS structure. The registrar MUST sign the registrar voucher-request. The entire registrar certificate chain, up to and including the Domain CA, MUST be included in the CMS structure.

MASA implementations SHOULD anticipate future media types but of course will simply fail the request if those types are not yet known.

The Registrar SHOULD include an [RFC7231] section 5.3.2 "Accept" header field indicating the response media types that are acceptable. This list SHOULD be the entire list presented to the Registrar in the Pledge’s original request (see Section 5.2) but MAY be a subset. MASA’s are expected to be flexible in what they accept.

The registrar populates the voucher-request fields as follows:

- **created-on**: The Registrars SHOULD populate this field with the current date and time when the Registrar formed this voucher request. This field provides additional information to the MASA.
nonce: This value, if present, is copied from the pledge voucher-request. The registrar voucher-request MAY omit the nonce as per Section 3.1.

serial-number: The serial number of the pledge the registrar would like a voucher for. The registrar determines this value by parsing the authenticated pledge IDevID certificate. See Section 2.3. The registrar MUST verify that the serial number field it parsed matches the serial number field the pledge provided in its voucher-request. This provides a sanity check useful for detecting error conditions and logging. The registrar MUST NOT simply copy the serial number field from a pledge voucher request as that field is claimed but not certified.

idevid-issuer: The Issuer value from the pledge IDevID certificate is included to ensure a uniqueness of the serial-number. In the case of nonceless (offline) voucher-request, then an appropriate value needs to be configured from the same out-of-band source as the serial-number.

prior-signed-voucher-request: The signed pledge voucher-request SHOULD be included in the registrar voucher-request. The entire CMS signed structure is to be included, base64 encoded for transport in the JSON structure.

A nonceless registrar voucher-request MAY be submitted to the MASA. Doing so allows the registrar to request a voucher when the pledge is offline, or when the registrar anticipates not being able to connect to the MASA while the pledge is being deployed. Some use cases require the registrar to learn the appropriate IDevID SerialNumber field and appropriate 'Accept header field' values from the physical device labeling or from the sales channel (out-of-scope for this document).

All other fields MAY be omitted in the registrar voucher-request.

The "proximity-registrar-cert" field MUST NOT be present in the registrar voucher-request.

Example JSON payloads of registrar voucher-requests are in Section 3.3 Examples 2 through 4.

The MASA verifies that the registrar voucher-request is internally consistent but does not necessarily authenticate the registrar certificate since the registrar MAY not be known to the MASA in advance. The MASA performs the actions and validation checks described in the following sub-sections before issuing a voucher.
5.5.1. MASA renewal of expired vouchers

As described in [RFC8366] vouchers are normally short lived to avoid revocation issues. If the request is for a previous (expired) voucher using the same registrar (that is, a Registrar with the same Domain CA) then the request for a renewed voucher SHOULD be automatically authorized. The MASA has sufficient information to determine this by examining the request, the registrar authentication, and the existing audit-log. The issuance of a renewed voucher is logged as detailed in Section 5.6.

To inform the MASA that existing vouchers are not to be renewed one can update or revoke the registrar credentials used to authorize the request (see Section 5.5.4 and Section 5.5.3). More flexible methods will likely involve sales channel integration and authorizations (details are out-of-scope of this document).

5.5.2. MASA pinning of registrar

The registrar’s certificate chain is extracted from the signature method. The entire registrar certificate chain was included in the CMS structure, as specified in Section 5.5. This CA certificate will be used to populate the "pinned-domain-cert" of the voucher being issued.

If this domain CA is unknown to the MASA, then it is to be considered a temporary trust anchor for the rest of the steps in this section. The intention is not to authenticate the message as having come from a fully validated origin, but to establish the consistency of the domain PKI.

5.5.3. MASA checking of voucher request signature

As described in Section 5.5.2, the MASA has extracted Registrar’s domain CA. This is used to validate the CMS signature ([RFC5652]) on the voucher-request.

Normal PKIX revocation checking is assumed during voucher-request signature validation. This CA certificate MAY have Certificate Revocation List distribution points, or Online Certificate Status Protocol (OCSP) information ([RFC6960]). If they are present, the MASA MUST be able to reach the relevant servers belonging to the Registrar’s domain CA to perform the revocation checks.

The use of OCSP Stapling is preferred.
5.5.4. MASA verification of domain registrar

The MASA MUST verify that the registrar voucher-request is signed by a registrar. This is confirmed by verifying that the id-kp-cmcRA extended key usage extension field (as detailed in EST RFC7030 section 3.6.1) exists in the certificate of the entity that signed the registrar voucher-request. This verification is only a consistency check that the unauthenticated domain CA intended the voucher-request signer to be a registrar. Performing this check provides value to the domain PKI by assuring the domain administrator that the MASA service will only respect claims from authorized Registration Authorities of the domain.

Even when a domain CA is authenticated to the MASA, and there is strong sales channel integration to understand who the legitimate owner is, the above cmcRC check prevents arbitrary End-Entity certificates (such as an LDevID certificate) from having vouchers issued against them.

Other cases of inappropriate voucher issuance are detected by examination of the audit log.

If a nonceless voucher-request is submitted the MASA MUST authenticate the registrar as described in either EST [RFC7030] section 3.2.3, section 3.3.2, or by validating the registrar’s certificate used to sign the registrar voucher-request using a configured trust anchor. Any of these methods reduce the risk of DDoS attacks and provide an authenticated identity as an input to sales channel integration and authorizations (details are out-of-scope of this document).

In the nonced case, validation of the Registrar’s identity (via TLS Client Certificate or HTTP authentication) MAY be omitted if the device policy is to accept audit-only vouchers.

5.5.5. MASA verification of pledge prior-signed-voucher-request

The MASA MAY verify that the registrar voucher-request includes the ‘prior-signed-voucher-request’ field. If so the prior-signed-voucher-request MUST include a ‘proximity-registrar-cert’ that is consistent with to the certificate used to sign the registrar voucher-request. Additionally the voucher-request serial-number leaf MUST match the pledge serial-number that the MASA extracts from the signing certificate of the prior-signed-voucher-request. The consistency check described above is checking that the ‘proximity-registrar-cert’ SPKI fingerprint exists within the registrar voucher-request CMS signature’s certificate chain. This is substantially the
same as the pin validation described in in [RFC7469] section 2.6, paragraph three.

If these checks succeed the MASA updates the voucher and audit-log assertion leafs with the "proximity" assertion.

5.5.6. MASA nonce handling

The MASA does not verify the nonce itself. If the registrar voucher-request contains a nonce, and the prior-signed-voucher-request exists, then the MASA MUST verify that the nonce is consistent. (Recall from above that the voucher-request might not contain a nonce, see Section 5.5 and Section 5.5.4).

The MASA populates the audit-log with the nonce that was verified. If a nonceless voucher is issued, then the audit-log is to be populated with the JSON value "null".

5.6. MASA and Registrar Voucher Response

The MASA voucher response to the registrar is forwarded without changes to the pledge; therefore this section applies to both the MASA and the registrar. The HTTP signaling described applies to both the MASA and registrar responses.

When a voucher request arrives at the registrar, if it has a cached response from the MASA for the corresponding registrar voucher-request, that cached response can be used according to local policy; otherwise the registrar constructs a new registrar voucher-request and sends it to the MASA.

Registrar evaluation of the voucher itself is purely for transparency and audit purposes to further inform log verification (see Section 5.8.3) and therefore a registrar could accept future voucher formats that are opaque to the registrar.

If the voucher-request is successful, the server (MASA responding to registrar or registrar responding to pledge) response MUST contain an HTTP 200 response code. The server MUST answer with a suitable 4xx or 5xx HTTP [RFC7230] error code when a problem occurs. In this case, the response data from the MASA MUST be a plaintext human-readable (UTF-8) error message containing explanatory information describing why the request was rejected.

The registrar MAY respond with an HTTP 202 ("the request has been accepted for processing, but the processing has not been completed") as described in EST [RFC7030] section 4.2.3 wherein the client "MUST wait at least the specified 'Retry-After' time before repeating the
same request". (see [RFC7231] section 6.6.4) The pledge is RECOMMENDED to provide local feedback (blinded LED etc) during this wait cycle if mechanisms for this are available. To prevent an attacker registrar from significantly delaying bootstrapping the pledge MUST limit the ‘Retry-After’ time to 60 seconds. Ideally the pledge would keep track of the appropriate Retry-After header field values for any number of outstanding registrars but this would involve a state table on the pledge. Instead the pledge MAY ignore the exact Retry-After value in favor of a single hard coded value (a registrar that is unable to complete the transaction after the first 60 seconds has another chance a minute later). A pledge SHOULD only maintain a 202 retry-state for up to 4 days, which is longer than a long weekend, after which time the enrollment attempt fails and the pledge returns to discovery state.

A pledge that retries a request after receiving a 202 message MUST resend the same voucher-request. It MUST NOT sign a new voucher-request each time, and in particular, it MUST NOT change the nonce value.

In order to avoid infinite redirect loops, which a malicious registrar might do in order to keep the pledge from discovering the correct registrar, the pledge MUST NOT follow more than one redirection (3xx code) to another web origins. EST supports redirection but requires user input; this change allows the pledge to follow a single redirection without a user interaction.

A 403 (Forbidden) response is appropriate if the voucher-request is not signed correctly, stale, or if the pledge has another outstanding voucher that cannot be overridden.

A 404 (Not Found) response is appropriate when the request is for a device that is not known to the MASA.

A 406 (Not Acceptable) response is appropriate if a voucher of the desired type or using the desired algorithms (as indicated by the Accept: header fields, and algorithms used in the signature) cannot be issued such as because the MASA knows the pledge cannot process that type. The registrar SHOULD use this response if it determines the pledge is unacceptable due to inventory control, MASA audit-logs, or any other reason.

A 415 (Unsupported Media Type) response is appropriate for a request that has a voucher-request or Accept: value that is not understood.

The voucher response format is as indicated in the submitted Accept header fields or based on the MASA’s prior understanding of proper format for this Pledge. Only the [RFC8366] "application/voucher-
The syntactic details of vouchers are described in detail in [RFC8366]. Figure 14 shows a sample of the contents of a voucher.

```json
{
  "ietf-voucher:voucher": {
    "nonce": "62a2e7693d82fcda2624de58fb6722e5",
    "assertion": "logging",
    "pinned-domain-cert": "base64encodedvalue==",
    "serial-number": "JADA123456789"
  }
}
```

Figure 14: An example voucher

The MASA populates the voucher fields as follows:

nonce: The nonce from the pledge if available. See Section 5.5.6.

assertion: The method used to verify the relationship between pledge and registrar. See Section 5.5.5.

pinned-domain-cert: The domain CA cert. See Section 5.5.2. This figure is illustrative, for an example, see Appendix D.2

serial-number: The serial-number as provided in the voucher-request. Also see Section 5.5.5.

domain-cert-revocation-checks: Set as appropriate for the pledge’s capabilities and as documented in [RFC8366]. The MASA MAY set this field to ‘false’ since setting it to ‘true’ would require that revocation information be available to the pledge and this document does not make normative requirements for [RFC6961] or equivalent integrations.

expires-on: This is set for nonceless vouchers. The MASA ensures the voucher lifetime is consistent with any revocation or pinned-domain-cert consistency checks the pledge might perform. See section Section 2.6.1. There are three times to consider: (a) a configured voucher lifetime in the MASA, (b) the expiry time for the registrar’s certificate, (c) any certificate revocation information (CRL) lifetime. The expires-on field SHOULD be before the earliest of these three values. Typically (b) will be some significant time in the future, but (c) will typically be short (on the order of a week or less). The RECOMMENDED period for (a) is on the order of 20 minutes, so it will typically determine the lifespan of the resulting voucher. 20 minutes is sufficient time to reach the post-provisional state in the pledge, at which point
there is an established trust relationship between pledge and registrar. The subsequent operations can take as long as required from that point onwards. The lifetime of the voucher has no impact on the lifespan of the ownership relationship.

Whenever a voucher is issued the MASA MUST update the audit-log sufficiently to generate the response as described in Section 5.8.1. The internal state requirements to maintain the audit-log are out-of-scope.

5.6.1. Pledge voucher verification

The pledge MUST verify the voucher signature using the manufacturer installed trust anchor(s) associated with the manufacturer’s MASA (this is likely included in the pledge’s firmware). Management of the manufacturer installed trust anchor(s) is out-of-scope of this document; this protocol does not update these trust anchor(s).

The pledge MUST verify the serial-number field of the signed voucher matches the pledge’s own serial-number.

The pledge MUST verify that the voucher nonce field is accurate and matches the nonce the pledge submitted to this registrar, or that the voucher is nonceless (see Section 7.2).

The pledge MUST be prepared to parse and fail gracefully from a voucher response that does not contain a ‘pinned-domain-cert’ field. Such a thing indicates a failure to enroll in this domain, and the pledge MUST attempt joining with other available Join Proxy.

The pledge MUST be prepared to ignore additional fields that it does not recognize.

5.6.2. Pledge authentication of provisional TLS connection

The ‘pinned-domain-cert’ element of the voucher contains the domain CA’s public key. The pledge MUST use the ‘pinned-domain-cert’ trust anchor to immediately complete authentication of the provisional TLS connection.

If a registrar’s credentials cannot be verified using the pinned-domain-cert trust anchor from the voucher then the TLS connection is immediately discarded and the pledge abandons attempts to bootstrap with this discovered registrar. The pledge SHOULD send voucher status telemetry (described below) before closing the TLS connection. The pledge MUST attempt to enroll using any other proxies it has found. It SHOULD return to the same proxy again after unsuccessful attempts with other proxies. Attempts should be made repeated at
intervals according to the backoff timer described earlier. Attempts
SHOULD be repeated as failure may be the result of a temporary
inconsistently (an inconsistently rolled registrar key, or some other
mis-configuration). The inconsistently could also be the result an
active MITM attack on the EST connection.

The registrar MUST use a certificate that chains to the pinned-
domain-cert as its TLS server certificate.

The pledge’s PKIX path validation of a registrar certificate’s
validity period information is as described in Section 2.6.1. Once
the PKIX path validation is successful the TLS connection is no
longer provisional.

The pinned-domain-cert MAY be installed as an trust anchor for future
operations such as enrollment (e.g. [RFC7030] as recommended) or
trust anchor management or raw protocols that do not need full PKI
based key management. It can be used to authenticate any dynamically
discovered EST server that contain the id-kp-cmcRA extended key usage
extension as detailed in EST RFC7030 section 3.6.1; but to reduce
system complexity the pledge SHOULD avoid additional discovery
operations. Instead the pledge SHOULD communicate directly with the
registrar as the EST server. The ‘pinned-domain-cert’ is not a
complete distribution of the [RFC7030] section 4.1.3 CA Certificate
Response, which is an additional justification for the recommendation
to proceed with EST key management operations. Once a full CA
Certificate Response is obtained it is more authoritative for the
domain than the limited ‘pinned-domain-cert’ response.

5.7. Pledge BRSKI Status Telemetry

The domain is expected to provide indications to the system
administrators concerning device lifecycle status. To facilitate
this it needs telemetry information concerning the device’s status.

To indicate pledge status regarding the voucher, the pledge MUST post
a status message to the Registrar.

The posted data media type: application/json

The client HTTP POSTs the following to the server at the URI ".well-
known/est/voucher_status".

The format and semantics described below are for version 1. A
version field is included to permit significant changes to this
feedback in the future. A Registrar that receives a status message
with a version larger than it knows about SHOULD log the contents and
alert a human.
The Status field indicates if the voucher was acceptable. Boolean values are acceptable.

If the voucher was not acceptable the Reason string indicates why. In the failure case this message may be sent to an unauthenticated, potentially malicious registrar and therefore the Reason string SHOULD NOT provide information beneficial to an attacker. The operational benefit of this telemetry information is balanced against the operational costs of not recording that an voucher was ignored by a client the registrar expected to continue joining the domain.

The reason-context attribute is an arbitrary JSON object (literal value or hash of values) which provides additional information specific to this pledge. The contents of this field are not subject to standardization.

The version, and status fields MUST be present. The Reason field SHOULD be present whenever the status field is negative. The Reason-Context field is optional.

The keys to this JSON hash are case-insensitive. Figure 15 shows an example JSON.

```json
{
    "version":"1",
    "status":false,
    "reason":"Informative human readable message",
    "reason-context": { "additional" : "JSON" }
}
```

Figure 15: Example Status Telemetry

The server SHOULD respond with an HTTP 200 but MAY simply fail with an HTTP 404 error. The client ignores any response. Within the server logs the server SHOULD capture this telemetry information.

Additional standard JSON fields in this POST MAY be added, see Section 8.4. A server that sees unknown fields should log them, but otherwise ignore them.

5.8. Registrar audit-log request

After receiving the pledge status telemetry Section 5.7, the registrar SHOULD request the MASA audit-log from the MASA service.

This is done with an HTTP POST using the operation path value of "/.well-known/est/requestauditlog".
The registrar SHOULD HTTP POST the same registrar voucher-request as it did when requesting a voucher (using the same Content-Type). It is posted to the /requestauditlog URI instead. The "idevid-issuer" and "serial-number" informs the MASA which log is requested so the appropriate log can be prepared for the response. Using the same media type and message minimizes cryptographic and message operations although it results in additional network traffic. The relying MASA implementation MAY leverage internal state to associate this request with the original, and by now already validated, voucher-request so as to avoid an extra crypto validation.

A registrar MAY request logs at future times. If the registrar generates a new request then the MASA is forced to perform the additional cryptographic operations to verify the new request.

A MASA that receives a request for a device that does not exist, or for which the requesting owner was never an owner returns an HTTP 404 ("Not found") code.

It is reasonable for a Registrar, that the MASA does not believe to be the current owner, to request the audit-log. There are probably reasons for this which are hard to predict in advance. For instance, such a registrar may not be aware that the device has been resold; it may be that the device has been resold inappropriately, and this is how the original owner will learn of the occurrence. It is also possible that the device legitimately spends time in two different networks.

Rather than returning the audit-log as a response to the POST (with a return code 200), the MASA MAY instead return a 201 ("Created") response ([RFC7231] sections 6.3.2 and 7.1), with the URL to the prepared (and idempotent, therefore cachable) audit response in the Location: header field.

In order to avoid enumeration of device audit-logs, MASA that return URLs SHOULD take care to make the returned URL unguessable. [W3C.WD-capability-urls-20140218] provides very good additional guidance. For instance, rather than returning URLs containing a database number such as https://example.com/auditlog/1234 or the EUI of the device such https://example.com/auditlog/10-00-00-11-22-33, the MASA SHOULD return a randomly generated value (a "slug" in web parlance). The value is used to find the relevant database entry.

A MASA that returns a code 200 MAY also include a Location: header for future reference by the registrar.
5.8.1. MASA audit log response

A log data file is returned consisting of all log entries associated with the device selected by the IDevID presented in the request. The audit log may be abridged by removal of old or repeated values as explained below. The returned data is in JSON format ([RFC8259]), and the Content-Type SHOULD be "application/json". For example:

```
{
  "version": "1",
  "events": [
    
    "date": "<date/time of the entry>",
    "domainID": "<domainID extracted from voucher-request>",
    "nonce": "<any nonce if supplied (or NULL)>",
    "assertion": "<the value from the voucher assertion leaf>",
    "truncated": "<the number of domainID entries truncated>",
  
    "date": "<date/time of the entry>",
    "domainID": "<anotherDomainID extracted from voucher-request>",
    "nonce": "<any nonce if supplied (or NULL)>",
    "assertion": "<the value from the voucher assertion leaf>",
  
  ]

  "truncation": {
    "nonced duplicates": "<total number of entries truncated>",
    "nonceless duplicates": "<total number of entries truncated>",
    "arbitrary": "<number of domainID entries removed entirely>",
  }
```

Figure 16: Example of audit-log response

The domainID is a binary value calculated SubjectKeyIdentifier according to Section 5.8.2. It is encoded once in base64 in order to be transported in this JSON container.

Distribution of a large log is less than ideal. This structure can be optimized as follows: Nonced or Nonceless entries for the same domainID MAY be abridged from the log leaving only the single most recent nonced or nonceless entry for that domainID. In the case of truncation the ‘event’ truncation value SHOULD contain a count of the number of events for this domainID that were omitted. The log SHOULD NOT be further reduced but there could exist operational situation where maintaining the full log is not possible. In such situations the log MAY be arbitrarily abridged for length, with the number of removed entries indicated as ‘arbitrary’.
If the truncation count exceeds 1024 then the MASA MAY use this value without further incrementing it.

A log where duplicate entries for the same domain have been omitted ("nonced duplicates" and/or "nonceless duplicates) could still be acceptable for informed decisions. A log that has had "arbitrary" truncations is less acceptable but manufacturer transparency is better than hidden truncations.

A registrar that sees a version value greater than 1 indicates an audit log format that has been enhanced with additional information. No information will be removed in future versions; should an incompatible change be desired in the future, then a new HTTP end point will be used.

This document specifies a simple log format as provided by the MASA service to the registrar. This format could be improved by distributed consensus technologies that integrate vouchers with technologies such as block-chain or hash trees or optimized logging approaches. Doing so is out of the scope of this document but is an anticipated improvement for future work. As such, the registrar SHOULD anticipate new kinds of responses, and SHOULD provide operator controls to indicate how to process unknown responses.

5.8.2. Calculation of domainID

The domainID is a binary value (a BIT STRING) that uniquely identifies a Registrar by the "pinned-domain-cert"

If the "pinned-domain-cert" certificate includes the SubjectKeyIdentifier (Section 4.2.1.2 [RFC5280]), then it is to be used as the domainID. If not, then it is the SPKI Fingerprint as described in [RFC7469] section 2.4 is to be used. This value needs to be calculated by both MASA (to populate the audit-log), and by the Registrar (to recognize itself).

[RFC5280] section 4.2.1.2 does not mandate that the SubjectKeyIdentifier extension be present in non-CA certificates. It is RECOMMENDED that Registrar certificates (even if self-signed), always include the SubjectKeyIdentifier to be used as a domainID.

The domainID is determined from the certificate chain associated with the pinned-domain-cert and is used to update the audit-log.
5.8.3. Registrar audit log verification

Each time the Manufacturer Authorized Signing Authority (MASA) issues a voucher, it appends details of the assignment to an internal audit log for that device. The internal audit log is processed when responding to requests for details as described in Section 5.8. The contents of the audit log can express a variety of trust levels, and this section explains what kind of trust a registrar can derive from the entries.

While the audit log provides a list of vouchers that were issued by the MASA, the vouchers are issued in response to voucher-requests, and it is the contents of the voucher-requests which determines how meaningful the audit log entries are.

A registrar SHOULD use the log information to make an informed decision regarding the continued bootstrapping of the pledge. The exact policy is out of scope of this document as it depends on the security requirements within the registrar domain. Equipment that is purchased pre-owned can be expected to have an extensive history. The following discussion is provided to help explain the value of each log element:

- **date**: The date field provides the registrar an opportunity to divide the log around known events such as the purchase date. Depending on context known to the registrar or administrator events before/after certain dates can have different levels of importance. For example for equipment that is expected to be new, and thus have no history, it would be a surprise to find prior entries.

- **domainID**: If the log includes an unexpected domainID then the pledge could have imprinted on an unexpected domain. The registrar can be expected to use a variety of techniques to define "unexpected" ranging from white lists of prior domains to anomaly detection (e.g. "this device was previously bound to a different domain than any other device deployed"). Log entries can also be compared against local history logs in search of discrepancies (e.g. "this device was re-deployed some number of times internally but the external audit log shows additional re-deployments our internal logs are unaware of").

- **nonce**: Nonceless entries mean the logged domainID could theoretically trigger a reset of the pledge and then take over management by using the existing nonceless voucher.

- **assertion**: The assertion leaf in the voucher and audit log indicates why the MASA issued the voucher. A "verified" entry means that the MASA issued the associated voucher as a result of positive
verification of ownership but this can still be problematic for registrar’s that expected only new (not pre-owned) pledges. A "logged" assertion informs the registrar that the prior vouchers were issued with minimal verification. A "proximity" assertion assures the registrar that the pledge was truly communicating with the prior domain and thus provides assurance that the prior domain really has deployed the pledge.

A relatively simple policy is to white list known (internal or external) domainIDs. To require all vouchers to have a nonce. Alternatively to require that all nonceless vouchers be from a subset (e.g. only internal) of domainIDs. If the policy is violated a simple action is to revoke any locally issued credentials for the pledge in question or to refuse to forward the voucher. The Registrar MUST then refuse any EST actions, and SHOULD inform a human via a log. A registrar MAY be configured to ignore (i.e. override the above policy) the history of the device but it is RECOMMENDED that this only be configured if hardware assisted (i.e. TPM anchored) Network Endpoint Assessment (NEA) [RFC5209] is supported.

5.9. EST Integration for PKI bootstrapping

The pledge SHOULD follow the BRSKI operations with EST enrollment operations including "CA Certificates Request", "CSR Attributes" and "Client Certificate Request" or "Server-Side Key Generation", etc. This is a relatively seamless integration since BRSKI REST calls provide an automated alternative to the manual bootstrapping method described in [RFC7030]. As noted above, use of HTTP 1.1 persistent connections simplifies the pledge state machine.

Although EST allows clients to obtain multiple certificates by sending multiple CSR requests, BRSKI does not support this mechanism directly. This is because BRSKI pledges MUST use the CSR Attributes request ([RFC7030] section 4.5). The registrar MUST validate the CSR against the expected attributes. This implies that client requests will "look the same" and therefore result in a single logical certificate being issued even if the client were to make multiple requests. Registrars MAY contain more complex logic but doing so is out-of-scope of this specification. BRSKI does not signal any enhancement or restriction to this capability.

5.9.1. EST Distribution of CA Certificates

The pledge SHOULD request the full EST Distribution of CA Certificates message. See RFC7030, section 4.1.

This ensures that the pledge has the complete set of current CA certificates beyond the pinned-domain-cert (see Section 5.6.2 for a
discussion of the limitations inherent in having a single certificate instead of a full CA Certificates response.) Although these limitations are acceptable during initial bootstrapping, they are not appropriate for ongoing PKIX end entity certificate validation.

5.9.2. EST CSR Attributes

Automated bootstrapping occurs without local administrative configuration of the pledge. In some deployments it is plausible that the pledge generates a certificate request containing only identity information known to the pledge (essentially the X.509 IDevID information) and ultimately receives a certificate containing domain specific identity information. Conceptually the CA has complete control over all fields issued in the end entity certificate. Realistically this is operationally difficult with the current status of PKI certificate authority deployments, where the CSR is submitted to the CA via a number of non-standard protocols. Even with all standardized protocols used, it could operationally be problematic to expect that service specific certificate fields can be created by a CA that is likely operated by a group that has no insight into different network services/protocols used. For example, the CA could even be outsourced.

To alleviate these operational difficulties, the pledge MUST request the EST "CSR Attributes" from the EST server and the EST server needs to be able to reply with the attributes necessary for use of the certificate in its intended protocols/services. This approach allows for minimal CA integrations and instead the local infrastructure (EST server) informs the pledge of the proper fields to include in the generated CSR (such as rfc822Name). This approach is beneficial to automated bootstrapping in the widest number of environments.

In networks using the BRSKI enrolled certificate to authenticate the ACP (Autonomic Control Plane), the EST CSR attributes MUST include the ACP Domain Information Fields defined in [I-D.ietf-anima-autonomic-control-plane] section 6.1.1.

The registrar MUST also confirm that the resulting CSR is formatted as indicated before forwarding the request to a CA. If the registrar is communicating with the CA using a protocol such as full CMC, which provides mechanisms to override the CSR attributes, then these mechanisms MAY be used even if the client ignores CSR Attribute guidance.
5.9.3. EST Client Certificate Request

   The pledge MUST request a new client certificate. See RFC7030, section 4.2.

5.9.4. Enrollment Status Telemetry

   For automated bootstrapping of devices, the administrative elements providing bootstrapping also provide indications to the system administrators concerning device lifecycle status. This might include information concerning attempted bootstrapping messages seen by the client. The MASA provides logs and status of credential enrollment. [RFC7030] assumes an end user and therefore does not include a final success indication back to the server. This is insufficient for automated use cases.

   In order to communicate this indicator, the client HTTP POSTs the following to the server at the new EST endpoint at "/.well-known/est/enrollstatus".

   To indicate successful enrollment the client SHOULD first re-establish the EST TLS session using the newly obtained credentials. TLS 1.2 supports doing this in-band, but TLS 1.3 does not. The client SHOULD therefore close the existing TLS connection, and start a new one.

   In the case of a FAIL, the Reason string indicates why the most recent enrollment failed. The SubjectKeyIdentifier field MUST be included if the enrollment attempt was for a keypair that is locally known to the client. If EST /serverkeygen was used and failed then the field is omitted from the status telemetry.

   In the case of a SUCCESS the Reason string is omitted. The SubjectKeyIdentifier is included so that the server can record the successful certificate distribution.

   An example status report can be seen below. It is sent with with the media type: application/json

   {  
      "version":"1",  
      "Status":true,  
      "Reason":"Informative human readable message",  
      "reason-context": "Additional information"  
   }

   Figure 17: Example of enrollment status POST
The server SHOULD respond with an HTTP 200 but MAY simply fail with an HTTP 404 error.

Within the server logs the server MUST capture if this message was received over an TLS session with a matching client certificate.

5.9.5. Multiple certificates

Pledges that require multiple certificates could establish direct EST connections to the registrar.

5.9.6. EST over CoAP

This document describes extensions to EST for the purposes of bootstrapping of remote key infrastructures. Bootstrapping is relevant for CoAP enrollment discussions as well. The definition of EST and BRSKI over CoAP is not discussed within this document beyond ensuring proxy support for CoAP operations. Instead it is anticipated that a definition of CoAP mappings will occur in subsequent documents such as [I-D.ietf-ace-coap-est] and that CoAP mappings for BRSKI will be discussed either there or in future work.

6. Clarification of transfer-encoding

[RFC7030] defines its endpoints to include a "Content-Transfer-Encoding" heading, and the payloads to be [RFC4648] Base64 encoded DER.

When used within BRSKI, the original RFC7030 EST endpoints remain Base64 encoded, but the new BRSKI end points which send and receive binary artifacts (specifically, /requestvouchers) are binary. That is, no encoding is used.

In the BRSKI context, the EST "Content-Transfer-Encoding" header field if present, SHOULD be ignored. This header field does not need to be included.

7. Reduced security operational modes

A common requirement of bootstrapping is to support less secure operational modes for support specific use cases. The following sections detail specific ways that the pledge, registrar and MASA can be configured to run in a less secure mode for the indicated reasons.

This section is considered non-normative in the generality of the protocol. Use of the suggested mechanism here MUST be detailed in specific profiles of BRSKI, such as in Section 9.
7.1. Trust Model

This section explains the trust relationships detailed in Section 2.4:

+--------+      +---------+      +------------+      +------------+
| Pledge  |      | Join Proxy |      | Domain Registrar |      | Manufacturer Service |
|         |      |            |      |                 |      | (Internet)           |
+--------+      +---------+      +------------+      +------------+

Figure 10

Pledge: The pledge could be compromised and providing an attack vector for malware. The entity is trusted to only imprint using secure methods described in this document. Additional endpoint assessment techniques are RECOMMENDED but are out-of-scope of this document.

Join Proxy: Provides proxy functionalities but is not involved in security considerations.

Registrar: When interacting with a MASA a registrar makes all decisions. For Ownership Audit Vouchers (see [RFC8366]) the registrar is provided an opportunity to accept MASA decisions.

Vendor Service, MASA: This form of manufacturer service is trusted to accurately log all claim attempts and to provide authoritative log information to registrars. The MASA does not know which devices are associated with which domains. These claims could be strengthened by using cryptographic log techniques to provide append only, cryptographic assured, publicly auditable logs.

Vendor Service, Ownership Validation: This form of manufacturer service is trusted to accurately know which device is owned by which domain.

7.2. Pledge security reductions

The following are a list of alternatives behaviours that the pledge can be programmed to implement. These behaviours are not mutually exclusive, nor are they dependant upon other. Some of these methods enable offline and emergency (touch based) deployment use cases. Normative language is used as these behaviours are referenced in later sections in a normative fashion.

1. The pledge MUST accept nonceless vouchers. This allows for a use case where the registrar can not connect to the MASA at the
deployment time. Logging and validity periods address the security considerations of supporting these use cases.

2. Many devices already support "trust on first use" for physical interfaces such as console ports. This document does not change that reality. Devices supporting this protocol MUST NOT support "trust on first use" on network interfaces. This is because "trust on first use" over network interfaces would undermine the logging based security protections provided by this specification.

3. The pledge MAY have an operational mode where it skips voucher validation one time. For example if a physical button is depressed during the bootstrapping operation. This can be useful if the manufacturer service is unavailable. This behavior SHOULD be available via local configuration or physical presence methods (such as use of a serial/craft console) to ensure new entities can always be deployed even when autonomic methods fail. This allows for unsecured imprint.

4. A craft/serial console could include a command such as "est-enroll [2001:db8:0:1]:443" that begins the EST process from the point after the voucher is validated. This process SHOULD include server certificate verification using an on-screen fingerprint.

It is RECOMMENDED that "trust on first use" or any method of skipping voucher validation (including use of craft serial console) only be available if hardware assisted Network Endpoint Assessment (NEA: [RFC5209]) is supported. This recommendation ensures that domain network monitoring can detect inappropriate use of offline or emergency deployment procedures when voucher-based bootstrapping is not used.

7.3. Registrar security reductions

A registrar can choose to accept devices using less secure methods. These methods are acceptable when low security models are needed, as the security decisions are being made by the local administrator, but they MUST NOT be the default behavior:

1. A registrar MAY choose to accept all devices, or all devices of a particular type, at the administrator’s discretion. This could occur when informing all registrars of unique identifiers of new entities might be operationally difficult.

2. A registrar MAY choose to accept devices that claim a unique identity without the benefit of authenticating that claimed
identity. This could occur when the pledge does not include an X.509 IDevID factory installed credential. New Entities without an X.509 IDevID credential MAY form the Section 5.2 request using the Section 5.5 format to ensure the pledge’s serial number information is provided to the registrar (this includes the IDevID AuthorityKeyIdentifier value, which would be statically configured on the pledge.) The pledge MAY refuse to provide a TLS client certificate (as one is not available.) The pledge SHOULD support HTTP-based or certificate-less TLS authentication as described in EST RFC7030 section 3.3.2. A registrar MUST NOT accept unauthenticated New Entities unless it has been configured to do so by an administrator that has verified that only expected new entities can communicate with a registrar (presumably via a physically secured perimeter.)

3. A registrar MAY submit a nonceless voucher-requests to the MASA service (by not including a nonce in the voucher-request.) The resulting vouchers can then be stored by the registrar until they are needed during bootstrapping operations. This is for use cases where the target network is protected by an air gap and therefore cannot contact the MASA service during pledge deployment.

4. A registrar MAY ignore unrecognized nonceless log entries. This could occur when used equipment is purchased with a valid history being deployed in air gap networks that required permanent vouchers.

5. A registrar MAY accept voucher formats of future types that can not be parsed by the Registrar. This reduces the Registrar’s visibility into the exact voucher contents but does not change the protocol operations.

7.4. MASA security reductions

Lower security modes chosen by the MASA service affect all device deployments unless the lower-security behavior is tied to specific device identities. The modes described below can be applied to specific devices via knowledge of what devices were sold. They can also be bound to specific customers (independent of the device identity) by authenticating the customer’s Registrar.

7.4.1. Issuing Nonceless vouchers

A MASA has the option of not including a nonce in the voucher, and/or not requiring one to be present in the voucher-request. This results in distribution of a voucher that never expires and in effect makes the Domain an always trusted entity to the pledge during any
subsequent bootstrapping attempts. That a nonceless voucher was issued is captured in the log information so that the registrar can make appropriate security decisions when a pledge joins the Domain. This is useful to support use cases where registrars might not be online during actual device deployment.

While a nonceless voucher may include an expiry date, a typical use for a nonceless voucher is for it to be long-lived. If the device can be trusted to have an accurate clock (the MASA will know), then a nonceless voucher CAN be issued with a limited lifetime.

A more typical case for a nonceless voucher is for use with offline onboarding scenarios where it is not possible to pass a fresh voucher-request to the MASA. The use of a long-lived voucher also eliminates concern about the availability of the MASA many years in the future. Thus many nonceless vouchers will have no expiry dates.

Thus, the long lived nonceless voucher does not require the proof that the device is online. Issuing such a thing is only accepted when the registrar is authenticated by the MASA and the MASA is authorized to provide this functionality to this customer. The MASA is RECOMMENDED to use this functionality only in concert with an enhanced level of ownership tracking (out-of-scope.)

If the pledge device is known to have a real-time-clock that is set from the factory, use of a voucher validity period is RECOMMENDED.

7.4.2. Trusting Owners on First Use

A MASA has the option of not verifying ownership before responding with a voucher. This is expected to be a common operational model because doing so relieves the manufacturer providing MASA services from having to track ownership during shipping and supply chain and allows for a very low overhead MASA service. A registrar uses the audit log information as a defense in depth strategy to ensure that this does not occur unexpectedly (for example when purchasing new equipment the registrar would throw an error if any audit log information is reported.) The MASA SHOULD verify the 'prior-signed-voucher-request' information for pledges that support that functionality. This provides a proof-of-proximity check that reduces the need for ownership verification.

A MASA that practices Trust-on-First-Use (TOFU) for Registrar identity may wish to annotate the origin of the connection by IP address or netblock, and restrict future use of that identity from other locations. A MASA that does this SHOULD take care to not create nuissance situations for itself when a customer has multiple
7.4.3. Updating or extending voucher trust anchors

A manufacturer could offer a management mechanism that allows the list of voucher verification trust anchors to be extended. [I-D.ietf-netconf-keystore] is one such interface that could be implemented using YANG. Pretty much any configuration mechanism used today could be extended to provide the needed additional update. A manufacturer could even decide to install the domain CA trust anchors received during the EST "cacerts" step as voucher verification anchors. Some additional signals will be needed to clearly identify which keys have voucher validation authority from among those signed by the domain CA. This is future work.

With the above change to the list of anchors, vouchers can be issued by an alternate MASA. This could be the previous owner (the seller), or some other trusted third party who is mediating the sale. If it was a third party, then the seller would need to have taken steps to introduce the third party configuration to the device prior to disconnection. The third party (e.g. a wholesaler of used equipment) could however use a mechanism described in Section 7.2 to take control of the device after receiving it physically. This would permit the third party to act as the MASA for future onboarding actions. As the IDevID certificate probably cannot be replaced, the new owner’s Registrar would have to support an override of the MASA URL.

To be useful for resale or other transfers of ownership one of two situations will need to occur. The simplest is that the device is not put through any kind of factory default/reset before going through onboarding again. Some other secure, physical signal would be needed to initiate it. This is most suitable for redeploying a device within the same Enterprise. This would entail having previous configuration in the system until entirely replaced by the new owner, and represents some level of risk.

The second mechanism is that there would need to be two levels of factory reset. One would take the system back entirely to manufacturer state, including removing any added trust anchors, and the second (more commonly used) one would just restore the configuration back to a known default without erasing trust anchors. This weaker factor reset might leave valuable credentials on the device and this may be unacceptable to some owners.

As a third option, the manufacturer’s trust anchors could be entirely overwritten with local trust anchors. A factory default would never...
restore those anchors. This option comes with a lot of power, but also a lot of responsibility: if the new anchors are lost the manufacturer may be unable to help.

8. IANA Considerations

This document requires the following IANA actions:

8.1. The IETF XML Registry

This document registers a URI in the "IETF XML Registry" [RFC3688]. IANA has registered the following:

Registrant Contact: The ANIMA WG of the IETF.
XML: N/A, the requested URI is an XML namespace.

8.2. Well-known EST registration

This document extends the definitions of "est" (so far defined via RFC7030) in the "https://www.iana.org/assignments/well-known-uris/well-known-uris.xhtml" registry. IANA is asked to change the registration of "est" to include RFC7030 and this document.

8.3. PKIX Registry

IANA is requested to register the following:

This document requests a number for id-mod-MASAURLExtn2016(TBD) from the pkix(7) id-mod(0) Registry.

This document has received an early allocation from the id-pe registry (SMI Security for PKIX Certificate Extension) for id-pe-masa-url with the value 32, resulting in an OID of 1.3.6.1.5.5.7.1.32.

8.4. Pledge BRSKI Status Telemetry

IANA is requested to create a new Registry entitled: "BRSKI Parameters", and within that Registry to create a table called: "Pledge BRSKI Status Telemetry Attributes". New items can be added using the Specification Required. The following items are to be in the initial registration, with this document (Section 5.7) as the reference:

- version
- Status
8.5. DNS Service Names

IANA is requested to register the following Service Names:

Service Name: brski-proxy
Transport Protocol(s): tcp
Assignee: IESG <iesg@ietf.org>.
Contact: IESG <iesg@ietf.org>
Description: The Bootstrapping Remote Secure Key Infrastructures Proxy
Reference: [This document]

Service Name: brski-registrar
Transport Protocol(s): tcp
Assignee: IESG <iesg@ietf.org>.
Contact: IESG <iesg@ietf.org>
Description: The Bootstrapping Remote Secure Key Infrastructures Registrar
Reference: [This document]

8.6. MUD File Extension for the MASA

The IANA is requested to list the name "masa" in the MUD extensions registry defined in [RFC8520]. Its use is documented in Appendix C.

9. Applicability to the Autonomic Control Plane (ACP)

This document provides a solution to the requirements for secure bootstrap set out in Using an Autonomic Control Plane for Stable Connectivity of Network Operations, Administration, and Maintenance [RFC8368], A Reference Model for Autonomic Networking [I-D.ietf-anima-reference-model] and specifically the An Autonomic Control Plane (ACP) [I-D.ietf-anima-autonomic-control-plane], section 3.2 (Secure Bootstrap), and section 6.1 (ACP Domain, Certificate and Network).

The protocol described in this document has appeal in a number of other non-ANIMA use cases. Such uses of the protocol will be deploying into other environments with different tradeoffs of privacy, security, reliability and autonomy from manufacturers. As such those use cases will need to provide their own applicability statements, and will need to address unique privacy and security considerations for the environments in which they are used.
The autonomic control plane (ACP) that is bootstrapped by the BRSKI protocol is typically used in medium to large Internet Service Provider organizations. Equivalent enterprises that has significant layer-3 router connectivity also will find significant benefit, particularly if the Enterprise has many sites. (A network consisting of primarily layer-2 is not excluded, but the adjacencies that the ACP will create and maintain will not reflect the topology until all devices participate in the ACP).

As specified in the ANIMA charter, this work "...focuses on professionally-managed networks." Such a network has an operator and can do things like install, configure and operate the Registrar function. The operator makes purchasing decisions and is aware of what manufacturers it expects to see on its network.

Such an operator is also capable of performing bootstrapping of a device using a serial-console (craft console). The zero-touch mechanism presented in this and the ACP document [I-D.ietf-anima-autonomic-control-plane] represents a significant efficiency: in particular it reduces the need to put senior experts on airplanes to configure devices in person.

There is a recognition as the technology evolves that not every situation may work out, and occasionally a human may still have to visit. In recognition of this, some mechanisms are presented in Section 7.2. The manufacturer MUST provide at least one of the one-touch mechanisms described that permit enrollment to be proceed without availability of any manufacturer server (such as the MASA).

The BRSKI protocol is going into environments where there have already been quite a number of vendor proprietary management systems. Those are not expected to go away quickly, but rather to leverage the secure credentials that are provisioned by BRSKI. The connectivity requirements of said management systems are provided by the ACP.

10. Privacy Considerations

10.1. MASA audit log

The MASA audit log includes the domainID for each domain a voucher has been issued to. This information is closely related to the actual domain identity. A MASA may need additional defenses against Denial of Service attacks (Section 11.1), and this may involve collecting additional (unspecified here) information. This could provide sufficient information for the MASA service to build a detailed understanding the devices that have been provisioned within a domain.
There are a number of design choices that mitigate this risk. The domain can maintain some privacy since it has not necessarily been authenticated and is not authoritatively bound to the supply chain.

Additionally the domainID captures only the unauthenticated subject key identifier of the domain. A privacy sensitive domain could theoretically generate a new domainID for each device being deployed. Similarly a privacy sensitive domain would likely purchase devices that support proximity assertions from a manufacturer that does not require sales channel integrations. This would result in a significant level of privacy while maintaining the security characteristics provided by Registrar based audit log inspection.

10.2. What BRSKI-EST reveals to the registrar

During the provisional phase of the BRSKI-EST connection between the Pledge and the Registrar, each party reveals its certificates to each other. For the Pledge, this includes the serialNumber attribute, the MASA URL, and the identity that signed the IDevID certificate.

TLS 1.2 reveals the certificate identities to on-path observers, including the Join Proxy.

TLS 1.3 reveals the certificate identities only to the end parties, but as the connection is provisional, an on-path attacker will see the certificates. This includes not just malicious attackers, but also Registrars that are visible to the Pledge, but which are not part of the the intended domain.

10.3. What BRSKI-MASA reveals to the manufacturer

The so-called "call-home" mechanism that occurs as part of the BRSKI-MASA connection standardizes what has been deemed by some as a sinister mechanism for corporate oversight of individuals. ([livingwithIoT] and [IoTstrangeThings] for a small sample).

As the Autonomic Control Plane (ACP) usage of BRSKI is not targeted at individual usage of IoT devices, but rather at the Enterprise and ISP creation of networks in a zero-touch fashion, the "call-home" represents a different kind of concern.

It needs to be re-iterated that the BRSKI-MASA mechanism only occurs once during the commissioning of the device. It is well defined, and although encrypted with TLS, it could in theory be made auditable as the contents are well defined. This connection does not occur when the device powers on or is restarted for normal routines. It is conceivable that a device could be forced to go through a full
factory reset during an exceptional firmware update situation, after which enrollment would have been repeated.

The BRSKI call-home mechanism is mediated via the owner’s Registrar, and the information that is transmitted is directly auditable by the device owner. This is in stark contrast to many "call-home" protocols where the device autonomously calls home and uses an undocumented protocol.

While the contents of the signed part of the pledge voucher request can not be changed, they are not encrypted at the registrar. The ability to audit the messages by the owner of the network a mechanism to defend against exfiltration of data by a nefarious pledge. Both are, to re-iterate, encrypted by TLS while in transit.

The BRSKI-MASA exchange reveals the following information to the manufacturer:

- the identity of the device being enrolled (down to the serial-number!).
- an identity of the domain owner in the form of the domain trust anchor. However, this is not a global PKI anchored name within the WebPKI, so this identity could be pseudonymous. If there is sales channel integration, then the MASA will have authenticated the domain owner, either via pinned certificate, or perhaps another HTTP authentication method, as per Section 5.5.4.
- the time the device is activated,
- the IP address of the domain Owner’s Registrar. For ISPs and Enterprises, the IP address provides very clear geolocation of the owner. No amount of IP address privacy extensions ([RFC4941]) can do anything about this, as a simple whois lookup likely identifies the ISP or Enterprise from the upper bits anyway. A passive attacker who observes the connection definitely may conclude that the given enterprise/ISP is a customer of the particular equipment vendor. The precise model that is being enrolled will remain private.

Based upon the above information, the manufacturer is able to track a specific device from pseudonymous domain identity to the next pseudonymous domain identity. If there is sales-channel integration, then the identities are not pseudonymous.

The above situation is to be distinguished from a residential/individual person who registers a device from a manufacturer: that an enterprise/ISP purchases routing products is hardly worth mentioning.
Deviations from a historical trend or an establish baseline would, however, be notable.

The situation is not improved by the enterprise/ISP using anonymization services such as ToR [Dingledine2004], as a TLS 1.2 connection will reveal the ClientCertificate used, clearly identifying the enterprise/ISP involved. TLS 1.3 is better in this regard, but an active attacker can still discover the parties involved by performing a Man-In-The-Middle-Attack on the first attempt (breaking/killing it with a TCP RST), and then letting subsequent connection pass through.

A manufacturer could attempt to mix the BRSKI-MASA traffic in with general traffic their site by hosting the MASA behind the same (set) of load balancers that the companies normal marketing site is hosted behind. This makes lots of sense from a straight capacity planning point of view as the same set of services (and the same set of Distributed Denial of Service mitigations) may be used. Unfortunately, as the BRSKI-MASA connections include TLS ClientCertificate exchanges, this may easily be observed in TLS 1.2, and a traffic analysis may reveal it even in TLS 1.3. This does not make such a plan irrelevant. There may be other organizational reasons to keep the marketing site (which is often subject to frequent re-designs, outsourcing, etc.) separate from the MASA, which may need to operate reliably for decades.

10.4. Manufacturers and Used or Stolen Equipment

As explained above, the manufacturer receives information each time that a device which is in factory-default mode does a zero-touch bootstrap, and attempts to enroll into a domain owner’s registrar.

The manufacturer is therefore in a position to decline to issue a voucher if it detects that the new owner is not the same as the previous owner.

1. This can be seen as a feature if the equipment is believed to have been stolen. If the legitimate owner notifies the manufacturer of the theft, then when the new owner brings the device up, if they use the zero-touch mechanism, the new (illegitimate) owner reveals their location and identity.

2. In the case of Used equipment, the initial owner could inform the manufacturer of the sale, or the manufacturer may just permit resales unless told otherwise. In which case, the transfer of ownership simply occurs.
3. A manufacturer could however decide not to issue a new voucher in response to a transfer of ownership. This is essentially the same as the stolen case, with the manufacturer having decided that the sale was not legitimate.

4. There is a fourth case, if the manufacturer is providing protection against stolen devices. The manufacturer then has a responsibility to protect the legitimate owner against fraudulent claims that the equipment was stolen. In the absence of such manufacturer protection, such a claim would cause the manufacturer to refuse to issue a new voucher. Should the device go through a deep factory reset (for instance, replacement of a damaged main board component, the device would not bootstrap.

5. Finally, there is a fifth case: the manufacturer has decided to end-of-line the device, or the owner has not paid a yearly support amount, and the manufacturer refuses to issue new vouchers at that point. This last case is not new to the industry: many license systems are already deployed that have significantly worse effect.

This section has outlined five situations in which a manufacturer could use the voucher system to enforce what are clearly license terms. A manufacturer that attempted to enforce license terms via vouchers would find it rather ineffective as the terms would only be enforced when the device is enrolled, and this is not (to repeat), a daily or even monthly occurrence.

10.5. Manufacturers and Grey market equipment

Manufacturers of devices often sell different products into different regional markets. Which product is available in which market can be driven by price differentials, support issues (some markets may require manuals and tech-support to be done in the local language), government export regulation (such as whether strong crypto is permitted to be exported, or permitted to be used in a particular market). When an domain owner obtains a device from a different market (they can be new) and transfers it to a different location, this is called a Grey Market.

A manufacturer could decide not to issue a voucher to an enterprise/ISP based upon their location. There are a number of ways which this could be determined: from the geolocation of the registrar, from sales channel knowledge about the customer, and what products are (un-)available in that market. If the device has a GPS the coordinates of the device could even be placed into an extension of the voucher.
The above actions are not illegal, and not new. Many manufacturers have shipped crypto-weak (exportable) versions of firmware as the default on equipment for decades. The first task of an enterprise/ISP has always been to login to a manufacturer system, show one's "entitlement" (country information, proof that support payments have been made), and receive either a new updated firmware, or a license key that will activate the correct firmware.

BRSKI permits the above process to automated (in an autonomic fashion), and therefore perhaps encourages this kind of differentiation by reducing the cost of doing it.

An issue that manufacturers will need to deal with in the above automated process is when a device is shipped to one country with one set of rules (or laws or entitlements), but the domain registry is in another one. Which rules apply is something will have to be worked out: the manufacturer could come to believe they are dealing with Grey market equipment, when it is simply dealing with a global enterprise.

10.6. Some mitigations for meddling by manufacturers

The most obvious mitigation is not to buy the product. Pick manufacturers that are up-front about their policies, who do not change them gratuitiously.

Section Section 7.4.3 describes some ways in which a manufacturer could provide a mechanism to manage the trust anchors and built-in certificates (IDevID) as an extension. There are a variety of mechanism, and some may take a substantial amount of work to get exactly correct. These mechanisms do not change the flow of the protocol described here, but rather allow the starting trust assumptions to be changed. This is an an area for future standardization work.

Replacement of the voucher validation anchors (usually pointing to the original manufacturer's MASA) with those of the new owner permits the new owner to issue vouchers to subsequent owners. This would be done by having the selling (old) owner to run a MASA.

The BRSKI protocol depends upon a trust anchor on the device and an identity on the device. Management of these entities facilitates a few new operational modes without making any changes to the BRSKI protocol. Those modes include: offline modes where the domain owner operates an internal MASA for all devices, resell modes where the first domain owner becomes the MASA for the next (resold-to) domain owner, and services where an aggregator acquires a large variety of
devices, and then acts as a pseudonymized MASA for a variety of devices from a variety of manufacturers.

Although replacement of the IDevID is not required for all modes described above, a manufacturers could support such a thing. Some may wish to consider replacement of the IDevID as an indication that the device’s warrantee is terminated. For others, the privacy requirements of some deployments might consider this a standard operating practice.

As discussed at the end of Section 5.8.1, new work could be done to use a distributed consensus technology for the audit log. This would permit the audit log to continue to be useful, even when there is a chain of MASA due to changes of ownership.

11. Security Considerations

This document details a protocol for bootstrapping that balances operational concerns against security concerns. As detailed in the introduction, and touched on again in Section 7, the protocol allows for reduced security modes. These attempt to deliver additional control to the local administrator and owner in cases where less security provides operational benefits. This section goes into more detail about a variety of specific considerations.

To facilitate logging and administrative oversight, in addition to triggering Registrar verification of MASA logs, the pledge reports on voucher parsing status to the registrar. In the case of a failure, this information is informative to a potentially malicious registrar. This is mandated anyway because of the operational benefits of an informed administrator in cases where the failure is indicative of a problem. The registrar is RECOMMENDED to verify MASA logs if voucher status telemetry is not received.

To facilitate truly limited clients EST RFC7030 section 3.3.2 requirements that the client MUST support a client authentication model have been reduced in Section 7 to a statement that the registrar "MAY" choose to accept devices that fail cryptographic authentication. This reflects current (poor) practices in shipping devices without a cryptographic identity that are NOT RECOMMENDED.

During the provisional period of the connection the pledge MUST treat all HTTP header and content data as untrusted data. HTTP libraries are regularly exposed to non-secured HTTP traffic: mature libraries should not have any problems.

Pledges might chose to engage in protocol operations with multiple discovered registrars in parallel. As noted above they will only do
so with distinct nonce values, but the end result could be multiple vouchers issued from the MASA if all registrars attempt to claim the device. This is not a failure and the pledge chooses whichever voucher to accept based on internal logic. The registrars verifying log information will see multiple entries and take this into account for their analytics purposes.

11.1. Denial of Service (DoS) against MASA

There are uses cases where the MASA could be unavailable or uncooperative to the Registrar. They include active DoS attacks, planned and unplanned network partitions, changes to MASA policy, or other instances where MASA policy rejects a claim. These introduce an operational risk to the Registrar owner in that MASA behavior might limit the ability to bootstrap a pledge device. For example this might be an issue during disaster recovery. This risk can be mitigated by Registrars that request and maintain long term copies of "nonceless" vouchers. In that way they are guaranteed to be able to bootstrap their devices.

The issuance of nonceless vouchers themselves creates a security concern. If the Registrar of a previous domain can intercept protocol communications then it can use a previously issued nonceless voucher to establish management control of a pledge device even after having sold it. This risk is mitigated by recording the issuance of such vouchers in the MASA audit log that is verified by the subsequent Registrar and by Pledges only bootstrapping when in a factory default state. This reflects a balance between enabling MASA independence during future bootstrapping and the security of bootstrapping itself. Registrar control over requesting and auditing nonceless vouchers allows device owners to choose an appropriate balance.

The MASA is exposed to DoS attacks wherein attackers claim an unbounded number of devices. Ensuring a registrar is representative of a valid manufacturer customer, even without validating ownership of specific pledge devices, helps to mitigate this. Pledge signatures on the pledge voucher-request, as forwarded by the registrar in the prior-signed-voucher-request field of the registrar voucher-request, significantly reduce this risk by ensuring the MASA can confirm proximity between the pledge and the registrar making the request. Supply chain integration ("know your customer") is an additional step that MASA providers and device vendors can explore.
11.2. Availability of good random numbers

Although the nonce used by the Pledge in the voucher-request does not require a strong cryptographic randomness, the use of TLS in all of the protocols in this document does.

In particular implementations should pay attention to the advance in [RFC4086] section 3, particularly section 3.4. Devices which are reset to factory default in order to perform a second bootstrap with a new owner MUST NOT seed their random number generators in the same way.

11.3. Freshness in Voucher-Requests

A concern has been raised that the pledge voucher-request should contain some content (a nonce) provided by the registrar and/or MASA in order for those actors to verify that the pledge voucher-request is fresh.

There are a number of operational problems with getting a nonce from the MASA to the pledge. It is somewhat easier to collect a random value from the registrar, but as the registrar is not yet vouched for, such a registrar nonce has little value. There are privacy and logistical challenges to addressing these operational issues, so if such a thing were to be considered, it would have to provide some clear value. This section examines the impacts of not having a fresh pledge voucher-request.

Because the registrar authenticates the pledge, a full Man-in-the-Middle attack is not possible, despite the provisional TLS authentication by the pledge (see Section 5.) Instead we examine the case of a fake registrar (Rm) that communicates with the pledge in parallel or in close time proximity with the intended registrar. (This scenario is intentionally supported as described in Section 4.1.)

The fake registrar (Rm) can obtain a voucher signed by the MASA either directly or through arbitrary intermediaries. Assuming that the MASA accepts the registrar voucher-request (either because Rm is collaborating with a legitimate registrar according to supply chain information, or because the MASA is in audit-log only mode), then a voucher linking the pledge to the registrar Rm is issued.

Such a voucher, when passed back to the pledge, would link the pledge to registrar Rm, and would permit the pledge to end the provisional state. It now trusts Rm and, if it has any security vulnerabilities leveragable by an Rm with full administrative control, can be assumed to be a threat against the intended registrar.
This flow is mitigated by the intended registrar verifying the audit logs available from the MASA as described in Section 5.8. Rm might chose to collect a voucher-request but wait until after the intended registrar completes the authorization process before submitting it. This pledge voucher-request would be ‘stale’ in that it has a nonce that no longer matches the internal state of the pledge. In order to successfully use any resulting voucher the Rm would need to remove the stale nonce or anticipate the pledge’s future nonce state. Reducing the possibility of this is why the pledge is mandated to generate a strong random or pseudo-random number nonce.

Additionally, in order to successfully use the resulting voucher the Rm would have to attack the pledge and return it to a bootstrapping enabled state. This would require wiping the pledge of current configuration and triggering a re-bootstrapping of the pledge. This is no more likely than simply taking control of the pledge directly but if this is a consideration the target network is RECOMMENDED to take the following steps:

- Ongoing network monitoring for unexpected bootstrapping attempts by pledges.
- Retrieval and examination of MASA log information upon the occurrence of any such unexpected events. Rm will be listed in the logs along with nonce information for analysis.

### 11.4. Trusting manufacturers

The BRSKI extensions to EST permit a new pledge to be completely configured with domain specific trust anchors. The link from built-in manufacturer-provided trust anchors to domain-specific trust anchors is mediated by the signed voucher artifact.

If the manufacturer’s IDevID signing key is not properly validated, then there is a risk that the network will accept a pledge that should not be a member of the network. As the address of the manufacturer’s MASA is provided in the IDevID using the extension from Section 2.3, the malicious pledge will have no problem collaborating with it’s MASA to produce a completely valid voucher.

BRSKI does not, however, fundamentally change the trust model from domain owner to manufacturer. Assuming that the pledge used its IDevID with RFC7030 EST and BRSKI, the domain (registrar) still needs to trust the manufacturer.

Establishing this trust between domain and manufacturer is outside the scope of BRSKI. There are a number of mechanisms that can adopt including:
o Manually configuring each manufacturer’s trust anchor.

o A Trust-On-First-Use (TOFU) mechanism. A human would be queried upon seeing a manufacturer’s trust anchor for the first time, and then the trust anchor would be installed to the trusted store. There are risks with this; even if the key to name mapping is validated using something like the WebPKI, there remains the possibility that the name is a look alike: e.g, dem0.example. vs demO.example.

o scanning the trust anchor from a QR code that came with the packaging (this is really a manual TOFU mechanism)

o some sales integration process where trust anchors are provided as part of the sales process, probably included in a digital packing "slip", or a sales invoice.

o consortium membership, where all manufacturers of a particular device category (e.g, a light bulb, or a cable-modem) are signed by an certificate authority specifically for this. This is done by CableLabs today. It is used for authentication and authorization as part of TR-79: [docsisroot] and [TR069].

The existing WebPKI provides a reasonable anchor between manufacturer name and public key. It authenticates the key. It does not provide a reasonable authorization for the manufacturer, so it is not directly useable on it’s own.

11.5. Manufacturer Maintenance of trust anchors

BRSKI depends upon the manufacturer building in trust anchors to the pledge device. The voucher artifact which is signed by the MASA will be validated by the pledge using that anchor. This implies that the manufacturer needs to maintain access to a signing key that the pledge can validate.

The manufacturer will need to maintain the ability to make signatures that can be validated for the lifetime that the device could be onboarded. Whether this onboarding lifetime is less than the device lifetime depends upon how the device is used. An inventory of devices kept in a warehouse as spares might not be onboarded for many decades.

There are good cryptographic hygiene reasons why a manufacturer would not want to maintain access to a private key for many decades. A manufacturer in that situation can leverage a long-term certificate authority anchor, built-in to the pledge, and then a certificate chain may be incorporated using the normal CMS certificate set. This
may increase the size of the voucher artifacts, but that is not a significant issues in non-constrained environments.

There are a few other operational variations that manufacturers could consider. For instance, there is no reason that every device need have the same set of trust anchors pre-installed. Devices built in different factories, or on different days, or any other consideration could have different trust anchors built in, and the record of which batch the device is in would be recorded in the asset database. The manufacturer would then know which anchor to sign an artifact against.

Aside from the concern about long-term access to private keys, a major limiting factor for the shelf-life of many devices will be the age of the cryptographic algorithms included. A device produced in 2019 will have hardware and software capable of validating algorithms common in 2019, and will have no defense against attacks (both quantum and von-neuman brute force attacks) which have not yet been invented. This concern is orthogonal to the concern about access to private keys, but this concern likely dominates and limits the lifespan of a device in a warehouse. If any update to firmware to support new cryptographic mechanism were possible (while the device was in a warehouse), updates to trust anchors would also be done at the same time.

The set of standard operating procedures for maintaining high value private keys is well documented. For instance, the WebPKI provides a number of options for audits at \{cabforumaudit\}, and the DNSSEC root operations are well documented at \{dnssecroot\}.

It is not clear if Manufacturers will take this level of precaution, or how strong the economic incentives are to maintain an appropriate level of security.

This next section examines the risk due to a compromised MASA key. This is followed by examination of the risk of a compromised manufacturer IDevID signing key. The third section sections below examines the situation where MASA web server itself is under attacker control, but that the MASA signing key itself is safe in a not-directly connected hardware module.

11.5.1. Compromise of Manufacturer IDevID signing keys

An attacker that has access to the key that the manufacturer uses to sign IDevID certificates can create counterfeit devices. Such devices can claim to be from a particular manufacturer, but be entirely different devices: Trojan horses in effect.
As the attacker controls the MASA URL in the certificate, the registrar can be convinced to talk to the attackers’ MASA. The Registrar does not need to be in any kind of promiscuous mode to be vulnerable.

In addition to creating fake devices, the attacker may also be able to issue revocations for existing certificates if the IDevID certificate process relies upon CRL lists that are distributed.

There does not otherwise seem to be any risk from this compromise to devices which are already deployed, or which are sitting locally in boxes waiting for deployment (local spares). The issue is that operators will be unable to trust devices which have been in an uncontrolled warehouse as they do not know if those are real devices.

11.5.2. Compromise of MASA signing keys

There are two periods of time in which to consider: when the MASA key has fallen into the hands of an attacker, and after the MASA recognizes that the key has been compromised.

11.5.2.1. Attacker opportunities with compromised MASA key

An attacker that has access to the MASA signing key could create vouchers. These vouchers could be for existing deployed devices, or for devices which are still in a warehouse. In order to exploit these vouchers two things need to occur: the device has to go through a factory default boot cycle, and the registrar has to be convinced to contact the attacker’s MASA.

If the attacker controls a Registrar which is visible to the device, then there is no difficulty in delivery of the false voucher. A possible practical example of an attack like this would be in a data center, at an ISP peering point (whether a public IX, or a private peering point). In such a situation, there are already cables attached to the equipment that lead to other devices (the peers at the IX), and through those links, the false voucher could be delivered. The difficult part would be get the device put through a factory reset. This might be accomplished through social engineering of data center staff. Most locked cages have ventilation holes, and possibly a long "paperclip" could reach through to depress a factory reset button. Once such a piece of ISP equipment has been compromised, it could be used to compromise equipment that was connected to (through long haul links even), assuming that those pieces of equipment could also be forced through a factory reset.

The above scenario seems rather unlikely as it requires some element of physical access; but were there a remote exploit that did not
cause a direct breach, but rather a fault that resulted in a factory
reset, this could provide a reasonable path.

The above deals with ANI uses of BRSKI. For cases where 802.11 or
802.15.4 is involved, the need to connect directly to the device is
eliminated, but the need to do a factory reset is not. Physical
possession of the device is not required as above, provided that
there is some way to force a factory reset. With some consumers
devices with low overall implementation quality, the end users might
be familiar with needing to reset the device regularly.

The authors are unable to come up with an attack scenario where a
compromised voucher signature enables an attacker to introduce a
compromised pledge into an existing operator's network. This is the
case because the operator controls the communication between
Registrar and MASA, and there is no opportunity to introduce the fake
voucher through that conduit.

11.5.2.2. Risks after key compromise is known

Once the operator of the MASA realizes that the voucher signing key
has been compromised it has to do a few things.

First, it MUST issue a firmware update to all devices that had that
key as a trust anchor, such that they will no longer trust vouchers
from that key. This will affect devices in the field which are
operating, but those devices, being in operation, are not performing
onboarding operations, so this is not a critical patch.

Devices in boxes (in warehouses) are vulnerable, and remain
vulnerable until patched. An operator would be prudent to unbox the
devices, onboard them in a safe environment, and then perform
firmware updates. This does not have to be done by the end-operator;
it could be done by a distributor that stores the spares. A
recommended practice for high value devices (which typically have a
<4hr service window) may be to validate the device operation on a
regular basis anyway.

If the onboarding process includes attestations about firmware
versions, then through that process the operator would be advised to
upgrade the firmware before going into production. Unfortunately,
this does not help against situations where the attacker operates
their own Registrar (as listed above).

[RFC8366] section 6.1 explains the need for short-lived vouchers.
The nonce guarantees freshness, and the short-lived nature of the
voucher means that the window to deliver a fake voucher is very
short. A nonceless, long-lived voucher would be the only option for
the attacker, and devices in the warehouse would be vulnerable to such a thing.

A key operational recommendation is for manufacturers to sign nonceless, long-lived vouchers with a different key that they sign short-lived vouchers. That key needs significantly better protection. If both keys come from a common trust-anchor (the manufacturer’s CA), then a compromise of the manufacturer’s CA would compromise both keys. Such a compromise of the manufacturer’s CA likely compromises all keys outlined in this section.

11.5.3. Compromise of MASA web service

An attacker that takes over the MASA web service has a number of attacks. The most obvious one is simply to take the database listing customers and devices and to sell this data to other attackers who will now know where to find potentially vulnerable devices.

The second most obvious thing that the attacker can do is to kill the service, or make it operate unreliably, making customers frustrated. This could have a serious affect on ability to deploy new services by customers, and would be a significant issue during disaster recovery.

While the compromise of the MASA web service may lead to the compromise of the MASA voucher signing key, if the signing occurs offboard (such as in a hardware signing module, HSM), then the key may well be safe, but control over it resides with the attacker.

Such an attacker can issue vouchers for any device presently in service. Said device still needs to be convinced to do through a factory reset process before an attack.

If the attacker has access to a key that is trusted for long-lived nonceless vouchers, then they could issue vouchers for devices which are not yet in service. This attack may be very hard to verify and as it would involve doing firmware updates on every device in warehouses (a potentially ruinously expensive process), a manufacturer might be reluctant to admit this possibility.

12. Acknowledgements

We would like to thank the various reviewers for their input, in particular William Atwood, Brian Carpenter, Fuyu Eleven, Eliot Lear, Sergey Kasatkin, Anoop Kumar, Markus Stenberg, Peter van der Stok, and Thomas Werner.

Significant reviews were done by Jari Arko, Christian Huitema and Russ Housley.
This document started it’s life as a two-page idea from Steinthor Bjarnason.

In addition, significant review comments were received by many IESG members, including Adam Roach, Alexey Melnikov, Alissa Cooper, Benjamin Kaduk, Eric Vyncke, Roman Danyliw, and Magnus Westerlund.

13. References

13.1. Normative References

[cabforumaudit]

dnsssecroot]

[I-D.ietf-anima-autonomic-control-plane]

[I-D.ietf-anima-grasp]

[IDevID]


[RFC5652]  Housley, R., "Cryptographic Message Syntax (CMS)", STD 70,
RFC 5652, DOI 10.17487/RFC5652, September 2009,

RFC 5660, DOI 10.17487/RFC5660, October 2009,

Extensions: Extension Definitions", RFC 6066,
DOI 10.17487/RFC6066, January 2011,

[RFC6125]  Saint-Andre, P. and J. Hodges, "Representation and
Verification of Domain-Based Application Service Identity
within Internet Public Key Infrastructure Using X.509
(PKIX) Certificates in the Context of Transport Layer
Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March

[RFC6762]  Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762,
DOI 10.17487/RFC6762, February 2013,

[RFC6763]  Cheshire, S. and M. Krochmal, "DNS-Based Service
Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013,

"Enrollment over Secure Transport", RFC 7030,
DOI 10.17487/RFC7030, October 2013,

Protocol (HTTP/1.1): Message Syntax and Routing",
RFC 7230, DOI 10.17487/RFC7230, June 2014,

Protocol (HTTP/1.1): Semantics and Content", RFC 7231,
DOI 10.17487/RFC7231, June 2014,

[RFC7469]  Evans, C., Palmer, C., and R. Sleevi, "Public Key Pinning
Extension for HTTP", RFC 7469, DOI 10.17487/RFC7469, April


13.2. Informative References

[docsisroot]

[I-D.ietf-ace-coap-est]

[I-D.ietf-anima-constrained-voucher]

[I-D.ietf-anima-reference-model]

[I-D.ietf-anima-stable-connectivity]

[I-D.ietf-netconf-keystore]

[I-D.richardson-anima-state-for-joinrouter]
Richardson, M., "Considerations for stateful vs stateless join router in ANIMA bootstrap", draft-richardson-anima-state-for-joinrouter-02 (work in progress), January 2018.

[imprinting]

[IoTstrangeThings]


Appendix A.  IPv4 and non-ANI operations

The specification of BRSKI in Section 4 intentionally only covers the mechanisms for an IPv6 pledge using Link-Local addresses. This section describes non-normative extensions that can be used in other environments.
A.1. IPv4 Link Local addresses

Instead of an IPv6 link-local address, an IPv4 address may be generated using [RFC3927] Dynamic Configuration of IPv4 Link-Local Addresses.

In the case that an IPv4 Link-Local address is formed, then the bootstrap process would continue as in the IPv6 case by looking for a (circuit) proxy.

A.2. Use of DHCPv4

The Plege MAY obtain an IP address via DHCP [RFC2131]. The DHCP provided parameters for the Domain Name System can be used to perform DNS operations if all local discovery attempts fail.

Appendix B. mDNS / DNSSD proxy discovery options

Pledge discovery of the proxy (Section 4.1) MAY be performed with DNS-based Service Discovery [RFC6763] over Multicast DNS [RFC6762] to discover the proxy at "_brski-proxy._tcp.local.".

Proxy discovery of the registrar (Section 4.3) MAY be performed with DNS-based Service Discovery over Multicast DNS to discover registrars by searching for the service "_brksi-registrar._tcp.local.".

To prevent unacceptable levels of network traffic, when using mDNS, the congestion avoidance mechanisms specified in [RFC6762] section 7 MUST be followed. The pledge SHOULD listen for an unsolicited broadcast response as described in [RFC6762]. This allows devices to avoid announcing their presence via mDNS broadcasts and instead silently join a network by watching for periodic unsolicited broadcast responses.

Discovery of registrar MAY also be performed with DNS-based service discovery by searching for the service "_brksi-registrar._tcp.<domain>". In this case the domain "example.com" is discovered as described in [RFC6763] section 11 (Appendix A.2 suggests the use of DHCP parameters).

If no local proxy or registrar service is located using the GRASP mechanisms or the above mentioned DNS-based Service Discovery methods, the pledge MAY contact a well known manufacturer provided bootstrapping server by performing a DNS lookup using a well known URI such as "brksi-registrar.manufacturer.example.com". The details of the URI are manufacturer specific. Manufacturers that leverage this method on the pledge are responsible for providing the registrar service. Also see Section 2.7.
The current DNS services returned during each query are maintained until bootstrapping is completed. If bootstrapping fails and the pledge returns to the Discovery state, it picks up where it left off and continues attempting bootstrapping. For example, if the first Multicast DNS _bootstrapks._tcp.local response doesn’t work then the second and third responses are tried. If these fail the pledge moves on to normal DNS-based Service Discovery.

Appendix C. MUD Extension

The following extension augments the MUD model to include a single node, as described in [RFC8520] section 3.6, using the following sample module that has the following tree structure:

```plaintext
module: ietf-mud-brski-masa
augment /ietf-mud:mud:
  +--rw masa-server?  inet:uri
```

The model is defined as follows:
The MUD extensions string "masa" is defined, and MUST be included in the extensions array of the mud container of a MUD file when this extension is used.
Appendix D. Example Vouchers

Three entities are involved in a voucher: the MASA issues (signs) it, the registrar’s public key is mentioned in the voucher, and the pledge validates it. In order to provide reproducible examples the public and private keys for an example MASA and registrar are first listed.

D.1. Keys involved

The Manufacturer has a Certificate Authority that signs the pledge’s IDevID. In addition the Manufacturer’s signing authority (the MASA) signs the vouchers, and that certificate must distributed to the devices at manufacturing time so that vouchers can be validated.

D.1.1. MASA key pair for voucher signatures

This private key signs vouchers:

```
-----BEGIN EC PRIVATE KEY-----
MIGkAgEBBDAgiRoYqKoEcOfvRvmZ5P5Azn58tuI7nSnIy7ogFnceiNo+bm5gWno
r61cu60qwVagwYFK4EEAChkZAN1AAT2AH3Rb2FvIJOnts+vGxUW35ofyNbcHxjAz
oi2kwZFE1ByurKJmNcNMFGirGnRXIXGqWCfw5ICgJ8CuM3vV5ty9bf7KU0kejTvw+
5PV++e1k9P9HQQ839qTaws2WwWTxI=
-----END EC PRIVATE KEY-----
```

This public key validates vouchers:

```
-----BEGIN CERTIFICATE-----
MIIBzzCCAVgAwIBAgIBATAXBggqhkjOPQDAjBNMRIwEAYKCIzImizPyLGQBGRYC
Y2ExGTAXBgoJkiaJk/IszAEZFg1zYW5kZ2xkYW4xHDAaQBVAMME1Vuc3ryd5n
IEhpZz2h3YXkgQ0EwHhcNMTcwMzI2MTYyMDEyNzUwWjBHMRIwEAYKCIzImizPyLGQBGRYC
Y2ExGTAXBgoJkiaJk/IszAEZFg1zYW5kZ2xkYW4xJjAUBgNVBAMMDVVuc3ryd5nIIEI1
BuoedjAQBgcghkjOPQJBBgUqOBAglNiAAT2AH3Rb2FvIJOnts+vGxUW35ofyNbcHxjAz
oi2kwZFE1ByurKJmNcNMFGirGnRXIXGqWCfw5ICgJ8CuM3vV5ty9bf7KU0kejTvw+
5PV++e1k9P9HQQ839qTaws2WwWTxKjEDAO
-----END CERTIFICATE-----
```

D.1.2. Manufacturer key pair for IDevID signatures

This private key signs IDevID certificates:

```
-----BEGIN CERTIFICATE-----
MIIBzzCCAVgAwIBAgIBATAXBggqhkjOPQDAjBNMRIwEAYKCIzImizPyLGQBGRYC
Y2ExGTAXBgoJkiaJk/IszAEZFg1zYW5kZ2xkYW4xHDAaQBVAMME1Vuc3ryd5n
IEhpZz2h3YXkgQ0EwHhcNMTcwMzI2MTYyMDEyNzUwWjBHMRIwEAYKCIzImizPyLGQBGRYC
Y2ExGTAXBgoJkiaJk/IszAEZFg1zYW5kZ2xkYW4xJjAUBgNVBAMMDVVuc3ryd5nIIEI1
BuoedjAQBgcghkjOPQJBBgUqOBAglNiAAT2AH3Rb2FvIJOnts+vGxUW35ofyNbcHxjAz
oi2kwZFE1ByurKJmNcNMFGirGnRXIXGqWCfw5ICgJ8CuM3vV5ty9bf7KU0kejTvw+
5PV++e1k9P9HQQ839qTaws2WwWTxKjEDAO
-----END CERTIFICATE-----
```

D.1.3. Registrar key pair

The registrar key (or chain) is the representative of the domain owner. This key signs registrar voucher-requests:

-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIF+obiToYYYMiFsZvrrjW0yFsCJwIFhpskmT/TULmXoAoGCCqGSM49
AwEhUQDQgAENWQOzcNMUjP0NrtfeBc0DJLWfeMGcFdvF6Uz4DifM1ujMc/6g
6W/P6boMyTgDFoH/8HWKUerL5bpneK8sg==
-----END EC PRIVATE KEY-----

The public key is indicated in a pledge voucher-request to show proximity.

-----BEGIN CERTIFICATE-----
MIIBrjCCATOgAwIBAgIBAzAKBggqhkjOPQDAzBOMRIwEAYKZCMImZyLPQBGRYCY
Y2ExGTAXBgoJkiaJk/IszAEZFlgJzYW5kZWxtYW4xHTAbBgNVBAMMDVVuc3RydW5n
IEZzdWNyZWF0aW9uc1N0cmluZwY4Mjg2MzIwMDMwOTkzMTA4NzEwNTIwMS5j
MBAGCgmSJomT8ixkARkWAmNhMRkwFwYKCZImiZPyLQBGRYJC2FuZGVsbWFuMRIw
EAYDVQQDAlsb2NhBghvcm3qWTATegbQECAwIwIBAgIBAzAKBggqhkjOPQDAzBOM
AwEhUQDQgAENWQOzcNMUjP0NrtfeBc0DJLWfeMGcFdvF6Uz4DifM1ujMc/6g
6W/P6boMyTgDFoH/8HWKUerL5bpneK8sg==
-----END CERTIFICATE-----

The registrar public certificate as decoded by openssl’s x509 utility. Note that the registrar certificate is marked with the cmcRA extension.

Certificate:
  Data:
  
  Version: 3 (0x2)
  Serial Number: 3 (0x3)
  Signature Algorithm: ecdsa-with-SHA384
  
  Issuer: DC=ca, DC=sandelman, CN=Unstrung Fountain CA
  Validity
  Not Before: Sep 5 01:12:45 2017 GMT
  Not After : Sep 5 01:12:45 2019 GMT
  
  Subject Public Key Info:
  Public Key Algorithm: id-ecPublicKey
  Public-Key: (256 bit)
  pub:
  8:17:
  3:3e:
  9:ba:
  f:96:
  e9:9d:e2:bc:b2
  ASN1 OID: prime256v1
  X509v3 extensions:
  X509v3 Basic Constraints:
  CA:FALSE
  Signature Algorithm: ecdsa-with-SHA384
  5b:
  b6:
  02:
  c3:
  4b:

D.1.4. Pledge key pair

The pledge has an IDevID key pair built in at manufacturing time:

```
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIBgR6SV+uEvWf15zCQXWzWhjYbMhXPYnqdHJ3Kph1lmm4oAoGCCqGSM49
AwEHoUQDoqAEW/jgQPpRj0JqWgh2RgeZ1LkutbXVjmnHb+1AYaEF/YQjeZg5FZV8
Kj1R/bkEl+18M4onIC7RHaXKkuagu9S6Ttw==
-----END EC PRIVATE KEY-----
```

The public key is used by the registrar to find the MASA. The MASA URL is in an extension described in Section 2.3.

```
-----BEGIN CERTIFICATE-----
MIICBDCAYugAwIBAgIECze20qTAKBggghkjoOPQDADjBNMRIwEAYKCIzPpyLQgB
GRYCY2ExGTAXBgoJk1ajk/IsZAE2FglzYW5kZWhxYW4xDAAbGVBAMMElVuc3Rh
dw5N1EhpZ2h3Xx9q0EiwBcNMTkwNDI0MDIxNjU4WhqPMjk5OTEyMzEwMDAwMDA=
MBwv3jAYBnNVBAUMETawLWQwLWU1LTayLTAwLTJkMFkwEwYHKcZIzj0CAQYIKoZI
zjDQAQCqDqAEW/jgPpRj0JqWgh2RgeZ1LkutbXVjmnHb+1AYaEF/YQjeZg5FZV8
Kj1R/bkEl+18M4onIC7RHaXKkuagu9S6T6OahC6s2DgWVDwE6NjFglZQlBjU0j8KD
OvJ0k8c5b5WdYwQdYwCQYV0TBA1wADArBgNVHREEJDAioCAKCSgSgAQBguS5g
AaATDBEwMC1EMC1FNS0wMiowMC0yRDArBgkrBrGEEAYLwUqIERwcbwFBwYS5ob251
ewR1a2VzLnNnbnRlbG1b5jYTAKBggghkjoOPQDADgNnADBkA0AmVjmmNgjypDhc
fynMV3kMuIpsKrzRWr4g3PtTWdsAE00iTTTj4QtU1bajhoTkCMGMBhbsW2Q4IF
z9t6PDvdeOAbAP1tVIDuO9nmLz5kU+uQctPRFxUBXK3kg==
-----END CERTIFICATE-----
```

The pledge public certificate as decoded by openssl’s x509 utility so that the extensions can be seen. There is a second Custom Extension is included to provided to contain the EUI48/EUI64 that the pledge will configure as it’s layer-2 address (this is non-normative).
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 166573225 (0x9edb4a9)
Signature Algorithm: ecdsa-with-SHA256
Issuer: DC = ca, DC = sandelman, CN = Unstrung Highway CA
Validity
  Not Before: Apr 24 02:16:58 2019 GMT
  Not After : Dec 31 00:00:00 2999 GMT
Subject: serialNumber = 00-d0-e5-02-00-2d
Subject Public Key Info:
  Public Key Algorithm: id-ecPublicKey
  pub:
    9a:83:d4:ba:4f
  ASN1 OID: prime256v1
  NIST CURVE: P-256
X509v3 extensions:
  X509v3 Subject Key Identifier:
  X509v3 Basic Constraints:
    CA:FALSE
  X509v3 Subject Alternative Name:
    othername:<unsupported>
    1.3.6.1.4.1.46930.2:
      ..masa.honeydukes.sandelman.ca
Signature Algorithm: ecdsa-with-SHA256

D.2. Example process

The JSON examples below are wrapped at 60 columns. This results in strings that have newlines in them, which makes them invalid JSON as is. The strings would otherwise be too long, so they need to be unwrapped before processing.
D.2.1. Pledge to Registrar

As described in Section 5.2, the pledge will sign a pledge vouchercontaining the registrar’s public key in the proximityregistrar-cert field. The base64 has been wrapped at 60 characters for presentation reasons.

-----BEGIN CMS-----
MIIGtQYJKoZIhvcaNhQcCoIGjCCbqICAQExDTALBglghkgBZQMEAgEwggNRbgqkhIg9w0BBgqghgNCAIBIDPlsaiWvOZ1i2zbyJyAgyLX1cV1c3Q6dm9yY2hlcIiEeyJh3NcniPnzb24iOiJwcm94a1pWdhiLCJcmVhdG9kLiI6eHJ1cXZpOw0sN0xNVQxQ2V0YToI1NS42aXM6MDQ6MDAIcLCJzZXJyYWt3b3JvIjoiIMdAT2Z3dFZTeUtMDtMTDAtM3piQ1JLCjUb25jY2Z1S1lZPVUZLUd3cV2ME1sQVFFSG9WN1EiLCJwcm94a1pWdHkbtcmVnaXN0cmFyLWN1cnQoIiJNLSUmCMFRDQ0FYWtDb01CMQdJQFqFqUE1CTZ2dxaQtc1BIURRUReJk4TVJkJ0DWBWhDkltavPpeuUXHJUH1lDTWJFJeEdUQVhcZ29ka21hSm5vSXAxQUVWbmdsellXWtavV3h0WVc0ePFqFqStCZ05WQkFNU5XTTzhV M2x6E2EdWdFzdRn1nV0pZykDVbNKn11Z3dNREF3TURb03HWTNVZeuTOUQZ1XNzXnpk SEoxVmljZ1JtOFTib1JocjYcO0z1sWXdIaGNOTVRejE1UQTNKnawotI1RjNfdotY05N VGt4TVRBOM1tDBtBE0k00CReI1EXsDQVLoQJpbWjIuU1HR1FRC1JQ1kqRXxH VEYFQmdmv6mtpYUrPLOz1WkBFKZnbnHrZvVrWld4d4f1XHhFaKFrQmdOeVkJBTU1D V3h2WJTJgc2FHQXkpREJaTUJNR0J5cUdTTPQsWQFR0NCdUdTTPQSOQXDFESEWUFC S1psVuhJMHWvl2Wz2ZVpmOXZQdmIrbE1ub0VNRWdjN1JNk1q3QrQii4kQHZkQzQxzmpl S1IvaE1e5eURSdfjYDLW1OrmJSQgQ5Zn1hcm2zrendNYHawelRpenFqQFRBTE1Ba0dD MVkbrXrdQ0B0QBzLs21j2s29aSxpqMEVbD01EYVFBd1psXnBHFFTNVYzj0djuW bfJ3PRDVEUVhI0RUIKs5X1MFVWhm5UUVRQFRMRk1K0ZUH10U5iQarDveBvpe aEV17GdejEFKNG5zx5k50Kjg1YlpsS21laVFYVY13E1oiR1ZYYIMI89GN24OXOdS3 S2NCQ1NPbmR0UHFeDC9F9E9g2CQpE1Qxlpxq10UT09i1901CCDCCAgwQgLoAMCQAIC BAnntKkwCgYIKoZiZj08AEiwITTTMSMBACGcmSjOMt8ixxaKrkWAmXMNrkWFWKYCI2sm iPzyLQBGyRJc2fuzGZvswFwMRw0GqvYDVOQDBBBNbnNN0cnuZy8iBawdof2F5IFEN MCAF2fSTR0MQdYnqtiMTY1OFoVDi50tKMjMxMDAwMDAwaWJcRwomRqDqAYQVQDFQwDEB Mc1ikcm1i1NS0wmi0wMCm0zDB2MMBMBygSSmM49aEGCCqGSM89AwEAAoIBC4f46j6 USdCyc0yIWUY0mZSrYw11i5pxz/TQGHHBf2EIoxNoOR WFUbC04k5BjpfDOkAyCuyh2y1pLmMcUuk+jgCd07wQHQDVR00BEYEF/CI/MhKviDyEdK110g4sFIsIqFqJ2 MqAKnGludcwcQCAwKXyDVR0BCQ1WqAgBgrBqBGEAALgqGgewrMDA0dRDArRUTUt MDt1MdbMrKMKwYtYWBAhBGC71ICB48H1I2cEua9GzX1lKctcy5y3K5WdWyt4WVUY12ZqyKgQIs0ZjU0iwBDzwA2IAwZ0rJzr15y178q3X48XpZ5D9L11kUaZQ2MVQ +InZ8U8FW7AhK1rU04+EELNMWQ405n4A5BjJDWTFkONrc/bejwXbtI1nnMwwW9U VaB5USQQLyj52Zjp182Z3pnFkrGTRQWQF951xsggeMIIABJwIBATBVEWMEjEAOBojGk kiaJk/isZAEZgFqJjYTEZMBcGcmZjOMt8ixxaAKrKXnnonb1GljbECmBCGOAUE AwwTVW5zdHD1hmcsCGLaAnRdeSNEQQI1CEa2oqTALBglgkQ2ZQMEAgGgaTAYBkgq jhi9wGbQBCMxWYJK0ZihrvHqACMBMBgWCSqG1b3DQJE1BFTrFw0xOTA1MUTyMT1l NTVAhMC8CSqGSG1b3DQJE1BDd1BCQN1j7aqywyhmj9qUH6qK/SlbTOPXF0w1nvwv 5YQYcgDABqgghkQ0PQDAGHMEUCIEYQhTo0rhrFyQv2R0TwWPe7tx2Z1DHEr6t t/DR/ZAIeA47u9bIz/p6NFK/wctKHER/cuyZQYS6h9odMo+1lkC= -----END CMS-----

file: examples/vr_00-D0-05-02-02.pkcs

The ASN1 decoding of the artifact:

0:d=0 h1=4 l=1717 cons: SEQUENCE
4:d=1 h1=2 l= 9 prim: OBJECT :pkcs7-signedData
15:d=1 h1=4 l=1702 cons: cont [ 0 ]
19:d=2 h1=4 l=1698 cons: SEQUENCE
23:d=3 h1=2 l= 1 prim: INTEGER :01
26:d=3 h1=2 l= 13 cons: SET
28:d=4 h1=2 l= 11 cons: SEQUENCE
30:d=5 h1=2 l= 9 prim: OBJECT :sha256
41:d=3 h1=4 l= 849 cons: SEQUENCE
45:d=4 h1=2 l= 9 prim: OBJECT :pkcs7-data
56:d=4 h1=4 l= 834 cons: cont [ 0 ]
60:d=5 h1=4 l= 830 prim: OCTET STRING :"ietf-voucher-request:v
894:d=3 h1=4 l= 520 cons: cont [ 0 ]
898:d=4 h1=4 l= 516 cons: SEQUENCE
902:d=5 h1=4 l= 395 cons: SEQUENCE
906:d=6 h1=2 l= 3 cons: cont [ 0 ]
908:d=7 h1=2 l= 1 prim: INTEGER :02
911:d=6 h1=2 l= 4 prim: INTEGER :09EDB4A9
917:d=6 h1=2 l= 10 cons: SEQUENCE
919:d=7 h1=2 l= 8 prim: OBJECT :ecdsa-with-SHA256
929:d=6 h1=2 l= 77 cons: SEQUENCE
931:d=7 h1=2 l= 18 cons: SET
933:d=8 h1=2 l= 16 cons: SEQUENCE
935:d=9 h1=2 l= 10 prim: OBJECT :domainComponent
947:d=9 h1=2 l= 2 prim: IA5STRING :ca
951:d=7 h1=2 l= 25 cons: SET
953:d=8 h1=2 l= 23 cons: SEQUENCE
955:d=9 h1=2 l= 10 prim: OBJECT :domainComponent
967:d=9 h1=2 l= 9 prim: IA5STRING :sandelman
978:d=7 h1=2 l= 28 cons: SET
980:d=8 h1=2 l= 26 cons: SEQUENCE
982:d=9 h1=2 l= 3 prim: OBJECT :commonName
987:d=9 h1=2 l= 19 prim: UTF8STRING :Unstrung Highway CA
1008:d=6 h1=2 l= 32 cons: SEQUENCE
1010:d=7 h1=2 l= 13 prim: UTCTIME :190424021658Z
1025:d=7 h1=2 l= 15 prim: GENERALIZEDTIME :29991231000000Z
1042:d=6 h1=2 l= 28 cons: SEQUENCE
1044:d=7 h1=2 l= 26 cons: SET
1046:d=8 h1=2 l= 24 cons: SEQUENCE
1048:d=9 h1=2 l= 3 prim: OBJECT :serialNumber
1053:d=9 h1=2 l= 17 prim: UTF8STRING :00-d0-e5-02-00-2d
1072:d=6 h1=2 l= 89 cons: SEQUENCE
1074:d=7 h1=2 l= 19 cons: SEQUENCE
1076:d=8 h1=2 l= 7 prim: OBJECT :id-ecPublicKey
1085:d=8 h1=2 l= 8 prim: OBJECT :prime256v1
1095:d=7 h1=2 l= 66 prim: BIT STRING
1163:d=6 hl=3 l= 135 cons: cont [ 3 ]
1166:d=7 hl=3 l= 132 cons: SEQUENCE
1169:d=8 hl=2 l=  29 cons: SEQUENCE
1171:d=9 hl=2 l=  3 prim: OBJECT :X509v3 Subject Key Ident
1176:d=9 hl=2 l=  22 prim: OCTET STRING [HEX DUMP]:04148FC298754A
1200:d=8 hl=2 l=  9 cons: SEQUENCE
1202:d=9 hl=2 l=  3 prim: OBJECT :X509v3 Basic Constraints
1207:d=9 hl=2 l=  2 prim: OCTET STRING [HEX DUMP]:3000
1211:d=8 hl=2 l= 43 cons: SEQUENCE
1213:d=9 hl=2 l=  3 prim: OBJECT :X509v3 Subject Alternati
1218:d=9 hl=2 l=  36 prim: OCTET STRING [HEX DUMP]:3022A02006092B
1256:d=8 hl=2 l=  43 cons: SEQUENCE
1258:d=9 hl=2 l=  9 prim: OBJECT :1.3.6.1.4.1.46930.2
1269:d=9 hl=2 l=  30 prim: OCTET STRING [HEX DUMP]:0C1C6D6173612E
1298:d=8 hl=2 l=  43 cons: SEQUENCE
1301:d=9 hl=2 l=  10 prim: OBJECT :1.3.6.1.4.1.46930.2
1303:d=6 hl=2 l=  8 prim: OBJECT :ecdsa-with-SHA256
1313:d=5 hl=2 l=103 prim: BIT STRING :Unstrung Highway CA
1418:d=3 hl=4 l= 299 cons: SET
1422:d=4 hl=4 l= 295 cons: SEQUENCE
1426:d=5 hl=2 l=  1 prim: INTEGER :01
1429:d=5 hl=2 l=  85 cons: SEQUENCE
1431:d=6 hl=2 l=  77 cons: SEQUENCE
1433:d=7 hl=2 l=  18 cons: SET
1435:d=8 hl=2 l=  16 cons: SEQUENCE
1437:d=9 hl=2 l=  10 prim: OBJECT :domainComponent
1449:d=9 hl=2 l=  2 prim: IA5STRING :ca
1453:d=7 hl=2 l=  25 cons: SET
1455:d=8 hl=2 l=  23 cons: SEQUENCE
1457:d=9 hl=2 l=  10 prim: OBJECT :domainComponent
1469:d=9 hl=2 l=  9 prim: IA5STRING :sandelman
1480:d=7 hl=2 l=  28 cons: SET
1482:d=8 hl=2 l=  26 cons: SEQUENCE
1484:d=9 hl=2 l=  9 prim: OCTET STRING :commonName
1489:d=9 hl=2 l=  19 prim: UTF8STRING :Unstrung Highway CA
1510:d=6 hl=2 l=  4 prim: INTEGER :09EDB4A9
1516:d=5 hl=2 l=  11 cons: SEQUENCE
1518:d=6 hl=2 l=  9 prim: OBJECT :sha256
1529:d=5 hl=2 l=  105 cons: cont [ 0 ]
1531:d=6 hl=2 l=  24 cons: SEQUENCE
1533:d=7 hl=2 l=  9 prim: OBJECT :contentLength
1544:d=7 hl=2 l= 11 cons: SET
1546:d=8 hl=2 l=  9 prim: OCTET STRING :pkcs7-data
1557:d=6 hl=2 l=  28 cons: SEQUENCE
1559:d=7 hl=2 l=  9 prim: OCTET STRING :signingTime
1570:d=7 hl=2 l=  15 cons: SET
1572:d=8 hl=2 l=  13 prim: UTCTIME :190515212555Z
1587:d=6 hl=2 l=  47 cons: SEQUENCE
1589:d=7 hl=2 l=  9 prim: OCTET STRING :messageDigest
The JSON contained in the voucher request:

```
{"ietf-voucher-request:voucher":{"assertion":"proximity","created-on":"2019-05-15T17:25:55.644-04:00","serial-number":"00-d0-e5-02-00-2d","nonce":"VOUFT-WwrEv0NuA8EHoV7Q","proximity-registrar-cert":"MIIB0TCCAvagAwIBAgIBAJAKBggqhkjOPQQDAzBxMRIwEAYKZCMiZPyLQBGFRYCYZExGTAxBoGcJxMjA/IsZsA2EFlzYW5kZWxV4xQDBA+BgNVBAMMD2FzZTYXb3JrcmFwaWxzLmNvZGQwMHgGA1UEAwwXGCMCA4wDQYJKoZIhvcNAQEFBQADgYEAMA4GB8wEAOwIBAgIBADkCAgEBnByGTemperature:25
```

D.2.2. Registrar to MASA

As described in Section 5.5 the registrar will sign a registrar voucher request, and will include pledge’s voucher request in the prior-signed-voucher-request.
The ASN.1 decoding of the artifact:

```asn1
0:d=0 hl=4 l= 3987 cons: SEQUENCE
 4:d=1 hl=4 l=  92 cons: OBJECT  : pkcs7-signedData
15:d=1 hl=4 l= 3972 cons: cont [ 0 ]
19:d=2 hl=4 l= 3968 cons: SEQUENCE
23:d=3 hl=2 l=   1 cons: INTEGER  : 01
26:d=3 hl=2 l=  13 cons: SET
28:d=4 hl=4 l= 2516 cons: SEQUENCE
32:d=5 hl=4 l=  342 cons: SEQUENCE
34:d=6 hl=2 l=   3 cons: cont [ 0 ]
36:d=7 hl=2 l=   1 cons: INTEGER  : 02
38:d=6 hl=2 l=   1 cons: INTEGER  : 02
40:d=6 hl=2 l=  10 cons: SEQUENCE
42:d=7 hl=2 l=   8 cons: OBJECT  : ecdsa-with-SHA384
47:d=6 hl=2 l= 113 cons: SEQUENCE
49:d=7 hl=2 l=  16 cons: SET
51:d=8 hl=2 l=  10 cons: OBJECT  : domainComponent
```

---END CMS-----

file: examples/parboiled_vr_00_D0-E5-02-00-2D.pkcs

2611:d=9 hl=2 l=  2 prim: IA5STRING :ca
2615:d=7 hl=2 l=  25 cons: SET
2617:d=8 hl=2 l=  23 cons: SEQUENCE
2619:d=9 hl=2 l=  10 prim: OBJECT :domainComponent
2631:d=9 hl=2 l=   9 prim: IA5STRING :sandelman
2642:d=7 hl=2 l=  64 cons: SET
2644:d=8 hl=2 l=  62 cons: SEQUENCE
2646:d=9 hl=2 l=  3 prim: OBJECT :commonName
2651:d=9 hl=2 l=  55 prim: UTF8STRING :#<SystemVariable:0x00000
2708:d=6 hl=2 l=  30 cons: SEQUENCE
2710:d=7 hl=2 l=  13 prim: UTCTIME :171107234528Z
2725:d=7 hl=2 l=  13 prim: UTCTIME :191107234528Z
2740:d=6 hl=2 l=  67 cons: SEQUENCE
2742:d=7 hl=2 l=  18 cons: SET
2744:d=8 hl=2 l=  16 cons: SEQUENCE
2746:d=9 hl=2 l=  10 prim: OBJECT :domainComponent
2758:d=9 hl=2 l=   2 prim: IA5STRING :ca
2762:d=7 hl=2 l=  25 cons: SET
2764:d=8 hl=2 l=  23 cons: SEQUENCE
2766:d=9 hl=2 l=  10 prim: OBJECT :domainComponent
2778:d=9 hl=2 l=  9 prim: IA5STRING :sandelman
2789:d=7 hl=2 l=  18 cons: SET
2791:d=8 hl=2 l=  16 cons: SEQUENCE
2793:d=9 hl=2 l=  3 prim: OBJECT :commonName
2798:d=9 hl=2 l=  9 prim: UTF8STRING :localhost
2809:d=6 hl=2 l=  89 cons: SEQUENCE
2811:d=7 hl=2 l=  19 cons: SEQUENCE
2813:d=8 hl=2 l=  7 prim: OBJECT :id-ecPublicKey
2822:d=8 hl=2 l=  8 prim: OBJECT :prime256v1
2832:d=7 hl=2 l=  66 prim: BIT STRING
2900:d=6 hl=2 l=  13 cons: cont [ 3 ]
2902:d=7 hl=2 l=  11 cons: SEQUENCE
2904:d=8 hl=2 l=  9 cons: SEQUENCE
2906:d=9 hl=2 l=  3 prim: OBJECT :X509v3 Basic Constraints
2911:d=9 hl=2 l=  2 prim: OCTET STRING [HEX DUMP]:3000
2915:d=5 hl=2 l=  10 cons: SEQUENCE
2917:d=6 hl=2 l=  8 prim: OBJECT :ecdsa-with-SHA384
2927:d=5 hl=2 l= 105 prim: BIT STRING
3034:d=4 hl=4 l=  617 cons: SEQUENCE
3038:d=5 hl=4 l=  495 cons: SEQUENCE
3042:d=6 hl=2 l=  3 cons: cont [ 0 ]
3044:d=7 hl=2 l=  1 prim: INTEGER :02
3047:d=6 hl=2 l=  1 prim: INTEGER :03
3050:d=6 hl=2 l=  10 cons: SEQUENCE
3052:d=7 hl=2 l=  8 prim: OBJECT :ecdsa-with-SHA256
3062:d=6 hl=2 l= 109 cons: SEQUENCE
3064:d=7 hl=2 l=  18 cons: SET
3066:d=8 hl=2 l=  16 cons: SEQUENCE
Internet-Draft                    BRSKI                      August 2019

3068:d=9  hl=2 l= 10 prim: OBJECT            :domainComponent
3080:d=9  hl=2 l=  2 prim: IA5STRING        :ca
3084:d=7  hl=2 l=  25 cons: SET
3086:d=8  hl=2 l=  23 cons: SEQUENCE
3088:d=9  hl=2 l= 10 prim: OBJECT            :domainComponent
3100:d=9  hl=2 l=   9 prim: IA5STRING        :sandelman
3111:d=7  hl=2 l=  60 cons: SET
3113:d=8  hl=2 l=  58 cons: SEQUENCE
3115:d=9  hl=2 l=   3 prim: OBJECT            :commonName
3120:d=9  hl=2 l=  51 prim: UTF8STRING        :fountain-test.example.co
3173:d=6  hl=2 l=  30 cons: SEQUENCE
3175:d=7  hl=2 l=  13 prim: UTCTIME           :190113225444Z
3190:d=7  hl=2 l=  13 prim: UTCTIME           :210112225444Z
3205:d=6  hl=2 l=  109 cons: SEQUENCE
3207:d=7  hl=2 l=  18 cons: SET
3209:d=8  hl=2 l=  16 cons: SEQUENCE
3211:d=9  hl=2 l=  10 prim: OBJECT            :domainComponent
3223:d=9  hl=2 l=  2 prim: IA5STRING        :ca
3227:d=7  hl=2 l=  25 cons: SET
3229:d=8  hl=2 l=  23 cons: SEQUENCE
3231:d=9  hl=2 l=  10 prim: OBJECT            :domainComponent
3243:d=9  hl=2 l=  10 prim: IA5STRING        :sandelman
3254:d=7  hl=2 l=  60 cons: SET
3256:d=8  hl=2 l=  58 cons: SEQUENCE
3258:d=9  hl=2 l=   3 prim: OBJECT            :commonName
3263:d=9  hl=2 l=  51 prim: UTF8STRING        :fountain-test.example.co
3316:d=6  hl=2 l=  118 cons: SEQUENCE
3318:d=7  hl=2 l=  16 cons: SEQUENCE
3320:d=8  hl=2 l=   7 prim: OBJECT            :id-ecPublicKey
3329:d=8  hl=2 l=  55 cons: OBJECT            :secp384r1
3336:d=7  hl=2 l=  98 prim: BIT STRING
3436:d=6  hl=2 l=  99 cons: cont [ 3 ]
3438:d=7  hl=2 l=  97 cons: SEQUENCE
3440:d=8  hl=2 l=  15 cons: SEQUENCE
3442:d=9  hl=2 l=  10 prim: OBJECT            :X509v3 Basic Constraints
3447:d=9  hl=2 l=   1 prim: BOOLEAN           :255
3450:d=9  hl=2 l=  5 prim: OCTET STRING      [HEX DUMP]:30030101FF
3457:d=8  hl=2 l=  14 cons: SEQUENCE
3459:d=9  hl=2 l=   3 prim: OBJECT            :X509v3 Key Usage
3464:d=9  hl=2 l=   1 prim: BOOLEAN           :255
3467:d=9  hl=2 l=  14 prim: OCTET STRING      [HEX DUMP]:03020106
3473:d=8  hl=2 l=  29 cons: SEQUENCE
3475:d=9  hl=2 l=   3 prim: OBJECT            :X509v3 Subject Key Ident
3480:d=9  hl=2 l=  22 prim: OCTET STRING      [HEX DUMP]:0414B9A5F6CB11
3504:d=8  hl=2 l=  31 cons: SEQUENCE
3506:d=9  hl=2 l=   3 prim: OBJECT            :X509v3 Authority Key Id
3511:d=9  hl=2 l=  24 prim: OCTET STRING      [HEX DUMP]:30168014B9A5F6
3537:d=5  hl=2 l=  10 cons: SEQUENCE
D.2.3. MASA to Registrar

The MASA will return a voucher to the registrar, to be relayed to the pledge.
file: examples/voucher_00-D0-E5-02-00-2D.pkcs

The ASN1 decoding of the artifact:

```plaintext
0:d=0  hl=4 l=1714 cons: SEQUENCE
 4:d=1  hl=2 l= 9 prim: OBJECT :pkcs7-signedData
15:d=1  hl=4 l=1699 cons: cont [ 0 ]
19:d=2  hl=4 l=1695 cons: SEQUENCE
23:d=3  hl=2 l=  1 prim: INTEGER :01

26:d=3  hl=2  l=  13 cons:  SET
28:d=4  hl=2  l=  11 cons:  SEQUENCE
30:d=5  hl=2  l=   9 prim:  OBJECT  :sha256
41:d=3  hl=4  l=  832 cons:  SEQUENCE
45:d=4  hl=2  l=   9 prim:  OBJECT  :pkcs7-data
56:d=4  hl=4  l=  817 cons:  cont [ 0 ]
60:d=5  hl=4  l=  813 prim:  OCTET STRING  :{"ietf-voucher:voucher":
877:d=3  hl=4  l=  501 cons:  cont [ 0 ]
881:d=4  hl=4  l=  497 cons:  SEQUENCE
885:d=5  hl=4  l=  376 cons:  SEQUENCE
889:d=6  hl=2  l=   3 cons:  cont [ 0 ]
891:d=7  hl=2  l=   1 prim:  INTEGER  :02
894:d=6  hl=2  l=   4 prim:  INTEGER  :23CC8913
900:d=6  hl=2  l=  10 cons:  SEQUENCE
902:d=7  hl=2  l=   8 prim:  OBJECT  :ecdsa-with-SHA256
912:d=6  hl=2  l=  77 cons:  SEQUENCE
914:d=7  hl=2  l=  18 cons:  SET
916:d=8  hl=2  l=  16 cons:  SEQUENCE
918:d=9  hl=2  l=  10 prim:  OBJECT  :domainComponent
930:d=9  hl=2  l=   2 prim:  IA5STRING  :ca
934:d=7  hl=2  l=  25 cons:  SET
936:d=8  hl=2  l=  23 cons:  SEQUENCE
938:d=9  hl=2  l=  10 prim:  OBJECT  :domainComponent
950:d=9  hl=2  l=   9 prim:  IA5STRING  :sandelman
961:d=7  hl=2  l=  28 cons:  SET
963:d=8  hl=2  l=  26 cons:  SEQUENCE
965:d=9  hl=2  l=   3 prim:  OBJECT  :commonName
970:d=9  hl=2  l=  19 prim:  UTF8STRING  :Unstrung Highway CA
991:d=6  hl=2  l=  30 cons:  SEQUENCE
993:d=7  hl=2  l=  13 prim:  UTCTIME  :190423232107Z
1008:d=7  hl=2  l=  13 prim:  UTCTIME  :190524092107Z
1023:d=6  hl=2  l=  102 cons:  SEQUENCE
1025:d=7  hl=2  l=  15 cons:  SET
1027:d=8  hl=2  l=  13 cons:  SEQUENCE
1029:d=9  hl=2  l=   3 prim:  OBJECT  :countryName
1034:d=9  hl=2  l=   6 prim:  PRINTABLESTRING  :Canada
1042:d=7  hl=2  l=  18 cons:  SET
1044:d=8  hl=2  l=  16 cons:  SEQUENCE
1046:d=9  hl=2  l=   3 prim:  OBJECT  :organizationName
1051:d=9  hl=2  l=   9 prim:  UTF8STRING  :Sandelman
1062:d=7  hl=2  l=  19 cons:  SET
1064:d=8  hl=2  l=  17 cons:  SEQUENCE
1066:d=9  hl=2  l=   3 prim:  OBJECT  :organizationalUnitName
1071:d=9  hl=2  l=  10 prim:  UTF8STRING  :honeydukes
1083:d=7  hl=2  l=  42 cons:  SET
1085:d=8  hl=2  l=  40 cons:  SEQUENCE
1087:d=9  hl=2  l=   3 prim:  OBJECT  :commonName
1092:d=9  hl=2  l=  33 prim:  UTF8STRING  :masa.honeydukes.sandelma
Authors’ Addresses

Max Pritikin
Cisco
Email: pritikin@cisco.com

Michael C. Richardson
Sandelman Software Works
Email: mcr+ietf@sandelman.ca
URI: http://www.sandelman.ca/

Toerless Eckert
Futurewei Technologies Inc. USA
2330 Central Expy
Santa Clara 95050
USA
Email: tte+ietf@cs.fau.de

Michael H. Behringer
Email: Michael.H.Behringer@gmail.com

Kent Watsen
Watsen Networks
Email: kent+ietf@watsen.net
Abstract

This document defines a strategy to securely assign a pledge to an owner, using an artifact signed, directly or indirectly, by the pledge’s manufacturer. This artifact is known as a "voucher".

This document builds upon the work in [RFC8366], encoding the resulting artifact in CBOR. Use with two signature technologies are described.

Additionally, this document explains how constrained vouchers may be transported as an extension to the [I-D.ietf-ace-coap-est] protocol.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 9, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.
Internet-Draft       Constrained Voucher    July 2019

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(https://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1.  Introduction .......................................................... 3
2.  Terminology ........................................................... 4
3.  Requirements Language ............................................... 4
4.  Survey of Voucher Types ............................................ 4
5.  Discovery and URI .................................................... 5
6.  Artifacts .............................................................. 7
   6.1.  Voucher Request artifact ......................................... 7
   6.1.1.  Tree Diagram .................................................... 7
   6.1.2.  SID values ...................................................... 8
   6.1.3.  YANG Module .................................................... 9
   6.1.4.  Example voucher request artifact ................................ 13
   6.2.  Voucher artifact .................................................. 13
   6.2.1.  Tree Diagram .................................................... 13
   6.2.2.  SID values ...................................................... 14
   6.2.3.  YANG Module .................................................... 14
   6.2.4.  Example voucher artifacts ........................................ 17
   6.3.  Signing voucher and voucher-request artifacts .................. 18
   6.3.1.  CMS signing ..................................................... 18
   6.3.2.  COSE signing .................................................... 19
7.  Design Considerations ................................................. 19
8.  Security Considerations .............................................. 19
   8.1.  Clock Sensitivity ................................................ 19
   8.2.  Protect Voucher PKI in HSM ....................................... 20
   8.3.  Test Domain Certificate Validity when Signing .................... 20
9.  IANA Considerations .................................................. 20
   9.1.  Resource Type Registry .......................................... 20
   9.2.  The IETF XML Registry ............................................ 20
   9.3.  The YANG Module Names Registry ................................... 20
   9.4.  The RFC SID range assignment sub-registry ......................... 21
   9.5.  The SMI Security for S/MIME CMS Content Type Registry ............ 21
   9.6.  Media-Type Registry ............................................. 21
   9.6.1.  application/voucher-cms+cbor .................................. 21
   9.6.2.  application/voucher-cose+cbor .................................. 22
   9.7.  CoAP Content-Format Registry .................................... 23
10. Acknowledgements ..................................................... 23
11. Changelog .............................................................. 24
1. Introduction

Enrollment of new nodes into constrained networks with constrained
nodes present unique challenges.

There are bandwidth and code space issues to contend. A solution
such as [I-D.ietf-anima-bootstrapping-keyinfra] may be too large in
terms of code space or bandwidth required.

This document defines a constrained version of [RFC8366]. Rather
than serializing the YANG definition in JSON, it is serialized into
CBOR ([RFC7049]).

This document follows a similar, but not identical structure as
[RFC8366]. Some sections are left out entirely. Additional sections
have been added concerning:

1. Addition of voucher-request specification as defined in
   [I-D.ietf-anima-bootstrapping-keyinfra],

2. Addition to [I-D.ietf-ace-coap-est] of voucher transport requests
   over CoAP.
The CBOR definitions for this constrained voucher format are defined using the mechanism describe in [I-D.ietf-core-yang-cbor] using the SID mechanism explained in [I-D.ietf-core-sid]. As the tooling to convert YANG documents into an list of SID keys is still in its infancy, the table of SID values presented here should be considered normative rather than the output of the pyang tool.

Two methods of signing the resulting CBOR object are described in this document:

1. One is CMS [RFC5652].
2. The other is COSE_Sign1 [RFC8152] objects.

2. Terminology

The following terms are defined in [RFC8366], and are used identically as in that document: artifact, imprint, domain, Join Registrar/Coordinator (JRC), Manufacturer Authorized Signing Authority (MASA), pledge, Trust of First Use (TOFU), and Voucher.

3. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] when, and only when, they appear in all capitals, as shown here.

4. Survey of Voucher Types

[RFC8366] provides for vouchers that assert proximity, that authenticate the registrar and that include different amounts of anti-replay protection.

This document does not make any extensions to the types of vouchers.

Time based vouchers are included in this definition, but given that constrained devices are extremely unlikely to have accurate time, their use is very unlikely. Most users of these constrained vouchers will be online and will use live nonces to provide anti-replay protection.

[RFC8366] defined only the voucher artifact, and not the Voucher Request artifact, which was defined in [I-D.ietf-anima-bootstrapping-keyinfra].
This document defines both a constrained voucher and a constrained voucher-request. They are presented in the order voucher-request, followed by a voucher response as this is the time order that they occur.

This document defines both CMS-signed voucher requests and responses, and COSE signed voucher requests and responses. The use of CMS signatures implies the use of PKIX format certificates. The pinned-domain-cert present in such a voucher, is the certificate of the Registrar.

The constrained voucher and constrained voucher request MUST be signed.

The use of the two signing formats permit the use of both PKIX format certificates, and raw public keys (RPK). When RPKs are used, the voucher produced by the MASA pins the raw public key of the Registrar: the pinned-domain-subject-public-key-info in such a voucher, is the raw public key of the Registrar. This is described in the YANG definition for the constrained voucher.

5. Discovery and URI

This section describes the BRSKI extensions to EST-coaps [I-D.ietf-ace-coap-est] to transport the voucher between registrar, proxy and pledge over CoAP. The extensions are targeted to low-resource networks with small packets. Saving header space is important and the EST-coaps URI is shorter than the EST URI.

The presence and location of (path to) the management data are discovered by sending a GET request to "/.well-known/core" including a resource type (RT) parameter with the value "ace.est" [RFC6690]. Upon success, the return payload will contain the root resource of the EST resources. It is up to the implementation to choose its root resource; throughout this document the example root resource /est is used.

The EST-coaps server URIs differ from the EST URI by replacing the scheme https by coaps and by specifying shorter resource path names:

coaps://www.example.com/est/short-name

Figure 5 in section 3.2.2 of [RFC7030] enumerates the operations and corresponding paths which are supported by EST. Table 1 provides the mapping from the BRSKI extension URI path to the EST-coaps URI path.
Table 1: BRSKI path to EST-coaps path

:requestvoucher, /voucher_status and /enrollstatus are needed between pledge and Registrar.

When discovering the root path for the EST resources, the server MAY return the full resource paths and the used content types. This is useful when multiple content types are specified for EST-coaps server. For example, the following more complete response is possible.

REQ: GET /.well-known/core?rt=ace.est*

RES: 2.05 Content
   </est>; rt="ace.est"
   </est/rv>; rt="ace.est/rv"; ct=TBD2 TBD3
   </est/vs>; rt="ace.est/vs"; ct=50 60
   </est/es>; rt="ace.est/es"; ct=50 60
   </est/ra>; rt="ace.est/ra"; ct=TBD2 TBD3

The return of the content-types allows the client to choose the most appropriate one from multiple content types.

cT=TBD2 stands for Content-Format "application/voucher-cms+cbor, and
cT=TBD3 stands for Content-Format "application/voucher-cose+cbor".

Content-Formats TBD2 and TBD3 are defined in this document.

The Content-Format ("application/json") 50 MAY be supported.
Content-Formats ("application/cbor") 60, TBD2, and TBD3 MUST be supported.
6. Artifacts

This section describes the abstract (tree) definition as explained in [I-D.ietf-netmod-yang-tree-diagrams] first. This provides a high-level view of the contents of each artifact.

Then the assigned SID values are presented. These have been assigned using the rules in [I-D.ietf-core-sid], with an allocation that was made via the http://comi.space service.

6.1. Voucher Request artifact

6.1.1. Tree Diagram

The following diagram is largely a duplicate of the contents of [RFC8366], with the addition of proximity-registrar-subject-public-key-info, proximity-registrar-cert, and prior-signed-voucher-request. prior-signed-voucher-request is only used between the Registrar and the MASA. proximity-registrar-subject-public-key-info replaces proximity-registrar-cert for the extremely constrained cases.
module: ietf-constrained-voucher-request

grouping voucher-request-constrained-grouping
  +-- voucher
    |   +-- created-on?
    |   |   yang:date-and-time
    |   +-- expires-on?
    |   |   yang:date-and-time
    |   +-- assertion
    |   |   enumeration
    |   +-- serial-number
    |   |   string
    |   +-- idevid-issuer?
    |   |   binary
    |   +-- pinned-domain-cert?
    |   |   binary
    |   +-- domain-cert-revocation-checks?
    |   |   boolean
    |   +-- nonce?
    |   |   binary
    |   +-- last-renewal-date?
    |   |   yang:date-and-time
    |   +-- proximity-registrar-subject-public-key-info?
    |   |   binary
    |   +-- proximity-registrar-sha256-of-subject-public-key-info?
    |   |   binary
    |   +-- proximity-registrar-cert?
    |   |   binary
    |   +-- prior-signed-voucher-request?
    |   |   binary

6.1.2. SID values
6.1.3. YANG Module

In the constrained-voucher-request YANG module, the voucher is "augmented" within the "used" grouping statement such that one continuous set of SID values is generated for the constrained-voucher-request module name, all voucher attributes, and the constrained-voucher-request attribute. Two attributes of the voucher are "refined" to be optional.

```yang
<CODE BEGINS> file "ietf-constrained-voucher-request@2018-09-01.yang"
module ietf-constrained-voucher-request {  
  yang-version 1.1;

  namespace  
  prefix "constrained";

  import ietf-restconf {  
    prefix rc;
    description  
      "This import statement is only present to access  
      the yang-data extension defined in RFC 8040.";
    reference "RFC 8040: RESTCONF Protocol";
  }

  import ietf-voucher {  
    prefix "v";
  }

  organization  
    "IETF ANIMA Working Group";
```
This module defines the format for a voucher request, which is produced by a pledge to request a voucher. The voucher-request is sent to the potential owner’s Registrar, which in turn sends the voucher request to the manufacturer or delegate (MASA).

A voucher is then returned to the pledge, binding the pledge to the owner. This is a constrained version of the voucher-request present in draft-ietf-anima-bootstrap-keyinfra.txt.

This version provides a very restricted subset appropriate for very constrained devices.
In particular, it assumes that nonce-ful operation is always required, that expiration dates are rather weak, as no clocks can be assumed, and that the Registrar is identified by a pinned Raw Public Key.


revision "2018-09-01" {
  description
  "Initial version";
  reference
  "RFC XXXX: Voucher Profile for Constrained Devices";
}

rc:yang-data voucher-request-constrained-artifact {
  // YANG data template for a voucher.
  uses voucher-request-constrained-grouping;
}

// Grouping defined for future usage
grouping voucher-request-constrained-grouping {
  description
"Grouping to allow reuse/extensions in future work."

uses v:voucher-artifact-grouping {

refine voucher/created-on {
    mandatory false;
}

refine voucher/pinned-domain-cert {
    mandatory false;
}

augment "voucher" {
    description "Base the constrained voucher-request upon the regular one";

leaf proximity-registrar-subject-public-key-info {
    type binary;
    description "The proximity-registrar-subject-public-key-info replaces the proximity-registrar-cert in constrained uses of the voucher-request. The proximity-registrar-subject-public-key-info is the Raw Public Key of the Registrar. This field is encoded as specified in RFC7250, section 3. The ECDSA algorithm MUST be supported. The EdDSA algorithm as specified in draft-ietf-tls-rfc4492bis-17 SHOULD be supported. Support for the DSA algorithm is not recommended. Support for the RSA algorithm is MAY, but due to size is discouraged.";
}

leaf proximity-registrar-sha256-of-subject-public-key-info {
    type binary;
    description "The proximity-registrar-sha256-of-subject-public-key-info is an alternative to proximity-registrar-subject-public-key-info. and pinned-domain-cert. In many cases the public key of the domain has already been transmitted during the key agreement protocol, and it is wasteful to transmit the public key another two times. The use of a hash of public key info, at 32-bytes for sha256 is a significant savings compared to an RSA public key, but is only a minor savings compared to a 256-bit ECDSA public-key.";
}
Algorithm agility is provided by extensions to this specifications which define new leaf for other hash types.

leaf proximity-registrar-cert {
    type binary;
    description "An X.509 v3 certificate structure as specified by RFC 5280, Section 4 encoded using the ASN.1 distinguished encoding rules (DER), as specified in ITU-T X.690. The first certificate in the Registrar TLS server certificate_list sequence (see [RFC5246]) presented by the Registrar to the Pledge. This MUST be populated in a Pledge’s voucher request if the proximity assertion is populated.";
}

leaf prior-signed-voucher-request {
    type binary;
    description "If it is necessary to change a voucher, or re-sign and forward a voucher that was previously provided along a protocol path, then the previously signed voucher SHOULD be included in this field. For example, a pledge might sign a proximity voucher, which an intermediate registrar then re-signs to make its own proximity assertion. This is a simple mechanism for a chain of trusted parties to change a voucher, while maintaining the prior signature information. The pledge MUST ignore all prior voucher information when accepting a voucher for imprinting. Other parties MAY examine the prior signed voucher information for the purposes of policy decisions. For example this information could be useful to a MASA to determine that both pledge and registrar agree on proximity assertions. The MASA SHOULD remove all prior-signed-voucher-request information when signing a voucher for imprinting so as to minimize the final voucher size.";
}
6.1.4. Example voucher request artifact

Below is a CBOR serialization of the constrained-voucher-request is shown in diagnostic CBOR notation. The enum value of the assertion field is calculated to be zero by following the algorithm described in section 9.6.4.2 of [RFC7950].

```
{  
  1001154: {  
    +2: "2016-10-07T19:31:42Z", / SID= 1001156, created-on /  
    +4: "2016-10-21T19:31:42Z", / SID= 1001158, expires-on /  
    +1: 2, / SID= 1001155, assertion /  
    +13: "JADA123456789", / SID= 1001167, serial-number /  
    +5: h'01020D0F', / SID= 1001159, idevid-issuer /  
    +10: h'01020D0F', / SID=1001064, proximity-registrar-cert/  
    +3: true, / SID= 1001157, domain-cert  
      -revocation-checks/  
    +6: "2017-10-07T19:31:42Z", / SID= 1001160, last-renewal-date /  
    +12: h'01020D0F' / SID= 1001166, proximity-registrar  
      -subject-public-key-info /  
  }  
}
```

6.2. Voucher artifact

The voucher’s primary purpose is to securely assign a pledge to an owner. The voucher informs the pledge which entity it should consider to be its owner.

This document defines a voucher that is a CBOR encoded instance of the YANG module defined in Section 5.3 that has been signed with CMS or with COSE.

6.2.1. Tree Diagram

The following diagram is largely a duplicate of the contents of [RFC8366], with only the addition of pinned-domain-subject-public-key-info.
module: ietf-constrained-voucher

grouping voucher-constrained-grouping
    +++ voucher
        +++ created-on?
            | yang:date-and-time
        +++ expires-on?
            | yang:date-and-time
        +++ assertion
            enumeration
        +++ serial-number
            string
        +++ idevid-issuer?
            binary
        +++ domain-cert?
            binary
        +++ domain-cert-revocation-checks?
            boolean
        +++ nonce?
            binary
        +++ last-renewal-date?
            | yang:date-and-time
        +++ pinned-domain-subject-public-key-info?
            binary
        +++ pinned-sha256-of-subject-public-key-info?
            binary

6.2.2. SID values

<table>
<thead>
<tr>
<th>SID Assigned to</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001104 data /ietf-constrained-voucher:voucher</td>
</tr>
<tr>
<td>1001105 data /ietf-constrained-voucher:voucher/assertion</td>
</tr>
<tr>
<td>1001106 data /ietf-constrained-voucher:voucher/created-on</td>
</tr>
<tr>
<td>1001107 data .../domain-cert-revocation-checks</td>
</tr>
<tr>
<td>1001108 data /ietf-constrained-voucher:voucher.expires-on</td>
</tr>
<tr>
<td>1001109 data /ietf-constrained-voucher:voucher/idevid-issuer</td>
</tr>
<tr>
<td>1001110 data .../last-renewal-date</td>
</tr>
<tr>
<td>1001111 data /ietf-constrained-voucher:voucher/nonce</td>
</tr>
<tr>
<td>1001112 data .../pinned-domain-cert</td>
</tr>
<tr>
<td>1001113 data .../pinned-domain-subject-public-key-info</td>
</tr>
<tr>
<td>1001115 data .../pinned-sha256-of-subject-public-key-info</td>
</tr>
<tr>
<td>1001114 data /ietf-constrained-voucher:voucher/serial-number</td>
</tr>
</tbody>
</table>

6.2.3. YANG Module

In the constrained-voucher YANG module, the voucher is "augmented" within the "used" grouping statement such that one continuous set of SID values is generated for the constrained-voucher module name, all voucher attributes, and the constrained-voucher attribute. Two attributes of the voucher are "refined" to be optional.

<CODE BEGINS> file "ietf-constrained-voucher@2018-09-01.yang"
module ietf-constrained-voucher {
    yang-version 1.1;

namespace
  "urn:ietf:params:xml:ns:yang:ietf-constrained-voucher";
prefix "constrained";

import ietf-restconf {
  prefix rc;
  description
    "This import statement is only present to access
    the yang-data extension defined in RFC 8040."
    reference "RFC 8040: RESTCONF Protocol";
}

import ietf-voucher {
  prefix "v";
}

organization
  "IETF ANIMA Working Group";

contact
  "WG Web:  <http://tools.ietf.org/wg/anima/>
  WG List:  <mailto:anima@ietf.org>
  Author:   Michael Richardson
            <mailto:mcr+ietf@sandelman.ca>
  Author:   Peter van der Stok
            <mailto:consultancy@vanderstok.org>
  Author:   Panos Kampanakis
            <mailto: pkampana@cisco.com>"

description
  "This module defines the format for a voucher, which is produced
  by a pledge’s manufacturer or delegate (MASA) to securely assign
  one or more pledges to an ‘owner’, so that the pledges may
  establish a secure connection to the owner’s network
  infrastructure.

  This version provides a very restricted subset appropriate
  for very constrained devices.
  In particular, it assumes that nonce-ful operation is
  always required, that expiration dates are rather weak, as no
  clocks can be assumed, and that the Registrar is identified
  by a pinned Raw Public Key.

  The key words ‘MUST’, ‘MUST NOT’, ‘REQUIRED’, ‘SHALL’,
  and ‘OPTIONAL’ in the module text are to be interpreted as
  described in RFC 2119.";
description
"Initial version";
reference
"RFC XXXX: Voucher Profile for Constrained Devices";
}

rc:yang-data voucher-constrained-artifact {
  // YANG data template for a voucher.
  uses voucher-constrained-grouping;
}

// Grouping defined for future usage
grouping voucher-constrained-grouping {
  description
  "Grouping to allow reuse/extensions in future work.";

  uses v:voucher-artifact-grouping {
    refine voucher/created-on {
      mandatory false;
    }

    refine voucher/pinned-domain-cert {
      mandatory false;
    }

    augment "voucher" {
      description "Base the constrained voucher
      upon the regular one";
      leaf pinned-domain-subject-public-key-info {
        type binary;
        description
          "The pinned-domain-subject-public-key-info replaces the
          pinned-domain-cert in constrained uses of
          the voucher. The pinned-domain-subject-public-key-info
          is the Raw Public Key of the Registrar.
          This field is encoded as specified in RFC7250,
          section 3.
          The ECDSA algorithm MUST be supported.
          The EdDSA algorithm as specified in
          draft-ietf-tls-rfc4492bis-17 SHOULD be supported.
          Support for the DSA algorithm is not recommended.
          Support for the RSA algorithm is a MAY."
        }

      leaf pinned-sha256-of-subject-public-key-info {
        type binary;
        description
          
        }
      }
  }
}
"The pinned-hash-subject-public-key-info is a second alternative to pinned-domain-cert. In many cases the public key of the domain has already been transmitted during the key agreement process, and it is wasteful to transmit the public key another two times. The use of a hash of public key info, at 32-bytes for sha256 is a significant savings compared to an RSA public key, but is only a minor savings compared to a 256-bit ECDSA public-key. Algorithm agility is provided by extensions to this specifications which define new leaf for other hash types";

6.2.4. Example voucher artifacts

Below a the CBOR serialization of the constrained-voucher is shown in diagnostic CBOR notation. The enum value of the assertion field is calculated to be zero by following the algorithm described in section 9.6.4.2 of [RFC7950].

```
{ 1001104: {  
    +2 : "2016-10-07T19:31:42Z", / SID = 1001106, created-on /  
    +4 : "2016-10-21T19:31:42Z", / SID = 1001108, expires-on /  
    +1 : 0, / SID = 1001105, assertion /  
    "verified" /  
    +11: "JADA123456789", / SID = 1001115, serial-number /  
    +5 : h'01020D0F', / SID = 1001109, idevid-issuer /  
    +8 : h'01020D0F', / SID = 1001112, pinned-domain-cert/  
    +3 : true, / SID = 1001107, domain-cert-revocation-checks /  
    +6 : "2017-10-07T19:31:42Z", / SID = 1001110, last-renewal-date /  
    +9 : h'01020D0F' / SID = 1001113, pinned-domain-subject-public-key-info /  
  }
}
```

The signing of the example is shown in Appendix B.1.
6.3. Signing voucher and voucher-request artifacts

6.3.1. CMS signing

The IETF evolution of PKCS#7 is CMS [RFC5652]. The CMS signed voucher is much like the equivalent voucher defined in [RFC8366].

A different eContentType of TBD1 is used to indicate that the contents are in a different format than in [RFC8366].

The ContentInfo structure contains a payload consisting of the CBOR encoded voucher. The [I-D.ietf-core-yang-cbor] use of delta encoding creates a canonical ordering for the keys on the wire. This canonical ordering is not important as there is no expectation that the content will be reproduced during the validation process.

Normally the recipient is the pledge and the signer is the MASA.

[I-D.ietf-anima-bootstrapping-keyinfra] supports both signed and unsigned voucher requests from the pledge to the JRC. In this specification, voucher-request artifact MUST be signed from the pledge to the registrar. From the JRC to the MASA, the voucher-request artifact MUST be signed by the domain owner key which is requesting ownership.

The considerations of [RFC5652] section 5.1, concerning validating CMS objects which are really PKCS7 objects (cmsVersion=1) applies.

The CMS structure SHOULD also contain all the certificates leading up to and including the signer’s trust anchor certificate known to the recipient. The inclusion of the trust anchor is unusual in many applications, but without it third parties can not accurately audit the transaction.

The CMS structure MAY also contain revocation objects for any intermediate certificate authorities (CAs) between the voucher-issuer and the trust anchor known to the recipient. However, the use of CRLs and other validity mechanisms is discouraged, as the pledge is unlikely to be able to perform online checks, and is unlikely to have a trusted clock source. As described below, the use of short-lived vouchers and/or pledge provided nonce provides a freshness guarantee.

[EDnote: compulsory signing algorithms are ....]

In Appendix B.1 an example for the CMS signing of the voucher-request is shown.
6.3.2. COSE signing

The COSE-Sign1 structure is discussed in section 4.2 of [RFC8152]. The CBOR object that carries the body, the signature, and the information about the body and signature is called the COSE_Sign1 structure. It is used when only one signature is used on the body. Support for EdDSA 256 with Ed25519 is compulsory.

The supported COSE-sign1 object structure is shown in Figure 1.

```
COSE_Sign1(
  h'\x10\x12\x06', #{ "alg": EDdsa 256 }
  "crv": Ed25519,
  "kty": OKP,
  "key_ops": "verify"
),
  h'123', #voucher-request binary content
  h'456', #voucher-request binary public signature
)
```

Figure 1: The cose-sign1 structure.

The [COSE-registry] specifies the integers that replace the strings and the mnemonics in Figure 1. In Appendix C a binary cose-sign1 object is shown based on the voucher-request example of Section 6.1.4.

7. Design Considerations

The design considerations for the CBOR encoding of vouchers is much the same as for [RFC8366].

One key difference is that the names of the leaves in the YANG does not have a material effect on the size of the resulting CBOR, as the SID translation process assigns integers to the names.

8. Security Considerations

8.1. Clock Sensitivity

TBD.
8.2. Protect Voucher PKI in HSM

TBD.

8.3. Test Domain Certificate Validity when Signing

TBD.

9. IANA Considerations

9.1. Resource Type Registry

Additions to the sub-registry "CoAP Resource Type", within the "CoRE parameters" registry are specified below. These can be registered either in the Expert Review range (0-255) or IETF Review range (256-9999).

ace.rt.rv needs registration with IANA
ace.rt.vs needs registration with IANA
ace.rt.es needs registration with IANA
ace.rt.ra needs registration with IANA

9.2. The IETF XML Registry

This document registers two URIs in the IETF XML registry [RFC3688]. Following the format in [RFC3688], the following registration is requested:

Registrant Contact: The ANIMA WG of the IETF.
XML: N/A, the requested URI is an XML namespace.

Registrant Contact: The ANIMA WG of the IETF.
XML: N/A, the requested URI is an XML namespace.

9.3. The YANG Module Names Registry

This document registers two YANG modules in the YANG Module Names registry [RFC6020]. Following the format defined in [RFC6020], the following registration is requested:
9.4. The RFC SID range assignment sub-registry

<table>
<thead>
<tr>
<th>Entry-point</th>
<th>Size</th>
<th>Module name</th>
<th>RFC Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001100</td>
<td>50</td>
<td>ietf-constrained-voucher</td>
<td>[ThisRFC]</td>
</tr>
<tr>
<td>1001150</td>
<td>50</td>
<td>ietf-constrained-voucher-request</td>
<td>[ThisRFC]</td>
</tr>
</tbody>
</table>

Warning: These SID values will change when they transfer to the range 1000-59,999 allocated for SIDs in YANG modules defined in RFCs.

9.5. The SMI Security for S/MIME CMS Content Type Registry

This document registers an OID in the "SMI Security for S/MIME CMS Content Type" registry (1.2.840.113549.1.9.16.1), with the value:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD1</td>
<td>id-ct-animaCBORVoucher</td>
<td>[ThisRFC]</td>
</tr>
</tbody>
</table>

EDNOTE: should a separate value be used for Voucher Requests?

9.6. Media-Type Registry

This section registers the 'application/voucher-cms+cbor' media type and the 'application/voucher-cose+cbor' in the "Media Types" registry. These media types are used to indicate that the content is a CBOR voucher either signed with a cms structure or a COSE_Sign1 structure [RFC8152].

9.6.1. application/voucher-cms+cbor
Type name:  application
Subtype name:  voucher-cms+cbor
Required parameters:  none
Optional parameters:  none
Encoding considerations:  CMS-signed CBOR vouchers are CBOR encoded.
Security considerations:  See Security Considerations, Section
Interoperability considerations:  The format is designed to be broadly interoperable.
Published specification:  THIS RFC.
Applications that use this media type:  ANIMA, 6tisch, and other zero-touch imprinting systems
Additional information:
  Magic number(s):  None
  File extension(s):  .vch
  Macintosh file type code(s):  none
Person & email address to contact for further information:  IETF ANIMA WG
Intended usage:  LIMITED
Restrictions on usage:  NONE
Author:  ANIMA WG
Change controller:  IETF
Provisional registration? (standards tree only):  NO

9.6.2.  application/voucher-cose+cbor
Type name: application
Subtype name: voucher-cose+cbor
Required parameters: none
Optional parameters: cose-type
Encoding considerations: COSE_Sign1 CBOR vouchers are COSE objects signed with one sender.
Security considerations: See Security Considerations, Section
Interoperability considerations: The format is designed to be broadly interoperable.
Published specification: THIS RFC.
Applications that use this media type: ANIMA, 6tisch, and other zero-touch imprinting systems
Additional information:
  Magic number(s): None
  File extension(s): .vch
  Macintosh file type code(s): none
Person & email address to contact for further information: IETF ANIMA WG
Intended usage: LIMITED
Restrictions on usage: NONE
Author: ANIMA WG
Change controller: IETF
Provisional registration? (standards tree only): NO

9.7. CoAP Content-Format Registry

Additions to the sub-registry "CoAP Content-Formats", within the "CoRE Parameters" registry are needed for two media types. These can be registered either in the Expert Review range (0-255) or IETF Review range (256-9999).

<table>
<thead>
<tr>
<th>Media type</th>
<th>mime type</th>
<th>Encoding</th>
<th>ID</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>application/voucher-cms+cbor</td>
<td>-</td>
<td>CBOR</td>
<td>TBD2</td>
<td>[This RFC]</td>
</tr>
<tr>
<td>application/voucher-cose+cbor &quot;COSE-Sign1&quot;</td>
<td>CBOR</td>
<td>TBD3</td>
<td></td>
<td>[This RFC]</td>
</tr>
</tbody>
</table>

10. Acknowledgements

We are very grateful to Jim Schaad for explaining COSE and CMS choices.

Michel Veillette did extensive work on pyang to extend it to support the SID allocation process, and this document was among the first users.

We are grateful for the suggestions done by Esko Dijk.
11. Changelog

-04 voucher and request-voucher MUST be signed examples for signed request are added in appendix IANA SID registration is updated SID values in examples are aligned signed cms examples aligned with new SIDs

-03

Examples are inverted.

-02

Example of requestvoucher with unsigned application/cbor is added attributes of voucher "refined" to optional CBOR serialization of vouchers improved Discovery port numbers are specified

-01

application/json is optional, application/cbor is compulsory Cms and cose mediatypes are introduced

12. References

12.1. Normative References

[I-D.ietf-ace-cbor-web-token]

[I-D.ietf-ace-coap-est]

[I-D.ietf-anima-bootstrapping-keyinfra]

[I-D.ietf-core-object-security]
[I-D.ietf-core-sid]

[I-D.ietf-core-yang-cbor]

[ieee802-1AR]


12.2. Informative References


Appendix A. EST messages to EST-coaps

This section extends the examples from Appendix A of [I-D.ietf-ace-coap-est]. The CoAP headers are only worked out for the enrollstatus example.

A.1. enrollstatus

A coaps enrollstatus message can be:

GET coaps://[192.0.2.1:8085]/est/es

The corresponding coap header fields are shown below.

Ver = 1
T = 0 (CON)
Code = 0x01 (0.01 is GET)
Options
  Option (Uri-Path)
    Option Delta = 0xb   (option nr = 11)
    Option Length = 0x3
    Option Value = "est"
  Option (Uri-Path)
    Option Delta = 0x0   (option nr = 11)
    Option Length = 0x2
    Option Value = "es"
Payload = [Empty]

The Uri-Host and Uri-Port Options are omitted because they coincide with the transport protocol destination address and port respectively.

A 2.05 Content response with an unsigned voucher status (ct=60) will then be:

  2.05 Content (Content-Format: application/cbor)

With CoAP fields and payload:
Ver=1
T=2 (ACK)
Code = 0x45 (2.05 Content)
Options
  Option1 (Content-Format)
  Option Delta = 0xC  (option nr 12)
  Option Length = 0x2
  Option Value = 60 (application/cbor)

Payload (CBOR diagnostic) =
{
"version":"1",
"Status": 1,  / 1 = Success, 0 = Fail  /
"Reason": "Informative human readable message",
"reason-context": "Additional information"
}

Payload (binary) =
A46776657273696F6E61311665374617475730166526561736F6E7822
496E666F726661746976652068756D616E207265616466266D617469
6573736167656e726561736F6E74657874
76416466974696F6E616C20696E666F72656174696F6E

---

##voucher_status

A coaps voucher_status message can be:

GET coaps://[2001:db8::2:1]:61616]/est/vs ----

A 2.05 Content response with a non signed CBOR voucher (ct=60) will then be:

2.05 Content (Content-Format: application/cbor)
Payload =
A46776657273696F6E61311665374617475730166526561736F6E7822
496E666F726661746976652068756D616E207265616466266D617469
6573736167656e726561736F6E74657874
76416466974696F6E616C20696E666F72656174696F6E

A.2. requestvoucher

Signed request-voucher-request payloads are sent from pledge to Registrar, as explained in Section 5.2 of [I-D.ietf-anima-bootstrapping-keyinfra].
A.2.1. signed requestvoucher

A CMS signed requestvoucher message from JRC to MASA is shown below. It would be CoAP POSTED to /est/rv.

```plaintext
POST coaps://[2001:db8::2:1]:61616]/est/rv
(Content-Format: application/voucher-cms+cbor)
```

The payload would be in binary, but is presented in base64 in this document.

```
MIIDugYJKoZIhvcNAQcCoIIDqzCCA6cCAEQExDTALBgglhkgkBZQMEAgEwCwYJ
KoZIhvcNAQcBoIICQtCCAj0wggHioAMCAQQCCh52Yde1TkYyMAoGCCqGSM49
BAMCMF0xcZaABgNVBAYTAlVTMqswCQYDVQQIDAjdQTELMAkGA1UEcgwL
bXBSZBBJbmNxfjAUBgNVBAAsMDWN1cnRpZmljYXRpb24xExARBgNVBAMC
jgwM14xQV1gQ0EwIICrNMTMkWkMTMxMTEyOTE2WhgPOTk5OjEyMzE5NTIaMFwx
CzaABgNVBAYTAlVTMqswCQYDVQQIDAjdQTELMAkGA1UEcgwL
BAoMCV4Y1wibUgSw5jMQwCqYDVQQfLDAiMjIwMjEiMjMwMjAsMjMwMjAs
NDBZMBMGBygGSM49AgECQCCqGSM49AwEHA0IABM1iIEdCjEw0sVxL787n9x7
TkwKLwhMgMA/FQ1gDVFjvYXbVnGmokXF+ueQvpXdpfVC+RUmGpGwOIrV7vjj
lN9mggqogwYywGcQyDVQR0TBAlwADAdBGvNHQ4EFgQuLmAnhxa/f9D8tCszg3
rWZdAqAwHwYDVR0jBBgwFoAUaNF1uf1rv8y9y2w8nwi8LSBbEAWdYDVR0
AQH/BAOAgWqMCCoGAL1ueEQQjMCggHwYxKwYBBUHCAgEzARBrgkrBEGEabQ7
CqEEBAAECAwQwQgYKoZiz0EwIDsQAsRdqhAMDYGZbSUH1pFzXiRwXluiJ9G
ptshQjNzRgF0zYIb2DgAIeAep3SYn0wyGlzyXYMqTTNqCk1n3yDmUQhGIoK
3m00krxyge/MIIBOWIBATBpm0xcZaABgNVBAYTAlVTMqswCQYDVQQIDAjd
QTELMAkGA1UEcgwLbXBSZBBJbmNxfjAUBgNVBAAsMDWN1cnRmZmljYXR
b24xExARBgNVBAMCjgwM14xQV1gQ0ECh52Yde1TkYyMAoGCCqGSM49AwEA
qAbBPmBSCqGSIbDQEFAEwQMBQwDQYJKoZIhvcNAQELBglhkgBZQMEAgEw
DTE5MDQwODEwNjowNte3Zw7y7tw3LgZvS
XEazd3LnnoPBs6FMMF91RaMAoGCCqGSM49BAMCBEcwRQlGA5JDsIpr0Tw/
n6dRHqvgcssz1HhtFfEnRtBfWhS5KD4C1QDDUEqc5wTmRGf0adEQQVzqmIgh
MEqF10vqXv02gLljLw==
```

A 2.04 Changed response returning CBOR voucher signed with a cms structure(ct=TBD2) will then be:

```plaintext
2.04 Changed (Content-Format: application/voucher-cms+cbor)
```

A.3. requestauditing

A coaps requestauditing message contains the signed CBOR voucher:

MIIDuwYJKoZIhvcNAQcCoiDDrDCCA6gCAQExDTALBglghkgBZQMEAgEwCwYJ
Ko2IhvcNAQcBoICICTCAj0wggHioAMCAQICH52Yde1TkyYMAoGCCqGSM49
BAMCMF0xCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJTDTEUMBIGA1UECgwLQ5h
bXs3ZSBJbmJxfjAUBgNVBAsMDWNlcnRmRz5Z3jYXprb24xgEwARBgNVBAMMCjgw
Mi4xQVlgO0EwIbCNCMTk0MTEy0TE2WhgP0Tk5OTEmZ5zMeUMS1aMFXw
CzAJBgNVBAYTAlVTMQswCQYDVQQIDAJTDTEUMBIGA1UECgwLQ5h
bXs3ZSBJbmJxfjAUBgNVBAsMDWNlcnRmRz5Z3jYXprb24xgEwARBgNVBAMMCjgw
Mi4xQVlgO0EwIbCNCMTk0MTEy0TE2WhgP0Tk5OTEmZ5zMeUMS1aMFXw

A.3. requestauditing

A coaps requestauditing message contains the signed CBOR voucher:

MIIDuwYJKoZIhvcNAQcCoiDDrDCCA6gCAQExDTALBglghkgBZQMEAgEwCwYJ
Ko2IhvcNAQcBoICICTCAj0wggHioAMCAQICH52Yde1TkyYMAoGCCqGSM49
BAMCMF0xCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJTDTEUMBIGA1UECgwLQ5h
bXs3ZSBJbmJxfjAUBgNVBAsMDWNlcnRmRz5Z3jYXprb24xgEwARBgNVBAMMCjgw
Mi4xQVlgO0EwIbCNCMTk0MTEy0TE2WhgP0Tk5OTEmZ5zMeUMS1aMFXw
CzAJBgNVBAYTAlVTMQswCQYDVQQIDAJTDTEUMBIGA1UECgwLQ5h
bXs3ZSBJbmJxfjAUBgNVBAsMDWNlcnRmRz5Z3jYXprb24xgEwARBgNVBAMMCjgw
Mi4xQVlgO0EwIbCNCMTk0MTEy0TE2WhgP0Tk5OTEmZ5zMeUMS1aMFXw

A 2.05 Content response returning a log of the voucher (ct=60) will then be:

2.05 Content (Content-Format: application/cbor)
Payload =
{
  "version": "1",
  "events": [
    {
      "date": "<date/time of the entry>",
      "domainID": "<domainID extracted from voucher-request>",
      "nonce": "<any nonce if supplied (or the exact string ‘NULL’)>",
      "assertion": "<the value from the voucher assertion leaf>",
      "truncated": "<the number of domainID entries truncated>",
    },
    {
      "date": "<date/time of the entry>",
      "domainID": "<anotherDomainID extracted from voucher-request>",
      "nonce": "<any nonce if supplied (or the exact string ‘NULL’)>",
      "assertion": "<the value from the voucher assertion leaf>",
    }
  ],
  "truncation": {
    "nonced duplicates": "<total number of entries truncated>",
    "nonceless duplicates": "<total number of entries truncated>",
    "arbitrary": "<number of domainID entries removed entirely>",
  }
}

[EDNOTE: Change JSON to CBOR; Serialize CBOR payload to binary]

Appendix B. Signed voucher-request examples

B.1. CMS signed voucher-request example

The voucher-request example, visualized in CBOR diagnostic notation in Section 6.1.4 is shown as a hexadecimal dump of the binary file.

A11A000F46C2A90274323031362D31302D30375431393A33313A34325A0
473432031362D31302D32315431393A33313A34325A01020d6d4A414441
313233343536373839054401020D0F0A4401020D0F03F50674323031372
D31302D30375431393A33313A34325A0c4401020D0F

The voucher-request example has been signed by using the WT1234 certificate and key pair shown in Appendix C of [I-D.ietf-ace-coap-est]. The CMS signing of the binary voucher-request leads to a binary signed voucher-request, shown with a hexadecimal representation shown in the payload of the request part of Appendix A.2.1 and Appendix A.3.
The breakdown of the CMS signed binary voucher-request file is visualized below:

CMS_ContentInfo:
  contentType: pkcs7-signedData (1.2.840.113549.1.7.2)
  d.signedData:
    version: 1
    digestAlgorithms:
      algorithm: sha256 (2.16.840.1.101.3.4.2.1)
      parameter: <ABSENT>
    encapContentInfo:
      eContentType: pkcs7-data (1.2.840.113549.1.7.1)
      eContent: <ABSENT>
    certificates:
      d.certificate:
        cert_info:
          version: 2
          serialNumber: 911257847511846130
          signature:
            algorithm: ecdsa-with-SHA256 (1.2.840.10045.4.3.2)
            parameter: <ABSENT>
            issuer: C=US, ST=CA, O=Example Inc, OU=certification, CN=802.1AR CA
          validity:
            notBefore: Jan 31 11:29:16 2019 GMT
            notAfter: Dec 31 23:59:59 9999 GMT
          subject: C=US, ST=CA, L=LA, O=example Inc, OU=IoT/serialNumber=Wt1234
          key:
            algor:
              algorithm: id-ecPublicKey (1.2.840.10045.2.1)
              parameter: OBJECT:prime256v1 (1.2.840.10045.3.1.7)
            public_key:  (0 unused bits)
              0000 - 04 c8 b4 21 f1 1c 25 e4–7e 3a c5 71 23 bf
              000e - 2d 9f dc 49 4f 02 8b c3–51 cc 80 c0 3f 15
              001c - 0b f5 0c ff 95 8d 75 41–9d 81 a6 a2 45 df
              002a - 03 e7 90 be 95 cf 75 f6–02 f9 15 26 18 f8
              0038 - 16 a2 b2 3b 56 38 e5 9f–d9
          issuerUID: <ABSENT>
          subjectUID: <ABSENT>
        extensions:
          object: X509v3 Basic Constraints (2.5.29.19)
          critical: BOOL ABSENT
          value:
            0000 - 30
            0002 - <SPACES/NULS>
          object: X509v3 Subject Key Identifier (2.5.29.14)
critical: BOOL ABSENT
value:
0000 - 04 14 96 60 0d 87 16 bf-7f d0 e7 52 d0
000d - ac 76 07 77 ad 66 5d 02-a0

object: X509v3 Authority Key Identifier (2.5.29.35)
critical: BOOL ABSENT
value:
0000 - 30 16 80 14 68 d1 65 51-f9 51 bf c8 2a
000d - 43 1d 0d 9f 08 bc 2d 20-5b 11 60

object: X509v3 Key Usage (2.5.29.15)
critical: TRUE
value:
0000 - 03 02 05 a0

object: X509v3 Subject Alternative Name (2.5.29.17)
critical: BOOL ABSENT
value:
0000 - 30 21 a0 1f 06 08 2b 06-01 05 05 07 08
000d - 04 a0 13 30 11 06 09 2b-06 01 04 01 b4
001a - 3b 0a 01 04 04 01 02 03-04

sig_alg:
algorithm: ecdsa-with-SHA256 (1.2.840.10045.4.3.2)
parameter: <ABSENT>
signature: (0 unused bits)
0000 - 30 46 02 21 00 c0 d8 19-96 d2 50 7d 69 3f 3c
000f - 48 ea a5 ee 94 91 bd a6-db 21 40 99 d9 81 17
001e - c6 3b 36 13 74 cd 86 02-21 00 a7 74 98 9f 4c
002d - 32 1a 5c f2 5d 83 2a 4d-33 6a 08 ad 67 df 20
003c - f1 50 64 21 18 8a 0a de-6d 34 92 36

crls:
<EMPTY>
signerInfos:
version: 1
d.issuerAndSerialNumber:
issuer: C=US, ST=CA, O=Example Inc, OU=certification, CN=802.1AR CA
serialNumber: 9112578475118446130
digestAlgorithm:
algorithm: sha256 (2.16.840.1.101.3.4.2.1)
parameter: <ABSENT>
signedAttrs:
object: contentType (1.2.840.113549.1.9.3)
value.set: OBJECT:pkcs7-data (1.2.840.113549.1.7.1)

object: signingTime (1.2.840.113549.1.9.5)
value.set:
  UTCTIME: Jul  3 08:53:30 2019 GMT

object: messageDigest (1.2.840.113549.1.9.4)
value.set:
  OCTET STRING:
    0000 - d4 b0 5c dd c8 b4 91 28-4a 18 ca 25 9d
    000d - be d0 60 23 cf ad a0 aa-c2 95 ac e9 3f
    001a - 0b 4f 44 9e 25

signatureAlgorithm:
  algorithm: ecdsa-with-SHA256 (1.2.840.10045.4.3.2)
  parameter: <ABSENT>

signature:
  0000 - 30 46 02 21 00 e5 e1 7f-23 c3 aa 14 9f 35 64
  000f - 1e c4 4a 0f 6f a0 16-3b e6 7c 06 51 af bf
  001e - 5a a0 99 59 e0 28 1f 02-21 00 b4 07 2f 7c c4
  002d - f9 26 0c 6d 47 a7 93 56-de b8 da f7 23 f0 af
  003c - 2b 59 16 cc 36 63 e7 91-89 39 df df

unsignedAttrs:
  <EMPTY>

Appendix C. COSE examples

These examples are from the https://minerva.sandelman.ca/ reference code, using the unit test case key pairs, with a flow between pledge ("reach" code), JRC ("fountain") code, and MASA ("highway") code. This example comes from the spec/files/product/00-D0-E5-F2-00-03 directory.

Thanks to Jim Schaad for verifying the COSE Sign1 objects: faults were found and corrected.

C.1. Device, Registrar and MASA keys

This first section documents the public and private keys used in the subsequent test vectors below. These keys come from test code and are not used in any production system, and should only be used only to validate implementations.

C.1.1. Device IDevID certificate
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 787697345 (0x2ef34ec1)
    Signature Algorithm: ecdsa-with-SHA256
    Issuer: C = Canada, ST = Ontario, OU = Sandelman, CN = highway-test.example.com CA
    Validity
      Not Before: Feb 14 17:05:09 2019 GMT
      Not After : Dec 31 00:00:00 2999 GMT
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (256 bit)
        pub:
          4d:7e:b0:00:ed:c0:de:bd:4d:25:55:4e:35:9f:d5:
          86:a4:0c:8b:b7
        ASN1 OID: prime256v1
        NIST CURVE: P-256
  X509v3 extensions:
    X509v3 Subject Key Identifier:
    P:D7:52
  X509v3 Subject Key Identifier:
    Signature Algorithm: ecdsa-with-SHA256
C.1.2. Device private key

-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIA1sa0I4bkj/RJxPUNIbKSBNYolVVzx+T28wo60cYpuaoAoGCCqGSM49
AwEHoUQDgAEGsQoWJ3zWxjikBTcy/RNfeAA7cDevU01VU41+dVqVxS01K/OoVF
YMLdUz8sG0Lxw1tzfWxs89y10u0aSpAyLt==
-----END EC PRIVATE KEY-----
C.1.3. Registrar Certificate

```
-----BEGIN CERTIFICATE-----
MIIB0TCCAvagAwIBAgIBAjAKBggqhkjOPQDQwBxMRkwJwYIKoZIzj0EsMCIgQCAo
YDAgZGR0MS0xKjAwDQYJKoZIzj0DAQcDQGAEQgQVo0S54kT4yfkbBxumdHoCrpsqb
opMKiMln3oB1HAw25MjVgRw8q1t4MFsJoiEwt8ksZfWK4rLgJS2mnpQ==
-----END CERTIFICATE-----
```

C.1.4. Registrar private key

```
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIFhdd0eDdzip67kXx72K+KHGJQYJHNy8pkiLJ6CcvxMGoAoGCCqGSM4
9AwEHoUQDqgAElmcgSY6UicgQwSBztGj5dkK2MAjQIPV8181H+EqjLOYdji10VTEiFj/
Jqt+T0Bfint8NLOg==
-----END EC PRIVATE KEY-----
```

C.1.5. MASA Certificate

```
-----BEGIN CERTIFICATE-----
MIIB3zCCAWsgAwIBAgIEG5lfVDAKBggqhkjOPQDAjBdMQ8wDQYDVQQGEwZDYW5h
ZGEvEDA0gbNVBagMS09udGdyY29tbW9yZ2tlcm9sZWNyZXQgQ0EwMCYGA1UEA
w1Ra2F0aW9uc2NvZGF0ZS10cnVzdC5oZWFzdGluZ3MgQ0EgMCMgQ2FnY29mdHdh
Z2UgSWRhdGxlLmV4YW1wbGUuY29tMB0GA1UEBhMMDWhpZ2h3YXkgQ0EgQ2FuZ2xl
LmNsaWdub20uY29tMIIEqTADBmcgVzZXcgU2VjdXJlc3QgUm9vdCBDdW50ZWFs
ZS5sYXN0LmNsb3NhcmRzLmNybDMgUzAAMB0GA1UdDQQMCBwYIKoZIzj0BAAwH
DAQUFBwEBggEGBQMCBwYIKoZIzj0BAAwHDAQUFBwEIBgMCBAHGMGCQGCS0G
AwEHBhNHRSAQIEhM2MjBQMA4wDAYDVR0TAQH/BAIwADAD
-----END CERTIFICATE-----
```

C.1.6. MASA private key

```
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIFhdd0eDdzip67kXx72K+KHGJQYJHNy8pkiLJ6CcvxMGoAoGCCqGSM4
9AwEHoUQDqgAEqgVQo0S54kT4yfkbBxumdHoCrpsqbOpMKiMln3oB1HAw25MjVgRw
8q1t4MFsJoiEwt8ksZfWK4rLgJS2mnpQ==
-----END EC PRIVATE KEY-----
```
C.2. COSE signed request voucher with registrar certificate pinned

This voucher request has been signed by the pledge, using the private key given above, and has been sent to the JRC over CoAPS. This example uses the proximity-registrar-certificate mechanism to request a voucher that pins the certificate of the registrar.

This is the CBOR diagnostic format, folded to 60 characters:

```
18({h'0A', {}, h'A11A000F46C2A5016970726F78696D69749702C11A5
D1E49970A5130302D44302D45352D46322D30302D303307765F715674477
738565342626C65394D34557036354C770C5901D4308201D030820157A00
302010202028ECD727300A06082A8648CE3D040302306E31123010060A0
** KNOWN TO BE BAD, NOT YET VALIDATED **
0340F4E6D0F9F702553FA53BE572ACF0EDE858275B6AC75994332FB25FB3
A54411E9FA02E6F75FD1AAB7EA9A61F5409E02303E615E75C8F07432A59
0C8D4879869BEC49E4E7D8E0EA1188BD17A02D02F0313D144816002F756
B528AB1D0ADB749D', h'96B82530AC57650346C2BBF5A6CC16B28F16F
ACF5E2F1D1BFCD5DF5627337F7812D67D43BE1CF9906E356F0C2BDD36
777FD7DBA22B8CEB07D518F55AD3'})
```

This is the raw binary, encoded in base64:

```
0oRBoKBZhAhyhGqAPRs12AW1wcm94aWlpdHcKwRpdHkmXC1EmC1wMC1wMC1w
M14wMC0wMwd2X3FWdEd3OFZTQmJzZ1uWvWvWvWvNjVmdwZAdQwghHQMIIIB6AD
** KNOWN TO BE BAD, NOT YET VALIDATED **
NA9ObO+fcCv+V+VyrDu2FgmnWzDrHWOxQzL7Jfs6VEEm6ub3X9q236pph9
UCeAaIa+VY5LyPB0MqWqYNSHmL7aHrSeXn2ODqEyVRegLQIwMTU8BYAL3Vr
Ugo9gwrbdJ1YQJa4JTCsV2UDRsK/+1pswWso8W+s/lov0bzz1fXWJzp394Et
Z9Q74c+ZBuNW+wwr3TZ3f9fbriK4zrB9Udj1WtM=
```

C.3. COSE signed parboiled request voucher

This voucher request has been signed by the JRC using the private key from Appendix C.1.4. Contained within this voucher request is the pledge voucher request above.

This is the CBOR diagnostic format, folded to 60 characters:
The resulting voucher is created by the MASA and returned via the JRC to the Pledge. It is signed by the MASA’s private key Appendix C.1.6 and can be verified by the pledge using the MASA’s public key.

This is the CBOR diagnostic format, folded to 60 characters:
This is the raw binary, encoded in base64:

0oRBoKBZArmhGgAPRoylBWZsb2dnZWQGwRpdHkmaDnEwMC1EMC1FNS1GMi0wMC0wMwt2X3FWdEd3OFZTQmJsZTlNNFVwNjVMdwx5AnRNSUlCMFRdQ0FWYdWd0lCQwQdQfQcQtCZzxdaQtcTIBRUURBekJ4TVJdOVBWtCDkLtaVpQeUXHUUJH0lDMTUEdJQeUQQVhCZ29Ka2hSmstSNuQuVaRmdse1LXNjVtV3h0WVc0eFFEQScC05WqkFNTU5T7hVMXz6EDWdFZrnV0yzVdkWnlI1Z3DNREF3TURd055HWNVfZEV0TUQZ129XKpxCheXNy1j1JtOTFbLJoYVc0Z1eWRxIDaGNQTVrigjE1QUtNMk0wTlRJNFdoY05NVGt4TVRBM0lqTTOVEkV0ZpCREISXdfQV1I1Qpb1Wb1u1MN1FRC1JR1QjykxyRHFETYQmYmdvSmtpYUpLl0Z1kWFFWzk2nbPHpVzVrl4dFLXNHhpFkFQmdOVkJBTU1DH3vWJGc2FHOPkReJARkUTJNR0J5uCDTTTQ5WdFROndcduCDTTQ5XkFDEeEwUSFC1psVUHJMHWVZLwzZVpmOZd2QmIrbeUboUNVRwJ1NJVKlhaQ3rQquqQ0x2kpms1livaEl5eURtSFD5W0RMnJQQQ0g51nhcmZr3emdyNHANw1lpenFqKFRE181a0dBMVxkRQ01BQXdZ11JS29aASxpqMEVBD01EYFB8dplnSXhBTFTFNvZyjhdjouWFJPRDUEVUHIUR9Ksk5XMIWFmcSUvKxRNeRmk1ZK0FvU3JCJU1H05qSaDRvbEvPAeEL17GdeEFKNG5Xz5kXJqy1lps21JavVFY1K35EIoR1ZYY1U1W9GN2zOXd3J2NCQ1NPbROUHFdEc9F7GW2YnEzQlpxUT09WEBOa9bAPAf2vUQZ/Woj2e+45c6+iW1d6IS3JAO85uiu/sNmzeREy3SGUS+1NHL54319216aKtIEacch2
Authors’ Addresses

Michael Richardson
Sandelman Software Works
Email: mcr+ietf@sandelman.ca

Peter van der Stok
vanderstok consultancy
Email: consultancy@vanderstok.org

Panos Kampanakis
Cisco Systems
Email: pkampana@cisco.com
Abstract

This document is a conceptual outline of an application programming interface (API) for the Generic Autonomic Signaling Protocol (GRASP). Such an API is needed for Autonomic Service Agents (ASA) calling the GRASP protocol module to exchange autonomic network messages with other ASAs.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 25, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents.
carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . 2
2. GRASP API for ASA . . . . . . . . . . . . . . . . . . . . . . 3
   2.1. Design Principles . . . . . . . . . . . . . . . . . . . . . 4
   2.2. Asynchronous Operations . . . . . . . . . . . . . . . . 5
   2.3. API definition . . . . . . . . . . . . . . . . . . . . . . 6
      2.3.1. Parameters and data structures . . . . . . . . . . . 6
      2.3.2. Registration . . . . . . . . . . . . . . . . . . . . . 10
      2.3.3. Discovery . . . . . . . . . . . . . . . . . . . . . . 12
      2.3.4. Negotiation . . . . . . . . . . . . . . . . . . . . . 13
      2.3.5. Synchronization and Flooding . . . . . . . . . . . . 17
      2.3.6. Invalid Message Function . . . . . . . . . . . . . . 21
3. Implementation Status [RFC Editor: please remove] . . . . . . 22
4. Security Considerations . . . . . . . . . . . . . . . . . . . . 22
5. IANA Considerations . . . . . . . . . . . . . . . . . . . . . . 22
6. Acknowledgements . . . . . . . . . . . . . . . . . . . . . . 22
7. References . . . . . . . . . . . . . . . . . . . . . . . . . 22
   7.1. Normative References . . . . . . . . . . . . . . . . . . . 22
   7.2. Informative References . . . . . . . . . . . . . . . . . 22
Appendix A. Error Codes . . . . . . . . . . . . . . . . . . . . . 23
Appendix B. Change log [RFC Editor: Please remove] . . . . . . . 24
Authors’ Addresses . . . . . . . . . . . . . . . . . . . . . . . 26

1. Introduction

As defined in [I-D.ietf-anima-reference-model], the Autonomic Service Agent (ASA) is the atomic entity of an autonomic function, and it is instantiated on autonomic nodes. When ASAs communicate with each other, they should use the Generic Autonomic Signaling Protocol (GRASP) [I-D.ietf-anima-grasp].

As the following figure shows, a GRASP implementation could contain two major sub-layers. The bottom is the GRASP base protocol module, which is only responsible for sending and receiving GRASP messages and maintaining shared data structures. The upper layer contains some extended functions based upon GRASP basic protocol. For example, [I-D.liu-anima-grasp-distribution] describes a possible extended function.

It is desirable that ASAs can be designed as portable user-space programs using a portable API. In many operating systems, the GRASP

module will therefore be split into two layers, one being a library that provides the API and the other being core code containing common components such as multicast handling and the discovery cache. The details of this are system-dependent. In particular, the GRASP library might need to communicate with the GRASP core via an inter-process communication (IPC) mechanism.

```
+----+                              +----+
|ASAs|                              |ASAs|
+----+                              +----+
| GRASP Function API |
+---------------------+
| GRASP Extended |
| Function Modules |
+---------------------+
| GRASP Library |
| GRASP Module - - - - - - - - - - |
| GRASP Core |
```

Both the GRASP library and the extended function modules should be available to the ASAs. Thus, there need to be two sub-sets of API. However, since the extended functions are expected to be added in an incremental manner, it is inappropriate to define all the function APIs in a single document. This document only describes the basic GRASP API.

Note that a very simple autonomic node might contain only a single ASA in addition to the autonomic infrastructure components described in [I-D.ietf-anima-bootstrapping-keyinfra] and [I-D.ietf-anima-autonomic-control-plane]. Such a node might directly integrate GRASP in its autonomic code and therefore not require this API to be installed.

This document gives a conceptual outline of the API. It is not a formal specification for any particular programming language or operating system, and it is expected that details will be clarified in individual implementations.

2. GRASP API for ASA
2.1. Design Principles

The assumption of this document is that any Autonomic Service Agent (ASA) needs to call a GRASP module that handles protocol details (security, sending and listening for GRASP messages, waiting, caching discovery results, negotiation looping, sending and receiving synchronization data, etc.) but understands nothing about individual objectives. The semantics of objectives are unknown to the GRASP module and are handled only by the ASAs. Thus, this is a high level abstract API for use by ASAs. Individual language bindings should be defined in separate documents.

An assumption of this API is that ASAs may fall into various classes:

- ASAs that only use GRASP for discovery purposes.
- ASAs that use GRASP negotiation but only as an initiator (client).
- ASAs that use GRASP negotiation but only as a responder.
- ASAs that use GRASP negotiation as an initiator or responder.
- ASAs that use GRASP synchronization but only as an initiator (recipient).
- ASAs that use GRASP synchronization but only as a responder and/or flooder.
- ASAs that use GRASP synchronization as an initiator, responder and/or flooder.

The API also assumes that one ASA may support multiple objectives. Nothing prevents an ASA from supporting some objectives for synchronization and others for negotiation.

The API design assumes that the operating system and programming language provide a mechanism for simultaneous asynchronous operations. This is discussed in detail in Section 2.2.

The functions provided by the API do not map one-to-one onto GRASP messages. Rather, they are intended to offer convenient support for message sequences (such as a discovery request followed by responses from several peers, or a negotiation request followed by various possible responses).

This is a preliminary version. A few gaps exist:

- Authorization of ASAs is out of scope.
2. User-supplied explicit locators for an objective are not supported.

2. The Rapid mode of GRASP is not supported.

2.2. Asynchronous Operations

GRASP includes asynchronous operations and wait states. Most ASAs will need to support several simultaneous operations; for example an ASA might need to negotiate one objective with a peer while discovering and synchronizing a different objective with a different peer. Alternatively, an ASA which acts as a resource manager might need to run simultaneous negotiations for a given objective with multiple different peers. Thus, both the GRASP core and most ASAs need to support asynchronous operations. Depending on both the operating system and the programming language in use, there are two main techniques for such parallel operations: multi-threading, or an polling or 'event loop' structure.

In multi-threading, the operating system and language will provide the necessary support for asynchronous operations, including creation of new threads, context switching between threads, queues, locks, and implicit wait states. In this case, all API calls can be treated naturally as synchronous, even if they include wait states, blocking and queuing. Simultaneous operations will each run in their own threads. For example, the discover() call will not return until discovery results have arrived or a timeout has occurred. If the ASA has other work to do, the discover() call must be in a thread of its own.

In an event loop implementation, synchronous blocking calls are not acceptable. Therefore all calls must be non-blocking, and the main loop will support multiple GRASP sessions in parallel by repeatedly checking each one for a change of state. To facilitate this, the API implementation will provide non-blocking versions of all the functions that otherwise involve blocking and queuing. In these calls, a 'noReply' code will be returned by each call instead of blocking, until such time as the event for which it is waiting (or a failure) has occurred. Thus, for example, discover() would return "noReply" instead of waiting until discovery has succeeded or timed out. The discover() call would be repeated in every cycle of the main loop until it completes. A 'session_nonce' parameter (described below) is used to distinguish simultaneous GRASP sessions from each other, so that any number of sessions may proceed in parallel.

The following calls involve waiting for a remote operation, so they could use this mechanism:
In all these calls, the 'session_nonce' is a read/write parameter. On the first call, it is set to a null value, and the API returns the 'noReply' code and a non-null session_nonce value. This value must be used in all subsequent calls for the same session. By this mechanism, multiple overlapping sessions can be distinguished, both in the ASA and in the GRASP core.

An additional mechanism that might increase efficiency for event loop implementations is to add a general call, say notify(), which would check the status of all outstanding operations for the calling ASA and return the session_nonce values for all sessions that have changed state. This would eliminate the need for repeated calls to the individual functions returning a "noReply". This call is not described below as the details are likely to be implementation-specific.

An implication of the above for all GRASP implementations is that the GRASP core must keep state for each GRASP operation in progress, most likely keyed by the GRASP Session ID and the GRASP source address of the session initiator. Even in a threaded implementation, the GRASP core will need such state internally. The session_nonce parameter exposes this aspect of the implementation.

2.3. API definition

2.3.1. Parameters and data structures

This section describes parameters and data structures used in multiple API calls.

2.3.1.1. Errorcode

All functions in the API have an unsigned 'errorcode' integer as their return value (the first returned value in languages that allow multiple returned parameters). An errorcode of zero indicates success. Any other value indicates failure of some kind. The first three errorcodes have special importance:
1. Declined: used to indicate that the other end has sent a GRASP Negotiation End message (M_END) with a Decline option (O_DECLINE).

2. No reply: used in non-blocking calls to indicate that the other end has sent no reply so far (see Section 2.2).

3. Unspecified error: used when no more specific error code applies.

Appendix A gives a full list of currently suggested error codes, based on implementation experience. While there is no absolute requirement for all implementations to use the same error codes, this is highly recommended for portability of applications.

2.3.1.2. Timeout

Wherever a 'timeout' parameter appears, it is an integer expressed in milliseconds. If it is zero, the GRASP default timeout (GRASP_DEF_TIMEOUT, see [I-D.ietf-anima-grasp]) will apply. If no response is received before the timeout expires, the call will fail unless otherwise noted.

2.3.1.3. Objective

An 'objective' parameter is a data structure with the following components:

- name (UTF-8 string) - the objective’s name
- neg (Boolean flag) - True if objective supports negotiation (default False)
- synch (Boolean flag) - True if objective supports synchronization (default False)
- dry (Boolean flag) - True if objective supports dry-run negotiation (default False)

* Note 1: All objectives are assumed to support discovery, so there is no Boolean for that.
* Note 2: Only one of 'synch' or 'neg' may be True.
* Note 3: 'dry' must not be True unless 'neg' is also True.
* Note 4: In a language such as C the preferred implementation may be to represent the Boolean flags as bits in a single byte.
o loop_count (integer) - Limit on negotiation steps etc. (default GRASP_DEF_LOOPCT, see [I-D.ietf-anima-grasp])

o value - a specific data structure expressing the value of the objective. The format is language dependent, with the constraint that it can be validly represented in CBOR (default integer = 0).

An essential requirement for all language mappings and all implementations is that, regardless of what other options exist for a language-specific representation of the value, there is always an option to use a CBOR byte string as the value. The API will then wrap this byte string in CBOR Tag 24 for transmission via GRASP, and unwrap it after reception.

An example data structure definition for an objective in the C language is:

typedef struct {
  char *name;
  uint8_t flags;            // flag bits as defined by GRASP
  int loop_count;
  int value_size;           // size of value
  uint8_t cbor_value[];     // CBOR bytestring of value
} objective;

An example data structure definition for an objective in the Python language is:

class objective:
  """A GRASP objective"
  def __init__(self, name):
    self.name = name  #Unique name, string
    self.neg = False  #True if objective supports negotiation
    self.dry = False  #True if objective supports dry-run neg.
    self.synch = False  #True if objective supports synch
    self.loop_count = GRASP_DEF_LOOPCT  #Default starting value
    self.value = 0   #Place holder; any valid Python object

2.3.1.4. ASA_locator

An 'ASA_locator' parameter is a data structure with the following contents:

o locator - The actual locator, either an IP address or an ASCII string.

o ifi (integer) - The interface identifier index via which this was discovered - probably no use to a normal ASA
o expire (system dependent type) - The time on the local system
clock when this locator will expire from the cache

o is_ipaddress (Boolean) - True if the locator is an IP address

o is_fqdn (Boolean) - True if the locator is an FQDN

o is_uri (Boolean) - True if the locator is a URI

o diverted (Boolean) - True if the locator was discovered via a
  Divert option

o protocol (integer) - Applicable transport protocol (IPPROTO_TCP or
  IPPROTO_UDP)

o port (integer) - Applicable port number

2.3.1.5. Tagged_objective

A ‘tagged_objective’ parameter is a data structure with the following
contents:

o objective - An objective

o locator - The ASA_locator associated with the objective, or a null
  value.

2.3.1.6. Asa_nonce

In most calls, an ‘asa_nonce’ parameter is required. It is generated
when an ASA registers with GRASP, and any call in which an invalid
nonce is presented will fail. It is an up to 32-bit opaque value
(for example represented as a uint32_t, depending on the language).
It should be unpredictable; a possible implementation is to use the
same mechanism that GRASP uses to generate Session IDs
[I-D.ietf-anima-grasp]. Another possible implementation is to hash
the name of the ASA with a locally defined secret key.

2.3.1.7. Session_nonce

In some calls, a ‘session_nonce’ parameter is required. This is an
opaque data structure as far as the ASA is concerned, used to
identify calls to the API as belonging to a specific GRASP session
(see Section 2.2). In fully threaded implementations this parameter
might not be needed, but it is included to act as a session handle if
necessary. It will also allow GRASP to detect and ignore malicious
calls or calls from timed-out sessions. A possible implementation is
to form the nonce from the underlying GRASP Session ID and the source address of the session.

2.3.2. Registration

These functions are used to register an ASA and the objectives that it supports with the GRASP module. If an authorization model is added to GRASP, it would also be added at this point in the API.

- **register_asa()**
  
  Input parameter:

  name of the ASA (UTF-8 string)

  Return parameters:

  - errorcode (integer)
  - asa_nonce (integer) (if successful)

  This initialise state in the GRASP module for the calling entity (the ASA). In the case of success, an ‘asa_nonce’ is returned which the ASA must present in all subsequent calls. In the case of failure, the ASA has not been authorized and cannot operate.

- **deregister_asa()**
  
  Input parameters:

  - asa_nonce (integer)
  - name of the ASA (UTF-8 string)

  Return parameter:

  - errorcode (integer)

  This removes all state in the GRASP module for the calling entity (the ASA), and deregisters any objectives it has registered. Note that these actions must also happen automatically if an ASA crashes.

  Note - the ASA name is strictly speaking redundant in this call, but is present for clarity.

- **register_objective()**
Input parameters:

asa_nonce (integer)

objective (structure)

ttl (integer - default GRASP_DEF_TIMEOUT)

discoverable (Boolean - default False)

overlap (Boolean - default False)

local (Boolean - default False)

Return parameter:

errorcode (integer)

This registers an objective that this ASA supports and may modify. The ‘objective’ becomes a candidate for discovery. However, discovery responses should not be enabled until the ASA calls listen_negotiate() or listen_synchronize(), showing that it is able to act as a responder. The ASA may negotiate the objective or send synchronization or flood data. Registration is not needed if the ASA only wants to receive synchronization or flood data for the objective concerned.

The ‘ttl’ parameter is the valid lifetime (time to live) in milliseconds of any discovery response for this objective. The default value should be the GRASP default timeout (GRASP_DEF_TIMEOUT, see [I-D.ietf-anima-grasp]).

If the parameter ‘discoverable’ is True, the objective is immediately discoverable. This is intended for objectives that are only defined for GRASP discovery, and which do not support negotiation or synchronization.

If the parameter ‘overlap’ is True, more than one ASA may register this objective in the same GRASP instance.

If the parameter ‘local’ is True, discovery must return a link-local address. This feature is for objectives that must be restricted to the local link.

This call may be repeated for multiple objectives.

- deregister_objective()
2.3.3. Discovery

**discover()**

- **Input parameters:**
  - asa_nonce (integer)
  - objective (structure)
  - timeout (integer)
  - flush (Boolean - default False)

- **Return parameters:**
  - errorcode (integer)
  - locator_list (structure)

This returns a list of discovered ‘ASA_locator’s for the given objective. If the parameter ‘flush’ is True, any locally cached locators for the objective are deleted first. Otherwise, they are returned immediately. If not, GRASP discovery is performed, and all results obtained before the timeout expires are returned. If no results are obtained, an empty list is returned after the timeout. That is not an error condition.

Threaded implementation: This should be called in a separate thread if asynchronous operation is required.

Event loop implementation: An additional read/write ‘session_nonce’ parameter is used.
2.3.4. Negotiation

- request_negotiate()

  Input parameters:
  - asa_nonce (integer)
  - objective (structure)
  - peer (ASA_locator)
  - timeout (integer)

  Return parameters:
  - errorcode (integer)
  - session_nonce (structure) (if successful)
  - proffered_objective (structure) (if successful)
  - reason (string) (if negotiation declined)

  This function opens a negotiation session. The 'objective' parameter must include the requested value, and its loop count should be set to a suitable value by the ASA. If not, the GRASP default will apply.

  Note that a given negotiation session may or may not be a dry-run negotiation; the two modes must not be mixed in a single session.

  The 'peer' parameter is the target node; it must be an 'ASA_locator' as returned by discover(). If the peer is null, GRASP discovery is performed first.

  If the 'errorcode' return parameter is 0, the negotiation has successfully started. There are then two cases:

  1. The 'session_nonce' parameter is null. In this case the negotiation has succeeded (the peer has accepted the request). The returned 'proffered_objective' contains the value accepted by the peer.

  2. The 'session_nonce' parameter is not null. In this case negotiation must continue. The returned 'proffered_objective' contains the first value proffered by
the negotiation peer. Note that this instance of the objective must be used in the subsequent negotiation call because it also contains the current loop count. The 'session_nonce' must be presented in all subsequent negotiation steps.

This function must be followed by calls to 'negotiate_step' and/or 'negotiate_wait' and/or 'end_negotiate' until the negotiation ends. 'request_negotiate' may then be called again to start a new negotiation.

If the 'errorcode' parameter has the value 1 ('declined'), the negotiation has been declined by the peer (M_END and O_DECLINE features of GRASP). The 'reason' string is then available for information and diagnostic use, but it may be a null string. For this and any other error code, an exponential backoff is recommended before any retry.

Threaded implementation: This should be called in a separate thread if asynchronous operation is required.

Event loop implementation: The 'session_nonce' parameter is used in read/write mode.

Special note for the ACP infrastructure ASA: It is likely that this ASA will need to discover and negotiate with its peers in each of its on-link neighbors. It will therefore need to know not only the link-local IP address but also the physical interface and transport port for connecting to each neighbor. One implementation approach to this is to include these details in the 'session_nonce' data structure, which is opaque to normal ASAs.

- listen_negotiate()

  Input parameters:
  
  asa_nonce (integer)

  objective (structure)

  Return parameters:

  errorcode (integer)

  session_nonce (structure) (if successful)

  requested_objective (structure) (if successful)
This function instructs GRASP to listen for negotiation requests for the given ‘objective’. It also enables discovery responses for the objective.

Threaded implementation: It will block waiting for an incoming request, so should be called in a separate thread if asynchronous operation is required.

Event loop implementation: A read/write ‘session_nonce’ parameter is used.

Unless there is an unexpected failure, this call only returns after an incoming negotiation request. When it does so, ‘requested_objective’ contains the first value requested by the negotiation peer. Note that this instance of the objective must be used in the subsequent negotiation call because it also contains the current loop count. The ‘session_nonce’ must be presented in all subsequent negotiation steps.

This function must be followed by calls to ‘negotiate_step’ and/or ‘negotiate_wait’ and/or ‘end_negotiate’ until the negotiation ends. ‘listen_negotiate’ may then be called again to await a new negotiation.

If an ASA is capable of handling multiple negotiations simultaneously, it may call ‘listen_negotiate’ simultaneously from multiple threads. The API and GRASP implementation must support re-entrant use of the listening state and the negotiation calls. Simultaneous sessions will be distinguished by the threads themselves, the GRASP Session IDs, and the underlying unicast transport sockets.

o stop_listen_negotiate()

Input parameters:

  asa_nonce (integer)

  objective (structure)

Return parameter:

  errorcode (integer)

Instructs GRASP to stop listening for negotiation requests for the given objective, i.e., cancels ‘listen_negotiate’.
Threaded implementation: Must be called from a different thread than 'listen_negotiate'.

Event loop implementation: no special considerations.

- **negotiate_step()**

  Input parameters:
  - asa_nonce (integer)
  - session_nonce (structure)
  - objective (structure)
  - timeout (integer)

  Return parameters:
  - Exactly as for 'request_negotiate'

  Executes the next negotiation step with the peer. The 'objective' parameter contains the next value being proffered by the ASA in this step.

  Threaded implementation: Called in the same thread as the preceding 'request_negotiate' or 'listen_negotiate', with the same value of 'session_nonce'.

  Event loop implementation: Must use the same value of 'session_nonce' returned by the preceding 'request_negotiate' or 'listen_negotiate'.

- **negotiate_wait()**

  Input parameters:
  - asa_nonce (integer)
  - session_nonce (structure)
  - timeout (integer)

  Return parameters:
  - errorcode (integer)

  Delay negotiation session by 'timeout' milliseconds.
Threaded implementation: Called in the same thread as the preceding ‘request_negotiate’ or ‘listen_negotiate’, with the same value of ‘session_nonce’.

Event loop implementation: Must use the same value of ‘session_nonce’ returned by the preceding ‘request_negotiate’ or ‘listen_negotiate’.

- end_negotiate()

Input parameters:

  asa_nonce (integer)

  session_nonce (structure)

  reply (Boolean)

  reason (UTF-8 string)

Return parameters:

  errorcode (integer)

End the negotiation session.

‘reply’ = True for accept (successful negotiation), False for decline (failed negotiation).

‘reason’ = optional string describing reason for decline.

Threaded implementation: Called in the same thread as the preceding ‘request_negotiate’ or ‘listen_negotiate’, with the same value of ‘session_nonce’.

Event loop implementation: Must use the same value of ‘session_nonce’ returned by the preceding ‘request_negotiate’ or ‘listen_negotiate’.

### 2.3.5. Synchronization and Flooding

- synchronize()

Input parameters:

  asa_nonce (integer)

  objective (structure)
peer (ASA_locator)

timeout (integer)

Return parameters:

errorcode (integer)

objective (structure) (if successful)

This call requests the synchronized value of the given ‘objective’.

Since this is essentially a read operation, any ASA can do it. Therefore the API checks that the ASA is registered but the objective doesn’t need to be registered by the calling ASA.

If the objective was already flooded, the flooded value is returned immediately in the ‘result’ parameter. In this case, the ‘source’ and ‘timeout’ are ignored.

Otherwise, synchronization with a discovered ASA is performed. The ‘peer’ parameter is an ‘ASA_locator’ as returned by discover(). If ‘peer’ is null, GRASP discovery is performed first.

This call should be repeated whenever the latest value is needed.

Threaded implementation: Call in a separate thread if asynchronous operation is required.

Event loop implementation: An additional read/write ‘session_nonce’ parameter is used.

Since this is essentially a read operation, any ASA can use it. Therefore GRASP checks that the calling ASA is registered but the objective doesn’t need to be registered by the calling ASA.

In the case of failure, an exponential backoff is recommended before retrying.

- listen_synchronize()

Input parameters:

asa_nonce (integer)
objective (structure)

Return parameters:

   errorcode (integer)

This instructs GRASP to listen for synchronization requests for the given objective, and to respond with the value given in the ‘objective’ parameter. It also enables discovery responses for the objective.

This call is non-blocking and may be repeated whenever the value changes.

- stop_listen_synchronize()

   Input parameters:

   asa_nonce (integer)

   objective (structure)

   Return parameters:

   errorcode (integer)

   This call instructs GRASP to stop listening for synchronization requests for the given ‘objective’, i.e. it cancels a previous listen_synchronize.

- flood()

   Input parameters:

   asa_nonce (integer)

   ttl (integer)

   tagged_objective_list (structure)

   Return parameters:

   errorcode (integer)

   This call instructs GRASP to flood the given synchronization objective(s) and their value(s) and associated locator(s) to all GRASP nodes.
The 'ttl' parameter is the valid lifetime (time to live) of the flooded data in milliseconds (0 = infinity)

The 'tagged_objective_list' parameter is a list of one or more 'tagged_objective' couplets. The 'locator' parameter that tags each objective is normally null but may be a valid 'ASA_locator'. Infrastructure ASAs needing to flood an (address, protocol, port) 3-tuple with an objective create an ASA_locator object to do so. If the IP address in that locator is the unspecified address ('::') it is replaced by the link-local address of the sending node in each copy of the flood multicast, which will be forced to have a loop count of 1. This feature is for objectives that must be restricted to the local link.

The function checks that the ASA registered each objective.

This call may be repeated whenever any value changes.

o get_flood()

Input parameters:

  asa_nonce (integer)
  objective (structure)

Return parameters:

  errorcode (integer)
  tagged_objective_list (structure) (if successful)

This call instructs GRASP to return the given synchronization objective if it has been flooded and its lifetime has not expired.

Since this is essentially a read operation, any ASA can do it. Therefore the API checks that the ASA is registered but the objective doesn’t need to be registered by the calling ASA.

The 'tagged_objective_list' parameter is a list of 'tagged_objective' couplets, each one being a copy of the flooded objective and a corresponding locator. Thus if the same objective has been flooded by multiple ASAs, the recipient can distinguish the copies.
Note that this call is for advanced ASAs. In a simple case, an ASA can simply call synchronize() in order to get a valid flooded objective.

- **expire_flood()**
  
  **Input parameters:**
  
  asa_nonce (integer)
  
  tagged_objective (structure)
  
  **Return parameters:**
  
  errorcode (integer)
  
  This is a call that can only be used after a preceding call to get_flood() by an ASA that is capable of deciding that the flooded value is stale or invalid. Use with care.

  The ’tagged_objective’ parameter is the one to be expired.

2.3.6. Invalid Message Function

- **send_invalid()**

  **Input parameters:**
  
  asa_nonce (integer)
  
  session_nonce (structure)
  
  info (bytes)
  
  **Return parameters:**
  
  errorcode (integer)
  
  Sends a GRASP Invalid Message (M_INVALID) message, as described in [I-D.ietf-anima-grasp]. Should not be used if end_negotiate() would be sufficient. Note that this message may be used in response to any unicast GRASP message that the receiver cannot interpret correctly. In most cases this message will be generated internally by a GRASP implementation.

  ’info’ = optional diagnostic data. May be raw bytes from the invalid message.
3. Implementation Status [RFC Editor: please remove]

A prototype open source Python implementation of GRASP, including an API similar to this document, has been used to verify the concepts for the threaded model. It may be found at <https://github.com/becarpenter/graspy> with associated documentation and demonstration ASAs.

4. Security Considerations

Security issues for the GRASP protocol are discussed in [I-D.ietf-anima-grasp]. Authorization of ASAs is a subject for future study.

The ‘asa_nonce’ parameter is used in the API as a first line of defence against a malware process attempting to imitate a legitimately registered ASA. The ‘session_nonce’ parameter is used in the API as a first line of defence against a malware process attempting to hijack a GRASP session.

5. IANA Considerations

This document currently makes no request of the IANA.

Open question: Do we need an IANA registry for the error codes?

6. Acknowledgements

Excellent suggestions were made by Ignas Bagdonas, Michael Richardson and other participants in the ANIMA WG.

7. References

7.1. Normative References

[I-D.ietf-anima-grasp]

7.2. Informative References

[I-D.ietf-anima-autonomic-control-plane]
Appendix A.  Error Codes

This Appendix lists the error codes defined so far, with suggested symbolic names and corresponding descriptive strings in English. It is expected that complete API implementations will provide for localisation of these descriptive strings, and that additional error codes will be needed according to implementation details.

An open issue for these values is whether there is an advantage in aligning them with existing error codes in the socket API, where the meanings coincide, and using different values otherwise. This is to be balanced against the advantage of having a compact and completely portable set of error codes for GRASP alone.
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ok</td>
<td>0 &quot;OK&quot;</td>
</tr>
<tr>
<td>declined</td>
<td>1 &quot;Declined&quot;</td>
</tr>
<tr>
<td>noReply</td>
<td>2 &quot;No reply&quot;</td>
</tr>
<tr>
<td>unspec</td>
<td>3 &quot;Unspecified error&quot;</td>
</tr>
<tr>
<td>ASAfull</td>
<td>4 &quot;ASA registry full&quot;</td>
</tr>
<tr>
<td>dupASA</td>
<td>5 &quot;Duplicate ASA name&quot;</td>
</tr>
<tr>
<td>noASA</td>
<td>6 &quot;ASA not registered&quot;</td>
</tr>
<tr>
<td>notYourASA</td>
<td>7 &quot;ASA registered but not by you&quot;</td>
</tr>
<tr>
<td>notBoth</td>
<td>8 &quot;Objective cannot support both negotiation and synchronization&quot;</td>
</tr>
<tr>
<td>notDry</td>
<td>9 &quot;Dry-run allowed only with negotiation&quot;</td>
</tr>
<tr>
<td>notOverlap</td>
<td>10 &quot;Overlap not supported by this implementation&quot;</td>
</tr>
<tr>
<td>objFull</td>
<td>11 &quot;Objective registry full&quot;</td>
</tr>
<tr>
<td>objReg</td>
<td>12 &quot;Objective already registered&quot;</td>
</tr>
<tr>
<td>notYourObj</td>
<td>13 &quot;Objective not registered by this ASA&quot;</td>
</tr>
<tr>
<td>notObj</td>
<td>14 &quot;Objective not found&quot;</td>
</tr>
<tr>
<td>notNeg</td>
<td>15 &quot;Objective not negotiable&quot;</td>
</tr>
<tr>
<td>noSecurity</td>
<td>16 &quot;No security&quot;</td>
</tr>
<tr>
<td>noDiscReply</td>
<td>17 &quot;No reply to discovery&quot;</td>
</tr>
<tr>
<td>sockErrNegRq</td>
<td>18 &quot;Socket error sending negotiation request&quot;</td>
</tr>
<tr>
<td>noSession</td>
<td>19 &quot;No session&quot;</td>
</tr>
<tr>
<td>noSocket</td>
<td>20 &quot;No socket&quot;</td>
</tr>
<tr>
<td>loopExhausted</td>
<td>21 &quot;Loop count exhausted&quot;</td>
</tr>
<tr>
<td>sockErrNegStep</td>
<td>22 &quot;Socket error sending negotiation step&quot;</td>
</tr>
<tr>
<td>noPeer</td>
<td>23 &quot;No negotiation peer&quot;</td>
</tr>
<tr>
<td>CBORfail</td>
<td>24 &quot;CBOR decode failure&quot;</td>
</tr>
<tr>
<td>invalidNeg</td>
<td>25 &quot;Invalid Negotiate message&quot;</td>
</tr>
<tr>
<td>invalidEnd</td>
<td>26 &quot;Invalid end message&quot;</td>
</tr>
<tr>
<td>noNegReply</td>
<td>27 &quot;No reply to negotiation step&quot;</td>
</tr>
<tr>
<td>noValidStep</td>
<td>28 &quot;No valid reply to negotiation step&quot;</td>
</tr>
<tr>
<td>sockErrWait</td>
<td>29 &quot;Socket error sending wait message&quot;</td>
</tr>
<tr>
<td>sockErrEnd</td>
<td>30 &quot;Socket error sending end message&quot;</td>
</tr>
<tr>
<td>IDclash</td>
<td>31 &quot;Incoming request Session ID clash&quot;</td>
</tr>
<tr>
<td>notSynch</td>
<td>32 &quot;Not a synchronization objective&quot;</td>
</tr>
<tr>
<td>notFloodDisc</td>
<td>33 &quot;Not flooded and no reply to discovery&quot;</td>
</tr>
<tr>
<td>sockErrSynRq</td>
<td>34 &quot;Socket error sending synch request&quot;</td>
</tr>
<tr>
<td>noListener</td>
<td>35 &quot;No synch listener&quot;</td>
</tr>
<tr>
<td>noSynchReply</td>
<td>36 &quot;No reply to synchronization request&quot;</td>
</tr>
<tr>
<td>noValidSynch</td>
<td>37 &quot;No valid reply to synchronization request&quot;</td>
</tr>
<tr>
<td>invalidLoc</td>
<td>38 &quot;Invalid locator&quot;</td>
</tr>
</tbody>
</table>

Appendix B. Change log [RFC Editor: Please remove]

draft-ietf-anima-grasp-api-03, 2019-01-21:

Replaced empty "logic flows" section by "implementation status". Minor clarifications.
Editorial improvements.
draft-ietf-anima-grasp-api-02, 2018-06-30:
Additional suggestion for event-loop API.
Discussion of error code values.
draft-ietf-anima-grasp-api-01, 2018-03-03:
Editorial updates
draft-ietf-anima-grasp-api-00, 2017-12-23:
WG adoption
Editorial improvements.
draft-liu-anima-grasp-api-06, 2017-11-24:
Improved description of event-loop model.
Changed intended status to Informational.
Editorial improvements.
draft-liu-anima-grasp-api-05, 2017-10-02:
Added send_invalid()
draft-liu-anima-grasp-api-04, 2017-06-30:
Noted that simple nodes might not include the API.
Minor clarifications.
draft-liu-anima-grasp-api-03, 2017-02-13:
Changed error return to integers.
Required all implementations to accept objective values in CBOR.
Added non-blocking alternatives.
draft-liu-anima-grasp-api-02, 2016-12-17:
Updated for draft-ietf-anima-grasp-09
draft-liu-anima-grasp-api-02, 2016-09-30:
Added items for draft-ietf-anima-grasp-07
Editorial corrections

draft-liu-anima-grasp-api-01, 2016-06-24:
Updated for draft-ietf-anima-grasp-05
Editorial corrections

draft-liu-anima-grasp-api-00, 2016-04-04:
Initial version

Authors' Addresses

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland 1142
New Zealand

Email: brian.e.carpenter@gmail.com

Bing Liu (editor)
Huawei Technologies
Q14, Huawei Campus
No.156 Beiqing Road
Hai-Dian District, Beijing 100095
P.R. China

Email: leo.liubing@huawei.com

Wendong Wang
BUPT University
Beijing University of Posts & Telecom.
No.10 Xitucheng Road
Hai-Dian District, Beijing 100876
P.R. China

Email: wdwang@bupt.edu.cn
Abstract

This document discusses the requirement to autonomic nodes supporting information distribution based over GRASP in autonomic networks. In general, information distribution can be categorized into two different modes: 1) one autonomic node instantly sends information to other nodes in the domain; 2) one autonomic node publishes some information and asynchronously some other interested nodes request the published information. In the former case, information data will be generated and consumed instantly. In the latter case, information data live longer in the network.

These capabilities are basic and fundamental to an autonomous network system (i.e. ANI [I-D.ietf-anima-reference-model]). This document clarifies possible use cases of information distribution in ANI and requirements to ANI so that rich information distribution can be natively supported. Extensions to autonomic nodes are proposed and detailed embodiments based on GRASP are discussed.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months.
1 Introduction

In an autonomic network, autonomic functions (AFs) running on autonomic nodes would exchange information constantly, both for controlling/management signaling and data exchange. This document discusses the information distribution capability of such exchanges between AFs.

According to the number of participants, information distribution can happen with the following scenarios:

1) Point-to-point (P2P) Communication: information are exchanged between two communicating parties from one node to another node.

2) One-to-Many Communication: information exchanges involve an information source and multiple receivers.

The approaches of distributing information could be categorized into two basic modes:

1) An instant communication: a sender connects and sends the information data (e.g. control/management signaling, synchronization data and so on) to the receiver(s) immediately.

2) An asynchronous communication: a sender saves the information in the network, may or may not publish the information to the other who is interested in the published information, to which a node asks to retrieve.

The ANI should have provided a generic way to support these information distribution scenarios among AFs, rather than AFs managing to use other transport or routing protocols (HTTP, BGP/IGP as bearing protocols etc.). In fact, GRASP already provides part of the capabilities.

In this document, we first analyze requirements of information distribution in autonomic networks (Section 3), and then introduce its relationship to the other modules in ANI (Section 4). After that, the node behaviors and extensions to the existing GRASP are introduced in Section 5 and Section 6, respectively.

2. Terminology
3. Requirements of Advanced Information Distribution

If the information exchanged is just short and simple, this can be done instantly. In practice, however, this is not always the case. In the following cases, a mixture of instant and asynchronous communication models is more appropriate.

1) Long Communication Intervals. The time interval of the communication is not necessarily always short and instant. Advanced AFs may rather involve heavy jobs/tasks (e.g. database lookup, authentication etc.) when gearing the network, so the instant mode may introduce unnecessary pending time and become less efficient. If simply using an instant mode, the AF has to wait until the tasks finish and return. A better way is that an AF instantly sends the request but switches to an synchronous mode, once the jobs are finished, AFs will get notified.

2) Common Interest Distribution. As mentioned, some information are common interests among AFs. For example, the network intent is distributed to network nodes enrolled, which is a typical one-to-many scenario. We can also finish the intent distribution by an instant flooding (e.g. via GRASP) to every network nodes across the network domain. Because of network dynamic, however, not every node can be just ready at the moment when the network intent is flooded. Actually, nodes may join in the network sequentially. In this situation, an asynchronous communication model could be a better choice where every (newly joining) node can subscribe the intent information and will get notified if it is ready (or updated).

3) Distributed Coordination. With computing and storage resources on autonomic nodes, alive AFs not only consumes but also generates data information. For example, AFs coordinating with each other as distributed schedulers, responding to service requests and distributing tasks. It is critical for those AFs to make correct decisions based on local information, which might be asymmetric as well. AFs may also need synthetic/aggregated data information (e.g. statistic info, like average values of several AFs, etc.) to make decisions. In these situations, AFs will need an efficient way to form a global view of the network (e.g. about resource consumption, bandwidth and statistics). Obviously, purely relying on instant communication model is inefficient, while a scalable, common, yet distributed data layer, on which AFs can store and share information in an asynchronous way, should be a better
choice.

For ANI, in order to support various communication scenarios, an information distribution module is required, and both instant and asynchronous communication models should be supported.

4. Information Distribution in ANI

This section describes how the information distribution module fits into the ANI including what extensions of GRASP are required [I-D.ietf-anima-grasp].

```
+-------------------+
|       ASAs        |
+-------------------+

^                      +------------------------Info-Dist. APIs-----------------------+
| | Selective Flooding |---| Event Queue |---| Info. Storage |
| +-------------------+   +-------------+   +---------------+ |
|                         +--------------------------------------------------------------|
|                         | ^
|                         | v
|                         | +-------------GRASP APIs----------------+|
|                         | | GRASP Base |---| Extension |
|                         | +---------------+   +---------------+ |
```

Figure 1. Information Distribution Module and GRASP Extension.

As the Fig 1 shows, the information distribution module includes three sub-modules, all of which provides APIs for ASAs. Specific behaviors of these modules is described in Section 5. In order to support the modules, the GRASP is also extended, which is described in Section 6.

5. Node Behaviors

In this section, we discuss how each autonomic node should behave in order to support the two modes of information distribution introduced before. ANI is a distributed system, so the information distribution module must be implemented in a distributed way as well, where every node participates to contribute.
5.1 Instant Information Distribution

In this case, sender(s) and receiver(s) are specified. Information will be directly sent from the sender(s) to the receiver(s). This requires that every node is equipped by some signaling/transport protocols so that they can coordinate with each other and correctly deliver the information.

5.1.1 Instant P2P and Flooding Communications

Current GRASP already provides the capability to support instant P2P and flooding. It is natural to use the GRASP Synchronization message directly for P2P distribution. Furthermore, it is also natural to use the GRASP Flood Synchronization message for broadcast.

However, as mentioned in Section 3, in some scenarios one node needs to actively send some information to another. GRASP Synchronization just lacks such capability, therefore an un-solicited synchronization mechanism is needed. An extension of GRASP message (i.e. M_UNSOLIDSYN) is defined in Section 6.1.

5.1.2 Instant Selective Flooding Communication

When doing selective flooding, the distributed information needs to contain the criteria for nodes to judge which interfaces should be sent the distributed information and which are not. Specifically, the criteria contain:

- Matching condition: a set of matching rules.
- Matching object: the object that the match condition would be applied to. For example, the matching object could be node itself or its neighbors.
- Action: what behavior the node needs to do when the matching object matches or failed the matching condition. For example, the action could be forwarding or discarding the distributed message.

The criteria information must be include in the message that carries the distributed information from the sender. The receiving node decides the action according to the criteria carried in the message. Still considering the criteria attached with the distributed information, the node behaviors can be:

- When the Matching Object is "Neighbors", then the node matches the relevant information of its neighbors to the Matching Condition. If the node finds one neighbor matches the Matching Condition, then it forwards the distributed message to the
neighbor. If not, the node discards forwarding the message to the neighbor.

- When the Matching Object is the node itself, then the node matches the relevant information of its own to the Matching Condition. If the node finds itself matches the Matching Condition, then it forwards the distributed message to its neighbors; if not, the node discards forwarding the message to the neighbors.

GRASP is extended with a new option field (i.e. selective-flood-option) to support selective flooding, shown in Section 6.2. This option will be included in the original flooding message of GRASP. An example of selective flooding is briefly described in the Appendix A.

5.2 Asynchronous Information Distribution

Asynchronous information distribution happens in a different way where sender(s) and receiver(s) are not immediately specified. Both senders and receivers may come up in an asynchronous way. First of all, this requires that the information can be stored; secondly, it requires an information publication and subscription (Pub/Sub) mechanism (corresponding protocol specification of Pub/Sub is defined in Section 6).

As we sketched in the previous section that in general each node requires two modules: 1) Information Storage (IS) module and 2) Event Queue (EQ) module in the information distribution module. We introduce details of the two modules in the following sections.

5.2.1 Information Storage

IS module handles how to save and retrieve information for ASAs across the network. The IS module uses a syntax to index information, generating the hash index value (e.g. a hash key) of the information and mapping the hash index to a certain node in ANI. Note that, this mechanism can use existing solutions. Specifically, storing information in an ANIMA network will be realized in the following steps.

1) ASA-to-IS Negotiation. An ASA calls the API provided by information distribution module (directly supported by IS sub-module) to request to store the information somewhere in the network. Such a request will be checked by the IS module who will be responsible for the request whether such a request is feasible according to criteria such as permitted information size.

2) Destination Node Mapping. The information block will be handled
by the IS module in order to calculate/map to a destination node in the network. Since ANIMA network is a peer-to-peer network, a typical way is to use dynamic hash table (DHT) to map information to a unique index identifier. For example, if the size of the information is reasonable, the information block itself can be hashed, otherwise, some meta-data of the information block can be used to generate the mapping.

3) Destination Node Negotiation Request. Negotiation request of storing the information will be sent from the IS module to the IS module on the destination node. The negotiation request contains parameters about the information block from the source IS module. According to the parameters as well as the local available resource, the destination node will feedback the source IS module.

4) Destination Node Negotiation Response. Negotiation response from the destination node is sent back to the source IS module. If the source IS module gets confirmation that the information can be stored, source IS module will prepare to transfer the information block; otherwise, a new destination node must be discovered (i.e. going to step 7).

5) Information Block Transfer. Before sending the information block to the destination node that accepts the request, the IS module of the source node will check if the information block can be afforded by one GRASP message. If so, the information block will be directly sent by calling a GRASP API. Otherwise, bulk data transmission with GRASP will be triggered, where multi-time GRASP message sending will be used so that one information block will be transferred by smaller pieces [I-D.ietf-anima-reference-model].

6) Information Writing. Once the information block (or a smaller block) is received, the IS module of the destination node will store the data block in the local storage, which is accessible.

7) (Optional) New Destination Node Discovery. If the previously selected destination node is not available to store the information block, the source IS module will have to identify a new destination node to start a new negotiation. In this case, the discovery can be done by using discovery GRASP API to identify a new candidate, or more complex mechanisms can be introduced.

Similarly, Getting information from an ANIMA network will be realized in the following steps.

1) ASA-to-IS Request. An ASA accesses the IS module via the APIs exposed by the information distribution module. The key/index of the interested information will be sent to the IS module. An
assumption here is that the key/index should be ready to an ASA before an ASA can ask for the information. This relates to the publishing/subscribing of the information, which are handled by other modules (e.g. Event Queue with Pub/Sub supported by GRASP).

2) Destination Node Mapping. IS module maps the key/index of the requested information to a destination node, and prepares to start to request the information. The mapping here follows the same mechanism when the information is stored.

3) Retrieval Negotiation Request. The source IS module sends a request to the destination node identified in the previous step and asks if such an information object is available.

4) Retrieval Negotiation Response. The destination node checks the key/index of the requested information, and replies to the source IS module. If the information is found and the information block can be afforded within one GRASP message, the information will be sent together with the response to the source IS module.

5) (Optional) New Destination Request. If the information is not found after the source IS module gets the response from the original destination node, the source IS module will have to discover where the location storing the requested information is.

IS module can reuse distributed databases and key value stores like NoSQL, Cassandra, DHT technologies. Storage and retrieval of information are all event-driven responsible by the EQ module.

5.2.2 Event Queue

The main job of Event Queue (EQ) module is to help ASAs to show interests to particular information and notify the occurrences of that in asynchronous communication scenarios. In ANI, information generated on network nodes is labeled as an event identified with an event ID, which is semantically related to the topic of the information. Key features of EQ module are summarized as follows.

1) Event Group: EQ module provides isolated queues for different event groups. If two groups of AFs could have completely different purposes or interests, EQ module allows to create multiple queues where only AFs interested in the same topic will be aware of the corresponding event queue.

2) Event Prioritization: Events do not have to be delivered in the same priority. This corresponds to how much important the event implies. Some of them are more urgent than regular ones. Prioritization allows AFs to differentiate events (i.e. information)
they publish/subscribe.

3) Event Matching: an information consumer has to be identified from the queue in order to deliver the information from the provider. Event matching keeps looking for the subscriptions in the queue to see if there is an exact published event there. Whenever a match is found, it will notify the upper layer to inform the corresponding ASAs who are the information provider and subscriber(s) respectively.

The procedure of how EQ module on every network node works is introduced as follows.

1) Event ID Generation: If information of an ASA is ready, an event ID is generated according to the content of the information. This is also related to how the information is stored/saved by the IS module introduced before. Meanwhile, the type of the event is also specified where it can be of control purpose or user plane data.

2) Priority Specification: According to the type of the event, the ASA may specify its priority to say how this event is wanted to be processed. By considering both aspects, the priority of the event will be determined and ready for enqueuing.

3) Event Enqueue: Given the event ID, event group and its priority, a queue is identified locally if all criteria can be satisfied. If there is such a queue, the event will be simply added into the queue, otherwise a new queue will be created to accommodate such an event.

4) Event Propagation: The published event will be propagated to the other network nodes in the ANIMA domain. A propagation algorithm can be employed to here in order to optimize the propagation efficiency of the updated event queue states.

5) Event Match and Notification: While propagating updated event states, EQ module in parallel keeps matching published events and its interested consumers. Once a match is found, the provider and subscriber(s) will be notified for final information retrieval.

Event contains the address where the information is stored, after a subscriber is notified, it directly retrieves the information from the given location.

5.2.3 Integrating with GRASP APIs

Actions triggered to the information distribution module will
eventually invoke underlying GRASP APIs. Moreover, EQ and IS modules are usually correlated. When an AF(ASA) publishes information, not only such an event is translated and sent to EQ module, but also the information is indexed and stored simultaneously. Similarly, when an AF(ASA) subscribes information, not only subscribing event is triggered and sent to EQ module, but also the information will be retrieved by IS module at the same time.

- Storing and publishing information: This action involves both IS and EQ modules where a node that can store the information will be discovered first and related event will be published to the network. For this, GRASP APIs `discover()`, `synchronize()` and `flood()` are combined to compose such a procedure. In specific, `discover()` call will specify its objective being to "store_data" and the return parameters could be either an ASA_locator who will accept to store the data, or an error code indicating that no one could afford such data; after that, `synchronize()` call will send the data to the specified ASA_locator and the data will be stored at that node, with return of processing results like `store_data_ack`; meanwhile, such a successful event (i.e. data is stored successfully) will be flooded via a `flood()` call to interesting parties (such a multicast group existed).

- Subscribing and getting information: This action involves both IS and EQ modules as well where a node that is interested in a topic will subscribe the topic by triggering EQ module and if the topic is ready IS module will retrieve the content of the topic (i.e. the data). GRASP APIs such as `register_objective()`, `flood()`, `synchronize()` are combined to compose the procedure. In specific, any subscription action received by EQ module will be translated to `register_objective()` call where the interested topic will be the parameter inside of the call; the registration will be (selectively) flooded to the network by an API call of `flood()` with the option we extended in this draft; once a matched topic is found (because of the previous procedure), the node finding such a match will call API `synchronize()` to send the stored data to the subscriber.

5.3 Summary

In summary, the general requirements for the information distribution module on each autonomic node are two sub-modules handling instant communications and asynchronous communications, respectively. For instant communications, node requirements are simple, in which signaling protocols have to be supported. With minimum efforts, reusing the existing GRASP is possible. For asynchronous communications, information distribution module requires event queue and information storage mechanism to be supported.
6. Protocol Specification (GRASP extension)

There are multiple ways to integrate the information distribution module. The principle we follow is to minimize modifications made to the current ANI. We consider to use GRASP as a base to build up the information distribution module. The main reason is that the current version of GRASP is already an information distribution module for the cases of P2P and flooding. In the following discussions, we introduce how to complete the missing part.

6.1 Un-solicited Synchronization Message (A new GRASP Message)

In fragmentary CDDL, a Un-solicited Synchronization message follows the pattern:

\[
\text{unsolicited_synch-message} = [\text{M_UNSOLIDSYNCH, session-id, objective}]
\]

A node MAY actively send a unicast Un-solicited Synchronization message with the Synchronization data, to another node. This MAY be sent to port GRASP_LISTEN_PORT at the destination address, which might be obtained by GRASP Discovery or other possible ways. The synchronization data are in the form of GRASP Option(s) for specific synchronization objective(s).

6.2 Selective Flooding Option

In fragmentary CDDL, the selective flood follows the pattern:

\[
\text{selective-flood-option} = [\text{O_SELECTIVE_FLOOD, +O_MATCH-CONDITION, match-object, action}]
\]

\[
\text{O_MATCH-CONDITION} = [\text{O_MATCH-CONDITION, Obj1, match-rule, Obj2}]
\]

\[
\text{Obj1} = \text{text}
\]

\[
\text{match-rule} = \text{GREATER / LESS / WITHIN / CONTAIN}
\]

\[
\text{Obj2} = \text{text}
\]

\[
\text{match-object} = \text{NEIGHBOR / SELF}
\]

\[
\text{action} = \text{FORWARD / DROP}
\]

The selective flood option encapsulates a match-condition option which represents the conditions regarding to continue or discontinue flood the current message. For the match-condition option, the Obj1 and Obj2 are to objects that need to be compared. For example, the Obj1 could be the role of the device and Obj2 could be "RSG". The match rules between the two objects could be greater, less than, within, or contain. The match-object represents of which Obj1 belongs to, it could be the device itself or the neighbor(s) intended to be flooded. The action means, when the match rule applies, the current device just continues flood or discontinues.
6.3 Subscription Objective Option

In fragmentary CDDL, a Subscription Objective Option follows the pattern:

```
subscription-objection-option = [SUBSCRIPTION, 2, 2, subobj]
objective-name = SUBSCRIPTION
objective-flags = 2
loop-count = 2
subobj = text
```

This option MAY be included in GRASP M_Synchronization, when included, it means this message is for a subscription to a specific object.

6.4 Un_Subscription Objective Option

In fragmentary CDDL, a Un_Subscribe Objective Option follows the pattern:

```
Unsubscribe-objection-option = [UNSUBSCRIB, 2, 2, unsubobj]
objective-name = SUBSCRIPTION
objective-flags = 2
loop-count = 2
unsubobj = text
```

This option MAY be included in GRASP M_Synchronization, when included, it means this message is for a un-subscription to a specific object.

6.5 Publishing Objective Option

In fragmentary CDDL, a Publish Objective Option follows the pattern:

```
publish-objection-option = [PUBLISH, 2, 2, pubobj] objective-name = PUBLISH
objective-flags = 2
loop-count = 2
pubobj = text
```

This option MAY be included in GRASP M_Synchronization, when included, it means this message is for a publish of a specific object data.

Note that extended GRASP messages with new arguments inside here will be triggered by interactions/actions from information distribution module introduced in Section 5.
7. Security Considerations

The distribution source authentication could be done at multiple layers:

- Outer layer authentication: the GRASP communication is within ACP (Autonomic Control Plane, [I-D.ietf-anima-autonomic-control-plane]). This is the default GRASP behavior.

- Inner layer authentication: the GRASP communication might not be within a protected channel, then there should be embedded protection in distribution information itself. Public key infrastructure might be involved in this case.

8. IANA Considerations

TBD.

9. References

9.1 Normative References

[I-D.ietf-anima-grasp]

9.2 Informative References


[I-D.ietf-anima-autonomic-control-plane]

[I-D.ietf-anima-stable-connectivity-10]

[I-D.ietf-anima-reference-model]
Appendix A.

GRASP includes flooding criteria together with the delivered information so that every node will process and act according to the criteria specified in the message. An example of extending GRASP with
selective criteria can be:

- Matching condition: "Device role=IPRAN_RSG"
- Matching objective: "Neighbors"
- Action: "Forward"

This example means: only distributing the information to the neighbors who are IPRAN_RSG.

Authors’ Addresses

Bing Liu
Huawei Technologies
Q27, Huawei Campus
No.156 Beiqing Road
Hai-Dian District, Beijing 100095
P.R. China

Email: leo.liubing@huawei.com

Sheng Jiang
Huawei Technologies
Q27, Huawei Campus
No.156 Beiqing Road
Hai-Dian District, Beijing 100095
P.R. China

Email: jiangsheng@huawei.com

Xun Xiao
Munich Research Center
Huawei technologies
Riesstr. 25, 80992, Muenchen, Germany

Emails: xun.xiao@huawei.com

Artur Hecker
Munich Research Center
Huawei technologies
Riesstr. 25, 80992, Muenchen, Germany

Emails: artur.hecker@huawei.com

Zoran Despotovic
Appendix A  Real-world Use Cases of Information Distribution

The requirement analysis in Section 3 shows that generally information distribution should be better of as an infrastructure layer module, which provides to upper layer utilizations. In this section, we review some use cases from the real-world where an information distribution module with powerful functions do plays a critical role there.

A.1 Service-Based Architecture (SBA) in 3GPP 5G

In addition to Internet, the telecommunication network (i.e. carrier mobile wireless networks) is another world-wide networking system. The architecture of the upcoming 5G mobile networks from 3GPP has already been defined to follow a service-based architecture (SBA) where any network function (NF) can be dynamically associated with any other NF(s) when needed to compose a network service. Note that one NF can simultaneously associate with multiple other NFs, instead of being physically wired as in the previous generations of mobile networks. NFs communicate with each other over service-based interface (SBI), which is also standardized by 3GPP [3GPP.23.501].

In order to realize an SBA network system, detailed requirements are further defined to specify how NFs should interact with each other with information exchange over the SBI. We now list three requirements that are related to information distribution here.

1) NF Pub/Sub: Any NF should be able to expose its service status to the network and any NF should be able to subscribe the service status of an NF and get notified if the status is available. An concrete example is that a session management function (SMF) can subscribe the REGISTER notification from an access management function (AMF) if there is a new user entity trying to access the mobile network [3GPP.23.502].

2) Network Exposure Function (NEF): A particular network function that is required to manage the event exposure and distributions. In specific, SBA requires such a functionality to register network events from the other NFs (e.g. AMF, SMF and so on), classify the events and properly handle event distributions accordingly in
terms of different criteria (e.g. priorities) [3GPP.23.502].

3) Network Repository Function (NRF): A particular network function where all service status information is stored for the whole network. An SBA network system requires all NFs to be stateless so as to improve the resilience as well as agility of providing network services. Therefore, the information of the available NFs and the service status generated by those NFs will be globally stored in NRF as a repository of the system. This clearly implies storage capability that keeps the information in the network and provides those information when needed. A concrete example is that whenever a new NF comes up, it first of all registers itself at NRF with its profile. When a network service requires a certain NF, it first inquires NRF to retrieve the availability information and decides whether or not there is an available NF or a new NF must be instantiated [3GPP.23.502].

(Note: 3GPP CT might finally adopt HTTP2.0/JSON to be the protocol communicating between NFs, but autonomic networks can also load HTTP2.0 with in ACP.)

A.2 Vehicle-to-Everything

Carrier networks On-boarding services of vertical industries are also one of some blooming topics that are heavily discussed. Connected car is clearly one of the important scenarios interested in automotive manufacturers, carriers and vendors. 5G Automotive Alliance - an industry collaboration organization defines many promising use cases where services from car industry should be supported by the 5G mobile network. Here we list two examples as follows [5GAA.use.cases].

1) Software/Firmware Update: Car manufacturers expect that the software/firmware of their car products can be remotely updated/upgraded via 5G network in future, instead of onsite visiting their 4S stores/dealers offline as nowadays. This requires the network to provide a mechanism for vehicles to receive the latest software updates during a certain period of time. In order to run such a service for a car manufacturer, the network shall not be just like a network pipe anymore. Instead, information data have to be stored in the network, and delivered in a publishing/subscribing fashion. For example, the latest release of a software will be first distributed and stored at the access edges of the mobile network, after that, the updates can be pushed by the car manufacturer or pulled by the car owner as needed.

2) Real-time HD Maps: Autonomous driving clearly requires much finer details of road maps. Finer details not only include the
details of just static road and streets, but also real-time information on the road as well as the driving area for both local urgent situations and intelligent driving scheduling. This asks for situational awareness at critical road segments in cases of changing road conditions. Clearly, a huge amount of traffic data that are real-time collected will have to be stored and shared across the network. This clearly requires the storage capability, data synchronization and event notifications in urgent cases from the network, which are still missing at the infrastructure layer.

A.3 Summary

Through the general analysis and the concrete examples from the real-world, we realize that the ways information are exchanged in the coming new scenarios are not just short and instant anymore. More advanced as well as diverse information distribution capabilities are required and should be generically supported from the infrastructure layer. Upper layer applications (e.g. ASAs in ANIMA) access and utilize such a unified mechanism for their own services.
Constrained Join Proxy for Bootstrapping Protocols

draft-vanderstok-anima-constrained-join-proxy-02

Abstract

This document defines a protocol to securely assign a pledge to an owner, using an intermediary node between pledge and owner. This intermediary node is known as a "constrained Join Proxy".

This document extends the work of [ietf-anima-bootstrapping-keyinfra] by replacing the Circuit-proxy by a stateless constrained Join Proxy, that transports routing information.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 6, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents.
1. Introduction

Enrolment of new nodes into constrained networks with constrained nodes present is described in [I-D.ietf-anima-bootstrapping-keyinfra] and makes use of Enrolment over Secure Transport (EST) [RFC7030]. The specified solutions use https and may be too large in terms of
code space or bandwidth required. Constrained devices in constrained networks [RFC7228] typically implement the IPv6 over Low-Power Wireless personal Area Networks (6LoWPAN) [RFC4944] and Constrained Application Protocol (CoAP) [RFC7252].

CoAP has chosen Datagram Transport Layer Security (DTLS) [RFC6347] as the preferred security protocol for authenticity and confidentiality of the messages. A constrained version of EST, using Coap and DTLS, is described in [I-D.ietf-ace-coap-est].

DTLS is a client-server protocol relying on the underlying IP layer to perform the routing between the DTLS Client and the DTLS Server. However, the new "joining" device will not be IP routable until it is authenticated to the network. A new "joining" device can only initially use a link-local IPv6 address to communicate with a neighbour node using neighbour discovery [RFC6775] until it receives the necessary network configuration parameters. However, before the device can receive these configuration parameters, it needs to authenticate itself to the network to which it connects. In [I-D.ietf-anima-bootstrapping-keyinfra] Enrolment over Secure Transport (EST) [RFC7030] is used to authenticate the joining device. However, IPv6 routing is necessary to establish a connection between joining device and the EST server.

This document specifies a Join Proxy and protocol to act as intermediary between joining device and EST server to establish a connection between joining device and EST server.

This document is very much inspired by text published earlier in [I-D.kumar-dice-dtls-relay].

2. Terminology

The following terms are defined in [RFC8366], and are used identically as in that document: artifact, imprint, domain, Join Registrar/Coordinator (JRC), Manufacturer Authorized Signing Authority (MASA), pledge, Trust of First Use (TOFU), and Voucher.

3. Requirements Language

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119] and indicate requirement levels for compliant STuPiD implementations.
4. Join Proxy functionality

As depicted in the Figure 1, the joining Device, or pledge (P), is more than one hop away from the EST server (E) and not yet authenticated into the network. At this stage, it can only communicate one-hop to its nearest neighbour, the Join Proxy (J) using their link-local IPv6 addresses. However, the Pledge (P) needs to communicate with end-to-end security with a Registrar hosting the EST server (E) to authenticate and get the relevant system/network parameters. If the Pledge (P) initiates a DTLS connection to the EST server whose IP address has been pre-configured, then the packets are dropped at the Join Proxy (J) since the Pledge (P) is not yet admitted to the network or there is no IP routability to Pledge (P) for any returned messages.

![Figure 1: multi-hop enrolment.](image)

Furthermore, the Pledge (P) may wish to establish a secure connection to the EST server (E) in the network assuming appropriate credentials are exchanged out-of-band, e.g. a hash of the Pledge (P)’s raw public key could be provided to the EST server (E). However, the Pledge (P) may be unaware of the IP address of the EST-server (E) to initiate a DTLS connection and perform authentication with.

A DTLS connection is required between Pledge and EST server. To overcome the problems with non-routability of DTLS packets and/or discovery of the destination address of the EST Server to contact, the Join Proxy is introduced. This Join Proxy functionality is configured into all authenticated devices in the network which may act as the Join Proxy for newly joining nodes. The Join Proxy allows for routing of the packets from the Pledge using IP routing to the intended EST Server.

5. Join Proxy specification

The Join Proxy can operate in two modes:

- Statefull mode
5.1. Statefull Join Proxy

In stateful mode, the joining node forwards the DTLS messages to the EST Server.

Assume that the Pledge does not know the IP address of the EST Server it needs to contact. In that situation, the Join Proxy knows the (configured or discovered) IP address of a EST Server that the Pledge needs to contact. The Pledge initiates its request as if the Join Proxy is the intended EST Server. The Join Proxy changes the IP packet (without modifying the DTLS message) as in the previous case by modifying both the source and destination addresses to forward the message to the intended EST Server. The Join Proxy maintains a 4-tuple array to translate the DTLS messages received from the EST Server and forward it to the EST Client. In Figure 2 the various steps of the message flow are shown:

<table>
<thead>
<tr>
<th>EST Client</th>
<th>Join Proxy</th>
<th>EST Server</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>(P)</td>
<td>(J)</td>
<td>(E)</td>
<td>Src_IP:port</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Dst_IP:port</td>
</tr>
</tbody>
</table>

+------------------;+------------------;+------------------;+------------------+
| EST Client     | Join Proxy  | EST Server   | Message          |
| (P)            | (J)         | (E)          | Src_IP:port      |
|                |             |              | Dst_IP:port      |
| --ClientHello--|            |              | IP_P:p_P         |
| --ClientHello--|            |              | IP_Ja:5684       |
| <--ServerHello--|              |              | IP_E:5684        |
|                 |              |              | IP_Jb:p_Jb       |

IP_P:p_P = Link-local IP address and port of Pledge (DTLS Client)
IP_E:5684 = Global IP address and coaps port of EST Server
IP_Ja:5684 = Link-local IP address and coaps port of Join Proxy
IP_Jb:p_Jb = Global IP address and port of Join proxy

Figure 2: constrained statefull joining message flow with EST server address known to Join Proxy.
5.2. Stateless Join Proxy

The Join Proxy is stateless to minimize the requirements on the constrained Join Proxy device.

When a joining device as a client attempts a DTLS connection to the EST server, it uses its link-local IP address as its IP source address. This message is transmitted one-hop to a neighbour node. Under normal circumstances, this message would be dropped at the neighbour node since the joining device is not yet IP routable or it is not yet authenticated to send messages through the network. However, if the neighbour device has the Join Proxy functionality enabled, it routes the DTLS message to a specific EST Server. Additional security mechanisms need to exist to prevent this routing functionality being used by rogue nodes to bypass any network authentication procedures.

If an untrusted DTLS Client that can only use link-local addressing wants to contact a trusted end-point EST Server, it sends the DTLS message to the Join Proxy. The Join Proxy extends this message into a new type of message called Join ProxY (JPY) message and sends it on to the EST server. The JPY message payload consists of two parts:

- Header (H) field: consisting of the source link-local address and port of the Pledge (P), and
- Contents (C) field: containing the original DTLS message.

On receiving the JPY message, the EST Server retrieves the two parts. The EST Server transiently stores the Header field information. The EST server uses the Contents field to execute the EST server functionality. However, when the EST Server replies, it also extends its DTLS message with the header field in a JPY message and sends it back to the Join Proxy. The Header contains the original source link-local address and port of the DTLS Client from the transient state stored earlier (which can now be discarded) and the Contents field contains the DTLS message.

On receiving the JPY message, the Join Proxy retrieves the two parts. It uses the Header field to route the DTLS message retrieved from the Contents field to the Pledge.

The Figure 3 depicts the message flow diagram:
## 5.3. Stateless Message structure

The JPY message is constructed as a payload with media-type application/multipart-core specified in [I-D.ietf-core-multipart-ct]. Header and Contents fields use different media formats:

1. **header field:** application/CBOR containing a CBOR array [RFC7049] with the pledge IPv6 Link Local address as a 16-byte binary value, the pledge’s UDP port number, if different from 5684, as a CBOR integer, and the proxy’s ifindex or other identifier for the physical port on which the pledge is connected. Header is not DTLS encrypted.

2. **Content field:** Any of the media types specified in [I-D.ietf-ace-coap-est] and [I-D.ietf-anima-constrained-voucher] dependent on the function that is requested:

### Table: Join-Proxy Message Flow

<table>
<thead>
<tr>
<th>EST Client (P)</th>
<th>Join Proxy (J)</th>
<th>EST server (E)</th>
<th>Message Src_IP:port</th>
<th>Dst_IP:port</th>
</tr>
</thead>
<tbody>
<tr>
<td>--ClientHello--</td>
<td></td>
<td></td>
<td>IP_P:p_P</td>
<td>IP_Ja:5684</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IP_Jb:p_Jb</td>
<td>IP_E:5684</td>
</tr>
<tr>
<td>&lt;--JPY[H(IP_P:p_P),--</td>
<td></td>
<td></td>
<td>IP_E:5684</td>
<td>IP_Jb:p_Jb</td>
</tr>
<tr>
<td></td>
<td>C(ClientHello)]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;--JPY[H(IP_P:p_P),--</td>
<td></td>
<td></td>
<td>IP_E:5684</td>
<td>IP_Jb:p_Jb</td>
</tr>
<tr>
<td></td>
<td>C(ServerHello)]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--ServerHello--</td>
<td></td>
<td></td>
<td>IP_Ja:5684</td>
<td>IP_P:p_P</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--Finished--&gt;</td>
<td></td>
<td></td>
<td>IP_P:p_P</td>
<td>IP_Ja:5684</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IP_Jb:p_Jb</td>
<td>IP_E:5684</td>
</tr>
<tr>
<td>&lt;--JPY[H(IP_P:p_P),--</td>
<td></td>
<td></td>
<td>IP_E:5684</td>
<td>IP_Jb:p_Jb</td>
</tr>
<tr>
<td></td>
<td>C(Finished)]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;--Finished--</td>
<td></td>
<td></td>
<td>IP_Ja:5684</td>
<td>IP_P:p_P</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IP_P:p_P** = Link-local IP address and port of the Pledge  
**IP_E:5684** = Global IP address and coaps port of EST Server  
**IP_Ja:5684** = Link-local IP address and coaps port of Join Proxy  
**IP_Jb:p_Jb** = Global IP address and port of Join Proxy

**JPY[H(),C()]** = Join Proxy message with header H and content C

Figure 3: constrained stateless joining message flow.
The content fields are DTLS encrypted. In CBOR diagnostic notation the payload JPY[H(IP_P:p_P), with cf is content-format of DTLS-content, will look like:

\[
[60: [IP_p, p_P, ident]
\text{cf: h'DTLS-content'}]
\]

Examples are shown in Appendix A.

6. Comparison of stateless and statefull modes

The stateful and stateless mode of operation for the Join Proxy have their advantages and disadvantages. This section should enable to make a choice between the two modes based on the available device resources and network bandwidth.
Properties | Stateful mode | Stateless mode |
---|---|---|
State Information | The Join Proxy needs additional storage to maintain mapping between the address and port number of the pledge and those of the EST-server. | No information is maintained by the Join Proxy |
Packet size | The size of the forwarded message is the same as the original message. | Size of the forwarded message is bigger than the original, it includes additional source and destination addresses. |
Specification complexity | The Join Proxy needs additional functionality to maintain state information, and modify the source and destination addresses of the DTLS handshake messages. | New JPY message to encapsulate DTLS message The EST server and the Join Proxy have to understand the JPY message in order to process it. |

Figure 4: Comparison between stateful and stateless mode

7. Discovery

It is assumed that Join Proxy seamlessly provides a coaps connection between Pledge and coaps EST-server. An additional Registrar is needed to connect the Pledge to an http EST server, see section 8 of [I-D.ietf-ace-coap-est]. In particular this section replaces section 4.2 of [I-D.ietf-anima-bootstrapping-keyinfra].

Three discovery cases are discussed: coap discovery, 6tisch discovery and GRASP discovery.

7.1. Join Proxy discovers EST server

7.1.1. Coap discovery

The discovery of the coaps EST server, using coap discovery, by the Join Proxy follows section 6 of [I-D.ietf-ace-coap-est].
7.1.2. Autonomous Network

In the context of autonomous networks, the Join Proxy uses the DULL GRASP M_FLOOD mechanism to announce itself. Section 4.1.1 of [I-D.ietf-anima-bootstrapping-keyinfra] discusses this in more detail. The EST-server announces itself using ACP instance of GRASP using M_FLOOD messages. Autonomous Network Join Proxies MUST support GRASP discovery of EST-server as described in section 4.3 of [I-D.ietf-anima-bootstrapping-keyinfra].

7.1.3. 6tisch discovery

The discovery of EST server by the pledge uses the enhanced beacons as discussed in [I-D.ietf-6tisch-enrollment-enhanced-beacon].

7.2. Pledge discovers Join Proxy

The pledge and Join Proxy are assumed to communicate via Link-Local addresses.

7.2.1. Autonomous Network

The pledge MUST listen for GRASP M_FLOOD [I-D.ietf-anima-grasp] announcements of the objective: "AN_Proxy". See section 4.1.1 [I-D.ietf-anima-bootstrapping-keyinfra] for the details of the objective.

7.2.2. Coap discovery

In the context of a CoAP network without Autonomous Network support, discovery follows the standard CoAP policy. The Pledge can discover a Join Proxy by sending a link-local multicast message to ALL CoAP Nodes with address FF02::FD. Multiple or no nodes may respond. The handling of multiple responses and the absence of responses follow section 4 of [I-D.ietf-anima-bootstrapping-keyinfra].

The presence and location of (path to) the Join Proxy resource are discovered by sending a GET request to "/.well-known/core" including a resource type (rt) parameter with the value "brski-proxy" [RFC6690]. Upon success, the return payload will contain the root resource of the Join Proxy resources. It is up to the implementation to choose its root resource; throughout this document the example root resource /jp is used. The example below shows the discovery of the presence and location of Join Proxy resources.
REQ: GET coap://[FF02::FD]/.well-known/core?rt=brski-proxy

RES: 2.05 Content
   </jp>; rt="brski-proxy";ct=62

Port numbers, not returned in the example, are assumed to be the
default numbers 5683 and 5684 for coap and coaps respectively
(sections 12.6 and 12.7 of [RFC7252]). Discoverable port numbers MAY
be returned in the <href> of the payload (see section 5.1 of
[I-D.ietf-ace-coap-est]).

8. Security Considerations

It should be noted here that the contents of the CBOR map are not
protected, but that the communication is between the Proxy and a
known registrar (a connected UDP socket), and that messages from
other origins are ignored.

9. IANA Considerations

This document needs to create a registry for key indices in the CBOR
map. It should be given a name, and the amending formula should be
IETF Specification.

9.1. Resource Type registry

This specification registers a new Resource Type (rt=) Link Target
Attributes in the "Resource Type (rt=) Link Target Attribute Values"
subregistry under the "Constrained RESTful Environments (CoRE)
Parameters" registry.

   rt="brski-proxy". This EST resource is used to query and return
the supported EST resource of a Join Proxy placed between Pledge
and EST server.

10. Acknowledgements

Many thanks for the comments by Brian Carpenter.

11. Contributors

Sandee p Kumar, Sye loong Keoh, and Oscar Garcia-Morchon are the co-
authors of the draft-kumar-dice-dtls-relay-02. Their draft has
served as a basis for this document. Much text from their draft is
copied over to this draft.
12. Changelog

12.1. 01 to 02
- extended the discovery section
- removed inconsistencies from the flow diagrams
- improved readability of the examples.
- stateful configurations reduced to one

12.2. 00 to 01
- added Contributors section
- adapted content-formats to est-coaps formats
- aligned examples with est-coaps examples
- added statefull Proxy to stateless proxy

12.3. 00 to 00
- added payload examples in appendix
- discovery for three cases: AN, 6tisch and coaps

13. References

13.1. Normative References

[I-D.ietf-6tisch-enrollment-enhanced-beacon]

[I-D.ietf-ace-coap-est]

[I-D.ietf-anima-bootstrapping-keyinfra]


13.2. Informative References


Appendix A. Stateless Proxy payload examples

Examples are extensions of two examples shown in [I-D.ietf-ace-coap-est]. The following content formats are used:

- 60: application/cbor
- 62: application/multipart
- 281: application/pkcs7-mime; smime-type=certs-only
- 284: application/pkcs8
- 286: application/pkcs10
For presentation purposes the payloads are abbreviated as follows:

cacrts request payload:

\[
<\text{cacrts request payload}> = \langle\text{empty}\rangle
\]

cacrts response payload:

\[
<\text{cacrts response payload}> =
\text{DTLS\_encrypt}(\text{...})
\]

serverkeygen request payload:

\[
<\text{serverkeygen request payload}> =
\text{DTLS\_encrypt}(\text{...})
\]

serverkeygen response payload:

\[
<\text{serverkeygen response payload}> =
\text{DTLS\_encrypt}(\text{...})
\]
A.1. cacerts

The request from Join Proxy to EST-server looks like:

```
Get coaps://192.0.2.1/est/crts
(Accept: 62)
(Content-format: 62)

payload =
```

```
82                     # array(2)
3C                     # unsigned(60)
83                     # array(3)
69                     # text(9)
464538303A3A14238     # "FE80::AB8"
237D                   # unsigned(9085)
65                     # text(5)
9646565E74            # "ident"
```

In CBOR Diagnostic:

payload = [60, ["FE80::AB8", 9085, "ident"]]

The response will then be:

2.05 Content
(Content-format: 62)
 Payload =
  84 # array(4)
  18 3C # unsigned(60)
  83 # array(3)
  69 # text(9)
    464538303A3A414238 # "FE80::AB8"
  19 237D # unsigned(9085)
  65 # text(5)
    "ident"
  19 0119 # unsigned(281)
  59 027F # bytes(639)
  <cacrts response payload>
}

In CBOR diagnostic:

payload = [60, ["FE80::AB8", 9085, "ident"], 62, h'cacrts response payload']

A.2. serverkeygen

The request from Join Proxy to EST-server looks like:

Get coaps://192.0.2.1/est/skg
 (Accept: 62)
 (Content-Format: 62)
 Payload =
  83 # array(4)
  18 3C # unsigned(60)
  83 # array(3)
  69 # text(9)
    464538303A3A414238 # "FE80::AB8"
  19 237D # unsigned(9085)
  65 # text(5)
    "ident"
  19 011E # unsigned(286)
  58 D2 # bytes(210)
 <serverkeygen request payload>

In CBOR diagnostic:
payload = [60, ["FE80::AB8", 9085, "ident"],
    286, h’<serverkeygen request payload’]

The response will then be:

2.05 Content
(Content-format: 62)
Payload =
83                                # array(4)
18 3C                             # unsigned(60)
83                                # array(3)
69                                 # text(9)
    464538303A3A414238            # "FE80::AB8"
19 237D                           # unsigned(9085)
65                                 # text(5)
    6964656E74                    # "ident"
19 011E                           # unsigned(286)
59 0269                           # bytes(617)
<serverkeygen response payload>

In CBOR diagnostic:

payload = [60, ["FE80::AB8", 9085, "ident"],
    286, h’<serverkeygen response payload’]

Authors’ Addresses

Michael Richardson
Sandelman Software Works
Email: mcr+ietf@sandelman.ca

Peter van der Stok
vanderstok consultancy
Email: consultancy@vanderstok.org

Panos Kampanakis
Cisco Systems
Email: pkampana@cisco.com