Update on BRSKI-AE: Alternative Enrollment Protocols in BRSKI

draft-ietf-anima-brski-ae-04

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

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

IETF 116 – ANIMA Working Group
BRISKI-AE status: changes since IETF 115

SECDIR Early Review of draft version 03 by Barry Lea
- Clarified terminology
- Clarified normative requirements
- Enhanced security considerations with paragraph on additional use of TLS for CMP

Clarifications based on further internal reviews and suggestions
- Significant reduction of introduction and motivation to focus on proposed solution
- Pledge-registrar communication not restricted to TLS (may be DTLS for constrained BRISKI).
- Registrar must be in the loop regarding decision to grant LDevID.
- Clarify that BRISKI-AE replaces section 5.9 in RFC 8995, except enrollment status telemetry in section 5.9.4).
- If end-to-end authentication across the registrar to the PKI is required, the enrollment protocol used between pledge and registrar needs to be used also upstream (to the PKI).
- Remove former Appendix A: "Using EST for Certificate Enrollment“ and integrate relevant points into Section 1.1: "Supported Scenarios".
BRSKI-AE status: waiting for WGLC results

• Done already for IETF 115
  • IETF PoC implementation ✓
  • Decision on removal of details on applying EST-fullCMC ✓
  • WG review done by Michael Richardson ✓
  • Document shepherd review done by Toerless Eckert ✓
• SECDIR early review ✓
• WGLC ongoing
• Finalization of document, shepherd writeup
BRSKI-AE: abstract protocol overview

Pledge (caller)
- IDevID
- Manufacturer trust anchor
- Domain Registrar, RA / LRA / enrollment proxy
- Accept registrar certificate
- Voucher request (S/N, reg-cert, ...
- Voucher (reg-cert, assertion, ...
- Request CA certificates (opt.)
- CA certificates (opt.)
- Request certificate attributes (opt.)
- Certificate attributes (opt.)
- Certification request (self-contained)
- Certification response (LDevID cert)
- Certificate confirmation (opt.)
- PKI/Registrar confirmation (opt.)
- Enrollment-status

Domain Registrar, RA / LRA / enrollment proxy
- TLS with provisional accept of registrar certificate
- Voucher-request (S/N, reg-cert, ...
- Accept registrar certificate
- Voucher-status
- Request CA certificates (opt.)
- CA certificates (opt.)
- Request certificate attributes (opt.)
- Certificate attributes (opt.)
- Certification request (self-contained)
- Certification response (LDevID cert)
- Certificate confirmation (opt.)
- PKI/Registrar confirmation (opt.)
- Enrollment-status

PKI RA
- S/N verification
- Verification of pledge signature and IDevID (pledge)
- Voucher request (prior-signed-voucher, ...
- Voucher (reg-cert, assertion, ...
- Request CA certificates (opt.)
- CA certificates (opt.)
- Request certificate attributes (opt.)
- Certificate attributes (opt.)
- Certification request (self-contained)
- Certification response (LDevID cert)
- Certificate confirmation (opt.)
- PKI/Registrar confirmation (opt.)
- Enrollment-status

PKI CA
- PKI RA credentials
- PKI RA credentials
- PKI CA credentials
- PKI CA credentials
- PKI CA

MASA
- MASA credentials
- MASA credentials
- MASA credentials

Initial steps: Voucher request/respon handling as in BRSKI

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

Verification of LDevID cert

Full / partial / no processing of request

Any remaining verification of request and
authorization

Device audit log

BRSKI-AE status
2023-03
David von Oheimb, Siemens

David von Oheimb, Siemens