Update on BRSKI-AE:
Alternative Enrollment Protocols in BRSKI

draft-ietf-anima-brski-async-enroll-05

Repo so far: https://github.com/anima-wg/anima-brski-async-enroll
Proposed new repo URL: https://github.com/anima-wg/anima-brski-ae

David von Oheimb, Steffen Fries, Hendrik Brockhaus, Eliot Lear
David von Oheimb (Ed.)

IETF 113 – ANIMA Working Group
BRSKI-AE: abstract protocol overview

**Initial steps**: Voucher request/response handling as in BRSKI

**Adapted step**: Application of alternative enrollment protocol (e.g., Lightweight CMP)

**BRSKI-AE status**

2022-March-25

David von Oheimb, Siemens
BRSKI-AE status: recent changes

From draft version 04 to version 05:

• After the split with BRSKI-PRM, David von Oheimb became the editor.
• Shifted the emphasis towards supporting alternative enrollment protocols.
• Updated the title accordingly - preliminary change to be approved.
• Moved comments on EST and detailed application examples to informative annex.
• Moved the remaining text of section 3 as two new sub-sections of section 1.
• Streamlined wording, consolidated terminology, improved grammar, etc.
BRSKI-AE status: next steps

• Clarification of open issues stated in the draft (currently no open issues on the ANIMA git):
  • Application of Lightweight CMP Profile: some details to be clarified/defined
    • Whether to use /getcacerts or the caPubs and extraCerts fields when further to-be-trusted (root CA) certificates and possibly other CA certs are needed
    • Whether to use /getcertreqtemplate or let the registrar modify the CRMF and use raVerified
    • Specify the optional use of implicitConfirm as alternative to certConf
    • Whether to specify the use of /p10
  • Application of EST with /fullCMC
  • Further updates pending to fix the above and potential further issues
• WG review appreciated
• PoC implementation ongoing; please email us if you are interested in interop testing