Group OSCORE - Secure Group Communication for CoAP

draft-ietf-core-oscore-groupcomm-13

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

IETF 112, CoRE WG, November 8th, 2021

Update since IETF 111

- Version -13 submitted

- Terminology on formats of public keys
  - UCCS → CCS (CWT Claims Set)
  - Sufficient to refer to RFC 8392
  - Same as in *draft-ietf-lake-edhoc*

- Group Mode: fix in the derivation of the “Group Encryption Key”
  - Used for generating a keystream, to separately encrypt the message signature
  - Now the right key size is indicated in the key derivation step

Update since IETF 111

- Updated Section 10 on MTI compliance requirements
  - Constrained devices might not be able to support multiple signature algorithms
  - Goal: enable as much interoperability as we can reasonably achieve
  - Now following the same rationale of *draft-ietf-lake-edhoc*

If supporting the Group Mode

- Less constrained endpoints SHOULD implement both: the EdDSA signature algorithm with elliptic curve Ed25519; and the ECDSA signature algorithm with elliptic curve P-256.
- Constrained endpoints SHOULD implement: the EdDSA signature algorithm with elliptic curve Ed25519; or the ECDSA signature algorithm with elliptic curve P-256.

If supporting the Pairwise Mode

- Less constrained endpoints SHOULD implement both ECDH curves X25519 and P-256.
- Constrained endpoints SHOULD implement the X25519 or P-256 curve as ECDH curve.

Next steps

- No open issues or open points we are aware of
  - Recently closed 4 Github issues, 3 of which already addressed in v -12
- Updated implementation for Eclipse Californium
- Ready for the 2nd WGLC
- Started to produce test vectors, for both group mode and pairwise mode
  - Appendices to this draft would be pretty long. Alternative release venue?
    - Just a CoRE Github repo?
    - Separate informational draft, as in LAKE? Should it be published as RFC?

Thank you!

Comments/questions?

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