Key Management for OSCORE Groups in ACE

Work in progress towards:

draft-ietf-ace-key-groupcomm-11

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

ACE Interim Meeting, April 13th, 2021

Updates since IETF 110 (1/3)

- Now captured in the Editor's copy
  - https://github.com/ace-wg/ace-key-groupcomm-oscore/tree/v-11

- Alignments with draft-ietf-core-oscore-groupcomm
  - Enable recycling of Group IDs (was issue #46)
  - Remove redundancies about key type capabilities (was issue #47)

- Recycling of Group IDs (GIDs) is now allowed to the Group Manager (GM)
  - When a node (re-)joins the group, it receives the GID used in the group
  - The GM stores that GID as the node's "Birth GID", until the node leaves the group
  - When rekeying the group and assigning a new GID*
    - The GM evicts also the nodes with GID* as their Birth GID (and rekeys the group accordingly)

Updates since IETF 110 (2/3)

- Removed redundacies about key type capabilities
  - To be stated only once, in the pertinent sets of parameters

General format	OLD CONTENT	NEW CONTENT	
sign_info_entry = [			Response from /authz-info
…			
sign_parameters : [any],	[[+sign alg capab], [+sign_key_type_capab]]	[+sign alg capab]	
sign_key_parameters : [any],	[+sign_key_type_capab]	[+sign_key_type_capab]	
…]			
ecdh_info_entry = [			
…			
ecdh_parameters : [any],	[[+ecdh alg capab], [+ecdh_key_type_capab]]	[+ecdh alg capab]	
ecdh_key_parameters : [any],	[+ecdh_key_type_capab]	[+ecdh_key_type_capab]	
…]			
key = {			Joining Response
…			
cs_params : [+item],	[[+sign alg capab], [+sign_key_type_capab]]	[[+sign alg capab], [+sign_key_type_capab]]	
cs_key_params : [+item],	[+sign_key_type_capab]	DELETED PARAMETER	
… }			

→ Take ‘cs_params’ and copy it in the OSCORE Security Context as is

Updates since IETF 110 (3/3)

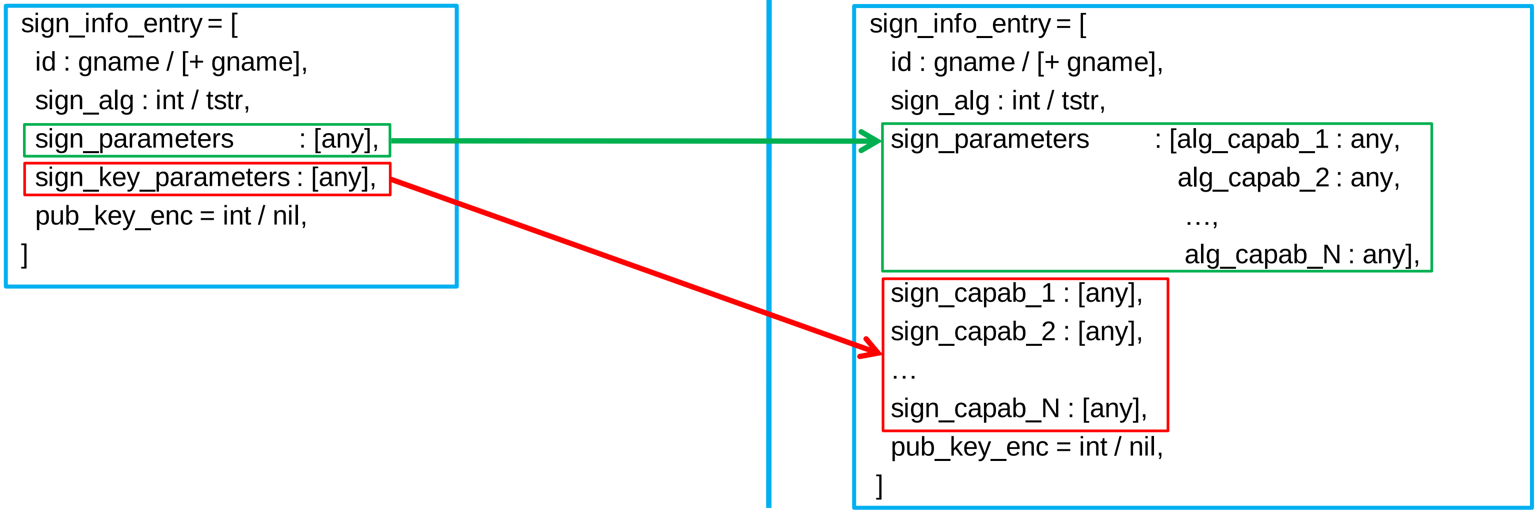
- Generalized format of parameters on COSE capabilities (was issue #48)
  - Current Appendix B in the Editor’s copy
  - Aligned with Appendix H of *draft-ietf-core-oscore-groupcomm*
  - Ready for future algorithms with more capabilities than the COSE Key Type
  - If applied to today’s algorithms, the result is just what already in the document body

- Consistency check – This affects:
  - Fields in the ‘key’ map of the Joining Response
    - Defined in this document → OK
  - ‘ecdh_info_entry’ in the response from /authz-info
    - Defined in this document → OK
  - ‘sign_info_entry’ in the response from /authz-info
    - Defined in *ace-key-groupcomm* → Open point

Open point

ace-key-groupcomm defines an ‘sign_info_entry’ as:

The **new generalized format** in *ace-key-groupcomm-oscore* is:



```
sign_info_entry = [
  id : gname / [+ gname],
  sign_alg : int / tstr,
  sign_parameters        : [any],
  sign_key_parameters : [any],
  pub_key_enc = int / nil,
]
```

```
sign_info_entry = [
  id : gname / [+ gname],
  sign_alg : int / tstr,
  sign_parameters        : [alg_capab_1 : any,
                            alg_capab_2 : any,
                             …,
                             alg_capab_N : any],
  sign_capab_1 : [any],
  sign_capab_2 : [any],
  …
  sign_capab_N : [any],
  pub_key_enc = int / nil,
]
```

- Option 1: add the following in *ace-key-groupcomm* when defining ‘sign_info_entry’

```
Profiles of this specification MAY define an alternative, extended format to use for each
'sign_info_entry', as including multiple elements between 'sign_parameters' and 'pub_key_enc', rather
than only 'sign_key_parameters' (OPT13). The alternative format must still provide all the required
information to successfully perform signing operations in the group, consistent with the algorithm
specified in 'sign_alg'.
```

- Option 2: have the generalized format of ‘sign_info_entry’ already in an appendix of *ace-key-groupcomm*

Thank you!