Update on BRSDKI-AE — Support for asynchronous enrollment

draft-ietf-anima-brski-sync-enroll-04
Steffen Fries, Hendrik Brockhaus, Elliot Lear, David von Oheimb

BRSDKI with Pledge in Responder Mode (BRSDKI-PRM)

draft-ietf-anima-brski-prm-00
Steffen Fries, Thomas Werner, Elliot Lear, Michael Richardson

Steffen Fries

IETF 112 – ANIMA Working Group
Discussion on draft split

- Original BRSKI-AE discussed two use cases, which have evolved into different directions
- Discussion (ANIMA Design Teamm, mailing list) to split the draft along the two use cases
- UC1 stays as "Support of Asynchronous Enrollment in BRSKI (BRSKI-AE)" covering the application of alternative enrollment protocols. It will cover the description of utilizing other enrollment protocol than EST /simpleenroll in general and using Lightweight CMP specifically. Focus is the interaction between pledge and registrar.
- UC2 became "BRSKI with Pledge in Responder Mode (BRSKI- PRM)", and addresses the communication between the pledge and the registrar by reversing the initiator and responder role (compared to RFC 8995) introducing a registrar-agent component to facilitate the communication.
BR斯基-AE Status
History of changes

• From version 02 to version 03
  • Housekeeping, deleted open issue regarding YANG voucher-request in UC2 as ietf-voucher-request was enhanced with additional leaf.
  • Included open issues of Voucher YANG model in UC2 regarding assertion value agent-proximity and CSR encapsulation using SZTP sub module.

• From version 03 to version 04
  • Moved UC2 related parts defining pledge in responder mode to BR斯基-PRM (#19).
  • Updated references to the Lightweight CMP Profile.
  • Change of authors: Added David von Oheimb as co-author. Thomas Werner left.
BRSKI-AE

Next Steps

• Clarification of open issues stated in the draft (currently no open issues on ANIMA git)
• Further update general description using alternative enrollment protocols and the concrete examples
  • Lightweight CMP Profile
  • EST with /fullCMC
• Updates will be circulated
• WG review appreciated
• PoC implementation ongoing → Interest from others welcome for interop testing
BRSKI-PRM Status
History of changes from BRSKI-AE-03 to BRSKI-PRM-00

• Moved UC2 defining pledge in responder mode from BRSKI-AE-03 to BRSKI-PRM-00.

• Yang doctor early review addressed (ietf-voucher-request enhancements (Section 6, Security Considerations Section).

• Aligned naming of ietf-voucher-request-xxx with other ANIMA drafts (#20).

• Utilized ietf-voucher-request-prm in voucher exchanges (to use enhancements for agent-signed-data).

• Included changes from draft-ietf-netconf-sztp-csr-06 regarding the YANG definition of csr-types into the enrollment request exchange.
BRSKI-PRM Status
Next Steps

• Further rework the draft (structure and application examples)
• Clarification of open issues stated in ANIMA git and also in the draft
  • Verification of usage of ietf-ztp-types to convey PKCS#10 in BRSKI-PRM enrollment request (#5)
  • Option to generate multiple CSRs (domain specific, application specific) (#7)
  • Signature on enrollment response object? Protection of additional data contained or identification of registrar providing the certificate (audit) (#8)
• Circulate outcome on the mailing list for further discussion
• WG review appreciated
• PoC implementation ongoing → Interest from others welcome for interop testing
Backup
BRSKI-AE
Abstract Protocol Overview

Step 1: Voucher request/response handling as in BRSKI

Voucher-request {S/N, reg-cert, ...}

Voucher-status

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

Voucher {reg-cert, assertion, ...}

Voucher {reg-cert, assertion, ...}

Step 2: Application of alternative enrollment protocol, (e.g. Lightweight-CMP)

Request CA certificates (opt.)
CA certificates (opt.)
Request certificate attributes (opt.)
Certificate attributes (opt.)

Certification-request

Certification-response (LDevID Cert)

Verification of LDevID Cert

Enrollment-status

Voucher-request {S/N, reg-cert, ...}

Voucher {reg-cert, assertion, ...}

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

Voucher {reg-cert, assertion, ...}
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 and LDevID Cert to pledge

First floor, connectivity to backend