Cachable OSCORE

draft-amsuess-core-cachable-oscore

Christian Amsüss, Marco Tiloca

2020-11-05
Background

multicast-notifications

Comparison with ICNs

OSCON
Focus today

deterministic requests

(Token requests are really just motivation and history)
Concrete Example

FETCH /

OSCORE:
   kid=client
   Partial IV=0
   KID Detail={Hash of CoAP encoding of plaintext, AAD and symmetric key}

Payload: Ciphertext plus tag of
   GET /temperature
   Accept: 112
Prerequisites

- Group set up with two members (server and client).
  - Client a bit special (next slide)

- AEAD algorithm is deterministic (Flag in COSE registry).

- The key is only ever used to encrypt this very message.
  - KID details goes in there, no variability in AEAD left.

- All clients generate same request ("Accept"?)

Out of scope.
What's actually new?

▶ “KID Detail”

Like KID Context; also goes into the salt, new extension bit.

▶ “Look Ma, no signature.”

Yes, this has no source authentication.

Precise discussion that led to that requirement?

Shipping a public key would just be avoiding the argument, better talk it out now than in a year.

Technically, this one participant uses the signature algorithm 0.
Afterthought: Possible further optimization

OSCORE is cache-key

OSCORE option with this flag set could be used as *standalone* short-hand into cache:

```
FETCH / OSCORE={...}
```

4.00 Bad Request "too short to even have a tag"

```
FETCH / OSCORE={...} Payload=ciphertext
```

2.05 Content and data