Update on BRSKI-AE:
Alternative Enrollment Protocols in BRSKI

draft-ietf-anima-brski-ae-02


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

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

IETF 114 – ANIMA Working Group
BRSKI-AE: abstract protocol overview

Initial steps: Voucher request/response handling as in BRSKI

- 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

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

- Request CA certificates (opt.)
- CA certificates (opt.)
- Request certificate attributes (opt.)
- Certificate attributes (opt.)

- Certification request (self-contained)
- Certification response (LDevID cert)

Verification of LDevID cert

Full / partial / no processing of request

Any remaining verification of request and authorization

Device audit log

2022-July-08
David von Oheimb, Siemens
BRSKI-AE status: changes since IETF 113

• From draft async-enroll-05 to draft ae-01:
  • Renamed the repo and files from anima-brski-async-enroll to anima-brski-ae
  • Added graphics for abstract protocol overview as suggested by Toerless Eckert
  • Balanced (sub-)sections and their headers
  • Added details on CMP instance, now called BRSKI-CMP

• From draft ae-01 to draft ae-02:
  • Architecture: clarified registrar role including RA/LRA/enrollment proxy
  • CMP: added reference to CoAP Transport for CMPV2 and Constrained BRSKI

• PoC implementation done
BRSKI-AE status: open points

• Possibly add detail on applying EST with /fullCMC (→ Eliot Lear)
• Document shepherd review (→ Toerless Eckert)
• WG review appreciated
• Ready for WGLC?