Update on BRSKI with Pledge in Responder Mode (BRSKI-PRM)

draft-ietf-anima-brski-prm-08
Repo URL: https://github.com/anima-wg/anima-brski-prm

Steffen Fries, Thomas Werner, Elliot Lear, Michael Richardson
Shepherd: Matthias Kovatsch

IETF 116 – ANIMA Working Group
BRISKI-PRM Status
History of main changes 05→ 06

– Issue #67, shortened the pledge endpoints to prepare for constraint deployments
– Included table for new registrar endpoints in section 5.3
– Addressed review comments from SECDIR early review (mainly editorial improvements)
– Addressed review comments from IOTDIR early review (Update of return codes in case of errors, terminology clarifications, consequent use of normative language, editorial improvements, update of references)
BR斯基-PRM Status
History of main changes 06 → 07 → 08

– WGLC resulted in a removal of the voucher enhancements completely from this document to RFC 8366bis, containing all enhancements and augmentations of the voucher, including the voucher-request as well as the tree diagrams

– Resolved editorial issues discovered after WGLC (still open issues remaining see next slide)

– Resolved comments from the Shepherd review as discussed in PR #85 on the ANIMA github (editorial, terminology alignments)
BRISKI-PRM
Open Issues collected after WGLC

– Discovery related issues
  – #79 discovery of registrar with BRISKI-PRM function set (DNS-SD subtypes vs. text parameters)
  – #80 pledge discovery using GRASP? → Alternative to be stated but out-of-scope for the draft

– Interaction Pledge and Registrar-agent (and Infrastructure)
  – #81 Additional text to motivate and explain usage of agent-signed data
  – #82 Enhance text explaining that IDevID cannot be used as TLS server certificate
  – #87 Available information on registrar-agent (serial number sufficient, avoid requirement for IDevID CA certificates)
  – #88 IDevID certificate chain in PVR (omitted to address constraint environments)
BRSKI-PRM Open
Issues collected after WGLC (cont.)

- Interaction Registrar-agent and Registrar
  - BRSKI-PRM assumes the registrar can distinguish LDevID (registrar-agent) vs. IDevID (pledge) also on existing endpoints → proposal to keep this handling
  - #84 use of registrar endpoints for responder vs. initiator mode
  - #86 pledge/registrar recognition based on credential
  - #91 PER processing (refer to handling as in BRSKI to sent PVR and PER over the same connection)
    - #83 Clarify re-enrollment support in BRSKI-PRM (current focus initial enrollment)
    - #92 Necessity for new registrar enrollment endpoint

- Voucher Request and Voucher
  - #89 Naming: agent-proximity vs. agent-invited (or similar)
  - #90 Concept of second signature on voucher
BRSKI-PRM Status
Next Steps

• Address open issues (see ANIMA git)
• Restructure section 5 and 6 for better readability and understanding

• Interop testing with others welcome 😊,
  PoC implementations of all components available, please get in touch

• Finalization of document, shepherd writeup
**Backup: BRSKI-PRM – Abstract Protocol Overview**

**Pledge (callee)**
- IDevID
- Manufacturer trust anchor

**Registrar-Agent**
- LDevID (RegAgt)
- LDevID Cert (Reg)
- S/N Pledge

**Domain Registrar RA**
- LDevID (Reg)
- LDevID Cert CA
- S/N Pledge

**Domain CA**
- Domain CA credentials

**MASA**
- MASA credentials

---

**Step 1:** Collect Bootstrapping request information from pledge

**Step 2:** Infrastructure Interaction based on BRSKI approach to collect voucher and LDevID Cert

**Step 3:** Provisioning of voucher, CA certs, and LDevID cert to pledge

---

**Device audit log**

**Voucher status**

**Enrollment status**

**First floor, connectivity to backend**

**Basement no connectivity to backend**