BRSKI – Support for asynchronous enrollment

draft-fries-anima-brski-async-enroll-00

Steffen Fries, Hendrik Brockhaus, Elliot Lear

IETF 104 – ANIMA Working Group
Problem statement

• Some industrial scenarios are restricted regarding their online connectivity either technically or by policy. This limits the exchange of
  • voucher information with a MASA for domain trust establishment with pledge
  • certification request/response messages with a PKI for issuing an LDevID
• Other scenarios 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
• Use cases with 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 different enrolment mechanisms on the central side in parallel, while letting the pledge pick
BRSKI – Current support of asynchronous 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 supports asynchronous enrollment

• Utilizes self-contained-object for certification request/response (CSR wrapping using existing certificate (IDevID)).

• BRSKI-AE 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

• Support of in-band and out-of-band certificate management throughout the device lifecycle

• Allows BRSKI application in domains that already selected (other) certificate management approaches.

• May be combined with voucher exchange
Next Steps

• Enhancement of BRSKI with support of asynchronous certificate enrollment using self-contained objects
  • 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
• Support of coupling of voucher exchange and certificate enrollment (from transport protocol point of view) when target domain has no connection to the outside
  • Use case description / information processing for closed environments
  • Keep voucher and trust assumptions (Pledge, Domain Registrar, MASA), but allow for protocol independent transport
• Is the WG interested in this work?
Backup
Need for asynchronous enrollment (Examples)

• Rolling stock, railroad cars: sensors/actors/controller prepared to communicate locally (within the wagon), but not “aware” of backend connectivity (to PKI / asset management).

• Building automation: small or side building equipped with sensor, actuators, and controllers with limited or no connectivity to centralized building management system (Example: School)

• Substation automation: Control center, typically hosts PKI services, issues certificates for substations. Communication between the substation and control center done through a proxy/gateway/DMZ terminating the connection. Note that substation automation assumes central support SCEP/EST (IEC 62351)

• Electric vehicle infrastructure: communication limited to single protocol handling all information exchange with the backend (OCPP to carry CSRs); no second protocol allowed.