

COSE Header parameter for RFC 3161 Time-Stamp Tokens

Henk Birkholz

draft-birkholz-cose-tsa-tst-header-parameter@ietf.org

IETF 116

17 March 2023

Yokohama



RFC 3161 TST COSE Header Parameter Recap

- <https://datatracker.ietf.org/doc/html/draft-birkholz-cose-tsa-tst-header-parameter-01>
- Using the output of an RFC 3161 Time Stamp Authority (TSA) in COSE headers
- A hash of the byte string used to create the COSE signature is used as input to the TSA to retrieve a corresponding TimeStampToken (TST).
- New header parameter NAME: let the working group decide
- New header parameter VALUE: one (or more?) DER-encoded RFC 3161 TimeStampToken byte strings

Next Steps

- Request for WG adoption call (WGAC)