

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 7 September 2022

O. Friel
Cisco
R. Shekh-Yusef
Auth0
M. Richardson
Sandelman Software Works
6 March 2022

BRSKI Cloud Registrar
draft-ietf-anima-brski-cloud-03

Abstract

This document specifies the behaviour of a BRSKI Cloud Registrar, and how a pledge can interact with a BRSKI Cloud Registrar when bootstrapping.

RFCED REMOVE: It is being actively worked on at <https://github.com/anima-wg/brski-cloud>

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 7 September 2022.

Copyright Notice

Copyright (c) 2022 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

Internet-Draft

BRSKI-CLOUD

March 2022

extracted from this document must include Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

Table of Contents

1.	Introduction	3
1.1.	Terminology	3
1.2.	Target Use Cases	3
1.2.1.	Owner Registrar Discovery	4
1.2.2.	Bootstrapping with no Owner Registrar	4
2.	Architecture	5
2.1.	Interested Parties	6
2.2.	Network Connectivity	6
2.3.	Pledge Certificate Identity Considerations	6
3.	Protocol Operation	7
3.1.	Pledge Requests Voucher from Cloud Registrar	7
3.1.1.	Cloud Registrar Discovery	7
3.1.2.	Pledge - Cloud Registrar TLS Establishment Details	7
3.1.3.	Pledge Issues Voucher Request	8
3.2.	Cloud Registrar Handles Voucher Request	8
3.2.1.	Pledge Ownership Lookup	8
3.2.2.	Cloud Registrar Redirects to Owner Registrar	9
3.2.3.	Cloud Registrar Issues Voucher	9
3.3.	Pledge Handles Cloud Registrar Response	9
3.3.1.	Redirect Response	9
3.3.2.	Voucher Response	10
4.	Protocol Details	10
4.1.	Voucher Request Redirected to Local Domain Registrar	10
4.2.	Voucher Request Handled by Cloud Registrar	12
5.	YANG extension for Voucher based redirect	14
5.1.	YANG Tree	14
5.2.	YANG Voucher	15
6.	IANA Considerations	17
6.1.	The IETF XML Registry	17
6.2.	The YANG Module Names Registry	17
7.	Security Considerations	18
7.1.	Issues with Security of HTTP Redirect	18
7.2.	Security Updates for the Pledge	19
7.3.	Trust Anchors for Cloud Registrar	19
7.4.	Issues with Redirect via Voucher	20
8.	References	20
8.1.	Normative References	20

8.2. Informative References	21
Authors' Addresses	22

[1.](#) Introduction

Bootstrapping Remote Secure Key Infrastructures [[BRSKI](#)] specifies automated bootstrapping of an Autonomic Control Plane. BRSKI [Section 2.7](#) describes how a 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".

This document further specifies use of a BRSKI cloud registrar and clarifies operations that are not sufficiently specified in BRSKI.

[1.1.](#) 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.

This document uses the terms Pledge, Registrar, MASA, and Voucher from [[BRSKI](#)] and [[RFC8366](#)].

- * Local Domain: The domain where the pledge is physically located and bootstrapping from. This may be different to the pledge owner's domain.
- * Owner Domain: The domain that the pledge needs to discover and bootstrap with.
- * Cloud Registrar: The default Registrar that is deployed at a URI that is well known to the pledge.
- * Owner Registrar: The Registrar that is operated by the Owner, or the Owner's delegate. There may not be an Owner Registrar in all deployment scenarios.

- * Local Domain Registrar: The Registrar discovered on the Local Domain. There may not be a Local Domain Registrar in all deployment scenarios.

[1.2.](#) Target Use Cases

Two high level use cases are documented here. There are more details provided in sections [Section 4.1](#) and [Section 4.2](#). While both use cases aid with incremental deployment of BRSKI infrastructure, for many smaller sites (such as teleworkers) no further infrastructure are expected.

The pledge is not expected to know which of these two situations it is in. The pledge determines this based upon signals that it receives from the Cloud Registrar. The Cloud Registrar is expected to make the determination based upon the identity presented by the pledge.

While a Cloud Registrar will typically handle all the devices of a particular product line from a particular manufacturer there are no restrictions on how the Cloud Registrar is horizontally (many sites) or vertically (more equipment at one site) scaled. It is also entirely possible that all devices sold by through a particular VAR might be preloaded with a configuration that changes the Cloud Registrar URL to point to a VAR. Such an effort would require unboxing each device in a controlled environment, but the provisioning could occur using a regular BRSKI or SZTP [[RFC8572](#)] process.

[1.2.1.](#) Owner Registrar Discovery

A pledge is bootstrapping from a remote location with no local domain registrar (specifically: with no local infrastructure to provide for automated discovery), and needs to discover its owner registrar. The cloud registrar is used by the pledge to discover the owner registrar. The cloud registrar redirects the pledge to the owner registrar, and the pledge completes bootstrap against the owner registrar.

A typical example is an enduser deploying a pledge in a home or small branch office, where the pledge belongs to the enduser's employer.

There is no local domain registrar, and the pledge needs to discover and bootstrap with the employer's registrar which is deployed in headquarters. For example, an enduser is deploying an IP phone in a home office and the phone needs to register to an IP PBX deployed in their employer's office.

[1.2.2.](#) Bootstrapping with no Owner Registrar

A pledge is bootstrapping where the owner organization does not yet have an owner registrar deployed. The cloud registrar issues a voucher, and the pledge completes trust bootstrap using the cloud registrar. The voucher issued by the cloud includes domain information for the owner's [\[EST\]](#) service the pledge should use for certificate enrollment.

In one use case, an organization has an EST service deployed, but does not have yet a BRSKI capable Registrar service deployed. The pledge is deployed in the organizations domain, but does not discover a local domain, or owner, registrar. The pledge uses the cloud registrar to bootstrap, and the cloud registrar provides a voucher that includes instructions on finding the organization's EST service.

[2.](#) Architecture

The high level architecture is illustrated in Figure 1.

The pledge connects to the cloud registrar during bootstrap.

The cloud registrar may redirect the pledge to an owner registrar in order to complete bootstrap against the owner registrar.

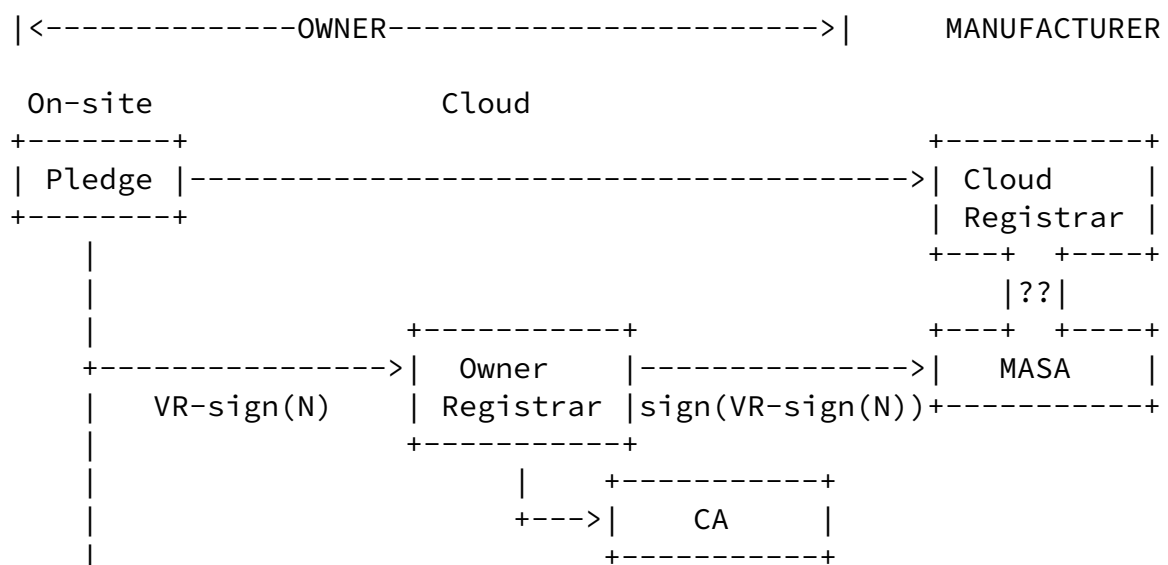
If the cloud registrar issues a voucher itself without redirecting the pledge to an owner registrar, the cloud registrar will inform the pledge what domain to use for accessing EST services in the voucher response.

Finally, when bootstrapping against an owner registrar, this

registrar may interact with a backend CA to assist in issuing certificates to the pledge. The mechanisms and protocols by which the registrar interacts with the CA are transparent to the pledge and are out-of-scope of this document.

The architecture shows the cloud registrar and MASA as being logically separate entities. The two functions could of course be integrated into a single service.

TWO CHOICES: 1. Cloud Registrar redirects to Owner Registrar 2. Cloud Registrar returns VOUCHER pinning Owner Register.



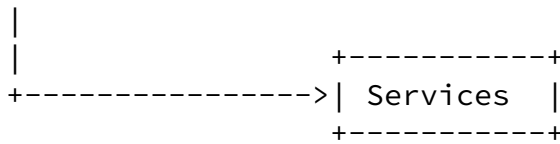


Figure 1: High Level Architecture

[2.1.](#) Interested Parties

1. OEM - Equipment manufacturer. Operate the MASA.
2. Network operator. Operate the Owner Registrar. Often operated by end owner (company), or by outsourced IT entity.
3. Network integrator. They operate a Cloud Registrar.

[2.2.](#) Network Connectivity

The assumption is that the pledge already has network connectivity prior to connecting to the cloud registrar. The pledge must have an IP address, must be able to make DNS queries, and must be able to send HTTP requests to the cloud registrar. The pledge operator has already connected the pledge to the network, and the mechanism by which this has happened is out of scope of this document.

[2.3.](#) Pledge Certificate Identity Considerations

BRSKI [section 5.9.2](#) specifies that the pledge MUST send a CSR Attributes request to the registrar. The registrar MAY use this mechanism to instruct the pledge about the identities it should include in the CSR request it sends as part of enrollment. The registrar may use this mechanism to tell the pledge what Subject or Subject Alternative Name identity information to include in its CSR

request. This can be useful if the Subject must have a specific value in order to complete enrollment with the CA.

For example, the pledge may only be aware of its IDevID Subject which includes a manufacturer serial number, but must include a specific fully qualified domain name in the CSR in order to complete domain ownership proofs required by the CA.

As another example, the registrar may deem the manufacturer serial number in an IDevID as personally identifiable information, and may want to specify a new random opaque identifier that the pledge should use in its CSR.

[3.](#) Protocol Operation

[3.1.](#) Pledge Requests Voucher from Cloud Registrar

[3.1.1.](#) Cloud Registrar Discovery

BRSKI defines how a pledge MAY contact a well known URI of a cloud registrar if a local domain registrar cannot be discovered. Additionally, certain pledge types may never attempt to discover a local domain registrar and may automatically bootstrap against a cloud registrar.

The details of the URI are manufacturer specific, with BRSKI giving the example "brski-registrar.manufacturer.example.com".

The Pledge SHOULD be provided with the entire URL of the Cloud Registrar, including the path component, which is typically "/.well-known/brski/requestvoucher", but may be another value.

[3.1.2.](#) Pledge - Cloud Registrar TLS Establishment Details

The pledge MUST use an Implicit Trust Anchor database (see [\[EST\]](#)) to authenticate the cloud registrar service. The Pledge can be done with pre-loaded trust-anchors that are used to validate the TLS connection. This can be using a public Web PKI trust anchors using [\[RFC6125\]](#) DNS-ID mechanisms, a pinned certification authority, or even a pinned raw public key. This is a local implementation decision.

The pledge MUST NOT establish a provisional TLS connection (see BRSKI [section 5.1](#)) with the cloud registrar.

The cloud registrar MUST validate the identity of the pledge by sending a TLS CertificateRequest message to the pledge during TLS session establishment. The cloud registrar MAY include a

certificate_authorities field in the message to specify the set of

allowed IDevID issuing CAs that pledges may use when establishing connections with the cloud registrar.

The cloud registrar MAY only allow connections from pledges that have an IDevID that is signed by one of a specific set of CAs, e.g. IDevIDs issued by certain manufacturers.

The cloud registrar MAY allow pledges to connect using self-signed identity certificates or using Raw Public Key [[RFC7250](#)] certificates.

[3.1.3](#). Pledge Issues Voucher Request

After the pledge has established a full TLS connection with the cloud registrar and has verified the cloud registrar PKI identity, the pledge generates a voucher request message as outlined in BRSKI [section 5.2](#), and sends the voucher request message to the cloud registrar.

[3.2](#). Cloud Registrar Handles Voucher Request

The cloud registrar must determine pledge ownership. Once ownership is determined, or if no owner can be determined, then the registrar may:

- * return a suitable 4xx or 5xx error response to the pledge if the registrar is unwilling or unable to handle the voucher request
- * redirect the pledge to an owner register via 307 response code
- * issue a voucher and return a 200 response code

[3.2.1](#). Pledge Ownership Lookup

The cloud registrar needs some suitable mechanism for knowing the correct owner of a connecting pledge based on the presented identity certificate. For example, if the pledge establishes TLS using an IDevID that is signed by a known manufacturing CA, the registrar could extract the serial number from the IDevID and use this to lookup a database of pledge IDevID serial numbers to owners.

Alternatively, if the cloud registrar allows pledges to connect using self-signed certificates, the registrar could use the thumbprint of the self-signed certificate to lookup a database of pledge self-signed certificate thumbprints to owners.

The mechanism by which the cloud registrar determines pledge ownership is out-of-scope of this document.

[3.2.2.](#) Cloud Registrar Redirects to Owner Registrar

Once the cloud registrar has determined pledge ownership, the cloud registrar may redirect the pledge to the owner registrar in order to complete bootstrap. Ownership registration will require the owner to register their local domain. The mechanism by which pledge owners register their domain with the cloud registrar is out-of-scope of this document.

The cloud registrar replies to the voucher request with a suitable HTTP 307 response code, including the owner's local domain in the HTTP Location header.

[3.2.3.](#) Cloud Registrar Issues Voucher

If the cloud registrar issues a voucher, it returns the voucher in a HTTP response with a 200 response code.

The cloud registrar MAY issue a 202 response code if it is willing to issue a voucher, but will take some time to prepare the voucher.

The voucher MUST include the "est-domain" field as defined below. This tells the pledge where the domain of the EST service to use for completing certificate enrollment.

The voucher MAY include the "additional-configuration" field.. This points the pledge to a URI where application specific additional configuration information may be retrieved. Pledge and Registrar behavior for handling and specifying the "additional-configuration" field is out-of-scope of this document.

[3.3.](#) Pledge Handles Cloud Registrar Response

[3.3.1.](#) Redirect Response

The cloud registrar returned a 307 response to the voucher request.

The pledge should restart the process using a new voucher request using the location provided in the HTTP redirect. Note if the pledge is able to validate the new server using a trust anchor found in its Implicit Trust Anchor database, then it MAY accept another 307 redirect. The pledge MUST never visit a location that it has already been to. If that happens then the pledge MUST fail the onboarding attempt and go back to the beginning, which includes listening to other sources of onboarding information as specified in [[BRSKI](#) [section 4.1](#) and 5.0.

Internet-Draft

BRSKI-CLOUD

March 2022

The pledge should establish a provisional TLS connection with specified local domain registrar. The pledge should not use its Implicit Trust Anchor database for validating the local domain registrar identity. The pledge should send a voucher request message via the local domain registrar. When the pledge downloads a voucher, it can validate the TLS connection to the local domain registrar and continue with enrollment and bootstrap as per standard BRSKI operation.

[3.3.2.](#) Voucher Response

The cloud registrar returned a voucher to the pledge. The pledge should perform voucher verification as per standard BRSKI operation. The pledge should verify the voucher signature using the manufacturer-installed trust anchor(s), should verify the serial number in the voucher, and must verify any nonce information in the voucher.

The pledge should extract the "est-domain" field from the voucher, and should continue with EST enrollment as per standard BRSKI operation.

[4.](#) Protocol Details

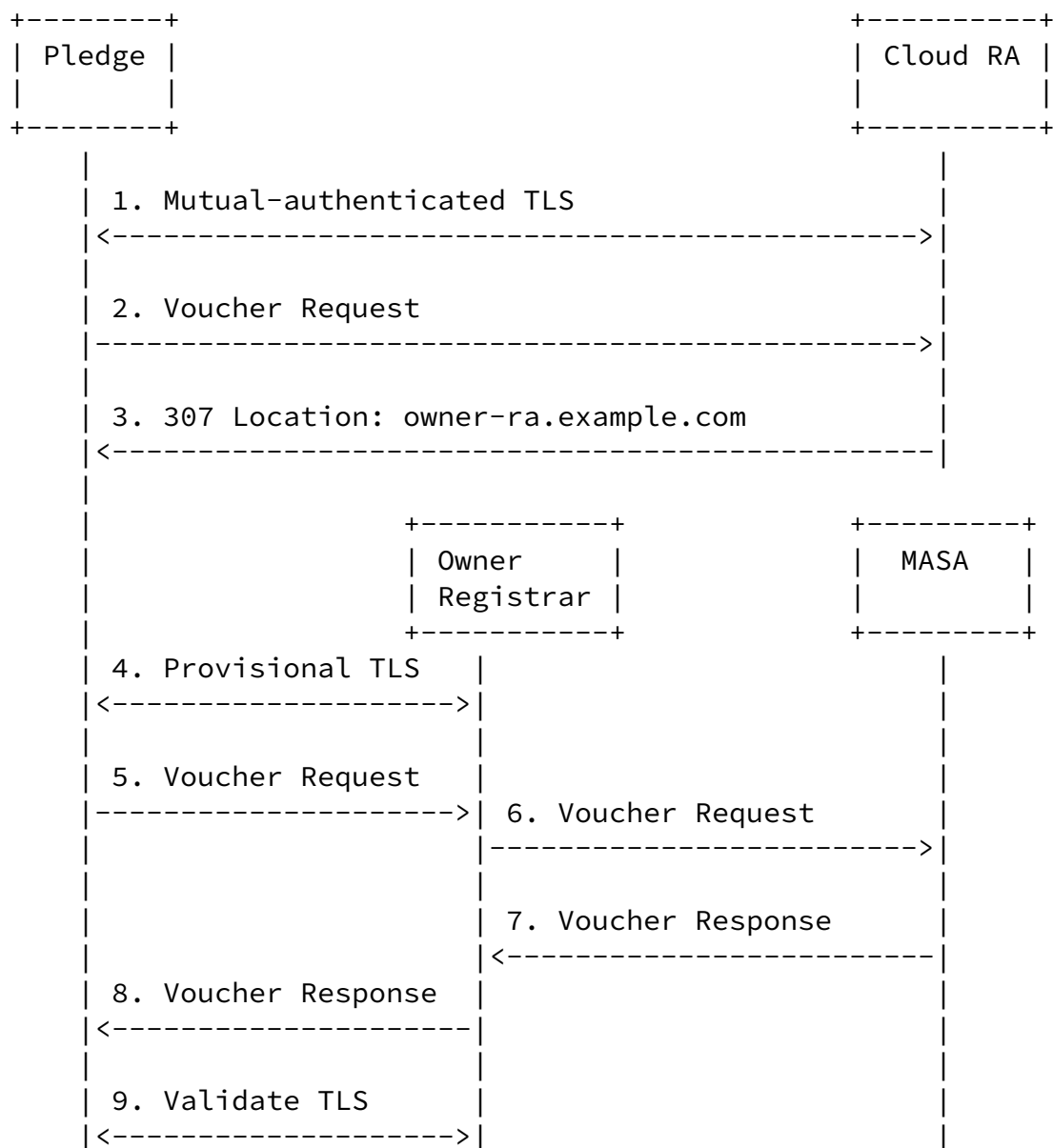
[4.1.](#) Voucher Request Redirected to Local Domain Registrar

This flow illustrates the Owner Registrar Discovery flow. A pledge is bootstrapping in a remote location with no local domain registrar. The assumption is that the owner registrar domain is accessible and the pledge can establish a network connection with the owner registrar. This may require that the owner network firewall exposes the registrar on the public internet.

Internet-Draft

BRSKI-CLOUD

March 2022



	10. etc.			
	----->			

The process starts, in step 1, when the Pledge establishes a Mutual TLS channel with the Cloud RA using artifacts created during the manufacturing process of the Pledge.

In step 2, the Pledge sends a voucher request to the Cloud RA.

The Cloud RA completes pledge ownership lookup as outlined in [Section 3.2.1](#), and determines the owner registrar domain. In step 3, the Cloud RA redirects the pledge to the owner registrar domain.

Steps 4 and onwards follow the standard BRSKI flow. The pledge establishes a provisional TLS connection with the owner registrar, and sends a voucher request to the owner registrar. The registrar forwards the voucher request to the MASA. Assuming the MASA issues a voucher, then the pledge validates the TLS connection with the registrar using the pinned-domain-cert from the voucher and completes the BRSKI flow.

[4.2.](#) Voucher Request Handled by Cloud Registrar

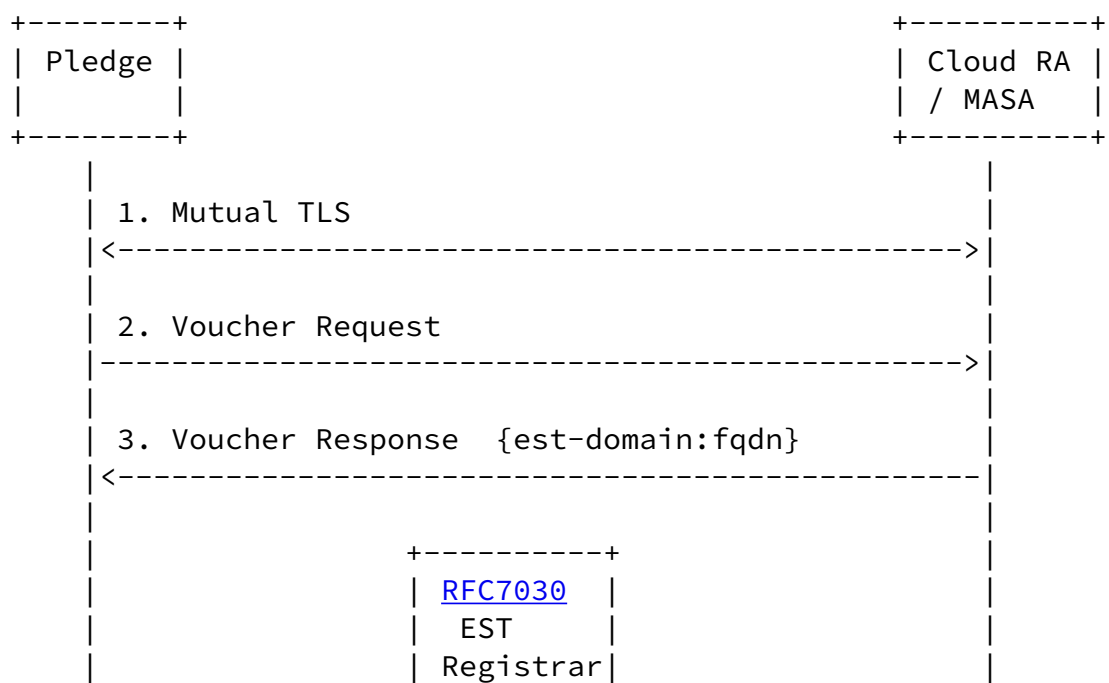
The Voucher includes the EST domain to use for EST enroll. It is assumed services are accessed at that domain too. As trust is already established via the Voucher, the pledge does a full TLS handshake against the local RA indicated by the voucher response.

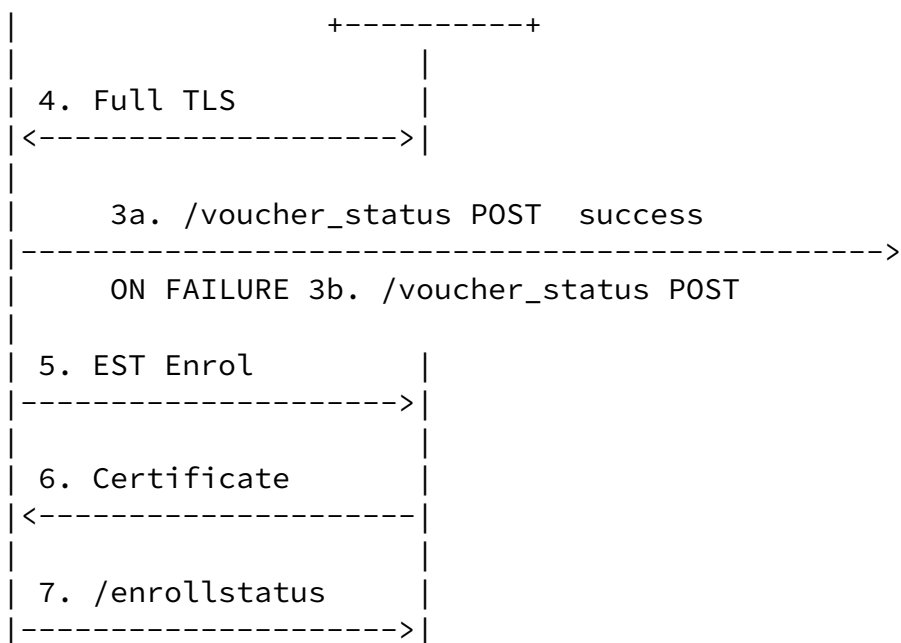
The returned voucher contains an attribute, "est-domain", defined in [Section 5](#) below. The pledge is directed to continue enrollment using the EST registrar found at that URI. The pledge uses the pinned-domain-cert from the voucher to authenticate the EST registrar.

Internet-Draft

BRSKI-CLOUD

March 2022





The process starts, in step 1, when the Pledge establishes a Mutual TLS channel with the Cloud RA/MASA using artifacts created during the manufacturing process of the Pledge. In step 2, the Pledge sends a voucher request to the Cloud RA/MASA, and in response the Pledge receives an [\[RFC8366\]](#) format voucher from the Cloud RA/MASA that includes its assigned EST domain in the est-domain attribute.

At this stage, the Pledge should be able to establish a TLS channel with the EST Registrar. The connection may involve crossing the Internet requiring a DNS lookup on the provided name. It may also be a local address that includes an IP address literal including both [\[RFC1918\]](#) and IPv6 Unique Local Address. The EST Registrar is

validated using the pinned-domain-cert value provided in the voucher as described in [\[BRSKI\] section 5.6.2](#). This involves treating the artifact provided in the pinned-domain-cert as a trust anchor, and attempting to validate the EST Registrar from this anchor only.

There is a case where the pinned-domain-cert is the identical End-Entity (EE) Certificate as the EST Registrar. It also explicitly includes the case where the EST Registrar has a self-signed EE Certificate, but it may also be an EE certificate that is part of a larger PKI. If the certificate is not a self-signed or EE certificate, then the Pledge SHOULD apply [\[RFC6125\]](#) DNS-ID validation

on the certificate against the URL provided in the est-domain attribute. If the est-domain was provided by with an IP address literal, then it is unlikely that it can be validated, and in that case, it is expected that either a self-signed certificate or an EE certificate will be pinned.

The Pledge also has the details it needs to be able to create the CSR request to send to the RA based on the details provided in the voucher.

In step 4, the Pledge establishes a TLS channel with the Cloud RA/MASA, and optionally the pledge should send a request, steps 3.a and 3.b, to the Cloud RA/MASA to inform it that the Pledge was able to establish a secure TLS channel with the EST Registrar.

The Pledge then follows that, in step 5, with an EST Enroll request with the CSR and obtains the requested certificate. The Pledge must validate that the issued certificate has the expected identifier obtained from the Cloud RA/MASA in step 3.

[5.](#) YANG extension for Voucher based redirect

An extension to the [[RFC8366](#)] voucher is needed for the case where the client will be redirected to a local EST Registrar.

[5.1.](#) YANG Tree

module: ietf-voucher-redirected

grouping voucher-redirected-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
+-- est-domain?	ietf:uri
+-- additional-configuration?	ietf:uri

5.2. YANG Voucher

```
<CODE BEGINS> file "ietf-voucher-redirected@2020-09-23.yang"
module iETF-voucher-redirected {
  yang-version 1.1;

  namespace
    "urn:ietf:params:xml:ns:yang:ietf-voucher-redirected";
  prefix "redirected";

  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-inet-types {
    prefix ietf;
    reference "RFC 6991: Common YANG Data Types";
  }

  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: Owen Friel
<mailto:ofriel@cisco.com>
Author: Rifaat Shekh-Yusef
<mailto:rifaat.ietf@gmail.com>;

description

"This module extends the base [RFC8366](#) voucher format to include a redirect to an EST server to which enrollment should continue.

The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' in the module text are to be interpreted as described in [BCP14](#), [RFC 2119](#), and [RFC8174](#).";

```
revision "2020-09-23" {  
  description  
    "Initial version";  
  reference  
    "RFC XXXX: Voucher Profile for Cloud redirected Devices";  
}
```

```
rc:yang-data voucher-redirected-artifact {  
  // YANG data template for a voucher.  
  uses voucher-redirected-grouping;  
}
```

```
// Grouping defined for future usage  
grouping voucher-redirected-grouping {  
  description  
    "Grouping to allow reuse/extensions in future work.";  
  
  uses v:voucher-artifact-grouping {  
  
    augment "voucher" {  
      description "Base the constrained voucher  
                  upon the regular one";  
      leaf est-domain {  
        type ietf:uri;  
        description  
          "The est-domain is a URL to which the Pledge should  
          continue doing enrollment rather than with the  
          Cloud Registrar.  
          The pinned-domain-cert contains a trust-anchor  
          which is to be used to authenticate the server
```

found at this URI.

```
        ";
    }
    leaf additional-configuration {
        type ietf:uri;
        description
            "The additional-configuration attribute contains a
            URL to which the Pledge can retrieve additional
            configuration information.
            The contents of this URL are vendor specific.
            This is intended to do things like configure
            a VoIP phone to point to the correct hosted
            PBX, for example.";
    }
}
}
}
}
}
<CODE ENDS>
```

[6.](#) IANA Considerations

[6.1.](#) The IETF XML Registry

This document registers one URI in the IETF XML registry [[RFC3688](#)]. Following the format in [[RFC3688](#)], the following registration is requested:

```
{: newline="true"}
URI:
: urn:ietf:params:xml:ns:yang:ietf-voucher-redirected
```

```
Registrant Contact:
: The ANIMA WG of the IETF.
```

```
XML:
: N/A, the requested URI is an XML namespace.
```

[6.2.](#) 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 the following registration is requested:

```
{: newline="true"}
name:
: ietf-voucher-redirected

namespace:
: urn:ietf:params:xml:ns:yang:ietf-voucher-redirected

prefix:
: vch

reference:
: THIS DOCUMENT
```

[7.](#) Security Considerations

The Cloud-Registrar described in this document inherits all of the issues that are described in [[BRSKI](#)]. This includes dependency upon continued operation of the manufacturer provided MASA, as well as potential complications where a manufacturer might interfere with resale of a device.

In addition to the dependency upon the MASA, the successful enrollment of a device using a Cloud Registrar depends upon the correct and continued operation of this new service. This internet accessible service may be operated by the manufacturer and/or by one or more value-added-resellers. All of the considerations for operation of the MASA also apply to operation of the Cloud Registrar.

[7.1.](#) Issues with Security of HTTP Redirect

If the Redirect to Registrar method is used, as described in [Section 4.1](#), there may be a series of 307 redirects. An example of why this might occur is that the manufacturer only knows that it

resold the device to a particular value added reseller (VAR), and there may be a chain of such VARs. It is important the pledge avoid being drawn into a loop of redirects. This could happen if a VAR does not think they are authoritative for a particular device. A "helpful" programmer might instead decide to redirect back to the manufacturer in an attempt to restart at the top: perhaps there is another process that updates the manufacturer's database and this process is underway. Instead, the VAR MUST return a 404 error if it can not process the device. This will force the device to stop, timeout, and then try all mechanisms again.

There is another case where a connection problem may occur: when the pledge is behind a captive portal or an intelligent home gateway that provides access control on all connections. Captive portals that do not follow the requirements of [\[RFC8952\] section 1](#) may forcibly

redirect HTTPS connections. While this is a deprecated practice as it breaks TLS in a way that most users can not deal with, it is still common in many networks.

On the first connection, the incorrect connection will be discovered because the Pledge will be unable to validate the connection to it's cloud registrar via DNS-ID. That is, the certificate returned from the captive portal will not match.

At this point a network operator who controls the captive portal, noticing the connection to what seems a legitimate destination (the cloud registrar), may then permit that connection. This enables the first connection to go through.

The connection is then redirected to the Registrar, either via 307, or via est-domain in a voucher. If it is a 307 redirect, then a provisional TLS connection will be initiated, and it will succeed. The provisional TLS connection does not do [\[RFC6125\]](#) DNS-ID validation at the beginning of the connection, so a forced redirection to a captive portal system will not be detected. The subsequent BRSKI POST of a voucher will most likely be met by a 404 or 500 HTTP code. As the connection is provisional, the pledge will be unable to determine this.

It is RECOMMENDED therefore that the pledge look for [\[RFC8910\]](#) attributes in DHCP, and if present, use the [\[RFC8908\]](#) API to learn if

it is captive.

[7.2.](#) Security Updates for the Pledge

Unlike many other uses of BRSKI, in the Cloud Registrar case it is assumed that the Pledge has connected to a network on which there is addressing and connectivity, but there is no other local configuration available.

There is another advantage to being online: the pledge may be able to contact the manufacturer before onboarding in order to apply the latest firmware updates. This may also include updates to the Implicit list of Trust Anchors. In this way, a Pledge that may have been in a dusty box in a warehouse for a long time can be updated to the latest (exploit-free) firmware before attempting onboarding.

[7.3.](#) Trust Anchors for Cloud Registrar

The Implicit TA database is used to authenticate the Cloud Registrar. This list is built-in by the manufacturer along with a DNS name to which to connect. (The manufacturer could even build in IP addresses as a last resort)

The Cloud Registrar does not have have a certificate that can be validated using a public (WebPKI) anchor. The pledge may have any kind of Trust Anchor built in: from full multi-level WebPKI to the single self-signed certificate used by the Cloud Registrar. There are many tradeoffs to having more or less of the PKI present in the Pledge, which is addresses in part in [\[I-D.richardson-t2trg-idevid-considerations\]](#) in sections [3](#) and [5](#).

[7.4.](#) Issues with Redirect via Voucher

The second redirect case is handled by returning a special extension in the voucher. The Cloud Registrar actually does all of the voucher processing as specified in [\[BRSKI\]](#). In this case, the Cloud Registrar may be operated by the same entity as the MASA, and it might even be combined into a single server. Whether or not this is the case, it behaves as if it was separate.

It may be the case that one or more 307-Redirects have taken the Pledge from the built-in Cloud Registrar to one operated by a VAR.

When the Pledge is directed to the Owner's [EST] Registrar, the Pledge validates the TLS connection with this server using the "pinned-domain-cert" attribute in the voucher. There is no provisional TLS connection, and therefore there are no risks associated with being behind a captive portal.

8. References

8.1. Normative References

- [BRSKI] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", [RFC 8995](#), DOI 10.17487/RFC8995, May 2021, <<https://www.rfc-editor.org/info/rfc8995>>.
- [EST] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", [RFC 7030](#), DOI 10.17487/RFC7030, October 2013, <<https://www.rfc-editor.org/info/rfc7030>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

Friel, et al.

Expires 7 September 2022

[Page 20]

Internet-Draft

BRSKI-CLOUD

March 2022

- [RFC8366] Watsen, K., Richardson, M., Pritikin, M., and T. Eckert, "A Voucher Artifact for Bootstrapping Protocols", [RFC 8366](#), DOI 10.17487/RFC8366, May 2018, <<https://www.rfc-editor.org/info/rfc8366>>.

8.2. Informative References

- [I-D.richardson-t2trg-idevid-considerations] Richardson, M., "A Taxonomy of operational security considerations for manufacturer installed keys and Trust Anchors", Work in Progress, Internet-Draft, [draft-richardson-t2trg-idevid-considerations-06](#), 3 February

2022, <<https://www.ietf.org/archive/id/draft-richardson-t2trg-idevid-considerations-06.txt>>.

[IEEE802.1AR]

IEEE Standard, ., "IEEE 802.1AR Secure Device Identifier", 2018, <<http://standards.ieee.org/findstds/standard/802.1AR-2018.html>>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", [BCP 5](#), [RFC 1918](#), DOI 10.17487/RFC1918, February 1996, <<https://www.rfc-editor.org/info/rfc1918>>.

[RFC3688] Mealling, M., "The IETF XML Registry", [BCP 81](#), [RFC 3688](#), DOI 10.17487/RFC3688, January 2004, <<https://www.rfc-editor.org/info/rfc3688>>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", [RFC 6020](#), DOI 10.17487/RFC6020, October 2010, <<https://www.rfc-editor.org/info/rfc6020>>.

[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 2011, <<https://www.rfc-editor.org/info/rfc6125>>.

[RFC7250] Wouters, P., Ed., Tschofenig, H., Ed., Gilmore, J., Weiler, S., and T. Kivinen, "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", [RFC 7250](#), DOI 10.17487/RFC7250, June 2014, <<https://www.rfc-editor.org/info/rfc7250>>.

[RFC8572] Watsen, K., Farrer, I., and M. Abrahamsson, "Secure Zero Touch Provisioning (SZTP)", [RFC 8572](#), DOI 10.17487/RFC8572, April 2019, <<https://www.rfc-editor.org/info/rfc8572>>.

- [RFC8908] Pauly, T., Ed. and D. Thakore, Ed., "Captive Portal API", [RFC 8908](https://www.rfc-editor.org/info/rfc8908), DOI 10.17487/RFC8908, September 2020, <<https://www.rfc-editor.org/info/rfc8908>>.
- [RFC8910] Kumari, W. and E. Kline, "Captive-Portal Identification in DHCP and Router Advertisements (RAs)", [RFC 8910](https://www.rfc-editor.org/info/rfc8910), DOI 10.17487/RFC8910, September 2020, <<https://www.rfc-editor.org/info/rfc8910>>.
- [RFC8952] Larose, K., Dolson, D., and H. Liu, "Captive Portal Architecture", [RFC 8952](https://www.rfc-editor.org/info/rfc8952), DOI 10.17487/RFC8952, November 2020, <<https://www.rfc-editor.org/info/rfc8952>>.

Authors' Addresses

Owen Friel
Cisco
Email: ofriel@cisco.com

Rifaat Shekh-Yusef
Auth0
Email: rifaat.s.ietf@gmail.com

Michael Richardson
Sandelman Software Works
Email: mcr+ietf@sandelman.ca