Update on BRSKI-AE: Alternative Enrollment Protocols in BRSKI

draft-ietf-anima-brski-aе-12

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

David von Oheimb (ed.), Steffen Fries, Hendrik Brockhaus
Shepherd: Toerless Eckert

IETF 120 – ANIMA Working Group
BRSKI-AE status: recent activity

- AD review of version 10 by Mahesh Jethanandani: done on May 1st
- Handled COMMENTS and NITs
- Gen-ART review of version 11 by Meral Shirazipour: done on June 19th: ready w/nits
- Handled nits, resulting in version 12

**Changes** between versions 10 and 12:

- In response to AD review by Mahesh Jethanandani:
  - rearrange few paragraphs in abstract, introduction, and appendix
  - replace most occurrences of 'Note:' by 'Note that' or the like
  - convert some words to normative language, e.g., replacing 'may' by 'MAY'
  - change re-use of TLS channel by enrollment prot. from RECOMMENDED to MANDATORY
  - fix ambiguities and hard-to-read sentences by re-phrasing them
  - make wording more consistent, fix (mostly grammar) nits
- Fix nits spotted in Gen-ART review by Meral Shirazipour
BRSKI-AE status: waiting for AD Go-Ahead

- WGLC done ✓
- Yangdoctors review: ready ✓
- SECDIR Last Call Review: ready ✓
- shepherd writeup: done ✓
- AD review : done ✓
- Gen-ART Last Call review: ready w/nits ✓
- minor editorial fixups ✓
- IESG state: Waiting for AD Go-Ahead
- Next: IESG evaluation
Backup slide: BRSKI-AE abstract protocol overview

- **Pledge (caller)**
  - S/N verification
  - Verification of pledge signature and IDevID (pledge)

- **Domain Registrar, RA / LRA / enrollment proxy**
  - S/N verification
  - Verification of registrar certificate signature and IDevID (registration)

- **PKI RA**
  - Verification of LDevID cert
  - Certificate confirmation (opt.)

- **PKI CA**
  - PKI RA credentials
  - 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)

Verification of LDevID cert

Full / partial / no processing of request

Any remaining verification of request and authorization