Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 20 September 2022

G. Selander
J. Preuß Mattsson
Ericsson

19 March 2022

Integer value for the CBOR Object Signing and Encryption (COSE) key identifier
draft-selander-cose-kid-int-01

Abstract

This document extends the CBOR Object Signing and Encryption (COSE) parameter kid to CBOR integer values.

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 20 September 2022.

Table of Contents

1. Introduction

Many Internet of Things (IoT) deployments require technologies which are highly performant in constrained environments [RFC7228]. The connectivity for these settings may exhibit extremely restricted bandwidth constraints, for which byte level optimizations are motivated, see [I-D.ietf-lake-reqs].

The use of CBOR [RFC8949] enables a compact encoding of protected data as COSE objects [I-D.ietf-cose-rfc8152bis-struct], which is a basic building block in various IoT security settings such as CWT [RFC8392], OSCORE [RFC8613], and ACE-OAuth [I-D.ietf-ace-oauth-authz]. COSE defines the key identifier parameter kid used to identify keys used in the COSE object.

The value of the kid parameter is specified to be encoded as a CBOR byte string, which (with the exception of the empty string) requires at least two bytes on the wire. For comparison, CBOR encoding of small integers (-24, ..., 23) need only one byte on the wire. Since many IoT deployments may use local identifiers for which a few unique identifiers are sufficient, the use of CBOR integers as key identifiers would reduce the overhead due to transport of COSE objects.

This specification amends this limitation by extending the COSE parameter kid to allow CBOR integer values. kid is used in different instances, which all need to be extended to CBOR int encoding:

* The kid COSE header parameter, see Section 3.1.

* The kid COSE Key Common Parameter, see Section 3.2.

* The kid CWT Confirmation Method, see Section 3.3.

2. Security Considerations

There are no additional security considerations compared to key identifiers to being byte strings.

3. IANA Considerations

3.1. COSE Header Parameters Registry

IANA has extended the Value Type of kid in the "COSE Header Parameters" registry under the group name "CBOR Object Signing and Encryption (COSE)" to also allow the Value Type int. The resulting Value Type is bstr / int. The Value Registry for this item is empty and omitted from the table below.

Name	Label	Value Type	Description
kid	4	bstr / int	Key identifier

3.2. COSE Key Common Parameters Registry

IANA has extended the Value Type of kid in the "COSE Key Common Parameters" registry under the group name "CBOR Object Signing and Encryption (COSE)" to also allow the Value Type int. The resulting Value Type is bstr / int. The Value Registry for this item is empty and omitted from the table below.

Name	Label	Value Type	Description
kid	2	bstr / int	Key identification value - match to kid in message

3.3. CWT Confirmation Methods

IANA has extended the Value Type of kid in the "CWT Confirmation Methods" registry under the group name "CBOR Web Token (CWT) Claims" to also allow the Value Type int. The resulting Value Type is bstr / int. The Value Registry for this item is empty and omitted from the table below.

Name	Label	Value Type	Description
kid	3	bstr / int	Key identification value - match to kid in message

4. References

4.1. Normative References

[I-D.ietf-cose-rfc8152bis-struct]
Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", Work in Progress, Internet-Draft, draft-ietf-cose-rfc8152bis-struct-15, 1 February 2021, <https://www.ietf.org/archive/id/draft-ietf-cose-rfc8152bis-struct-15.txt>.

[RFC8949] 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/info/rfc8949>.

4.2. Informative References

[I-D.ietf-ace-oauth-authz]
Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0

Framework (ACE-OAuth)", Work in Progress, Internet-Draft, draft-ietf-ace-oauth-authz-46, 8 November 2021, <https://www.ietf.org/archive/id/draft-ietf-ace-oauth-authz-46.txt>.

[I-D.ietf-lake-reqs]
Vucinic, M., Selander, G., Mattsson, J. P., and D. Garcia-Carrillo, "Requirements for a Lightweight AKE for OSCORE", Work in Progress, Internet-Draft, draft-ietf-lake-reqs-04, 8 June 2020, <https://www.ietf.org/archive/id/draft-ietf-lake-reqs-04.txt>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <https://www.rfc-editor.org/info/rfc7228>.

[RFC8392] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <https://www.rfc-editor.org/info/rfc8392>.

[RFC8613] Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, DOI 10.17487/RFC8613, July 2019, <https://www.rfc-editor.org/info/rfc8613>.

Acknowledgments

Authors' Addresses

Göran Selander
Ericsson AB
SE-164 80 Stockholm
Sweden
Email: goran.selander@ericsson.com

John Preuß Mattsson
Ericsson AB

SE-164 80 Stockholm
Sweden
Email: john.mattsson@ericsson.com