6tisch Working Group
Internet-Draft
Intended status: Informational
Expires: July 30, 2018

M. Richardson
Sandelman Software Works

January 26, 2018

Device Enrollment in IETF protocols -- a roadmap
draft-richardson-enrollment-roadmap-00

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 July 30, 2018.

Table of Contents

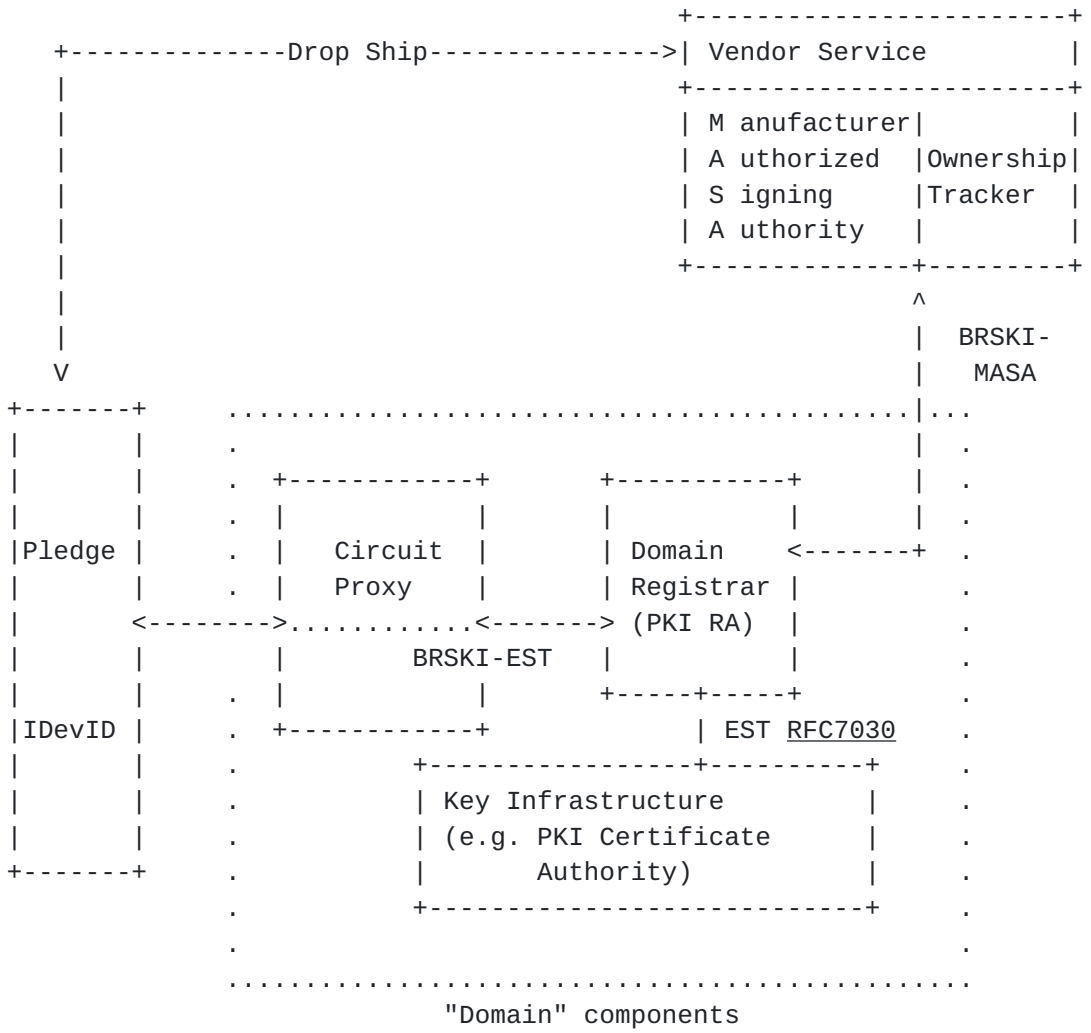
1. Introduction

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
Transition to Constrained Bootstrap
BRSKI
Netconf
constrained voucher (CBOR)
JSON format voucher
COSE-8152
standard signature (CMS - RFC5652)
EDHOC
EST-COAPS w/DTLS sec.
EST-HTTPS TLS sec.
constrained object security (OSCORE)
call-home
ssh/tls
.usbkey
CoAP proxy,stateless
DTLS proxy
circuit proxy
stateful proxy
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 [I-D.ietf-anima-voucher].

4.2. constrained voucher

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

This document does NOT yet have a home.

4.3. JSON format voucher

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

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.vanderstok-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.vanderstok-ace-coap-est].

The ACE WG has agreed to adopt 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.

7.2. BRSKI

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

7.3. Transition to Constrained Bootstrap

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 is going to adopt [I-D.vanderstok-ace-coap-est].

7.4. 6tisch Zero Touch

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

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.

All other methods are considered zero "touch".

8. Security Considerations

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

9. IANA Considerations

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

10. Acknowledgements

TBD

11. References

11.1. 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-01 (work in progress), October 2017.

[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-04 (work in progress), October 2017.

[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-09 (work in progress), October 2017.

[I-D.ietf-anima-voucher]
Watsen, K., Richardson, M., Pritikin, M., and T. Eckert, "Voucher Profile for Bootstrapping Protocols", draft-ietf-anima-voucher-06 (work in progress), October 2017.

[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-08 (work in progress), January 2018.

[I-D.ietf-netconf-zerotouch]
Watsen, K., Abrahamsson, M., and I. Farrer, "Zero Touch Provisioning for NETCONF or RESTCONF based Management", draft-ietf-netconf-zerotouch-19 (work in progress), October 2017.

[I-D.richardson-anima-ace-constrained-voucher]
Richardson, M., "Constrained Voucher Profile for Bootstrapping Protocols", draft-richardson-anima-ace-constrained-voucher-02 (work in progress), December 2017.

[I-D.selander-ace-cose-ecdhe]
Selander, G., Mattsson, J., and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)", draft-selander-ace-cose-ecdhe-07 (work in progress), July 2017.

[I-D.vanderstok-ace-coap-est]
Stok, P., Kampanakis, P., Kumar, S., Richardson, M., Furuhed, M., and S. Raza, "EST over secure CoAP (EST-coaps)", draft-vanderstok-ace-coap-est-04 (work in progress), January 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>.

11.2. Informative References

[duckling] Stajano, F. and R. Anderson, "The resurrecting duckling: security issues for ad-hoc wireless networks", 1999, <https://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling.pdf>.

[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-01 (work in progress), July 2016.

[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