6tisch Working Group
Internet-Draft
Intended status: Informational
Expires: November 24, 2018

M. Richardson
Sandelman Software Works

May 23, 2018

Device Enrollment in IETF protocols -- A Roadmap
draft-richardson-enrollment-roadmap-02

Abstract

This document provides an overview of enrollment or imprinting mechanisms in current IETF protocols.

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 November 24, 2018.

Copyright Notice

Copyright (c) 2018 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

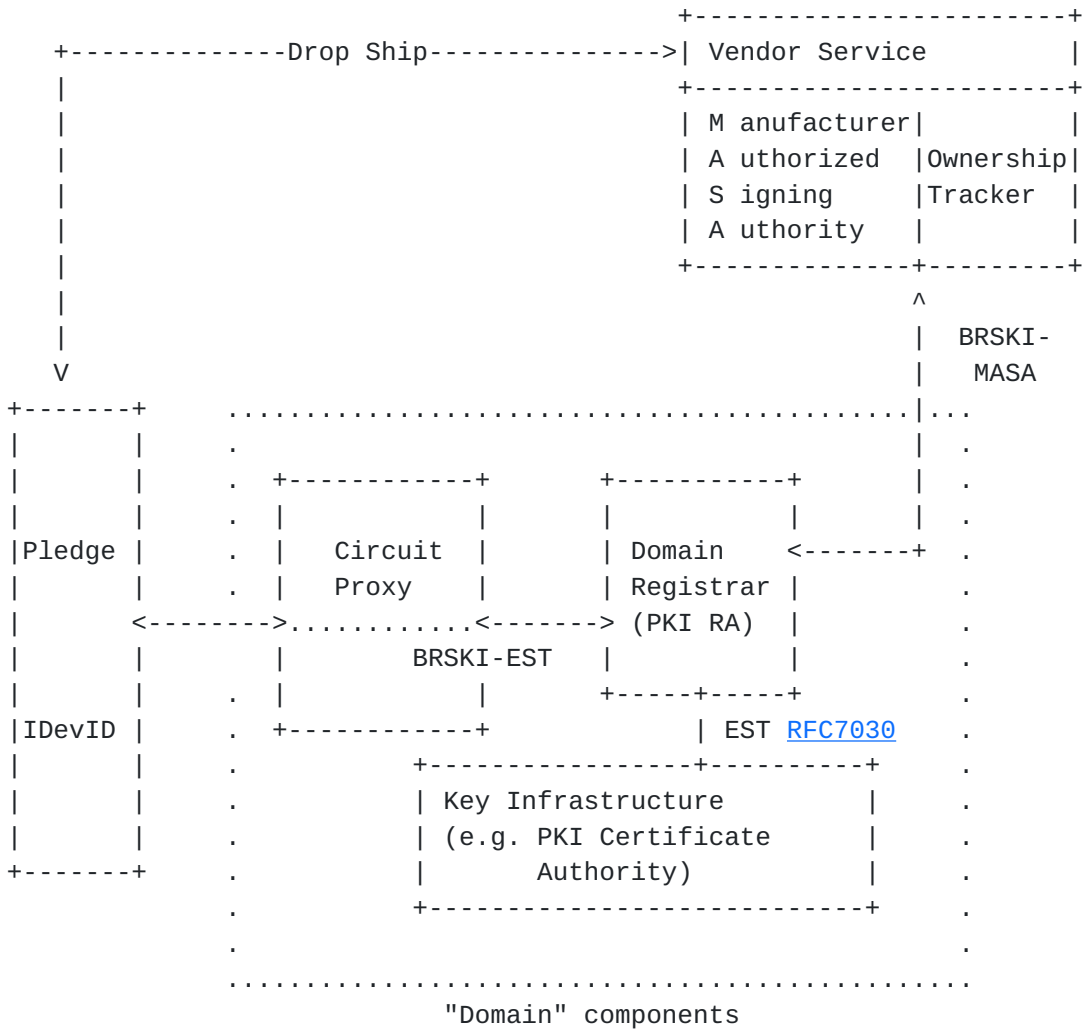
1. Introduction

There are numerous mechanisms being proposed to solve the problem of securely introducing a new devices into an existing managed network.

This document provides an overview of the different mechanisms showing what technologies are common. The document starts with a diagram showing the various components and how they go together to form five enrollment scenarios.

2. Components of enrollment solutions

This diagram is taken from [I-D.ietf-anima-bootstrapping-keyinfra], which is where this work started.



Five major components are described:

1. pledge: The node that is attempting to enroll.

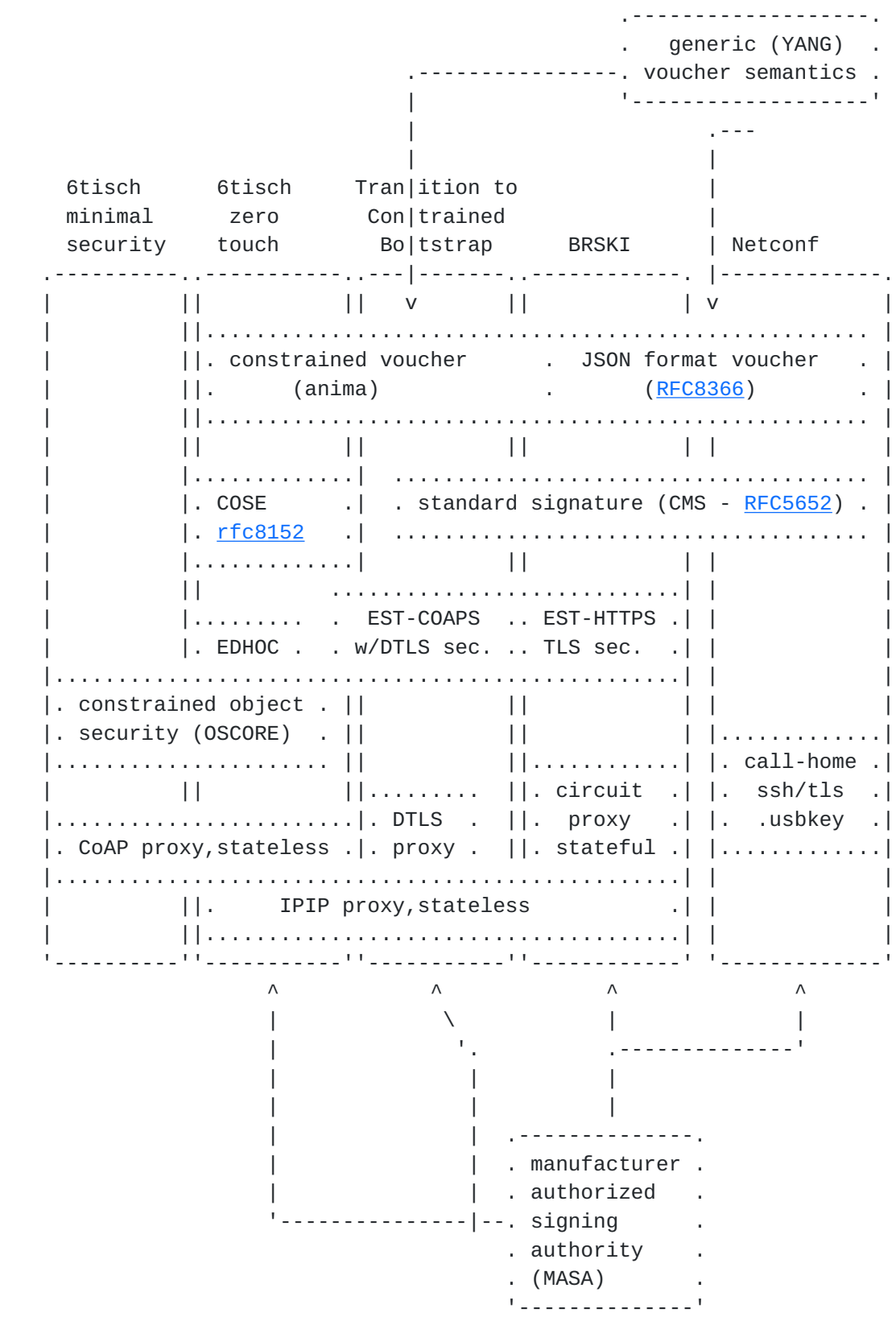
2. proxy: A node that is within one layer-2 hop of the pledge that is helping.

3. domain registrar: the Join Registrar/Coordinator (JRC) that will determine eligibility of the pledge.

4. MASA: the representative of the manufacturer that has a pre-established trust relationship with the pledge.

5. the domain PKI (if any)

3. Map of Enrollment solution


generic (YANG)
voucher semantics
6tisch minimal security
6tisch zero touch
Tran|ition to
Con|trained
Bo|tstrap
BRSKI
Netconf
constrained voucher (anima)
JSON format voucher (RFC8366)
COSE
rfc8152
standard signature (CMS - RFC5652)
EST-COAPS
w/DTLS sec.
EST-HTTPS
TLS sec.
EDHOC
constrained object security (OSCORE)
call-home
ssh/tls
.usbkey
circuit proxy
stateful
DTLS proxy
CoAP proxy,stateless
IPIP proxy,stateless
manufacturer authorized signing authority (MASA)

4. Components

4.1. generic voucher semantics

The abstract semantics of the voucher, described in YANG, are in [RFC8366].

4.2. constrained voucher

The semantics of the constrained voucher, represented in CBOR, are described in [I-D.ietf-anima-constrained-voucher].

4.3. JSON format voucher

The semantics of the basic voucher, represented in JSON, are described in [RFC8366].

4.4. COSE-8152

In constrained systems the voucher is signed using the COSE mechanism described in [RFC8152].

4.5. standard signature (CMS)

In un-constrained systems the voucher is signed using the Cryptographic Message Syntax (CMS) described in [RFC5652].

4.6. EDHOC

On constrained and challenged networks, the session key management can be formed by [I-D.selander-ace-cose-ecdhe].

This document does NOT have a home.

The CoAP-EST layer on top is described by [I-D.ietf-ace-coap-est]

4.7. EST-COAPS 2/DTLS sec(urity)

On unconstrained networks, the session key management is provided by [RFC6347]. The CoAP-EST layer on top is described by [I-D.ietf-ace-coap-est].

The ACE WG has adopted this document.

4.8. EST-HTTPS TLS sec(urity)

On unconstrained networks with unconstrained nodes, the EST layer and session key management is described by [RFC7030] as modified by [I-D.ietf-anima-bootstrapping-keyinfra] (BRSKI).

4.9. constrained object security (OSCORE)

On constained networks with constrained nodes, the CoAP transactions are secured by [I-D.ietf-core-object-security] using symmetric keys. The symmetric key may be pre-shared (for 6tisch minimal security), or MAY be derived using EDHOC.

4.10. Pledge traffic proxy mechanisms

Traffic between the Pledge and the JRC does not flow directly as the pledge does not typically have a globally reachable address, nor does it have any network access keys (whether WEP, WPA, 802.1x, or 802.15.4 keys).

Communication between the pledge and JRC is mediated by a proxy. This is primarily to protect the network against attacks. The proxy mechanism is provided by as many nodes as can afford to as a benefit to the network, and therefore MUST be as light weight as possible. There are therefore stateless mechanisms and stateful mechanisms. The costs of the various methods is analysized in [I-D.richardson-anima-state-for-joinrouter].

4.10.1. COAP proxy,stateless

The CoAP proxy mechanism uses the OSCORE Context Hint to statelessly store the address of the proxy within the CoAP structure. It is described in [I-D.ietf-6tisch-minimal-security].

4.11. DTLS proxy

There has been no specific DTLS specific stateless proxy described, although the mechanism described by the Thread Group is being considered, if it can be referenced easily.

4.12. IPIP proxy,stateless

An IPIP proxy mechanism uses a layer of IP-in-IP header (protocol 98) to encapsulate the traffic between Join Proxy and JRC. It has some complexities to implement on typical POSIX platforms. It is intended to be described in [I-D.ietf-6tisch-dtsecurity-zerotouch-join], in an Appendix. Another home for the text is also desired.

4.13. circuit proxy stateful

The circuit proxy method utilitizes either an application layer gateway (which in canonical 1990-era implementation requires a process per connection), or the use of NAT66. It maintains some state for each connection whether TCP or UDP.

It is this most expensive and most easily abused, but also the most widely available, code-wise.

5. call-home ssh/tls/usbkey

The NETCONF call-home mechanism assumes that the device can get basic connectivity, enough for an out "outgoing" TCP connection to the manufacturer.

6. manufacturer authorized signing authority (MASA)

The MASA is the manufacturers anchor of the manufacturer/pledge trust relationship that is established at the factory where the pledge is built.

7. Enrollment Mechanisms

7.1. NETCONF

The NETCONF WG is describing this in [I-D.ietf-netconf-zerotouch] document.

The NETCONF Zerotouch mechanism provides configuration and ownership information by having the pledge "call home" to a location determined by a mix of local hints (DHCPv4, DHCPv6, and mDNS), as well as built-in anchors. Additionally, ownership vouchers can be alternatively distributed by portable storage such as USB key.

Upon reaching a validated call-home server, Zerotouch typically "reverses" the connection providing either an SSH or TLS connection _to_ the pledge device such that it can be configured automatically.

Zerotouch relies upon either open or very easy access to network connectivity, along with the ability to make an outgoing TCP connection to the Internet, or to the provided local configuration agent.

Zerotouch is seen as an updated version of TR-69 by some, appropriate for configuration of residential appliances which are drop-shiped by ISPs or other service providers to homes. That is not the only targetted use.

7.2. BRSKI

The ANIMA WG is describing BRSKI in [I-D.ietf-anima-bootstrapping-keyinfra] document.

The ANIMA WG does enrollment with the aim of creating a secure channel with a public-key infrastructure (PKI) Registrar. The secured channel is used to perform Enrollment over Secure Transport (EST, RFC7030). The real goal is the enrollment a new device which was probably been drop-shipped into ANIMA's Autonomic Control Plane.

That is, after the pledge has been assigned a certificate within the (autonomic) domain, the device (no longer a pledge) will then form secure channels (typically using IKEv2 to key an IPsec channel). On top of that channel a routing protocol (RPL) is run to form the Autonomic Control Plane (ACP). The ACP is then used as a management network with which to configure the new device.

BRSKI is therefore step one of a number of steps, the ultimate goal of which is to bring the pledge into the ACP as a new device.

BRSKI itself does not provide for any direct keying of the network (802.11 WEP/WPA, or 802.15.4 security). The provision of a domain certificate at each node can, however, be used to do that kind of keying: for instance 802.15.9 provides for use of HIP and IKEv2 to key 802.15.4 networks.

7.3. Transition to Constrained Bootstrap

This category of usage could use a better name.

The bulk of this work has no home as yet. It is distinguished from BRSKI in that it uses DTLS (rather than TLS) and constrained (CBOR) vouchers. It is distinguished from 6tisch Zero Touch in that uses CMS to sign rather than COSE.

The ACE WG has adopted [I-D.ietf-ace-coap-est], but this is not a sufficient. This work depends depends upon [I-D.ietf-anima-constrained-voucher].

The use of this technology slice is attractive to IoT deployments where the devices are not battery powered (lighting for instance, AMI for electric meters). In such situations, the processors in each device have significantly more resources, and in particular far more code space available. The use of DTLS to secure application traffic (as described in the ACE documents) is already common, and so reuse of DTLS is desireable from a code point of view.

However, the network capacity is still limited so TCP and CBOR are still important. The network may also contain extremely constrained devices (kinetically powered light switches for instance).

7.4. 6tisch Zero Touch

The 6tisch WG is describing this in [I-D.ietf-6tisch-dtsecurity-zerotouch-join] document.

The 6tisch use case consists of very constrained devices with very constrained networks. Code space in the devices is larger than typical class 2, but the devices are typically battery powered and wish to sleep significantly.

The use of CBOR for vouchers, COSE to sign the vouchers saves significant network bandwidth and code space. Both CBOR, COSE and OSCORE are typically already in use for the application support. The addition of EDHOC to provide asymmetric bootstrap of OSCORE completes the suite of constrained security protocols.

7.5. 6tisch minimal security

The 6tisch WG is describing this in [I-D.ietf-6tisch-minimal-security] document. This mechanism does enrollment in a single request/response message, but requires at least one "touch" to pre-share symmetric keys.

The 6tisch WG felt that the number of round trips required to do EDHOC, and the size of the vouchers required an even simpler protocol. As existing 6tisch-type technology is typically deployed with network keys built-in at manufacturer time (no "drop-ship"), the switch from a static network key to a PSK for authenticaiton is considered an incremental improvement.

All other methods are considered zero "touch".

8. Discussion

A goal of this document is to provide some guidance in selecting which enrollment profile to use for a given scenario. This section tries to provide some constrasting comments between the various mechanisms.

(BUT, it does not yet do that..)

9. Security Considerations

This document includes a tradeoff of the security attributes of the different protocols, and so the entire document contains security advice.

10. IANA Considerations

This document does not define any new protocols, and therefore does not have any IANA Considerations.

11. Acknowledgements

TBD

12. References

12.1. Normative References

[I-D.ietf-6tisch-dtsecurity-zerotouch-join]
Richardson, M. and B. Damm, "6tisch Zero-Touch Secure Join protocol", draft-ietf-6tisch-dtsecurity-zerotouch-join-02 (work in progress), April 2018.

[I-D.ietf-6tisch-minimal-security]
Vucinic, M., Simon, J., Pister, K., and M. Richardson, "Minimal Security Framework for 6TiSCH", draft-ietf-6tisch-minimal-security-05 (work in progress), March 2018.

[I-D.ietf-ace-coap-est]
Stok, P., Kampanakis, P., Kumar, S., Richardson, M., Furuhed, M., and S. Raza, "EST over secure CoAP (EST-coaps)", draft-ietf-ace-coap-est-00 (work in progress), February 2018.

[I-D.ietf-anima-bootstrapping-keyinfra]
Pritikin, M., Richardson, M., Behringer, M., Bjarnason, S., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructures (BRSKI)", draft-ietf-anima-bootstrapping-keyinfra-15 (work in progress), April 2018.

[I-D.ietf-anima-constrained-voucher]
Richardson, M., Stok, P., and P. Kampanakis, "Constrained Voucher Artifacts for Bootstrapping Protocols", draft-ietf-anima-constrained-voucher-00 (work in progress), May 2018.

[I-D.ietf-core-object-security]
Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", draft-ietf-core-object-security-12 (work in progress), March 2018.

[I-D.ietf-netconf-zerotouch]
Watsen, K., Abrahamsson, M., and I. Farrer, "Zero Touch Provisioning for Networking Devices", draft-ietf-netconf-zerotouch-21 (work in progress), March 2018.

[I-D.selander-ace-cose-ecdhe]
Selander, G., Mattsson, J., and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)", draft-selander-ace-cose-ecdhe-08 (work in progress), March 2018.

[ieee802-1AR]
IEEE Standard, ., "IEEE 802.1AR Secure Device Identifier", 2009, <http://standards.ieee.org/findstds/standard/802.1AR-2009.html>.

[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>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/info/rfc6347>.

[RFC7030] 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>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[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>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[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>.

12.2. Informative References

[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.

[pledge] Dictionary.com, ., "Dictionary.com Unabridged", 2015, <http://dictionary.reference.com/browse/pledge>.

Author's Address

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca