Update on BRSKI-AE:
Alternative Enrollment Protocols in BRSKI

draft-ietf-anima-brski-ae-03

Repo URL: https://github.com/anima-wg/anima-brski-ae

David von Oheimb (Ed.), Steffen Fries, Hendrik Brockhaus

IETF 115 – ANIMA Working Group
BRSKI-AE: abstract protocol overview

Pledge (caller)
- IDevID
- Manufacturer trust anchor

Domain Registrar, RA / LRA / enrollment proxy
- LDevID (Reg)
- IDevID Cert CA
- S/N Pledge

PKI RA
- PKI RA credentials

PKI CA
- PKI CA credentials

MASA
- MASA credentials

Initial steps:
Voucher request/response handling as in BRSKI

Adapted step:
Using alternative enrollment protocol (e.g., Lightweight CMP)

TLS with provisional accept of registrar certificate
Voucher-request {S/N, reg-cert, …}
Accept registrar certificate
Voucher {reg-cert, assertion, …}

Verification of LDevID cert
Certificate confirmation (opt.)
Certificate attributes (opt.)
Certification request (self-contained)
Certification response (LDevID cert)
PKI/Registrar conformation (opt.)
Enrollment-status

Full / partial / no processing of request
Any remaining verification of request and authorization

Device audit log

BRSKI-AE status
2022-Nov-10
David von Oheimb, Siemens
BRISKI-AE status: changes since IETF 114

Mostly in response to internal review, WG review, and document shepherd review.
Many editorial improvements, e.g., on
• comparison of BRISKI-AE to plain BRISKI
• differentiation of RA flavors (local RA vs. PKI RA in backend)
• description of offline vs. synchronous msg transfer

Clarifications on requirements:
• The registrar MUST support at least one certificate enrollment protocol that uses for certificate requests authenticated self-contained objects.
• For cert enrollment, messages between pledge and registrar the established TLS channel is used, which MUST be supported by the enrollment protocol.
• The cert enrollment protocol used between pledge and registrar MUST also be used for the upstream enrollment exchange with the PKI to retain the end-to-end POI/POP.
• During the cert enrollment phase, the registrar MAY handle requests by the pledge itself (as a local RA), otherwise MUST forward them to the responsible PKI and forward responses to the pledge.

Removed tentative instantiation to EST-fullCMC, changed role of Eliot Lear: co-author → contributor.
BRSKI-AE status: all open points resolved

• PoC implementation ✓
• Decision on removal of details on applying EST-fullCMC ✓
• WG review done by Michael Richardson ✓
• Document shepherd review done by Toerless Eckert ✓
• Ready for WGLC – ok?