Workgroup: CBOR Object Signing and Encryption
Internet-Draft: draft-fossati-cose-profiles-00
Published: 13 March 2023
Intended Status: Standards Track
Expires: 14 September 2023
Authors: T. Fossati H. Birkholz
Arm Limited Fraunhofer SIT

COSE Profiles

Abstract

COSE (STD96) is not an end-to-end system with guaranteed interoperability. It is designed to serve a range of use cases and therefore it has a lot of options. In general, two COSE implementations that want to interoperate require an agreement on which subset of COSE features they will use. This document provides a set of rules for specifying such agreements as "COSE profiles" and registers a new COSE header parameter for in-band signalling of profile information.

About This Document

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

The latest revision of this draft can be found at https://thomas-fossati.github.io/draft-fossati-cose-profile/draft-fossati-cose-profiles.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-fossati-cose-profiles/.

Discussion of this document takes place on the CBOR Object Signing and Encryption 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/thomas-fossati/draft-fossati-cose-profile.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents

at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 14 September 2023.

Table of Contents

1. Introduction

COSE [STD96] is not an end-to-end system with guaranteed interoperability. It is designed to serve a range of use cases and therefore it has a lot of options. In general, two COSE implementations that want to interoperate require an agreement on which subset of COSE features they will use.

This document provides a set of rules for specifying such agreements as "COSE profiles" and registers a new COSE header parameter for in-band signalling of profile information.

2. Conventions and Definitions

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Profiling Rules

A COSE profile:

* **MUST** be specified in a document

* **MUST NOT** change the syntax or semantics of any already defined header attribute

  - but does allow restricting their values

* **MAY** define new header attributes

  - if so, it **MUST** provide their definition in the same document

* **MUST** use CDDL [RFC8610] to fully specify the syntax rules for the profile

* **MUST** use the cose-profile header attribute (see Section 4) in the protected header

  - The value of cose-profile **MUST** be globally unique. Possible choices include:

    o IANA registry (Section 8.2)

    o using an OID [RFC9090], URI [STD66] or CRI [I-D.ietf-core-href]

    o using a UUID [RFC4122]

  - The chosen value **SHOULD** be appropriate for the intended usage scope (e.g., a short value when used in constrained node environments)

* **MAY** define its own CBOR tag that can be used together with, or in lieu of, the underlying COSE CBOR tag (Table 1, Section 2 of [STD96])

*__SHOULD__ define its complementary media-type and content-format

4. COSE profile header parameter

```
COSE-profile = registered-profile / oid-profile / uri-profile
             / cri-profile / uuid-profile
registered-profile = int
oid-profile = oid ; tagged
uri-profile = ~uri ; unwrapped -- any tstr is a uri
cri-profile = cri
uuid-profile = uuid ; naked bstr is a UUID

uuid = bstr .size 16

; imported from RFC 9090
oid = #6.111(bstr)
; import from CRI spec when ready
cri = [*any]
```

5. Profile Registration Template

Note: This is just an initial sketch.

Tracked at: https://github.com/ietf-rats-wg/draft-ietf-rats-corim/issues/10

*What is the profile identifier?

*Requires certain header keys?

*Constrains any header keys?

*Constrains any header values?

*Defines new header keys?

*Defines its own CBOR Tag?

*Defines its own Media Type?

*What payload(s) allows?

6. CoSWID COSE Profile Definition

Note: This is just an initial sketch.

Tracked at: https://github.com/ietf-rats-wg/draft-ietf-rats-corim/issues/10

This section defines the COSE profile for CoSWID [I-D.ietf-sacm-coswid].

This definition is semantically and syntactically equivalent with what is described in Section 7 of [I-D.ietf-sacm-coswid], with the exception of the explicit CoSWID COSE profile indicator that is added to the protected header.

6.1. CDDL Definition

```
protected-signed-coswid-header = {
  &(alg: 1) => int
  &(content-type: 3) => "application/swid+cbor"
  &(cose-profile-CPA: 13) => &(CoSWID-COSE-profile-CPA: 0)
  * cose-label => cose-values
}

cose-label = int / text
cose-values = any
```

6.2. Checklist

*Mandatory header keys? YES

*Constrains header keys? NO

*Constrains header values? YES (alg is only int)

*New header keys? NO

*Defines its own CBOR Tag? YES

*Defines its own Media Type? YES

7. Security Considerations

TODO Security

8. IANA Considerations

8.1. New COSE Profile Header Parameter

This document requests IANA to allocate a new header parameter cose-profile-CPA (suggested value 13) in the "COSE Header Parameters" [IANA.cose] registry.

8.2. COSE Profile Sub-registry

This specification requests IANA to create a new sub-registry for COSE [IANA.cose], with the policy "specification required" (Section 4.6 of [RFC8126]).

Each entry in the registry must include:

Key value:
integer value for the profile

Brief description:
a brief description

Change Controller:
(see Section 2.3 of [RFC8126])

Reference:
a reference document

The expert is requested to assign the shortest key values (1+0 and 1+1 encoding) to registrations that are likely to enjoy wide use and can benefit from short encodings.

9. References

9.1. Normative References

[I-D.ietf-core-href] Bormann, C. and H. Birkholz, "Constrained Resource Identifiers", Work in Progress, Internet-Draft, draft-ietf-core-href-12, 6 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-core-href-12>.

[I-D.ietf-sacm-coswid] Birkholz, H., Fitzgerald-McKay, J., Schmidt, C., and D. Waltermire, "Concise Software Identification Tags", Work in Progress, Internet-Draft, draft-ietf-sacm-coswid-24, 24 February 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-sacm-coswid-24>.

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI

10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/rfc/rfc4122>.

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/rfc/rfc8610>.

[RFC9090] Bormann, C., "Concise Binary Object Representation (CBOR) Tags for Object Identifiers", RFC 9090, DOI 10.17487/RFC9090, July 2021, <https://www.rfc-editor.org/rfc/rfc9090>.

[STD66] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/rfc/rfc3986>.

[STD96] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/rfc/rfc9052>.

9.2. Informative References

[GlueCOSE] The GlueCOSE Community, "Test Vectors", <https://github.com/gluecose/test-vectors>.

Appendix A. GlueCOSE Test Cases

The community effort [GlueCOSE] provides test vectors for the COSE specification.

The CDDL definition for the test vector format used for COSE profiles will be provided in a future version of this document.

Tracked at: https://github.com/ietf-rats-wg/draft-ietf-rats-corim/issues/4

Acknowledgments

Laurence Lundblade who - unknowingly :-) - provided the introduction.

Authors' Addresses

Thomas Fossati
Arm Limited

Email: thomas.fossati@arm.com

Henk Birkholz
Fraunhofer SIT

Email: henk.birkholz@sit.fraunhofer.de