COSE WG
TSA-TST Header Parameter

Henk Birkholz <henk.birkholz@ietf.contact>

IETF120 Vancouver, 23rd July

Emergency Presenter:

Carsten Bormann <cabo@tzi.org>

Usage (I)

https://datatracker.ietf.org/doc/draft-ietf-cose-tsa-tst-header-parameter/

- COSE Header parameter for RFC 3161 Time-Stamp Tokens
- For COSE Signing (i.e., COSE_Sign and COSE_Sign1)
- Two modes:
  - Time-Stamp, then COSE (TTC)
  - COSE, then Time-Stamp (CTT)

Usage (II)

https://www.ietf.org/archive/id/draft-ietf-cose-tsa-tst-header-parameter-02.html#section-2.1

- Time-Stamp then COSE (TTC)

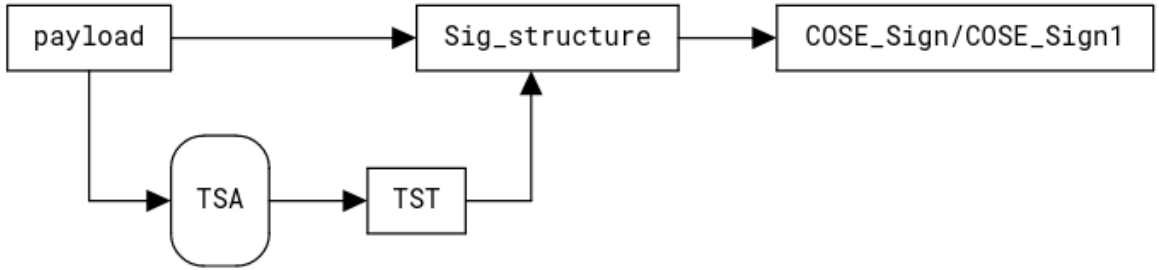

Figure 1: Timestamp, then COSE (TTC)

IETF

Usage (III)

https://www.ietf.org/archive/id/draft-ietf-cose-tsa-tst-header-parameter-02.html#section-2.2

- COSE then Time-Stamp (CTT)

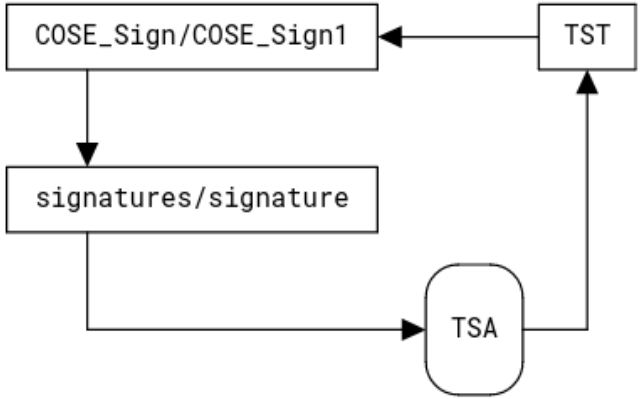

Figure 2: COSE, then Timestamp (CTT)

IETF

WGLC

- Added some nuances on "leaking" a payload identifier in the TTC sequence to the Security Consideration Section
- The Editors think this I-D is ready for WGLC