Joining OSCORE groups in ACE

draft-tiloca-ace-oscoap-joining-03

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

IETF 101, ACE WG, London, March 19\textsuperscript{th}, 2018
Action points from IETF100

1. Define the exact content of exchanged messages
   - Aligned with the guidelines in draft-ietf-core-oscore-groupcomm

2. Address similarities with the Pub-Sub profile of ACE
   - Both drafts address key provisioning for group communication
   - Avoid defining multiple sets of messages for the same goal

Result
   - Build on the generic formats in draft-palombini-ace-key-groupcomm
   - Finalize the message content for joining OSCORE groups
   - The Group Manager acts as the “KDC” of the generic scenario
   - There is no participant node acting as “Dispatcher”
C -> AS  Authorization Request

- The "scope" parameter includes:
  - The Group Identifier (Gid) of the OSCORE group to join.
  - The role(s) that the joining node wishes to have in the group.

- The "aud" parameter is set to the address of the GM

- The "get_pub_keys" parameter is present if:
  - The GM stores the public keys of group members
  - The joining node wants those public keys at joining time

"get_pub_keys" is defined in draft-palombini-ace-key-groupcomm
AS -> C Authorization Response

› Access Token as in draft-palombini-ace-key-groupcomm

› The “exp” parameter must be present

› The “scope” parameter is present if:
   – The joining node is authorized for different roles than in the request

› The “profile” parameter is present
   – The joining node and GM establish a secure channel accordingly
C -> GM (RS)  Join Request

› After Token Post and processing on the GM

› The “get_pub_keys” parameter:
  – Is included if present also in the Authorization Request.

› The “client_cred” parameter (optional) includes:
  – Public key or certificate of the joining node
  – Exact content depends on the GM storing public keys or not
  – Omitted if the GM already acquired the public key or certificate

› The “pub_keys_repos” parameter (optional):
  – May be present if “client_cred” is present and includes a certificate
  – It includes a list of repos storing the joining node’s certificate
The “key” parameter includes:

- "kty" with value “Symmetric”.
- "k" as the OSCORE Master Secret.
- "alg" (opt) as the AEAD algorithm used in the group.
- "kid" (opt) as the identifier of “k”.
- "base IV" (opt) as the OSCORE Common IV.
- “clientID” as the Endpoint ID of the joining node.
- “serverID” as the Group Identifier (Gid) of the group.
- "kdf" (opt) as the KDF algorithm used in the group.
- "slt" (opt) as the OSCORE Master Salt.
- "cs_alg" as the countersignature algorithm used in the group.

* defined in RFC8152
** defined in draft-ietf-ace-oscore-profile
GM (RS) -> C  Join Response (2/2)

› The “pub_keys” parameter:
  – Is present if “get_pub_keys” was in the Join Request.
  – Includes the public keys of the current group members.

› The “group_policies” parameter:
  – Includes a list of policies enforced in the group.
  – E.g. synchronization of sequence numbers, rekeying protocol.

› The “mgt_key_material” parameter:
  – Includes administrative key material to participate to the rekeying.
  – Content and format are specific of the rekeying protocol.
Conclusion

› Aligned with:
  – General message formats from *draft-palombini-ace-key-groupcomm*
  – Now providing specific message format for joining OSCORE groups

› Aligned with:
  – The general join description in *draft-ietf-core-oscore-groupcomm*
  – Pointer to this document as recommended joining approach
  – Should this approach be more than recommended?

› “High-priority” at the ACE interim meeting (October 2017)

› Ready for adoption?
Thank you!

Comments/questions?

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

› Join an OSCORE group through its Group Manager (GM)
   – Using the ACE framework and its profiles
   – Keeping the approach oblivious to the used security profile
   – Preserving flexible arrangements and managements of groups

› Objectives
   – Authorize joining nodes according to group join policies
   – Secure channel establishment between joining nodes and the GM
   – Initialization of joining nodes and key provisioning through the GM

› Out of scope
   – Authorization to access resources at group members
   – Actual secure communication in the OSCORE group
Protocol overview

› Join an OSCORE group using the ACE framework
  – Client → Joining node
  – Resource Server (RS) → Group Manager (GM)
  – The AS enforces access policies on behalf of the GM
  – Leverage profiles of ACE for secure communication with the GM

› Joining process
  – CoAP request to the GM resource associated to the group to join
  – The GM provides keying material and other parameters to the joining node

› The GM may store the members’ public keys
  – It receives new members’ public key upon their joining
  – If requested so, it provides members’ public keys to joining nodes
**Step-by-step message formats**

(2) **Authorization Response**
- AT: access token
- Exp: lifetime of the AT
- Scope: confirmation of the roles requested in (1)
- Profile: security protocol between Client and GM

(6) **Join Response**
- Keying material for the OSCORE Security Context
- Pub_keys: if get_pub_keys was in (5), includes public keys of current group members
- Group_policies: includes list of policies (synchronization of seq number, rekeying protocol)
- Mgt_key_material: administrative key material to participate to the rekeying; content and format depends on the specific rekeying protocol

(1) **Authorization Request**
- Scope
  - Gid: Group ID that joining node wants to join
  - Roles: \{Sender, Listener, Pure Listener\}
- Aud: Group Manager’s address
- Get_pub_keys: request to get public keys of members

(3) **Token Post**
- Simple post of AT

(4) **Authorization Response**
- Secure channel establishment according to the signalled profile of ACE

(5) **Join Request**
- If get_pub_keys is included in (1), also included here
- Client_cred: public_key or certificate of the Client
- pub_keys_repos: including a list of public repos if client_cred is present and includes a certificate

(7) **OSCORE group communication**
Group OSCORE

*draft-ietf-core-oscore-groupcomm*

- Use of OSCORE (*) in group communication scenarios

**Main features**

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

(*) *draft-ietf-core-object-security*
Use cases for Group OSCORE

› Lighting control

› Integrated building control

› Software and firmware updates

› Parameter and configuration updates

› Commissioning of LLNs systems

› Emergency multicast

See “Appendix B” of draft-ietf-core-oscore-groupcomm-01
Group Manager (GM)

› Can be responsible of multiple OSCORE 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/provide public keys of group members