# Misc. COSE Topics

COSE WG interim, October 12, 2021

# Topics for discussion

- draft-ietf-cose-rfc8152bis-struct: Extend ‘kid’ to int
- draft-ieft-cbor-encoded-cert: Looking for reviews
- Potential new draft: cose-x509-like draft for CWTs
- draft-ietf-cose-x509: Usage of x5*-sender

# Extend ‘kid’ to int, PR #34

- RFC 8152 defines ‘kid’ as bstr
- Beneficial to extend ‘kid’ to also support value type int
- Mail thread starting with

https://mailarchive.ietf.org/arch/msg/cose/WUVutFNTVHd5m45xzS5mXPjwWsM/

- PR #34
  - Common header params
  - COSE Key

| Name | Label | CBOR Type | Value Registry | Description |
|---|---|---|---|---|
| kty | 1 | tstr / int | COSE Key Types | Identificati the key type |
| kid | 2 | bstr / int | | Key identifi value -- mat kid in messa |
| alg | 3 | tstr / int | COSE Algorithms | Key usage restriction this algorit |

# draft-ieft-cbor-encoded-cert

- The base specification of C509 is stable
- Last update was IETF 111
  - New supported extensions
  - CSRs and CRLs
  - Rust code in github repo [1]

- Reviews?

[1] https://github.com/cose-wg/CBOR-certificates/tree/master/c509

# CWT as authentication credential in COSE

- LAKE defines COSE header parameters for CWTs and CWT Claims Sets [1]:
  - CWTs containing a COSE key in a 'cnf' claim (RFC 8747)

| Name | Label | Value Type | Description |
|---|---|---|---|
| kcwt | TBD1 | COSE_Messages | A CBOR Web Token (CWT) containing a COSE_Key in a 'cnf' claim |
| kccs | TBD2 | map / #6(map) | A CWT Claims Set (CCS) containing a COSE_Key in a 'cnf' claim |

- Do we need to specify more general use of CWT as authentication credential?
  - The analogue of draft-ietf-cose-x509 but using CWT instead of X.509

[1] https://datatracker.ietf.org/doc/html/draft-ietf-lake-edhoc-11#section-9.6

# Usage of x5*-sender

- cose-x509 distinguishes between COSE header parameters for sender and recipient
  - based on what kind of COSE object the header goes into (Section 2):
    - "COSE_Signature and COSE_Sign1 objects:
      in these objects the identify the certificate to be used for validating the signature.
    - COSE_recipient objects:
      in this location they identify the certificate for the recipient of the message."

- Section 3:
  - "The header parameters defined in the previous section are used to identify the recipient certificates for the ECDH key agreement algorithms. In this section we define the algorithm specific parameters that are used for identifying or transporting the sender's key for **static-static key agreement algorithms**."

- Why is this limited to static-static?

# Usage of x5*-sender

— Tables 1 & 2 in draft-ietf-cose-x509:

| | | | |
|---|---|---|---|
| | | | X.509 certi |
| x5chain | TBD3 | COSE_X509 | An ordered X.509 certi |
| x5t | TBD1 | COSE_CertHash | Hash of an certificate |
| x5u | TBD2 | uri | URI pointin X.509 certi |

Table 1: X.509 COSE Header Parameters

Table 2: Static ECDH Algorithm Values

| Name | Label | Type | Algorithm | Description |
|---|---|---|---|---|
| x5t-sender | TBD | COSE_CertHash | ECDH-SS+HKDF-256, ECDH-SS+HKDF-512, ECDH-SS+A128KW, ECDH-SS+A192KW, ECDH-SS+A256KW | Thumbprint for the senders X.509 certificate |
| x5u-sender | TBD | uri | ECDH-SS+HKDF-256, ECDH-SS+HKDF-512, ECDH-SS+A128KW, ECDH-SS+A192KW, | URI for the senders X.509 certificate |