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**

Legend:
- □ = 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*

![Diagram showing resource access over IPsec channel]

1. Access Token Request
2. Access Token Response
3. Resource access over IPsec channel

**Profile description**

AS

C

RS

**profile**: “coap_ipsec”

**kmp**: “ikev2”

POST /authz-info Access Token

IKE_SA_INIT

IKE_SA_INIT

....
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

Thank you!

Comments/questions?

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

CoAP-DTLS Profile of ACE

Joining of OSCORE multicast groups in ACE

CoAP Pub-Sub

IPsec Profile of ACE

ACE Framework

OSCORE Profile of ACE

Secure Group Communication for CoAP

Requirements for CoAP e2e Security

DTLS

IPsec

IKEv2

OAuth 2.0

COSE

CoAP

Group Communication for CoAP

JOSE (JWS/JWE/...)

CBOR

= ACE WG

= CoRE WG

= 6tisch WG

= Individual submission

= Adopted by an IETF WG

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

Figure 1: Basic Protocol Flow.
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
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