IPsec profile of ACE

draft-aragon-ace-ipsec-profile-00

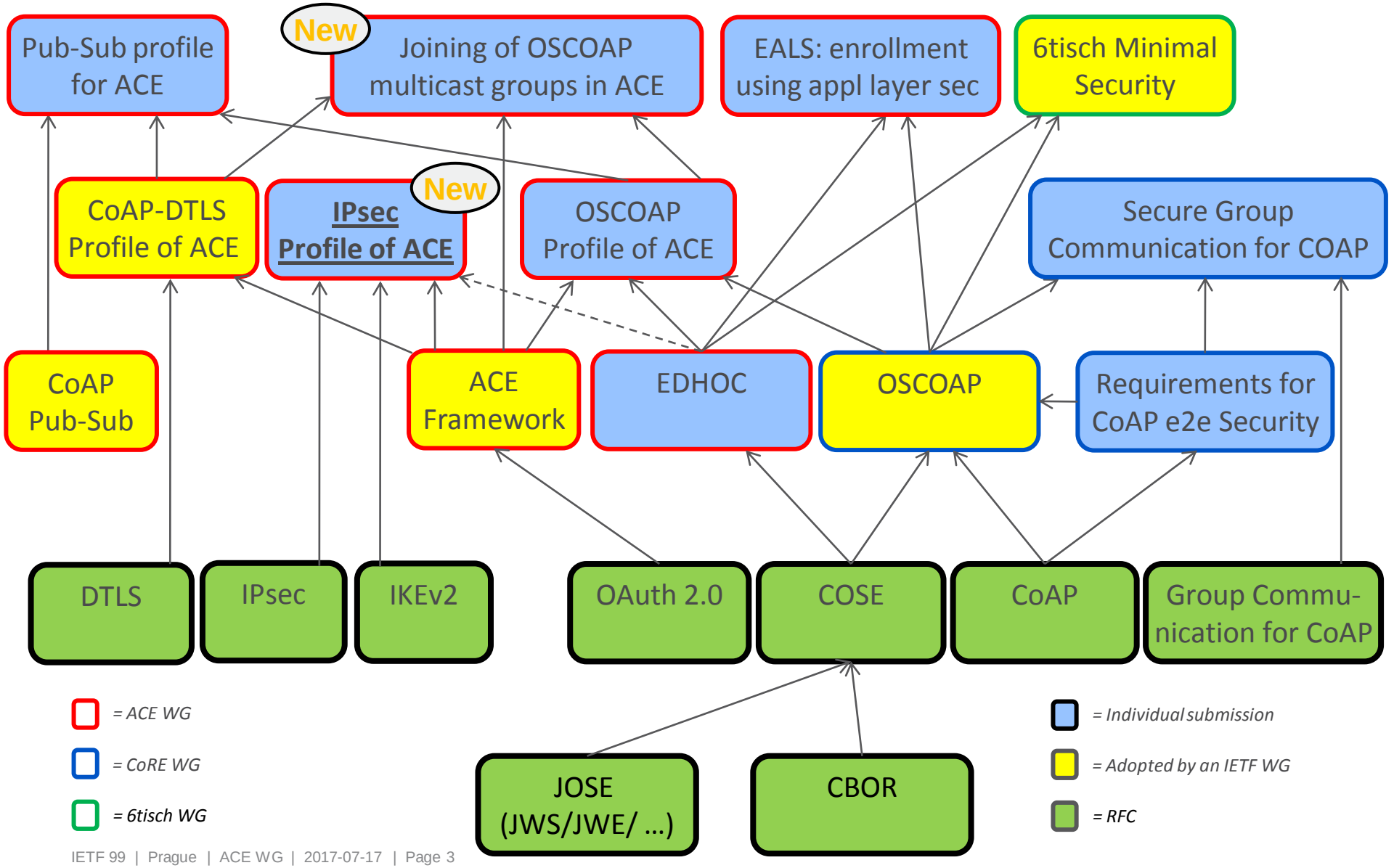
Santiago Aragón, RISE SICS
Marco Tiloca, RISE SICS
Shahid Raza, RISE SICS

IETF 99, ACE WG, Prague, July 17th, 2017

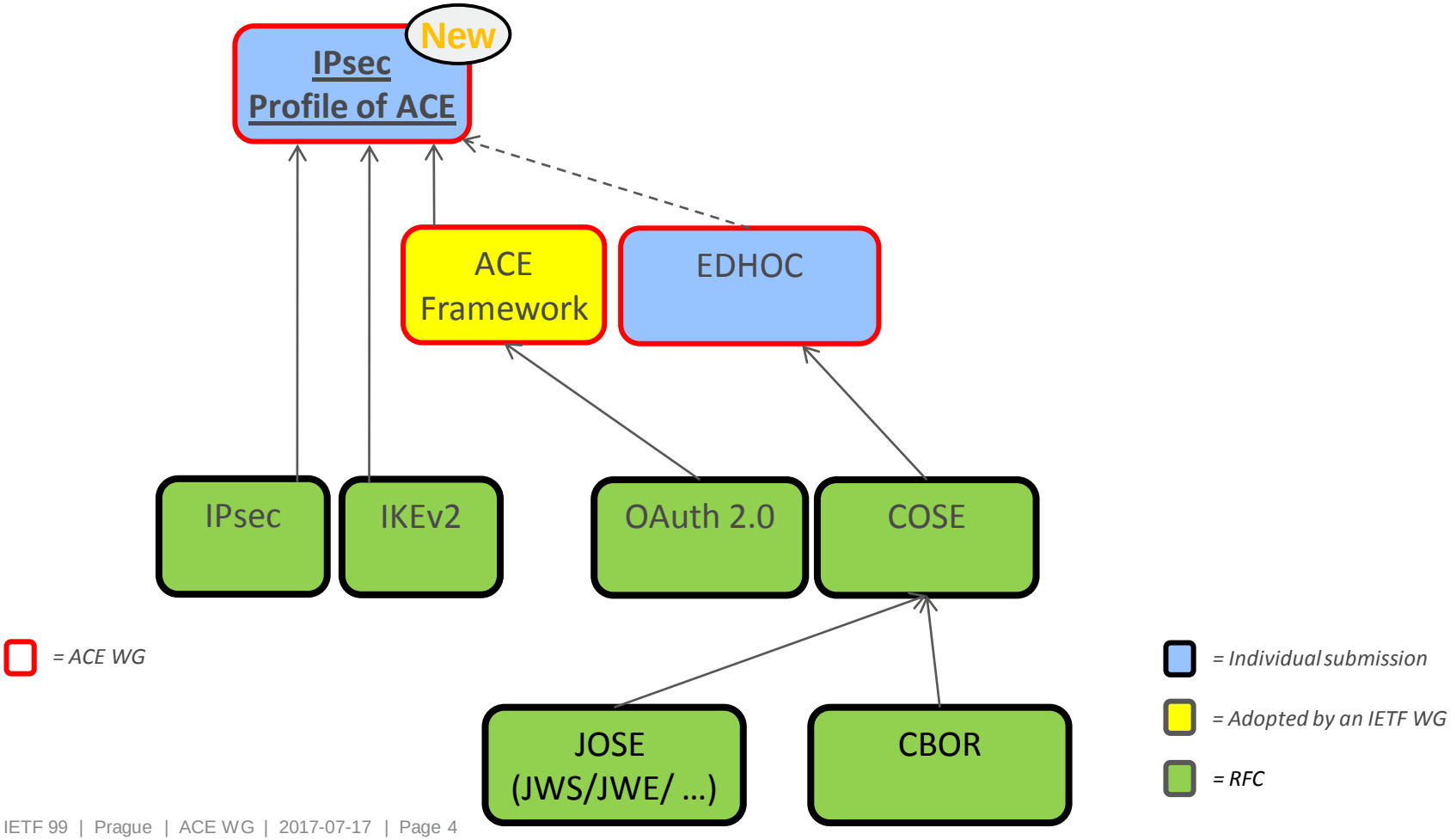
Motivation

- 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)
  - Possible alternative Key Management Protocols (e.g. EDHOC-based)
- Agnostic to the application layer

Related Work



Related Work



ACE Framework
(draft-ietf-ace-oauth-authz-06)

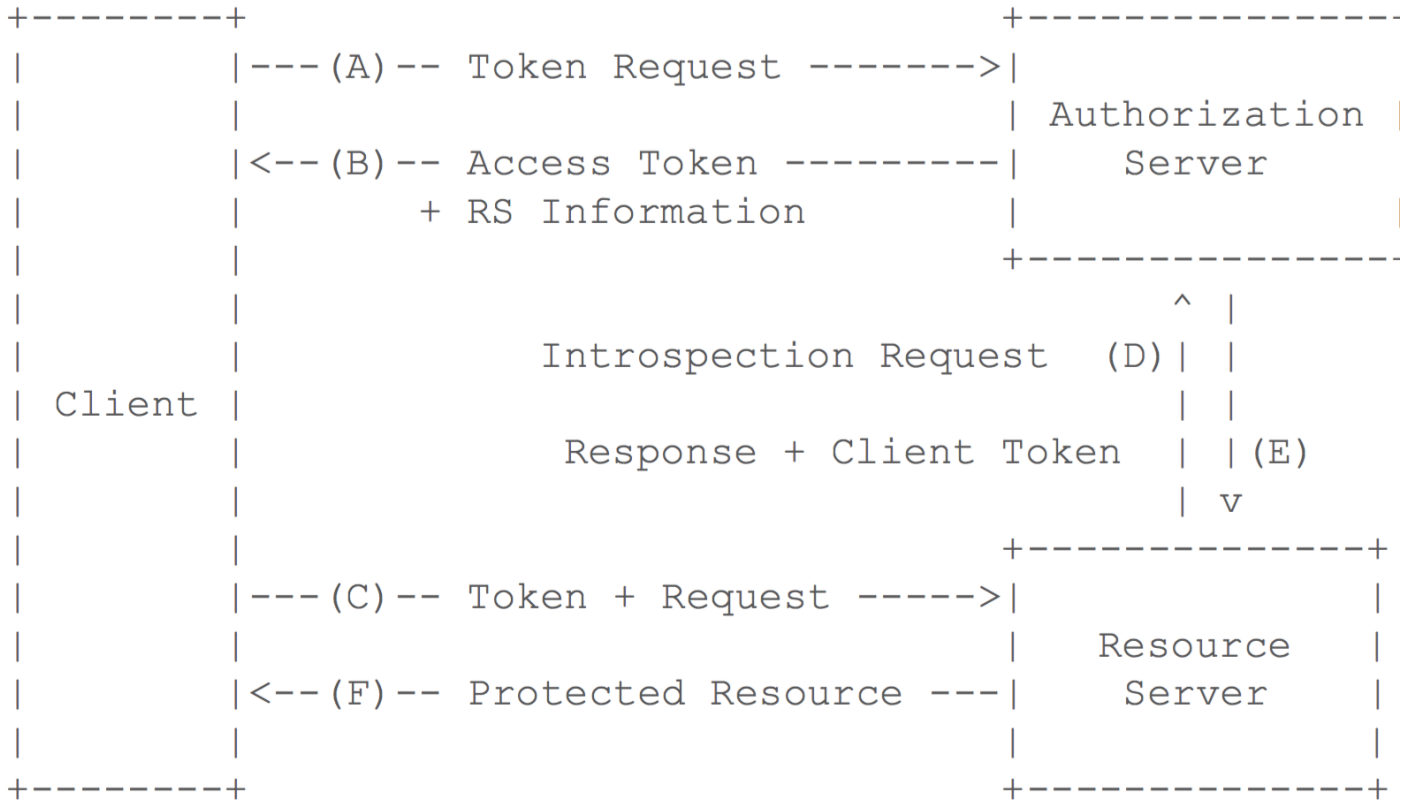


Figure 1: Basic Protocol Flow.

› *https://tools.ietf.org/html/draft-ietf-ace-oauth-authz-06*

Protocol overview

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

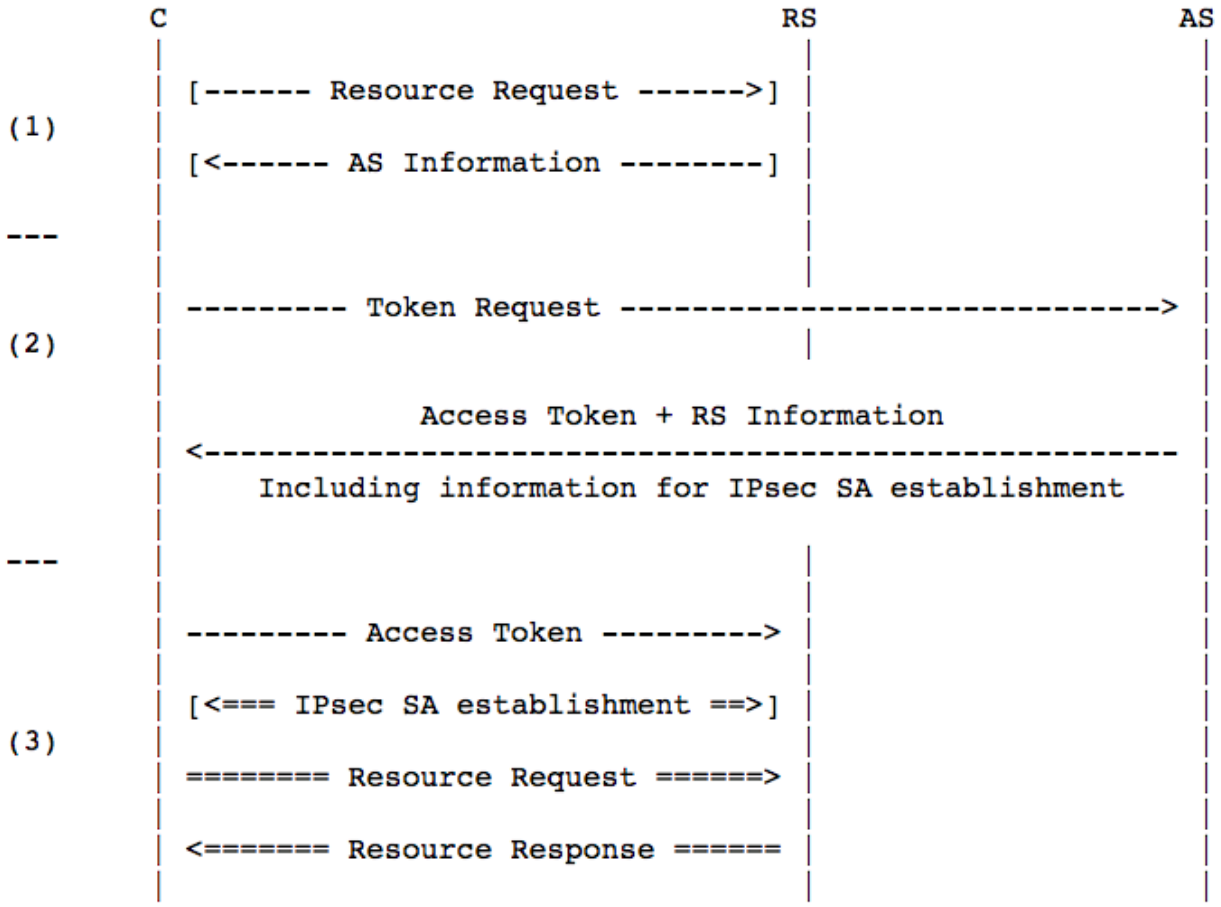
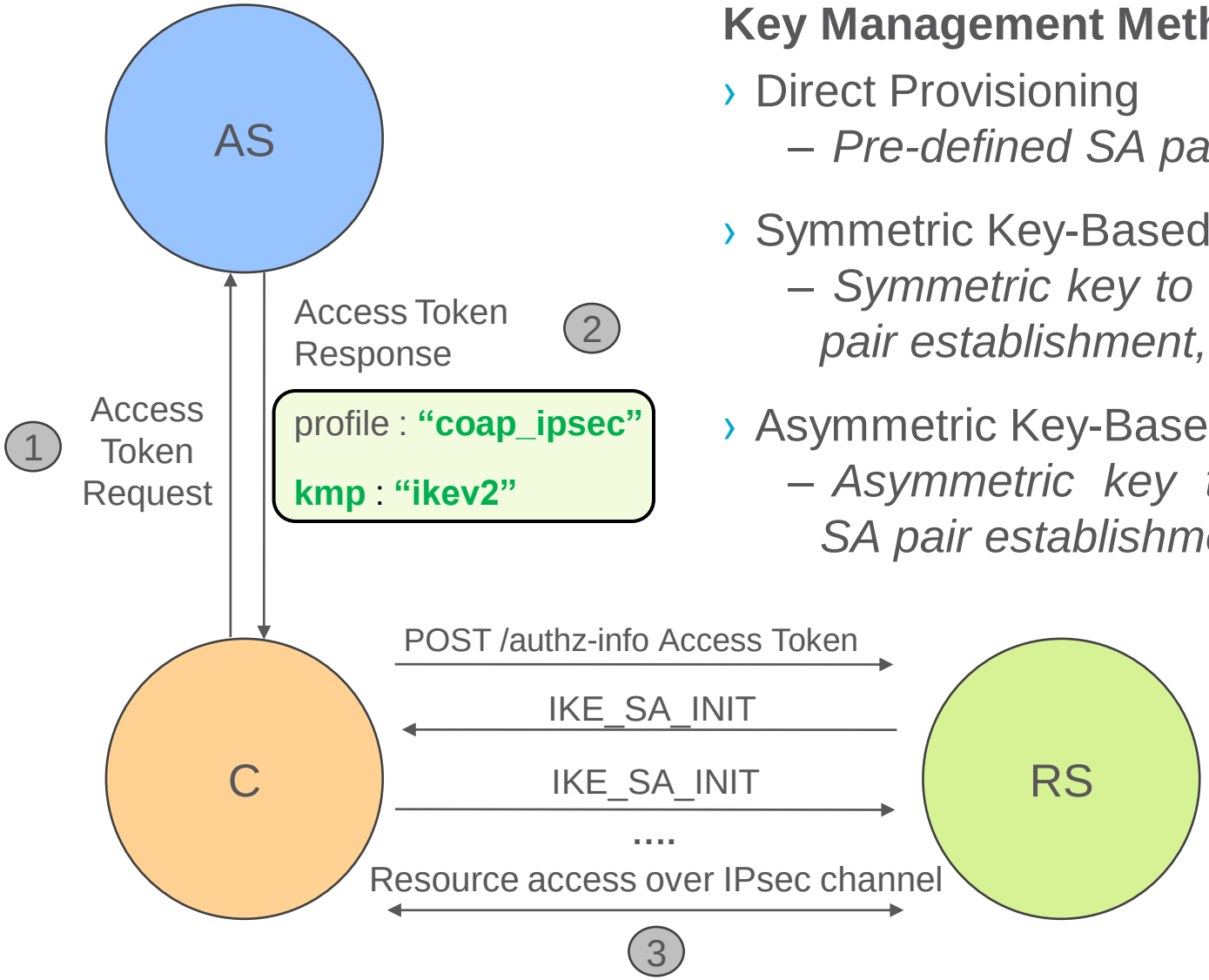


Figure 4: Protocol Overview

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*

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. OSCOAP, DTLS, IPsec (*) (**)

* *https://tools.ietf.org/html/draft-ietf-ace-dtls-authorize-01*

** *https://tools.ietf.org/html/draft-seitz-ace-oscoap-profile-03*

Alternative key management

- IPsec and OSCOAP can co-exist
  - Can be used together in the presence of CoAP Proxies (Appendix A)

- Appendix B describes how EDHOC can be used as an alternative to IKEv2 for establishing IPsec SA pairs

- This makes it possible to use EDHOC for establishing both IPsec SA pairs and OSCOAP Security Contexts

Planned Next Steps

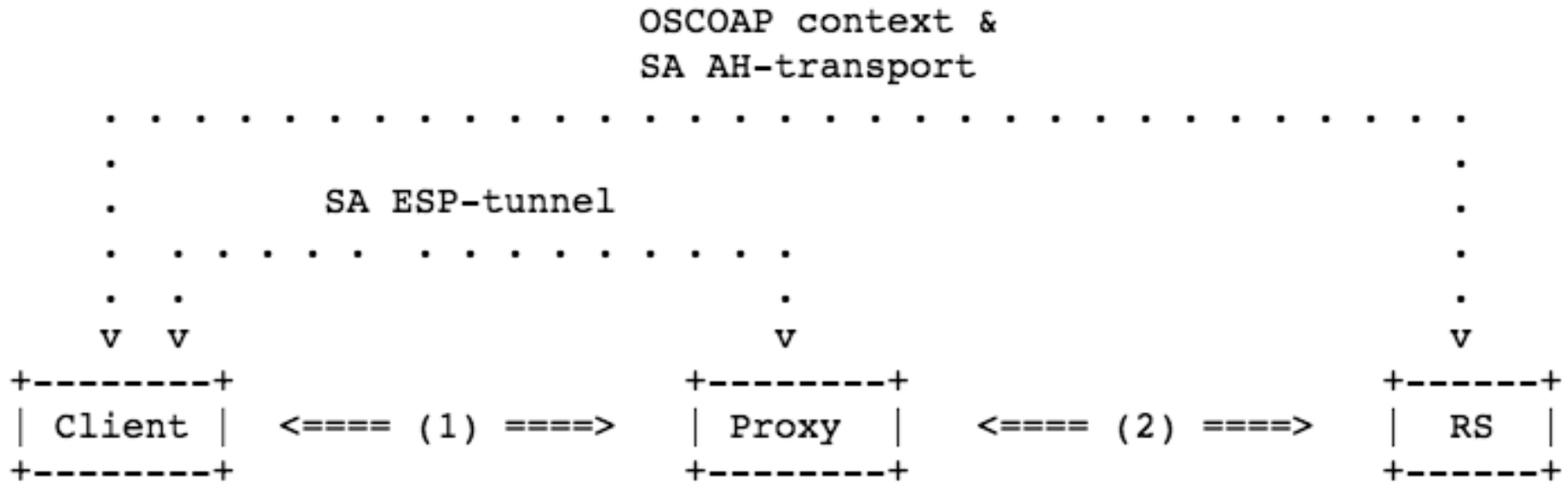
- Get feedback
- SICS implementation in Contiki

Thank you!

Comments/questions?

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

Co-existence of OSCOAP and IPsec



(1): |IP:P|ESP|IP:RS|AH|UDP|OSCOAP|ESP_T|ESP_Auth|
(2): |IP:RS|AH|UDP|OSCOAP|

Figure 9: OSCOAP and IPsec - Scenario overview