COSE WG draft status

IETF 113
March 21, 2022

Ivaylo Petrov

Bis drafts

- RFC 9052-to-be and 9053-to-be
  - Ben Kaduk has been leading most discussions
  - A few topics to discuss, but mostly need a consistency check

Bis drafts

- RFC 9052-to-be
  - Ben Kaduk has been leading most discussions
  - One open point: Table 5 in Sec 7.1:

    Require private key in Key Operation Values

    - Expected to be consistent with RFC 7517 and W3C's WebCrypto
    - Neither has such restrictions

Name	Value	Description
sign	1	The key is used to create signatures. Requires private key fields.
verify	2	The key is used for verification of signatures.
encrypt	3	The key is used for key transport encryption.
decrypt	4	The key is used for key transport decryption. Requires private key fields.
wrap key	5	The key is used for key wrap encryption.
unwrap key	6	The key is used for key wrap decryption. Requires private key fields.
derive key	7	The key is used for deriving keys.
derive bits	8	The key is used for deriving bits not to be used as a key.
MAC create	9	The key is used for creating MACs.
MAC verify	10	The key is used for validating MACs.

Table 5: Key Operation Values

Bis drafts

- RFC 9053-to-be
  - Ben Kaduk has been leading most discussions
  - Orig:

    Some situations have been identified where identification of capabilities of an algorithm or a key type needs to be specified.

The capabilities of an algorithm or key type need to be specified in some situations. One example of this is in [OSCORE-GROUPCOMM], where the capabilities of the countersignature algorithm are mixed into the process of traffic-key derivation. This has a counterpart in the S/MIME specifications, where SMIMECapabilities is defined in Section 2.5.2 of [RFC8551]. This document defines the same concept for COSE.

Bis drafts - Comments from Carsten

- Unclear text - now fixed

  If
  the message is not rejected as malformed, attributes MUST be obtained
  from the protected bucket, and only if not found in the unprotected
  bucket.

- Inconsistent text between 9052 and 9053 - to be fixed

  structures. CBOR was designed specifically to be small in terms of
  both messages transported and implementation size and be/have a schema-
  free decoder. A need exists to provide message security services for

- CDDL is not grammar, but ***standard definition language for CBOR data structure***
  - Affects both RFC-to-be 9052 and 9053

Bis drafts - Comments from Carsten

Sec 9 in both documents

Orig:

Encoder needs to work. The new encoding restrictions are aligned with the deterministically encoded CBOR requirements specified in [STD94]. It has been narrowed down to the following restrictions:

New:

The new encoding restrictions are aligned
with the Core Deterministic Encoding Requirements
specified in Section 4.2.1 of
[STD94].

hash-algs

Final pass by Ben/AD and it should be ready for publication.

x509

- Published a new version of the draft as previously discussed
- issue #31: https://github.com/cose-wg/X509/issues/31

Countersignatures

With Roman Danyliw - awaiting AD review.

CBOR Encoded X.509 Certificates

- More reviews are needed
- Some small TODOs are still pending