Internet Engineering Task Force (IETF)
Request for Comments: 9596
Category: Standards Track
ISSN: 2070-1721

M.B. Jones
Self-Issued Consulting
O. Steele
Transmute

June 2024

CBOR Object Signing and Encryption (COSE) "typ" (type) Header Parameter

Abstract

This specification adds the equivalent of the JSON Object Signing and Encryption (JOSE) "typ" (type) header parameter to CBOR Object Signing and Encryption (COSE). This enables the benefits of explicit typing (as defined in RFC 8725, "JSON Web Token Best Current Practices") to be brought to COSE objects. The syntax of the COSE type header parameter value is the same as the existing COSE content type header parameter.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9596.

Table of Contents

1. Introduction

CBOR Object Signing and Encryption (COSE) [RFC9052] defines header parameters that parallel many of those defined by the JSON Object Signing and Encryption (JOSE) specifications [RFC7515] [RFC7516]. However, one way in which COSE does not provide equivalent functionality to JOSE is that it does not define an equivalent of the "typ" (type) header parameter, which is used for declaring the type of the entire JOSE data structure. The security benefits of having "typ" (type) are described in Section 3.11 of [RFC8725], which recommends its use for "explicit typing" -- using "typ" values to distinguish between different kinds of JSON Web Tokens (JWTs) [RFC7519].

This specification adds the equivalent of the JOSE "typ" (type) header parameter to COSE so that the benefits of explicit typing can be brought to COSE objects. The syntax of the COSE type header parameter value is the same as the existing COSE content type header parameter, allowing both unsigned integers as registered in the "CoAP Content-Formats" registry [CoAP.ContentFormats] and string media type values [MediaTypes] to be used.

The term "COSE object" is used as defined in [RFC9052]. An example of a COSE object is a COSE_Sign1 structure, as described in Section 4.2 of [RFC9052].

1.1. Requirements Notation and Conventions

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.

2. COSE "typ" (type) Header Parameter

The "typ" (type) header parameter is used by COSE applications to declare the type of this complete COSE object, as compared to the content type header parameter, which declares the type of the COSE object payload. This is intended for use by the application when more than one kind of COSE object could be present in an application data structure that can contain a COSE object; the application can use this value to disambiguate among the different kinds of COSE objects that might be present. It will typically not be used by applications when the kind of COSE object is already known. Use of this header parameter is OPTIONAL.

The syntax of this header parameter value is the same as the content type header parameter defined in Section 3.1 of [RFC9052]; it is either an unsigned integer as registered in the "CoAP Content-Formats" registry [CoAP.ContentFormats] or a string content type value. Content type values have a media type name [MediaTypes] and MAY include media type parameters.

The "typ" (type) header parameter is ignored by COSE implementations (libraries implementing [RFC9052] and this specification), other than being passed through to applications using those implementations. Any processing of this parameter is performed by the COSE application using application-specific processing rules. For instance, an application might verify that the "typ" value is a particular application-chosen media type and reject the data structure if it is not.

The "typ" parameter MUST NOT be present in unprotected headers.

The "typ" parameter does not describe the content of unprotected

headers. Changes to unprotected headers do not change the type of the COSE object.

3. Security Considerations

The case for explicit typing of COSE objects is equivalent to the case made for explicit typing in Section 3.11 of [RFC8725]: Explicit typing can prevent confusion between different kinds of COSE objects.

COSE applications employing explicit typing should reject COSE objects with a type header parameter value different than values that they expect in that application context. They should also reject COSE objects without a type header parameter when one is expected.

4. IANA Considerations

4.1. COSE Header Parameter Registrations

IANA has registered the following value in the IANA "COSE Header Parameters" registry [COSE.HeaderParameters].

Name	Label	Value Type	Value Registry	Description	Reference
typ (type)	16	uint / tstr	[CoAP.ContentFormats] or [MediaTypes] registry	Content type of the complete COSE object	Section 2 of RFC 9596

Table 1

5. References

5.1. Normative References

[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/info/rfc2119>.

[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/info/rfc8174>.

[RFC8725] Sheffer, Y., Hardt, D., and M. Jones, "JSON Web Token Best Current Practices", BCP 225, RFC 8725, DOI 10.17487/RFC8725, February 2020, <https://www.rfc-editor.org/info/rfc8725>.

[RFC9052] 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/info/rfc9052>.

5.2. Informative References

[CoAP.ContentFormats] IANA, "CoAP Content-Formats", <https://www.iana.org/assignments/core-parameters>.

[COSE.HeaderParameters] IANA, "COSE Header Parameters", <https://www.iana.org/assignments/cose>.

[MediaTypes]
IANA, "Media Types",
<https://www.iana.org/assignments/media-types>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

[RFC7516] Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, DOI 10.17487/RFC7516, May 2015, <https://www.rfc-editor.org/info/rfc7516>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

Acknowledgements

We would like to thank Henk Birkholz, Carsten Bormann, Susan Hares, Dan Harkins, Murray Kucherawy, Marco Tiloca, Gunter Van de Velde, ric Vyncke, and Dale Worley for their valuable contributions to this specification.

Authors' Addresses

Michael B. Jones
Self-Issued Consulting
Email: michael_b_jones@hotmail.com
URI: https://self-issued.info/

Orie Steele
Transmute
Email: orie@transmute.industries