Network Working Group
Internet-Draft
Updates: draft-ietf-cose-x509 (if approved)
Intended status: Standards Track
Expires: September 10, 2020

J. Preuss Mattsson
G. Selander
Ericsson AB
S. Raza
J. Hoeglund
RISE AB
M. Furuhed
Nexus Group

March 09, 2020

CBOR Object Signing and Encryption (COSE): Headers for Carrying CBOR Compressed Certificates
draft-mattsson-cose-cbor-cert-compress-00

Abstract

Certificate chains often take up the majority of the bytes transmitted in COSE message that carry certificates. Large messages can cause problems, particularly in constrained IoT environments. RFC 7925 defines a certificate profile for constrained IoT. General purpose compression algorithms can in many cases not compress RFC 7925 profiled certificates at all. By using the fact that the certificates are profiled, the CBOR certificate compression algorithms can in many cases compress RFC 7925 profiled certificates with over 50%. This document specifies the CBOR certificate compression algorithm for use with COSE.

Table of Contents

1. Introduction

[I-D.ietf-cose-x509] provides attributes that refer to or contain X.509 certificates. X.509 certificates often take up the majority of the bytes transmitted in COSE messages that carry certificates. Large messages negatively affect latency, but can also result in that the security protocol cannot be completed [I-D.ietf-emu-eaptlscert].

Large messages is particularly a problem for constrained IoT environments [RFC7228] [I-D.ietf-lake-reqs]. [RFC7925] defines a X.509 certificate profile for constrained IoT. The certificate profile in [RFC7925] is defined for TLS/DTLS 1.2 but works well also for COSE and other protocols. For such RFC 7925 profiled IoT certificates, general purpose compression algorithms can in many cases only provide negligible or no compression at all.

[I-D.raza-ace-cbor-certificates] therefore defines a CBOR [RFC7049] compression algorithm for RFC 7925 profiled certificates. The algorithm works for all RFC 7925 profiled certificates and provide significant reduction in size, in many cases over 50%.

This document specifies the CBOR certificate compression algorithm [I-D.raza-ace-cbor-certificates] for use with COSE.

2. Notational 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.

3. CBOR Certificate Compression Algorithm

This document specifies the CBOR certificate compression algorithm specified in Section 3 of [I-D.raza-ace-cbor-certificates] for use with COSE.

The CBOR Certificate compression algorithm takes as input an RFC 7925 profiled X.509 certificate. The output of the CBOR compression algorithm is a CBOR Sequence [I-D.ietf-cbor-sequence], i.e. a sequence of concatenated CBOR encoded CBOR data items [RFC7049]. Compressed certificates can be analysed with any CBOR decoder and be validated against the CDDL specification defined in Section 3 of [I-D.raza-ace-cbor-certificates].

The algorithm works for all RFC 7925 profiled certificates and provide significant reduction in size, in many cases over 50%. An example compression of a RFC 7925 profiled certificate is given below. See Appendix A of [I-D.raza-ace-cbor-certificates] for details.

	RFC 7925	zlib	CBOR Certificate
Certificate Size	314	295	136

The header attributes defined in this document are:

CBORchain: This header attribute contains an ordered array of certicates similar to x5chain [I-D.ietf-cose-x509]. The difference being that all the included certificates are CBOR certificates [I-D.raza-ace-cbor-certificates] instead of DER encoded X.509 certificates.

Name	Label	Value Type	Description
CBORchain	TBD1	COSE_CBOR_Cert	An ordered chain of CBOR certificates

Below is an equivalent CDDL [RFC8610] description of the text above.

```
COSE_CBOR_Cert = bstr / [ 2*certs: bstr ]
```

4. Security Considerations

The security considerations in [I-D.ietf-cose-x509] and [I-D.raza-ace-cbor-certificates] apply.

5. IANA Considerations

This document registers the COSE Header items in Table 1 in the "COSE Header Parameters" registry under the "CBOR Object Signing and Encryption (COSE)" heading. For each item, the 'Reference' field points to this document.

6. References

6.1. Normative References

[I-D.ietf-cbor-sequence]
Bormann, C., "Concise Binary Object Representation (CBOR)

Sequences", draft-ietf-cbor-sequence-02 (work in progress), September 2019.

[I-D.ietf-cose-x509]
Schaad, J., "CBOR Object Signing and Encryption (COSE): Headers for carrying and referencing X.509 certificates", draft-ietf-cose-x509-05 (work in progress), November 2019.

[I-D.raza-ace-cbor-certificates]
Raza, S., Hoglund, J., Selander, G., Mattsson, J., and M. Furuhed, "CBOR Profile of X.509 Certificates", draft-raza-ace-cbor-certificates-03 (work in progress), December 2019.

[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>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[RFC7925] Tschofenig, H., Ed. and T. Fossati, "Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things", RFC 7925, DOI 10.17487/RFC7925, July 2016, <https://www.rfc-editor.org/info/rfc7925>.

[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>.

6.2. Informative References

[I-D.ietf-emu-eaptlscert]
Sethi, M., Mattsson, J., and S. Turner, "Handling Large Certificates and Long Certificate Chains in TLS-based EAP Methods", draft-ietf-emu-eaptlscert-01 (work in progress), March 2020.

[I-D.ietf-lake-reqs]
Vucinic, M., Selander, G., Mattsson, J., and D. Garcia-Carillo, "Requirements for a Lightweight AKE for OSCORE", draft-ietf-lake-reqs-01 (work in progress), February 2020.

[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>.

[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/info/rfc8610>.

Acknowledgments

The authors want to thank TBD for their valuable comments and feedback.

Authors' Addresses

John Preuss Mattsson
Ericsson AB

Email: john.mattsson@ericsson.com

Goeran Selander
Ericsson AB

Email: goran.selander@ericsson.com

Shahid Raza
RISE AB

Email: shahid.raza@ri.se

Joel Hoeglund
RISE AB

Email: joel.hoglund@ri.se

Martin Furuhed
Nexus Group

Email: martin.furuhed@nexusgroup.com