# Group OSCORE - Secure Group Communication for CoAP

draft-ietf-core-oscore-groupcomm-08

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

IETF CoRE WG, Virtual Interim, April 8th, 2020

# Selected updates from -06

- Comments and reviews from Jim and Christian – Thanks!
  - Addressed specific comments from IETF 106
  - Addressed Jim's review of -06 [1]
  - Addressed Jim's review of -07 [2] (some open points left)
  - Addressed Christian's review of -07 [3] (some open points left)

[1] https://mailarchive.ietf.org/arch/msg/core/UEXWZLXP6VnpykN-C7A-Z0qYWxY/
[2] https://mailarchive.ietf.org/arch/msg/core/GdqlGpoLBi-2Q61N_iQeqXC5UL4/
[3] https://mailarchive.ietf.org/arch/msg/core/-F9oo5lIo6TuZHv-6-vVCpFTd5k/

# Selected updates from -06

- Message processing across group rekeying
  - Responses always protected with the latest keying material
  - A response may be processed with a different context than the request
  - Include server's 'Partial IV' and new 'kid_context'

- Support for Observe
  - Dedicated sections for requests and response processing
  - The client 'kid' from the original Observe request is stored for reference

- Using group keying material for unicast requests: NOT RECOMMENDED
  - An external adversary can redirect the request to the group or a different server
  - Bad especially for non-safe methods; impact on Echo option and Block-wise

# Three modes of operations

- Three different protecting modes
  - **Signature mode** – Main and usual mode
    - Encryption with group keying material; signature included
  - **Optimized/Hybrid mode** – Section 9
    - Request: encryption with group keying material; stripped MAC; signature included
    - Response (*): encryption with derived pairwise keying material; no signature
  - **Pairwise mode (*)** – Appendix G
    - Encryption with derived pairwise keying material; no signature

(*) Not for use cases with an intermediary that verifies signatures

# Pairwise keys

- Key derivation
  - Same construction from 3.2.1 of RFC 8613
  - **Pairwise key = HKDF(Sender/Recipient key, DH shared secret, info, L)**
    - Sender Key of the sender node, i.e. Recipient Key of the recipient side
    - Static-static DH shared secret, from one's private key and the other's public key
  - Compatible with ECDSA and EdDSA (with mapping to Montgomery coordinates)

- New Pairwise Flag bit in the OSCORE option
  - Set to 1 if the message is protected with pairwise keying material
    - Optimized/Hybrid mode – Responses only
    - Pairwise mode – Requests and responses

# Open points

- Sender Sequence Number (SSN). Reset after rekeying?
  - Reset (as in OSCORE)
    - Pro: maximum lifetime of SSN, at each key epoch
    - Con: observations have to terminate after rekeying.
  - Don't reset --- Default behavior, app policies may override
    - Pro: observations can continue throughout a rekeying
    - Con: non-maximum lifetime of SSN, at each key epoch

- Optimized/hybrid mode
  - Concerns from Jim and Christian
  - Move to an appendix, and only about the optimized request
  - Instead, move the pairwise mode up in the document body

# Open points

- Normative statements on the modes. Proposal:
  - Signature mode MUST be supported
  - Pairwise mode MAY be supported
    - MUST be supported if Echo and/or Block-wise is supported
  - Applications can protect a request in one mode, and responses in another mode

- (a) OSCORE; (b) Group OSCORE in pairwise mode. Difference for a node?
  - a) Multiple full context establishments, on the wire
  - b) 1 full context establishment on the wire, through the Group Manager
    - Derivations of Recipient Contexts happen locally and when needed
  - The difference is about key management.
  - Add considerations about this in the section on pairwise mode?

# Open points

- Use of the pairwise mode in the group
  - Signaled as a group policy?

- Does the pairwise flag bit have a more general applicability? (Christian)
  - Thought about it with Group OSCORE in mind. No further obvious meanings.

- Should we flip the value of the pairwise flag bit? (Christian)
  - 0: Group OSCORE pairwise mode; same for OSCORE
  - 1: Signature mode
  - Need to (easily) update implementations

# Open points

- Error handling on not supporting the pairwise mode
  - Not so much to do on the client
  - The server can respond with an error, possibly with diagnostic information
  - Issues with that?

- Group ID in all notifications following a rekeying (Jim)
  - The client has two observations with the server
    - One observations with CTX1, one observation with CTX2
  - The server uses the same ‘kid’ in both CTX1 and CTX2
  - Is this really an issue?
    - The two observations started with two different requests, with different tokens
    - Tokens are associated to security contexts

# Open points

- Appendix E.2 – “Baseline” synchronization of Client’s Sequence Number
  - First request to be accepted or not by the server? (Christian, Jim)
- For the pairwise mode, the client has to know
  - Address, ‘kid’, and public key of the server
  - Generic discovery mechanisms in Appendix G.1. Good enough?
- Silent servers supporting the pairwise mode
  - Need to have a public key and a ‘kid’ as its identifier
  - These silent-server-only provide a public key, and get a Sender ID. Issues with that?
- Remove IANA registries on signature params and key params
  - Point at the recently extended registries in *cose-rfc8152bis-algs-07*
- Considerations on what should be done after reboot. New Appendix?

# Next steps

- Close open points
  - From Jim's and Christian's review of -07
  - Other pending issues raised today
  - From Jim's review of -08 [1] – Thanks!

- Test message protection in pairwise mode

- Once done, move to WGLC ?

[1] https://mailarchive.ietf.org/arch/msg/core/kmh1KjqEsR156m7EZ4yawaJnaG8/

# Thank you!

# Comments/questions?

https://github.com/core-wg/oscore-groupcomm