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

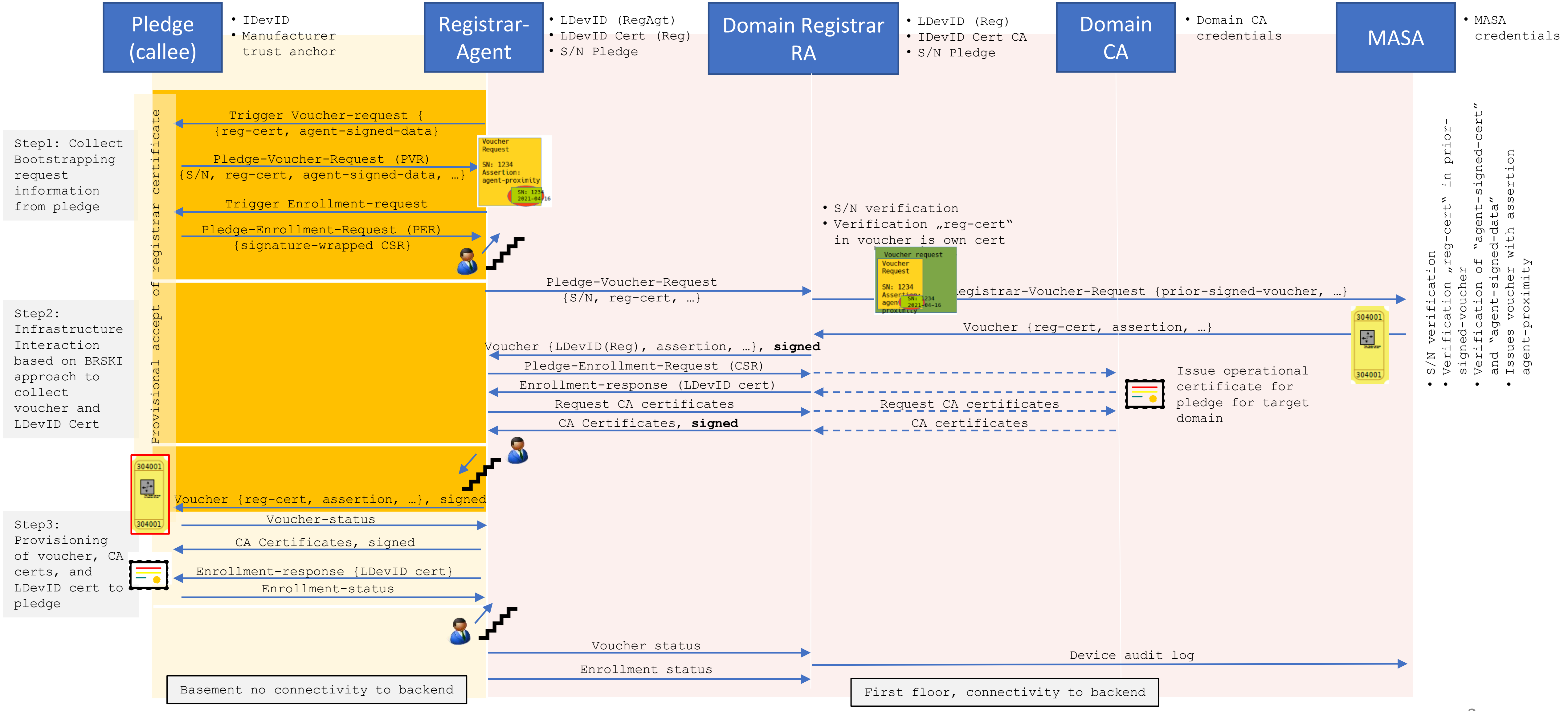
draft-ietf-anima-brski-prm-05

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

Steffen Fries, Thomas Werner, Elliot Lear, Michael Richardson

IETF 115 – ANIMA Working Group

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)
- IDevID Cert CA
- S/N Pledge

Domain CA
- Domain CA credentials

MASA
- MASA credentials

Provisional accept of registrar certificate

Step1: Collect Bootstrapping request information from pledge

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

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

Trigger Enrollment-request

Pledge-Enrollment-Request (PER)
{signature-wrapped CSR}

Step2: Infrastructure Interaction based on BRSKI approach to collect voucher and LDevID Cert

Pledge-Voucher-Request
{S/N, reg-cert, …}

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

Registrar-Voucher-Request {prior-signed-voucher, …}

Voucher {reg-cert, assertion, …}

Voucher {LDevID(Reg), assertion, …}, **signed**

Pledge-Enrollment-Request (CSR)

Enrollment-response (LDevID cert)

Request CA certificates

Request CA certificates

CA Certificates, **signed**

CA certificates

Issue operational certificate for pledge for target domain

- S/N verification
- Verification „reg-cert" in prior-signed-voucher
- Verification of "agent-signed-cert" and "agent-signed-data"
- Issues voucher with assertion agent-proximity

Step3: Provisioning of voucher, CA certs, and LDevID cert to pledge

Voucher {reg-cert, assertion, …}, signed

Voucher-status

CA Certificates, signed

Enrollment-response {LDevID cert}

Enrollment-status

Voucher status

Enrollment status

Device audit log

Basement no connectivity to backend

First floor, connectivity to backend

BRSKI-PRM Status
History of main changes 04→ 05

- Enhancements
  - Issues #32 and #49: Included registrar signature on voucher as mandatory. Provides PoP of registrars private key to pledge and ends provisional accept of the registrar certificate.
  - Issue #35: Defined new endpoint for pledge (bootstrapping) status inquiry. Allows registrar-agent to query status of pledge (results in factory-default, voucher-success/error, enroll-success/error, connect-success/error).
  - Issue #39 and #64: Enhanced error codes to allow a more fine grained error handling.
  - Issue #47 and #36: MASA verification of LDevID(RegAgt) to the same LDevID(Reg) domain CA to ensure registrar-agent and registrar are under the same administrative control. Domain CA cert needed on MASA to verify LDevID(RegAgt) and LDevID(Reg), to issue voucher with assertion "agent-proximity"
  - Issue #59: Enhanced security considerations and privacy considerations.
  - Issue #70: Registrar-Agent Certificate removed from pledge trigger (was optional) and only contained in RVR. Saves bandwidth and simplifies the handling (less options).

BRSKI-PRM Status
History of main changes 04→ 05

- Clarifications/Editorial improvements
  - Issue #27: Reworked terminology of "enrollment object", "certification object", "enrollment request object". → utilized rather short forms like PER, PVR, etc.
  - Issue #31: clarified that combined pledge may act as client/server for further (re)enrollment
  - Issue #42: clarified that registrar needs to verify the pledge status responses and ensure that they match the audit log response from the MASA, otherwise it needs drop the pledge and revoke the already issued certificate for the pledge.
  - Issue #43: clarified that the pledge shall use the created-on time from the PVR-trigger object if the time has not been synchronized, yet.
  - Issue #65: Removed reference to CAB Forum as not needed for BRSKI-PRM specifically.
  - Reworked all object representations (prototypes) to align with JSON encoding
  - Included examples for several objects in Appendix A (included size information. Issue #33)

BRSKI-PRM Status
Next Steps

- Clarification on YANG usage (together with other ANIMA documents)

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

- Document shepherd (still) needed

- Authors agree the document is ready for WGLC