COSE Key Thumbprint

draft-ietf-cose-key-thumbprint

Kohei Isobe
Hannes Tschofenig
Orie Steele
Since IETF117

• Update: Supporting Symmetric Keys
  • Security Consideration enhanced

• New: CWT Confirmation Method

• New: COSE Key Thumbprint URI

Implementations updated.
Supporting Symmetric Keys

• Definition of Symmetric Key Objects for calculating Thumbprint
  • The required parameters for a symmetric key are:
    "kty" (label: 1, data type: int, value: 4)
    "k" (label: -1, data type: bstr)

• Security Consideration
  • Low-entropy enables attackers to guess symmetric keys.
  • Solution: Symmetric key must have enough entropy!
CWT Confirmation Method

• RFC 8747 Proof-of-Possession Key Semantics for CBOR Web Tokens (CWTs) defines `cnf` claim to convey key information for confirmation.
  • Currently 3 Confirmation Methods are defined and registered in IANA registry.
    • COSE_Key, Encrypted_COSE_Key, kid

• Add COSE Key Thumbprint as confirmation method
  • Define `ckt` as a new confirmation method.

```json
{
  /iss/ 1 : "coaps://as.example.com",
  /aud/ 3 : "coaps://resource.example.org",
  /exp/ 4 : 1361398824,
  /cnf/ 8 : {
    /ckt/ [[TBD1]] : h'496bd8afadfl307e5b08c64b0421bf9dc01528a344a43bda88fadd1669da253ec'
  }
}
```
COSE Key Thumbprint URI

urn:ietf:params:oauth:ckt:sha-256:SWvYr63zB-WwjGSwQhv53AFSijRKQ72oj63RZp2iU-w

• Based on JWK Thumbprint URI (RFC 9278)
  • ckt
    • Prefix for COSE Key Thumbprint URI

• Hash Algorithm
  • Choose from IANA Named Information Hash Algorithm Registry

• Value
  • Base64url-encoded COSE Key Thumbprint bstr
Comparison with JOSE Functionality

Both support symmetric and asymmetric keys.

COSE and DPoP define jkt and ckt claims respectively.

JWK and COSE Key define the prefix ‘jwk-thumbprint’ and ‘ckt’ respectively.

- COSE Key Thumbprint (This I-D)
- JWK Thumbprint (RFC 7638)
- OAuth 2.0 DPoP (RFC 9449)
- JWK Thumbprint URI (RFC 9278)
Next Steps

• Document shepherded by Mike.
• Ready for the IESG