```
ANIMA Working Group                                      M. Richardson
Internet-Draft                                  Sandelman Software Works
Intended status: Informational                         October 07, 2020
Expires: April 10, 2021
```

Device Enrollment in IETF protocols -- A Roadmap
draft-richardson-enrollment-roadmap-03

Abstract

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

   This document is being worked on in the ANIMA-WG, and on github at:
   https://github.com/anima-wg/enrollment-roadmap

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 April 10, 2021.

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
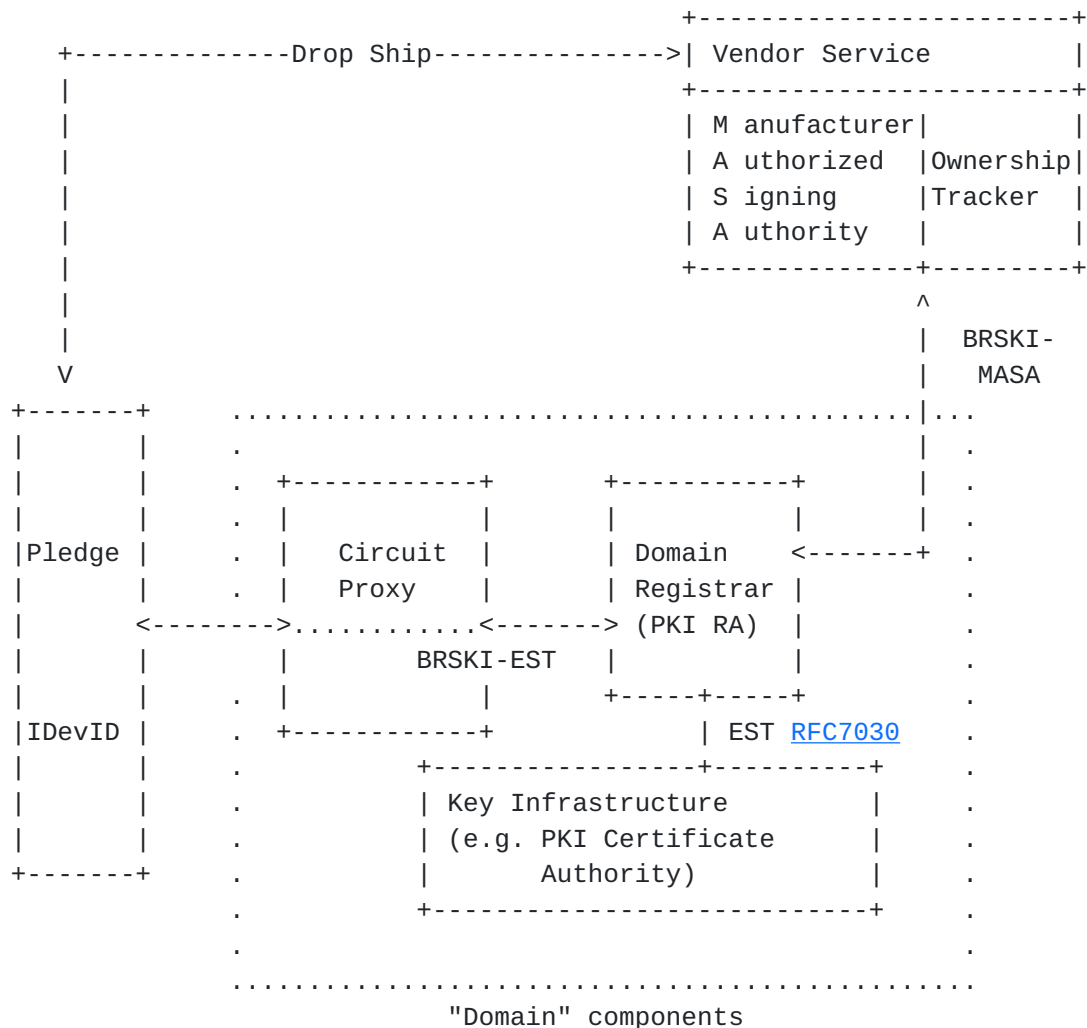   showing what technologies are common.

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.

```
                                       +------------------------+
    +-------------Drop Ship-------------->| Vendor Service       |
    |                                    +------------------------+
    |                                    | M anufacturer|         |
    |                                    | A uthorized  |Ownership|
    |                                    | S igning     |Tracker  |
    |                                    | A uthority   |         |
    |                                    +--------------+---------+
    |                                            ^
    |                                            |  BRSKI-
    V                                            |   MASA
+-------+        .........................................|...
|       |    |   .                                        |  .
|       |    |   . +------------+      +-----------+       |  .
|       |    |   . |            |      |           |       |  .
|Pledge |    .   . |   Circuit  |      | Domain    <-------+  .
|       |    .   . |   Proxy    |      | Registrar |          .
|       <-------->............<------> (PKI RA)  |          .
|       |    |   |        BRSKI-EST   |           |          .
|       |    .   . |            |      +-----+-----+          .
|IDevID |    .   . +------------+            | EST RFC7030    .
|       |    .                   +----------------+---------+ .
|       |    .                   | Key Infrastructure     |  .
|       |    .                   | (e.g. PKI Certificate  |  .
+-------+    .                   |       Authority)       |  .
             .                   +--------------------------+  .
             .                                             .
             ...............................................
                         "Domain" components
```

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      6tisch    Tran|ition to       |
      minimal      zero     Con|trained         |
      security     touch    Bo|tstrap    BRSKI   | Netconf
     .----------..----------..---|-------..------------. |------------.
     |          ||          ||   v       ||           | v             |
     |          ||..................................... |
     |          ||. constrained voucher   .  JSON format voucher   . |
     |          ||.        (anima)         .        (RFC8366)       . |
     |          ||..................................... |
     |          ||          ||           ||           | |             |
     |          |.............|  ..................................... |
     |          |. COSE      .|  . standard signature (CMS - RFC5652) . |
     |          |. rfc8152   .|  ..................................... |
     |          |.............|         ||           | |             |
     |          ||          ............................| |             |
     |          |........  .  EST-COAPS  .. EST-HTTPS .| |             |
     |          |. EDHOC .  . w/DTLS sec. .. TLS sec.  .| |             |
     |.....................................................| |             |
     |. constrained object . ||           ||           | |             |
     |. security (OSCORE)  . ||           ||           | |.............|
     |...................... ||           ||...........| |. call-home .|
     |          ||          ||........  ||. circuit  .| |.  ssh/tls  .|
     |......................|. DTLS   .  ||. proxy    .| |.  .usbkey  .|
     |. CoAP proxy,stateless .|. proxy .  ||. stateful .| |.............|
     |...................................................| |             |
     |          ||. 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]. This is to be replaced with
   [I-D.ietf-cose-rfc8152bis-algs] (now in RFC-EDITOR Q) and
   [I-D.ietf-cose-rfc8152bis-struct] (in WGLC, being revised to remove
   countersignatures).

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.ietf-lake-edhoc].

   This document has a WG called LAKE.

   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], which is in the RFC-EDITOR Q, waiting for
   DTLS 1.3.

   The ACE WG adopted this document, and published it.

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).

BRSKI is in the RFC-EDITOR Q, waiting for
[I-D.ietf-anima-autonomic-control-plane], which is awaiting IESG go-
ahead.

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. ultra-constrained enrollment

The document [I-D.selander-ace-ake-authz]. Version -01 expired in
September 2020, but is expected to be reposted for discussion in the
ACE WG.

4.11. 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].

4.11.1. 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].

4.12. DTLS proxy

A DTLS specific mechanism for COAPS, is described in
[I-D.vanderstok-anima-constrained-join-proxy].

4.13. 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.

At one point, it was described in
[I-D.ietf-6tisch-dtsecurity-zerotouch-join], in an Appendix. Another
home for the text is desired.

4.14. 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

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.

The constrained version of BRSKI is current described as part of
[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 n instance).

7.4. Cloud-based Registrars

BRSKI depends upon a local join proxy to direct the pledge device to
the location of the Registrar. Not only does this require that a
join proxy be widely available, but it also assumes that the owner is
able to operate a Registrar.

[I-D.friel-anima-brski-cloud] deals with two use cases:

1. where there is a Registrar, but no join proxy. A redirection
    through a manufacturer or VAR operated register points the device
    to a Registrar located on the Internet.

2. where there is no Registrar (yet), but the network operator does
    have an RFC7030 EST server. The cloud registrar provides a
    voucher connecting the pledge to the appropriate EST server.

7.5. BRSKY Asynchronous Enrollment

BRSKI depends the join proxy being available in the location where
the devices are installed, and for that proxy to also be able to
communicate to the Registrar (possibly over the Internet).

In a number of environments, such as new construction, a number of devices need to go through an onboarding process, but there is no connectivity available. (Possibly not even LTE/3G due to metal walls, lack of towers, etc.).

The [I-D.ietf-anima-brski-async-enroll] proposes two amendments to BRSKI:

1. the use of CMP rather than EST for enrollment, which eliminates the need to keep a live TLS connection between pledge and Registrar.

2. a discovery, store-and-forward mechanism for moving voucher requests and vouchers between the Registrar and Pledge, including a batch mechanism that aims to reduce the amount of walking that an installer might have to do.

7.6. 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.

7.7. 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".

[I-D.ietf-6tisch-minimal-security] is in the RFC-EDITOR Q, waiting
for core-stateless on which is depends to leave the WG.

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. OPEN ISSUE

1. insufficient guidance if there is no internet connection.

2. classes of devices where the manufacturer will never have an HSM/
    PKI. so, it will only be a self-signed key.

3. how does a supply-chain manage BRSKI?

10. Security Considerations

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

11. IANA Considerations

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

12. Acknowledgements

TBD

13. References

13.1. Normative References

[I-D.ietf-6tisch-dtsecurity-zerotouch-join]
          Richardson, M., "6tisch Zero-Touch Secure Join protocol",
          draft-ietf-6tisch-dtsecurity-zerotouch-join-04 (work in
          progress), July 2019.

   [I-D.ietf-6tisch-minimal-security]
              Vucinic, M., Simon, J., Pister, K., and M. Richardson,
              "Constrained Join Protocol (CoJP) for 6TiSCH", draft-ietf-
              6tisch-minimal-security-15 (work in progress), December
              2019.

   [I-D.ietf-ace-coap-est]
              Stok, P., Kampanakis, P., Richardson, M., and S. Raza,
              "EST over secure CoAP (EST-coaps)", draft-ietf-ace-coap-
              est-18 (work in progress), January 2020.

   [I-D.ietf-anima-bootstrapping-keyinfra]
              Pritikin, M., Richardson, M., Eckert, T., Behringer, M.,
              and K. Watsen, "Bootstrapping Remote Secure Key
              Infrastructures (BRSKI)", draft-ietf-anima-bootstrapping-
              keyinfra-44 (work in progress), September 2020.

   [I-D.ietf-anima-constrained-voucher]
              Richardson, M., Stok, P., and P. Kampanakis, "Constrained
              Voucher Artifacts for Bootstrapping Protocols", draft-
              ietf-anima-constrained-voucher-08 (work in progress), July
              2020.

   [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-16 (work in
              progress), March 2019.

   [I-D.ietf-netconf-zerotouch]
              Watsen, K., Abrahamsson, M., and I. Farrer, "Secure Zero
              Touch Provisioning (SZTP)", draft-ietf-netconf-
              zerotouch-29 (work in progress), January 2019.

   [I-D.selander-ace-cose-ecdhe]
              Selander, G., Mattsson, J., and F. Palombini, "Ephemeral
              Diffie-Hellman Over COSE (EDHOC)", draft-selander-ace-
              cose-ecdhe-14 (work in progress), September 2019.

   [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>.

13.2. Informative References

   [I-D.friel-anima-brski-cloud]
              Friel, O., Shekh-Yusef, R., and M. Richardson, "BRSKI
              Cloud Registrar", draft-friel-anima-brski-cloud-03 (work
              in progress), September 2020.

   [I-D.ietf-anima-autonomic-control-plane]
              Eckert, T., Behringer, M., and S. Bjarnason, "An Autonomic
              Control Plane (ACP)", draft-ietf-anima-autonomic-control-
              plane-29 (work in progress), September 2020.

   [I-D.ietf-anima-brski-async-enroll]
              Fries, S., Brockhaus, H., and E. Lear, "Support of
              asynchronous Enrollment in BRSKI (BRSKI-AE)", draft-ietf-
              anima-brski-async-enroll-00 (work in progress), July 2020.

[I-D.ietf-cose-rfc8152bis-algs]
          Schaad, J., "CBOR Object Signing and Encryption (COSE):
          Initial Algorithms", draft-ietf-cose-rfc8152bis-algs-12
          (work in progress), September 2020.

[I-D.ietf-cose-rfc8152bis-struct]
          Schaad, J., "CBOR Object Signing and Encryption (COSE):
          Structures and Process", draft-ietf-cose-rfc8152bis-
          struct-14 (work in progress), September 2020.

[I-D.ietf-lake-edhoc]
          Selander, G., Mattsson, J., and F. Palombini, "Ephemeral
          Diffie-Hellman Over COSE (EDHOC)", draft-ietf-lake-
          edhoc-01 (work in progress), August 2020.

[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-03 (work in progress), September
          2020.

[I-D.selander-ace-ake-authz]
          Selander, G., Mattsson, J., Vucinic, M., Richardson, M.,
          and A. Schellenbaum, "Lightweight Authorization for
          Authenticated Key Exchange.", draft-selander-ace-ake-
          authz-01 (work in progress), March 2020.

[I-D.vanderstok-anima-constrained-join-proxy]
          Richardson, M., Stok, P., and P. Kampanakis, "Constrained
          Join Proxy for Bootstrapping Protocols", draft-vanderstok-
          anima-constrained-join-proxy-04 (work in progress),
          September 2020.

[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