Stateless OSCORE

draft-amsuess-core-stateless-oscore

Christian Amsüss

IETF121 Dublin, LAKE, 2024-11-05

NTP can do it.

So I was curious.

What

Arbitrary number of clients can have security contexts with a server, while server's memory is constant.

How

- Server keeps a long-term secret internal key.
- For each new client, server assigns an incremented Recipient ID.
- Master Secret is `hash(internal key | recipient ID)`.
- Server treats all requests like 0-RTT requests.

Limits

- Only GET & FETCH[1].
- Key must be sent, not agreed on.
- Server's sender sequence number counts *all* uses[2].

[1] Only safe methods. Or at least operations where reordering is absolutely tolerated.

[2] Can be stretched by having a sequence number for shards of derived keys

Future

Maybe a -01-trick pony.

Talk to me if you would like to have it usable.