# Update on BRSKI-AE – Support for asynchronous enrollment

draft-fries-anima-brski-async-enroll-03

**Steffen Fries**, Hendrik Brockhaus, Elliot Lear

IETF 107 – 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), while relying on a backend or centralized PKI, to perform (final) authorization of certification requests for an operational certificate (LDevID).
  - may have limited connectivity to a registrar due to different technology stack or limited connectivity
- The draft addresses these issues by updating BRSKI to also support authenticated self-contained objects for the certificate enrolment as already applied for the voucher handling to be transport independent.

# Changes from version 02 → 03

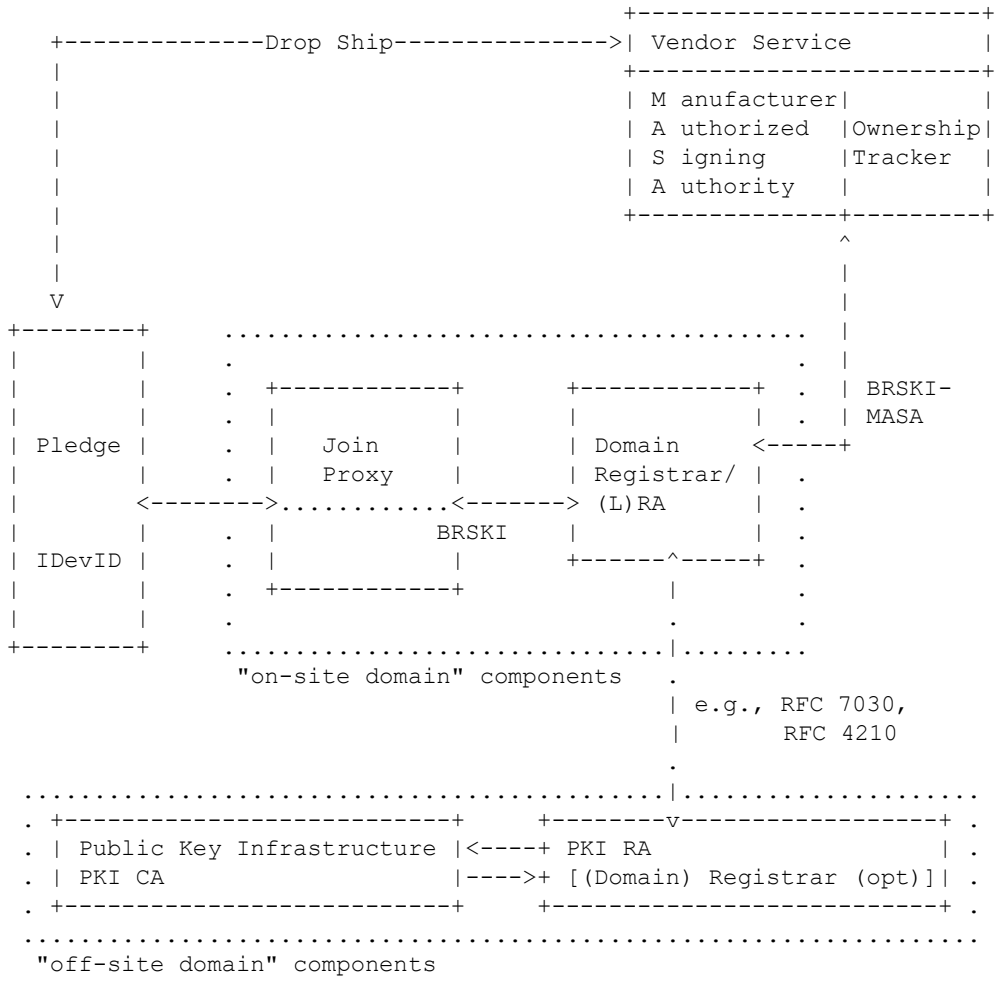
- Update of terminology from self-contained to authenticated self-contained object to be consistent in the wording and to underline the protection of the object with an existing credential.  Note that the naming of this object may be discussed.  An alternative name may be attestation object.
- Editorial improvements, simplification of the architecture picture for the initial use case having an offsite PKI (avoided the explicit inventory management).
- Introduction of a new application scenario also utilizing authenticated self-contained objects to onboard a pledge using a commissioning tool containing a pledge agent in case of limited connectivity to a registrar.
  - Requires changes in the BRSKI call flow sequence and potentially trust assumptions
  - Adoptions in introduction, application example, and related BRSKI-AE call flows.
- Update of provided examples of the addressing approach used in BRSKI to allow for support of multiple enrollment protocols in Section 5.1.5.

# 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-EST does the binding via the transport protocol, BRSKI-AE motivates self-contained objects, which can be supported by existing enrolment protocols/options.
- 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.

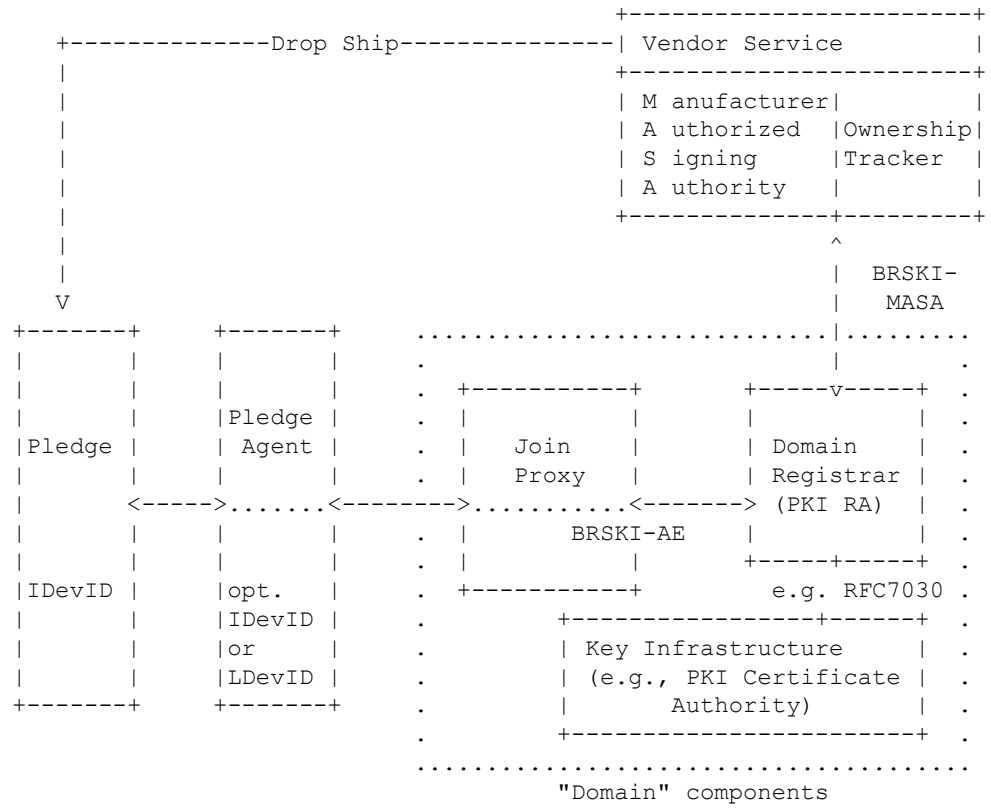
# BRSKI-AE Use Case 1: Off-site PKI components

- Keeps discovery and voucher handling as defined in BRSKI
- Main enhancement: Utilizes authenticated self-contained-object for LDevID certification request/response to support 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 off-site PKI
  - defines/maps certificate waiting indication
- Support for multiple enrollment protocols, which also allows application in domains that already selected different enrollment protocols → Utilizes well-known URI to allow for other enrolment protocol (options).



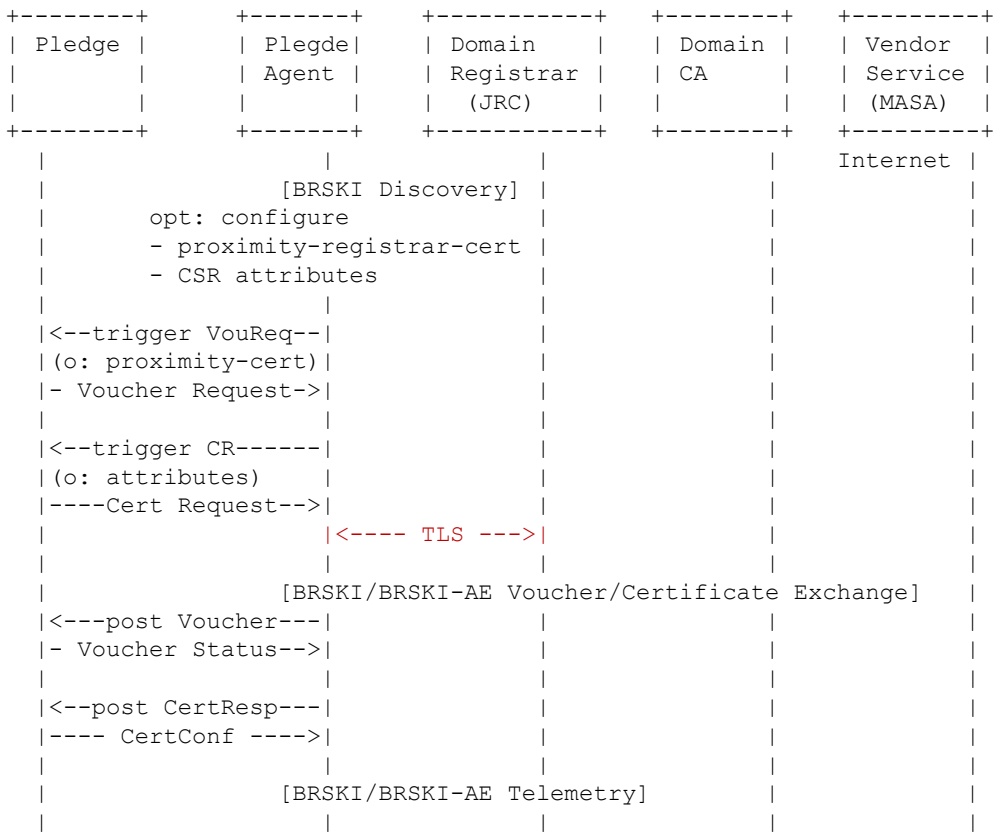
# BRSKI-AE Use Case 2: Pledge Agent (Architecture)

- Goal to reuse BRSKI interface at Registrar
- Introduces pledge agent as proxy of the pledge to allow onboarding of devices with different technology stack but request domain trust establishment.
- Main enhancement: Decouples voucher handling and certificate handling from transport layer security by completely relying on authenticated self-contained-objects.
- Allows for bulk onboarding of devices using the same connection.
- May require separate approach for pledge agent authentication/authorization.



# BRSKI-AE Use Case 2: Pledge Agent (Call Flow)

- Communication between pledge and pledge agent may be vendor specific, interoperability with infrastructure achieved by defined objects. Pledge agent uses BRSKI-AE to communicate to Registrar.
- Registrar discovery may be optionally performed between pledge agent and registrar. Alternative: could be configured.
- Agent may be preconfigured with proximity registrar cert and CSR attributes
- Agent triggers creation of Voucher Request and Certification Request
- Establishes connection to Registrar → only deviation from BRSKI call flow here as pledge agent may not authenticate in TLS with IDevID.
- Agent requests voucher and certificate and pushes both to pledge, which can validate the voucher first using based on availability of manufacturer root certificate and then the LDevID certificate.
- Allows for bulk onboarding of devices using the same connection.
- May require separate approach for pledge agent authentication/authorization, either with an own LDevID (initial bootstrapping as defined in BRSKI) or alternatively by authenticating the user of the pledge agent.



# Discussion, open issues

- Pledge agent authentication and authorization in use case 2?
  - Intention to not require specific device credentials (LDevID, IDevID) for the pledge agent to allow for arbitrary device usage.
  - 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.
- Provisioning of proximity registrar certificate to pledge necessary?
  - If provided via the pledge agent without authentication may not provide benefit.
  - Registrar created voucher-request contains registrar certificate and chain

# Discussion, open issues (cont.)

- Addressing scheme supporting multiple enrollment protocols introduced in draft-02 to specific?
  - Keep notation: "/.well-known/enrollment-protocol/request" or
  - change to "/.well-known/enrollment-protocol“

  Proposal to go with the latter avoid redefining syntax from existing enrollment protocols like EST (RFC 7030) or the lightweight CMP (draft-ietf-lamps-cmp-profile-01)
- Consideration of different transport options in the addressing scheme for the enrollment protocol?
  - BRSKI uses EST over HTTPS
  - draft-ietf-ace-coap-est utilizes COAPS to transport EST

  Proposal to align with BRSKI as BRSKI-AE is intended to update BRSKI
- Optional discovery mechanism for supported enrollment protocol options at the infrastructure side. May provide an enumeration of potential options, based on the defined namespace for the well-known URI.
- 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. Shorten motivation or move application use cases to an annex.
- 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).
- WG in favor of adopting the draft?