

Key Management for OSCORE Groups in ACE

draft-ietf-ace-key-groupcomm-oscore-08

Marco Tiloca, RISE
Jiye Park, Universität Duisburg-Essen
Francesca Palombini, Ericsson

IETF 108, ACE WG, July 29th, 2020

Recap

› Message content and exchanges for:

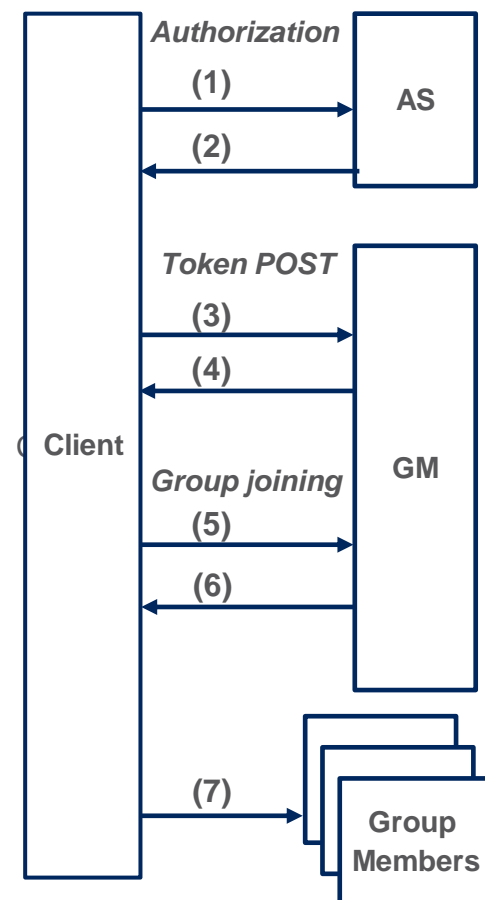
- Provisioning keying material to joining nodes and groups (rekeying)
- Joining an OSCORE group through its Group Manager (GM)
- More operations for current members at the GM

› Builds on *draf-ietf-ace-key-groupcomm*

- Agnostic of the ACE transport profile used by C and GM

› Out of Scope:

- Authorizing access to resources at group members
 - › *draft-tiloca-ace-group-oscore-profile*
- Actual secure communication in the OSCORE group
 - › *draft-ietf-core-oscore-groupcomm*



Updates in v -08

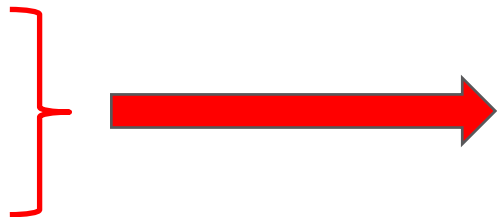
- › Closed open point on role combinations
 - Now checked by the Group Manager when getting the Joining Request
- › Parameters ‘cs_alg’, ‘cs_params’, ‘cs_key_params’, ‘cs_key_enc’
 - Default values moved here from *draft-tiloca-ace-oscore-gm-admin*
- › The format of ‘scope’ is now based on AIF
 - New AIF specific data model “AIF-OSCORE-GROUPCOMM”
 - AIF-Generic<Toid, Tperm> = [* [Toid, Tperm]]
 - AIF-OSCORE-GROUPCOMM = AIF_Generic<path, permissions>
- › Resulting scope format, using AIF-OSCORE-GROUPCOMM
 - scope entry: [Toid, Tperm]
 - scope: << [* [Toid, Tperm]] >>

Updates in v -08

- › AIF-OSCORE-GROUPCOMM = AIF_Generic<path, permissions>
 - path → Toid: text string, specifying the group name
 - permissions → Tperm: unsigned integer, encoding the roles for that group

```
AIF-OSCORE-GROUPCOMM = AIF_Generic<path, permissions>
```

```
path = tstr ; Group name
permissions = uint . bits roles
roles = &(
    Requester: 1,
    Responder: 2,
    Monitor: 3,
    Verifier: 4
)
```



Will be 1, 2, 4, 8 in the next version

- › Registered AIF Toid, Tperm, Media Type and Content Format
- › Created new registry for Group OSCORE roles

Updates in v -08

- › New common format for requesting public keys
 - [[role_combinations], [node_names]]
 - ‘get_pub_keys’ in the Joining Request (the second array is empty)
 - FETCH payload of the request to GROUPNAME/pub-key
- › Default values for the group policies
 - Sequence Number Synchronization Method: 1 (“Best Effort”)
 - Key Update Check Interval: 3600
 - Expiration Delta: 0
 - Group OSCORE Pairwise Mode Support: False

Next steps

› Open point

- ‘clientID’ in the Joining Response is the Sender ID of the joining node
- It is not related to being exactly client in the group → clarify in next version

› Resource type rt=core.osc.mbr

- Move registration here from *draft-tiloca-core-oscore-discovery* ?
 - › Based on pending decision about Resource Type in *ace-key-groupcomm*
- If so, different name? E.g., “grp.osc.mbr”

› Interop tests

› Then ready for WGLC (?)

Thank you!

Comments/questions?

<https://github.com/ace-wg/ace-key-groupcomm-oscore>

Backup slides

Old open point

- › Legitimate role combinations
 - Removed role combination [“Requester”, “Monitor”]
 - It doesn’t make sense inside a group. But, **when** should this be checked?
- › OLD: the AS checks that, when getting a Token Request:
 - › [“Requester”, “Responder”] is valid
 - › [“Requester”, “Monitor”] is not valid
 - › A node wanting to join first as Requester, then as Monitor needs 2 tokens
 - › This should be rather checked by the GM when getting a Joining Request
- › NEW: Distinguish ‘scope’ in Token Request and in Joining Request
 - › Token Request: any combination of any admitted role is fine
 - › Joining Request: any legitimate combination of roles in the token is fine