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

draft-ietf-ace-dtls-authorize-05

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

IETF103, 2018-11-08, Bangkok
Current Status (Version -05)

https://github.com/ace-wg/ace-dtls-profile

Since version -03:

▷ improved readability
▷ example cleanup
▷ clarify usage of COSE structures

Received one review (Jim Schaad) during WGLC.
1. Symmetric keys generated by AS need a kid for dynamic updates.
   - **Proposal:** AS SHOULD add a kid.

Related question:

a. Do we need special treatment of kids for RPKs?
   - Are there implicit assumptions about RPKs I am missing?
2. AS-to-Client response: Semantics of the symmetric key (Fig. 4)
Problem: C receives this:

    cnf : {
        COSE_Key : {
            kty: symmetric,
            kid: h'...',
            k : h'12...'
        }
    }

Now, how does C know if \(k\) is supposed to be...

...a pre-shared secret for AES-128? For AES-256? For...?

Question: Does it matter (as long as it is “good enough” for RS)?

> **Proposal:** Ignore and call this a “shared secret” instead of a key.
3. Clarify that RS should not terminate the DTLS session for simple authorization errors.

▶ **Proposal:** Say that RS should treat these as non-fatal, and keep the session until the access token has expired.
4. New cnf contents for key derivation.

**Goal:** Convey alg and salt for HKDF in AS-to-Client response and access token.

**Problem:** Cannot do this in COSE_Key structure because parameters describe a *different* key, i.e., the C—RS session key.

**Proposal:** Use kty, alg, salt without COSE_Key:

```plaintext
cnf : {
  kty   : symmetric,
  alg   : HKDF-SHA-256,
  salt  : h'eIiOFCa91Obw'
}
```