Update on BRSKI-AE: Alternative Enrollment Protocols in BRSKI

draft-ietf-anima-brski-ae-03

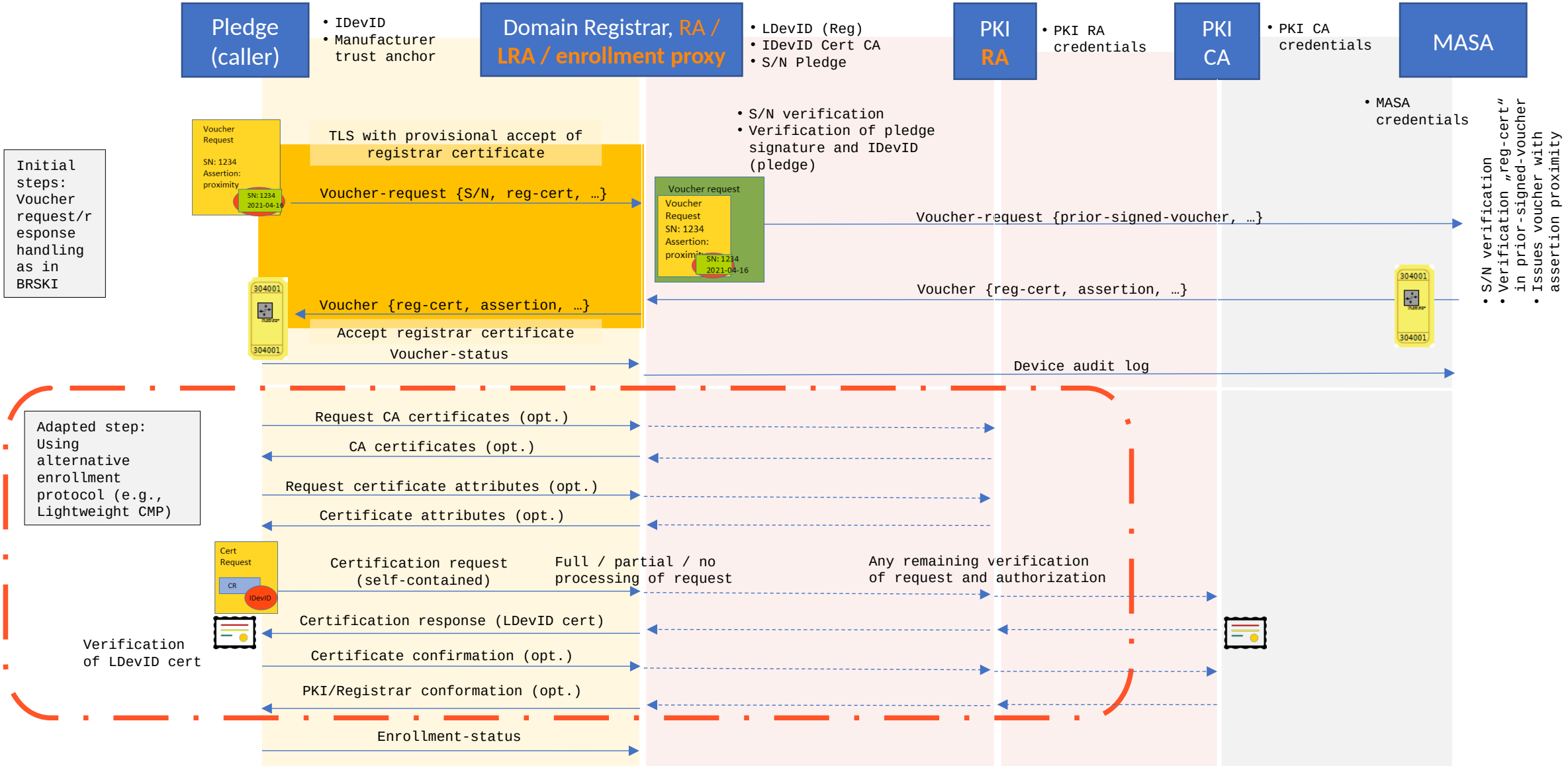
https://datatracker.ietf.org/doc/html/draft-ietf-anima-brski-ae

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

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

IETF 115 – ANIMA Working Group

BRSKI-AE: abstract protocol overview



BRSKI-AE status: changes since IETF 114

Mostly in response to internal review, WG review, and document shepherd review.
Many editorial improvements, e.g., on

- comparison of BRSKI-AE to plain BRSKI
- differentiation of RA flavors (local RA vs. PKI RA in backend)
- description of offline vs. synchronous msg transfer

Clarifications on requirements:

- The registrar MUST support at least one certificate enrollment protocol that uses for certificate requests authenticated self-contained objects.
- For cert enrollment, messages between pledge and registrar the established TLS channel is used, which MUST be supported by the enrollment protocol.
- The cert enrollment protocol used between pledge and registrar MUST also be used for the upstream enrollment exchange with the PKI to retain the end-to-end POI/POP.
- During the cert enrollment phase, the registrar MAY handle requests by the pledge itself (as a local RA), otherwise MUST forward them to the responsible PKI and forward responses to the pledge.

Removed tentative instantiation to EST-fullCMC, changed role of Eliot Lear: co-author → contributor.

BRSKI-AE status: all open points resolved

- PoC implementation ✓
- Decision on removal of details on applying EST-fullCMC ✓
- WG review done by Michael Richardson ✓
- Document shepherd review done by Toerless Eckert ✓
- Ready for WGLC – ok?