Work in progress towards

Key Provisioning for Group Communication using ACE
draft-ietf-ace-key-groupcomm-13

Key Management for OSCORE Groups in ACE
draft-ietf-ace-key-groupcomm-oscore-11

ACE WG Interim Meeting, June 8th, 2021

Since May interim meeting

- Submitted v -12 of *ace-key-groupcomm*
  - Now including the new Appendix B, to easily adapt to future COSE algorithms
  - Content removed from *ace-key-groupcomm-oscore* where initially defined

- Changes under discussion for Group OSCORE (*draft-ietf-core-oscore-groupcomm)*
  - These changes will have an impact on:
    - *ace-key-groupcomm* (KG)
    - *ace-key-groupcomm-oscore* (KGO)
    - *ace-oscore-gm-admin*
  - The discussion is converging, expect to apply changes in the following weeks
    - Most required changes to the ACE documents should be possible before the cut-off
    - The ACE implementation will also need to be fixed/extended

Expected changes (1/4)

- Group OSCORE will use an explicit format for public keys
  - E.g., list of CWT claims, certificates, … -– Aligned with recent design discussions for EDHOC
  - As identifiers of public key format, use (to-be-registered) values of COSE Header Parameters

- ➔ Both in KG and KGO
  - Still use ‘pub_key_enc’ to signal the used format of public keys in the group
    - Admit values from the list above, but not “plain COSE Key” anymore
  - Always use the already defined ‘peer_identifiers’ parameter
    - Indicate the node ID, as not specified in the public key itself

Expected changes (2/4)

- An OSCORE group can use the pairwise mode only
  - Never the case so far; the group mode with signatures was assumed as used for sure
- The same can apply to other types of security groups, not relying on signatures
- ➔ In KG, at Token POST/Response with the KDC, cover independently:
  - Possible exchange of information about the group operating in a signature-based mode
  - Possible exchange of information about the group operating in a non signature-based mode
- ➔ In KGO
  - Accordingly revise the inclusion and values of related parameters
  - Add parameters to reflect new upcoming additions specific to the Group OSCORE Security Context
    - Consistently, this will also affect the group creation/configuration in *draft-ietf-ace-oscore-gm-admin*

Expected changes (3/4)

- An OSCORE group can use the pairwise mode only
  - Never the case so far; the group mode with signatures was assumed as used for sure

- A new proof-of-possession for private keys is required, e.g. when joining
  - Nodes for this type of groups might not even support signatures altogether
  - Use a Diffie-Hellman proof-of-possession instead

- ➔ In KG, at Token POST/Response with the KDC:
  - Request also for the Diffie-Hellman public key of the KDC
  - 'client_cred_verify' of the Joining Request would include a MAC rather than a signature
    - The MAC is computed using a MAC key derived from a static-static Diffie-Hellman secret
    - The same applies when a group member uploads a new public key to the KDC

Expected changes (4/4)

- In the group mode of Group OSCORE, changes to the signature construction
  - Additional security assurances
  - Admit future encryption-only algorithms

- Concrete discussed direction
  - Have an “inner MAC” as additional element of the signing input, but not sent on the wire
  - The MAC is computed with a new Group MAC key

- ➔ In KGO
  - Add one more sub-resource at the GM, for authorized intermediaries like signature verifiers
  - The intermediary can retrieve the MAC key from that sub-resource at the GM, …
    - … and verify the signature like now, while still not able to access the plaintext

Next steps

- Need to do the required updates to *draft-ietf-core-oscore-groupcomm* first

- In the ACE drafts
  - Address as many points as possible before the July cut-off
  - Prioritize *draft-ietf-ace-key-groupcomm* over *draft-ietf-ace-key-groupcomm-oscore*

- Update the ACE implementation
  - OSCORE Group Manager and joining nodes

Thank you!