Update on BRSKI-AE – Support for asynchronous enrollment

draft-ietf-anima-brski-async-enroll-00

Steffen Fries, Hendrik Brockhaus, Elliot Lear

IETF 108 – ANIMA Working Group

Recall: Problem statement & Overview

- There exists various industrial scenarios, which have limited online connectivity to local or backend services either technically or by policy used during onboarding / enrollment.
  - Use Case 1: limited on-site PKI functionality support, requires relying on a backend PKI, to perform (final) authorization of certification requests for operational certificate (LDevID).
  - Use Case 2: limited connectivity to a domain registrar due to different technology stack or limited connectivity
- Draft addresses these issues by updating BRSKI to support authenticated self-contained objects (signed-wrapped objects) for the certificate enrolment to bind proof of possession and poof of identity to the objects in a similar way as already applied for the voucher handling to be transport independent.

Changes from individual version 03 IETF draft 00

- Inclusion of discovery options of enrollment endpoints at the domain registrar based on well-known endpoints in Section 5.3 as replacement of section 5.1.3 in the individual draft. This is intended to support both use cases in the document. An illustrative example is provided.
- Missing details provided for the description and call flow in pledge-agent use case Section 5.2, e.g. to accommodate distribution of CA certificates.
- Updated CMP example in Section 6 to use lightweight CMP instead of CMP
- Editorial changes to improve structure and readability

Changes from individual version 03 IETF draft 00 Discovery support

- If multiple enrollment protocols are intended to be supported by the domain registrar, a discovery option is necessary to allow the pledge to pick the appropriate.
- Draft proposes to define new URI for the discovery as "/.well-known/brski"
- GET on "/.well-known/brski“ shall return a link to endpoints available at the server
- Draft provides an illustrative example for EST and Lightweight-CMP (see next slide)

- Proposal to rename the endpoints for the voucher handling from “est” to “brski” in BRSKI to underline independence from the enrollment protocols

Changes from individual version 03 → IETF draft 00 Discovery Example

```
REQ: GET /.well-known/brski
RES: Content
   </brski/voucherrequest>,ct=voucher-cms+json
   </brski/voucher_status>,ct=json
   </brski/requestauditlog>,ct=json
   </brski/enrollstatus>,ct=json

   </est/cacerts>;ct=pkcs7-mime
   </est/simpleenroll>;ct=pkcs7-mime
   </est/simplereenroll>;ct=pkcs7-mime
   </est/fullcmc>;ct=pkcs7-mime
   </est/serverkeygen>;ct= pkcs7-mime
   </est/csrattrs>;ct=pkcs7-mime

   </cmp/initialization>;ct=pkixcmp
   </cmp/certification>;ct=pkixcmp
   </cmp/keyupdate>;ct=pkixcmp
   </cmp/p10>;ct=pkixcmp
   </cmp/getCAcert>;ct=pkixcmp
   </cmp/getCSRparam>;ct=pkixcmp
```

Changes from individual version 03 IETF draft 00 Details further changes

- Missing details provided for the description and call flow in pledge-agent use case (section 5.2.4):
  - Several editorial enhancements to better distinguish the standard BRSKI from the enhancements for the pledge-agent
  - Included optional distribution of CA certificates in the call flow.

- Updated CMP example in Section 6 to use lightweight CMP instead of CMP
  - Profile provides the necessary functionality for industrial use cases without requiring complete CMP support
  - Draft already provides the necessary /.well-known endpoints

Changes from individual version 03 IETF draft 00 Details editorial changes

- Editorial changes
  - Requirements discussion moved to separate section in Section 4. Shortened description of proof of identity binding and mapping to existing protocols.
  - Removal of copied call flows for voucher exchange and registrar discovery flow from [I-D.ietf-anima-bootstrapping-keyinfra] in Section 5.1 to avoid doubling or text or inconsistencies.
  - Reworked abstract and introduction to be more crisp regarding the targeted solution. Several structural changes in the document to have a better distinction between requirements, use case description, and solution description as separate sections. History moved to appendix.

Discussion, open issues

#1 Discovery of enrollment options

- Follow proposal in current draft using “GET / .well-known/brski/” resulting in the enumeration of available enrollment options?
- Alternatively align syntax with format provided in COAP related drafts to something like “GET / .well-known/core?rt=brski”

Discussion, open issues

#2 Pledge-agent authentication and authorization in use case 2 towards domain registrar? (relates to section 5.2.4)

- Intention to not require specific device credentials (LDevID, IDevID) for the pledge-agent to authenticate towards domain registrar to allow for arbitrary device usage running the pledge-agent.
- Pledge relies on signed objects from infrastructure (voucher from MASA to accept domain certificate). Infrastructure relies on signed objects from the pledge.
- Proposal to rely on (pledge-agent) operating user authentication if authorization of onboarding is required in the target domain.

Discussion, open issues (cont.)

#3 Provisioning of proximity registrar certificate to pledge necessary?

- If provided via the pledge agent without authentication may not provide benefit would result in requirements for the data exchange between pledge and pledge-agent (which is not part of this document) to be based on mutual trust between pledge and pledge-agent.
- Rely on voucher response containing the domain registrar certificate

#4 Consideration of different transport options in the addressing scheme for the enrollment protocol?

- Proposal to align with BRSKI (HTTPS) as BRSKI-AE is intended to update BRSKI

- IANA considerations for addressing scheme have to be defined.

Next Steps

- Further refinement of the approach. Address open issues and discussion points stated throughout the draft
- Goal is reuse of BRSKI architecture elements and described call flows for both use cases described in BRSKI-AE.
- The intended scope of the draft would update the BRSKI document.
- PoC currently being implemented for Use Case 2 (Pledge Agent).