



Comparison of CoAP Security Protocols

draft-ietf-iotops-security-protocol-comparison-07

Preuß Mattsson, Palombini, Vučinić

Current status

- Comments by Marco Tiloca and Thomas Fossati will be fixed in -08 shortly after IETF 121 Dublin:
 - *"I have reviewed this document and I think it's largely ready. Please find below some suggestions for rephrasing, clarifications, and minor fixes."*
 - *"I have reviewed -06 with a focus on the (D)TLS parts and it looks good to me. Nits:"*
- Suggested at IETF 119 to publish together with cTLS.
 - Not much cTLS activity on the TLS list ...
- 07 added a reference to a new relevant draft is "Large Record Sizes for TLS and DTLS with Reduced Overhead", which is currently in TLS WG adoption call. Not added to tables.

Protocol	Overhead	Overhead (GHC)
DTLS 1.2	21	8
DTLS 1.3	3	4
TLS 1.2	13	9
TLS 1.3	6	7
TLS 1.3 Reduced (WIP)	3	4
OSCORE request	5	
OSCORE response	3	