Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 26, 2017

J. Schaad
August Cellars

November 22, 2016

CBOR Encoded Message Syntax (COSE): Headers for carrying and referencing X.509 certificates

draft-schaad-cose-x509-00

Abstract

This document defines the headers and usage for referring to and transporting X.509 certificates in the CBOR Encoded Message (COSE) Syntax.

Contributing to this document

The source for this draft is being maintained in GitHub. Suggested changes should be submitted as pull requests at <https://github.com/cose-wg/X509>. Instructions are on that page as well. Editorial changes can be managed in GitHub, but any substantial issues need to be discussed on the COSE mailing list.

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 http://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 May 26, 2017.

Copyright Notice

Copyright (c) 2016 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 (http://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

1. Introduction

In the process of writing RFCXXXX [I-D.ietf-cose-msg] discussions where held on the question of X.509 certificates [RFC5280] and if there were needed. At the time there were no use cases presented that appeared to hve a sufficient set of support to include these headers. Since that time a number of cases where X.509 certificate support is necessary have been defined. This document provides a set of headers that will allow applications to transport and refer to X.509 certificates in a consistent manner.

1.1. Requirements Terminology

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 [RFC2119].

When the words appear in lower case, their natural language meaning is used.

2. X.509 COSE Headers

The use of X.509 certificates allows for an existing trust infrastructure to be used with COSE.

When the header parameters defined in this section are placed in a COSE_Signature or COSE_Sign0 object, they identify the key that was used for generating signature.

When the header parameters defined in this section are placed in a COSE_recipient structure, they identify the key that was used by the sender when used with static-static key agreement algorithms.

Certificates obtained from any of these methods MUST still be validated according to the PKIX rules in [RFC5280]. This includes matching against the trust anchors configured for the application. This applies certificates of a chain length of one as well as longer chains.

The header parameters defined in this document are:

x5c: This header parameter allows for a single or a bag of X.509 certificates to be carried in the message.

- If a single certificate is conveyed, it is placed in a CBOR bstr.

- If multiple certificates are conveyed, a CBOR array is used where:

  - The first element is a boolean value set to true if the certificates are arranged such that a each certificate is issued by the next certficate. In otherwords a chain of certificates is presented. The chain of certificates does not need to be complete and normally SHOULD omit the trust anchor certificate. If the first element is set to false, then the certificates are not ordered and can include certificates that are not needed to create a certificate chain from the end-entity certificate. This allows for a certificate with a key exchange algorithm to be carried in a signed message.

  - The second element is the end-entity certificate. This is true regardless of wheither the certificates are ordered or not. This permits the application to identify which certificate is the end-entity certificate without a second header attribute.

  - Elements three through the last are certificates.

x5t: This header parameter provides the ability to identify an X.509 certificate by a hash value. The parameter is an array of two elements. The first element is an algorithm identifier which is a signed integer, an unsigned integer or a string containing the hash algorithm identifier. The second element is a binary string containing the hash value.
For interoperability, applications which use this header parameter MUST support the hash algorithm 'sha256', but can use other hash algorithms.

x5u: This header parameter provides the ability to identify an X.509 certificate by a URL. The referenced resource can be any of the following media types:

- application/pkix-cert [RFC2585]

- application/pkcs7-mime; smime-type="certs-only" [I-D.ietf-lamps-rfc5751-bis]

- Should we support a PEM type? I cannot find a registered media type for one

The URL provided MUST provide integrity protection. For example, an HTTP GET request to retrieve a certificate MUST use TLS [RFC5246]. If the certificate does not chain to an existing trust anchor, the identity of the server MUST be configured as trusted to provide new trust anchors. This will normally be the situation when self-signed certificates are used.

name	label	value type	description
x5t	TBD1	COSE_CertHash	Hash of an X.509 certificate
x5u	TBD2	uri	URL pointing to an X.509 certificate
x5c	TBD3	COSE_X509	Collection of X.509 certificates

Table 1: X.509 COSE Headers

```
COSE_X509 = bstr / [ ordered: bool, certs: +bstr ]
COSE_CertHash = [ hashAlg: (int / tstr), hashValue: bstr ]
```

3. Hash Algorithm Identifiers

3.1. SHA-2 256-bit Hash

Define an algorithm identifier for SHA-256.

4. IANA Considerations

4.1. COSE Header Parameter Registry

Put in the registrations.

4.2. COSE Algorithm Registry

Put in the registrations.

5. Security Considerations

There are security considerations:

6. References

6.1. Normative References

[I-D.ietf-cose-msg]
Schaad, J., "CBOR Object Signing and Encryption (COSE)", draft-ietf-cose-msg-23 (work in progress), October 2016.

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

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

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

6.2. Informative References

[I-D.greevenbosch-appsawg-cbor-cddl]
Vigano, C. and H. Birkholz, "CBOR data definition language (CDDL): a notational convention to express CBOR data structures", draft-greevenbosch-appsawg-cbor-cddl-09 (work in progress), September 2016.

[I-D.ietf-lamps-rfc5751-bis]
Schaad, J., Ramsdell, B., and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", draft-ietf-lamps-rfc5751-bis-02 (work in progress), October 2016.

[RFC2585] Housley, R. and P. Hoffman, "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP", RFC 2585, DOI 10.17487/RFC2585, May 1999, <http://www.rfc-editor.org/info/rfc2585>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

Author's Address

Jim Schaad
August Cellars

Email: ietf@augustcellars.com