Update on BRSKI-AE: Alternative Enrollment Protocols in BRSKI

draft-ietf-anima-brski-ae-04

https://datatracker.ietf.org/doc/html/draft-ietf-anima-brski-ae

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

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

IETF 116 – ANIMA Working Group

BRSKI-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 BRSKI).
- Registrar must be in the loop regarding decision to grant LDevID.
- Clarify that BRSKI-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