Update on BRSKI-AE – Support for asynchronous enrollment

draft-ietf-anima-brski-async-enroll-01

Steffen Fries, Hendrik Brockhaus, Elliot Lear, Thomas Werner

IETF 110 – ANIMA Working Group

Recall: Problem statement & Overview

- There exists various Industrial IOT and OT use cases, which have limited online connectivity to local or backend services either technically or by policy used during bootstrapping.
  - Use Case 1: (follows the BRSKI model) limited on-site PKI functionality support, requires relying on a backend PKI, to perform (final) authorization of certification requests for bootstrapping the site certificate (LDevID). PULL model as the pledge (-caller) acts as a client to provide its onboarding information to the registrar.
  - Use Case 2: reversed pledge client –server role in deployment (e.g. limited connectivity to a domain registrar). Pledge is triggered (pushed) to generate and receive bootstrapping data.
- Draft addresses these issues utilizing authenticated self-contained objects (signature-wrapped objects) for the certificate enrolment to bind proof of possession and poof of identity to the enrolment exchanges (similar to voucher exchanges with pledge)

BRSKI-AE Status
History of changes from version 00 to version 01

- Update of scope in Section 3.1 to motivate use case 2 in which the pledge acts as server.
- Rework of use case 2 in Section 5.2 to consider the transport between the pledge and the pledge-agent. Includes TLS channel establishment between the pledge-agent and the pledge as well as the endpoint definition on the pledge.
  → Proposal to change current TLS approach, see slide 4-6
- First description of exchanged object types (needs more work) in the call flow.
- Clarification in discovery options for enrollment endpoints at the domain registrar based on well-known endpoints in Section 5.3 did not result in additional /.well-known URIs.
- Update of the illustrative example. Note naming to /brski for the voucher related endpoints has been taken over in the BRSKI main document (thanks to Michael).
- Start Security consideration section. Updated references.
- Included Thomas Werner as additional author for the document.

BRSKI-AE Status, Use Case 2
Trust Establishment (Pledge/Pledge-agent/Registrar)

- Goal: Trust Establishment between Pledge and Registrar based on authenticated self-contained objects (as signed objects). No binding to TLS.
- Discovery of pledge by the pledge-agent proposed via mDNS
- Trust Establishment between the pledge-agent and pledge (current focus) to protect the pledge endpoints against potential DoS attacks
  - TLS connection between pledge-agent and pledge based on a PSK (e.g., provided by QR code with pledge-specific information and random data).
    Assumption: pledge-agent must have been in physical proximity to get information.
  - Discussion (design team) showed that TLS-PSK may not be the favorized approach. Also a new definition using QR codes for connection setup was questioned.
  - Alternative to be discussed → see next slide
    (acme-star-delegation or TLS-subcerts were also named but need more investigation)

BRSKI-AE Status, Use Case 2
Trust Establishment (Pledge/Pledge-agent/Registrar)

- Alternative proposal not using TLS between pledge and pledge-agent
- DoS protection only for registrar endpoints → TLS between pledge-agent and registrar
- Registrar certificate provided by pledge-agent to be included in the voucher-request → included in the (IDevID signed) voucher-request as new leaf “agent-provided-registrar-cert”
- Enables the registrar (am I the right one) and the MASA verify the certificate contained in the voucher-request (besides further verification like the serial number of the pledge) → could use existing voucher assertion "verified" or "logged", or define a new assertion
- Pledge-agent may verify pledge serial number in voucher-request with information provided upfront
- Registrar verifies pledge serial number and its own certificate as part of the voucher-request
- What do we loose? Proximity to registrar via mutually authenticated TLS (and assertion in voucher).
- What do we gain? Flexibility in the bootstrapping approach by keeping the number of roundtrips.
- Thoughts?

BRSKI-AE Status, Use Case 2
Trust Establishment (Pledge/Pledge-agent/Registrar), cont.

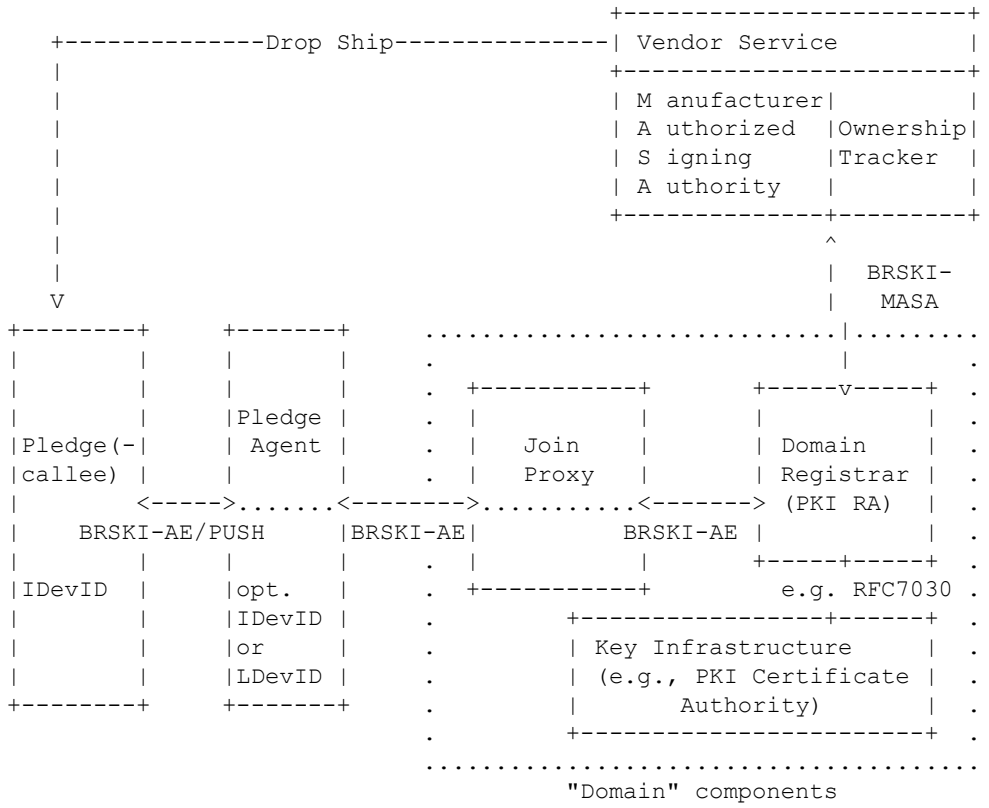
- Trust Establishment between the pledge-agent and registrar may be with LDevID of pledge-agent (could be provided through an independent BRSKI run or by manual task). Enables distinction on the registrar side if a pledge connects or a pledge-agent.
- Pledge-agent provides registrar certificate to pledge for inclusion into voucher-request provides the registrar to verify, it gets a voucher-request for a pledge to be bootstrapped and if it is the correct registrar. (see also slide before)
- Discussion in the design team regarding a potential authorization token, which is provided in a pre-run to the pledge-agent and then forwarded to the pledge for inclusion into the voucher-request, to be checked by the registrar during voucher-request verification, but was not further followed.

BRSKI-AE Status, Use Case 2
Pledge endpoints, content types, and objects

- Endpoints on pledge and potential object types (current state of discussion, first concrete example):
  - /triggervoucherrequest: initiates pledge(-callee) voucher request creation, potentially with additional information (e.g., registrar certificate) → application/json
    returns pledge(-callee) voucher request → to be discussed: e.g., JOSE object (application/voucher-jose+json)
  - /supplyvoucherresponse: provide voucher response to pledge(-callee) → to be discussed: e.g., JOSE object like the voucher-request (application/voucher-jose+json)
    returns pledge(-callee) voucher status → to be discussed: e.g., JWS
  - /triggerenrollrequest: initiates pledge(-callee) certification request creation → application/json
    returns certification request → PKCS#10-signed-with-IDevID (Format: e.g., JWS)
  - /supplyenrollresponse: provide domain credentials to pledge(-callee) → application/pkcs7-smime; smime-type=certs-only
    returns pledge(-callee) enroll status → to be discussed: e.g., JWS
- Note that the object types need to be aligned with the existing object types on the registrar.

BRSKI-AE Status, Use Case 2 Terminology discussion

- Pledge-agent vs. Registrar-agent
  - As the agent is intended to provide the interface to the registrar and also to be manufacturer independent, a better naming may be indeed registrar-agent.
  - Any objection to the renaming?
- PULL/PUSH
  - Currently used to distinguish between pledge acting as client or server.
  - Better naming to ensure no confusion with the communication direction and other components requested.
  - Alternative may be client/server mode for the pledge or pledge-initiated/agent initiated bootstrapping
  - Thoughts?



Note: Join Proxy may be optional, depending on pledge-agent configuration or registrar discovery

Discussion, open issues from IETF 109

#1 Discovery of enrollment options on registrar:

- removed “GET / .well-known/” approach (does not work over HTTP)
- Assumption: Pledge is the constraint only has one enrollment option. Hence, the flexibility is expected on the registrar side to be able to serve different enrolling. If an endpoint is not available on the domain registrar, it will answer with an error message resulting in the inability for onboarding the specific pledge.

#2 Pledge-agent authentication and authorization in use case 2 towards domain registrar
→ ongoing discussion in design team, current state is relying on LDevID

#3 Necessity of providing (proximity) registrar certificate to pledge for inclusion into voucher request:
→ approach of agent-provided certificate currently discussed in design team to support check that registrar is the target registrar

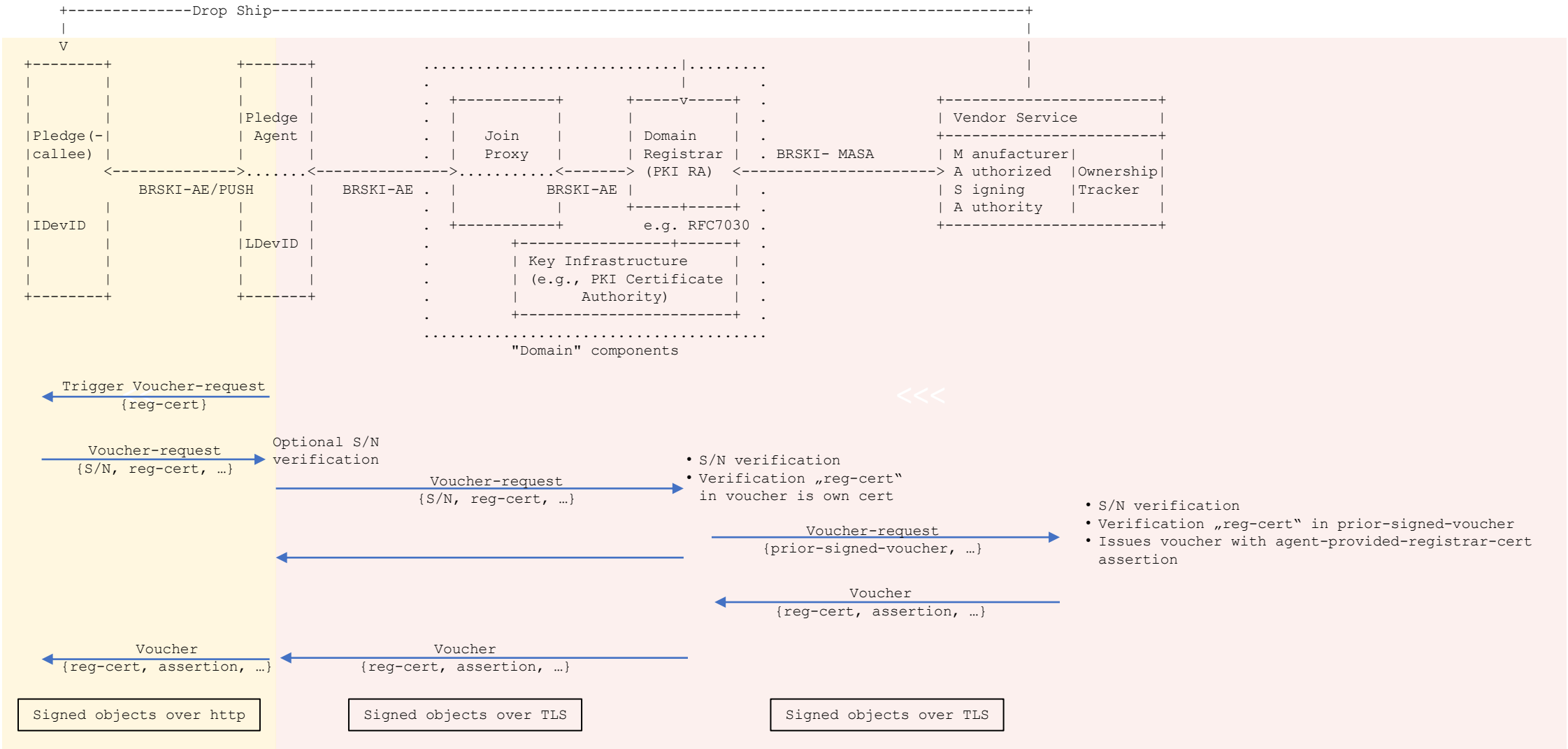
#4 Consideration of different transport options in the addressing scheme for the enrollment protocol: current draft assumed to follow the BRSKI approach (HTTP), but could be enhance for CoAP (over DTLS or with OSCORE)

Next Steps

- Further refinement of the pledge-server (PUSH) approach in the design team addressing the open issues and questions
  - Alignment of object types used in the interaction of the pledge-agent with pledge/registrar,
  - Clarification that these are implementation options also allowing other encoding preferably in additional drafts
- Terminology clarifications
- Clarification of further open issues stated in the draft
- Circulate outcome on the mailing list for further discussion

Backup

BRSKI-AE Status, Use Case 2
Trust Establishment (Pledge/Pledge-agent/Registrar)



BRSKI-AE Status, Use Case 2
Trust Establishment (Pledge/Pledge-agent/Registrar)

- Alternative proposal not using TLS between the pledge and the pledge-agent under the following assumptions
  - the TLS connection for DoS protection only necessary for the registrar endpoints
  - the registrar certificate is always included in the voucher request
  - the registrar and the MASA verify the certificate contained in the voucher-request (besides further verification like the serial number of the pledge)
- Pledge-agent communicates with the pledge via plain http and provides registrar certificate to the pledge
- Pledge constructs voucher-request, includes registrar certificate, signs with IDevID
- Pledge-agent may verify the pledge serial number in the IDevID by information provided upfront QR code from the pledge and forwards voucher-request via https to registrar
- Registrar verifies pledge serial number and its own certificate as part of the voucher-request