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 onboarding / enrollment.
  - Use Case 1: (follows the BRSKI PULL 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: (introduces PUSH mode to pledge) reversed pledge client –server roles in deployment (e.g. limited connectivity to a domain registrar). PUSH model as the pledge(-callee) acts as server (is triggered (PUSHed)) to generate and receives (gets PUSHed) the 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

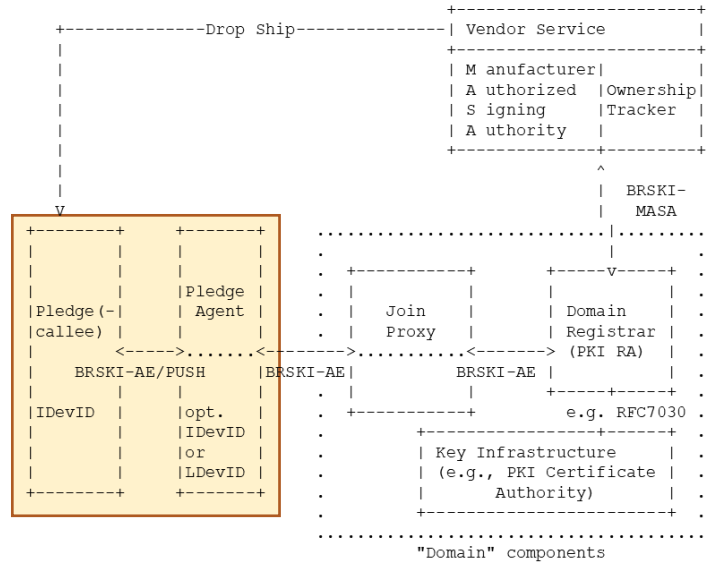
- Update of scope in Section 3.1 to include in which the pledge acts as a server. This is one main motivation for use case 2.
- Rework of use case 2 in Section 5.2 to consider the transport between the pledge and the pledge-agent. Addressed is the TLS channel establishment between the pledge-agent and the pledge as well as the endpoint definition on the pledge.
- 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.

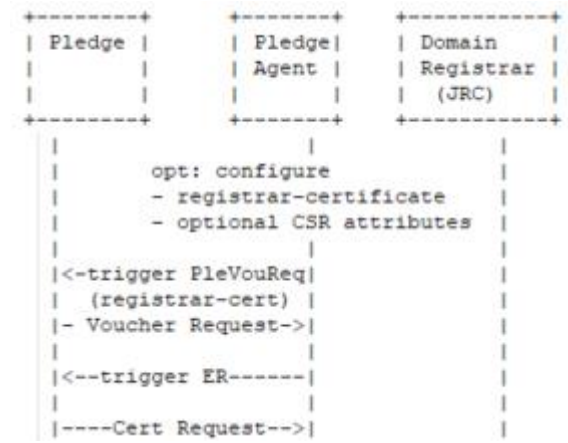
BRSKI-AE Status, Use Case 2
Trust Establishment (Pledge/Pledge-agent/Registrar)

- 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
  - Setup of TLS connection between pledge-agent and pledge proposed based on a PSK, which may be provided by a QR code and incorporates pledge specific information. Assumption is that the pledge-agent must have been in physical proximity to get this information and to be able to setup connection.
  - Discussion (design team) showed that TLS-PSK may not be the favorized approach
  - Alternatives to be discussed (acme-star-delegation or TLS-subcerts were named but need more investigation)

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

- Alternative proposal under the assumption that
  - the TLS connection for DoS protection is only necessary from the pledge-agent towards the registrar to protect the registrar endpoints also used by other components
  - the proximity 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 scanning information like a 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





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

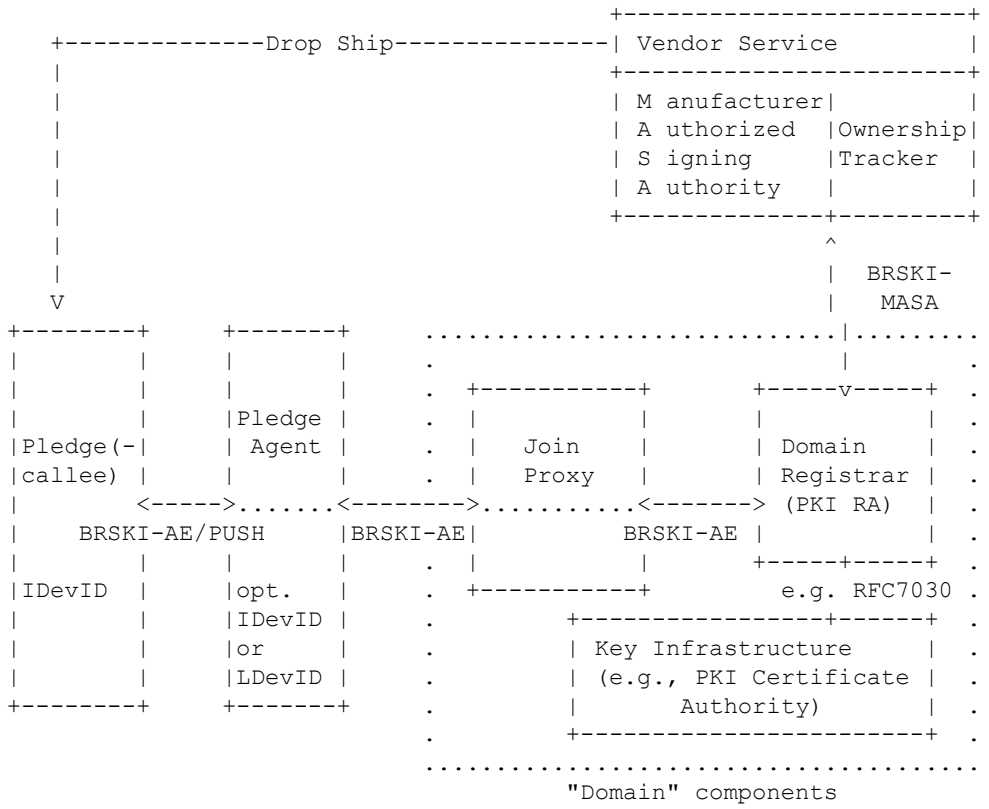
- Trust Establishment between the pledge-agent and registrar may be with LDevID of pledge-agent (could be provided through an independent BRSKI run or by manual task)
- Discussion in the design team regarding a potential authorization token, which is provided in a pre-run to the pledge-agent and then 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):
  - /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
  - Reflects the interaction with the pledge.
  - If the pledge acts as client, it would be in the PULL model as it pulls domain information from the registrar. Likewise if the pledge acts as server, domain specific information is provided to the pledge or the pledge is triggered (pushed) to create necessary onboarding information.
  - Alternative may be client/server mode for the pledge or pledge-initiated/agent initiated bootstrapping



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: initial proposal to use “GET / .well-known/” to get enumeration of available endpoints on the domain registrar does not work in the HTTP use case. Also, assumption is that the pledge is the constraint part and not able to provide different enrollment options. Hence, the flexibility is expected on the registrar side to be able to serve different pledges (with different enrollment options). 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 PUSH towards domain registrar
→ ongoing discussion in design team

#3 Necessity of providing (proximity) registrar certificate to pledge for inclusion into voucher request:
→ current discussion in design team tends to support this to enable registrar to verify that it 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 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
- Terminology clarifications
- Circulate outcome on the mailing list for further discussion
- Update draft with results