Joining OSCORE groups in ACE

draft-tiloca-ace-oscoap-joining-04

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

IETF 102, ACE WG, Montreal, July 16th, 2018

Updates from -03 (1/3)

- This revision addresses mostly:
  - Latest updates in *draft-ietf-core-oscore-groupcomm*
  - Message formats from *draft-palombini-ace-key-groupcomm*
  - Review from Peter van der Stok - Thanks a lot!

- Section 1.1 – “Terminology”
  - “Multicaster” → “Requester” // no focus on multicast traffic
  - “Pure listener” is the “Silent server” of group OSCORE
  - Use “Listener” to avoid confusion with ACE “Client” and “Server”

- Section 3.1 – “Authorization request”
  - Removed ‘get_pub_keys’ from this request
  - The AS has no reason to know this detail

Updates from -03 (2/3)

- Section 4.2 – “Join Response”
  - Added ‘exp’ in the ‘key’ parameter
  - ‘exp’ is defined in *draft-palombini-ace-key-groupcomm*
  - Clarified when ‘clientID’ is not needed in the ‘key’ parameter

The “**key**” parameter includes:

- “**kty**” with value “Symmetric”.
- “**k**” as the OSCORE Master Secret.
- “**exp**” specifies where ‘k’ expires.
- “**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**” (opt) 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.

Updates from -03 (3/3)

- Editorial improvements and text polishing
  - As to terminology from Group OSCORE
  - As to the usage of ACE profiles
  - As to interaction between actors
- Clarification on dynamic Group Identifier
  - A part of the Gid can vary over time, e.g., the Gid Epoch
  - The Gid initially included in ‘scope’ may differ from the current one
  - The current Gid is included in the Join Response as ‘key.ServerID’
- Storing and maintaining public keys
  - Now the Group Manager may be the public key repo
  - Should we only admit the Group Manager as repo?

Conclusion

› Addressed review from Peter van der Stok – Thanks a lot!

› Aligned with:
  – Latest updates in *draft-ietf-core-oscore-groupcomm*
  – Message formats from *draft-palombini-ace-key-groupcomm*

› 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

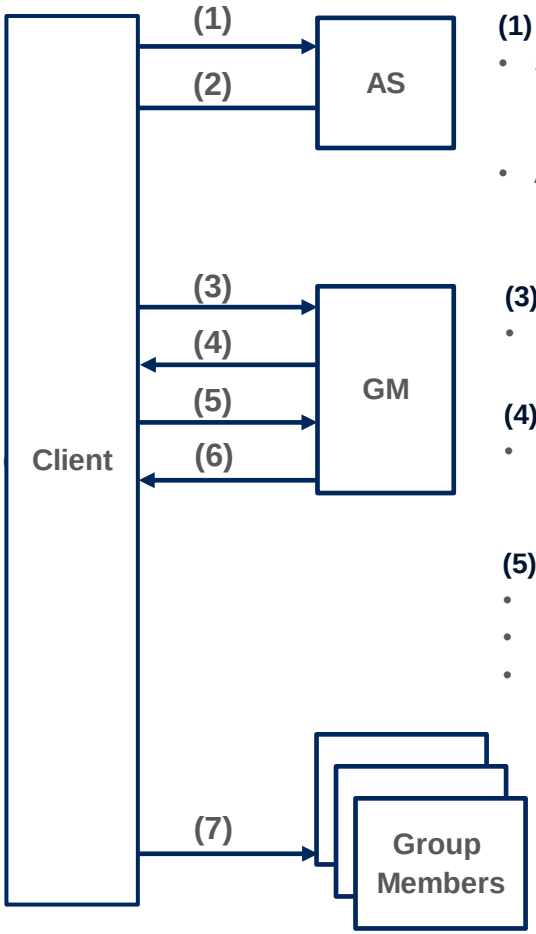
- Joining process
  - CoAP request to the GM resource associated to the group to join
  - The GM provides keying material and other parameters to the joining node

- 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

(3) Token Post
- Simple post of AT

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

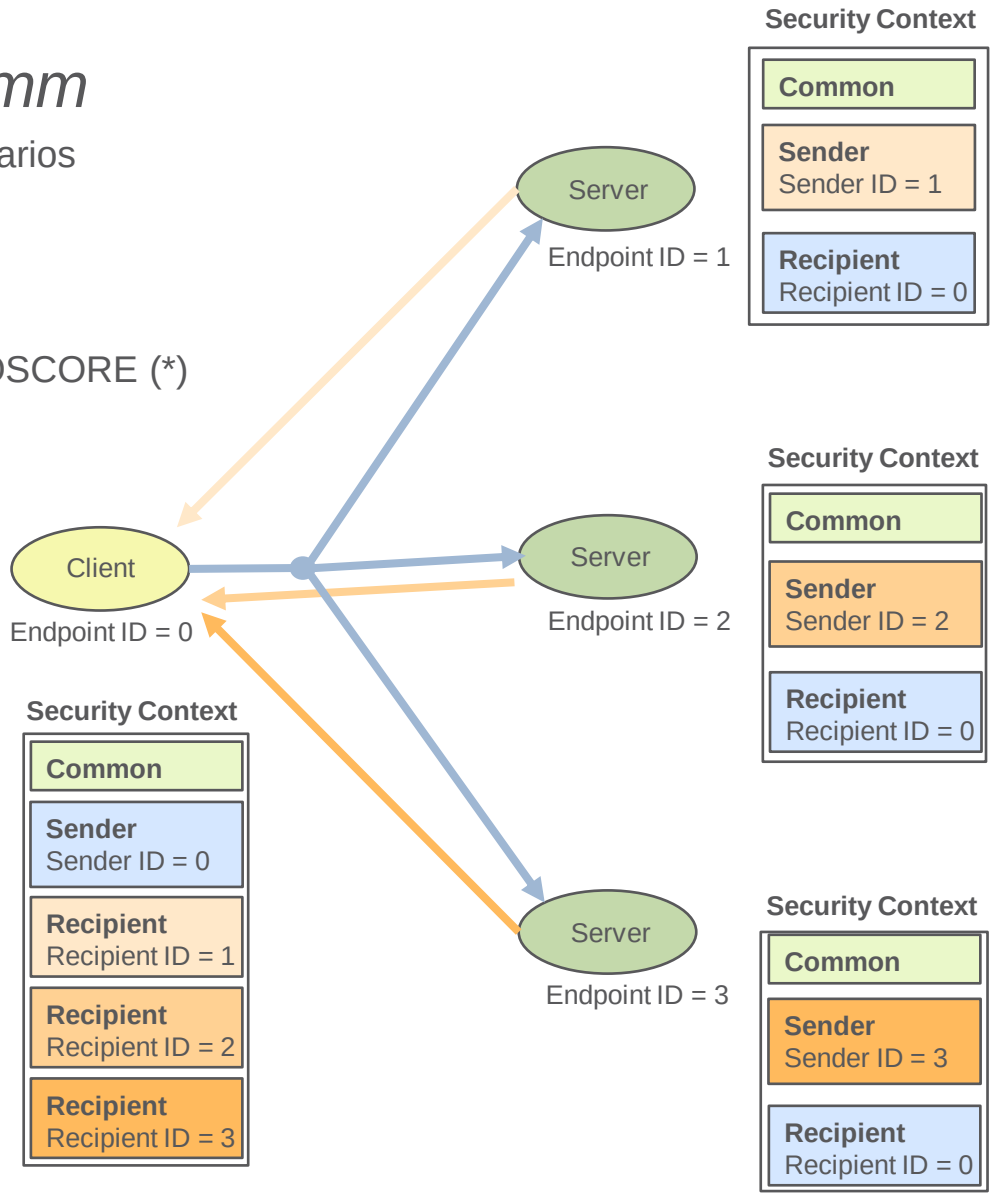
(5) Join Request
- Possibly include get_pub_keys to get public keys
- Client_cred: public_key or certificate of the Client
- pub_keys_repos: including a list of public repos if client_cred is present and includes a certificate

(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*