Key Management for OSCORE Groups in ACE

draft-ietf-ace-key-key-groupcomm-oscore-11

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

IETF 111, ACE WG, July 29th, 2021
Updates (1/4)

- An OSCORE group can work in three different ways
  - Only “group mode” (W1), only “pairwise mode” (W2), both modes (W3)

- Revised content of ‘key’ (e.g., in the Joining Response)
  - ‘sign_enc_alg’ is the encryption algorithm used in group mode
  - ‘alg’ is the encryption algorithm used in pairwise mode
  - Overall alignment with the new structure of the Security Context in Group OSCORE

- Revised proof-of-possesssion (PoP) of a node’s private key
  - The PoP evidence is a signature (W1)(W3) or a MAC (W2)
  - The MAC requires to compute a static-static DH secret with the node’s and GM’s key
  - Common single way to build the PoP input to be signed or MACed
Updates (2/4)

› Provisioning of the GM’s public key
  – Group OSCORE includes it in the external additional authenticated data of messages
  – In case of DH public key, possible early retrieval in the response to the Token POST
    › A joining node early needs it to compute the MAC PoP evidence for the Joining Request

› Proof-of-possession of the GM’s private key
  – Provided in the Joining Response, together with the GM’s public key
  – Same approach used for the PoP of a node’s private key
  – The PoP input is a nonce generated by the GM

› Used format of public keys in ‘pub_key_enc’
  – Any admitted by Group OSCORE and mapped in the COSE Header Parameters Registry
  – X.509/C509 certificates; CWTs; unprotected CWT claim set – Some to be registered
Updates (3/4)

› Revised and extended section on group rekeying
  – Better separation between general aspects and specific rekeying process to support
  – As per Group OSCORE, a rekeying indicates also the “stale Sender IDs”
    › Sender IDs relinquished due to a requested change or as belonging to a leaving node

› Tracking and maintenance of stale Sender IDs at the Group Manager
  – One set of stale Sender IDs per different Key Epoch (up to a pre-configured limit)
  – During a group rekeying, provide the most recent set (see above)
  – Allow to retrieve an aggregate set for the most recent Key Epochs
    › New sub-resource accessible by group members
    › Needed for group members that have missed one or more rekeying instances
Updates (4/4)

› Removed redundancy of key type capabilities
   – From the ‘sign_info’, ‘ecdh_info’ and ‘key’ parameters

› Enabled recycling of OSCORE Group IDs
   – By tracking the “Birth GID” got by each group member when joining the group
   – Aligned with what defined in draft-ietf-core-oscore-groupcomm

› Improved error handling
   – Also using ACE Group Error values introduced in draft-ietf-ace-key-groupcomm

› More examples of message exchanges with the Group Manager
Summary and next steps

- Version -11 is consistent and aligned with \textit{draft-ietf-core-oscore-groupcomm-12}

- Possible updates in Group OSCORE will likely require updates to this document
  - This document can be stable when Group OSCORE is stable – Hopefully in a few months

- Expected at least one more consistency update before WGLC
Thank you!

Comments/questions?

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