Update on BRSKI-AE: Alternative Enrollment Protocols in BRSKI

draft-ietf-anima-brski-ae-06

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

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

IETF 118 – ANIMA Working Group
BRSKI-AE status: recent activity

- **WGLC ended** April 3rd; all comments and suggestions addressed before IETF 117
- Yangdoctors review updated on Aug 31st; result: **Ready**
- SECDIR Last Call Review completed on Nov 4th; status: **Ready**
- Only **one issue remaining to be closed**: [RFC 8995] not supporting discovering of registrars with enhanced feature sets, as in BRSKI-AE

**Alignment reached** in design team:
- A general problem, to be solved in a general way, such as by new draft: [BRSKI-Discovery]
- How to handle the absence of such a solution?
  - Simple approach chosen for CMP: use specific service name, e.g., "brski-registrar-cmp"

**Changelog** from version 05 to 06:
- Extend section on discovery according to discussion in the BRSKI design team
- Make explicit that MASA voucher status telemetry is as in BRSKI
- Add a note that on delegation, RA may need info on pledge authorization
BRSKI-AE status: waiting for outcome on BRSKI discovery

• Done already for IETF 115:
  • IETF PoC implementation ✓
  • WG review done by Michael Richardson ✓
  • Document shepherd review done by Toerless Eckert ✓
• Done already for IETF 116:
  • SECDIR early review ✓
• WGLC ended on April 3rd ✓
• document shepherd writeup ✓
• Yangdoctors review: ready ✓
• SECDIR Last Call Review: ready ✓
• TODO: finalize section on discovery of registrars with BRSKI-AE feature set
• Soon ready for AD review
Backup slide: 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)

**Verification of LDevID cert**

**Device audit log**

---

**BRSKI-AE status**

David von Oheimb, Siemens

2023-11