Joining of OSCOAP multicast groups in ACE

draft-tiloca-ace-oscoap-joining-00

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

IETF 99, ACE WG, Prague, July 17\textsuperscript{th}, 2017
Motivation

› Specify how to join OSCOAP multicast groups through a Group Manager
  – Use the existing ACE framework (*) and profiles (**) for this specific scenario
  – Keep the approach as such oblivious to the specific underlying profile

› Focus on
  – Authorize a node to join according to group policies
  – Secure channel establishment with the Group Manager
  – Initialization of joining nodes and provisioning of public keys

› Covered by other documents
  – Authorization to access protected resources at group members (*) (**)  
  – Actual secure communication in the multicast group (***)

(*)  draft-ietf-ace-oauth-authz-06
(**)  draft-ietf-ace-dtls-authorize-01 ; draft-seitz-ace-oscoap-profile-03
(***) draft-tiloca-core-multicast-oscoap-02
Related Work

- Pub-Sub profile for ACE
- Joining of OSCOAP multicast groups in ACE
- EALS: enrollment using appl layer sec
- 6tisch Minimal Security
- CoAP-DTLS Profile of ACE
- IPsec Profile of ACE
- OSCOAP Profile of ACE
- Secure Group Communication for CoAP
- Requirements for CoAP e2e Security
- ACE Framework
- EDHOC
- OSCOAP
- JOSE (JWS/JWE/...)
- CBOR
- DTLS
- IPsec
- IKEv2
- OAuth 2.0
- COSE
- CoAP
- Group Communication for CoAP

Legend:
- = ACE WG
- = CoRE WG
- = 6tisch WG
- = Individual submission
- = Adopted by an IETF WG
- = RFC

IETF 99 | Prague | ACE WG | 2017-07-17 | Page 3
Related Work

- Joining of OSCOAP multicast groups in ACE
- Secure Group Communication for CoAP
- Requirements for CoAP e2e Security
- ACE Framework
- EDHOC
- OSCOAP
- OAuth 2.0
- COSE
- CoAP
- Group Communication for CoAP
- DTLS
- JOSE (JWS/JWE/...)
- CBOR

Legend:
- Red square: ACE WG
- Blue square: Core WG
- Yellow square: Adopted by an IETF WG
- Green square: RFC
- Grey square: Individual submission
Background - Multicast OSCOAP

› draft-tiloca-core-multicast-oscoap-02
  – Support for OSCOAP (*) in group communication contexts
  – Secure end-to-end communication in the presence of intermediaries

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

› Alternative modes
  – Group authentication only (appendix)
  – Unencrypted unicast w/ signatures (appendix)

(*) draft-ietf-core-object-security-03
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 overview

› Join an OSCOAP multicast group over the ACE framework
  – Joining node → Client
  – Group Manager → Resource Server (one join resource per group)
  – The AS enforces join policies on behalf of the Group Manager

› Leverage protocol-specific profiles of ACE
  – CoAP-DTLS profile   draft-ietf-ace-dtls-authorize-01
  – OSCOAP profile     draft-seitz-ace-oscoap-profile-03

› Related to Appendix A of Group OSCOAP v-02 (*)
  – Following comments at IETF97

› (*) draft-tiloca-core-multicast-oscoap-02
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
Joining process

› One separate CoAP request for each group to join

› The GM admits the joining node to the group
  – Provides the OSCOAP endpoint ID
  – Provides the OSCOAP Security Common Context

› The GM can store nodes’ public keys
  – Receives the joining node’s public key
  – Provides public keys of current group members to the joining node
Planned next steps

› Ensure alignment with:
  – ACE framework for authentication and authorization
  – CoAP-DTLS and OSCOAP profiles of ACE

› Consider additional profiles:
  – E.g., IPsec profile of ACE (*)

› Get comments and feedback

(*) draft-aragon-ace-ipsec-profile-00
Thank you!

Comments/questions?

https://gitlab.com/crimson84/draft-tiloca-ace-oscoop-joining/
Use cases for Multicast OSCOAP

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

See “Appendix B” of draft-tiloca-core-multicast-oscoap-02