Workgroup: TBD
Internet-Draft:
draft-birkholz-cose-tsa-tst-header-
parameter-00
Published: 24 October 2022
Intended Status: Standards Track
Expires: 27 April 2023
Authors: H. Birkholz
Fraunhofer SIT
M. Riechert
Microsoft

COSE Header parameter for RFC 3161 Time-Stamp Tokens

Abstract

RFC 3161 provides a method to time-stamp a message digest to prove that it was created before a given time. This document defines how signatures of CBOR Signing And Encrypted (COSE) message structures can be time-stamped using RFC 3161 along with the needed header parameter to carry the corresponding time-stamp.

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 27 April 2023.

Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

Useful new COSE [RFC9052] header member that is the TST output of RFC 3161.

1.1. Requirements Notation

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.

1.2. RFC 3161 Time-Stamp Tokens COSE Header Parameter

The use of RFC 3161 Time-Stamp Tokens, often in combination with X.509 certificates, allows for an existing trust infrastructure to be used with COSE.

The new COSE header parameter for carrying time-stamp tokens is defined as:

*Name: RFC 3161 time-stamp tokens

*Label: TBD

*Value Type: bstr / [+ bstr]

*Value Registry: none

*Description: One or more RFC 3161 time-stamp tokens.

*Reference: TBD

The content of the bstr are the bytes of the DER-encoded RFC 3161 TimeStampToken structure. This matches the content of the equivalent header attribute defined in [RFC3161] for Cryptographic Message Syntax (CMS, see [RFC2630]) envelopes.

This header parameter allows for a single time-stamp token or multiple time-stamp tokens to be carried in the message. If a single time-stamp token is conveyed, it is placed in a CBOR byte string. If multiple time-stamp tokens are conveyed, a CBOR array of byte strings is used, with each time-stamp token being in its own byte string.

Given that time-stamp tokens in this context are similar to a countersignature [I-D.ietf-cose-countersign], the header parameter can is included in the unprotected header of a COSE envelope.

When sending a request to an RFC 3161 Time Stamping Authority (TSA, see [RFC3161]) to obtain a time-stamp token, then the so-called message imprint of the request **MUST** be the hash of the bytes within the bstr of the signature field of the COSE structure to be time-stamped. The hash algorithm does not have to match the algorithm used for signing the COSE message.

RFC 3161 time-stamp tokens use CMS as signature envelope format. [RFC2630] illustrates details of signature verification and [RFC3161] details specific to time-stamp token validation. The payload of the signed time-stamp token is a TSTInfo structure as defined in [RFC3161] and contains the message imprint that was sent to the TSA. As part of validation, the message imprint **MUST** be matched to the hash of the bytes within the bstr of the signature field of the time-stamped COSE structure. The hash algorithm is contained in the message imprint structure, together with the hash itself.

Appendix B of RFC 3161 provides an example of how time-stamp tokens can be used during signature verification of a time-stamped message when using X.509 certificates.

2. Privacy Considerations

TBD

3. Security Considerations

TBD

Similar to the same security considerations as described in RFC 3161 apply.

4. IANA Considerations

TBD

IANA is requested to register the new COSE Header parameter described in section TBD in the "COSE Header Parameters" registry.

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>.

[RFC2630] Housley, R., "Cryptographic Message Syntax", RFC 2630, DOI 10.17487/RFC2630, June 1999, <https://www.rfc-editor.org/info/rfc2630>.

[RFC3161] Adams, C., Cain, P., Pinkas, D., and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, DOI 10.17487/RFC3161, August 2001, <https://www.rfc-editor.org/info/rfc3161>.

[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>.

[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

[I-D.ietf-cose-countersign] Schaad, J. and R. Housley, "CBOR Object Signing and Encryption (COSE): Countersignatures", Work in Progress, Internet-Draft, draft-ietf-cose-countersign-10, 20 September 2022, <https://www.ietf.org/archive/id/draft-ietf-cose-countersign-10.txt>.

Authors' Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
64295 Darmstadt
Germany

Email: henk.birkholz@sit.fraunhofer.de

Maik Riechert
Microsoft
United Kingdom

Email: Maik.Riechert@microsoft.com