Cacheable OSCORE

`draft-amsuess-core-cachable-oscore-11`

Christian Amsüss, Marco Tiloca

2025-07-22, CoRE at IETF123 / Madrid

Context

- CoAP: REST! Proxies!
- OSCORE: Proxies fragment and retransmit but do not cache.
- Cacheable OSCORE: … but maybe we can.

←: ietf-core-oscore-groupcomm (in Last Call)

→!: tiloca-t2trg-sw-update-groupcomm, ietf-core-observe-multicast-notifications[1]

→?: core-dns-over-coap, ietf-core-groupcomm-proxy, …

[1] Aspirationally.

WHAT WILL IT COST?
~~EVERYTHING~~

Security properties lost

1. Replay protection.
2. Source authentication on the request.
3. Freshness is limited.
4. Request privacy is limited.

Document structure

Sections, as presented at IETF112

2. What happens to OSCORE when source authentication is missing?
3. Deterministic requests:
    - Building requests with best-effort determinism.
    - Initializing key material that won't suffer nonce reuse.
    - Request-response binding as per 2.

Mechanics

Based on Group OSCORE

1. Establish Group OSCORE membership.

   GM indicates Sender ID of The Deterministic Client in extra field.

2. Prepare COSE Encrypt0 (no key yet).
3. Hash all inputs.
4. Derive key like pairwise, but use hash instead of ECDH output.
5. Send pairwise-ish request.
6. Response in group mode, request-bound by invisible Class-I option.

What is missing?

- Which AEAD algorithms are deterministic? All current.
- Extra pair of eyes on security (e. g. on whether constant-time is needed anywhere).
- Does anyone need more of Section 2?

Status

Successful interop between Californium and aiocoap implementations.
Test vectors present.

Working Group Adoption call is still open.

Questions? Reviewers?