Group OSCORE - Secure Group Communication for CoAP

Towards *draft-ietf-core-oscore-groupcomm-14*

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

CoRE WG interim meeting, January 19, 2022

Since IETF 112

- Version -13 completed the 2nd WGLC
- Review from Esko – Thanks a lot
  - Main comments [1]
  - Editorial comments [2] – Already addressed and in the GH Editor's copy
- One more review expected from Rikard
- Some points from [1] selected for discussion today

[1] https://mailarchive.ietf.org/arch/msg/core/7aOZ4YXBI0IvCBOYlHOftDzuCVY/

[2] https://mailarchive.ietf.org/arch/msg/core/nCJ86EjuZg1ajsjE559RmkBlW84/

Format and storage of public keys

- Need to clearly distinguish between:
  - **“Authentication credential”** : to derive pairwise keys ; to fill the external_aad
    - X.509/C509 certificates, CWT, CCS, … as including a public key
  - **“Public key”** : to verify signatures ; to derive Diffie-Hellman secrets
- “Authentication credentials” have to be fully stored to be used as a whole
  - They carry on key metadata (signature algorithm, issuer, subject, key use, expiration, …)
  - All endpoints see and use the same byte blob, as from the original issuer
- Trade-off between storage and complexity/flexibility/feasibility
  - Avoid to define a relevant subset of metadata to store (for current and future credentials)
  - Avoid to define a common canonical encoding for the relevant subset of metadata
- **Proposal**: keep storage of whole credentials; clarify the trade-off

Objections?

The “Birth Gid”

- When an endpoint X joins a group, it obtains the current Group ID, say G1
  - From then on, G1 will be the Birth Gid of X
- The Group Manager may rekey the group, thus changing Group ID
  - Eventually the Group Manager will start reassigning past Group ID values
  - If, upon rekeying, the new Group ID is the Birth Gid of X, then X is evicted from the group
- Why does this help and how?
  - X will re-join the group, thus terminating its possible (very very long-)living observations
  - “*This ensures that an Observe notification [RFC7641] can never successfully match against the Observe requests of two different observations.*”
- A step-by-step example was not included, as more about design considerations
  - Should we include a more detailed explanation? As part of the security considerations?

Implementation requirements

- Section 10 – “Mandatory-to-Implement Compliance Requirements”
- One would expect only “is mandatory to…” and MUST/SHALL statements
- A lot of SHOULD/RECOMMENDED and non-normative statements are used
  - And that is still the intented meaning of the text
- **Proposal**
  - Change the section title to “Implementation Compliance”
  - Its content is still also about MTI requirements, but not only

Objections?

Right type of reference

- *draft-mattsson-cfrg-det-sigs-with-noise* // Now an informative reference
  - On how to introduce randomness in deterministic signatures
- Now RECOMMENDED to implement when using elliptic curve signatures
- Note: signatures remain compatible with unmodified ECDSA/EdDSA verifiers
- **Proposal**
  - Keep the reference informative and do one of the following:
    1. Change “RECOMMENDED” to “recommended”; or
    2. Preferably, rephrase to say, e.g.: “If elliptic curve signatures are used, it is **RECOMMENDED** for deployments where side channel and fault injection attacks are a concern **to implement deterministic signatures with additional randomness**, **for example by using the constructions specified in [I-D.mattsson-cfrg-det-sigs-with-noise]**.”

Objections?

Preference?

Right type of reference

- *draft-ietf-ace-key-groupcomm-oscore* // Now an informative reference
- Specification of a Group Manager as an ACE Resource Server
- Now referred to as RECOMMENDED Group Manager to use (3 occurrences)
- **Proposal**
  - Keep the reference informative
  - Relax the text referring to the ACE draft
    - Point to the ACE Group Manager as a possible one to use
    - Still mention that the ACE draft provides a join process and a group rekeying process

Objections?

Right type of reference and section

- *draft-ietf-core-echo-request-tag* // Now an informative reference

- Appendix E – “Challenge-Response Synchronization”
  - Echo option to re-synch with a Client’s Sender Sequence Number
  - Possible approach, analogous to OSCORE Appendix B.1.2 but for groups

- The use of Echo as in Appendix E plays a bigger role
  - Section 2.5.1.2 has it as RECOMMENDED method (though not the only one) to make Replay Windows valid again, following an overloading of Recipient Contexts

- **Proposal**
  - Make the reference normative
  - Move current Appendix E to the document body

Objections?

Next steps

- Process Esko’s review
- Process more comments as they come
- Submit v -14 for IETF 113

Thank you!

Comments/questions?

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