

Network Working Group  
Internet-Draft  
Updates: [draft-ietf-tls-certificate-compression](#) (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 Certificate Algorithm for TLS Certificate Compression**  
**draft-mattsson-tls-cbor-cert-compress-00**

Abstract

Certificate chains often take up the majority of the bytes transmitted in TLS handshakes. Large handshakes can cause problems, particularly in constrained IoT environments. [RFC 7925](#) defines a TLS 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 TLS Certificate Compression in TLS 1.3 and DTLS 1.3.

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 September 10, 2020.

## Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

|                      |                                                  |                   |
|----------------------|--------------------------------------------------|-------------------|
| <a href="#">1.</a>   | Introduction . . . . .                           | <a href="#">2</a> |
| <a href="#">2.</a>   | Notational Conventions . . . . .                 | <a href="#">3</a> |
| <a href="#">3.</a>   | CBOR Certificate Compression Algorithm . . . . . | <a href="#">3</a> |
| <a href="#">4.</a>   | Security Considerations . . . . .                | <a href="#">4</a> |
| <a href="#">5.</a>   | IANA Considerations . . . . .                    | <a href="#">4</a> |
| <a href="#">6.</a>   | References . . . . .                             | <a href="#">4</a> |
| <a href="#">6.1.</a> | Normative References . . . . .                   | <a href="#">4</a> |
| <a href="#">6.2.</a> | Informative References . . . . .                 | <a href="#">5</a> |
|                      | Acknowledgments . . . . .                        | <a href="#">5</a> |
|                      | Authors' Addresses . . . . .                     | <a href="#">5</a> |

## [1.](#) Introduction

As stated in [[I-D.ietf-tls-certificate-compression](#)], certificate chains often take up the majority of the bytes transmitted in TLS handshakes. Large handshakes negatively affect latency, but can also result in that the handshake cannot be completed [[I-D.ietf-emu-eaptls-cert](#)]. To reduce handshake sizes, [[I-D.ietf-tls-certificate-compression](#)] specifies a mechanism for lossless compression of certificate chains in TLS 1.3 and defines three general purpose compression algorithms.

Large handshakes 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 also for TLS 1.3 [[RFC8446](#)] and DTLS 1.3 [[I-D.ietf-tls-dtls13](#)]. For such profiled IoT certificates, general purpose compression algorithms such as zlib are however far from optimal and the general purpose compression algorithms defined in [[I-D.ietf-tls-certificate-compression](#)] can in many cases not compress



[RFC 7925](#) profiled certificates 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 TLS Certificate Compression [[I-D.ietf-tls-certificate-compression](#)]. TLS Certificate Compression can be used in TLS 1.3 [[RFC8446](#)] and DTLS 1.3 [[I-D.ietf-tls-dtls13](#)].

## 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 TLS Certificate Compression [[I-D.ietf-tls-certificate-compression](#)]. TLS Certificate Compression can be used in TLS 1.3 [[RFC8446](#)] and DTLS 1.3 [[I-D.ietf-tls-dtls13](#)].

The CBOR Certificate compression algorithm takes as input a [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.

|                           |                          |      |                  |  |
|---------------------------|--------------------------|------|------------------|--|
| +-----+-----+-----+-----+ |                          |      |                  |  |
|                           | <a href="#">RFC 7925</a> | zlib | CBOR Certificate |  |
| +-----+-----+-----+-----+ |                          |      |                  |  |
| Certificate Size          | 314                      | 295  | 136              |  |
| +-----+-----+-----+-----+ |                          |      |                  |  |



#### 4. Security Considerations

The security considerations in [[I-D.ietf-tls-certificate-compression](#)] and [[I-D.raza-ace-cbor-certificates](#)] apply.

#### 5. IANA Considerations

This document registers the following entry in the "Certificate Compression Algorithm IDs" registry under the "Transport Layer Security (TLS) Extensions" heading.

| Algorithm Number | Description      | Reference       |
|------------------|------------------|-----------------|
| TBD              | CBOR Certificate | [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-tls-certificate-compression]  
Ghedini, A. and V. Vasiliev, "TLS Certificate Compression", [draft-ietf-tls-certificate-compression-10](#) (work in progress), January 2020.
- [I-D.ietf-tls-dtls13]  
Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", [draft-ietf-tls-dtls13-34](#) (work in progress), November 2019.
- [I-D.raza-ace-cbor-certificates]  
Raza, S., Hoglund, J., Selander, G., Mattsson, J., and M. Furuheid, "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>>.
- [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", [RFC 8446](#), DOI 10.17487/RFC8446, August 2018, <<https://www.rfc-editor.org/info/rfc8446>>.

## **6.2. Informative References**

- [I-D.ietf-emu-eaptls-cert]  
Sethi, M., Mattsson, J., and S. Turner, "Handling Large Certificates and Long Certificate Chains in TLS-based EAP Methods", [draft-ietf-emu-eaptls-cert-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>>.

## **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](mailto:john.mattsson@ericsson.com)





Goeran Selander  
Ericsson AB

Email: [goran.selander@ericsson.com](mailto:goran.selander@ericsson.com)

Shahid Raza  
RISE AB

Email: [shahid.raza@ri.se](mailto:shahid.raza@ri.se)

Joel Hoeglund  
RISE AB

Email: [joel.hoglund@ri.se](mailto:joel.hoglund@ri.se)

Martin Furuhed  
Nexus Group

Email: [martin.furuhed@nexusgroup.com](mailto:martin.furuhed@nexusgroup.com)

