Joining of OSCORE multicast groups in ACE

draft-tiloca-ace-oscoap-joining-02

Marco Tiloca, RISE SICS
Jiye Park, Universitaet Duisburg-Essen

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

Motivation

- Join OSCORE multicast groups through their Group Manager (GM)
  - Using the ACE framework and its profiles
  - Keeping the approach oblivious to the specifically used profile
  - Preserve flexible arrangements and managements of multicast groups

- Goals
  - Authorize a node to join according to group join policies
  - Secure channel establishment between joining nodes and the GM
  - Initialization of joining nodes and key provisioning through the GM

- Not covered in this document
  - Authorization to access resources at group members
  - Actual secure communication in the OSCORE multicast group

Protocol overview

- Join an OSCOAP multicast group over the ACE framework
  - Client → Joining node
  - Resource Server → Group Manager (GM)
  - The AS enforces access policies on behalf of the GM
  - Leverage protocol-specific profiles of ACE

- Joining process
  - One CoAP request for each group to join
  - GM performs key provisioning and initializes the joining node (*)

- It is recommended that GM stores the members' public keys
  - It receives new members' public key upon their joining
  - If requested so, it provides members' public keys to joining nodes

(*) Details in *draft-tiloca-core-multicast-oscoap-04*

Open points (1/2)

1. Exact message exchange between joining node and GM
   - Details are now in the Multicast OSCORE draft
   - Have them (also) in this draft? What's a good level of detail?

2. The AS authorizes the access to multicast groups
   - "The AS is not necessarily expected to release Access Tokens for any other purpose […]. However, the AS may be configured also to release Access Tokens for accessing resources at members of multicast groups." (Section 2)
   - Should we consider also such Access Token release? Perhaps combined with the main one for group joining?

Open points (2/2)

3. Similarities with the Pub-Sub profile of ACE
   - Previous thoughts on generalizing pub-sub for group communication
   - Both drafts address key provisioning, something may be merged
   - Avoid defining multiple sets of messages for the same goal
   - What's the best way to proceed?

Next steps

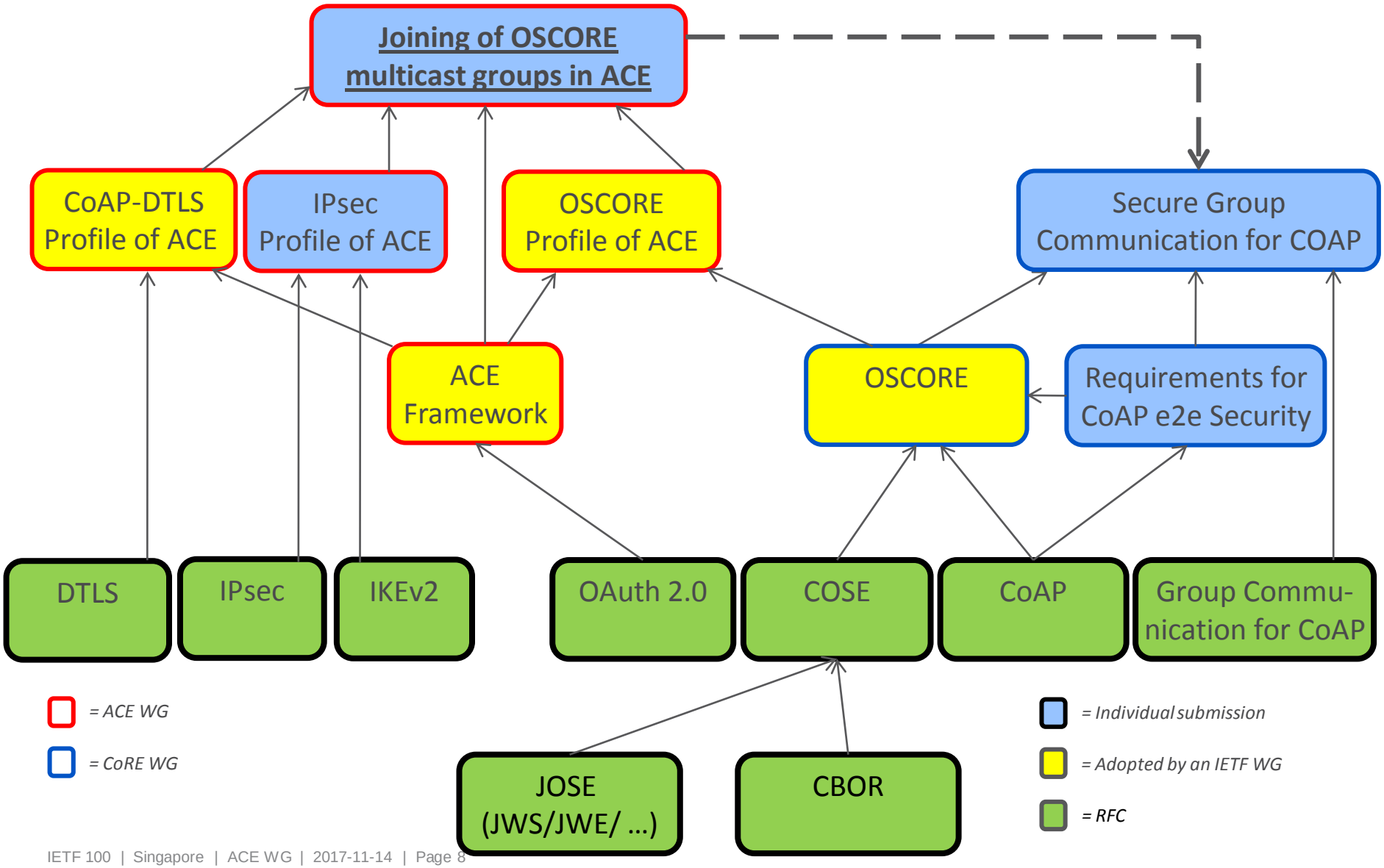
- Ensure alignment with:
  - The ACE framework and its profiles
  - The join process in the Multicast OSCORE document
- Get further comments and address the open points
- Got “High-priority” at the ACE interim meeting
  - What is needed to proceed towards adoption?

Thank you!

Comments/questions?

https://gitlab.com/crimson84/draft-tiloca-ace-oscoap-joining/

Related Work



Group Manager (GM)

- Can be responsible of multiple groups
  - Join of new group members
  - Renewal of group keying material
- Drive the joining process
  - Contact point for joining the group
  - Actual admission of new nodes in the group
  - Provides keying material to joining nodes (incl. security context)
- Possibly act as key repository
  - Store public keys of group members

Protocol steps

1. Joining node to Authorization Server (*)
   - Get an Access Token to access a join resource on GM
   - The response includes information to start a secure channel with GM
   - Possibly update previously released Access Tokens

2. Joining node to Group Manager (*)
   - Transfer the Access Token
   - Open a secure channel (if not already established)

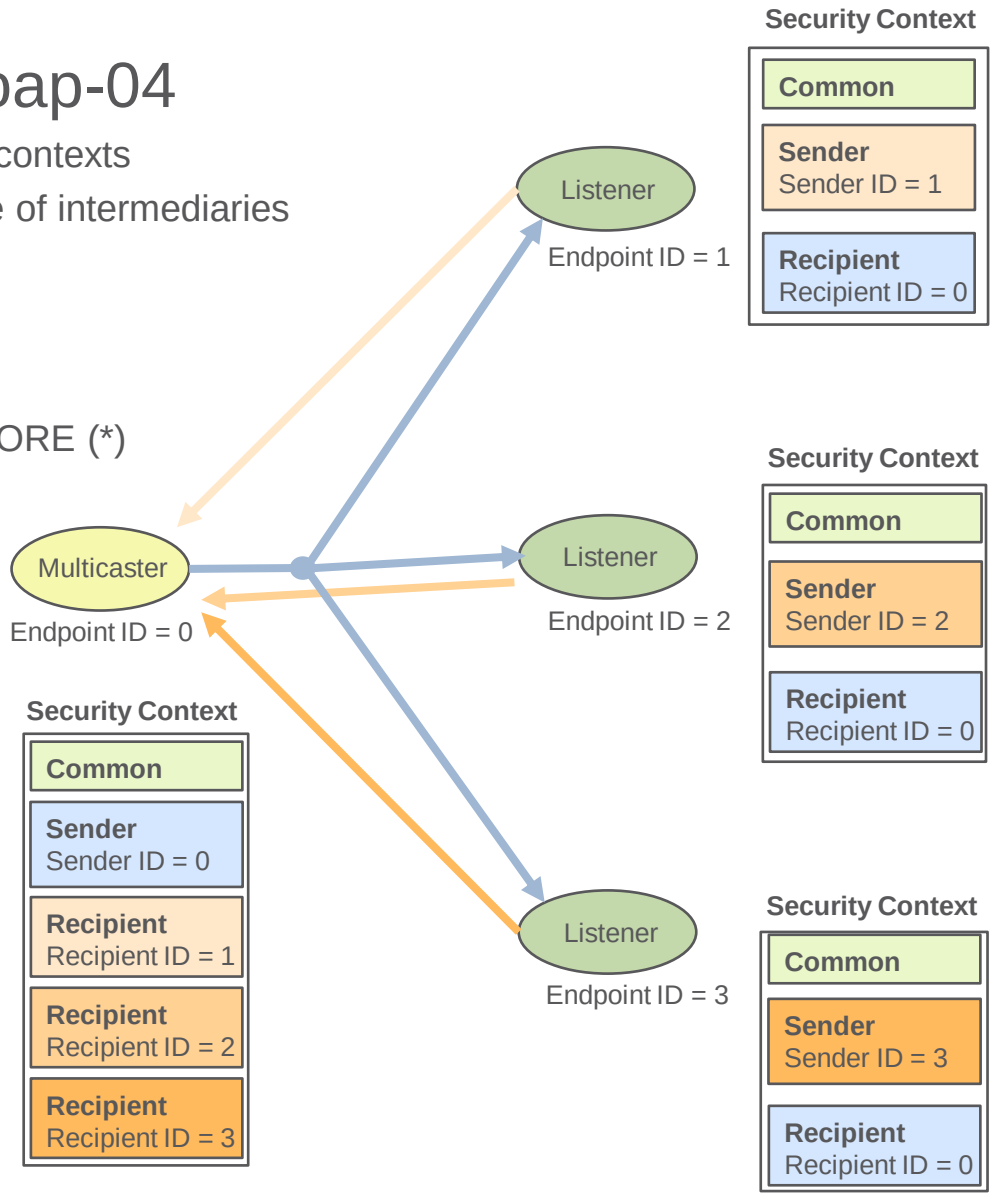
3. Joining node to Group Manager
   - Access the related join resource at GM
   - Perform the joining process

(*) Access Token and secure channel establishment are specified in the used profile

Background - Multicast OSCORE

- draft-tiloca-core-multicast-oscoap-04
  - Support for OSCORE (*) in group communication contexts
  - Secure end-to-end communication in the presence of intermediaries

- Main features
  - Same structures, constructs, mechanisms of OSCORE (*)
  - Confidentiality, integrity, replay protection
  - Source authentication through digital signatures
  - Request-response binding



(*) *draft-ietf-core-object-security-06*

Use cases for Multicast OSCORE

- Lighting control
- Integrated building control
- Software and firmware updates
- Parameter and configuration updates
- Commissioning of LLNs systems
- Emergency multicast

See “Appendix A” of *draft-tiloca-core-multicast-oscoap-04*