draft-ietf-anima-bootstrapping-keyinfra

Versions 44 and 45

IETF 109 – not Bangkok

Slides from:

Michael Richardson
mcr+ietf@sandelman.ca

Rename of EST extensions -44

- In August, shortly after IETF108, there was a discussion that started in the brski-async-enroll document.
  - DOCUMENT was stuck in MISREF anyway...
- Async-enroll would like to add some end-points, but they are CMP related and just don't belong under ***/.well-known/est.***
- Okay, should we move all the BRSKI endpoints?
- My input to the thread: https://mailarchive.ietf.org/arch/msg/anima/BYpLzpiES1EcXos3vmTy-nNwAvg/
- This was IMPLEMENTATION AFFECTING. And implementors were consulted, and we agreed that it made sense.
  - Was approved with an IETF LC on 2020-09-14.
  - Also took a pass through IANA and .well-known reviewer Mark Nottingham.

The change: a picture of a thousand words

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. In all places where a binary value must be carried in a JSON string, the use of base64 format ([RFC4648] section 4) is to be used, as per [RFC7951] section 6.6.

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

skipping to change at *page 41, line 40*

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]. This is also

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 "/.well-known/brski" URI tree, as well as implementing 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 a new communication channel, similar to EST, within the newly registred "/.well-known/brski" tree. For clarity this channel is referred to as "BRSKI-MASA". (See Figure 1).

The MASA URI is "https://" authority "/.well-known/brski".

BRSKI uses existing CMS message formats for existing EST operations. BRSKI uses JSON [RFC8259] for all new operations defined here, and voucher formats. In all places where a binary value must be carried in a JSON string, the use of base64 format ([RFC4648] section 4) is to be used, as per [RFC7951] section 6.6.

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

skipping to change at *page 41, line 6*

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.

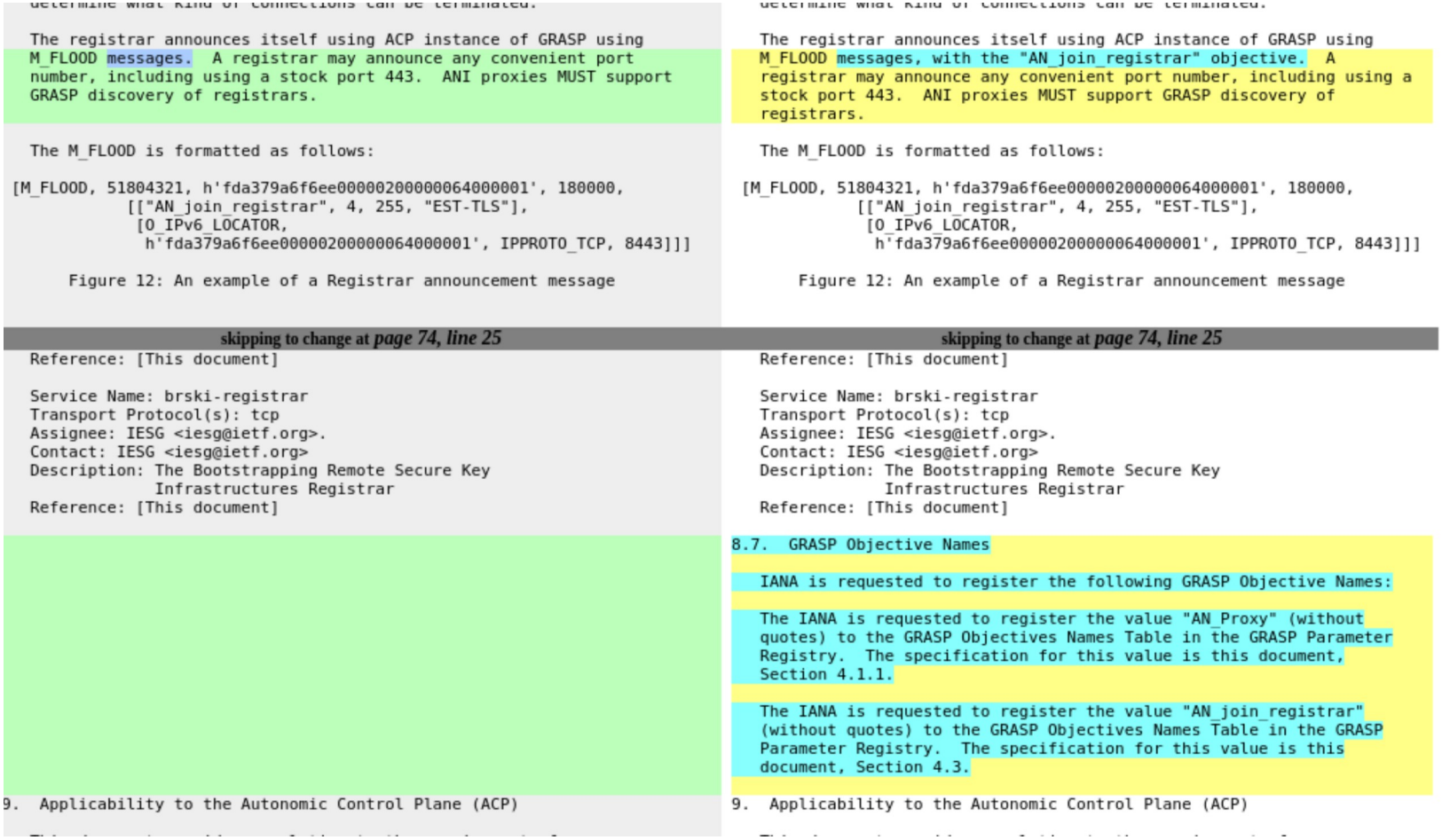
This is done with an HTTPS POST using the operation path value of "/.well-known/brski/requestvoucher".

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]. This is also

Added missing IANA action -45

- In October, Toerless noticed that the BRSKI draft was missing an IANA action for the GRASP objectives: AN_Proxy and AN_join_registrar
- A revision was created to fix the problem, and the AD approved it, and IANA was asked to review.



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, 51804321, h'fda379a6f6ee00000200000064000001', 180000,
           [["AN_join_registrar", 4, 255, "EST-TLS"],
            [O_IPv6_LOCATOR,
             h'fda379a6f6ee00000200000064000001', IPPROTO_TCP, 8443]]]
```

Figure 12: An example of a Registrar announcement message

skipping to change at *page 74, line 25*

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]

9. Applicability to the Autonomic Control Plane (ACP)

determine what kind of connections can be terminated.

The registrar announces itself using ACP instance of GRASP using M_FLOOD messages, with the "AN_join_registrar" objective. 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, 51804321, h'fda379a6f6ee00000200000064000001', 180000,
           [["AN_join_registrar", 4, 255, "EST-TLS"],
            [O_IPv6_LOCATOR,
             h'fda379a6f6ee00000200000064000001', IPPROTO_TCP, 8443]]]
```

Figure 12: An example of a Registrar announcement message

skipping to change at *page 74, line 25*

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]

8.7. GRASP Objective Names

IANA is requested to register the following GRASP Objective Names:

The IANA is requested to register the value "AN_Proxy" (without quotes) to the GRASP Objectives Names Table in the GRASP Parameter Registry. The specification for this value is this document, Section 4.1.1.

The IANA is requested to register the value "AN_join_registrar" (without quotes) to the GRASP Objectives Names Table in the GRASP Parameter Registry. The specification for this value is this document, Section 4.3.

9. Applicability to the Autonomic Control Plane (ACP)

Current state of cluster C325

Publication Queue

[About this page] [Summary statistics] [List of all active clusters]

Found 144 records

Current state	Weeks in state	Weeks in queue	Draft name (Authors)	Cluster	Pages	Submitted
EDIT*R	2.3	152.0	draft-ietf-anima-prefix-management-07 S. Jiang, Ed., Z. Du, B. Carpenter, Q. Sun	C325	22	2017-12-19
EDIT*R	2.3	103.4	draft-ietf-anima-reference-model-10 M. Behringer, Ed., B. Carpenter, T. Eckert, L. Ciavaglia, J. Nobre	C325	30	2018-11-24
EDIT*A*R	0.9	31.7	draft-ietf-anima-bootstrapping-keyinfra-45 M. Pritikin, M. Richardson, T.T.E. Eckert, M.H. Behringer, K.W. Watsen	C325	122	2020-04-09
EDIT*R	1.1	2.1	draft-ietf-anima-autonomic-control-plane-30 T. Eckert, Ed., M. Behringer, Ed., S. Bjarnason	C325	180	2020-11-02
EDIT	1.3	1.1	draft-huitema-rfc-eval-project-07 C. Huitema		50	2020-11-09

Looks like we are at the top of the Q!!!
No AUTH48 activity yet though