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

draft-ietf-anima-brski-prm-04
Repo URL: https://github.com/anima-wg/anima-brski-prm

Steffen Fries, Thomas Werner, Elliot Lear, Michael Richardson

IETF 114 – ANIMA Working Group
BRISKI-PRM Status
History of main changes 02–03

Mostly editorial improvements based on review comments
- Updated examples to state "base64encodedvalue==" for x5c occurrences
- Include link to SVG graphic as general overview (was proposed last IETF 113)
- Restructuring of section 5 to flatten hierarchy
- Enhanced requirements and motivation in Section 4
BRSKI-PRM Status
History of main changes 03–04

Peer review done by Esko Dijk (issues #22–#61)

- Majority of issues targets to improve and clarify the current description to avoid ambiguities. Technical issues are also contained

- Added support for nonceless voucher, issue #18
  - Allows for provisioning of voucher via the sales channel

- Defined pledge-CAcerts endpoint and usage, issue #21
  - Handling of providing a wrapped CA certs response to the pledge in section Section 5.5.3; also added new required registrar endpoint (section Section 5.5.2 and IANA considerations) for the registrar to provide a wrapped CA certs response, issue #21

- PoP registrar certificate as mandatory, issues #32 and #49

- Added clarification that registrar-agent may collect PVR or PER or both in one run, issue #17
BRSKI-PRM Status

History of main changes 03–04 (cont.)

- SKID format clarified to be just the octets of the SKID, without any ASN.1 information
- Simplified YANG definition by augmenting the voucher request from RFC 8995 instead of redefining it.
- Added explanation for terminology "endpoint" used in this document, issue #16
- Removed join proxy in Figure 1 and added explanatory text, issue #20
BRSKI-PRM Status
Next Steps

• Currently 14 open issues, which will be addressed after IETF 114. All of them target improvement of the approach by clarifying handling/response codes/endpoints.

• Security consideration section to be updated

• PoC implementation finished

• Interop testing with others welcome

• Document shepherd needed

• After addressing the remaining open issues ready for WGLC
Backup
BRSKI-PRM – Abstract Protocol Overview

**Step 1: Collect Bootstrapping request information from pledge**
- Pledge (callee)
  - IDevID
  - Manufacturer trust anchor

**Step 2: Infrastructure Interaction based on BRISKI approach to collect voucher and LDevID Cert**
- Registr-Agent
  - LDevID (RegAgt)
  - LDevID Cert (Reg)
  - S/N Pledge

**Step 3: Provisioning of voucher and LDevID cert to pledge**
- Domain Registrar RA
  - LDevID (Reg)
  - IDevID Cert CA
  - S/N Pledge

- Domain CA
  - Domain CA credentials

- MASA
  - MASA credentials

---

- **Voucher-request**
  
- **Voucher**
  
- **Voucher-status**

- **Enrollment-request**

- **Enrollment-response**

- **Voucher-status**

- **Enrollment-status**

- **First floor, connectivity to backend**

- **Device audit log**

---

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

- "Voucher-request (prior-signed-voucher, _)
  Voucher {reg-cert, assertion, _}
  
  Voucher request
  
  Voucher-request (signature-wrapped CSR)"

- "S/N Pledge
  - Manufacturer trust anchor
  
  IDevID
  
  IDevID Cert CA
  
  LDevID Cert (Reg)
  
  LDevID (RegAgt)
  
  MASA credentials
  
  MASACredentials
  
  Domain CA credentials

- "Device audit log
  
  Voucher {reg-cert, assertion, _}, signed
  
  Enrollment-response (LDevID cert)
  
  Step 1: Collect Bootstrapping request information from pledge
  
  Step 2: Infrastructure Interaction based on BRSIKI approach to collect voucher and LDevID Cert
  
  Step 3: Provisioning of voucher and LDevID cert to pledge

- "Pledge (callee)
  
  Registr-Agent
  
  Domain Registrar RA
  
  Domain CA
  
  MASA"