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

draft-ietf-anima-brski-prm-14

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

Steffen Fries, Thomas Werner, Elliot Lear, Michael Richardson

Shepherd: Matthias Kovatsch

IETF 120 – ANIMA Working Group

BRSKI-PRM
History of main changes 12→ 13

- Interim ANIMA Meeting: Clarification of CDDL usage, when no YANG definition is available for objects to use the description consistently
- Update of Examples in Annex A (1 (PVR), 2 (RVR), 4 (Voucher)) to match definitions in draft
- Clarification included when pledge has no synchronized clock in Section 7.2.2 (use of advanced created-on time from the agent-signed-data in PER)
- Updated RVR to contain idevid-issuer as described in RFC 8995 in Section 7.3.2

BRSKI-PRM
History of main changes 13→ 14

- Part 3 of Shepherd Review by Matthias Kovatsch led to the following main changes
  - Structural improvements of the document, terminology, and simplification
  - New section 6.4 in the architecture overview to outline MASA requirements when supporting BRSKI-PRM similar to existing description for registrar and pledge
  - Section 7 restructured to describe protocol steps following a general approach: Overview, Request Artifact, Response Artifact (resulted in shifting existing text)
  - Alignment of pledge status response data across Section 7.6.2.1 (vStatus), Section 7.8.2.1 (eStatus), and Section 7.11.2.1 (pStatus) to allows similar processing.
  - Inclusion of new section on logging hints Section 8 to give recommendations on which events to be logged for auditing

Food for thoughts: Supporting .local name in IDevID

- BRSKI-PRM uses http and relies on self-contained authenticated objects for the communication between the registrar-agent and the pledge
- For privacy reasons TLS may be used for this link, making the pledge the TLS server.
- BRSKI-PRM states (Annex B): Pledge can use its IDevID certificate to authenticate itself, but pledge does not have a FQDN, and hence cannot be identified by DNS name. Instead, a new mechanism is required, which authenticates the X520SerialNumber DN attribute that must be present in every IDevID.
- As BRSKI-PRM uses mDNS to discover the pledge it may provide its local name to the registrar-agent. If IDevID contains the local name the registrar-agent can use this information during the authentication in the handshake without a new mechanism.
- Note: .local is not an FQDN; CABF does not allow internal names in the dNSName

Food for thoughts: Multiple LDevID Provisioning (not BRSKI-PRM specific)

- BRSKI and variants handle the provisioning of a generic LDevID, which can be used to manage further LDevIDs in the operational phase.
- There may be cases for providing multiple LDevIDs during onboarding like:
  - application specific certificates
  - Handle handovers from domain 1 to domain 2 during installation and commissioning
- Technically, this may be achieved once the generic LDevID is enrolled using CSR attribute request messages of the enrollment protocol (as defined in BRSKI) or trigger messages for the pledge (as defined in BRSKI-PRM)
- Operational workflow discussions may be necessary: Should be used to enhance ID Operational Considerations for BRSKI Registrar.

BRSKI-PRM
Status & Next Steps

- WGLC before IETF 116 - DONE
- IOT DIR early review - DONE
- SECDIR early review – DONE
- YANGDOCTORS early review – DONE
- Shepherd review and writeup – DONE

- Ready for AD review

- Further Interop testing with other parties welcome ☺,
  PoC implementations of all components available, please get in touch

Backup: BRSKI-PRM – Abstract Protocol Overview