COSE
Internet-Draft
Intended status: Standards Track
Expires: 14 December 2025

H. Birkholz
Fraunhofer SIT
T. Fossati
Linaro
M. Riechert
Microsoft

12 June 2025

# COSE Header parameter for RFC 3161 Time-Stamp Tokens
draft-ietf-cose-tsa-tst-header-parameter-06

## Abstract

This document defines two CBOR Signing And Encrypted (COSE) header parameters for incorporating RFC 3161-based timestamping into COSE message structures (COSE_Sign and COSE_Sign1). This enables the use of established RFC 3161 timestamping infrastructure in COSE-based protocols.

## About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-cose-tsa-tst-header-parameter/.

Source for this draft and an issue tracker can be found at https://github.com/ietf-scitt/draft-birkholz-cose-tsa-tst-header-parameter.

## Status of This Memo

Table of Contents



## 1. Introduction

RFC 3161 [RFC3161] provides a method to timestamp a message digest to prove that it was created before a given time.

This document defines two new CBOR Object Signing and Encryption (COSE) [STD96] header parameters that carry the TimestampToken (TST) output of RFC 3161, thus allowing existing and widely deployed trust infrastructure to be used with COSE structures used for signing (COSE_Sign and COSE_Sign1).

### 1.1. Use Cases

This section discusses two use cases, each representing one of the two modes of use defined in Section 2.

The first use case is that of "long-term signatures", i.e., signatures that can still be verified even after the signing certificate has expired. This can address situations where it is important to prevent subsequent denial by the signer or to verify signatures made using (very) short-term certificates. To achieve this, the document signer acquires a fresh TST for the document's signature from a trusted TSA and concatenates it with the document. Later, when a relying party verifies the signed document and its associated TST, they can be certain that the document was signed _at least_ at the time specified by the TSA, and that the signing certificate was valid at the time the signature was made.

This usage scenario motivates the "COSE then Timestamp" mode described in Section 2.1.

The second use case is the notarization of a signed document by registering it with a transparency service. This is common practice for ensuring the accountability and auditability of issued documents, which are typically referred to as "statements" in this context. It is also common practice to only register the signed parts of a statement (the "signed statement" portion) with a transparency service, in order to reduce the complexity of consistency checks at a later stage, as well as avoiding the need to retrieve or reconstruct unsigned parts. Once the signed parts of a document have been registered in the append-only log at a transparency service, the log entry cannot be changed. In order to avoid losing the TST during the registration process, the TST must be included in the signed statement. To achieve this, the issuer acquires a TST from a TSA, includes it in the to-be-signed part of the statement so that the resulting signed statement includes the TST, and then registers the signed parts (rendering it a "transparent statement"). Later on, a relying party consuming the transparent statement including the TST can be certain that the statement was signed by the issuer _at least_ at the time specified by the TSA. If the issuer's signing key has expired (or been compromised), the authenticity of the statement can be ascertained by ensuring that no revocation information was made public before the time asserted by the issuer and registered at the transparency service.

This usage scenario motivates the "Timestamp then COSE" mode defined in Section 2.2.

### 1.2. 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.

## 2. Modes of Use

There are two different modes of composing COSE protection and timestamping, motivated by the usage scenarios discussed above.

The diagrams in this section illustrate the processing flow of the specified modes. For simplicity, only the COSE_Sign1 processing is shown. Similar diagrams for COSE_Sign can be derived by allowing multiple private-key parallelogram boxes and replacing the label [signature] with [signatures].

### 2.1. COSE then Timestamp (CTT)

Figure 1 shows the case where the signature(s) field of the signed COSE object is digested and submitted to a TSA to be timestamped. The obtained timestamp token is then added back as an unprotected header into the same COSE object.

This mode is utilized when a record of the timing of the signature operation is desired.

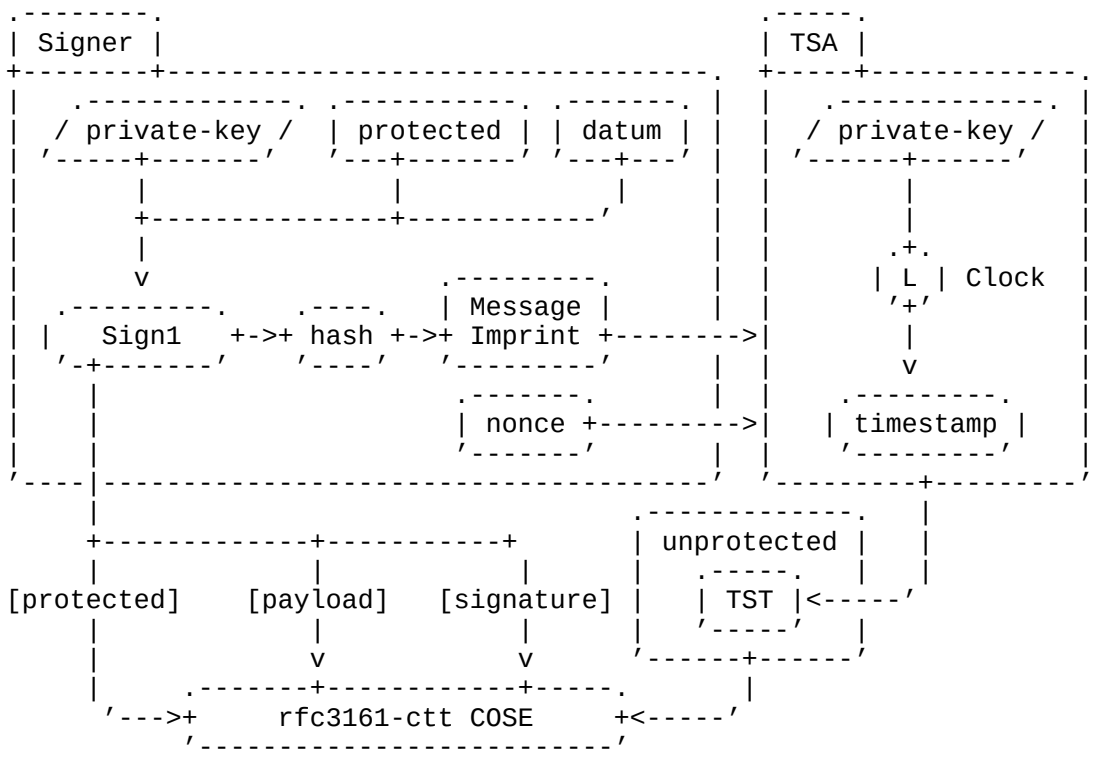


Figure 1: COSE, then Timestamp (CTT)

In this context, timestamp tokens are similar to a countersignature made by the TSA.

## 2.2. Timestamp then COSE (TTC)

Figure 2 shows the case where a datum is first digested and submitted to a TSA to be timestamped.

This mode is used to wrap the signed document and its timestamp together in an immutable payload.

A signed COSE message is then built as follows:

* The obtained timestamp token is added to the protected headers,

* The original datum becomes the payload of the signed COSE message.

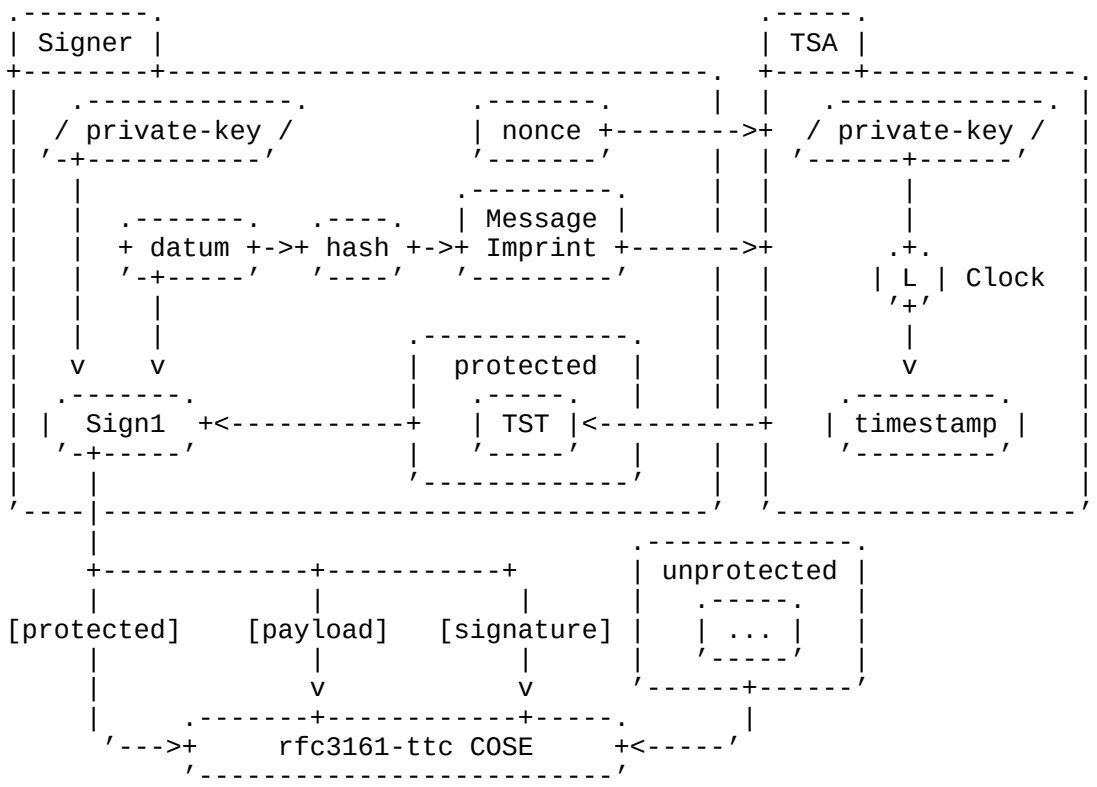


Figure 2: Timestamp, then COSE (TTC)

## 3. RFC 3161 Time-Stamp Tokens COSE Header Parameters

The two modes described in Section 2.2 and Section 2.1 use different inputs into the timestamping machinery, and consequently create different kinds of binding between COSE and TST. To clearly separate their semantics two different COSE header parameters are defined as described in the following subsections.

### 3.1. 3161-ctt

The 3161-ctt COSE _unprotected_ header parameter MUST be used for the mode described in Section 2.1.

The 3161-ctt unprotected header parameter contains a DER-encoded RFC3161 TimeStampToken wrapped in a CBOR byte string (Major type 2).

The MessageImprint sent in the request to the TSA MUST be:

* the hash of the CBOR-encoded signature field of the COSE_Sign1 message, or

* the hash of the CBOR-encoded signatures field of the COSE_Sign message.

In either case, to minimize dependencies, the hash algorithm SHOULD be the same as the algorithm used for signing the COSE message. This may not be possible if the timestamp token has been obtained outside the processing context in which the COSE object is assembled.

Refer to Section 3.1.1 and Section 3.1.2 for concrete examples of MessageImprint computation.

### 3.1.1. MessageImprint Computation for COSE_Sign1

The following illustrates how MessageImprint is computed using a sample COSE_Sign1 message.

Given the COSE_Sign1 message

```
18(
  [
    / protected h'a10126' / << {
      / alg / 1:-7 / ECDSA 256 /
    } >>,
    / unprotected / {
      / kid / 4:'11'
    },
    / payload / 'This is the content.',
    / signature / h'8eb33e4ca31d1c465ab05aac34cc6b23d58fef5c083106c4
d25a91aef0b0117e2af9a291aa32e14ab834dc56ed2a223444547e01f11d3b0916e5
a4c345cacb36'
  ]
)
```

the bstr-wrapped signature

```
58 40                                       # bytes(64)
   8eb33e4ca31d1c465ab05aac34cc6b23
   d58fef5c083106c4d25a91aef0b0117e
   2af9a291aa32e14ab834dc56ed2a2234
   44547e01f11d3b0916e5a4c345cacb36
```

(including the heading bytes 0x5840) is used as input for computing the MessageImprint.

When using SHA-256, the resulting MessageImprint is

```
SEQUENCE {
  SEQUENCE {
    OBJECT IDENTIFIER sha-256 (2 16 840 1 101 3 4 2 1)
    NULL
    }
  OCTET STRING
    44 C2 41 9D 13 1D 53 D5 55 84 B5 DD 33 B7 88 C2
    4E 55 1C 6D 44 B1 AF C8 B2 B8 5E 69 54 76 3B 4E
  }
```

#### 3.1.2. MessageImprint Computation for COSE_Sign

The following illustrates how MessageImprint is computed using a sample COSE_Sign message.

Given the COSE_Sign message

```
98(
  [
    / protected / h'',
    / unprotected / {},
    / payload / 'This is the content.',
    / signatures / [
      [
        / protected h'a10126' / << {
            / alg / 1:-7 / ECDSA 256 /
          } >>,
        / unprotected / {
          / kid / 4:'11'
        },
        / signature / h'e2aeafd40d69d19dfe6e52077c5d7ff4e408282cbefb
5d06cbf414af2e19d982ac45ac98b8544c908b4507de1e90b717c3d34816fe926a2b
98f53afd2fa0f30a'
      ]
    ]
  ]
)
```

the signatures array

```
81                                      # array(1)
   83                                   # array(3)
      43                                # bytes(3)
         a10126
      a1                                # map(1)
         04                             # unsigned(4)
         42                             # bytes(2)
            3131                        # "11"
      58 40                             # bytes(64)
         e2aeafd40d69d19dfe6e52077c5d7ff4
         e408282cbefb5d06cbf414af2e19d982
         ac45ac98b8544c908b4507de1e90b717
         c3d34816fe926a2b98f53afd2fa0f30a
```

is used as input for computing the MessageImprint.

When using SHA-256, the resulting MessageImprint is

```
SEQUENCE {
  SEQUENCE {
    OBJECT IDENTIFIER sha-256 (2 16 840 1 101 3 4 2 1)
    NULL
    }
  OCTET STRING
    80 3F AD A2 91 2D 6B 7A 83 3A 27 BD 96 1C C0 5B
    C1 CC 16 47 59 B1 C5 6F 7A A7 71 E4 E2 15 26 F7
  }
```

### 3.2. 3161-ttc

The 3161-ttc COSE _protected_ header parameter MUST be used for the mode described in Section 2.2.

The 3161-ttc protected header parameter contains a DER-encoded RFC3161 TimeStampToken wrapped in a CBOR byte string (Major type 2).

The MessageImprint sent to the TSA (Section 2.4 of [RFC3161]) MUST be the hash of the payload of the COSE signed object. This does not include the bstr-wrapping, only the payload bytes. (For an example, see Appendix A.1.)

To minimize dependencies, the hash algorithm used for signing the COSE message SHOULD be the same as the algorithm used in the RFC3161 MessageImprint. However, this may not be possible if the timestamp requester and the COSE message signer are different entities.

## 4. Timestamp Processing

RFC 3161 timestamp tokens use CMS as signature envelope format. [STD70] provides the details about signature verification, and [RFC3161] provides the details specific to timestamp token validation. The payload of the signed timestamp token is the TSTInfo structure defined in [RFC3161], which contains the MessageImprint that was sent to the TSA. The hash algorithm is contained in the MessageImprint structure, together with the hash itself.

As part of the signature verification, the receiver MUST make sure that the MessageImprint in the embedded timestamp token matches a hash of either the payload, signature, or signature fields, depending on the mode of use and type of COSE structure.

Appendix B of [RFC3161] provides an example that illustrates how timestamp tokens can be used to verify signatures of a timestamped message when utilizing X.509 certificates.

## 5. Security Considerations

Please review the Security Considerations section in [RFC3161]; these considerations apply to this document as well.

Also review the Security Considerations section in [STD96]. These considerations apply to this document as well, particularly with regard to the need for implementations to protect private key material. Additionally, solutions based on the COSE header parameters defined in this document must be able to report compromised keys promptly.

The following scenario assumes an attacker can manipulate the clocks on the COSE signer and its relying parties, but not the TSA. It is also assumed that the TSA is a trusted third party, so the attacker cannot impersonate the TSA and create valid timestamp tokens. In such a setting, any tampering with the COSE signer’s clock does not have an impact because, once the timestamp is obtained from the TSA, it becomes the only reliable source of time. However, in both CTT and TTC mode, a denial of service can occur if the attacker can adjust the relying party’s clock so that the CMS validation fails. This could disrupt the timestamp validation.

Implementers MUST clearly differentiate between RFC 3161 TSA timestamps proving the existence of payload data at an earlier point in time (TTC) and timestamps explicitly providing evidence of the existence of the cryptographic signature (CTT). Failure to clearly distinguish between these timestamp semantics can result in vulnerabilities, such as incorrectly accepting signatures created

after key revocation based on older payload-only timestamps. Validators must not interpret protected-header payload timestamps as proof of signature creation time and should rely exclusively on RFC 3161 TSA timestamps explicitly covering signature data for determining signature validity timing.

In CTT mode, an attacker could manipulate the unprotected header by removing or replacing the timestamp. To avoid that, the signed COSE object should be integrity protected during transit and at rest.

In TTC mode, the TSA is given an opaque identifier (a cryptographic hash value) for the payload. While this means that the content of the payload is not directly revealed, to prevent comparison with known payloads or disclosure of identical payloads being used over time, the payload would need to be armored, e.g., with a nonce that is shared with the recipient of the header parameter but not the TSA. Such a mechanism can be employed inside the ones described in this specification, but is out of scope for this document.

CTT and TTC modes have different semantic meanings. An implementation must ensure that the contents of the CTT and TCC headers are interpreted according to their specific semantics. In particular, symmetric to the signature and assembly mechanics, each mode has its own separate verification algorithm.

The resolution, accuracy, and precision of the TSA clock, as well as the expected latency introduced by round trips to and from the TSA must be taken into account when implementing solutions based on the COSE header parameters defined in this document.

## 6. IANA Considerations

IANA is requested to add the COSE header parameters defined in Table 1 to the "COSE Header Parameters" registry [IANA.cose_header-parameters].

| Name | Label | Value Type | Value Registry | Description | Reference |
|---|---|---|---|---|---|
| 3161-ttc | TBD1 | bstr | - | RFC 3161 timestamp token: Timestamp then COSE | RFCthis, Section 3.2 |
| 3161-ctt | TBD2 | bstr | - | RFC 3161 timestamp token: COSE then Timestamp | RFCthis, Section 3.1 |

Table 1: New COSE Header Parameters

## 7. Normative References

[IANA.cose_header-parameters]
IANA, "COSE Header Parameters",
<https://www.iana.org/assignments/cose>.

[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/rfc/rfc2119>.

[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/rfc/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/rfc/rfc8174>.

[STD70] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/rfc/rfc5652>.

[STD96] 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/rfc/rfc9052>.

# Appendix A. Examples

## A.1. TTC

The payload

This is the content.

is hashed using SHA-256 to create the TimeStampReq object

```
SEQUENCE {
  INTEGER 1
  SEQUENCE {
    SEQUENCE {
      OBJECT IDENTIFIER sha-256 (2 16 840 1 101 3 4 2 1)
      NULL
      }
    OCTET STRING
      09 E6 38 D4 AA 95 FD 72 71 86 62 03 59 53 03 BC
      E2 32 F4 62 A9 4D 38 E3 93 77 3C D3 AA E3 F6 B0
    }
  BOOLEAN TRUE
  }
```

which is sent to the Time Stamping Authority.

A TimeStampResp is returned which contains the TimeStampToken

```
SEQUENCE {
  OBJECT IDENTIFIER signedData (1 2 840 113549 1 7 2)
  [0] {
    SEQUENCE {
      INTEGER 3
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER sha-512 (2 16 840 1 101 3 4 2 3)
          NULL
          }
        }
      SEQUENCE {
        OBJECT IDENTIFIER tSTInfo (1 2 840 113549 1 9 16 1 4)
        [0] {
          OCTET STRING, encapsulates {
            SEQUENCE {
              INTEGER 1
              OBJECT IDENTIFIER '1 2 3 4 1'
              SEQUENCE {
                SEQUENCE {
                  OBJECT IDENTIFIER sha-256 (2 16 840 1 101 3 4 2 1)
                  NULL
                  }
                OCTET STRING
                  09 E6 38 D4 AA 95 FD 72 71 86 62 03 59 53 03 BC
                  E2 32 F4 62 A9 4D 38 E3 93 77 3C D3 AA E3 F6 B0
                }
              INTEGER 85048992
              GeneralizedTime 18/01/2025 11:20:06 GMT
              BOOLEAN TRUE
[...]
```

The contents of the TimeStampToken are bstr-wrapped and added to the protected headers bucket which is then signed alongside the original payload to obtain the COSE_Sign1 object

=============== NOTE: '\' line wrapping per RFC 8792 ================

```
18([
        <<{1: -7, 258: h'\
3082154906092a864886f70d010702a082153a3082153602010331 0f300d06096086\
480165030402030500308201840 60b2a864886f70d0109100104a08201730482016f\
3082016b02010106042a0304013031300d0609608648016503040201050004 2009e6\
38d4aa95fd7271866203595303bce232f462a94d38e393773cd3aae3f6b002040511\
bea0180f323032353031313831313230303 65a0101ffa0820111a482010d30820109\
3111300f060355040a1308467265652054534131 0c300a060355040b130354534131\
763074060355040d136d546869732063657274696669636174652064696769746 16c\
6c79207369676e7320646f63756d656e747320616e642074696d65207374616d7020\
```

```
   726571756573747320 6d616465207573696e67207468652066726565747 3612e6f72\
   67206f6e6c696e652073657276696365733118301606035504031 30f7777772e6672\
   65657473612e6f72673122302006092a864886f70d010901161362757 3696c657a61\
   7340676d61696c2e636f6d311230100603550407130957756572 7a62757267310b30\
   090603550406130244453 10f300d060355040813064261796572 6ea0821008308208\
   01308205e9a003020102020900c1e986160da8e982300d06092a864886f70d01010d\
   0500308195311130 0f060355040a1308467265652054534131103 00e060355040b13\
   07526f6f74204341311830160603550403130f7777772e667265657473612e6f7267\
   3122302006092a864886f70d010901161362757 3696c657a617340676d61696c2e63\
   6f6d311230100603550407130957756572 7a62757267310f300d0603550408130642\
   617965726e310b300906035504061302444530 1e170d313630333133303135373339\
   5a170d323630333131303135373339 5a308201093111300f060355040a1308467265\
   6520545341310c300a060355040b1303545341317630740603550 40d136d54686973\
   206365727469666963617465206469676974616c6c79207369676e7320646f63756d\
   656e747320616e642074696d65207374616d70207265717565737473206d61646520\
   7573696e672074686520667265657473612e6f7267206f6e6c696e65207365727669\
   6365733118301606035504031 30f7777772e667265657473612e6f72673122302006\
   092a864886f70d010901161362757 3696c657a617340676d61696c2e636f6d311230\
   100603550407130957756572 7a62757267310b300906035504061302444530 f300d\
   060355040813064261796572 6e30820222300d06092a864886f70d01010105000382\
   020f003082020a0282020100b591048c4e486f34e9dc08627fc2375162236984b82c\
   b130beff517cfc38f84bce5c65a874dab2621ae0bce7e33563e0ede934fd5f882315\
   9f07848808227460c1ed88261706f4281334359dfbb81bd1353fc179610af1a8c8c8\
   65dc00ea23b3a89be6bd03ba85a9ec827d60565905e22d6a584ed1380ae150280cee\
   397e98a012f380464007862443bc077cb95f421af31712d9683cdb6dffbaf3c8ba5b\
   a566ae523d459d6177346d4d840e27886b7c01c5b890d78a2e27bba8dd2f9a2812e1\
   57d62f921c65962548069dcdb7d06de181de0e9570d66f87220ce28b628ab55906f3\
   ee0c210f7051e8f4858af8b9a92d09e46af2d9cba5bfcfad168cdf604491a4b06603\
   b114caf7031f065e7eeefa53c575f3490c059d2e32ddc76ac4d4c4c710683b97fd1b\
   e591bc61055186d88f9a0391b307b6f91ed954daa36f9acd6a1e14aa2e4adf17464b\
   54db18dbb6ffe30080246547370436ce4e77bae5de6fe0f3f9d6e7ffbeb461e794e9\
   2fb0951f8aae61a412cce9b21074635c8be327ae1a0f6b4a646eb0f8463bc63bf845\
   530435d19e802511ec9f66c3496952d8becb69b0aa4d4c41f60515fe7dcbb89319cd\
   da59ba6aea4be3ceae718e6fcb6ccd7db9fc50bb15b12f3665b0aa307289c2e6dd4b\
   111ce48ba2d9efdb5a6b9a506069334fb34f6fc7ae330f0b34208aac80df3266fdd9\
   0465876ba2cb898d9505315b6e7b0203010001a38201db308201d730090603551d13\
   04023000301d0603551d0e041604146e760b7b4e4f9ce160ca6d2ce927a2a294b377\
   37301f0603551d23041830168014fa550d8c346651434cf7e7b3a76c95af7ae6a497\
   300b0603551d0f0404030206c030160603551d250101ff040c300a06082b06010505\
   070308306306082b06010505070101045730553 02a06082b06010505073002861e68\
   7474703a2f2f7777772e667265657473612e6f72672f7473612e637274302706082b\
   06010505073001861b687474703a2f2f7777772e667265657473612e6f72673a3235\
   363030370603551d1f0430302e302ca02aa0288626687474703a2f2f7777772e6672\
   65657473612e6f72672f63726c2f726f6f745f63612e63726c3081c60603551d2004\
   81be3081bb3081b80601003081b2303306082b06010505070201162768747 4703a2f\
   2f7777772e667265657473612e6f72672f667265657473615f6370732e68746d6c30\
   3206082b06010505070201162668747 4703a2f2f7777772e667265657473612e6f72\
   672f667265657473615f6370732e706466304706082b06010505070202303b1a3946\
```

```
   726565545341207472757374656420746 96d657374616d70696e6720536f66747761\
   726520617320612053657276696365202853616153293 00d06092a864886f70d0101\
   0d05000382020100a5c944e2c6fac0a14d930a7fd0a0b172b41fc1483c3e957c68a2\
   bcd9b9764f1a950161fd72472d41a5eed277786203b5422240fb3a26cde176087b6f\
   b1011df4cc19e2571aa4a051109665e94c46f50bd2adee6ac4137e251b25a39dabda\
   451515d8ff9e07209e8ec20b7874f7e1a0ede7c00937fe84a334f8b3265ced2d8ed9\
   df61396583677feb382c1ee3b23e6ea5f05df30de7b9f89005d25266f612f39c8b4f\
   6daba6d7bfbac19632b90637329f52a6f066a10e43eaa81f849a6c5fe3fe8b5ea232\
   75f687f2052e502ea6c30762a668cce07871dd8e97e315bba929e25589977a0a312c\
   e96c5106b1437c779f2b361b182888f3ee8a234374fa063e956192627f7c43107396\
   5d1260928eba009e803429ae324cf96f042354f37bca5afddc79f79346ab388bfc79\
   f01dc9861254ea6cc129941076b83d20556f3be51326837f2876f7833b370e7c3d41\
   0523827d4f53400c72218d75229ff10c6f8893a9a3a1c0c42bb4c898c13df41c7f65\
   73b4fc56515971a610a7b0d2857c8225a9fb204eaceca2e8971aa1af87886a2ae3c7\
   2fe0a0aae842980a77bef16b92115458090d982b5946603764e75a0ad3d11454b998\
   6f678b9ab6afe8497033ae3abfd4eb43b7bc9dee68815949e6481582a82e785277f2\
   282107efe390200e0508acb8ea82ea2505276f3c9da2a3d3b4ad38bbf8842bda36fc\
   2448291f558dc02dd1e0308207ff308205e7a003020102020900c1e986160da8e980\
   300d06092a864886f70d01010d05003081953111300f060355040a13084672656520\
   5453413110300e060355040b1307526f6f74204341311830160603550403130f7777\
   772e667265657473612e6f72673122302006092a864886f70d010901161362757369\
   6c657a617340676d61696c2e636f6d3112301006035504071309577565727a627572\
   67310f300d06035504081306426179657 26e310b300906035504061302445301e17\
   0d313630333133303135323133 5a170d343130333037303135323133 5a3081953111\
   300f060355040a13084672656520545341311030 0e060355040b1307526f6f742043\
   413118301606035504031 30f7777772e667265657473612e6f72673122302006092a\
   864886f70d010901161362757369 6c657a617340676d61696c2e636f6d3112301006\
   035504071309577565727a62757267310f300d06035504081306426179657 26e310b\
   300906035504061302445308202223 00d06092a864886f70d01010105000382020f\
   003082020a0282020100b6028e0e3032f11110d964cda94b9d0278e1942ae913aaa5\
   9907cda69793995bd9ac7e33bad9fe3704da1c01a98d21afe3f591a59d7067705167\
   998f5016722e0ab462b21f439171d2cfcc4593f3735af794a5ab311f6c010c7898de\
   33d75c4510ee76f4bd1d1498cf17d303f06a5dd9f796cc6ca9b657a56fe3ea4fefbe\
   7ce6b6a18d3e35a30cee5ff170d1cf39a333d3fda8964d22db685b29e561be890f0a\
   a845873b2e84ab26ab839ffe8fade9d23bb31e61d273cc9b880649185fabecfa0534\
   600aba901b614e2e854582dea2226fc19cd7df52bed50d8777cd9988c053a3fc7dc3\
   287a068a4ff12b713cd9803666e955385456ff38f80298cf6b93856e9224774a66cf\
   1cdd11c2f8efd85203d7458b25664b13ed639cded4ff8113d6cc5353d2729473c3c3\
   07157c722aa5b5dd0bfb2d6c38b1b93749c881ec60026d08951b3824bd71bacbce47\
   3aebd636f0b918b4a2c8ff4694f07457af2d6f1cf82554d1770fd79ff5d314dcd104\
   cddcabc94138056dfcf017e7eb8572fd52f70144f188da05f5823f58dd06297e7387\
   bed2d772c13da8266601045fe412dd70986c0c987ba7344b9037387516d258e7885b\
   51f8968b7f2601213bc4cb4c85f8ff0b84af6a988337cdfb81868f7ecf31dca6716d\
   7ec2dd802c1672629e5c0052cb357dd29aafc43f615b3b1ff9d4e1ce08c71c73e1fe\
   bb7dc56a33621329e9ed6c230203010001a382024e3082024a300c0603551d130405\
   30030101ff300e0603551d0f0101ff0404030201c6301d0603551d0e04160414fa55\
   0d8c346651434cf7e7b3a76c95af7ae6a4973081ca0603551d230481c23081bf8014\
   fa550d8c346651434cf7e7b3a76c95af7ae6a497a1819ba4819830819531113 00f06\
```

0355040a13084672656520545341311030 0e060355040b1307526f6f742043413118\
30160603550403130f7777772e667265657473612e6f72673122302006092a864886\
f70d010901161362757369 6c657a617340676d61696c2e636f6d3112301006035504\
071309577565727a62757267310f300d060355040813064261796572 6e310b300906\
035504061302444582090 0c1e986160da8e98030330603551d1f042c302a3028a026\
a0248622687474703a2f2f7777772e667265657473612e6f72672f726f6f745f6361\
2e63726c3081cf0603551d200481c73081c43081c1060a2b0601040181f224010130\
81b2303306082b0601050507020116 27687474703a2f2f7777772e66726565747361\
2e6f72672f667265657473615f6370732e68746d6c303206082b0601050507020116\
26687474703a2f2f7777772e667265657473612e6f72672f667265657473615f6370\
732e706466304706082b0601050507020230 3b1a3946726565545341207472757374\
65642074696d657374616d70696e6720536f667477617265206173206120536572 76\
696365202853616153293037060 82b0601050507010104 2b3029302706082b060105\
05073001861b687474703a2f2f7777772e667265657473612e6f72673a3235363030\
0d06092a864886f70d01010d0500038202010068af7ebf938562ef4ceb3b580be2fa\
f6cc35a26772962f3d95901fa5630c87d09198984ce8a06a33f8a9c282ed9f1cb11a\
c6c23e17108ee4efce6fb294de95c133262255725522ca61971d4a3b7f78250dfb8d\
4aeec0fb1959b164100520b9c10e64c62662e4ad4d0abae2298fc948fc4e99e8d9e6\
b8fdbe4404121ec7c1422eacb2c9d7328e07396e60b4f3bb803ad4a555c80fefb53f\
85e7764a0a9fb4afc399f4cd2f5fbf587105c6081cf3d05337b6bb7d1b010b749f48\
88c912f3696ba1b6902d77b7dfc046c04a0cc1ec4f8d185e2da55dfb7bc2a2036c62\
19246a4f99ddbb6f1f829398f3b803dc0ad90dcb59bef4c27c77404b99043b782718\
67991152c399f12cbfc4c625adc096355ae44e342100ec517a502e2f06f940b8d435\
99bbc1154f8ae761a0b0d555fb4a1391d4f3420af8dbf12f2d7ddb9d77dce1537804\
074af175e4f2d6d55b34b5d6f7dcbdd31730af56480d4c0cff143f9e83bc151866d0\
ba0f0bbdc47fe27864176bbd6c1ab85df325edf777889bc4471bf3fa73e56cc591e8\
b160cda7b0786a1ec04ac3b24fa2e28d5d19e5e48004d5e166a83c82ec6fd54fb385\
ebaf7133a85b52de46db5244e1c34ae8d36e712f9fce0d493d7d3edd586c6198e3ec\
3e6e96346f417ac9f221e0aff33a8f6a0b1ef4c023630b76adaa8d91433825ecc41c\
49a5b98b181c7da30e997ab954c73c2cd805afda993182038a308203860201013081\
a33081953111300f060355040a13084672656520545341311030 0e060355040b1307\
526f6f74204341311830160603550403130f7777772e667265657473612e6f726731\
22302006092a864886f70d010901161362757369 6c657a617340676d61696c2e636f\
6d3112301006035504071309577565727a62757267310f300d060355040813064261\
7965726e310b300906035504061302444582090 0c1e986160da8e982300d06096086\
480165030402030500a081b8301a06092a864886f70d010903310d060b2a864886f7\
0d0109100104301c06092a864886f70d010905310f170d323530313138313132303030\
365a302b060b2a864886f70d010910020c311c301a301830160414916da3d860ecca\
82e34bc59d1793e7e968875f14304f06092a864886f70d01090431420440d26c8a6d\
b748885b0cd9c4ff636cb5d3c7f81308ea3c0bd8f76ab2112b21c1ec762c8f0318ca\
477472ab2bfde5c9d25129a2b144734b1766c094d66d3aa24d19300d06092a864886\
f70d0101010500048202009808366698a20227b3a03017317dbcd3813c7ec8f29693\
9ef20082bcdb95e8ed0495f299c2c6484b2246ab81092c73d039b0e33647a9241df1\
35fd44b9860c26cc784463d292e79ce39d04c0cffb0f2fb7cc9220ca3cbe43b088e4\
355dd7fc38a22ef9ad80629b15cd82e861b57df8797a3968f760b0175151aa3dd2c3\
7aaf8361571441295157c063af57ee66031870d80f30696da7b130a0d07e8753d517\
3e773713e28eec29b6999e17e65de2b20a0d2a4c33bf0734d7463da3c67da1c76353\
028761f0f2eaab1525bc489525d6ed34b34ae00a7ce34ceefaa6df08026047e470e3\

```
   09d0507832b65dad717287dcef8c250d7d7ddf677dd3a6c267c2d29c86e04653ce84\
   f7376c2434e2e85ec0eeaf2031a5f8cb4025f13b67c3ed4062af46000dbb1e3b5699\
   d14cb309c8cdabb736651b76957cb4392f9e2452a88233936e39bd23dae37eeee3de\
   4733a1ce2545324deb8a2203eed8264e3d657e60479cc08fa93916c266dcd1027daa\
   1afd091bde8bea923d92b6e17615eb9f83210c4f2b6fcecb918cfa638a75679aa3df\
   b5f959edc50923ff70c0d45a647a714f01ea48d803f68bb5081c97a57dcbd00c15d9\
   44ba3a89e126bec18b9f49c0225cab0c9e9a9b24de43e5e767b7512a525d909a52e5\
   cb2d79f5221d4f056e60dafb1dcc6e46f6dd1bb553d8caa37ee6add7c1dc70796766\
                                        d126e88b37d69fec915aa3dd65'}>>,
           {4: '11'},
           'This is the content.',
           h'\
   1b512caa05005b7a2329c1b92cc5447de3a387acc2537ec579d26d38c5be8740ed85\
           b8d3888630cc080b5eaaad12c029cde6117599565e63ca8485e927958682'
       ])
```

## A.2. CTT

Starting with the following COSE_Sign1 object

```
   18(
     [
       / protected h'a10126' / << {
           / alg / 1:-7 / ECDSA 256 /
         } >>,
       / unprotected / {
         / kid / 4:'11'
       },
       / payload / 'This is the content.',
       / signature / h'8eb33e4ca31d1c465ab05aac34cc6b23d58fef5c083106c4d
   25a91aef0b0117e2af9a291aa32e14ab834dc56ed2a223444547e01f11d3b0916e5a4
   c345cacb36'
     ]
   )
```

The CBOR-encoded signature field is hashed using SHA-256 to create the following TimeStampReq object

```
SEQUENCE {
  INTEGER 1
  SEQUENCE {
    SEQUENCE {
      OBJECT IDENTIFIER sha-256 (2 16 840 1 101 3 4 2 1)
      NULL
      }
    OCTET STRING
      44 C2 41 9D 13 1D 53 D5 55 84 B5 DD 33 B7 88 C2
      4E 55 1C 6D 44 B1 AF C8 B2 B8 5E 69 54 76 3B 4E
    }
  BOOLEAN TRUE
  }
```

which is sent to the Time Stamping Authority.

A TimeStampResp is returned which contains the following TimeStampToken

```
SEQUENCE {
  OBJECT IDENTIFIER signedData (1 2 840 113549 1 7 2)
  [0] {
    SEQUENCE {
      INTEGER 3
      SET {
        SEQUENCE {
          OBJECT IDENTIFIER sha-512 (2 16 840 1 101 3 4 2 3)
          NULL
          }
        }
      SEQUENCE {
        OBJECT IDENTIFIER tSTInfo (1 2 840 113549 1 9 16 1 4)
        [0] {
          OCTET STRING, encapsulates {
            SEQUENCE {
              INTEGER 1
              OBJECT IDENTIFIER '1 2 3 4 1'
              SEQUENCE {
                SEQUENCE {
                  OBJECT IDENTIFIER sha-256 (2 16 840 1 101 3 4 2 1)
                  NULL
                  }
                OCTET STRING
                  44 C2 41 9D 13 1D 53 D5 55 84 B5 DD 33 B7 88 C2
                  4E 55 1C 6D 44 B1 AF C8 B2 B8 5E 69 54 76 3B 4E
                }
              INTEGER 84895155
              GeneralizedTime 17/01/2025 18:29:13 GMT
              BOOLEAN TRUE
[...]
```

The contents of the TimeStampToken are bstr-wrapped and added to the unprotected headers bucket in the original COSE_Sign1 object to obtain the following

=============== NOTE: '\' line wrapping per RFC 8792 ================

```
18(
  [
    / protected h'a10126' / << {
       / alg / 1:-7 / ECDSA 256 /
      } >>,
    / unprotected / {
      / 3161-ctt / 259 : h'\
3082154906092a864886f70d010702a082153a3082153602010331 0f300d06096086\
4801650304020305003082018406 0b2a864886f70d0109100104a08201730482016f\
3082016b02010106042a0304013031300d0609608648016503040201050004 2044c2\
```

```
   419d131d53d55584b5dd33b788c24e551c6d44b1afc8b2b85e6954763b4e0204050f\
   65b3180f323032353031313731383239313335a0101ffa0820111a482010d30820109\
   3111300f060355040a1308467265652054534131 0c300a060355040b130354534131\
   763074060355040d136d546869732063657274696669636174652064696769746 16c\
   6c79207369676e7320646f63756d656e747320616e642074696d65207374616d7020\
   726571756573737320 6d6164652075736 96e6720746865206672656573612e6f72\
   67206f6e6c696e65207365727669636573311830160603550403130f7777772e6672\
   65657473612e6f72673122302006092a864886f70d010901161362757369 6c657a61\
   7340676d61696c2e636f6d311230100603550407130957756572 7a62757267310b30\
   090603550406130244453 10f300d060355040813064261796572 6ea0821008308208\
   01308205e9a003020102020900c1e986160da8e982300d06092a864886f70d01010d\
   0500308195311130 0f060355040a1308467265652054534131311030 0e060355040b13\
   07526f6f7420434131183016060355040313 0f7777772e667265657473612e6f7267\
   3122302006092a864886f70d010901161362757369 6c657a617340676d61696c2e63\
   6f6d311230100603550407130957756572 7a62757267310f300d0603550408130642\
   617965726e310b300906035504061302444530 1e170d313630333133303135373339\
   5a170d323630333131303135373339 5a308201093111300f060355040a1308467265\
   6520545341310c300a060355040b130354534131763074060355040d136d54686973\
   206365727469666963617465206469676974616c6c79207369676e7320646f63756d\
   656e747320616e642074696d65207374616d70207265717565737473206d61646520\
   7573696e672074686520667265657473612e6f7267206f6e6c696e65207365727669\
   6365733118301606035504031 30f7777772e667265657473612e6f72673122302006\
   092a864886f70d010901161362757369 6c657a617340676d61696c2e636f6d311230\
   100603550407130957756572 7a62757267310b300906035504061302444530 1f300d\
   060355040813064261796572 6e30820222300d06092a864886f70d01010105000382\
   020f003082020a0282020100b591048c4e486f34e9dc08627fc2375162236984b82c\
   b130beff517cfc38f84bce5c65a874dab2621ae0bce7e33563e0ede934fd5f882315\
   9f07848808227460c1ed88261706f4281334359dfbb81bd1353fc179610af1a8c8c8\
   65dc00ea23b3a89be6bd03ba85a9ec827d60565905e22d6a584ed1380ae150280cee\
   397e98a012f380464007862443bc077cb95f421af31712d9683cdb6dffbaf3c8ba5b\
   a566ae523d459d6177346d4d840e27886b7c01c5b890d78a2e27bba8dd2f9a2812e1\
   57d62f921c65962548069dcdb7d06de181de0e9570d66f87220ce28b628ab55906f3\
   ee0c210f7051e8f4858af8b9a92d09e46af2d9cba5bfcfad168cdf604491a4b06603\
   b114caf7031f065e7eeefa53c575f3490c059d2e32ddc76ac4d4c4c710683b97fd1b\
   e591bc61055186d88f9a0391b307b6f91ed954daa36f9acd6a1e14aa2e4adf17464b\
   54db18dbb6ffe30080246547370436ce4e77bae5de6fe0f3f9d6e7ffbeb461e794e9\
   2fb0951f8aae61a412cce9b21074635c8be327ae1a0f6b4a646eb0f8463bc63bf845\
   530435d19e802511ec9f66c3496952d8becb69b0aa4d4c41f60515fe7dcbb89319cd\
   da59ba6aea4be3ceae718e6fcb6ccd7db9fc50bb15b12f3665b0aa307289c2e6dd4b\
   111ce48ba2d9efdb5a6b9a506069334fb34f6fc7ae330f0b34208aac80df3266fdd9\
   0465876ba2cb898d9505315b6e7b0203010001a38201db308201d730090603551d13\
   04023000301d0603551d0e041604146e760b7b4e4f9ce160ca6d2ce927a2a294b377\
   37301f0603551d23041830168014fa550d8c346651434cf7e7b3a76c95af7ae6a497\
   300b0603551d0f0404030206c030160603551d250101ff040c300a06082b06010505\
   070308306306082b06010505070101045730553 02a06082b06010505073002861e68\
   7474703a2f2f7777772e667265657473612e6f72672f7473612e637274302706082b\
   06010505073001861b687474703a2f2f7777772e667265657473612e6f72673a3235\
   363030370603551d1f0430302e302ca02aa028862668747 4703a2f2f7777772e6672\
```

```
   65657473612e6f72672f63726c2f726f6f745f63612e63726c3081c60603551d2004\
   81be3081bb3081b80601003081b2303306082b06010505070201162768747 4703a2f\
   2f7777772e667265657473612e6f72672f667265657473615f6370732e68746d6c30\
   3206082b06010505070201162668747 4703a2f2f7777772e667265657473612e6f72\
   672f667265657473615f6370732e706466304706082b06010505070202303b1a3946\
   726565545341207472757374656420746 96d657374616d70696e6720536f66747761\
   726520617320612053657276696365202853616153293 00d06092a864886f70d0101\
   0d05000382020100a5c944e2c6fac0a14d930a7fd0a0b172b41fc1483c3e957c68a2\
   bcd9b9764f1a950161fd72472d41a5eed277786203b5422240fb3a26cde176087b6f\
   b1011df4cc19e2571aa4a051109665e94c46f50bd2adee6ac4137e251b25a39dabda\
   451515d8ff9e07209e8ec20b7874f7e1a0ede7c00937fe84a334f8b3265ced2d8ed9\
   df61396583677feb382c1ee3b23e6ea5f05df30de7b9f89005d25266f612f39c8b4f\
   6daba6d7bfbac19632b90637329f52a6f066a10e43eaa81f849a6c5fe3fe8b5ea232\
   75f687f2052e502ea6c30762a668cce07871dd8e97e315bba929e25589977a0a312c\
   e96c5106b1437c779f2b361b182888f3ee8a234374fa063e956192627f7c43107396\
   5d1260928eba009e803429ae324cf96f042354f37bca5afddc79f79346ab388bfc79\
   f01dc9861254ea6cc129941076b83d20556f3be51326837f2876f7833b370e7c3d41\
   0523827d4f53400c72218d75229ff10c6f8893a9a3a1c0c42bb4c898c13df41c7f65\
   73b4fc56515971a610a7b0d2857c8225a9fb204eaceca2e8971aa1af87886a2ae3c7\
   2fe0a0aae842980a77bef16b92115458090d982b5946603764e75a0ad3d11454b998\
   6f678b9ab6afe8497033ae3abfd4eb43b7bc9dee68815949e6481582a82e785277f2\
   282107efe390200e0508acb8ea82ea2505276f3c9da2a3d3b4ad38bbf8842bda36fc\
   2448291f558dc02dd1e0308207ff308205e7a003020102020900c1e986160da8e980\
   300d06092a864886f70d01010d05003081953111300f060355040a13084672656520\
   5453413110300e060355040b1307526f6f7420434131183016060355040313 0f7777\
   772e667265657473612e6f72673122302006092a864886f70d010901161362757369\
   6c657a617340676d61696c2e636f6d3112301006035504071309577565727a627572\
   67310f300d060355040813064261796 5726e310b3009060355040613024445301e17\
   0d3136303331333031353231335a170d343130333037303135323133 5a3081953111\
   300f060355040a13084672656520545341311030 0e060355040b1307526f6f742043\
   413118301606035504031 30f7777772e667265657473612e6f72673122302006092a\
   864886f70d010901161362757369 6c657a617340676d61696c2e636f6d3112301006\
   0355040713095775657272 7a62757267310f300d060355040813064261796 5726e310b\
   3009060355040613024453082022 2300d06092a864886f70d01010105000382020f\
   003082020a0282020100b6028e0e3032f11110d964cda94b9d0278e1942ae913aaa5\
   9907cda69793995bd9ac7e33bad9fe3704da1c01a98d21afe3f591a59d7067705167\
   998f5016722e0ab462b21f439171d2cfcc4593f3735af794a5ab311f6c010c7898de\
   33d75c4510ee76f4bd1d1498cf17d303f06a5dd9f796cc6ca9b657a56fe3ea4fefbe\
   7ce6b6a18d3e35a30cee5ff170d1cf39a333d3fda8964d22db685b29e561be890f0a\
   a845873b2e84ab26ab839ffe8fade9d23bb31e61d273cc9b880649185fabecfa0534\
   600aba901b614e2e854582dea2226fc19cd7df52bed50d8777cd9988c053a3fc7dc3\
   287a068a4ff12b713cd9803666e955385456ff38f80298cf6b93856e9224774a66cf\
   1cdd11c2f8efd85203d7458b25664b13ed639cded4ff8113d6cc5353d2729473c3c3\
   07157c722aa5b5dd0bfb2d6c38b1b93749c881ec60026d08951b3824bd71bacbce47\
   3aebd636f0b918b4a2c8ff4694f07457af2d6f1cf82554d1770fd79ff5d314dcd104\
   cddcabc94138056dfcf017e7eb8572fd52f70144f188da05f5823f58dd06297e7387\
   bed2d772c13da8266601045fe412dd70986c0c987ba7344b9037387516d258e7885b\
   51f8968b7f2601213bc4cb4c85f8ff0b84af6a988337cdfb81868f7ecf31dca6716d\
```

```
   7ec2dd802c1672629e5c0052cb357dd29aafc43f615b3b1ff9d4e1ce08c71c73e1fe\
   bb7dc56a33621329e9ed6c230203010001a382024e3082024a300c0603551d130405\
   30030101ff300e0603551d0f0101ff0404030201c6301d0603551d0e04160414fa55\
   0d8c346651434cf7e7b3a76c95af7ae6a4973081ca0603551d230481c23081bf8014\
   fa550d8c346651434cf7e7b3a76c95af7ae6a497a1819ba4819830819531113 00f06\
   0355040a1308467265652054534131103 00e060355040b1307526f6f742043413118\
   30160603550403130f7777772e667265657473612e6f72673122302006092a864886\
   f70d0109011613627573696c657a617340676d61696c2e636f6d3112301006035504\
   071309577565727a62757267310f300d060355040813064261796572 6e310b300906\
   0355040613024445820900c1e986160da8e98030330603551d1f042c302a3028a026\
   a0248622687474703a2f2f7777772e667265657473612e6f72672f726f6f745f6361\
   2e63726c3081cf0603551d200481c73081c43081c1060a2b0601040181f224010130\
   81b2303306082b0601050507020116 27687474703a2f2f7777772e66726565747361\
   2e6f72672f667265657473615f6370732e68746d6c303206082b0601050507020116\
   26687474703a2f2f7777772e667265657473612e6f72672f667265657473615f6370\
   732e706466304706082b0601050507020230 3b1a3946726565545341207472757374\
   65642074696d657374616d70696e6720536f667477617265206173206120536572 76\
   6963652028536161532930370 6082b0601050507010104 2b3029302706082b060105\
   05073001861b687474703a2f2f7777772e667265657473612e6f72673a3235363030\
   0d06092a864886f70d01010d0500038202010068af7ebf938562ef4ceb3b580be2fa\
   f6cc35a26772962f3d95901fa5630c87d09198984ce8a06a33f8a9c282ed9f1cb11a\
   c6c23e17108ee4efce6fb294de95c133262255725522ca61971d4a3b7f78250dfb8d\
   4aeec0fb1959b164100520b9c10e64c62662e4ad4d0abae2298fc948fc4e99e8d9e6\
   b8fdbe4404121ec7c1422eacb2c9d7328e07396e60b4f3bb803ad4a555c80fefb53f\
   85e7764a0a9fb4afc399f4cd2f5fbf587105c6081cf3d05337b6bb7d1b010b749f48\
   88c912f3696ba1b6902d77b7dfc046c04a0cc1ec4f8d185e2da55dfb7bc2a2036c62\
   19246a4f99ddbb6f1f829398f3b803dc0ad90dcb59bef4c27c77404b99043b782718\
   67991152c399f12cbfc4c625adc096355ae44e342100ec517a502e2f06f940b8d435\
   99bbc1154f8ae761a0b0d555fb4a1391d4f3420af8dbf12f2d7ddb9d77dce1537804\
   074af175e4f2d6d55b34b5d6f7dcbdd31730af56480d4c0cff143f9e83bc151866d0\
   ba0f0bbdc47fe27864176bbd6c1ab85df325edf777889bc4471bf3fa73e56cc591e8\
   b160cda7b0786a1ec04ac3b24fa2e28d5d19e5e48004d5e166a83c82ec6fd54fb385\
   ebaf7133a85b52de46db5244e1c34ae8d36e712f9fce0d493d7d3edd586c6198e3ec\
   3e6e96346f417ac9f221e0aff33a8f6a0b1ef4c023630b76adaa8d91433825ecc41c\
   49a5b98b181c7da30e997ab954c73c2cd805afda993182038a308203860201013081\
   a33081953111300f060355040a1308467265652054534131103 00e060355040b1307\
   526f6f74204341311830160603550403130f7777772e667265657473612e6f726731\
   22302006092a864886f70d0109011613627573696c657a617340676d61696c2e636f\
   6d3112301006035504071309577565727a62757267310f300d060355040813064261\
   7965726e310b3009060355040613024445020900c1e986160da8e982300d06096086\
   4801650304020305 00a081b8301a06092a864886f70d010903310d060b2a864886f7\
   0d0109100104301c06092a864886f70d010905310f170d3235303131373138323931\
   335a302b060b2a864886f70d010910020c311c301a30183016041 4916da3d860ecca\
   82e34bc59d1793e7e968875f14304f06092a864886f70d0109043142044 05f98e6ad\
   02a79c3209de2048fbf258d852df9f13c9ebef826154ef27fe4325a96d868c99e083\
   8791ac37faf028647f94abab446f3a93a9a0f51431a6e3d36c34300d06092a864886\
   f70d0101010500048202002 43d5af44af116c62c6053076eb6283a2b73beafa5411e\
   aee73dcc273e1b6327ab917c75bdec1305d2680e899a160e2b42a05f330bdf44c54f\
```

```
   1796ba538a3abfdab04cef3bba22ea4767bd30925c42c0ab91b5929b7a9aa99f3876\
   f5c8b1da1a98c7cb1f959394f9d707fa7ec04fb6943059cc98d04653b6f8e967a1eb\
   29269caca57c9fdd5294b54d595b58541a9ec14b5a0e9484573c5568b4943a7df4ff\
   c101cd807d66f3a869b363fdd87be9854a8260c0877acccf3b42618b8948191ff36e\
   999842c2569c44f189d8ab9f587bb54222be7d20926b3312882352efe5d50f46647a\
   149b4e0c59cbaaddd5ba0ce22715e4ee09c82bee3a83dc86d85192912ecfb005ce0e\
   b28a6549f92aa8ae9beb63eb8fadabe7eca3be5ccc6b2cb4e55d803fc76682bf82b1\
   de06e97ed9a272ded198f0370cea6f59d2c1927f2c0667308fedf41ac565d3333dec\
   5065daddd2c89d75261f52bfad5f87b48140f39ff12ef0c4d571085f72d94eb0a9d8\
   d65bf5ece1cad4e65452d8abe083f60ff977f247df79c263bbd32bdc7c5aae9da84d\
   a7d1a93b4193bd1f287a0a32c06c015d66cdf36b29d2b289c1484e720982190eef9c\
   2cc58c4fac9bd99089d1ad6960c5d06c992c4936e5b22495743dfbd1fda6ed2475b3\
   d445fd8dde40bb09e624c77d5d97faf1a88b44dda8ce7735f2482f822acf68027e6b\
                                                ca81532e740cb0824ca501504b',
         / kid / 4:'11'
       },
       / payload / 'This is the content.',
       / signature / h'8eb33e4ca31d1c465ab05aac34cc6b23d58fef5c083106c4
   d25a91aef0b0117e2af9a291aa32e14ab834dc56ed2a223444547e01f11d3b0916e5
   a4c345cacb36'
     ]
   )
```

## Acknowledgments

The editors would like to thank Alexey Melnikov, Carl Wallace, Carsten Bormann, Deb Cooley, テ詠ic Vyncke, Francesca Palombini, Leonard Rosenthol, Linda Dunbar, Michael B. Jones, Michael Prorock, Mike Bishop, Mohamed Boucadair, Orie Steele, Roman Danyliw, Shuping Peng, Stefan Santesson, Steve Lasker, and Yingzhen Qu for their reviews and comments.

## Contributors

Carsten Bormann
Email: cabo@tzi.org

Carsten contributed part of the security considerations.

Orie Steele
Email: orie@transmute.industries

Orie contributed an improved version of the diagrams.

## Authors' Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
64295 Darmstadt
Germany
Email: henk.birkholz@sit.fraunhofer.de

Thomas Fossati
Linaro
Email: thomas.fossati@linaro.org

Maik Riechert
Microsoft
United Kingdom
Email: Maik.Riechert@microsoft.com