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

draft-ietf-ace-dtls-authorize-01

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

IETF99, 2017-07-17, Prague

Changes Since IETF-98

- re-submitted as WG document
  - sources and bug tracker still live at `https://github.com/obgm/ace-dtls-profile`
- received review from Jim Schaad
  - small editorial changes in version `-01`
  - many clarifications needed
  - move parts into framework document?
- (from IETF-98): change title to "Transport Layer Security (TLS) Profile ..."?

Open Issue #10

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

- how does C know which methods are supported by RS?
- ACE framework has (a) only
- does this imply that (a) is mandatory?
- options for handling case (b)
  - **b.1:** rely on external knowledge
  - **b.2:** trial-and-error
  - **b.3:** disallow

Open Issue #11

When is a request unauthorized?

- current text may be too restrictive (cf. `.well-known/core`):

  `...received on an unprotected channel and RS has no valid access token...`

- Proposal: change introductory text to limit to protected resources only

Open Issue #12

What to do when the last valid token has expired?

"no valid access token" covers three cases:

1. expired access token,
2. no token (but required for protected resource), and
3. rogue token.

- Tear down DTLS session (= `MUST`)?
  - pro: clear state early
  - con: reversing roles?

Open Issue #13

Mandatory curves for RPK mode?

1. Do we want to make a curve mandatory-to-implement?
2. If so, which?

Open Issue #14

Multiple options in `psk_identity`

- text allows three different things:

1. key identifier
2. access token with encrypted key
3. access token and key derivation info

- Code complexity for option (2) and (3)?

Open Issue #15

Permission update in existing session

1. The text should distinguish between cases where the permissions are updated vs where the key is updated.
2. Permission update `SHOULD NOT` require a new session to be established.

Open Issue #16

Section 5.1:

- C receives AS_Info that points to some AS
- C needs to have security relationship with that AS *a priori*
- otherwise, ignore the respective hint

Additional proposal:

- copy AS from AS_Info into Client-to-AS request

Framework Document (1/2)

Discovery

- AS discovery will be moved to framework document (also take link descriptions and AS_Info CDDL from DCAF proposal?)
- AS_Info has nonce to ensure freshness where RS and AS have no synchronized clocks.
  - Proposal: extend Client-to-AS request

RPK in Client-to-AS Request

- Scenario: C requests AT with RPK in `cnf` over DTLS w/ RPK
  - AT in AS-to-Client response is bound to RPK from cnf
  - **who is authorized**?

Framework Document (2/2)

Error Handling

- Return AS_Info for all error types? (cf. Issue #9)

AS_Info fields

- Allow more information in AS_Info messages over secured channels