Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE)

draft-ietf-ace-dtls-authorize-02

S. Gerdes, O. Bergmann, C. Bormann, **G. Selander**, L. Seitz

IETF100, 2017-11-14, Singapore

Changes Since IETF-99

- WG document sources now at `https://github.com/ace-wg/ace-dtls-profile`
- new text to close issues as discussed during IETF99
- addressed issues raised in review from Hannes
- small editorial changes
- Implementation status (cf. ACE Wiki)
  - SICS
  - jimsch
  - planned: TZI

Issue #10

(a) authz-info vs. (b) psk_identity "shortcut"

- **(a)** is mandatory
- Client needs external knowledge for (b) or just tries

One or Two Profiles?

Open Question: Are PSK and RPK two different profiles or two modes of the same profile?

- Small editorial change required (see -02)
- Do we need explicit signaling?
  - e.g.: `coap_dtls_rpk` and `coap_dtls_psk`
  - could do without (AS-to-Client response contains sufficient hints)

Thoughts from WG?

Issue #14

Multiple options in `psk_identity`

- Changed text to use kid in the first place
  optionally try to process `psk_identity` as access token

Thoughts from the WG?

Next Steps

- Issue #13
  - Mandatory curves for RPK mode?
  - proposal: use Ed25519
- Upcoming version -03: use binary data in `psk_identity`
- Examples
- Need more reviews
- What else do you think is missing?