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

draft-ietf-anima-brski-prm-09

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

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

IETF 117 – ANIMA Working Group
BRSKI-PRM Status
History of main changes 08–09

- Addressed almost all issues from WGLC in March 2023. Most resulted in structural improvements, clarifications in the text and the figures and additional examples.

- Technical comments related to the following
  - Support of optional TLS protection of the communication link between registrar-agent and pledge (Section 4, Section 6.1, Annex B). This addresses several privacy related issues and also added in the Privacy and Security Considerations.
  - Included option that a separate HTTP connection may also be used to provide the PER (Section 6.2.6) to allow also for repeated/delayed enrollment attempts.
  - Shortened the utilized endpoint names to take constraint devices into account (example: /tpvr: Trigger pledge voucher-request creation).
BRISKI-PRM
Open Issues

- Discovery of registrar with an enhanced feature set
  - #79 discovery of registrar with BRISKI-PRM feature set
  - #80 pledge discovery using GRASP
- Discovery is discussed as common issue, which applies to BRISKI-PRM and BRISKI-AE
- Current approach uses DNS-SD TXT parameters and intends to define 3 key-value pairs, which can also be mapped to GRASP (topic of separate slot):
  - mode of operation (Registrar/Pledge as responder)
  - engaged enrollment protocol (EST, CMP, ...)
  - voucher format (CMS-signed JSON, JOSE-signed JSON, ...)
- Further clarification in the specification to avoid ambiguities
- Restructure section 5 and 6 for clarity based on Shepherd review
BRuki-PRM Status
Next Steps

- Clarify remaining open issues (see ANIMA git) in design team meetings

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

- Shepherd writeup
- Finalization of document
Backup: BRSKI-PRM – Abstract Protocol Overview

**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

---

**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

---

**Trigger Voucher-request**
- \{reg-cert, agent-signed-data\}

**Pledge-Voucher-Request (PVR)**
- \{S/N, reg-cert, agent-signed-data, ...\}

- S/N verification
- Verification "reg-cert" in voucher is own cert

**Trigger Enrollment-request**
- **Pledge-Enrollment-Request (PER)**
  - \{signature-wrapped CSR\}

**Voucher**
- \{LDevID(Reg), assertion, ...\}, signed

**Voucher-status**
- CA Certificates, signed

**Enrollment-status**
- Enrollment-response \{LDevID cert\}

---

**Device audit log**

---

**First floor, connectivity to backend**