Workgroup: CBOR Object Signing and Encryption
Internet-Draft:
draft-bormann-cose-registration-principles-00
Published: 24 July 2023
Intended Status: Informational
Expires: 25 January 2024
Authors: C. Bormann
Universität Bremen TZI

# COSE: On Registration Principles

## Abstract

COSE (STD 96, RFC 9052 and RFC 9338) defines a number of registries that allow registrants to exercise the numerous extension points defined in COSE. Section 11.6 of RFC 9052 gives the Designated Experts for these registries considerable leeway in deciding about registration requests.

The present document is intended to collect information that has been the basis for initial population of and further registration in these registries. It is intended to be shaped by the Designated Experts and serve them as a collective memorandum and a checklist. As a secondary function, it is also intended to help registrants create registrations that are acceptable to the Designated Experts.

Revision -00 of this draft is an early skeleton that should allow us to decide whether such a collection of information is useful and whether we want to flesh out this document.

## About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-bormann-cose-registration-principles/.

Discussion of this document takes place on the CBOR Object Signing and Encryption (COSE) Working Group mailing list (mailto:cose@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/cose/. Subscribe at https://www.ietf.org/mailman/listinfo/cose/.

Source for this draft and an issue tracker can be found at https://github.com/cabo/cose-regprin.

## Status of This Memo



## Copyright Notice



## Table of Contents

## 1. Introduction

COSE (STD 96, RFC 9052 and RFC 9338) defines a number of registries that allow registrants to exercise the numerous extension points defined in COSE. Section 11.6 of RFC 9052 gives the Designated Experts for these registries considerable leeway in deciding about registration requests.

Specifically, Section 11.6 of [RFC9052] says:

> 11.6. Expert Review Instructions
>
> All the IANA registries established by [RFC8152] are, at least in part, defined as Expert Review [RFC8126]. This section gives some general guidelines for what the experts should be looking for, but they are being designated as experts for a reason, so they should be given substantial latitude.

([RFC8152] is the previous edition of what is now RFC9052 and [RFC9053]; this document established the registries being discussed, which together make up the [IANA.cose] registry group.)

The further text of Section 11.6 of [RFC9052] gives instructions about the general operations of the registries, but does not discuss the architectural and structural principles that might go into a registration decision.

The present document is intended to collect information that has been the basis for initial population of and further registration in these registries. It is intended to be shaped by the Designated Experts and serve them as a collective memorandum and a checklist. As a secondary function, it is also intended to help registrants create registrations that are acceptable to the Designated Experts.

Revision -00 of this draft is an early skeleton that should allow us to decide whether such a collection of information is useful and whether we want to flesh out this document.

### 1.1. Conventions and Definitions

The definitions of [STD94] and [STD96] apply.

## 2. COSE Registration Principles

This section is a skeleton and needs to be fleshed out.

At the time of writing, some 172 registrations have been made in the COSE registry group [IANA.cose]. These can serve as a body of examples how to make registrations. Unfortunately, not all registrations in this set demonstrate outstanding consistency in

decision-making, so this section will also collect information about where existing registration decisions turned out to be suboptimal or at least different in structure than registrations of a similar nature.

### 2.1. General Considerations

**Code Point Frugality:** COSE is designed to work in environments where at least some of the devices have limited resources; curation of codepoints so that the ones that are most frequently used with such constrained devices receive the codepoints with the shortest representation (and can continue to do so over a number of decades) is always an objective.

### 2.2. COSE Header Parameters

...

### 2.3. COSE Header Algorithm Parameters

...

### 2.4. COSE Algorithms

Algorithm identifiers in these registrations have a *Recommended* Tag, which indicates (Section 16.4 of [RFC8152]):

> **Recommended:** Does the IETF have a consensus recommendation to use the algorithm? The legal values are 'Yes', 'No', and 'Deprecated'.

Note that an algorithm can be *deprecated* already at registration time. This value was used in the registration of the [I-D.ietf-cose-aes-ctr-and-cbc] values which only can be used under very specific conditions.

Algorithm identifiers are usually assigned so that a single identifier stands for a collection of underlying algorithms, with main parameters such as key or hash length chosen, so that a single algorithm identifier suffices to fully characterize the cryptographic operations. A key is the obvious exception, but also parameters that go with a key such as its curve type.

Where a certain underlying algorithm has a small number of possible parameter sets, all registrations for the use of that underlying algorithm in a COSE Algorithm are made at the same time. For instance: A128GCM (AES-GCM mode w/ 128-bit key, 128-bit tag) we registered together with A192GCM (AES-GCM mode w/ 192-bit key, 128-bit tag) and A256GCM (AES-GCM mode w/ 256-bit key, 128-bit tag). The expert (in this case the author of [RFC9053]) did not make separate

assessments how useful or desirable the individual parameter sets were going to be, but registered them all at once. When the collection of AES-CCM-16-64-128, AES-CCM-16-64-256, AES-CCM-64-64-128, and AES-CCM-64-64-256, as well as AES-CCM-16-128-128, AES-CCM-16-128-256, AES-CCM-64-128-128, and AES-CCM-64-128-256 were registered, these were also registered all at once, but grouped into two groups with different representation sizes of the algorithm identifier.

### 2.5. COSE Key Common Parameters

...

### 2.6. COSE Key Type Parameters

...

### 2.7. COSE Key Types

...

### 2.8. COSE Elliptic Curves

This registry is governed by similar principles as the COSE Algorithms registry (Section 2.4). Curve types identify all parameters of a curve and are registered all at once where natural groups of such types exist.

## 3. Security Considerations

This document is about registrations in registries that have direct security impact; security considerations that require discussion beyond that are mentioned in the discussions above.

## 4. IANA Considerations

This document has no IANA actions.

## 5. Informative References

**[I-D.ietf-cose-aes-ctr-and-cbc]** Housley, R. and H. Tschofenig, "CBOR Object Signing and Encryption (COSE): AES-CTR and AES-CBC", Work in Progress, Internet-Draft, draft-ietf-cose-aes-ctr-and-cbc-06, 25 May 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-aes-ctr-and-cbc-06>.

**[IANA.cose]** IANA, "CBOR Object Signing and Encryption (COSE)", <https://www.iana.org/assignments/cose>.

**[RFC8126]** Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/rfc/rfc8126>.

**[RFC8152]** Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/rfc/rfc8152>.

**[RFC9053]** Schaad, J., "CBOR Object Signing and Encryption (COSE): Initial Algorithms", RFC 9053, DOI 10.17487/RFC9053, August 2022, <https://www.rfc-editor.org/rfc/rfc9053>.

**[STD94]** Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

**[STD96]** Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, August 2022. Schaad, J., "CBOR Object Signing and Encryption (COSE): Countersignatures", STD 96, RFC 9338, December 2022.

## Acknowledgments

This document was motivated by a discussion at IETF 117 Hackathon. The author is grateful to the many contributors to the discussions on the mailing lists that build the basis for this document.

## Author's Address

Carsten Bormann
Universität Bremen TZI
Postfach 330440
D-28359 Bremen
Germany

Phone: +49-421-218-63921
Email: cabo@tzi.org