

DTLS profile for ACE

draft-ietf-ace-dtls-authorize-07

Ludwig Seitz (ludwig.seitz@ri.se)

IETF 104 ACE WG meeting
March 29, 2019

Framework updates from 05 to 08

- 4.01 UNAUTHORIZED → non-fatal DTLS error
 - Update access token without redoing handshake
- “kid” in AS Request Creation Hints → framework
 - Generic enough to be useful for other profiles
- Example with `cnf == kid`
 - Derivation of pop-key
- Adjusted the use of normative words
- Added examples for each protocol step
- Added section about secure communication with AS

Next Steps

- Ready?