Lightweight Authorization for EDHOC

draft-selandер-lake-authz-03

Göran Selander, John Preuß Mattsson, Ericsson
Michael Richardson, SSW
Mališa Vučinić, INRIA
Aurelio Schellenbaum, ZHAW

IETF 117, LAKE WG, July 24, 2023

Photo by Christian Werther on Unsplash
The Device (U) wants to enroll into a domain over a constrained link. The Device and Domain Authenticator (V) mutually authenticate and authorize each other. The procedure is assisted by an Enrollment Server (W) located in a non-constrained network. Change name from “Authorization Server” to disambiguate with ACE. Maps to BRSKI MASA.
Core Protocol Overview

- U and V authenticates using EDHOC
- Authorization related information passed U → V → W → V → U
  - Between U and V in EAD fields of EDHOC (Voucher Info/Voucher)
  - Between V and W in REST exchange (Voucher Request/Voucher Response)

NOTE: Voucher much smaller than RFC 8366
State of -03

— Updated core protocol
  — Separated V ⇔ W security establishment, and proof-of-possession w.r.t. CRED_V
    — Not needed for every U ⇔ V connection
    — Allows reuse of EDHOC for PoP
  — Simplified protocol
    — Essentially forwarding of message_1 and Voucher
    — Enabled stateless operation of V during VREQ/VRES exchange

— Detailed REST interface at W
  — https/coaps/coap with OSCORE
  — Media type registration

— Aligned with edhoc-20
Core Protocol

Before VREQ/VRES:
- Secure channel between V and W
- V proves to W the possession of CRED_V private key

- LOC_W = URI or domain of W
- ENC_ID = Device ID encrypted for W

- U verifies Voucher
- ID_CRED_I in message_3 may reference CRED_U

After message_3: V looks up CRED_U (optional)
Next steps

— Appendix on scaling considerations for V
— Implementation and interop testing

— Next step
   — Review
   — Ready for adoption?