IPsec profile of ACE

draft-aragon-ace-ipsec-profile-01

Santiago Aragón, RISE SICS
Marco Tiloca, RISE SICS
Shahid Raza, RISE SICS

IETF 100, ACE WG, Singapore, November 14th, 2017

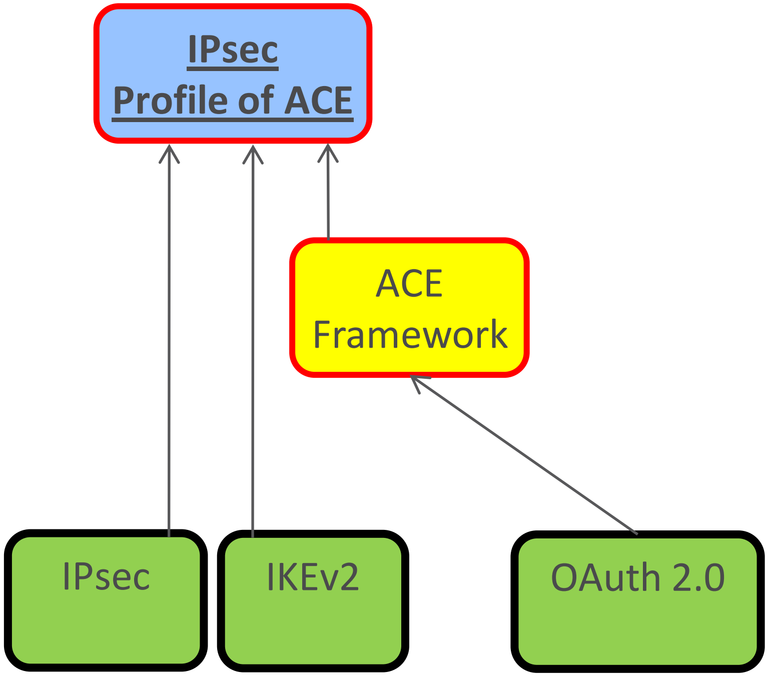
Motivation

- Enable IPsec-based communication in ACE
  - Set up of IPsec Security Association (SA) pairs
  - Message confidentiality/integrity/authentication at the IP layer
  - Message replay protection
  - Prevent IP spoofing

- Leverage IPsec independence from Key Management Protocols
  - Pre-established SA pair
  - IKEv2 (symmetric or asymmetric mode)

- Agnostic to the application layer

Related Work



IPsec Profile of ACE

ACE Framework

IPsec

IKEv2

OAuth 2.0

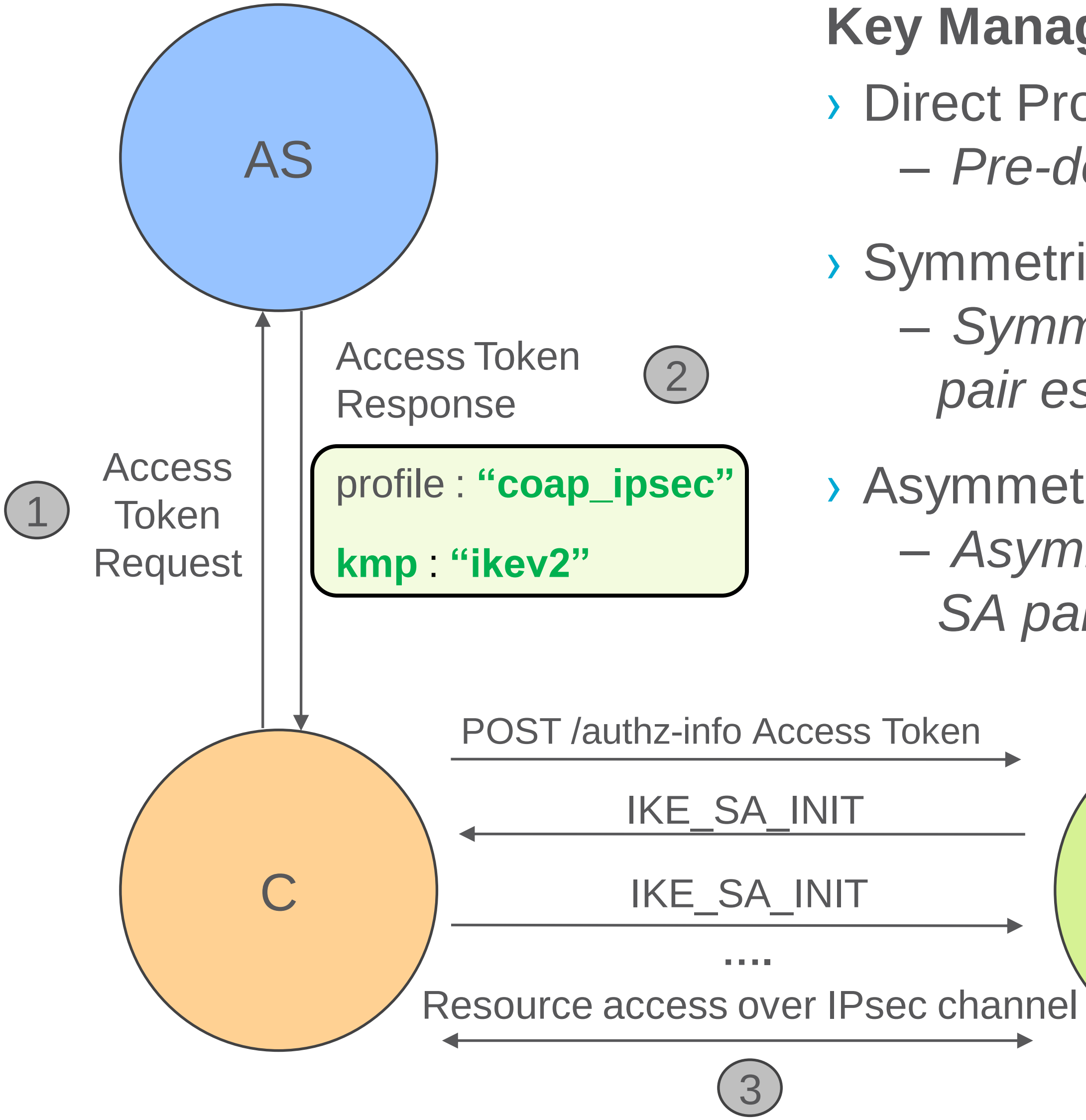
□ *= ACE WG*

🟦 *= Individual submission*

🟨 *= Adopted by an IETF WG*

🟩 *= RFC*

Profile description



Key Management Methods:

- Direct Provisioning
  - *Pre-defined SA pair issued by the AS*
- Symmetric Key-Based
  - *Symmetric key to authenticate the SA pair establishment, e.g. IKEV2*
- Asymmetric Key-Based
  - *Asymmetric key to authenticate the SA pair establishment, e.g. IKEV2*

Updates

- Draft (editorial) updates
  - It is OPTIONAL to use IPsec to secure communications with AS, either through pre-established SA or IKEv2-based establishment.
  - Other means MAY be used as alternative (e.g. DTLS, OSCORE)
  - Alternative key establishment is now purely informative.
  - Alignment to updated framework and other profiles.

- RISE SICS implementation
  - Available for the Contiki OS [1]
  - Support for Direct Provisioning of Security Associations
  - Support for symmetric/asymmetric key-based establishment (IKEv2)
  - Tested on the Zolertia Firefly motes
  - Working on experimental results for a paper

- Reviews are welcome

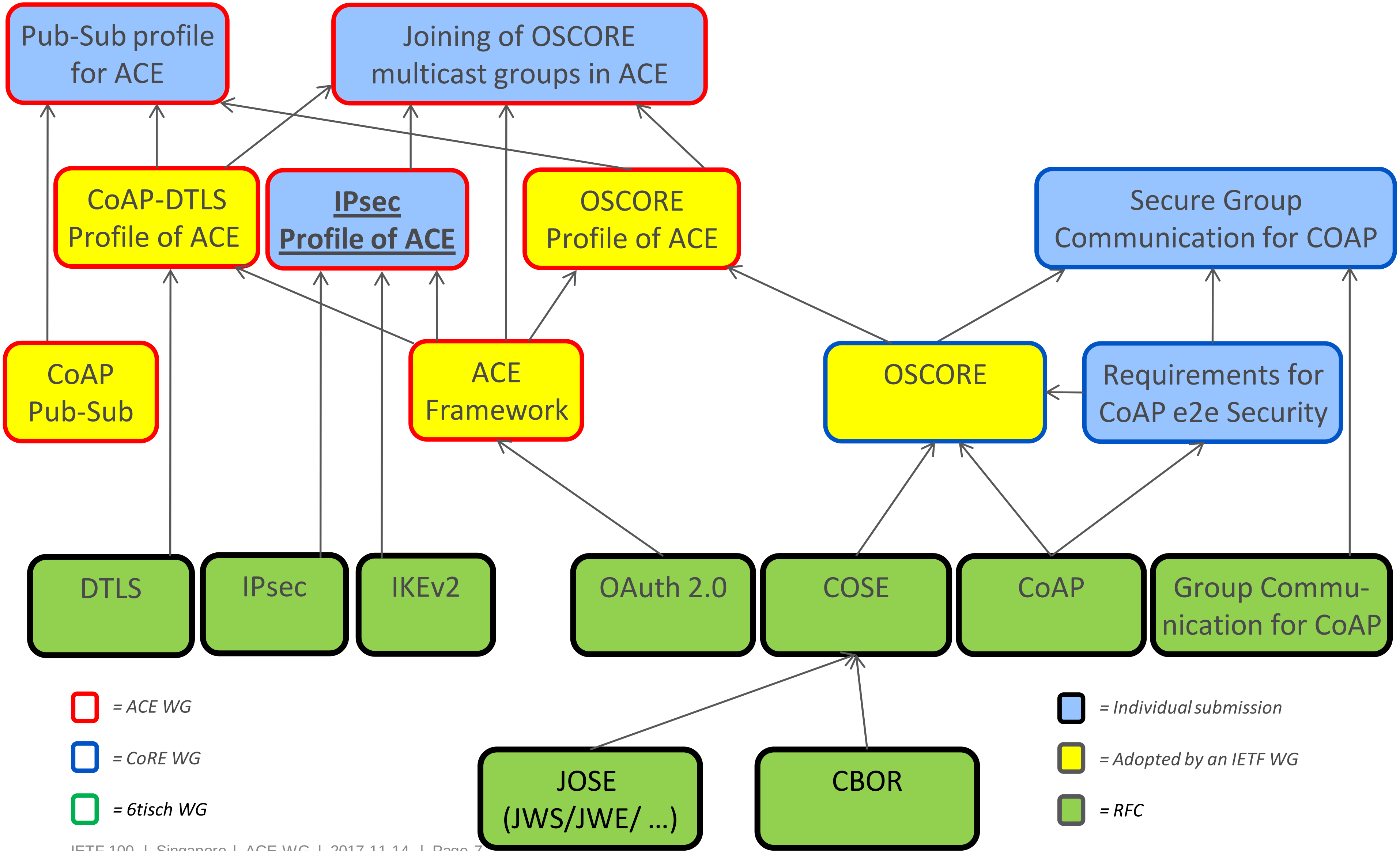
[1] https://gitlab.com/ace-ipsec-profile/internet-draft/tree/master/contiki_zoul_ipsec/examples/ace-token-ike

Thank you!

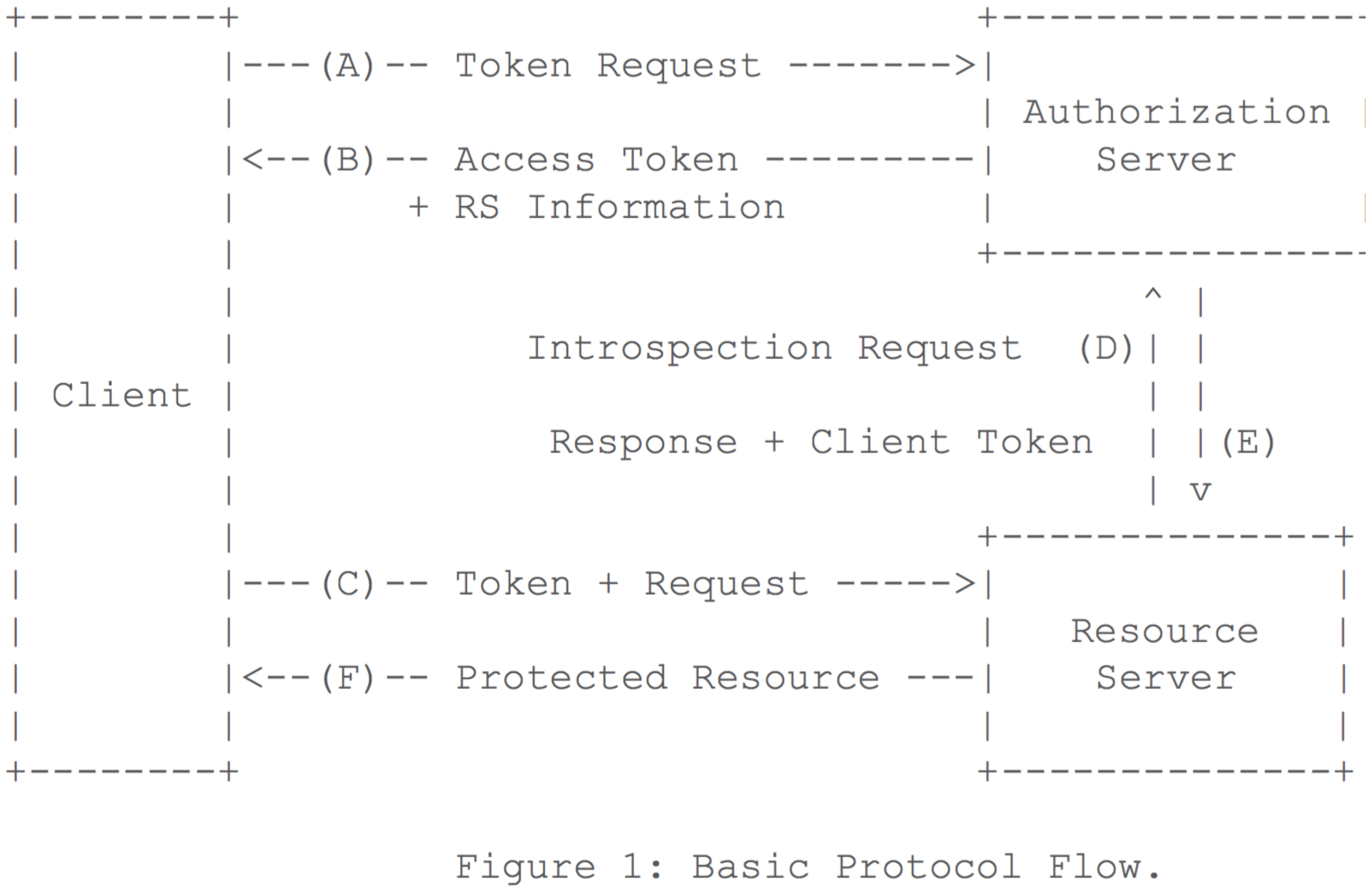
Comments/questions?

https://gitlab.com/ace-ipsec-profile/internet-draft

Related Work



ACE Framework
(draft-ietf-ace-oauth-authz-08)



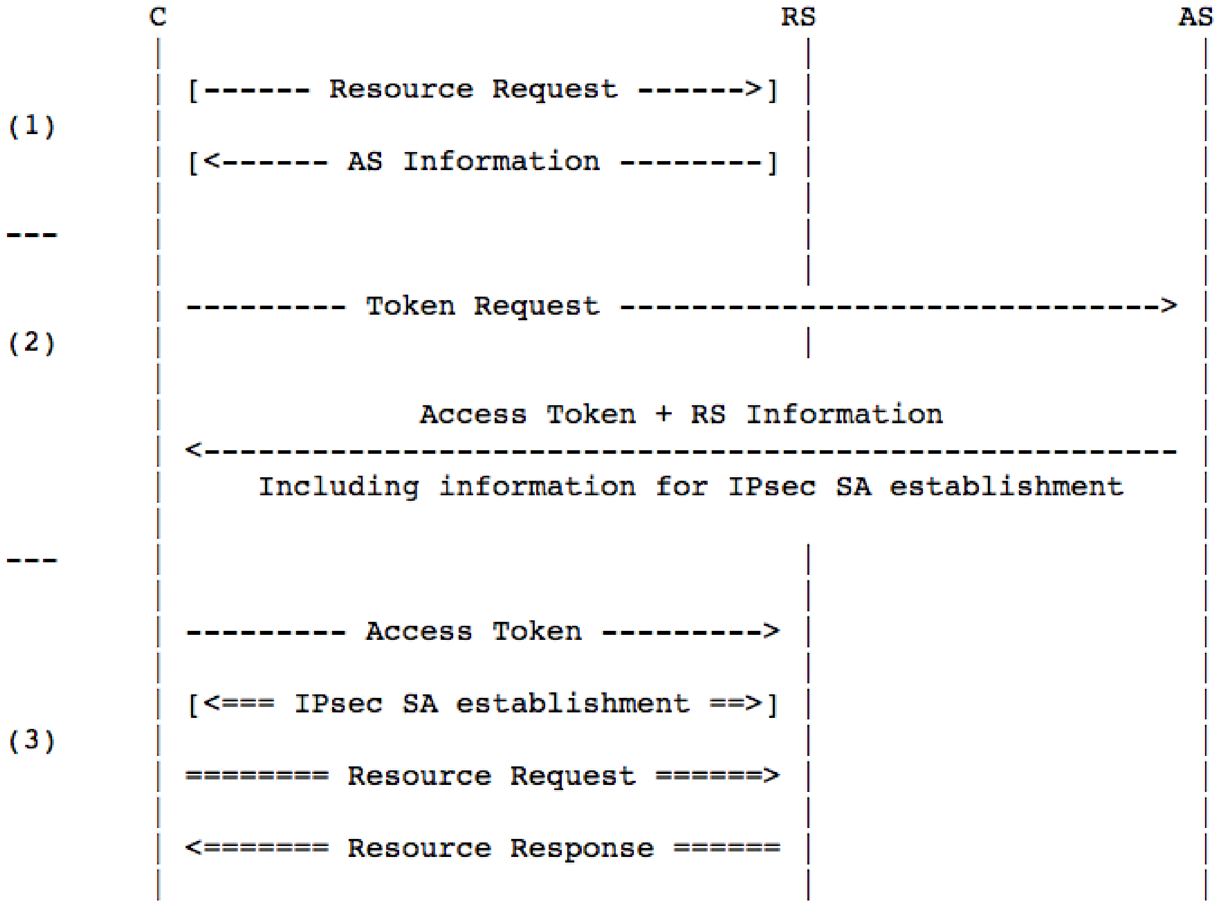
```
+--------+                               +---------------
|        |---(A)-- Token Request ------->|
|        |                               | Authorization |
|        |<--(B)-- Access Token ---------|     Server
|        |       + RS Information        |               |
|        |                               +---------------
|        |                                          ^  |
|        |         Introspection Request  (D)|  |
| Client |                                          |  |
|        |          Response + Client Token   |  |(E)
|        |                                          |  v
|        |                               +--------------+
|        |---(C)-- Token + Request ----->|              |
|        |                               |   Resource   |
|        |<--(F)-- Protected Resource ---|    Server    |
|        |                               |              |
+--------+                               +--------------+
```

Figure 1: Basic Protocol Flow.

- *https://tools.ietf.org/html/draft-ietf-ace-oauth-authz-08*

Protocol overview

- (1) Optional step for discovering the AS
- (2) Token Request and Token Response
- (3) IPsec channel establishment and authenticated resource request



```
            C                                     RS                      AS
            |                                     |                        |
            | [------ Resource Request ------>]   |                        |
   (1)      |                                     |                        |
            | [<------ AS Information --------]   |                        |
            |                                     |                        |
  ---       |                                     |                        |
            |                                     |                        |
            | --------- Token Request ---------------------------------->  |
   (2)      |                                     |                        |
            |                                                              |
            |          Access Token + RS Information                       |
            | <----------------------------------------------------------  |
            |     Including information for IPsec SA establishment         |
            |                                                              |
  ---       |                                     |                        |
            |                                     |                        |
            | --------- Access Token --------->   |                        |
            |                                     |                        |
            | [<=== IPsec SA establishment ==>]   |                        |
   (3)      |                                     |                        |
            | ======== Resource Request ======>   |                        |
            |                                     |                        |
            | <======= Resource Response ======   |                        |
            |                                     |                        |
```

Figure 4: Protocol Overview

Protocol steps

i. Client ↔ AS

- Get an Access Token to access a protected resource at RS
- The Token Response specifies how to set up an IPsec channel with RS
- Possibly update previously released Access Tokens

ii. Client ↔ RS

- Transfer the Access Token
- Set up the IPsec channel (different alternatives)

iii. Client ↔ RS

- Access the protected resource at RS

Alignment with other profiles

- Unauthorized Resource Request to find the AS (*)
- Token Update for IPsec session renegotiation (*)
- Communications between AS ↔ RS and AS ↔ C MUST be secured, e.g. OSCORE, DTLS, IPsec (*) (**)
- Same assumptions as to AS pre-knowledge

** https://tools.ietf.org/html/draft-ietf-ace-dtls-authorize-02*

*** https://tools.ietf.org/html/draft-seitz-ace-oscoap-profile-06*