Constrained Voucher
draft-ietf-anima-constrained-voucher-10

Michael Richardson, Peter van der Stok, Panos Kampanakis

IETF 110
ANIMA Working Group

Constrained Voucher

BRSKI uses EST, HTTP and TLS

This draft proposes
- constrained voucher additions to voucher and use of SIDs
- Extends coap-est draft with BRSKI extensions to EST
- CoAP, CBOR, CMS, and COSE
          to support voucher transport for constrained devices

EST: Enrollment over Secure Transport
BRSKI: Bootstrapping of Remote Secure Key Infrastructures
SID: YANG **S**chema **I**tem i**D**entifier

COSE: CBOR Signing and Encryption (RFC 8152)
CMS: Cryptographic message Syntax (RFC 5652)
CBOR: Concise Binary Object Representation (RFC 7049)

Updates in -10

- excised remaining "CMS" bits, returned content-type OID
- requestauditlog removed, not part of BRSKI-EST
- rewrote almost every page
- made discovery optional for pledge, required for Registrar
- allow pledge to avoid trust anchor retrieval, if pinned key is CA key
- extensive clarification around which certificate is pinned
- clarified how Raw Public Key would work
- clarify that BRSKI-MASA protocol does not change

Issues for -11

- "proximity-registrar-subject-public-key-info" is awkwardly long. (But never sent over the wire)
- "proximity-registrar-sha256-of-subject-public-key-info" is annoying and does not fit into table.
  - please bikeshed better name!
- still have some IANA considerations to fix after est→brski change.
-

Thanks to weekly discussions in BRSKI design team on Thursday

Issues

Conclusion

1) depends upon draft-ietf-core-sid-15 and draft-ietf-core-yang-cbor-15, which are now in WGLC.
2) Currently 3 pull requests, 18 issues.
3) Expect to have DESIGN team meetings March 18, 25, April 1,8,15,22. That's six meetings, expect to close all issues.
   1) **now** is time for cross-area review of documents.
   2) hoping to get same reviewers as for BRSKI

Draft relations

Draft	WG	uses	extends
BRSKI	ANIMA	HTTP/TLS EST CMS	EST with Voucher requests MASA Circuit proxy
EST-coaps	ACE	CoAP/DTLS EST multipart-ct draft	EST with CoAP/DTLS
Voucher	ANIMA	YANG/JSON CMS	BRSKI with voucher spec
Constrained voucher	ANIMA	YANG/CBOR Voucher COSE/CMS/CBOR	Voucher with 2 fields BRSKI with COSE/CBOR and SID BRSKI with CMS/CBOR and SID
Constrained Join-proxy	ANIMA	CBOR multipart-ct draft	BRSKI with constrained join proxy and EST-coaps

Challenges with Asynchronous Registrar and pinning of public key

- In Asychronous Registrar situation, the Southbound Pledge Interface has possibly many instances, each with it's own certificate/public key.

- The pledge will pin the public key that it sees as the `pinned-domain-subject-public-key-info.` This is **just** the public key, and contains no certificate chain information.

- In simple/synchronous Registrar, the parboiled voucher-request would get signed by the same key pair as is pinned by the pledge. The MASA would therefore be able to see an entire certificate chain (from the x5u COSE pair, see draft-ietf-cose-x509-06 section 2), and would know who the registrar is.

  - (it would still put the required public key into the voucher)

- In the asynchronous registrar situation, then the relationship is not obvious, so the Registrar MUST include additional certificates leading to a common Root Certificate.

```
                              .------------.
                              |   MASA     |
                              |   client   |
                              | BRSKI-MASA |
                              '------------'
                                    ^
                                    |
 .------------.                     |              .--------------.
 | management |      .----------.   |              | certification|
 | interface  |<---| database  |----->|   authority   |
 '------------'      '----------'                  '--------------'
                          |
                          |
                          v
 .------------.      .----------.         .------------.
 | Join Proxy |      |  Pledge  |--.      | EST/BRSKI  |
 |------------|      | Interface|  |      |------------|
 |  GRASP     |      | BRSKI-EST|e |      |   GRASP    |
 |  (DULL)    |      '----------'T |      '------------'
 '------------'         '----------'
```
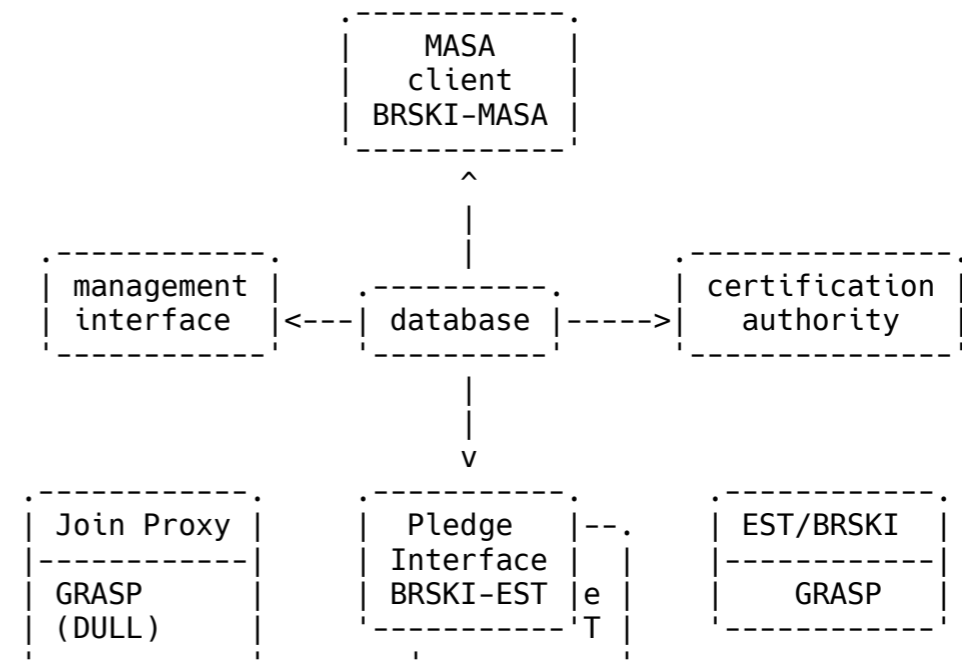
Figure 1: Reference Internal Architecture for Registrar

from
draft-richardson-anima-registrar-considerations
    section 1.3
and section 4.3 **Asynchronous Registrar**

BRSKI-EST1   BRSKI-EST2   BRSKI-MASA1   BRSKI-MASA2