Update on BRSKI-AE – Support for asynchronous enrollment

draft-fries-anima-brski-async-enroll-01

Steffen Fries, Hendrik Brockhaus, Eliot Lear

IETF 105 – ANIMA Working Group
Problem statement

• There exists various industrial scenarios, which
  • have limited online connectivity to backend services either technically or by policy. This may limit the exchange of certification request/response messages with an offsite PKI for issuing an LDevID.
  • assume only limited on-site PKI functionality support (Proxy)
    • 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.
  • required consistency for certificate management over device / system lifecycle (e.g. , existing industrial standards require support of multiple enrolment protocols on the central side, while letting the pledge pick)
Changes from version 00 → 01

• Update of examples, specifically for building automation as well as introduction of two new application use cases (Infrastructure isolation policy, Less operational security in the deployment domain) in section 4.2.

• Consideration of existing enrollment protocols in the context of mapping the requirements to existing solutions in Section 4.3.

• Enhancement of description of architecture elements and potential changes to influences on BRSKI in Section 5.

• Removal of combined asynchronous interaction with MASA to not complicate the use case in section 5.

• New section 7 starting with the mapping to existing enrollment protocols by collecting boundary conditions.
Asynchronous enrollment with 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)
  • Certificate waiting indication if the contacted RA is not able to issue the requested certificate immediately or is not reachable
Recap: BRSKI supports synchronous enrollment

- Use of self-contained voucher (RFC 8366) to transport domain certificate signed by MASA
  - does not rely on transport security
  - can be leveraged for asynchronous provisioning of the voucher

- Use of online enrollment protocol (EST, RFC 7030)
  - Utilizes PKCS#10 for CSR and uses IDevID of pledge for authentication during TLS handshake.
  - Assumes enrollment authorization based on IDevID at the on-site RA/CA with authorization database.
BRSKI-AE provides enhancements for asynchronous enrollment

- Utilizes self-contained-object for certification request/response (CSR wrapping using existing certificate (IDevID)). Combines proof of possession and proof of identity
- Allows interaction with an off-site PKI
  - rely on on-site simple store-and-forward (optionally no Domain Registrar)
  - CSR authorization in conjunction with off-site asset management system
  - But requires certificate waiting indication
- Support of in-band and out-of-band certificate management throughout the device lifecycle
- Allows BRSKI application in domains that already selected (other) enrollment protocols.
Requirement coping of (selected) enrollment protocols with respect to the asynchronous enrollment

- **EST (RFC 7030)**
  - **Proof of possession:** using PKCS #10 structure in the request method.
  - **Proof of identity:** only for /fullcmc request. EST references RFC 5272 for fullcmc request. Signature of the SignedData of Full PKI Request calculated using the IDevID credential.
  - **Cert waiting indication:** a 202 return code should be returned by the Join Registrar. Note that depending on the TLS binding, PKCS #10 has to be re-generated if teared down.

- **CMP (RFC 4210)**
  - **Proof of possession:** provided by using either CRMF or PKCS#10 for certification request.
  - **Proof of identity:** can be provided by using the MSG_SIG_ALG to protect the certificate request message with signatures
  - **Cert waiting indication:** returned in the PKIStatus by the Join Registrar. Pledge retries using PollReqContent with a request identifier certReqId provided in initial CertRequest
Next Steps

• Further refinement of the approach
• Definition of an abstract self-contained approach ▶ YANG model, protocol agnostic
• Should allow support of existing enrollment protocols
• Allow domain registrar to support different enrollment protocol options

• Is the WG interested in this work?
Backup