Update on BRSKI-AE – Support for asynchronous enrollment

draft-fries-anima-brski-async-enroll-02

Steffen Fries, Hendrik Brockhaus, Elliot Lear

IETF 106 – ANIMA Working Group

Problem statement

- There exists various industrial scenarios, which
  - have limited online connectivity to backend services either technically or by policy used during onboarding / enrollment.
  - assume only limited on-site PKI functionality support (Proxy), either
    - rely on a backend or centralized PKI, to perform (final) authorization of certification requests for an operational certificate (LDevID).
    - may not feature trusted domain component for store and forward
  - require multiple hops to the issuing PKI due to network segmentation or apply different transport protocols between the pledge and the issuing RA/CA.
  - required consistency for certificate management over device / system lifecycle (e.g. , pre-selected enrollment protocols)

Changes from version 01 → 02

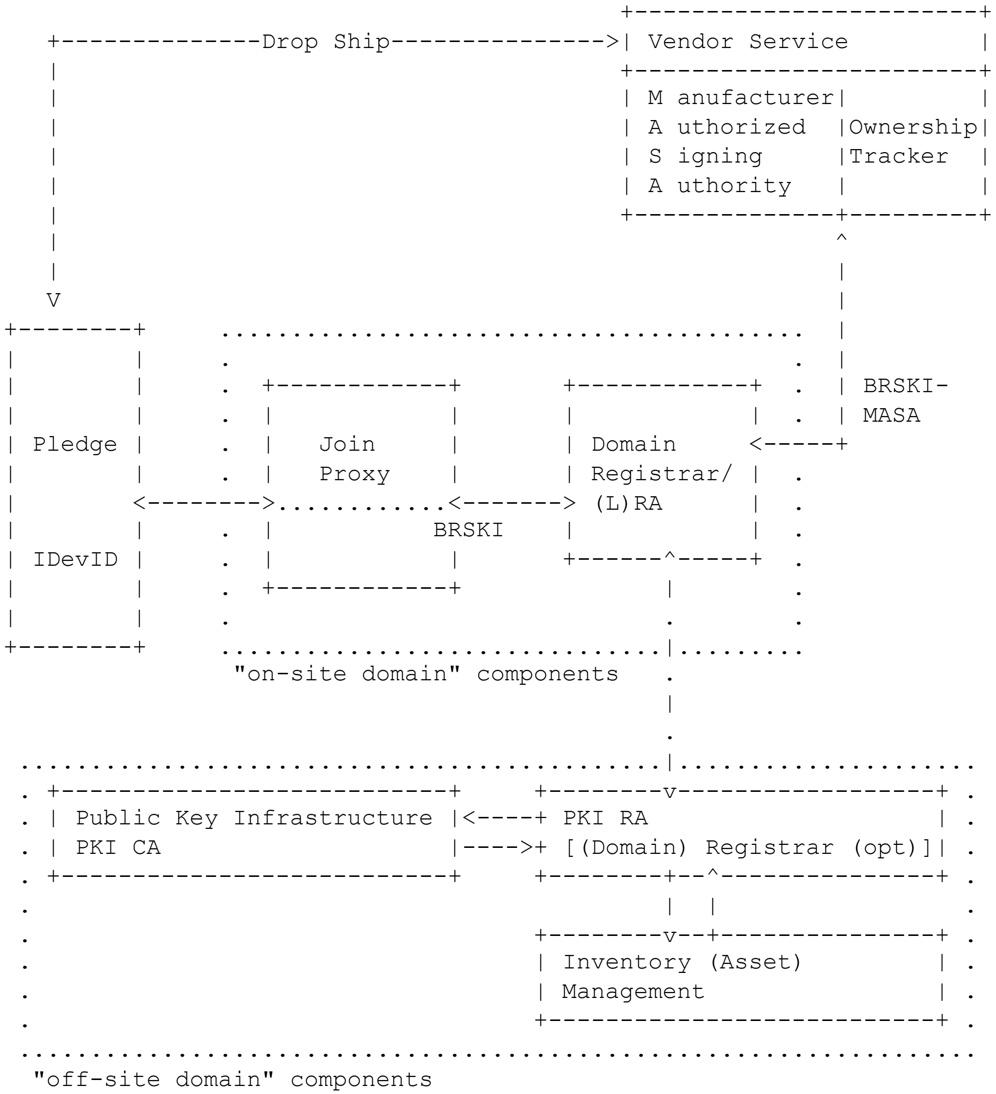
- Update of introduction text to clearly relate to the usage of IDevID and LDevID in the context of self-contained objects (approach described in a protocol agnostic way)
- Update of description of architecture elements and changes to BRSKI in Section 5
- Enhancement of addressing scheme used in BRSKI to allow for support of multiple enrollment protocols in BRSKI-AE in Section 5.3. Also considers first steps for an optional discovery mechanism to address situations in which the registrar supports more than one enrollment approach. (see next slides)
- Enhanced consideration of existing enrollment protocols in the context of mapping the requirements to existing solutions in Section 4.3 and in Section 7.

Recall: Asynchronous enrollment with authenticated self-contained objects

- Asynchronous enrollment has to cope with at least the following requirements:
  - Proof of possession of the private key corresponding to the public key contained in the certification request.
  - Proof of identity of the requestor, bound to the certification request (and thus to the proof of possession). → BRSKI does the binding via the transport protocol, BRSKI-AE motivates self-contained objects.
- Certificate waiting indication if the contacted RA is not able to issue the requested certificate immediately or is not reachable.
- Draft lists requirements for handling self-contained objects and is agnostic regarding the actual enrollment protocol, but already takes existing approaches into account.

BRSKI-AE provides enhancements for BRSKI to support asynchronous enrollment

- Utilizes authenticated self-contained-object for LDevID certification request/response (CSR wrapping using existing certificate (IDevID)).
- Allows interaction with on-site and off-site PKI
  - rely on on-site simple store-and-forward (optionally no RA functionality at Domain Registrar)
  - CSR authorization in conjunction with off-site asset management system
  - defines/maps certificate waiting indication
- Support for multiple enrollment protocols, which also allows application in domains that already selected different enrollment protocols.



Changes in draft-02: Addressing scheme for multiple enrollment protocol support

- If registrar supports multiple enrollment protocols, an addressing scheme is needed to distinguish between them. Note that enrollment protocol is considered as a sequence of at least a certification request and a certification response message.
- Proposal to follow the BRSKI approach using "/.well-known" tree specified [RFC5785]:
- Proposed notation: "/.well-known/enrollment-protocol/request"
    - *enrollment-protocol:* references EST, CMP, CMC, SCEP, or newly defined approaches, like EST wrapping with OSCORE from ACE WG (draft-selander-ace-coap-est-oscore-01).
    - *request:* describes required operation at the registrar side, e.g., for BRSKI base behavior this would be a "simpleenroll" and for BRSKI-AE a "FullCMCRequest.

Changes in draft-02: Addressing scheme for multiple enrollment protocol support (cont.)

- Discussion / Open Issues
  - Consideration of different transport options in the addressing scheme for the enrollment protocol, like on the example of EST:
    - BRSKI uses EST over HTTPS
    - draft-ietf-ace-coap-est utilizes COAPS to transport EST
  - Selection of a limited set of mandatory enrollment approaches for the infrastructure side to ensure interoperability (allows flexibility for the pledge side by requiring support of just one).
  - Optional discovery mechanism for supported enrollment protocol options at the infrastructure side. Could utilize the defined namespace.
  - 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.
- Discussion of operational modes for onboarding based on industrial use cases to leverage the existing architecture elements in different approaches:
    - Currently BRSKI and BRSKI-AE target PULL behavior of the pledge, i.e., pledge acts as client (caller/requestor) and starts onboarding after connectivity to network and power.
    - Further use cases exist, which rely on PUSH behavior, in which the pledge is natively working as server and therefore acting as calleé.
- Goal is reuse of BRSKI/BRSKI-AE architecture elements as much as possible to cope with both modes. → Not asking for adoption of draft this time as further discussion on operational modes seen necessary before incorporating this functionality into the draft.