Key Management for OSCORE Groups in ACE

draft-ietf-ace-key-groupcomm-oscore-04

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

Interim, ACE WG, Feb 25, 2020

Updates since January interim

- Addressed Jim’s review (thanks!) – One open point left (see next slide)
  https://mailarchive.ietf.org/arch/msg/ace/Uz1BfItsJfbwsNKdAbn4WT_wm9I

- New security consideration section on sizes of nonces N_C and N_S – Issue #17

- Fixed incosistency when retrieving only group current keying material – Issue #18
  - The ’clientId’ field is not included in ’key’

- Clarified what is newly distributed during group rekeying – Issue #20

- The version number of the keying material is incremented regardless confirmation – Issue #21

- Included nonce N_S also in the error response to a Joining Request – Issue #22

- Explicit error handling for requests from monitor-only group members

- Usage of the client’s ‘control_path’ and the public key uploading interface, from *ace-key-groupcomm*

- Added new sub-resource and handler to retrieve the current group status (set as per *ace-oscore-gm-admin*)

TODO left

- Align with next updates of *ace-key-groupcomm*

- Enforce role of ”legal requester” (Jim proposal) – Discuss in Vancouver if no time today

Thanks!