Header Parameters for Carrying and Referencing Chains of CBOR Web Tokens (CWTs)

draft-tschofenig-cose-cwt-chain-00

Brendan Moran, Hannes Tschofenig

Overview

- RFC 9360 defines
  - references to X.509 certificates and,
  - header parameters to carry chains of X.509 certificates.
- draft-tschofenig-cose-cwt-chain-00 does the same but for CWTs instead of X.509 certificates.
- Why?
  - Some applications use CWTs
  - Functionality was previously in SUIT specification

Constraints

- Defined for CWTs that carry a "confirmation" claim, defined in RFC 8747, used to carry the public key and the algorithm with which the key is used.

Parameters defined

- cwt-bag: unordered list of CWTs
- cwt-chain: ordered list of CWTs
- cwt-t: identifies the end entity CWT by a hash value (a thumbprint)
- cwt-u: provides the ability to identify a CWT by a URI

- Extra: algorithm-specific parameters that are used for identifying or transporting the sender's key for static-static key agreement algorithms.

Summary and Next Steps

- Wanted to keep the functionality as simple as possible for supporting the firmware/software update use cases.
- This document generalizes the work.