# Key Provisioning for Group Communication using ACE

*draft-ietf-ace-key-groupcomm-16*

# Key Management for OSCORE Groups in ACE

*draft-ietf-ace-key-groupcomm-oscore-15*

ACE WG Interim Meeting, September 12th, 2022

# -key-groupcomm (1/4)

- **Current status: “AD Review”**

- **Version -16 submitted on 2022-09-05, building on the proposal at [1]**
  - Early synching with Daniel and Paul (ACE AD) at IETF 114
  - No objection received on the mailing list

- **List of updates**
  - “UPDATE 1” in [1]: Revised optional signaling of scope semantics, now based solely on CBOR tags
  - “UPDATE 2” in [1]: When using AIF to express a scope, reduce restrictions for “Toid” encoding
  - Difference between “public key” and “authentication credential”
  - Renaming of parameters, messages and URI path segments

Pending since Göran’s review of *draft-ietf-ace-key-groupcomm-oscore*

[1] https://mailarchive.ietf.org/arch/msg/ace/cWlidk1FS8h00HSkzgubk_LJ0kI/

# -key-groupcomm (2/4)

- **UPDATE 1:** Revised optional signaling of scope semantics, now based solely on CBOR tags
- **Reminder: scope is a CBOR bstr, with value an array of scope entries**
  - scope_entry = AIF_format / Textual_format
  - scope = << [ + scope_entry ] >>
- **Goal:** signaling of the scope semantics in the Access Token (see Section 7)

- **OLD Approach**
  - 1 CBOR tag is registered overall
  - 1 integer is registered and used for each semantics
  - Tag a CBOR sequence including the integer and scope

```
semantics = int
sequence = [semantics, scope] ; CBOR sequence
extended_scope = #6.TBD_TAG(<< sequence >>)
```

- **NEW Approach (was issue #144; thanks Christian!)**
  - 1 CBOR tag is used for each semantics
  - The tag may be already registered!
    - Tags associated to a CoAP Content-Format are automatically registered when registering that Content-Format (RFC 9277)
    - This happens when defining an AIF specific data model to use: new media-type parameters are defined for "Toid" and "Tperm" → a new CoAP Content-Format is registered

```
extended_scope = #6.TAG_FOR_THIS_SEMANTICS(scope)
```

# -key-groupcomm (3/4)

- **UPDATE 2:** When using AIF to express a scope, reduce restrictions for “Toid” encoding
- **Reminder: if AIF is used …**
  - scope_entry = AIF_Generic<gname, permissions>
  - scope = << [ + scope_entry ] >>
- **OLD TEXT in Section 3.1**
  - *… The object identifier "Toid" corresponds to the group name and MUST be encoded as a CBOR text string. The permission set "Tperm" …*
- **NEW TEXT in Section 3.1 // In practice, nothing changes for the scope of joining nodes**
  - *… If a scope entry expresses a set of roles to take in a group as per this document, the object identifier "Toid" specifies the group name and MUST be encoded as a CBOR text string, while the permission set "Tperm" …*
- ***draft-ietf-ace-oscore-gm-admin* extends the AIF specific data model from *-key-groupcomm-oscore***
  - An "admin" scope entry may have a “Toid” different from a CBOR tstr, to express a name pattern or wildcard

# -key-groupcomm (4/4)

- **Renaming of parameters**
  - get_pub_keys → get_creds
  - pub_keys_repos → creds_repo
  - pub_keys → creds
  - gm_dh_pub_keys → kdc_dh_creds
  - pub_key_enc → cred_fmt
  - pub_key → cred
  - gm_dh_pub_keys → kdc_dh_creds

- **Renaming of messages**
  - Public Key Request/Response → Authentication Credential Request/Response
  - KDC Public Key Request/Response → KDC Authentication Credential Request/Response
  - Public Key Update Request/Response → Public Authentication Credential Request/Response

- **Renaming of URI path segments (to resources at the KDC)**
  - GROUPNAME/pub-key → GROUPNAME/creds
  - GROUPNAME/kdc-pub-key → GROUPNAME/kdc-cred
  - GROUPNAME/nodes/NODENAME/pub-key → GROUPNAME/nodes/NODENAME/cred

# -key-groupcomm-oscore (1/2)

- **Version -14 submitted before IETF 114**
- **Adopted WGLC comments from Göran's review [3] – Thanks!**
  - Major reordering of document sections
  - The HKDF Algorithm is specified by the HMAC Algorithm value (like in RFC 8613)
  - Group communication is not necessarily IP over multicast
- **Revised the single AIF specific data model defined here, to enable the expression of:**
  - Roles of group members, as intended and defined in this document; OR
  - Permitted operations of an Administrator, as intended and defined in *draft-ietf-ace-gm-admin*
  - The two types of scope entry display a different rightmost bit in "Tperm" and can coexist
  - Agreed at IETF 113, during the presentation of *draft-ietf-ace-gm-admin*

[3] https://mailarchive.ietf.org/arch/msg/ace/SIB_rte0orqkvDEtTAw-1F7Cdzo/

# -key-groupcomm-oscore (2/2)

- **Version -15 submitted on 2022-09-05**
- **Alignment with renaming in *draft-ietf-ace-key-groupcomm***
  - Renamed parameters, messages and URI path segments (see slide 5)
  - Accordingly updated implementation at https://bitbucket.org/marco-tiloca-sics/
- **Updated text on optional signaling of scope semantics**
  - Using a dedicated CBOR tag (see slide 3)
  - We do register a CoAP Content-Format for the (Toid, Tperm) of this AIF data model, hence …
  - … a corresponding CBOR tag to use will be automatically registered, as per RFC 9277
- **If the DTLS profile is used between joining node and Group Manager …**
  - … and the Access Token is uploaded within a DTLS Handshake message, …
  - … clarified which field of which message carries the Access Token, depending on DTLS 1.2 or 1.3
- **Fixes to IANA registrations and editorial nits**

# Summary and next steps

- ***draft-ietf-ace-key-groupcomm***
  - No pending actions; waiting for the AD review.

- ***draft-ietf-ace-key-groupcomm-oscore***
  - Consistent with *draft-ietf-ace-key-groupcomm*
  - No pending actions; any further WGLC comment?

- **Francesca (CoRE AD): request publication of *draft-ietf-ace-key-groupcomm-oscore* with:**
  - *draft-ietf-core-groupcomm-bis* – In WG Last Call
    - To confirm that review comments were well addressed
    - Waiting for more minor comments to address
  - *draft-ietf-core-oscore-groupcomm* – Waiting for Shepherd write-up (and Shepherd review)
    - Pending action: work on a new version, to better specify the handling of response messages
    - This would **NOT** impact the content of *draft-ietf-ace-key-groupcomm-oscore*

# Thank you!

https://github.com/ace-wg/ace-key-groupcomm

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