Workgroup: TEEP
Internet-Draft: draft-ietf-teep-protocol-08
Published: 7 March 2022
Intended Status: Standards Track
Expires: 8 September 2022
Authors: H. Tschofenig (Arm Ltd.), M. Pei (Broadcom), D. Wheeler (Amazon), D. Thaler (Microsoft), A. Tsukamoto (AIST)

Trusted Execution Environment Provisioning (TEEP) Protocol

Abstract

This document specifies a protocol that installs, updates, and deletes Trusted Components in a device with a Trusted Execution Environment (TEE). This specification defines an interoperable protocol for managing the lifecycle of Trusted Components.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Trusted Execution Environment (TEE) concept has been designed to separate a regular operating system, also referred as a Rich Execution Environment (REE), from security-sensitive applications. In a TEE ecosystem, device vendors may use different operating systems in the REE and may use different types of TEEs. When Trusted Component Developers or Device Administrators use Trusted Application Managers (TAMs) to install, update, and delete Trusted Applications and their dependencies on a wide range of devices with potentially different TEEs then an interoperability need arises.

This document specifies the protocol for communicating between a TAM and a TEEP Agent.

The Trusted Execution Environment Provisioning (TEEP) architecture document [I-D.ietf-teep-architecture] provides design guidance and introduces the necessary terminology.

2. 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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This specification re-uses the terminology defined in [I-D.ietf-teep-architecture].

As explained in Section 4.4 of that document, the TEEP protocol treats each Trusted Application (TA), any dependencies the TA has, and personalization data as separate components that are expressed in SUIT manifests, and a SUIT manifest might contain or reference multiple binaries (see [I-D.ietf-suit-manifest] for more details).

As such, the term Trusted Component (TC) in this document refers to a set of binaries expressed in a SUIT manifest, to be installed in a TEE. Note that a Trusted Component may include one or more TAs and/or configuration data and keys needed by a TA to operate correctly.

Each Trusted Component is uniquely identified by a SUIT Component Identifier (see [I-D.ietf-suit-manifest] Section 8.7.2.2).

3. Message Overview

The TEEP protocol consists of messages exchanged between a TAM and a TEEP Agent. The messages are encoded in CBOR and designed to provide end-to-end security. TEEP protocol messages are signed by the endpoints, i.e., the TAM and the TEEP Agent, but Trusted Applications may also be encrypted and signed by a Trusted Component Developer or Device Administrator. The TEEP protocol not only uses CBOR but also the respective security wrapper, namely COSE [RFC8152]. Furthermore, for software updates the SUIT manifest format [I-D.ietf-suit-manifest] is used, and for attestation the Entity Attestation Token (EAT) [I-D.ietf-rats-eat] format is supported although other attestation formats are also permitted.

This specification defines five messages: QueryRequest, QueryResponse, Update, Success, and Error.

A TAM queries a device's current state with a QueryRequest message. A TEEP Agent will, after authenticating and authorizing the request, report attestation information, list all Trusted Components, and provide information about supported algorithms and extensions in a

QueryResponse message. An error message is returned if the request could not be processed. A TAM will process the QueryResponse message and determine whether to initiate subsequent message exchanges to install, update, or delete Trusted Applications.

```
 +------------+           +-------------+
 | TAM        |           |TEEP Agent   |
 +------------+           +-------------+

   QueryRequest ------->

                          QueryResponse

              <-------       or

                            Error
```

With the Update message a TAM can instruct a TEEP Agent to install and/or delete one or more Trusted Components. The TEEP Agent will process the message, determine whether the TAM is authorized and whether the Trusted Component has been signed by an authorized Trusted Component Signer. A Success message is returned when the operation has been completed successfully, or an Error message otherwise.

```
+------------+           +-------------+
| TAM        |           |TEEP Agent   |
+------------+           +-------------+

           Update  ---->

                           Success

                 <----     or

                           Error
```

4. Detailed Messages Specification

TEEP messages are protected by the COSE_Sign1 structure. The TEEP protocol messages are described in CDDL format [RFC8610] below.

```
{
    teep-message                => (query-request /
                                    query-response /
                                    update /
                                    teep-success /
                                    teep-error ),
}
```

4.1. Creating and Validating TEEP Messages

4.1.1. Creating a TEEP message

To create a TEEP message, the following steps are performed.

1. Create a TEEP message according to the description below and populate it with the respective content. TEEP messages sent by TAMs (QueryRequest and Update) can include a "token". The TAM can decide, in any implementation-specific way, whether to include a token in a message. The first usage of a token generated by a TAM MUST be randomly created. Subsequent token values MUST be different for each subsequent message created by a TAM.

2. Create a COSE Header containing the desired set of Header Parameters. The COSE Header MUST be valid per the [RFC8152] specification.

3. Create a COSE_Sign1 object using the TEEP message as the COSE_Sign1 Payload; all steps specified in [RFC8152] for creating a COSE_Sign1 object MUST be followed.

4.1.2. Validating a TEEP Message

When TEEP message is received (see the ProcessTeepMessage conceptual API defined in [I-D.ietf-teep-architecture] section 6.2.1), the following validation steps are performed. If any of the listed steps fail, then the TEEP message MUST be rejected.

1. Verify that the received message is a valid CBOR object.

2. Verify that the message contains a COSE_Sign1 structure.

3. Verify that the resulting COSE Header includes only parameters and values whose syntax and semantics are both understood and supported or that are specified as being ignored when not understood.

4. Follow the steps specified in Section 4 of [RFC8152] ("Signing Objects") for validating a COSE_Sign1 object. The COSE_Sign1 payload is the content of the TEEP message.

5. Verify that the TEEP message is a valid CBOR map and verify the fields of the TEEP message according to this specification.

4.2. QueryRequest Message

A QueryRequest message is used by the TAM to learn information from the TEEP Agent, such as the features supported by the TEEP Agent, including ciphersuites and protocol versions. Additionally, the TAM can selectively request data items from the TEEP Agent via the request parameter. Currently, the following features are supported:

* Request for attestation information,
* Listing supported extensions,
* Querying installed Trusted Components, and
* Listing supported SUIT commands.

Like other TEEP messages, the QueryRequest message is signed, and the relevant CDDL snippet is shown below. The complete CDDL structure is shown in Appendix C.

```
query-request = [
  type: TEEP-TYPE-query-request,
  options: {
    ? token => bstr .size (8..64),
    ? supported-cipher-suites => [ + suite ],
    ? supported-freshness-mechanisms => [ + freshness-mechanism ],
    ? challenge => bstr .size (8..512),
    ? versions => [ + version ],
    * $$query-request-extensions
    * $$teep-option-extensions
  },
  data-item-requested: data-item-requested
]
```

The message has the following fields:

type
The value of (1) corresponds to a QueryRequest message sent from the TAM to the TEEP Agent.

token
The value in the token parameter is used to match responses to requests. This is particularly useful when a TAM issues multiple concurrent requests to a TEEP Agent. The token MUST be present if and only if the attestation bit is clear in the data-item-requested value. The size of the token is at least 8 bytes (64 bits) and maximum of 64 bytes, which is the same as in an EAT Nonce Claim (see [I-D.ietf-rats-eat] Section 3.3). The first usage of a token generated by a TAM MUST be randomly created. Subsequent token values MUST be different for each request message to distinguish the correct response from multiple requests. The token value MUST NOT be used for other purposes, such as a TAM to identify the devices and/or a device to identify TAMs or Trusted Components. The TAM SHOULD set an expiration time

for each token and MUST ignore any messages with expired tokens. The TAM MUST expire the token value after receiving the first response containing the token value and ignore any subsequent messages that have the same token value.

data-item-requested
The data-item-requested parameter indicates what information the TAM requests from the TEEP Agent in the form of a bitmap. Each value in the bitmap corresponds to an IANA registered information element. This specification defines the following initial set of information elements:

attestation (1) With this value the TAM requests the TEEP Agent to return attestation evidence (e.g., an EAT) in the response.

trusted-components (2) With this value the TAM queries the TEEP Agent for all installed Trusted Components.

extensions (4) With this value the TAM queries the TEEP Agent for supported capabilities and extensions, which allows a TAM to discover the capabilities of a TEEP Agent implementation.

Further values may be added in the future via IANA registration.

supported-cipher-suites
The supported-cipher-suites parameter lists the ciphersuites supported by the TAM. If this parameter is not present, it is to be treated the same as if it contained all ciphersuites defined in this document that are listed as "MUST". Details about the ciphersuite encoding can be found in Section 8.

supported-freshness-mechanisms
The supported-freshness-mechanisms parameter lists the freshness mechanism(s) supported by the TAM. Details about the encoding can be found in Section 9. If this parameter is absent, it means only the nonce mechanism is supported.

challenge
The challenge field is an optional parameter used for ensuring the freshness of the attestation evidence returned with a QueryResponse message. It MUST be absent if the attestation bit is clear (since the token is used instead in that case). When a challenge is provided in the QueryRequest and an EAT is returned with a QueryResponse message then the challenge contained in this request MUST be used to generate the EAT, such as by copying the challenge into the nonce claim found in the EAT if using the Nonce freshness mechanism. For more details see Section 9. If any format other than EAT is used, it is up to that format to define the use of the challenge field.

versions

The versions parameter enumerates the TEEP protocol version(s) supported by the TAM. A value of 0 refers to the current version of the TEEP protocol. If this field is not present, it is to be treated the same as if it contained only version 0.

4.3. QueryResponse Message

The QueryResponse message is the successful response by the TEEP Agent after receiving a QueryRequest message. As discussed in Section 7.2, it can also be sent unsolicited if the contents of the QueryRequest are already known and do not vary per message.

Like other TEEP messages, the QueryResponse message is signed, and the relevant CDDL snippet is shown below. The complete CDDL structure is shown in Appendix C.

```
query-response = [
  type: TEEP-TYPE-query-response,
  options: {
    ? token => bstr .size (8..64),
    ? selected-cipher-suite => suite,
    ? selected-version => version,
    ? evidence-format => text,
    ? evidence => bstr,
    ? tc-list => [ + tc-info ],
    ? requested-tc-list => [ + requested-tc-info ],
    ? unneeded-tc-list => [ + SUIT_Component_Identifier ],
    ? ext-list => [ + ext-info ],
    * $$query-response-extensions,
    * $$teep-option-extensions
  }
]

tc-info = {
  component-id => SUIT_Component_Identifier,
  ? tc-manifest-sequence-number => .within uint .size 8
}

requested-tc-info = {
  component-id => SUIT_Component_Identifier,
  ? tc-manifest-sequence-number => .within uint .size 8
  ? have-binary => bool
}
```

The QueryResponse message has the following fields:

type

The value of (2) corresponds to a QueryResponse message sent from the TEEP Agent to the TAM.

token
The value in the token parameter is used to match responses to requests. The value MUST correspond to the value received with the QueryRequest message if one was present, and MUST be absent if no token was present in the QueryRequest.

selected-cipher-suite
The selected-cipher-suite parameter indicates the selected ciphersuite. Details about the ciphersuite encoding can be found in Section 8.

selected-version
The selected-version parameter indicates the TEEP protocol version selected by the TEEP Agent. The absense of this parameter indicates the same as if it was present with a value of 0.

evidence-format
The evidence-format parameter indicates the IANA Media Type of the attestation evidence contained in the evidence parameter. It MUST be present if the evidence parameter is present and the format is not an EAT.

evidence
The evidence parameter contains the attestation evidence. This parameter MUST be present if the QueryResponse is sent in response to a QueryRequest with the attestation bit set. If the evidence-format parameter is absent, the attestation evidence contained in this parameter MUST be an Entity Attestation Token following the encoding defined in [I-D.ietf-rats-eat]. See Section 4.3.1 for further discussion.

tc-list
The tc-list parameter enumerates the Trusted Components installed on the device in the form of tc-info objects. This parameter MUST be present if the QueryResponse is sent in response to a QueryRequest with the trusted-components bit set.

requested-tc-list
The requested-tc-list parameter enumerates the Trusted Components that are not currently installed in the TEE, but which are requested to be installed, for example by an installer of an Untrusted Application that has a TA as a dependency, or by a Trusted Application that has another Trusted Component as a dependency. Requested Trusted Components are expressed in the form of requested-tc-info objects. A TEEP Agent can get this

information from the RequestTA conceptual API defined in [I-D.ietf-teep-architecture] section 6.2.1.

unneeded-tc-list
The unneeded-tc-list parameter enumerates the Trusted Components that are currently installed in the TEE, but which are no longer needed by any other application. The TAM can use this information in determining whether a Trusted Component can be deleted. Each unneeded Trusted Component is identified by its SUIT Component Identifier. A TEEP Agent can get this information from the UnrequestTA conceptual API defined in [I-D.ietf-teep-architecture] section 6.2.1.

ext-list
The ext-list parameter lists the supported extensions. This document does not define any extensions. This parameter MUST be present if the QueryResponse is sent in response to a QueryRequest with the extensions bit set.

The tc-info object has the following fields:

component-id
A SUIT Component Identifier.

tc-manifest-sequence-number
The suit-manifest-sequence-number value from the SUIT manifest for the Trusted Component, if a SUIT manifest was used.

The requested-tc-info message has the following fields:

component-id
A SUIT Component Identifier.

tc-manifest-sequence-number
The minimum suit-manifest-sequence-number value from a SUIT manifest for the Trusted Component. If not present, indicates that any sequence number will do.

have-binary
If present with a value of true, indicates that the TEEP agent already has the Trusted Component binary and only needs an Update message with a SUIT manifest that authorizes installing it. If have-binary is true, the tc-manifest-sequence-number field MUST be present.

4.3.1. Evidence and Attestation Results

Section 7 of [I-D.ietf-teep-architecture] lists information that may appear in evidence depending on the circumstance. However, the evidence is opaque to the TEEP protocol and there are no formal requirements on the contents of evidence.

TAMs however consume Attestation Results and do need enough information therein to make decisions on how to remediate a TEE that is out of compliance, or update a TEE that is requesting an authorized change. To do so, the information in Section 7 of [I-D.ietf-teep-architecture] is often required depending on the policy. When an Entity Attestation Token is used, the following claims can be used to meet those requirements:

Requirement	Claim	Reference
Device unique identifier	ueid	[I-D.ietf-rats-eat] section 3.4
Vendor of the device	oemid	[I-D.ietf-rats-eat] section 3.6
Class of the device	class-identifier	[I-D.birkholz-rats-suit-claims] section 3.1.2
TEE hardware type	chip-version	[I-D.ietf-rats-eat] section 3.7
TEE hardware version	chip-version	[I-D.ietf-rats-eat] section 3.7
TEE firmware type	sw-name	[I-D.ietf-rats-eat] section 3.9
TEE firmware version	sw-version	[I-D.ietf-rats-eat] section 3.10
Freshness proof	nonce	[I-D.ietf-rats-eat] section 3.3

Table 1

4.4. Update Message

The Update message is used by the TAM to install and/or delete one or more Trusted Components via the TEEP Agent.

Like other TEEP messages, the Update message is signed, and the relevant CDDL snippet is shown below. The complete CDDL structure is shown in Appendix C.

```
update = [
  type: TEEP-TYPE-update,
  options: {
    ? token => bstr .size (8..64),
    ? manifest-list => [ + bstr .cbor SUIT_Envelope ],
    * $$update-extensions,
    * $$teep-option-extensions
  }
]
```

The Update message has the following fields:

type

The value of (3) corresponds to an Update message sent from the TAM to the TEEP Agent. In case of successful processing, a Success message is returned by the TEEP Agent. In case of an error, an Error message is returned. Note that the Update message is used for initial Trusted Component installation as well as for updates and deletes.

token

The value in the token field is used to match responses to requests.

manifest-list

The manifest-list field is used to convey one or multiple SUIT manifests to install. A manifest is a bundle of metadata about a Trusted Component, such as where to find the code, the devices to which it applies, and cryptographic information protecting the manifest. The manifest may also convey personalization data. Trusted Component binaries and personalization data can be signed and encrypted by the same Trusted Component Signer. Other combinations are, however, possible as well. For example, it is also possible for the TAM to sign and encrypt the personalization data and to let the Trusted Component Developer sign and/or encrypt the Trusted Component binary.

Note that an Update message carrying one or more SUIT manifests will inherently involve multiple signatures, one by the TAM in the TEEP message and one from a Trusted Component Signer inside each manifest. This is intentional as they are for different purposes.

The TAM is what authorizes apps to be installed, updated, and deleted on a given TEE and so the TEEP signature is checked by the TEEP Agent at protocol message processing time. (This same TEEP security wrapper is also used on messages like QueryRequest so that Agents only send potentially sensitive data such as evidence to trusted TAMs.)

The Trusted Component signer on the other hand is what authorizes the Trusted Component to actually run, so the manifest signature could be checked at install time or load (or run) time or both, and this checking is done by the TEE independent of whether TEEP is used or some other update mechanism. See section 5 of [I-D.ietf-teep-architecture] for further discussion.

The Update Message has a SUIT_Envelope containing SUIT manifests. Following are some examples of using SUIT manifests in the Update Message.

4.4.1. Example 1: Having one SUIT Manifest pointing to a URI of a Trusted Component Binary

In this example, a SUIT Manifest has a URI pointing to a Trusted Component Binary.

A Trusted Component Developer creates a new Trusted Component Binary and hosts it at a Trusted Component Developer's URI. Then the Trusted Component Developer generates an associated SUIT manifest with the filename "tc-uuid.suit" that contains the URI. The filename "tc-uuid.suit" is used in Example 3 later.

The TAM receives the latest SUIT manifest from the Trusted Component Developer, and the URI it contains will not be changeable by the TAM since the SUIT manifest is signed by the Trusted Component Developer.

Pros:

* The Trusted Component Developer can ensure that the intact Trusted Component Binary is downloaded by devices

* The TAM does not have to send large Update messages containing the Trusted Component Binary

Cons:

* The Trusted Component Developer must host the Trusted Component Binary server

* The device must fetch the Trusted Component Binary in another connection after receiving an Update message

```
+------------+           +-------------+
| TAM        |           | TEEP Agent  |
+------------+           +-------------+

         Update  ---->

+=================== teep-protocol(TAM) ==================+
| TEEP_Message([                                          |
|   TEEP-TYPE-update,                                     |
|   options: {                                            |
|     manifest-list: [                                    |
|       += suit-manifest "tc-uuid.suit" (TC Developper) =+ |
|       | SUIT_Envelope({                                | |
|       |   manifest: {                                  | |
|       |     install: {                                 | |
|       |       set-parameter: {                         | |
|       |         uri: "https://example.org/tc-uuid.ta" | |
|       |       },                                       | |
|       |       fetch                                    | |
|       |     }                                          | |
|       |   }                                            | |
|       | })                                             | |
|       +================================================+ |
|     ]                                                   |
|   }                                                     |
| ])                                                      |
+=========================================================+

and then,

+-------------+           +--------------+
| TEEP Agent  |           | TC Developer |
+-------------+           +--------------+

                 <----

  fetch "https://example.org/tc-uuid.ta"

      +======= tc-uuid.ta =======+
      | 48 65 6C 6C 6F 2C 20 ... |
      +==========================+

Figure 1: URI of the Trusted Component Binary
```

For the full SUIT Manifest example binary, see Appendix "Example 1: SUIT Manifest pointing to URI of the Trusted Component Binary".

4.4.2. Example 2: Having a SUIT Manifest include the Trusted Component Binary

In this example, the SUIT manifest contains the entire Trusted Component Binary using the integrated-payload (see [I-D.ietf-suit-manifest] Section 7.6).

A Trusted Component Developer delegates to the TAM the task of delivering the Trusted Component Binary in the SUIT manifest. The Trusted Component Developer creates a SUIT manifest and embeds the Trusted Component Binary, which is referenced in the URI parameter with identifier "#tc". The Trusted Component Developer provides the SUIT manifest to the TAM.

The TAM serves the SUIT manifest containing the Trusted Component Binary to the device in an Update message.

Pros:

* The device can obtain the Trusted Component Binary and its SUIT manifest together in one Update message
* The Trusted Component Developer does not have to host a server to deliver the Trusted Component Binary directly to devices

Cons:

* The TAM must host the Trusted Component Binary itself, rather than delegating such storage to the Trusted Component Developer
* The TAM must deliver Trusted Component Binaries in Update messages, which result in increased Update message size

```
    +------------+           +-------------+
    | TAM        |           | TEEP Agent  |
    +------------+           +-------------+

             Update  ---->

      +=========== teep-protocol(TAM) ============+
      | TEEP_Message([                            |
      |   TEEP-TYPE-update,                       |
      |   options: {                              |
      |     manifest-list: [                      |
      |       +== suit-manifest(TC Developer) ==+ |
      |       | SUIT_Envelope({                 | |
      |       |   "#tc": h'48 65 6C 6C ...',    | |
      |       |   manifest: {                   | |
      |       |     install: {                  | |
      |       |       set-parameter: {          | |
      |       |         uri: "#tc"              | |
      |       |       },                        | |
      |       |       fetch                     | |
      |       |     }                           | |
      |       |   }                             | |
      |       | })                              | |
      |       +=================================+ |
      |     ]                                     |
      |   }                                       |
      | ])                                        |
      +===========================================+
```

Figure 2: Integrated Payload with Trusted Component Binary

For the full SUIT Manifest example binary, see Appendix "Example 2: SUIT Manifest including the Trusted Component Binary".

4.4.3. Example 3: Supplying Personalization Data for the Trusted Component Binary

In this example, Personalization Data is associated with the Trusted Component Binary "tc-uuid.suit" from Example 1.

The Trusted Component Developer places Personalization Data in a file named "config.json" and hosts it on an HTTPS server. The Trusted Component Developer then creates a SUIT manifest with the URI, specifying which Trusted Component Binary it correlates to in the parameter 'dependency-resolution', and signs the SUIT manifest.

The TAM delivers the SUIT manifest of the Personalization Data which depends on the Trusted Component Binary from Example 1.

```
+------------+           +-------------+
| TAM        |           | TEEP Agent  |
+------------+           +-------------+

         Update  ---->

  +================= teep-protocol(TAM) ======================+
  | TEEP_Message([                                            |
  |   TEEP-TYPE-update,                                       |
  |   options: {                                              |
  |     manifest-list: [                                      |
  |       +======== suit-manifest(TC Developer) ============+ |
  |       | SUIT_Envelope({                                 | |
  |       |   manifest: {                                   | |
  |       |     common: {                                   | |
  |       |       dependencies: [                           | |
  |       |         {{digest-of-tc.suit}}                   | |
  |       |       ]                                         | |
  |       |     }                                           | |
  |       |     dependency-resolution: {                    | |
  |       |       set-parameter: {                          | |
  |       |         uri: "https://example.org/tc-uuid.suit" | |
  |       |       }                                         | |
  |       |       fetch                                     | |
  |       |     }                                           | |
  |       |     install: {                                  | |
  |       |       set-parameter: {                          | |
  |       |         uri: "https://example.org/config.json"  | |
  |       |       },                                        | |
  |       |       fetch                                     | |
  |       |       set-dependency-index                      | |
  |       |       process-dependency                        | |
  |       |     }                                           | |
  |       |   }                                             | |
  |       | })                                              | |
  |       +=================================================+ |
  |     ]                                                     |
  |   }                                                       |
  | ])                                                        |
  +===========================================================+

and then,

+-------------+          +--------------+
| TEEP Agent  |          | TC Developer |
+-------------+          +--------------+

                 <----
  fetch "https://example.org/config.json"
```

```
      +=======config.json========+
      | 7B 22 75 73 65 72 22 ... |
      +==========================+
```

Figure 3: Personalization Data

For the full SUIT Manifest example binary, see Appendix "Example 3: Supplying Personalization Data for Trusted Component Binary".

4.4.4. Example 4: Unlinking Trusted Component

This subsection shows an example deleting the Trusted Component Binary in the TEEP Device.

A Trusted Component Developer can also generate SUIT Manifest which unlinks the installed Trusted Component. The TAM deliver it when the TAM want to uninstall the component.

The directive-unlink (see [I-D.moran-suit-trust-domains] Section-6.5.4) is located in the manifest to delete the Trusted Component. Note that in case other Trusted Components depend on it, i.e. the reference count is not zero, the TEEP Device SHOULD NOT delete it immediately.

```
 +------------+           +-------------+
 | TAM        |           | TEEP Agent  |
 +------------+           +-------------+

          Update  ---->

   +=========== teep-protocol(TAM) ============+
   | TEEP_Message([                            |
   |   TEEP-TYPE-update,                       |
   |   options: {                              |
   |     manifest-list: [                      |
   |       +== suit-manifest(TC Developper) ==+ |
   |       | SUIT_Envelope({                 | |
   |       |   manifest: {                   | |
   |       |     install: [                  | |
   |       |       unlink                    | |
   |       |     ]                           | |
   |       |   }                             | |
   |       | })                              | |
   |       +=================================+ |
   |     ]                                     |
   |   }                                       |
   | ])                                        |
   +===========================================+
```

 Figure 4: Unlink Trusted Component example (summary)

For the full SUIT Manifest example binary, see Appendix E. SUIT Example 4 (Appendix "E.4. Example 4: Unlink a Trusted Component")

4.5. Success Message

The Success message is used by the TEEP Agent to return a success in response to an Update message.

Like other TEEP messages, the Success message is signed, and the relevant CDDL snippet is shown below. The complete CDDL structure is shown in Appendix C.

```
teep-success = [
  type: TEEP-TYPE-teep-success,
  options: {
    ? token => bstr .size (8..64),
    ? msg => text .size (1..128),
    ? suit-reports => [ + suit-report ],
    * $$teep-success-extensions,
    * $$teep-option-extensions
  }
]
```

The Success message has the following fields:

type
The value of (5) corresponds to corresponds to a Success message sent from the TEEP Agent to the TAM.

token
The value in the token parameter is used to match responses to requests. It MUST match the value of the token parameter in the Update message the Success is in response to, if one was present. If none was present, the token MUST be absent in the Success message.

msg
The msg parameter contains optional diagnostics information encoded in UTF-8 [RFC3629] using Net-Unicode form [RFC5198] with max 128 bytes returned by the TEEP Agent.

suit-reports
If present, the suit-reports parameter contains a set of SUIT Reports as defined in Section 4 of [I-D.moran-suit-report]. If a token parameter was present in the Update message the Success message is in response to, the suit-report-nonce field MUST be present in the SUIT Report with a value matching the token parameter in the Update message.

4.6. Error Message

The Error message is used by the TEEP Agent to return an error in response to an Update message.

Like other TEEP messages, the Error message is signed, and the relevant CDDL snippet is shown below. The complete CDDL structure is shown in Appendix C.

```
teep-error = [
  type: TEEP-TYPE-teep-error,
  options: {
     ? token => bstr .size (8..64),
     ? err-msg => text .size (1..128),
     ? supported-cipher-suites => [ + suite ],
     ? supported-freshness-mechanisms => [ + freshness-mechanism ],
     ? versions => [ + version ],
     ? suit-reports => [ + suit-report ],
     * $$teep-error-extensions,
     * $$teep-option-extensions
  },
  err-code: uint (0..23)
]
```

The Error message has the following fields:

type
The value of (6) corresponds to an Error message sent from the TEEP Agent to the TAM.

token
The value in the token parameter is used to match responses to requests. It MUST match the value of the token parameter in the Update message the Success is in response to, if one was present. If none was present, the token MUST be absent in the Error message.

err-msg
The err-msg parameter is human-readable diagnostic text that MUST be encoded using UTF-8 [RFC3629] using Net-Unicode form [RFC5198] with max 128 bytes.

supported-cipher-suites
The supported-cipher-suites parameter lists the ciphersuite(s) supported by the TEEP Agent. Details about the ciphersuite encoding can be found in Section 8. This otherwise optional parameter MUST be returned if err-code is ERR_UNSUPPORTED_CIPHER_SUITES.

supported-freshness-mechanisms
The supported-freshness-mechanisms parameter lists the freshness mechanism(s) supported by the TEEP Agent. Details about the encoding can be found in Section 9. This otherwise optional

parameter MUST be returned if err-code is ERR_UNSUPPORTED_FRESHNESS_MECHANISMS.

versions
The versions parameter enumerates the TEEP protocol version(s) supported by the TEEP Agent. This otherwise optional parameter MUST be returned if err-code is ERR_UNSUPPORTED_MSG_VERSION.

suit-reports
If present, the suit-reports parameter contains a set of SUIT Reports as defined in Section 4 of [I-D.moran-suit-report]. If a token parameter was present in the Update message the Error message is in response to, the suit-report-nonce field MUST be present in the SUIT Report with a value matching the token parameter in the Update message.

err-code
The err-code parameter contains one of the error codes listed below). Only selected values are applicable to each message.

This specification defines the following initial error messages:

ERR_PERMANENT_ERROR (1)
The TEEP request contained incorrect fields or fields that are inconsistent with other fields. For diagnosis purposes it is RECOMMMENDED to identify the failure reason in the error message. A TAM receiving this error might refuse to communicate further with the TEEP Agent for some period of time until it has reason to believe it is worth trying again, but it should take care not to give up on communication when there is no attestation evidence indicating that the error is genuine. In contrast, ERR_TEMPORARY_ERROR is an indication that a more agressive retry is warranted.

ERR_UNSUPPORTED_EXTENSION (2)
The TEEP Agent does not support an extension included in the request message. For diagnosis purposes it is RECOMMMENDED to identify the unsupported extension in the error message. A TAM receiving this error might retry the request without using extensions.

ERR_UNSUPPORTED_FRESHNESS_MECHANISMS (3)
The TEEP Agent does not support any freshness algorithm mechanisms in the request message. A TAM receiving this error

might retry the request using a different set of supported freshness mechanisms in the request message.

ERR_UNSUPPORTED_MSG_VERSION (4)
: The TEEP Agent does not support the TEEP protocol version indicated in the request message. A TAM receiving this error might retry the request using a different TEEP protocol version.

ERR_UNSUPPORTED_CIPHER_SUITES (5)
: The TEEP Agent does not support any ciphersuites indicated in the request message. A TAM receiving this error might retry the request using a different set of supported ciphersuites in the request message.

ERR_BAD_CERTIFICATE (6)
: Processing of a certificate failed. For diagnosis purposes it is RECOMMMENDED to include information about the failing certificate in the error message. For example, the certificate was of an unsupported type, or the certificate was revoked by its signer. A TAM receiving this error might attempt to use an alternate certificate.

ERR_CERTIFICATE_EXPIRED (9)
: A certificate has expired or is not currently valid. A TAM receiving this error might attempt to renew its certificate before using it again.

ERR_TEMPORARY_ERROR (10)
: A miscellaneous temporary error, such as a memory allocation failure, occurred while processing the request message. A TAM receiving this error might retry the same request at a later point in time.

ERR_MANIFEST_PROCESSING_FAILED (17)
: The TEEP Agent encountered one or more manifest processing failures. If the suit-reports parameter is present, it contains the failure details. A TAM receiving this error might still attempt to install or update other components that do not depend on the failed manifest.

New error codes should be added sparingly, not for every implementation error. That is the intent of the err-msg field, which can be used to provide details meaningful to humans. New error codes should only be added if the TAM is expected to do something behaviorally different upon receipt of the error message, rather than just logging the event. Hence, each error code is responsible for saying what the behavioral difference is expected to be.

5. EAT Profile

The TEEP protocol operates between a TEEP Agent and a TAM. While the TEEP protocol does not require use of EAT, use of EAT is encouraged and Section 4.3 explicitly defines a way to carry an Entity Attestation Token evidence in a QueryResponse.

As discussed in Section 4.3.1, the content of attestation evidence is opaque to the TEEP architecture, but the content of Attestation Results is not, where Attestation Results flow between a Verifier and a TAM (as the Relying Party). Although Attestation Results required by a TAM are separable from the TEEP protocol per se, this section is included as part of the requirements for building a compliant TAM that uses EATs for Attestation Results.

Section 7 of [I-D.ietf-rats-eat] defines the requirement for Entity Attestation Token profiles. This section defines an EAT profile for use with TEEP.

*profile-label: The profile-label for this specification is the URI

https://datatracker.ietf.org/doc/html/draft-ietf-teep-protocol-08. (RFC-editor: upon RFC publication, replace string with "https://www.rfc-editor.org/info/rfcXXXX" where XXXX is the RFC number of this document.)

*Use of JSON, CBOR, or both: CBOR only.

*CBOR Map and Array Encoding: Only definite length arrays and maps.

*CBOR String Encoding: Only definite-length strings are allowed.

*CBOR Preferred Serialization: Encoders must use preferred serialization, and decoders need not accept non-preferred serialization.

*COSE/JOSE Protection: See Section 8.

*Detached EAT Bundle Support: DEB use is permitted.

*Verification Key Identification: COSE Key ID (kid) is used, where the key ID is the hash of a public key (where the public key may be used as a raw public key, or in a certificate).

*Endorsement Identification: Optional, but semantics are the same as in Verification Key Identification.

*Freshness: See Section 9.

*Required Claims: None.

*Prohibited Claims: None.

*Additional Claims: Optional claims are those listed in Section 4.3.1.

*Refined Claim Definition: None.

*CBOR Tags: CBOT Tags are not used.

*Manifests and Software Evidence Claims: The sw-name claim for a Trusted Component holds the URI of the SUIT manifest for that component.

6. Mapping of TEEP Message Parameters to CBOR Labels

In COSE, arrays and maps use strings, negative integers, and unsigned integers as their keys. Integers are used for compactness of encoding. Since the word "key" is mainly used in its other meaning, as a cryptographic key, this specification uses the term "label" for this usage as a map key.

This specification uses the following mapping:

Name	Label
supported-cipher-suites	1
challenge	2
version	3
selected-cipher-suite	5
selected-version	6
evidence	7
tc-list	8
ext-list	9
manifest-list	10
msg	11
err-msg	12
evidence-format	13
requested-tc-list	14
unneeded-tc-list	15
component-id	16
tc-manifest-sequence-number	17
have-binary	18
suit-reports	19
token	20
supported-freshness-mechanisms	21

Table 2

7. Behavior Specification

Behavior is specified in terms of the conceptual APIs defined in section 6.2.1 of [I-D.ietf-teep-architecture].

7.1. TAM Behavior

When the ProcessConnect API is invoked, the TAM sends a QueryRequest message.

When the ProcessTeepMessage API is invoked, the TAM first does validation as specified in Section 4.1.2, and drops the message if it is not valid. Otherwise, it proceeds as follows.

If the message includes a token, it can be used to match the response to a request previously sent by the TAM. The TAM MUST expire the token value after receiving the first response from the device that has a valid signature and ignore any subsequent messages that have the same token value. The token value MUST NOT be used for other purposes, such as a TAM to identify the devices and/or a device to identify TAMs or Trusted Components.

If a QueryResponse message is received that contains evidence, the evidence is passed to an attestation Verifier (see [I-D.ietf-rats-architecture]) to determine whether the Agent is in a trustworthy state. Based on the results of attestation, and the lists of installed, requested, and unneeded Trusted Components reported in the QueryResponse, the TAM determines, in any implementation specific manner, which Trusted Components need to be installed, updated, or deleted, if any. If any Trusted Components need to be installed, updated, or deleted, the TAM sends an Update message containing SUIT Manifests with command sequences to do the relevant installs, updates, or deletes. It is important to note that the TEEP Agent's Update Procedure requires resolving and installing any dependencies indicated in the manifest, which may take some time, and the resulting Success or Error message is generated only after completing the Update Procedure. Hence, depending on the freshness mechanism in use, the TAM may need to store data (e.g., a nonce) for some time.

If a Success or Error message is received containing one or more SUIT Reports, the TAM also validates that the nonce in any SUIT Report matches the token sent in the Update message, and drops the message if it does not match. Otherwise, the TAM handles the update in any implementation specific way, such as updating any locally cached information about the state of the TEEP Agent, or logging the results.

If any other Error message is received, the TAM can handle it in any implementation specific way, but Section 4.6 provides recommendations for such handling.

7.2. TEEP Agent Behavior

When the RequestTA API is invoked, the TEEP Agent first checks whether the requested TA is already installed. If it is already installed, the TEEP Agent passes no data back to the caller. Otherwise, if the TEEP Agent chooses to initiate the process of requesting the indicated TA, it determines (in any implementation specific way) the TAM URI based on any TAM URI provided by the RequestTA caller and any local configuration, and passes back the TAM URI to connect to. It MAY also pass back a QueryResponse message if all of the following conditions are true:

* The last QueryRequest message received from that TAM contained no token or challenge,

* The ProcessError API was not invoked for that TAM since the last QueryResponse message was received from it, and

* The public key or certificate of the TAM is cached and not expired.

When the RequestPolicyCheck API is invoked, the TEEP Agent decides whether to initiate communication with any trusted TAMs (e.g., it might choose to do so for a given TAM unless it detects that it has already communicated with that TAM recently). If so, it passes back a TAM URI to connect to. If the TEEP Agent has multiple TAMs it needs to connect with, it just passes back one, with the expectation that RequestPolicyCheck API will be invoked to retrieve each one successively until there are no more and it can pass back no data at that time. Thus, once a TAM URI is returned, the TEEP Agent can remember that it has already initiated communication with that TAM.

When the ProcessError API is invoked, the TEEP Agent can handle it in any implementation specific way, such as logging the error or using the information in future choices of TAM URI.

When the ProcessTeepMessage API is invoked, the Agent first does validation as specified in Section 4.1.2, and drops the message if it is not valid. Otherwise, processing continues as follows based on the type of message.

When a QueryRequest message is received, the Agent responds with a QueryResponse message if all fields were understood, or an Error message if any error was encountered.

When an Update message is received, the Agent attempts to update the Trusted Components specified in the SUIT manifests by following the Update Procedure specified in [I-D.ietf-suit-manifest], and responds with a Success message if all SUIT manifests were successfully installed, or an Error message if any error was encountered. It is important to note that the Update Procedure requires resolving and installing any dependencies indicated in the manifest, which may take some time, and the Success or Error message is generated only after completing the Update Procedure.

8. Ciphersuites

The TEEP protocol uses COSE for protection of TEEP messages. After a QueryResponse is received, the selected cryptographic algorithm is used in subsequent TEEP messages (Install, Success, and Error). To negotiate cryptographic mechanisms and algorithms, the TEEP protocol defines the following ciphersuite structure.

```
ciphersuite = [
    teep-cose-sign-algs / nil,
    teep-cose-encrypt-algs / nil ,
    teep-cose-mac-algs / nil
]
```

The ciphersuite structure is used to present the combination of mechanisms and cryptographic algorithms. Each suite value corresponds with a COSE-type defined in Section 2 of [RFC8152].

```
supported-cipher-suites = [ + suite ]
```

Cryptographic algorithm values are defined in the COSE Algorithms registry [COSE.Algorithm]. A TAM MUST support both of the following ciphersuites. A TEEP Agent MUST support at least one of the two but can choose which one. For example, a TEEP Agent might choose a given ciphersuite if it has hardware support for it.

```
teep-cose-sign-algs /= cose-alg-es256,
teep-cose-sign-algs /= cose-alg-eddsa
```

A TAM or TEEP Agent MUST also support the following algorithms:

```
teep-cose-encrypt-algs /= cose-alg-accm-16-64-128
```

```
teep-cose-mac-algs /= cose-alg-hmac-256
```

A TAM or TEEP Agent MAY also support one or more of the following algorithms:

```
teep-cose-sign-algs /= cose-alg-ps256,
teep-cose-sign-algs /= cose-alg-ps384,
teep-cose-sign-algs /= cose-alg-ps512,
teep-cose-sign-algs /= cose-alg-rsa-oaep-256,
teep-cose-sign-algs /= cose-alg-rsa-oaep-512
```

Any ciphersuites without confidentiality protection can only be added if the associated specification includes a discussion of security considerations and applicability, since manifests may carry sensitive information. For example, Section 6 of [I-D.ietf-teep-architecture] permits implementations that terminate transport security inside the TEE and if the transport security provides confidentiality then additional encryption might not be needed in the manifest for some use cases. For most use cases, however, manifest confidentiality will be needed to protect sensitive fields from the TAM as discussed in Section 9.8 of [I-D.ietf-teep-architecture].

9. Freshness Mechanisms

A freshness mechanism determines how a TAM can tell whether evidence provided in a Query Response is fresh. There are multiple ways this can be done as discussed in Section 10 of [I-D.ietf-rats-architecture].

Each freshness mechanism is identified with an integer value, which corresponds to an IANA registered freshness mechanism (see Section 11.2. This document defines the following freshness mechanisms:

Value	Freshness mechanism
1	Nonce
2	Timestamp
3	Epoch ID

Table 3

In the Nonce mechanism, the evidence MUST include a nonce provided in the QueryRequest challenge. In other mechanisms, a timestamp or epoch ID determined via mechanisms outside the TEEP protocol is used, and the challenge is only needed in the QueryRequest message if a challenge is needed in generating evidence for reasons other than freshness.

If a TAM supports multiple freshness mechanisms that require different challenge formats, the QueryRequest message can currently only send one such challenge. This situation is expected to be rare, but should it occur, the TAM can choose to prioritize one of them and exclude the other from the supported-freshness-mechanisms in the QueryRequest, and resend the QueryRequest with the other mechanism if an ERR_UNSUPPORTED_FRESHNESS_MECHANISMS Error is received that indicates the TEEP Agent supports the other mechanism.

10. Security Considerations

This section summarizes the security considerations discussed in this specification:

Cryptographic Algorithms
TEEP protocol messages exchanged between the TAM and the TEEP Agent are protected using COSE. This specification relies on the cryptographic algorithms provided by COSE. Public key based authentication is used by the TEEP Agent to authenticate the TAM and vice versa.

Attestation
A TAM can rely on the attestation evidence provided by the TEEP Agent. To sign the attestation evidence, it is necessary for the device to possess a public key (usually in the form of a certificate [RFC5280]) along with the corresponding private key. Depending on the properties of the attestation mechanism, it is possible to uniquely identify a device based on information in the attestation evidence or in the certificate used to sign the attestation evidence. This uniqueness may raise privacy concerns. To lower the privacy implications the TEEP Agent MUST present its attestation evidence only to an authenticated and authorized TAM and when using EATS, it SHOULD use encryption as discussed in [I-D.ietf-rats-eat], since confidentiality is not provided by the TEEP protocol itself and the transport protocol under the TEEP protocol might be implemented outside of any TEE. If any mechanism other than EATs is used, it is up to that mechanism to specify how privacy is provided.

Trusted Component Binaries
Each Trusted Component binary is signed by a Trusted Component Signer. It is the responsibility of the TAM to relay only verified Trusted Components from authorized Trusted Component Signers. Delivery of a Trusted Component to the TEEP Agent is then the responsibility of the TAM, using the security mechanisms provided by the TEEP protocol. To protect the Trusted Component binary, the SUIT manifest format is used and it offers a variety of security features, including digitial signatures and symmetric encryption.

Personalization Data
A Trusted Component Signer or TAM can supply personalization data along with a Trusted Component. This data is also protected by a SUIT manifest. Personalization data signed and encrypted by a Trusted Component Signer other than the TAM is opaque to the TAM.

TEEP Broker

As discussed in section 6 of [I-D.ietf-teep-architecture], the TEEP protocol typically relies on a TEEP Broker to relay messages between the TAM and the TEEP Agent. When the TEEP Broker is compromised it can drop messages, delay the delivery of messages, and replay messages but it cannot modify those messages. (A replay would be, however, detected by the TEEP Agent.) A compromised TEEP Broker could reorder messages in an attempt to install an old version of a Trusted Component. Information in the manifest ensures that TEEP Agents are protected against such downgrade attacks based on features offered by the manifest itself.

Trusted Component Signer Compromise

A TAM is responsible for vetting a Trusted Component and before distributing them to TEEP Agents.

It is RECOMMENDED to provide a way to update the trust anchor store used by the TEE, for example using a firmware update mechanism. Thus, if a Trusted Component Signer is later compromised, the TAM can update the trust anchor store used by the TEE, for example using a firmware update mechanism.

CA Compromise

The CA issuing certificates to a TEE or a Trusted Component Signer might get compromised. It is RECOMMENDED to provide a way to update the trust anchor store used by the TEE, for example using a firmware update mechanism. If the CA issuing certificates to devices gets compromised then these devices might be rejected by a TAM, if revocation is available to the TAM.

TAM Certificate Expiry

The integrity and the accuracy of the clock within the TEE determines the ability to determine an expired TAM certificate, if certificates are used.

Compromised Time Source

As discussed above, certificate validity checks rely on comparing validity dates to the current time, which relies on having a trusted source of time, such as [RFC8915]. A compromised time source could thus be used to subvert such validity checks.

11. IANA Considerations

11.1. Media Type Registration

IANA is requested to assign a media type for application/teep+cbor.

Type name: application

Subtype name:
teep+cbor

Required parameters: none

Optional parameters: none

Encoding considerations: Same as encoding considerations of application/cbor.

Security considerations: See Security Considerations Section of this document.

Interoperability considerations: Same as interoperability considerations of application/cbor as specified in [RFC7049].

Published specification: This document.

Applications that use this media type: TEEP protocol implementations

Fragment identifier considerations: N/A

Additional information:

Deprecated alias names for this type: N/A

Magic number(s): N/A

File extension(s): N/A

Macintosh file type code(s): N/A

Person to contact for further information: teep@ietf.org

Intended usage: COMMON

Restrictions on usage: none

Author: See the "Authors' Addresses" section of this document

Change controller: IETF

11.2. Freshness Mechanism Registry

IANA is also requested to create a new registry for freshness mechanisms.

Name of registry: TEEP Freshness Mechanisms

Policy: Specification Required [RFC8126]

Additional requirements: The specification must document relevant security considerations.

Initial values:

Value	Freshness mechanism	Specification
1	Nonce	RFC TBD Section 9
2	Timestamp	RFC TBD Section 9
3	Epoch ID	RFC TBD Section 9

Table 4

(RFC Editor: please replace TBD above with the number assigned to this document.)

12. References

12.1. Normative References

[COSE.Algorithm] IANA, "COSE Algorithms", n.d., <https://www.iana.org/assignments/cose/cose.xhtml#algorithms>.

[I-D.ietf-rats-architecture] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote Attestation Procedures Architecture", Work in Progress, Internet-Draft, draft-ietf-rats-architecture-15, 8 February 2022, <https://www.ietf.org/archive/id/draft-ietf-rats-architecture-15.txt>.

[I-D.ietf-rats-eat] Lundblade, L., Mandyam, G., and J. O'Donoghue, "The Entity Attestation Token (EAT)", Work in Progress, Internet-Draft, draft-ietf-rats-eat-12, 24 February 2022, <https://www.ietf.org/archive/id/draft-ietf-rats-eat-12.txt>.

[I-D.ietf-suit-manifest] Moran, B., Tschofenig, H., Birkholz, H., and K. Zandberg, "A Concise Binary Object Representation (CBOR)-based Serialization Format for the Software Updates for Internet of Things (SUIT) Manifest", Work in Progress, Internet-Draft, draft-ietf-suit-manifest-16, 25 October 2021, <https://www.ietf.org/archive/id/draft-ietf-suit-manifest-16.txt>.

[I-D.moran-suit-report] Moran, B., "Secure Reporting of Update Status", Work in Progress, Internet-Draft, draft-moran-suit-report-01, 22 February 2021, <https://www.ietf.org/archive/id/draft-moran-suit-report-01.txt>.

[I-D.moran-suit-trust-domains]
Moran, B., "SUIT Manifest Extensions for Multiple Trust Domains", Work in Progress, Internet-Draft, draft-moran-

suit-trust-domains-00, 25 October 2021, <https://www.ietf.org/archive/id/draft-moran-suit-trust-domains-00.txt>.

[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>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <https://www.rfc-editor.org/info/rfc3629>.

[RFC5198] Klensin, J. and M. Padlipsky, "Unicode Format for Network Interchange", RFC 5198, DOI 10.17487/RFC5198, March 2008, <https://www.rfc-editor.org/info/rfc5198>.

[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, <https://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, <https://www.rfc-editor.org/info/rfc7049>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[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>.

12.2. Informative References

[I-D.birkholz-rats-suit-claims] Birkholz, H. and B. Moran, "Trustworthiness Vectors for the Software Updates of Internet of Things (SUIT) Workflow Model", Work in Progress, Internet-Draft, draft-birkholz-rats-suit-claims-03, 12 January 2022, <https://www.ietf.org/archive/id/draft-birkholz-rats-suit-claims-03.txt>.

[I-D.ietf-teep-architecture] Pei, M., Tschofenig, H., Thaler, D., and D. Wheeler, "Trusted Execution Environment Provisioning (TEEP) Architecture", Work in Progress, Internet-Draft, draft-ietf-teep-architecture-16, 28 February 2022, <https://www.ietf.org/archive/id/draft-ietf-teep-architecture-16.txt>.

[RFC8126]
Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[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>.

[RFC8915] Franke, D., Sibold, D., Teichel, K., Dansarie, M., and R. Sundblad, "Network Time Security for the Network Time Protocol", RFC 8915, DOI 10.17487/RFC8915, September 2020, <https://www.rfc-editor.org/info/rfc8915>.

A. Contributors

We would like to thank Brian Witten (Symantec), Tyler Kim (Solacia), Nick Cook (Arm), and Minho Yoo (IoTrust) for their contributions to the Open Trust Protocol (OTrP), which influenced the design of this specification.

B. Acknowledgements

We would like to thank Eve Schooler for the suggestion of the protocol name.

We would like to thank Kohei Isobe (TRASIO/SECOM), Ken Takayama (SECOM) Kuniyasu Suzaki (TRASIO/AIST), Tsukasa Oi (TRASIO), and Yuichi Takita (SECOM) for their valuable implementation feedback.

We would also like to thank Carsten Bormann and Henk Birkholz for their help with the CDDL.

C. Complete CDDL

Valid TEEP messages MUST adhere to the following CDDL data definitions, except that SUIT_Envelope and SUIT_Component_Identifier are specified in [I-D.ietf-suit-manifest].

```
teep-message = $teep-message-type .within teep-message-framework

SUIT_Envelope = any

teep-message-framework = [
  type: uint (0..23) / $teep-type-extension,
  options: { * teep-option },
  * uint; further integers, e.g., for data-item-requested
]

teep-option = (uint => any)

; messages defined below:
$teep-message-type /= query-request
$teep-message-type /= query-response
$teep-message-type /= update
$teep-message-type /= teep-success
$teep-message-type /= teep-error

; message type numbers, uint (0..23)
TEEP-TYPE-query-request = 1
TEEP-TYPE-query-response = 2
TEEP-TYPE-update = 3
TEEP-TYPE-teep-success = 5
TEEP-TYPE-teep-error = 6

version = .within uint .size 4
ext-info = .within uint .size 4

; data items as bitmaps
data-item-requested = $data-item-requested .within uint .size 8
attestation = 1
$data-item-requested /= attestation
trusted-components = 2
$data-item-requested /= trusted-components
extensions = 4
$data-item-requested /= extensions

query-request = [
  type: TEEP-TYPE-query-request,
  options: {
    ? token => bstr .size (8..64),
    ? supported-cipher-suites => [ + suite ],
    ? supported-freshness-mechanisms => [ + freshness-mechanism ],
    ? challenge => bstr .size (8..512),
    ? versions => [ + version ],
    * $$query-request-extensions
    * $$teep-option-extensions
  },
  data-item-requested: data-item-requested
```

```
]

; ciphersuites
suite = [
    teep-cose-sign-algs / nil,
    teep-cose-encrypt-algs / nil,
    teep-cose-mac-algs / nil
]

teep-cose-sign-algs /= cose-alg-es256,
teep-cose-sign-algs /= cose-alg-eddsa
teep-cose-sign-algs /= cose-alg-ps256,
teep-cose-sign-algs /= cose-alg-ps384,
teep-cose-sign-algs /= cose-alg-ps512,
teep-cose-sign-algs /= cose-alg-rsa-oaep-256,
teep-cose-sign-algs /= cose-alg-rsa-oaep-512

teep-cose-encrypt-algs /= cose-alg-accm-16-64-128

teep-cose-mac-algs /= cose-alg-hmac-256

; algorithm identifiers defined in the IANA COSE Algorithms Registry
cose-alg-es256 = -7
cose-alg-eddsa = -8
cose-alg-ps256 = -37
cose-alg-ps384 = -38
cose-alg-ps512 = -39
cose-alg-rsa-oaep-256 = -41
cose-alg-rsa-oaep-512 = -42
cose-alg-accm-16-64-128 = 10
cose-alg-hmac-256 = 5

; freshness-mechanisms

freshness-mechanism = $TEEP-freshness-mechanism .within uint .size 4

FRESHNESS_NONCE = 0
FRESHNESS_TIMESTAMP = 1
FRESHNESS_EPOCH_ID = 2

$TEEP-freshness-mechanism /= FRESHNESS_NONCE
$TEEP-freshness-mechanism /= FRESHNESS_TIMESTAMP
$TEEP-freshness-mechanism /= FRESHNESS_EPOCH_ID

query-response = [
  type: TEEP-TYPE-query-response,
  options: {
    ? token => bstr .size (8..64),
    ? selected-cipher-suite => suite,
    ? selected-version => version,
    ? evidence-format => text,
    ? evidence => bstr,
    ? tc-list => [ + tc-info ],
    ? requested-tc-list => [ + requested-tc-info ],
    ? unneeded-tc-list => [ + SUIT_Component_Identifier ],
    ? ext-list => [ + ext-info ],
    * $$query-response-extensions,
    * $$teep-option-extensions
  }
]

tc-info = {
  component-id => SUIT_Component_Identifier,
  ? tc-manifest-sequence-number => .within uint .size 8
}

requested-tc-info = {
  component-id => SUIT_Component_Identifier,
  ? tc-manifest-sequence-number => .within uint .size 8
  ? have-binary => bool
}

update = [
  type: TEEP-TYPE-update,
  options: {
    ? token => bstr .size (8..64),
    ? manifest-list => [ + bstr .cbor SUIT_Envelope ],
    * $$update-extensions,
    * $$teep-option-extensions
  }
]

teep-success = [
  type: TEEP-TYPE-teep-success,
  options: {
    ? token => bstr .size (8..64),
    ? msg => text .size (1..128),
    ? suit-reports => [ + suit-report ],
    * $$teep-success-extensions,
    * $$teep-option-extensions
  }
]

teep-error = [
  type: TEEP-TYPE-teep-error,
  options: {
     ? token => bstr .size (8..64),
     ? err-msg => text .size (1..128),
     ? supported-cipher-suites => [ + suite ],
     ? supported-freshness-mechanisms => [ + freshness-mechanism ],
     ? versions => [ + version ],
     ? suit-reports => [ + suit-report ],
     * $$teep-error-extensions,
     * $$teep-option-extensions
  },
  err-code: uint (0..23)
]

; The err-code parameter, uint (0..23)
ERR_PERMANENT_ERROR = 1
ERR_UNSUPPORTED_EXTENSION = 2
ERR_UNSUPPORTED_FRESHNESS_MECHANISMS = 3
ERR_UNSUPPORTED_MSG_VERSION = 4
ERR_UNSUPPORTED_CIPHER_SUITES = 5
ERR_BAD_CERTIFICATE = 6
ERR_CERTIFICATE_EXPIRED = 9
ERR_TEMPORARY_ERROR = 10
ERR_MANIFEST_PROCESSING_FAILED = 17

; labels of mapkey for teep message parameters, uint (0..23)
supported-cipher-suites = 1
challenge = 2
versions = 3
selected-cipher-suite = 5
selected-version = 6
evidence = 7
tc-list = 8
ext-list = 9
manifest-list = 10
msg = 11
err-msg = 12
evidence-format = 13
requested-tc-list = 14
unneeded-tc-list = 15
component-id = 16
tc-manifest-sequence-number = 17
have-binary = 18
suit-reports = 19
token = 20
supported-freshness-mechanisms = 21
```

D. Examples of Diagnostic Notation and Binary Representation

This section includes some examples with the following assumptions:

- The device will have two TCs with the following SUIT Component Identifiers:
  - [0x000102030405060708090a0b0c0d0e0f]
  - [0x100102030405060708090a0b0c0d0e0f]
- SUIT manifest-list is set empty only for example purposes (see Appendix E for actual manifest examples)

D.1. QueryRequest Message

D.1.1. CBOR Diagnostic Notation

```
/ query-request = /
[
  1,  / type : TEEP-TYPE-query-request = 1 (uint (0..23)) /
  / options : /
  {
    20 : 0xa0a1a2a3a4a5a6a7a8a9aaabacadaeaf,
            / token = 20 (mapkey) :
              h'a0a1a2a3a4a5a6a7a8a9aaabacadaeaf' (bstr .size (8..64)),
              generated by TAM /
    1 : [ 1 ], / supported-cipher-suites = 1 (mapkey) :
                 TEEP-AES-CCM-16-64-128-HMAC256--256-X25519-EdDSA =
                 [ 1 ] (array of .within uint .size 4) /
    3 : [ 0 ] / version = 3 (mapkey) :
                 [ 0 ] (array of .within uint .size 4) /
  },
  3   / data-item-requested :
        attestation | trusted-components = 3 (.within uint .size 8) /
]
```

D.1.2. CBOR Binary Representation

```
83                       # array(3)
  01                     # unsigned(1) uint (0..23)
  A4                     # map(4)
    14                   # unsigned(20) uint (0..23)
    4F                   # bytes(16) (8..64)
      A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
    01                   # unsigned(1) uint (0..23)
    81                   # array(1)
      01                 # unsigned(1) within uint .size 4
    03                   # unsigned(3) uint (0..23)
    81                   # array(1)
      00                 # unsigned(0) within uint .size 4
    04                   # unsigned(4) uint (0..23)
    43                   # bytes(3)
      010203             # "\x01\x02\x03"
  03                     # unsigned(3) .within uint .size 8
```

D.2. Entity Attestation Token

This is shown below in CBOR diagnostic form. Only the payload signed by COSE is shown.

D.2.1. CBOR Diagnostic Notation

```
/ eat-claim-set = /
{
    / issuer /                   1: "joe",
    / timestamp (iat) /          6: 1(1526542894)
    / nonce /                   10: h'948f8860d13a463e8e',
    / secure-boot /             15: true,
    / debug-status /            16: 3, / disabled-permanently /
    / security-level /          14: 3, / secure-restricted /
    / device-identifier /    <TBD>: h'e99600dd921649798b013e9752dcf0c5',
    / vendor-identifier /    <TBD>: h'2b03879b33434a7ca682b8af84c19fd4',
    / class-identifier /     <TBD>: h'9714a5796bd245a3a4ab4f977cb8487f',
    / chip-version /            26: [ "MyTEE", 1 ],
    / component-identifier / <TBD>: h'60822887d35e43d5b603d18bcaa3f08d',
    / version /              <TBD>: "v0.1"
}
```

D.3. QueryResponse Message

D.3.1. CBOR Diagnostic Notation

```
/ query-response = /
[
  2,  / type : TEEP-TYPE-query-response = 2 (uint (0..23)) /
  / options : /
  {
    20 : 0xa0a1a2a3a4a5a6a7a8a9aaabacadaeaf,
            / token = 20 (mapkey) :
              h'a0a1a2a3a4a5a6a7a8a9aaabacadaeaf' (bstr .size (8..64)),
              given from TAM's QueryRequest message /
    5 : 1,  / selected-cipher-suite = 5 (mapkey) :
              TEEP-AES-CCM-16-64-128-HMAC256--256-X25519-EdDSA =
              1 (.within uint .size 4) /
    6 : 0,  / selected-version = 6 (mapkey) :
              0 (.within uint .size 4) /
    7 : ... / evidence = 7 (mapkey) :
              Entity Attestation Token /
    8 : [   / tc-list = 8 (mapkey) : (array of tc-info) /
      {
        16 : [ 0x000102030405060708090a0b0c0d0e0f ] / component-id =
               16 (mapkey) : [ h'000102030405060708090a0b0c0d0e0f' ]
               (SUIT_Component_Identifier =  [* bstr]) /
      },
      {
        16 : [ 0x100102030405060708090a0b0c0d0e0f ] / component-id =
               16 (mapkey) : [ h'100102030405060708090a0b0c0d0e0f' ]
               (SUIT_Component_Identifier =  [* bstr]) /
      }
        ]
    }
]
```

D.3.2. CBOR Binary Representation

```
82                       # array(2)
  02                     # unsigned(2) uint (0..23)
  A5                     # map(5)
    14                   # unsigned(20) uint (0..23)
    4F                   # bytes(16) (8..64)
      A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
    05                   # unsigned(5) uint (0..23)
    01                   # unsigned(1) .within uint .size 4
    06                   # unsigned(6) uint (0..23)
    00                   # unsigned(0) .within uint .size 4
    07                   # unsigned(7) uint (0..23)
      ...                # Entity Attestation Token
    08                   # unsigned(8) uint (0..23)
    82                   # array(2)
      81                 # array(1)
        4F               # bytes(16)
          000102030405060708090A0B0C0D0E0F
      81                 # array(1)
        4F               # bytes(16)
          100102030405060708090A0B0C0D0E0F
```

D.4. Update Message

D.4.1. CBOR Diagnostic Notation

```
/ update = /
[
  3,  / type : TEEP-TYPE-update = 3 (uint (0..23)) /
  / options : /
  {
    20 : 0xa0a1a2a3a4a5a6a7a8a9aaabacadaeaf,
             / token = 20 (mapkey) :
               h'a0a1a2a3a4a5a6a7a8a9aaabacadaeaf' (bstr .size (8..64)),
               generated by TAM /
    10 : [ ] / manifest-list = 10 (mapkey) :
               [ ] (array of bstr wrapped SUIT_Envelope(any)) /
             / empty, example purpose only /
  }
]
```

D.4.2. CBOR Binary Representation

```
82                       # array(2)
  03                     # unsigned(3) uint (0..23)
  A3                     # map(3)
    14                   # unsigned(20) uint (0..23)
    4F                   # bytes(16) (8..64)
      A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
    0A                   # unsigned(10) uint (0..23)
    80                   # array(0)
```

D.5. Success Message

D.5.1. CBOR Diagnostic Notation

```
/ teep-success = /
[
  5,  / type : TEEP-TYPE-teep-success = 5 (uint (0..23)) /
  / options : /
  {
    20 : 0xa0a1a2a3a4a5a6a7a8a9aaabacadaeaf,
             / token = 20 (mapkey) :
               h'a0a1a2a3a4a5a6a7a8a9aaabacadaeaf' (bstr .size (8..64)),
               given from TAM's Update message /
  }
]
```

D.5.2. CBOR Binary Representation

```
82                       # array(2)
  05                     # unsigned(5) uint (0..23)
  A1                     # map(1)
    14                   # unsigned(20) uint (0..23)
    4F                   # bytes(16) (8..64)
      A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
```

D.6. Error Message

D.6.1. CBOR Diagnostic Notation

```
/ teep-error = /
[
  6,  / type : TEEP-TYPE-teep-error = 6 (uint (0..23)) /
  / options : /
  {
    20 : 0xa0a1a2a3a4a5a6a7a8a9aaabacadaeaf,
           / token = 20 (mapkey) :
             h'a0a1a2a3a4a5a6a7a8a9aaabacadaeaf' (bstr .size (8..64)),
             given from TAM's Update message /
    12 : "disk-full"  / err-msg = 12 (mapkey) :
                        "disk-full" (text .size (1..128)) /
  },
  17, / err-code : ERR_MANIFEST_PROCESSING_FAILED = 17 (uint (0..23)) /
]
```

D.6.2. CBOR binary Representation

```
83                        # array(3)
  06                      # unsigned(6) uint (0..23)
  A2                      # map(2)
    14                    # unsigned(20) uint (0..23)
    4F                    # bytes(16) (8..64)
      A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
    0C                    # unsigned(12) uint (0..23)
    69                    # text(9) (1..128)
      6469736B2D66756C6C # "disk-full"
  11                      # unsigned(17) uint (0..23)
```

E. Examples of SUIT Manifests

This section shows some examples of SUIT manifests described in Section 4.4.

The examples are signed using the following ECDSA secp256r1 key with SHA256 as the digest function.

COSE_Sign1 Cryptographic Key:

```
-----BEGIN PRIVATE KEY-----
MIGHAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0wawIBAQQgApZYjZCUGLM50VBC
CjYStX+09jGmnyJPrpDLTz/hiXOhRANCAASEloEarguqq9JhVxie7NomvqqL8Rtv
P+bitWWchdvArTsfKktsCYExwKNtrNHXi9OB3N+wnAUtszmR23M4tKiW
-----END PRIVATE KEY-----
```

The corresponding public key can be used to verify these examples:

```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEhJaBGq4LqqvSYVcYnuzaJr6qi/Eb
bz/m4rVlnIXbwK07HypLbAmBMcCjbazR14vTgdzfsJwFLbM5kdtzOLSolg==
-----END PUBLIC KEY-----
```

Example 1: SUIT Manifest pointing to URI of the Trusted Component Binary

CBOR Diagnostic Notation of SUIT Manifest

```
/ SUIT_Envelope_Tagged / 107( {
  / suit-authentication-wrapper / 2: << [
    << [
      / suit-digest-algorithm-id: / -16 / suit-cose-alg-sha256 /,
      / suit-digest-bytes: / h'DB601ADE73092B58532CA03FBB663DE4953243533
    ] >>,
    << / COSE_Sign1_Tagged / 18( [
      / protected: / << {
        / algorithm-id / 1: -7 / ES256 /
      } >>,
      / unprotected: / {},
      / payload: / null,
      / signature: / h'5B2D535A2B6D5E3C585C1074F414DA9E10BD285C99A33916D
    ] ) >>
  ] >>,
  / suit-manifest / 3: << {
    / suit-manifest-version / 1: 1,
    / suit-manifest-sequence-number / 2: 3,
    / suit-common / 3: << {
      / suit-components / 2: [
        [
          h'544545502D446576696365',           / "TEEP-Device" /
          h'5365637572654653',                 / "SecureFS" /
          h'8D82573A926D4754935332DC29997F74', / tc-uuid /
          h'7461'                              / "ta" /
        ]
      ],
      / suit-common-sequence / 4: << [
        / suit-directive-override-parameters / 20, {
          / suit-parameter-vendor-identifier / 1: h'C0DDD5F15243566087DB
          / suit-parameter-class-identifier / 2: h'DB42F7093D8C55BAA8C52
          / suit-parameter-image-digest / 3: << [
            / suit-digest-algorithm-id: / -16 / suit-cose-alg-sha256 /,
            / suit-digest-bytes: / h'8CF71AC86AF31BE184EC7A05A411A8C3A14
          ] >>,
          / suit-parameter-image-size / 14: 20
        },
        / suit-condition-vendor-identifier / 1, 15,
        / suit-condition-class-identifier / 2, 15
      ] >>
    } >>,
    / suit-install / 9: << [
      / suit-directive-override-parameters / 20, {
        / suit-parameter-uri / 21: "https://example.org/8d82573a-926d-47
      },
      / suit-directive-fetch / 21, 15,
      / suit-condition-image-match / 3, 15
    ] >>
    } >>
} )
```

CBOR Binary Representation

```
D8 6B                                          # tag(107) / SUIT_En
   A2                                          # map(2)
      02                                       # unsigned(2) / suit
      58 73                                    # bytes(115)
         82                                    # array(2)
            58 24                              # bytes(36)
               82                              # array(2)
                  2F                           # negative(15) / -16
                  58 20                        # bytes(32)
                     DB601ADE73092B58532CA03FBB663DE49532435336F1558B49B
            58 4A                              # bytes(74)
               D2                              # tag(18) / COSE_Sig
                  84                           # array(4)
                     43                        # bytes(3)
                        A1                     # map(1)
                           01                  # unsigned(1) / algo
                           26                  # negative(6) / -7 =
                     A0                        # map(0)
                     F6                        # primitive(22) / nu
                     58 40                     # bytes(64)
                        5B2D535A2B6D5E3C585C1074F414DA9E10BD285C99A33916
      03                                       # unsigned(3) / suit
      58 D4                                    # bytes(212)
         A4                                    # map(4)
            01                                 # unsigned(1) / suit
            01                                 # unsigned(1)
            02                                 # unsigned(2) / suit
            03                                 # unsigned(3)
            03                                 # unsigned(3) / suit
            58 84                              # bytes(132)
               A2                              # map(2)
                  02                           # unsigned(2) / suit
                  81                           # array(1)
                     84                        # array(4)
                        4B                     # bytes(11)
                           544545502D446576696365   # "TEEP-Device"
                        48                     # bytes(8)
                           5365637572654653         # "SecureFS"
                        50                     # bytes(16)
                           8D82573A926D4754935332DC29997F74 # tc-uuid
                        42                     # bytes(2)
                           7461                # "ta"
                  04                           # unsigned(4) / suit
                  58 54                        # bytes(84)
                     86                        # array(6)
                        14                     # unsigned(20) / sui
                        A4                     # map(4)
                           01                  # unsigned(1) / suit
                           50                  # bytes(16)
                  C0DDD5F15243566087DB4F5B0AA26C2F
               02                      # unsigned(2) / suit
               50                      # bytes(16)
                  DB42F7093D8C55BAA8C5265FC5820F4E
               03                      # unsigned(3) / suit
               58 24                   # bytes(36)
                  82                   # array(2)
                     2F                # negative(15) / -16
                     58 20             # bytes(32)
                        8CF71AC86AF31BE184EC7A05A411A8C3A14F
               0E                      # unsigned(14) / sui
               14                      # unsigned(20)
            01                         # unsigned(1) / suit
            0F                         # unsigned(15)
            02                         # unsigned(2) / suit
            0F                         # unsigned(15)
09                                     # unsigned(9) / suit
58 45                                  # bytes(69)
   86                                  # array(6)
      14                               # unsigned(20) / sui
      A1                               # map(1)
         15                            # unsigned(21) / sui
         78 3B                         # text(59)
            68747470733A2F2F6578616D706C652E6F72672F38643832
      15                               # unsigned(21) / sui
      0F                               # unsigned(15)
      03                               # unsigned(3) / suit
      0F                               # unsigned(15)
```

CBOR Binary in Hex

```
D86BA2025873825824822F5820DB601ADE73092B58532CA03FBB663DE495
32435336F1558B49BB622726A2FEDD584AD28443A10126A0F658405B2D53
5A2B6D5E3C585C1074F414DA9E10BD285C99A33916DADE3ED38812504817
AC48B62B8E984EC622785BD1C411888BE531B1B594507816B201F6F28579
A40358D4A401010203035884A20281844B544545502D4465766963654853
6563757265465350 8D82573A926D4754935332DC29997F74427461045854
8614A40150C0DDD5F15243566087DB4F5B0AA26C2F0250DB42F7093D8C55
BAA8C5265FC5820F4E035824822F58208CF71AC86AF31BE184EC7A05A411
A8C3A14FD9B77A30D046397481469468ECE80E14010F020F0958458614A1
15783B68747470733A2F2F6578616D706C652E6F72672F38643832353733
612D393236642D343735342D393335332D33326463323939376637342E
7461150F030F
```

Example 2: SUIT Manifest including the Trusted Component Binary

CBOR Diagnostic Notation of SUIT Manifest

```
/ SUIT_Envelope_Tagged / 107( {
  / suit-authentication-wrapper / 2: << [
    << [
      / suit-digest-algorithm-id: / -16 / suit-cose-alg-sha256 /,
      / suit-digest-bytes: / h'14A98BE957DE38FAE37376EA491FD6CAD9BFBD3C9
    ] >>,
    << / COSE_Sign1_Tagged / 18( [
      / protected: / << {
        / algorithm-id / 1: -7 / ES256 /
      } >>,
      / unprotected: / {},
      / payload: / null,
      / signature: / h'4093B323953785981EB607C8BA61B21E5C4F85726A2AF48C1
    ] ) >>
  ] >>,
  / suit-integrated-payload / "#tc": h'48656C6C6F2C2053656375726520576F7
  / suit-manifest / 3: << {
    / suit-manifest-version / 1: 1,
    / suit-manifest-sequence-number / 2: 3,
    / suit-common / 3: << {
      / suit-components / 2: [
        [
          h'544545502D446576696365',           / "TEEP-Device" /
          h'5365637572654653',                 / "SecureFS" /
          h'8D82573A926D4754935332DC29997F74', / tc-uuid /
          h'7461'                              / "ta" /
        ]
      ],
      / suit-common-sequence / 4: << [
        / suit-directive-override-parameters / 20, {
          / suit-parameter-vendor-identifier / 1: h'C0DDD5F15243566087DB
          / suit-parameter-class-identifier / 2: h'DB42F7093D8C55BAA8C52
          / suit-parameter-image-digest / 3: << [
            / suit-digest-algorithm-id: / -16 / suit-cose-alg-sha256 /,
            / suit-digest-bytes: / h'8CF71AC86AF31BE184EC7A05A411A8C3A14
          ] >>,
          / suit-parameter-image-size / 14: 20
        },
        / suit-condition-vendor-identifier / 1, 15,
        / suit-condition-class-identifier / 2, 15
      ] >>
    } >>,
    / suit-install / 9: << [
      / suit-directive-override-parameters / 20, {
        / suit-parameter-uri / 21: "#tc"
      },
      / suit-directive-fetch / 21, 15,
      / suit-condition-image-match / 3, 15
    ] >>
    } >>
  } )
```

CBOR Binary Representation

```
D8 6B                                              # tag(107) / SUIT_En
   A3                                              # map(3)
      02                                           # unsigned(2) / suit
      58 73                                        # bytes(115)
         82                                        # array(2)
            58 24                                  # bytes(36)
               82                                  # array(2)
                  2F                               # negative(15) / -16
                  58 20                            # bytes(32)
                     14A98BE957DE38FAE37376EA491FD6CAD9BFBD3C90051C8F5B0
            58 4A                                  # bytes(74)
               D2                                  # tag(18) / COSE_Sig
                  84                               # array(4)
                     43                            # bytes(3)
                        A1                         # map(1)
                           01                      # unsigned(1) / algo
                           26                      # negative(6) / -7 =
                     A0                            # map(0)
                     F6                            # primitive(22) / nu
                     58 40                         # bytes(64)
                        4093B323953785981EB607C8BA61B21E5C4F85726A2AF48C
      63                                           # text(3) / suit-int
         237463                                    # "#tc"
      54                                           # bytes(20)
         48656C6C6F2C2053656375726520576F726C6421   # "Hello, Secure Wor
      03                                           # unsigned(3) / suit
      58 9A                                        # bytes(154)
         A4                                        # map(4)
            01                                     # unsigned(1) / suit
            01                                     # unsigned(1)
            02                                     # unsigned(2) / suit
            03                                     # unsigned(3)
            03                                     # unsigned(3) / suit
            58 84                                  # bytes(132)
               A2                                  # map(2)
                  02                               # unsigned(2) / suit
                  81                               # array(1)
                     84                            # array(4)
                        4B                         # bytes(11)
                           544545502D446576696365   # "TEEP-Device"
                        48                         # bytes(8)
                           5365637572654653        # "SecureFS"
                        50                         # bytes(16)
                           8D82573A926D4754935332DC29997F74 # tc-uuid
                        42                         # bytes(2)
                           7461                    # "ta"
                  04                               # unsigned(4) / suit
                  58 54                            # bytes(84)
                     86                            # array(6)
            14                         # unsigned(20) / sui
            A4                         # map(4)
               01                      # unsigned(1) / suit
               50                      # bytes(16)
                  C0DDD5F15243566087DB4F5B0AA26C2F
               02                      # unsigned(2) / suit
               50                      # bytes(16)
                  DB42F7093D8C55BAA8C5265FC5820F4E
               03                      # unsigned(3) / suit
               58 24                   # bytes(36)
                  82                   # array(2)
                     2F                # negative(15) / -16
                     58 20             # bytes(32)
                        8CF71AC86AF31BE184EC7A05A411A8C3A14F
               0E                      # unsigned(14) / sui
               14                      # unsigned(20)
            01                         # unsigned(1) / suit
            0F                         # unsigned(15)
            02                         # unsigned(2) / suit
            0F                         # unsigned(15)
09                                     # unsigned(9) / suit
4C                                     # bytes(12)
   86                                  # array(6)
      14                               # unsigned(20) / sui
      A1                               # map(1)
         15                            # unsigned(21) / sui
         63                            # text(3)
            237463                     # "#tc"
      15                               # unsigned(21) / sui
      0F                               # unsigned(15)
      03                               # unsigned(3) / suit
      0F                               # unsigned(15)
```

CBOR Binary in Hex

```
D86BA3025873825824822F582014A98BE957DE38FAE37376EA491FD6CAD9
BFBD3C90051C8F5B017D7A496C3B05584AD28443A10126A0F658404093B3
23953785981EB607C8BA61B21E5C4F85726A2AF48C1CB05BD4401B1B1565
070728FDA38E6496D631E1D23F966CFF7805EDE721D48507D9192993DA87
22632374635448656C6C6F2C2053656375726520576F726C642103589AA4
01010203035884A20281844B544545502D44657669636548536563757265
4653508D82573A926D4754935332DC29997F7442746104585486 14A40150
C0DDD5F15243566087DB4F5B0AA26C2F0250DB42F7093D8C55BAA8C5265F
C5820F4E035824822F58208CF71AC86AF31BE184EC7A05A411A8C3A14FD9
B77A30D046397481469468ECE80E14010F020F094C8614A1156323746315
0F030F
```

Example 3: Supplying Personalization Data for Trusted Component Binary

CBOR Diagnostic Notation of SUIT Manifest

```
/ SUIT_Envelope_Tagged / 107( {
  / suit-authentication-wrapper / 2: << [
    << [
      / suit-digest-algorithm-id: / -16 / suit-cose-alg-sha256 /,
      / suit-digest-bytes: / h'CE596D785169B72712560B3A246AA98F814498EA3
    ] >>,
    << / COSE_Sign1_Tagged / 18( [
      / protected: / << {
        / algorithm-id / 1: -7 / ES256 /
      } >>,
      / unprotected: / {},
      / payload: / null,
      / signature: / h'E9083AA71D2BFCE48253037B9C3116A5EDF23BE0F4B4357A8
    ] ) >>
  ] >>,
  / suit-manifest / 3: << {
    / suit-manifest-version / 1: 1,
    / suit-manifest-sequence-number / 2: 3,
    / suit-common / 3: << {
      / suit-dependencies / 1: [
        {
          / suit-dependency-digest / 1: [
            / suit-digest-algorithm-id: / -16 / suit-cose-alg-sha256 /,
            / suit-digest-bytes: / h'F8690E5A86D010BF2B5348ABB99F2254DB7
          ]
        }
      ],
      / suit-components / 2: [
        [
          h'544545502D446576696365', / "TEEP-Device" /
          h'5365637572654653',       / "SecureFS" /
          h'636F6E6669672E6A736F6E'  / "config.json" /
        ]
      ],
      / suit-common-sequence / 4: << [
        / suit-directive-set-component-index / 12, 0,
        / suit-directive-override-parameters / 20, {
          / suit-parameter-vendor-identifier / 1: h'C0DDD5F15243566087DB
          / suit-parameter-class-identifier / 2: h'DB42F7093D8C55BAA8C52
          / suit-parameter-image-digest / 3: << [
            / suit-digest-algorithm-id: / -16 / suit-cose-alg-sha256 /,
            / suit-digest-bytes: / h'AAABCCCDEEEF00012223444566678889ABB
          ] >>,
          / suit-parameter-image-size / 14: 64
        },
        / suit-condition-vendor-idnetifier / 1, 15,
        / suit-condition-class-identifier / 2, 15
      ] >>
    } >>,
    / suit-dependency-resolution / 7: << [
      / suit-directive-set-dependency-index / 13, 0,
      / suit-directive-override-parameters / 20, {
        / suit-parameter-uri / 21: "https://example.org/8d82573a-926d-47
      },
      / suit-directive-fetch / 21, 2,
      / suit-condition-image-match / 3, 15
    ] >>,
    / suit-install / 9: << [
      / suit-directive-set-dependency-index / 13, 0,
      / suit-directive-process-dependency / 18, 0,
      / suit-directive-set-component-index / 12, 0,
      / suit-directive-override-parameters / 20, {
        / suit-parameter-uri / 21: "https://example.org/config.json"
      },
      / suit-directive-fetch / 21, 2,
      / suit-condition-image-match / 3, 15
    ] >>,
    / suit-validate / 10: << [
      / suit-directive-set-component-index / 12, 0,
      / suit-condition-image-match/ 3, 15
    ] >>
  } >>
} )
```

CBOR Binary Represenation

```
D8 6B                                              # tag(107) / SUIT_En
   A2                                              # map(2)
      02                                           # unsigned(2) / suit
      58 73                                        # bytes(115)
         82                                        # array(2)
            58 24                                  # bytes(36)
               82                                  # array(2)
                  2F                               # negative(15) / -16
                  58 20                            # bytes(32)
                     CE596D785169B72712560B3A246AA98F814498EA3625EEBB72C
            58 4A                                  # bytes(74)
               D2                                  # tag(18) / COSE_Sig
                  84                               # array(4)
                     43                            # bytes(3)
                        A1                         # map(1)
                           01                      # unsigned(1) / algo
                           26                      # negative(6) / -7 =
                     A0                            # map(0)
                     F6                            # primitive(22) / nu
                     58 40                         # bytes(64)
                        E9083AA71D2BFCE48253037B9C3116A5EDF23BE0F4B4357A
      03                                           # unsigned(3) / suit
      59 0134                                      # bytes(308)
         A6                                        # map(6)
            01                                     # unsigned(1) / suit
            01                                     # unsigned(1)
            02                                     # unsigned(2) / suit
            03                                     # unsigned(3)
            03                                     # unsigned(3) / suit
            58 A7                                  # bytes(167)
               A3                                  # map(3)
                  01                               # unsigned(1) / suit
                  81                               # array(1)
                     A1                            # map(1)
                        01                         # unsigned(1) suit-d
                        82                         # array(2)
                           2F                      # negative(15) / -16
                           58 20                   # bytes(32)
                              F8690E5A86D010BF2B5348ABB99F2254DB7B608D0D
                  02                               # unsigned(2) / suit
                  81                               # array(1)
                     83                            # array(3)
                        4B                         # bytes(11)
                           544545502D446576696365   # "TEEP-Device"
                        48                         # bytes(8)
                           5365637572654653         # "SecureFS"
                        4B                         # bytes(11)
                           636F6E6669672E6A736F6E   # "config.json"
                  04                               # unsigned(4) / suit
```

```
          58 57                                  # bytes(87)
             88                                  # array(8)
                0C                               # unsigned(12) / sui
                00                               # unsigned(0)
                14                               # unsigned(20) / sui
                A4                               # map(4)
                   01                            # unsigned(1) / suit
                   50                            # bytes(16)
                      C0DDD5F15243566087DB4F5B0AA26C2F
                   02                            # unsigned(2) / suit
                   50                            # bytes(16)
                      DB42F7093D8C55BAA8C5265FC5820F4E
                   03                            # unsigned(3) / suit
                   58 24                         # bytes(36)
                      82                         # array(2)
                         2F                      # negative(15) / -16
                         58 20                   # bytes(32)
                            AAABCCCDEEEF00012223444566678889ABBB
                   0E                            # unsigned(14) / sui
                   18 40                         # unsigned(64)
                01                               # unsigned(1) / suit
                0F                               # unsigned(15)
                02                               # unsigned(2) / suit
                0F                               # unsigned(15)
    07                                           # unsigned(7) / suit
    58 49                                        # bytes(73)
       88                                        # array(8)
          0D                                     # unsigned(13) / sui
          00                                     # unsigned(0)
          14                                     # unsigned(20) / sui
          A1                                     # map(1)
             15                                  # unsigned(21) / sui
             78 3D                               # text(61)
                68747470733A2F2F6578616D706C652E6F72672F38643832
          15                                     # unsigned(21) / sui
          02                                     # unsigned(2)
          03                                     # unsigned(3) / suit
          0F                                     # unsigned(15)
    09                                           # unsigned(9) / suit
    58 2F                                        # bytes(47)
       8C                                        # array(12)
          0D                                     # unsigned(13) / sui
          00                                     # unsigned(0)
          12                                     # unsigned(18) / sui
          00                                     # unsigned(0)
          0C                                     # unsigned(12) / sui
          00                                     # unsigned(0)
          14                                     # unsigned(20) / sui
          A1                                     # map(1)
```

```
              15                             # unsigned(21) / sui
              78 1F                          # text(31)
                 68747470733A2F2F6578616D706C652E6F72672F636F6E66
           15                                # unsigned(21) / sui
           02                                # unsigned(2)
           03                                # unsigned(3) / suit
           0F                                # unsigned(15)
     0A                                      # unsigned(10) / sui
     45                                      # bytes(5)
        84                                   # array(4)
           0C                                # unsigned(12) / sui
           00
           03                                # unsigned(3) / suit
           0F                                # unsigned(15)
```

CBOR Binary in Hex

```
D86BA2025873825824822F5820CE596D785169B72712560B3A246AA98F81
4498EA3625EEBB72CED9AF273E7FFD584AD28443A10126A0F65840E9083A
A71D2BFCE48253037B9C3116A5EDF23BE0F4B4357A8A835F724660DA7482
C64345B4C73DE95F05513BD09FC2E58BD2CC865CC851AD797513A9A951A3
CA03590134A6010102030358A7A30181A101822F5820DB601ADE73092B58
532CA03FBB663DE49532435336F1558B49BB622726A2FEDD0281834B5445
45502D4465766963654853656375726546534B636F6E6669672E6A736F6E
045857880C0014A40150C0DDD5F15243566087DB4F5B0AA26C2F0250DB42
F7093D8C55BAA8C5265FC5820F4E035824822F5820AAABCCCDEEEF000122
23444566678889ABBBCDDDEFFF011123334555677789990E1840010F020F
075849880D0014A115783D68747470733A2F2F6578616D706C652E6F7267
2F3864383235373361 2D393236642D343735342D393335332D3332646332
39393937663734 2E737569741502030F09582F8C0D0012000C0014A11578
1F68747470733A2F2F6578616D706C652E6F72672F636F6E6669672E6A73
6F6E1502030F0A45840C00030F
```

E.4. Example 4: Unlink a Trusted Component

CBOR Diagnostic Notation of SUIT Manifest

```
/ SUIT_Envelope_Tagged / 107( {
  / suit-authentication-wrapper / 2: << [
    << [
      / suit-digest-algorithm-id: / -16 / suit-cose-alg-sha256 /,
      / suit-digest-bytes: / h'632454F19A9440A5B83493628A7EF8704C8A0205A
    ] >>,
    << / COSE_Sign1_Tagged / 18( [
      / protected / << {
        / algorithm-id / 1: -7 / ES256 /
      } >>,
      / unprotected: / {},
      / payload: / null,
      / signature: / h'A32CDB7C1D089C27408CED3C79087220EB0D77F105BB53309
    ] ) >>
  ] >>,
  / suit-manifest / 3: << {
    / suit-manifest-version / 1: 1,
    / suit-manifest-sequence-number / 2: 18446744073709551615 / UINT64_M
    / suit-common / 3: << {
      / suit-components / 2: [
        [
          h'544545502D446576696365',           / "TEEP-Device" /
          h'5365637572654653',                 / "SecureFS" /
          h'8D82573A926D4754935332DC29997F74', / tc-uuid /
          h'7461'                              / "ta" /
        ]
      ],
      / suit-common-sequence / 4: << [
        / suit-directive-override-parameters / 20, {
          / suit-parameter-vendor-identifier / 1: h'C0DDD5F15243566087DB
          / suit-parameter-class-identifier / 2: h'DB42F7093D8C55BAA8C52
        },
        / suit-condition-vendor-identifier / 1, 15,
        / suit-condition-class-identifier / 2, 15
      ] >>
    } >>,
    / suit-install / 9: << [
      / suit-directive-set-component-index: / 12, 0,
      / suit-directive-unlink: / 33, 0
    ] >>
  } >>
} )
```

CBOR Binary Representation

```
D8 6B                                              # tag(107) / SUIT_En
   A2                                              # map(2)
      02                                           # unsigned(2) / suit
      58 73                                        # bytes(115)
         82                                        # array(2)
            58 24                                  # bytes(36)
               82                                  # array(2)
                  2F                               # negative(15) / -16
                  58 20                            # bytes(32)
                     632454F19A9440A5B83493628A7EF8704C8A0205A62C34E425B
            58 4A                                  # bytes(74)
               D2                                  # tag(18) / COSE_Sig
                  84                               # array(4)
                     43                            # bytes(3)
                        A1                         # map(1)
                           01                      # unsigned(1) / algo
                           26                      # negative(6) / -7 =
                     A0                            # map(0)
                     F6                            # primitive(22) / nu
                     58 40                         # bytes(64)
                        A32CDB7C1D089C27408CED3C79087220EB0D77F105BB5330
      03                                           # unsigned(3) / suit
      58 73                                        # bytes(115)
         A4                                        # map(4)
            01                                     # unsigned(1) / suit
            01                                     # unsigned(1)
            02                                     # unsigned(2) / suit
            1B FFFFFFFFFFFFFFFF                    # unsigned(184467440
            03                                     # unsigned(3) / suit
            58 5B                                  # bytes(91)
               A2                                  # map(2)
                  02                               # unsigned(2) / suit
                  81                               # array(1)
                     84                            # array(4)
                        4B                         # bytes(11)
                           544545502D446576696365   # "TEEP-Device"
                        48                         # bytes(8)
                           5365637572654653         # "SecureFS"
                        50                         # bytes(16)
                           8D82573A926D4754935332DC29997F74 # tc-uuid
                        42                         # bytes(2)
                           7461                    # "ta"
                  04                               # unsigned(4) / suit
                  58 2B                            # bytes(84)
                     86                            # array(6)
                        14                         # unsigned(20) / sui
                        A2                         # map(2)
                           01                      # unsigned(1) / suit
                           50                      # bytes(16)
                  C0DDD5F15243566087DB4F5B0AA26C2F
               02                      # unsigned(2) / suit
               50                      # bytes(16)
                  DB42F7093D8C55BAA8C5265FC5820F4E
            01                         # unsigned(1) / suit
            0F                         # unsigned(15)
            02                         # unsigned(2) / suit
            0F                         # unsigned(15)
09                                     # unsigned(9) / suit
46                                     # bytes(6)
   84                                  # array(4)
      0C                               # unsigned(12) / sui
      00                               # unsigned(0)
      18 21                            # unsigned(33) / sui
      00                               # unsigned(0)
```

CBOR Binary in Hex

```
D86BA2025873825824822F5820632454F19A9440A5B83493628A7EF8704C
8A0205A62C34E425BAA34C71341F42584AD28443A10126A0F65840A32CDB
7C1D089C27408CED3C79087220EB0D77F105BB5330912875F4D94AD108D7
658C650463AEB7E1CCA5084F22B2F3993176E8B3529A3202ED735E4D39BB
BF035873A40101021BFFFFFFFFFFFFFFFF03585BA20281844B544545502D
4465766963654853656375726974655508D82573A926D4754935332DC2999
7F7442746104582B8614A20150C0DDD5F15243566087DB4F5B0AA26C2F02
50DB42F7093D8C55BAA8C5265FC5820F4E010F020F0946840C00182100
```

F. Examples of SUIT Reports

This section shows some examples of SUIT reports.

F.1. Example 1: Success

SUIT Reports have no records if no conditions have failed. The URI in this example is the reference URI provided in the SUIT manifest.

```
{
  / suit-report-manifest-digest / 1:<<[
    / algorithm-id / -16 / "sha256" /,
    / digest-bytes / h'a7fd6593eac32eb4be578278e6540c5c'
                     h'09cfd7d4d234973054833b2b93030609'
  ]>>,
  / suit-report-manifest-uri / 2: "tam.teep.example/personalisation.suit
  / suit-report-records / 4: []
}
```

F.2. Example 2: Faiure

```
{
  / suit-report-manifest-digest / 1:<<[
    / algorithm-id / -16 / "sha256" /,
    / digest-bytes / h'a7fd6593eac32eb4be578278e6540c5c09cfd7d4d23497305
  ]>>,
  / suit-report-manifest-uri / 2: "tam.teep.example/personalisation.suit
  / suit-report-records / 4: [
    {
      / suit-record-manifest-id / 1:[],
      / suit-record-manifest-section / 2: 7 / dependency-resolution /,
      / suit-record-section-offset / 3: 66,
      / suit-record-dependency-index / 5: 0,
      / suit-record-failure-reason / 6: 404
    }
  ]
}
```

where the dependency-resolution refers to:

```
107({
  authentication-wrapper,
  / manifest / 3:<<{
    / manifest-version / 1:1,
    / manifest-sequence-number / 2:3,
    common,
    dependency-resolution,
    install,
    validate,
    run,
    text
  }>>,
})
```

and the suit-record-section-offset refers to:

```
<<[
  / directive-set-dependency-index / 13,0 ,
  / directive-set-parameters / 19,{
    / uri / 21:'tam.teep.example/'
               'edd94cd8-9d9c-4cc8-9216-b3ad5a2d5b8a.suit',
    } ,
  / directive-fetch / 21,2 ,
  / condition-image-match / 3,15
]>>,
```

Authors' Addresses

Hannes Tschofenig
Arm Ltd.
6067 Absam
Austria

Email: hannes.tschofenig@arm.com

Mingliang Pei
Broadcom
350 Ellis St
Mountain View, CA 94043
United States of America

Email: mingliang.pei@broadcom.com

David Wheeler
Amazon
United States of America

Email: davewhee@amazon.com

Dave Thaler

Microsoft
United States of America

Email: dthaler@microsoft.com

Akira Tsukamoto
AIST
Japan

Email: akira.tsukamoto@aist.go.jp