# BRSKI with Pledge in Responder Mode (BRSKI-PRM)

draft-ietf-anima-brski-prm-02

Steffen Fries, Thomas Werner, Elliot Lear, Michael Richardson

IETF 113 – ANIMA Working Group

# BRSKI-PRM Status
# History of main changes 00→01

- Issue #11: New endpoint defined on registrar to enable delivery of wrapped enrollment request (in contrast to plain PKCS#10 in simpleenroll).
- Issue #8: Dropped additional signature on enrollment-response object by the registrar. Enrollment response will only contain the generic LDevID EE certificate.
- Issue #7: Dropped support for multiple CSRs during bootstrapping. Generic LDevID EE is expected to be used for further enrollment requests. Existing endpoints may be reused.
- Issue #5: Verification of YANG module ietf-ztp-types usage in draft via PoC
- Issue #4: Voucher assertion-type aligned with RFC8366bis

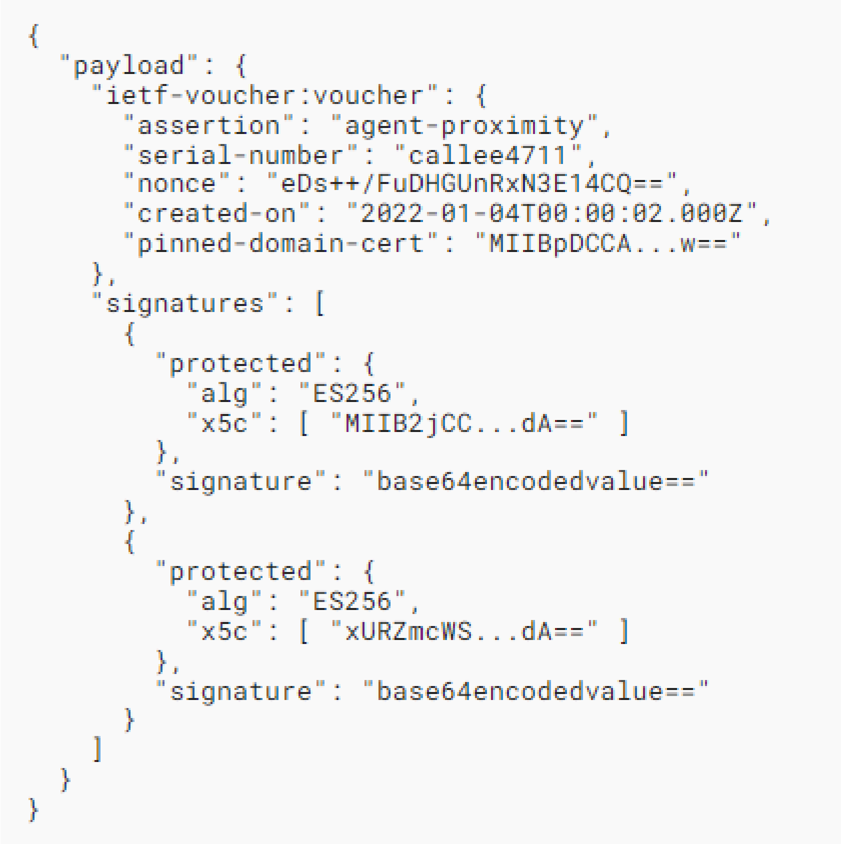
# BRSKI-PRM Status
# History of main changes 00→01 (cont.)

- Agent-sign-cert converted to an array to allow for certificate chain when LDevID (RegAgt) certificate is issued by a different CA than LDevID (Reg) certificate
  (changes in voucher enhancement and handling description)
- Authorization check of registrar-agent at registrar during TLS and during pledge-voucher-request processing (based on agent-signed-data) more elaborately described
- Limitation section added if pledge is in power save mode
- Housekeeping: Enhance draft with examples of trigger messages for pledge-voucher-request and enrollment-request. Editorial changes.

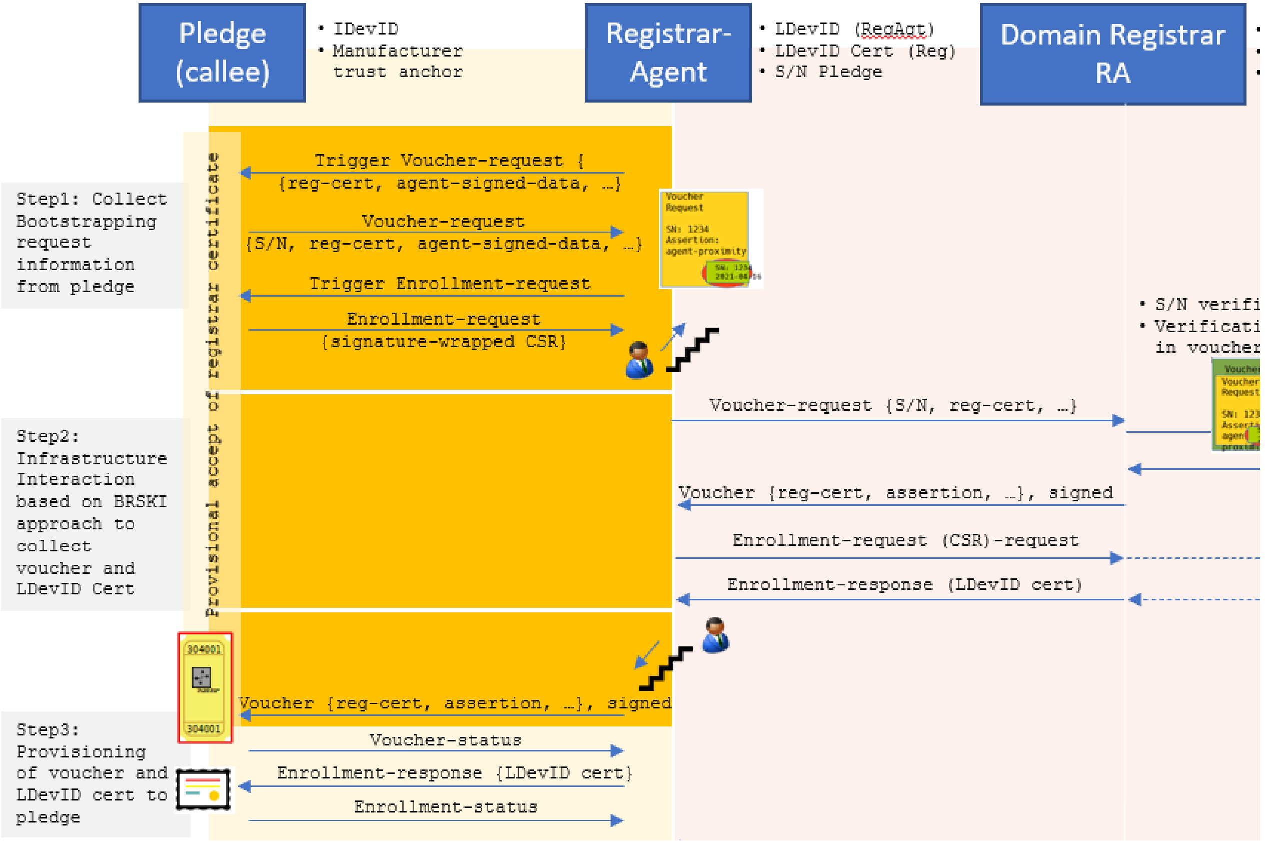
# BRSKI-PRM Status
# History of changes 01→02

- Issue #15: Included option and handling for additional signature of voucher to support verification of POP of the registrars private key → supports provisional accept
- Included representation of objects in General JWS JSON Serialization
- Included error responses from pledge if it is not able to create a pledge-voucher request or an enrollment request
- Issue 7+8+14: Resolved open issue regarding handling of multiple CSRs and enrollment responses during the bootstrapping:
  - Initial target is provisioning of generic LDevID certificate.
  - Defined endpoints on the pledge may also be used for management of further certificates.

# BRSKI-PRM Status
# Multiple signatures on voucher response



```
{
  "payload": {
    "ietf-voucher:voucher": {
      "assertion": "agent-proximity",
      "serial-number": "callee4711",
      "nonce": "eDs++/FuDHGUnRxN3E14CQ==",
      "created-on": "2022-01-04T00:00:02.000Z",
      "pinned-domain-cert": "MIIBpDCCA...w=="
    },
    "signatures": [
      {
        "protected": {
          "alg": "ES256",
          "x5c": [ "MIIB2jCC...dA==" ]
        },
        "signature": "base64encodedvalue=="
      },
      {
        "protected": {
          "alg": "ES256",
          "x5c": [ "xURZmcWS...dA==" ]
        },
        "signature": "base64encodedvalue=="
      }
    ]
  }
}
```



Pledge (callee)

- IDevID
- Manufacturer trust anchor

Registrar-Agent

- LDevID (RegAgt)
- LDevID Cert (Reg)
- S/N Pledge

Domain Registrar RA

Provisional accept of registrar certificate

Step1: Collect Bootstrapping request information from pledge

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

Voucher-request {S/N, reg-cert, agent-signed-data, …}

Trigger Enrollment-request

Enrollment-request {signature-wrapped CSR}

- S/N verifi
- Verificati in voucher

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

Voucher-request {S/N, reg-cert, …}

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

Enrollment-request (CSR)-request

Enrollment-response (LDevID cert)

Step3: Provisioning of voucher and LDevID cert to pledge

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

Voucher-status

Enrollment-response {LDevID cert}

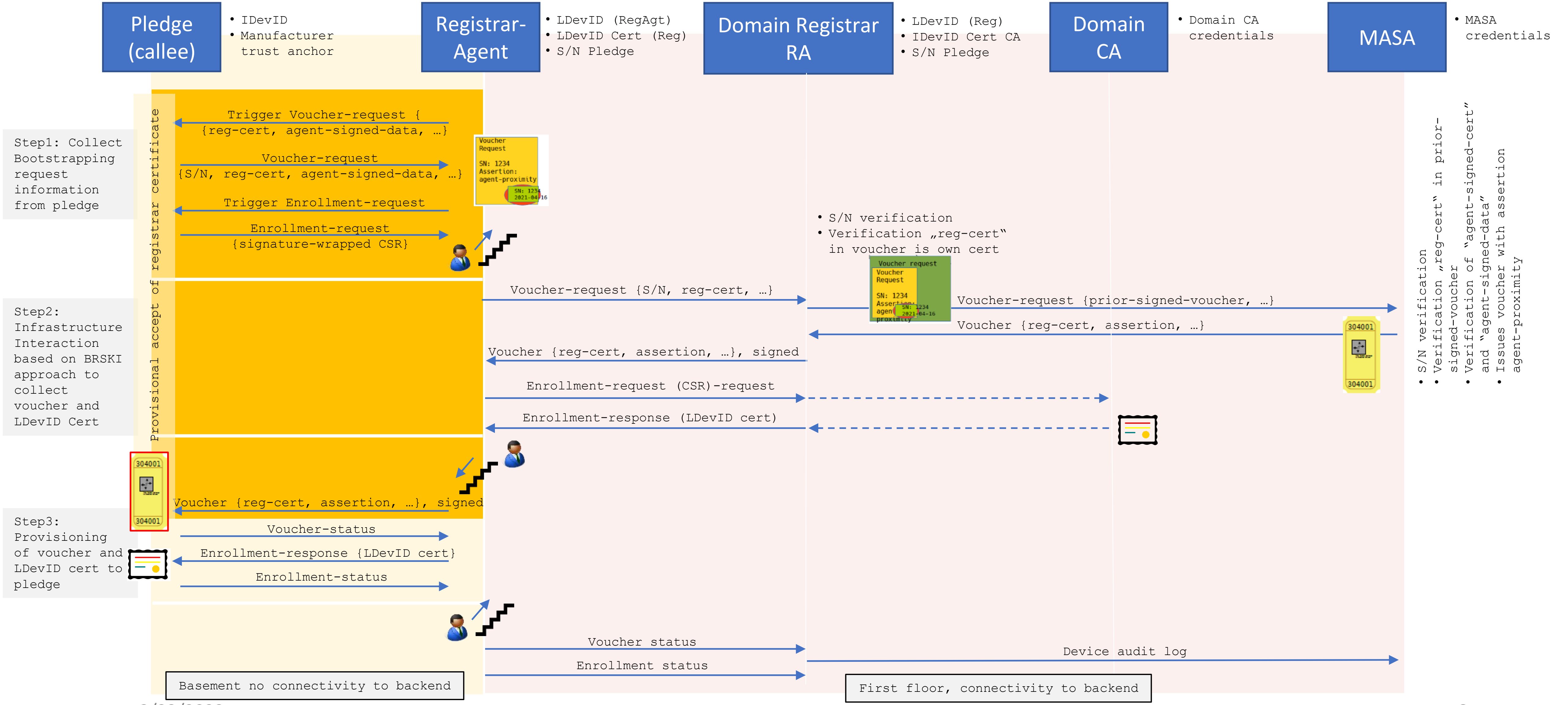
Enrollment-status

# BRSKI-PRM Status
# Next Steps

- Currently no open issues
- Security consideration section to be updated
- PoC implementation ongoing
- Peer review volunteers appreciated
- WG review requested

# 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)
- 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, …}

Voucher-request {S/N, reg-cert, agent-signed-data, …}

Trigger Enrollment-request

Enrollment-request {signature-wrapped CSR}

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

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

Voucher-request {S/N, reg-cert, …}

Voucher-request {prior-signed-voucher, …}

Voucher {reg-cert, assertion, …}

- 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

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

Enrollment-request (CSR)-request

Enrollment-response (LDevID cert)

Step3: Provisioning of voucher and LDevID cert to pledge

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

Voucher-status

Enrollment-response {LDevID cert}

Enrollment-status

Voucher status

Enrollment status

Device audit log

Basement no connectivity to backend

First floor, connectivity to backend