Update on BRSKI-AE – Support for asynchronous enrollment

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

Steffen Fries, Hendrik Brockhaus, Elliot Lear

IETF 109 – ANIMA Working Group

Recall: Problem statement & Overview (PULL model)

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: (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 operational certificate (LDevID). The pledge PULLs all necessary information from the registrar

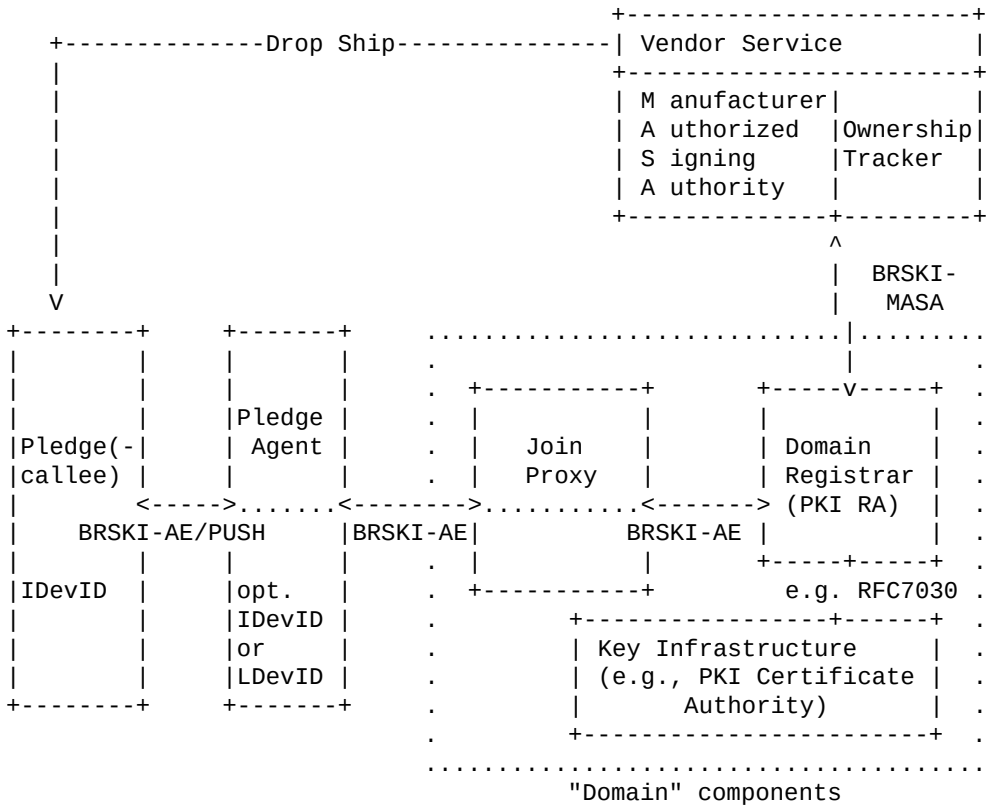
Recall: Problem statement & Overview (PUSH)

- Use Case 2: (introduces PUSH model) reversed client – server roles in deployment (e.g. limited connectivity to a domain registrar).
  - The pledge(-callee) is triggered to generate or to receive the necessary onboarding information.

Draft addresses these issues by enhancing 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 pledge voucher handling to be transport independent.

BRSKI-AE Status
Current focus on use case 2 – PUSH model

- Develop PUSH model interaction between pledge(-callee), pledge-agent, and domain registrar
- Protocol approach for the first step close to BRSKI, with the specifics of the PUSH model with reversed roles between pledge(-callee) and pledge-agent:
  - TLS between components
  - HTTP transport of objects
- Clarification ongoing on
  - Trust relations between components to ensure onboarding of the right pledge in the right domain
  - Endpoint definition for the pledge(-callee) modeled similar to BRSKI exchanges
  - Object format for exchange of signature wrapped objects (pledge voucher and certification request)



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

Backup (more details)

BRSKI design team discussions focus on use case 2: Trust relations

- Clarification of trust relation between pledge-agent and pledge and pledge-agent and domain registrar. Ideal: less trust assumptions on pledge-agent (could be ideally on a mobile device and only temporary available).
- Options
  - Pledge-agent / pledge(-callee): Potential use of a QR code or similar to show proximity between pledge(-callee) and pledge-agent.
  - Can be used for instance in a TLS cipher suite.
    Use of `draft-ietf-tls-subcerts` has been discussed, but not considered a good fit, as other use cases may not feature a TLS connection here and benefit a close protocol binding (e.g., BT or NFC or other)
  - Pledge-agent / registrar: Potential use of server side only TLS and HTTP authentication from the pledge-agent (e.g. allowing a service technician to authenticate) as alternative to LDevID on pledge-agent (both already stated in the 00 draft for use case 2)
- Ongoing discussion about potential attack and misuse cases when relying on signature wrapped object exchange between pledge(-callee) and domain registrar

Further discussions on use case 2: Pledge-endpoints

- Endpoints on the pledge are currently discussed allowing a pledge agent to trigger voucher request generation and enrollment request generation. Generally aligned with BRSKI interaction.
- Demand seen for at least four endpoints:
  - /triggervoucherrequest: initiates pledge(-callee) voucher request creation, potentially with additional information (e.g., registrar certificate), returns pledge(-callee) voucher request
  - /triggerenrollrequest: initiates pledge(-callee) certification request creation, returns certification request
  - /supplyvoucherresponse: provide voucher response to pledge(-callee), returns pledge(-callee) voucher status
  - /supplyenrollresponse: provide domain credentials to pledge(-callee), returns enrollment status
- Clarification has to start regarding supported encodings of the objects exchanged:
  - Current voucher object is CMC-signed-JSON. Discussion on relying on JWS-signed-JSON in the first step, would also align with using similar formats for the certification request.

Changes to IETF draft 00 for -01 (not submitted yet)

- Update of scope in Section 3.1 to include that specifically the pledge acts as a receiver in use case 2 (PUSH model). The Pledge(-callee) is receiving requests in the onboarding process in order to get his credentials pushed.
- Update of introduction of use case 2 in Section 5.2 to state that the transport between the pledge and the pledge agent will be HTTP in the context of this document but may also be done using other protocols. Introduction of sub section related to the discovery of pledge (-callee) and pledge-agent in use case 2 in Section 5.2.4.
- Clarification in discovery options for enrollment endpoints at the domain registrar based on well-known endpoints in Section 5.3. Note that the change to /brski for the voucher related endpoints has been taken over in the BRSKI main document.
- Updated references.

Discussion, open issues from IETF 108

#1 Discovery of enrollment options on registrar: uses “GET / .well-known/” resulting in the enumeration of available endpoints on the domain registrar, so pledge or pledge-agent may pick

#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 he 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)

Next Steps

- Further refinement of the PUSH approach in the design team addressing the open issues
- Circulate outcome on the mailing list for further discussion
- Update draft with results