

Workgroup: RATS

Internet-Draft: draft-ietf-rats-eat-27

Published: 26 May 2024

Intended Status: Standards Track

Expires: 27 November 2024

Authors: L. Lundblade

G. Mandyam

Security Theory LLC Mediatek USA

J. O'Donoghue

C. Wallace

Qualcomm Technologies Inc. Red Hound Software, Inc.

## **The Entity Attestation Token (EAT)**

### **Abstract**

An Entity Attestation Token (EAT) provides an attested claims set that describes state and characteristics of an entity, a device like a smartphone, IoT device, network equipment or such. This claims set is used by a relying party, server or service to determine the type and degree of trust placed in the entity.

An EAT is either a CBOR Web Token (CWT) or JSON Web Token (JWT) with attestation-oriented claims.

### **Status of This Memo**

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 27 November 2024.

### **Copyright Notice**

Copyright (c) 2024 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

- [1. Introduction](#)
  - [1.1. Entity Overview](#)
  - [1.2. EAT as a Framework](#)
  - [1.3. Operating Model and RATS Architecture](#)
    - [1.3.1. Relationship between Evidence and Attestation Results](#)
- [2. Terminology](#)
- [3. Top-Level Token Definition](#)
- [4. The Claims](#)
  - [4.1. eat\\_nonce \(EAT Nonce\) Claim](#)
  - [4.2. Claims Describing the Entity](#)
    - [4.2.1. ueid \(Universal Entity ID\) Claim](#)
      - [4.2.1.1. Rules for Creating UEIDs](#)
      - [4.2.1.2. Rules for Consuming UEIDs](#)
    - [4.2.2. sueids \(Semi-permanent UEIDs\) Claim \(SUEIDs\)](#)
    - [4.2.3. oemid \(Hardware OEM Identification\) Claim](#)
      - [4.2.3.1. Random Number Based OEM ID](#)
      - [4.2.3.2. IEEE Based OEM ID](#)
      - [4.2.3.3. IANA Private Enterprise Number Based OEM ID](#)
    - [4.2.4. hwmodel \(Hardware Model\) Claim](#)
    - [4.2.5. hwversion \(Hardware Version\) Claim](#)
    - [4.2.6. swname \(Software Name\) Claim](#)
    - [4.2.7. swversion \(Software Version\) Claim](#)
    - [4.2.8. oemboot \(OEM Authorized Boot\) Claim](#)
    - [4.2.9. dbgstat \(Debug Status\) Claim](#)
      - [4.2.9.1. Enabled](#)
      - [4.2.9.2. Disabled](#)
      - [4.2.9.3. Disabled Since Boot](#)
      - [4.2.9.4. Disabled Permanently](#)
      - [4.2.9.5. Disabled Fully and Permanently](#)
    - [4.2.10. location \(Location\) Claim](#)
    - [4.2.11. uptime \(Uptime\) Claim](#)
    - [4.2.12. bootcount \(Boot Count\) Claim](#)
    - [4.2.13. bootseed \(Boot Seed\) Claim](#)
    - [4.2.14. dloas \(Digital Letters of Approval\) Claim](#)
    - [4.2.15. manifests \(Software Manifests\) Claim](#)
    - [4.2.16. measurements \(Measurements\) Claim](#)
    - [4.2.17. measres \(Software Measurement Results\) Claim](#)
    - [4.2.18. submods \(Submodules\)](#)
      - [4.2.18.1. Submodule Claims-Set](#)
      - [4.2.18.2. Detached Submodule Digest](#)
      - [4.2.18.3. Nested Tokens](#)

- 4.3. [Claims Describing the Token](#)
  - 4.3.1. [iat \(Timestamp\) Claim](#)
  - 4.3.2. [eat\\_profile \(EAT Profile\) Claim](#)
  - 4.3.3. [intuse \(Intended Use\) Claim](#)
- 5. [Detached EAT Bundles](#)
- 6. [Profiles](#)
  - 6.1. [Format of a Profile Document](#)
  - 6.2. [Full and Partial Profiles](#)
  - 6.3. [List of Profile Issues](#)
    - 6.3.1. [Use of JSON, CBOR or both](#)
    - 6.3.2. [CBOR Map and Array Encoding](#)
    - 6.3.3. [CBOR String Encoding](#)
    - 6.3.4. [CBOR Preferred Serialization](#)
    - 6.3.5. [CBOR Tags](#)
    - 6.3.6. [COSE/JOSE Protection](#)
    - 6.3.7. [COSE/JOSE Algorithms](#)
    - 6.3.8. [Detached EAT Bundle Support](#)
    - 6.3.9. [Key Identification](#)
    - 6.3.10. [Endorsement Identification](#)
    - 6.3.11. [Freshness](#)
    - 6.3.12. [Claims Requirements](#)
  - 6.4. [The Constrained Device Standard Profile](#)
- 7. [Encoding and Collected CDDL](#)
  - 7.1. [Claims-Set and CDDL for CWT and JWT](#)
  - 7.2. [Encoding Data Types](#)
    - 7.2.1. [Common Data Types](#)
    - 7.2.2. [JSON Interoperability](#)
    - 7.2.3. [Labels](#)
    - 7.2.4. [CBOR Interoperability](#)
  - 7.3. [Collected CDDL](#)
    - 7.3.1. [Payload CDDL](#)
    - 7.3.2. [CBOR-Specific CDDL](#)
    - 7.3.3. [JSON-Specific CDDL](#)
- 8. [Privacy Considerations](#)
  - 8.1. [UEID and SUEID Privacy Considerations](#)
  - 8.2. [Location Privacy Considerations](#)
  - 8.3. [Boot Seed Privacy Considerations](#)
  - 8.4. [Replay Protection and Privacy](#)
- 9. [Security Considerations](#)
  - 9.1. [Claim Trustworthiness](#)
  - 9.2. [Key Provisioning](#)
    - 9.2.1. [Transmission of Key Material](#)
  - 9.3. [Freshness](#)
  - 9.4. [Multiple EAT Consumers](#)
  - 9.5. [Detached EAT Bundle Digest Security Considerations](#)
  - 9.6. [Verification Keys](#)
- 10. [IANA Considerations](#)
  - 10.1. [Reuse of CBOR and JSON Web Token \(CWT and JWT\) Claims Registries](#)

- [10.2. CWT and JWT Claims Registered by This Document](#)
- [10.3. UEID URN Registered by this Document](#)
- [10.4. CBOR Tag for Detached EAT Bundle Registered by this Document](#)
- [11. References](#)
  - [11.1. Normative References](#)
  - [11.2. Informative References](#)
- [Appendix A. Examples](#)
  - [A.1. Claims Set Examples](#)
    - [A.1.1. Simple TEE Attestation](#)
    - [A.1.2. Submodules for Board and Device](#)
    - [A.1.3. EAT Produced by Attestation Hardware Block](#)
    - [A.1.4. Key / Key Store Attestation](#)
    - [A.1.5. Software Measurements of an IoT Device](#)
    - [A.1.6. Attestation Results in JSON](#)
    - [A.1.7. JSON-encoded Token with Submodules](#)
  - [A.2. Signed Token Examples](#)
    - [A.2.1. Basic CWT Example](#)
    - [A.2.2. CBOR-encoded Detached EAT Bundle](#)
    - [A.2.3. JSON-encoded Detached EAT Bundle](#)
- [Appendix B. UEID Design Rationale](#)
  - [B.1. Collision Probability](#)
  - [B.2. No Use of UUID](#)
- [Appendix C. EAT Relation to IEEE.802.1AR Secure Device Identity \(DevID\)](#)
  - [C.1. DevID Used With EAT](#)
  - [C.2. How EAT Provides an Equivalent Secure Device Identity](#)
  - [C.3. An X.509 Format EAT](#)
  - [C.4. Device Identifier Permanence](#)
- [Appendix D. CDDL for CWT and JWT](#)
- [Appendix E. New Claim Design Considerations](#)
  - [E.1. Interoperability and Relying Party Orientation](#)
  - [E.2. Operating System and Technology Neutral](#)
  - [E.3. Security Level Neutral](#)
  - [E.4. Reuse of Extant Data Formats](#)
  - [E.5. Proprietary Claims](#)
- [Appendix F. Endorsements and Verification Keys](#)
  - [F.1. Identification Methods](#)
    - [F.1.1. COSE/JWS Key ID](#)
    - [F.1.2. JWS and COSE X.509 Header Parameters](#)
    - [F.1.3. CBOR Certificate COSE Header Parameters](#)
    - [F.1.4. Claim-Based Key Identification](#)
- [Appendix G. Changes from Previous Drafts](#)
  - [G.1. From draft-ietf-rats-eat-24](#)
- [Contributors](#)
- [Authors' Addresses](#)

## 1. Introduction

An Entity Attestation Token (EAT) is a message made up of claims about an entity. An entity may be a device, some hardware or some software. The claims are ultimately used by a relying party who decides if and how it will interact with the entity. The relying party may choose to trust, not trust or partially trust the entity. For example, partial trust may be allowing a monetary transaction only up to a limit.

The security model and goal for attestation are unique and are not the same as for other security standards like those for server authentication, user authentication and secured messaging. To give an example of one aspect of the difference, consider the association and life-cycle of key material. For authentication, keys are associated with a user or service and set up by actions performed by a user or an operator of a service. For attestation, the keys are associated with specific devices and are configured by device manufacturers. The reader is assumed to be familiar with the goals and security model for attestation as described in RATS Architecture [[RFC9334](#)] and are not repeated here.

This document defines some common claims that are potentially of broad use. EAT additionally allows proprietary claims and for further claims to be standardized. Here are some examples:

- \*Make and model of manufactured consumer device
- \*Make and model of a chip or processor, particularly for a security-oriented chip
- \*Identification and measurement of the software running on a device
- \*Configuration and state of a device
- \*Environmental characteristics of a device like its Global Positioning System (GPS) location
- \*Formal certifications received

EAT is constructed to support a wide range of use cases.

No single set of claims can accommodate all use cases so EAT is constructed as a framework for defining specific attestation tokens for specific use cases. In particular, EAT provides a profile mechanism to be able to clearly specify the claims needed, the cryptographic algorithms that should be used, and other characteristics for a particular token and use case. [Section 6](#) describes profile contents and provides a profile that is suitable for constrained device use cases.

The entity's EAT implementation generates the claims and typically signs them with an attestation key. It is responsible for protecting the attestation key. Some EAT implementations will use components with very high resistance to attack like Trusted Platform Modules or Secure Elements. Others may rely solely on simple software defenses.

Nesting of tokens and claims sets is accommodated for composite devices that have multiple subsystems.

An EAT may be encoded in either JavaScript Object Notation (JSON) [[RFC8259](#)] or Concise Binary Object Representation (CBOR) [[RFC8949](#)] as needed for each use case. EAT is built on CBOR Web Token (CWT) [[RFC8392](#)] and JSON Web Token (JWT) [[RFC7519](#)] and inherits all their characteristics and their security mechanisms. Like CWT and JWT, EAT does not imply any message flow.

Following is a very simple example. It is JSON format for easy reading, but could also be CBOR. Only the Claims-Set, the payload for the JWT, is shown.

```
{
  "eat_nonce": "MIDBNH28iioisjPy",
  "ueid":      "AgAEizrK3Q",
  "oemid":     76543,
  "swname":   "Acme IoT OS",
  "swversion": "3.1.4"
}
```

This example has a nonce for freshness. This nonce is the base64url encoding of a 12 byte random binary byte string. The ueid is effectively a serial number uniquely identifying the device. This ueid is the base64url encoding of a 48-bit MAC address preceded by the type byte 0x02. The oemid identifies the manufacturer using a Private Enterprise Number [[PEN](#)]. The software is identified by a simple string name and version. It could be identified by a full manifest, but this is a minimal example.

## 1.1. Entity Overview

This document uses the term "entity" to refer to the target of an EAT. Most of the claims defined in this document are claims about an entity. An entity is equivalent to a target environment in an attester as defined in [[RFC9334](#)].

Layered attestation and composite devices, as described in [[RFC9334](#)], are supported by a submodule mechanism (see [Section 4.2.18](#)). Submodules allow nesting of EATs and of claims-sets so that such hierarchies can be modeled.

An entity is the same as a "system component", as defined in the Internet Security Glossary [[RFC4949](#)].

Note that [[RFC4949](#)] defines "entity" and "system entity" as synonyms, and that they may be a person or organization in addition to being a system component. In the EAT context, "entity" never refers to a person or organization. The hardware and software that implement a web site server or service may be an entity in the EAT sense, but the organization that operates, maintains or hosts the web site is not an entity.

Some examples of entities:

- \*A Secure Element
- \*A Trusted Execution Environment (TEE)
- \*A network card in a router
- \*A router, perhaps with each network card in the router a submodule
- \*An Internet of Things (IoT) device
- \*An individual process
- \*An app on a smartphone
- \*A smartphone with many submodules for its many subsystems
- \*A subsystem in a smartphone like the modem or the camera

An entity may have strong security defenses against hardware invasive attacks. It may also have low security, having no special security defenses. There is no minimum security requirement to be an entity.

## 1.2. EAT as a Framework

EAT is a framework for defining attestation tokens for specific use cases, not a specific token definition. While EAT is based on and compatible with CWT and JWT, it can also be described as:

- \*An identification and type system for claims in claims-sets
- \*Definitions of common attestation-oriented claims
- \*Claims defined in CDDL and serialized using CBOR or JSON
- \*Security envelopes based on CBOR Object Signing and Encryption (COSE) and Javascript Object Signing and Encryption (JOSE)

\*Nesting of claims sets and tokens to represent complex and compound devices

\*A profile mechanism for specifying and identifying specific tokens for specific use cases

EAT uses the name/value pairs the same as CWT and JWT to identify individual claims. [Section 4](#) defines common attestation-oriented claims that are added to the CWT and JWT IANA registries. As with CWT and JWT, no claims are mandatory and claims not recognized should be ignored.

Unlike, but compatible with CWT and JWT, EAT defines claims using Concise Data Definition Language (CDDL) [[RFC8610](#)]. In most cases the same CDDL definition is used for both the CBOR/CWT serialization and the JSON/JWT serialization.

Like CWT and JWT, EAT uses COSE and JOSE to provide authenticity, integrity and optionally confidentiality. EAT places no new restrictions on cryptographic algorithms, retaining all the cryptographic flexibility of CWT, COSE, JWT and JOSE.

EAT defines a means for nesting tokens and claims sets to accommodate composite devices that have multiple subsystems and multiple attesters. Tokens with security envelopes or bare claims sets may be embedded in an enclosing token. The nested token and the enclosing token do not have to use the same encoding (e.g., a CWT may be enclosed in a JWT).

EAT adds the ability to detach claims sets and send them separately from a security-enveloped EAT that contains a digest of the detached claims set.

This document registers no media or content types for the identification of the type of EAT, its serialization encoding or security envelope. The definition and registration of EAT media types is addressed in [[EAT.media-types](#)].

Finally, the notion of an EAT profile is introduced that facilitates the creation of narrowed definitions of EATs for specific use cases in follow-on documents. One basic profile for constrained devices is normatively defined.

### **1.3. Operating Model and RATS Architecture**

EAT follows the operational model described in Figure 1 in RATS Architecture [[RFC9334](#)]. To summarize, an attester generates evidence in the form of a claims set describing various characteristics of an entity. Evidence is usually signed by a key that proves the attester



and the evidence it produces are authentic. The claims set includes a nonce or some other means to assure freshness.

A verifier confirms an EAT is valid by verifying the signature and may vet some claims using reference values. The verifier then produces attestation results, which may also be represented as an EAT. The attestation results are provided to the relying party, which is the ultimate consumer of the Remote Attestation Procedure. The relying party uses the attestation results as needed for its use case, perhaps allowing an entity to access a network, allowing a financial transaction or such. In some cases, the verifier and relying party are not distinct entities.

### **1.3.1. Relationship between Evidence and Attestation Results**

Any claim defined in this document or in the IANA CWT or JWT registry may be used in evidence or attestation results. The relationship of claims in attestation results to evidence is fundamentally governed by the verifier and the verifier's policy.

A common use case is for the verifier and its policy to perform checks, calculations and processing with evidence as the input to produce a summary result in attestation results that indicates the overall health and status of the entity. For example, measurements in evidence may be compared to reference values the results of which are represented as a simple pass/fail in attestation results.

It is also possible that some claims in the Evidence will be forwarded unmodified to the relying party in attestation results. This forwarding is subject to the verifier's implementation and policy. The relying party should be aware of the verifier's policy to know what checks it has performed on claims it forwards.

The verifier may modify claims it forwards, for example, to implement a privacy preservation functionality. It is also possible the verifier will put claims in the attestation results that give details about the entity that it has computed or looked up in a database. For example, the verifier may be able to put an "oemid" claim in the attestation results by performing a look up based on a "ueid" claim (e.g., serial number) it received in evidence.

This specification does not establish any normative rules for the verifier to follow, as these are a matter of local policy. It is up to each relying party to understand the processing rules of each verifier to know how to interpret claims in attestation results.

## **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.

In this document, the structure of data is specified in CDDL [[RFC8610](#)] [[RFC9165](#)].

The examples in [Appendix A](#) use CBOR diagnostic notation defined in [Section 8](#) of [[RFC8949](#)] and [Appendix G](#) of [[RFC8610](#)].

This document reuses terminology from JWT [[RFC7519](#)] and CWT [[RFC8392](#)]:

**base64url-encoded:** base64url-encoded is as described in [[RFC7515](#)], i.e., using URL- and filename-safe character set [[RFC4648](#)] with all trailing '=' characters omitted and without the inclusion of any line breaks, whitespace, or other additional characters.

**Claim:** A piece of information asserted about a subject. A claim is represented as a value and either a name or key to identify it.

**Claim Name:** A unique text string that identifies the claim. It is used as the claim name for JSON encoding.

**Claim Key:** The CBOR map key used to identify a claim. (The term "Claim Key" comes from CWT. This document, like COSE, uses the term "label" to refer to CBOR map keys to avoid confusion with cryptographic keys.)

**Claim Value:** The value portion of the claim. A claim value can be any CBOR data item or JSON value.

**Claims Set:** The CBOR map or JSON object that contains the claims conveyed by the CWT or JWT.

This document reuses terminology from RATS Architecture [[RFC9334](#)]:

**Attester:** A role performed by an entity (typically a device) whose evidence must be appraised in order to infer the extent to which the attester is considered trustworthy, such as when deciding whether it is authorized to perform some operation.

**Verifier:** A role that appraises the validity of evidence about an attester and produces attestation results to be used by a relying party.

**Relying Party:** A role that depends on the validity of information about an attester, for purposes of reliably applying application specific actions. Compare /relying party/ in [[RFC4949](#)].

**Evidence:**

A set of claims generated by an attester to be appraised by a verifier. Evidence may include configuration data, measurements, telemetry, or inferences.

**Attestation Results:** The output generated by a verifier, typically including information about an attester, where the verifier vouches for the validity of the results

**Reference Values:** A set of values against which values of claims can be compared as part of applying an appraisal policy for evidence. Reference Values are sometimes referred to in other documents as known-good values, golden measurements, or nominal values, although those terms typically assume comparison for equality, whereas here reference values might be more general and be used in any sort of comparison.

**Endorsement:** A secure statement that an Endorser vouches for the integrity of an attester's various capabilities such as claims collection and evidence signing.

This document reuses terminology from CDDL [[RFC8610](#)]:

**Group Socket:** refers to the mechanism by which a CDDL definition is extended, as described in [[RFC8610](#)] and [[RFC9165](#)]

### 3. Top-Level Token Definition

An "EAT" is an encoded (serialized) message the purpose of which is to transfer a Claims-Set between two parties. An EAT **MUST** always contain a Claims-Set. In this document an EAT is always a CWT or JWT.

An EAT **MUST** have authenticity and integrity protection. CWT and JWT provide that in this document.

Further documents may define other encodings and security mechanisms for EAT.

The identification of a protocol element as an EAT follows the general conventions used for CWTs and JWTs. Identification depends on the protocol carrying the EAT. In some cases it may be by media type (e.g., in a HTTP Content-Type field). In other cases it may be through use of CBOR tags. There is no fixed mechanism across all use cases.

This document also defines another message, the detached EAT bundle (see [Section 5](#)), which holds a collection of detached claims sets and an EAT that provides integrity and authenticity protection for them. Detached EAT bundles can be either CBOR or JSON encoded.

The following CDDL defines the top-level \$EAT-CBOR-Tagged-Token, \$EAT-CBOR-Untagged-Token and \$EAT-JSON-Token-Formats sockets (see [Section 3.9](#) of [[RFC8610](#)]), enabling future token formats to be defined. Any new format that plugs into one or more of these sockets **MUST** be defined by an IETF standards action. Of particular use may be a token type that provides no direct authenticity or integrity protection for use with transports mechanisms that do provide the necessary security services [[UCCS](#)].

Nesting of EATs is allowed and defined in [Section 4.2.18.3](#). This includes the nesting of an EAT that is a different format than the enclosing EAT, i.e., the nested EAT may be encoded using CBOR and the enclosing EAT encoded using JSON or vice versa. The definition of Nested-Token references the CDDL defined in this section. When new token formats are defined, the means for identification in a nested token **MUST** also be defined.

The top-level CDDL type for CBOR-encoded EATs is EAT-CBOR-Token and for JSON is EAT-JSON-Token (while CDDL and CDDL tools provide enough support for shared definitions of most items in this document, they don't provide enough support for this sharing at the top level).

EAT-CBOR-Token = \$EAT-CBOR-Tagged-Token / \$EAT-CBOR-Untagged-Token

\$EAT-CBOR-Tagged-Token /= CWT-Tagged-Message

\$EAT-CBOR-Tagged-Token /= BUNDLE-Tagged-Message

\$EAT-CBOR-Untagged-Token /= CWT-Untagged-Message

\$EAT-CBOR-Untagged-Token /= BUNDLE-Untagged-Message

EAT-JSON-Token = \$EAT-JSON-Token-Formats

\$EAT-JSON-Token-Formats /= JWT-Message

\$EAT-JSON-Token-Formats /= BUNDLE-Untagged-Message

#### 4. The Claims

This section describes new claims defined for attestation that are to be added to the CWT [[IANA.CWT.Claims](#)] and JWT [[IANA.JWT.Claims](#)] IANA registries.

All definitions, requirements, creation and validation procedures, security considerations, IANA registrations and so on from CWT and JWT carry over to EAT.

This section also describes how several extant CWT and JWT claims apply in EAT.

The set of claims that an EAT must contain to be considered valid is context dependent and is outside the scope of this specification.

Specific applications of EATs will require implementations to understand and process some claims in particular ways. However, in the absence of such requirements, all claims that are not understood by implementations **MUST** be ignored.

CDDL, along with a text description, is used to define each claim independent of encoding. Each claim is defined as a CDDL group. In [Section 7](#) on encoding, the CDDL groups turn into CBOR map entries and JSON name/value pairs.

Each claim defined in this document is added to the \$\$Claims-Set-Claims group socket. Claims defined by other specifications **MUST** also be added to the \$\$Claims-Set-Claims group socket.

All claims in an EAT **MUST** use the same encoding except where otherwise explicitly stated (e.g., in a CBOR-encoded token, all claims must be CBOR-encoded).

This specification includes a CDDL definition of most of what is defined in [[RFC8392](#)]. Similarly, this specification includes CDDL for most of what is defined in [[RFC7519](#)]. These definitions are in [Appendix D](#) and are not normative.

Each claim described has a unique text string and integer that identifies it. CBOR-encoded tokens **MUST** use only the integer for claim keys. JSON-encoded tokens **MUST** use only the text string for claim names.

#### 4.1. `eat_nonce` (EAT Nonce) Claim

An EAT nonce is either a byte or text string or an array of byte or text strings. The array option supports multistage EAT verification and consumption.

A claim named "nonce" was defined and registered with IANA for JWT, but **MUST NOT** be used because it does not support multiple nonces. No previous "nonce" claim was defined for CWT. To distinguish from the previously defined JWT "nonce" claim, this claim is named "eat\_nonce" in JSON-encoded EATs. The CWT nonce defined here is intended for general purpose use and retains the "Nonce" claim name instead of an EAT-specific name.

An EAT nonce **MUST** have at least 64 bits of entropy. A maximum EAT nonce size is set to limit the memory required for an implementation. All receivers **MUST** be able to accommodate the maximum size.

In CBOR, an EAT nonce is a byte string between 8 and 64 bytes in length. In JSON, an EAT nonce is a text string between 8 and 88 bytes in length.

```
$$Claims-Set-Claims //=  
  (nonce-label => nonce-type / [ 2* nonce-type ] )  
  
nonce-type = JC< tstr .size (8..88), bstr .size (8..64)>
```

## 4.2. Claims Describing the Entity

The claims in this section describe the entity itself. They describe the entity whether they occur in evidence or occur in attestation results. See [Section 1.3.1](#) for discussion on how attestation results relate to evidence.

### 4.2.1. ueid (Universal Entity ID) Claim

The "ueid" claim conveys a UEID, which identifies an individual manufactured entity like a mobile phone, a water meter, a Bluetooth speaker or a networked security camera. It may identify the entire entity or a submodule. It does not identify types, models or classes of entities. It is akin to a serial number, though it does not have to be sequential.

UEIDs **MUST** be universally and globally unique across manufacturers and countries, as described in [Section 4.2.1.1](#). UEIDs **MUST** also be unique across protocols and systems, as tokens are intended to be embedded in many different protocols and systems. No two products anywhere, even in completely different industries made by two different manufacturers in two different countries should have the same UEID (if they are not global and universal in this way, then relying parties receiving them will have to track other characteristics of the entity to keep entities distinct between manufacturers).

UEIDs are not designed for direct use by humans (e.g., printing on the case of a device), so no such representation is defined.

There are privacy considerations for UEIDs. See [Section 8.1](#).

A Device Identifier URN is registered for UEIDs. See [Section 10.3](#).

```
$$Claims-Set-Claims //=(ueid-label => ueid-type)  
  
ueid-type = JC<base64-url-text .size (10..44) , bstr .size (7..33)>
```

#### 4.2.1.1. Rules for Creating UEIDs

These rules are solely for the creation of UEIDs. The EAT consumer need not have any awareness of them.

A UEID is constructed of a single type byte followed by the unique bytes for that type. The type byte assures global uniqueness of a UEID even if the unique bytes for different types are accidentally the same.

UEIDS are variable length to accommodate the types defined here and future-defined types.

UEIDs **SHOULD NOT** be longer than 33 bytes. If they are longer, there is no guarantee that a receiver will be able to accept them. See [Appendix B](#).

A UEID is permanent. It **MUST** never change for a given entity.

The different types of UEIDs 1) accommodate different manufacturing processes, 2) accommodate small UEIDs, 3) provide an option that doesn't require registration fees and central administration.

In the unlikely event that a new UEID type is needed, it **MUST** be defined in a standards-track update to this document.

A manufacturer of entities **MAY** use different types for different products. They **MAY** also change from one type to another for a given product or use one type for some items of a given produce and another type for other.

Type Byte	Type Name	Specification
0x01	RAND	This is a 128, 192 or 256-bit random number generated once and stored in the entity. This may be constructed by concatenating enough identifiers to make up an equivalent number of random bits and then feeding the concatenation through a cryptographic hash function. It may also be a cryptographic quality random number generated once at the beginning of the life of the entity and stored. It <b>MUST NOT</b> be smaller than 128 bits. See the length analysis in <a href="#">Appendix B</a> .
0x02	IEEE EUI	This makes use of the device identification scheme operated by the IEEE. An EUI is either an EUI-48, EUI-60 or EUI-64 and made up of an OUI, OUI-36 or a CID, different registered company identifiers, and some unique per-entity identifier. EUIs are often the same as or similar to MAC addresses. This type includes MAC-48, an obsolete name for EUI-48. (Note that while entities with multiple network interfaces may have multiple MAC addresses, there is only one UEID for an entity; changeable MAC addresses that don't meet the permanence

Type Byte	Type Name	Specification
		requirements in this document <b>MUST NOT</b> be used for the UEID or SUEID) [ <a href="#">IEEE.802-2001</a> ], [ <a href="#">OUI.Guide</a> ].
0x03	IMEI	This makes use of the International Mobile Equipment Identity (IMEI) scheme operated by the GSMA. This is a 14-digit identifier consisting of an 8-digit Type Allocation Code (TAC) and a 6-digit serial number allocated by the manufacturer, which <b>SHALL</b> be encoded as byte string of length 14 with each byte as the digit's value (not the ASCII encoding of the digit; the digit 3 encodes as 0x03, not 0x33). The IMEI value encoded <b>SHALL NOT</b> include Luhn checksum or SVN information. See [ <a href="#">ThreeGPP.IMEI</a> ].

Table 1: UEID Composition Types

#### 4.2.1.2. Rules for Consuming UEIDs

For the consumer, a UEID is solely a globally unique opaque identifier. The consumer does not and should not have any awareness of the rules and structure used to achieve global uniqueness.

All implementations **MUST** be able to receive UEIDs up to 33 bytes long. 33 bytes is the longest defined in this document and gives necessary entropy for probabilistic uniqueness.

The consumer of a UEID **MUST** treat it as a completely opaque string of bytes and **MUST NOT** make any use of its internal structure. The reasons for this are:

- \*UEIDs types vary freely from one manufacturer to the next.

- \*New types of UEIDs may be defined.

- \*The manufacturer of an entity is allowed to change from one type of UEID to another anytime they want.

For example, when the consumer receives a type 0x02 UEID, they should not use the OUI part to identify the manufacturer of the device because there is no guarantee all UEIDs will be type 0x02. Different manufacturers may use different types. A manufacturer may make some of their product with one type and others with a different type or even change to a different type for newer versions of their product. Instead, the consumer should use the "oemid" claim.

#### 4.2.2. sueids (Semi-permanent UEIDs) Claim (SUEIDs)

The "sueids" claim conveys one or more semi-permanent UEIDs (SUEIDs). An SUEID has the same format, characteristics and requirements as a



UEID, but **MAY** change to a different value on entity life-cycle events. An entity **MAY** have both a UEID and SUEIDs, neither, one or the other.

Examples of life-cycle events are change of ownership, factory reset and on-boarding into an IoT device management system. It is beyond the scope of this document to specify particular types of SUEIDs and the life-cycle events that trigger their change. An EAT profile **MAY** provide this specification.

There **MAY** be multiple SUEIDs. Each has a text string label the purpose of which is to distinguish it from others. The label **MAY** name the purpose, application or type of the SUEID. For example, the label for the SUEID used by XYZ Onboarding Protocol could thus be "XYZ". It is beyond the scope of this document to specify any SUEID labeling schemes. They are use case specific and **MAY** be specified in an EAT profile.

If there is only one SUEID, the claim remains a map and there still **MUST** be a label.

An SUEID provides functionality similar to an IEEE LDevID [[IEEE.802.1AR](#)].

There are privacy considerations for SUEIDs. See [Section 8.1](#).

A Device Identifier URN is registered for SUEIDs. See [Section 10.3](#).

```
$$Claims-Set-Claims // = (sueids-label => sueids-type)
```

```
sueids-type = {  
  + tstr => ueid-type  
}
```

#### 4.2.3. oemid (Hardware OEM Identification) Claim

The "oemid" claim identifies the Original Equipment Manufacturer (OEM) of the hardware. Any of the three forms described below **MAY** be used at the convenience of the claim sender. The receiver of this claim **MUST** be able to handle all three forms.

Note that the "hwmodel" claim in [Section 4.2.4](#), the "oemboot" claim in [Section 4.2.8](#) and "dbgstat" claim in [Section 4.2.9](#) depend on this claim.

Sometimes one manufacturer will acquire or merge with another. Depending on the situation and use case newly manufactured devices may continue to use the old OEM ID or switch to a new one. This is left to the discretion of the manufacturers, but they should consider how it affects the above-mentioned claims and the attestation eco-system

for their devices. The considerations are the same for all three forms of this claim.

#### 4.2.3.1. Random Number Based OEM ID

The random number based OEM ID **MUST** always be 16 bytes (128 bits) long.

The OEM may create their own ID by using a cryptographic-quality random number generator. They would perform this only once in the life of the company to generate the single ID for said company. They would use that same ID in every entity they make. This uniquely identifies the OEM on a statistical basis and is large enough should there be ten billion companies.

In JSON-encoded tokens this **MUST** be base64url-encoded.

#### 4.2.3.2. IEEE Based OEM ID

The IEEE operates a global registry for MAC addresses and company IDs. This claim uses that database to identify OEMs. The contents of the claim may be either an IEEE MA-L, MA-M, MA-S or an IEEE CID [[IEEE-RA](#)]. An MA-L, formerly known as an OUI, is a 24-bit value used as the first half of a MAC address. MA-M similarly is a 28-bit value uses as the first part of a MAC address, and MA-S, formerly known as OUI-36, a 36-bit value. Many companies already have purchased one of these. A CID is also a 24-bit value from the same space as an MA-L, but not for use as a MAC address. IEEE has published Guidelines for Use of EUI, OUI, and CID [[OUI.Guide](#)] and provides a lookup service [[OUI.Lookup](#)].

Companies that have more than one of these IDs or MAC address blocks **SHOULD** select one and prefer that for all their entities.

Commonly, these are expressed in Hexadecimal Representation as described in [[IEEE.802-2001](#)]. It is also called the Canonical format. When this claim is encoded the order of bytes in the bstr are the same as the order in the Hexadecimal Representation. For example, an MA-L like "AC-DE-48" would be encoded in 3 bytes with values 0xAC, 0xDE, 0x48.

This format is always 3 bytes in size in CBOR.

In JSON-encoded tokens, this **MUST** be base64url-encoded and always 4 bytes.

#### 4.2.3.3. IANA Private Enterprise Number Based OEM ID

IANA maintains a registry for Private Enterprise Numbers (PEN) [[PEN](#)]. A PEN is an integer that identifies an enterprise and may be used to

construct an object identifier (OID) relative to the following OID arc that is managed by IANA: iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1).

For EAT purposes, only the integer value assigned by IANA as the PEN is relevant, not the full OID value.

In CBOR this value **MUST** be encoded as a major type 0 integer and is typically 3 bytes. In JSON, this value **MUST** be encoded as a number.

```
$$Claims-Set-Claims //= (  
    oemid-label => oemid-pen / oemid-ieee / oemid-random  
)
```

```
oemid-pen = int
```

```
oemid-ieee = JC<oemid-ieee-json, oemid-ieee-cbor>
```

```
oemid-ieee-cbor = bstr .size 3
```

```
oemid-ieee-json = base64-url-text .size 4
```

```
oemid-random = JC<oemid-random-json, oemid-random-cbor>
```

```
oemid-random-cbor = bstr .size 16
```

```
oemid-random-json = base64-url-text .size 24
```

#### 4.2.4. hwmodel (Hardware Model) Claim

The "hwmodel" claim differentiates hardware models, products and variants manufactured by a particular OEM, the one identified by OEM ID in [Section 4.2.3](#). It **MUST** be unique within a given OEM ID. The concatenation of the OEM ID and "hwmodel" give a global identifier of a particular product. The "hwmodel" claim **MUST** only be present if an "oemid" claim described in [Section 4.2.3](#) is present.

The granularity of the model identification is for each OEM to decide. It may be very granular, perhaps including some version information. It may be very general, perhaps only indicating top-level products.

The "hwmodel" claim is for use in protocols and not for human consumption. The format and encoding of this claim should not be human-readable to discourage use other than in protocols. If this claim is to be derived from an already-in-use human-readable identifier, it can be run through a hash function.

There is no minimum length so that an OEM with a very small number of models can use a one-byte encoding. The maximum length is 32 bytes. All receivers of this claim **MUST** be able to receive this maximum size.

The receiver of this claim **MUST** treat it as a completely opaque string of bytes, even if there is some apparent naming or structure. The OEM is free to alter the internal structure of these bytes as long as the claim continues to uniquely identify its models.

```
$$Claims-Set-Claims // = (
    hardware-model-label => hardware-model-type
)
```

```
hardware-model-type = JC<base64-url-text .size (4..44),
    bytes .size (1..32)>
```

#### 4.2.5. hwversion (Hardware Version) Claim

The "hwversion" claim is a text string the format of which is set by each manufacturer. The structure and sorting order of this text string can be specified using the version-scheme item from CoSWID [[RFC9393](#)]. It is useful to know how to sort versions so the newer can be distinguished from the older. A "hwversion" claim **MUST** only be present if a "hwmodel" claim described in [Section 4.2.4](#) is present.

```
$$Claims-Set-Claims // = (
    hardware-version-label => hardware-version-type
)
```

```
hardware-version-type = [
    version: tstr,
    ? scheme: $version-scheme
]
```

#### 4.2.6. swname (Software Name) Claim

The "swname" claim contains a very simple free-form text value for naming the software used by the entity. Intentionally, no general rules or structure are set. This will make it unsuitable for use cases that wish precise naming.

If precise and rigorous naming of the software for the entity is needed, the "manifests" claim described in [Section 4.2.15](#) may be used instead.

```
$$Claims-Set-Claims // = ( sw-name-label => tstr )
```

#### 4.2.7. swversion (Software Version) Claim

The "swversion" claim makes use of the CoSWID version-scheme defined in [[RFC9393](#)] to give a simple version for the software. A "swversion" claim **MUST** only be present if a "swname" claim described in [Section 4.2.6](#) is present.

The "manifests" claim [Section 4.2.15](#) may be instead if this is too simple.

```
$$Claims-Set-Claims //=(sw-version-label => sw-version-type)
```

```
sw-version-type = [  
  version: tstr  
  ? scheme: $version-scheme  
]
```

#### 4.2.8. oemboot (OEM Authorized Boot) Claim

An "oemboot" claim with value of true indicates the entity booted with software authorized by the manufacturer of the entity as indicated by the "oemid" claim described in [Section 4.2.3](#). It indicates the firmware and operating system are fully under control of the OEM and may not be replaced by the end user or even the enterprise that owns the device. The means of control may be by cryptographic authentication of the software, by the software being in Read-Only Memory (ROM), a combination of the two or other. If this claim is present the "oemid" claim **MUST** be present.

```
$$Claims-Set-Claims //=(oem-boot-label => bool)
```

#### 4.2.9. dbgstat (Debug Status) Claim

The "dbgstat" claim applies to entity-wide or submodule-wide debug facilities of the entity like [\[JTAG\]](#) and diagnostic hardware built into chips. It applies to any software debug facilities related to privileged software that allows system-wide memory inspection, tracing or modification of non-system software like user mode applications.

This characterization assumes that debug facilities can be enabled and disabled in a dynamic way or be disabled in some permanent way, such that no enabling is possible. An example of dynamic enabling is one where some authentication is required to enable debugging. An example of permanent disabling is blowing a hardware fuse in a chip. The specific type of the mechanism is not taken into account. For example, it does not matter if authentication is by a global password or by per-entity public keys.

As with all claims, the absence of the "dbgstat" claim means it is not reported.

This claim is not extensible so as to provide a common interoperable description of debug status. If a particular implementation considers this claim to be inadequate, it can define its own proprietary claim. It may consider including both this claim as a coarse indication of debug status and its own proprietary claim as a refined indication.

The higher levels of debug disabling requires that all debug disabling of the levels below it be in effect. Since the lowest level requires that all of the target's debug be currently disabled, all other levels require that too.

There is no inheritance of claims from a submodule to a superior module or vice versa. There is no assumption, requirement or guarantee that the target of a superior module encompasses the targets of submodules. Thus, every submodule must explicitly describe its own debug state. The receiver of an EAT **MUST NOT** assume that debug is turned off in a submodule because there is a claim indicating it is turned off in a superior module.

An entity may have multiple debug facilities. The use of plural in the description of the states refers to that, not to any aggregation or inheritance.

The architecture of some chips or devices may be such that a debug facility operates for the whole chip or device. If the EAT for such a chip includes submodules, then each submodule should independently report the status of the whole-chip or whole-device debug facility. This is the only way the receiver can know the debug status of the submodules since there is no inheritance.

#### **4.2.9.1. Enabled**

If any debug facility, even manufacturer hardware diagnostics, is currently enabled, then this level must be indicated.

#### **4.2.9.2. Disabled**

This level indicates all debug facilities are currently disabled. It may be possible to enable them in the future. It may also be that they were enabled in the past, but they are currently disabled.

#### **4.2.9.3. Disabled Since Boot**

This level indicates all debug facilities are currently disabled and have been so since the entity booted/started.

#### **4.2.9.4. Disabled Permanently**

This level indicates all non-manufacturer facilities are permanently disabled such that no end user or developer can enable them. Only the manufacturer indicated in the "oemid" claim can enable them. This also indicates that all debug facilities are currently disabled and have been so since boot/start. If this debug state is reported, the "oemid" claim **MUST** be present.

#### 4.2.9.5. Disabled Fully and Permanently

This level indicates that all debug facilities for the entity are permanently disabled.

```
$$Claims-Set-Claims // = ( debug-status-label => debug-status-type )
```

```
debug-status-type = ds-enabled /  
                   disabled /  
                   disabled-since-boot /  
                   disabled-permanently /  
                   disabled-fully-and-permanently
```

```
ds-enabled          = JC< "enabled", 0 >  
disabled            = JC< "disabled", 1 >  
disabled-since-boot = JC< "disabled-since-boot", 2 >  
disabled-permanently = JC< "disabled-permanently", 3 >  
disabled-fully-and-permanently =  
                    JC< "disabled-fully-and-permanently", 4 >
```

#### 4.2.10. location (Location) Claim

The "location" claim gives the geographic position of the entity from which the attestation originates. Latitude, longitude, altitude, accuracy, altitude-accuracy, heading and speed **MUST** be as defined in the W3C Geolocation API [[W3C.GeoLoc](#)] (which, in turn, is based on [[WGS84](#)]). If the entity is stationary, the heading is NaN (floating-point not-a-number). Latitude and longitude **MUST** always be provided. If any other of these values are unknown, they are omitted.

The location may have been cached for a period of time before token creation. For example, it might have been minutes or hours or more since the last contact with a GNSS satellite. Either the timestamp or age data item can be used to quantify the cached period. The timestamp data item is preferred as it a non-relative time. If the entity has no clock or the clock is unset but has a means to measure the time interval between the acquisition of the location and the token creation the age may be reported instead. The age is in seconds.

See location-related privacy considerations in [Section 8.2](#).

```
$$Claims-Set-Claims //=( location-label => location-type)
```

```
location-type = {  
    latitude => number,  
    longitude => number,  
    ? altitude => number,  
    ? accuracy => number,  
    ? altitude-accuracy => number,  
    ? heading => number,  
    ? speed => number,  
    ? timestamp => ~time-int,  
    ? age => uint  
}
```

```
latitude          = JC< "latitude",          1 >  
longitude         = JC< "longitude",         2 >  
altitude         = JC< "altitude",          3 >  
accuracy         = JC< "accuracy",          4 >  
altitude-accuracy = JC< "altitude-accuracy", 5 >  
heading          = JC< "heading",           6 >  
speed           = JC< "speed",              7 >  
timestamp       = JC< "timestamp",          8 >  
age             = JC< "age",                 9 >
```

#### 4.2.11. uptime (Uptime) Claim

The "uptime" claim contains the number of seconds that have elapsed since the entity or submodule was last booted.

```
$$Claims-Set-Claims //=( uptime-label => uint)
```

#### 4.2.12. bootcount (Boot Count) Claim

The "bootcount" claim contains a count of the number times the entity or submodule has been booted. Support for this claim requires a persistent storage on the device.

```
$$Claims-Set-Claims //=( boot-count-label => uint)
```

#### 4.2.13. bootseed (Boot Seed) Claim

The "bootseed" claim contains a value created at system boot time that allows differentiation of attestation reports from different boot sessions of a particular entity (e.g., a certain UEID).

This value is usually public. It is not a secret and **MUST NOT** be used for any purpose that a secret seed is needed, such as seeding a random number generator.

There are privacy considerations for this claim. See [Section 8.3](#).



```
$$Claims-Set-Claims // = (boot-seed-label => binary-data)
```

#### 4.2.14. dloas (Digital Letters of Approval) Claim

The "dloas" claim conveys one or more Digital Letters of Approval (DLOAs). A DLOA [[DLOA](#)] is a document that describes a certification that an entity has received. Examples of certifications represented by a DLOA include those issued by Global Platform and those based on Common Criteria. The DLOA is unspecific to any particular certification type or those issued by any particular organization.

This claim is typically issued by a verifier, not an attester. Verifiers **MUST NOT** issue this claim unless the entity has received the certification indicated by the DLOA.

This claim **MAY** contain more than one DLOA. If multiple DLOAs are present, verifiers **MUST NOT** issue this claim unless the entity has received all of the certifications.

DLOA documents are always fetched from a registrar that stores them. This claim contains several data items used to construct a Uniform Resource Locator (URL) for fetching the DLOA from the particular registrar.

This claim **MUST** be encoded as an array with either two or three elements. The first element **MUST** be the URL for the registrar. The second element **MUST** be a platform label indicating which platform was certified. If the DLOA applies to an application, then the third element is added which **MUST** be an application label. The method of constructing the registrar URL, platform label and possibly application label is specified in [[DLOA](#)].

The retriever of a DLOA **MUST** follow the recommendation in [[DLOA](#)] and use TLS or some other means to be sure the DLOA registrar they are accessing is authentic. The platform and application labels in the claim indicate the correct DLOA for the entity.

```
$$Claims-Set-Claims // = (  
  dloas-label => [ + dloa-type ]  
)  
  
dloa-type = [  
  dloa_registrar: general-uri  
  dloa_platform_label: text  
  ? dloa_application_label: text  
]
```

#### 4.2.15. manifests (Software Manifests) Claim

The "manifests" claim contains descriptions of software present on the entity. These manifests are installed on the entity when the software is installed or are created as part of the installation process. Installation is anything that adds software to the entity, possibly factory installation, the user installing elective applications and so on. The defining characteristic of a manifest is that it is created by the software manufacturer. The purpose of this claim is to relay unmodified manifests to the verifier and possibly to the relying party.

Some manifests are signed by their software manufacturer independently, and some are not either because they do not support signing or the manufacturer chose not to sign them. For example, a CoSWID might be signed independently before it is included in an EAT. When signed manifests are put into an EAT, the manufacturer's signature **SHOULD** be included even though an EAT's signature will also cover the manifest. This allows the receiver to directly verify the manufacturer-originated manifest.

This claim allows multiple manifest formats. For example, the manifest may be a CBOR-encoded CoSWID, an XML-encoded SWID or other. Identification of the type of manifest is always by a Constrained Application Protocol (CoAP) Content-Format integer [[RFC7252](#)]. If there is no CoAP identifier registered for a manifest format, one **MUST** be registered.

This claim **MUST** be an array of one or more manifests. Each manifest in the claim **MUST** be an array of two. The first item in the array of two **MUST** be an integer CoAP Content-Format identifier. The second item is **MUST** be the actual manifest.

In JSON-encoded tokens the manifest, whatever encoding it is, **MUST** be placed in a text string. When a non-text encoded manifest like a CBOR-encoded CoSWID is put in a JSON-encoded token, the manifest **MUST** be base-64 encoded.

This claim allows for multiple manifests in one token since multiple software packages are likely to be present. The multiple manifests **MAY** be of different encodings. In some cases EAT submodules may be used instead of the array structure in this claim for multiple manifests.

A CoSWID manifest **MUST** be a payload CoSWID, not an evidence CoSWID. These are defined in [[RFC9393](#)].

This claim is extensible for use of manifest formats beyond those mentioned in this document. No particular manifest format is preferred. For manifest interoperability, an EAT profile as defined

in [Section 6](#), should be used to specify which manifest format(s) are allowed.

```
$$Claims-Set-Claims ::= (
    manifests-label => manifests-type
)

manifests-type = [+ manifest-format]

manifest-format = [
    content-type:    coap-content-format,
    content-format: JC< $manifest-body-json,
                    $manifest-body-cbor >
]

$manifest-body-cbor /= bytes .cbor untagged-coswid
$manifest-body-json /= base64-url-text
```

#### 4.2.16. measurements (Measurements) Claim

The "measurements" claim contains descriptions, lists, evidence or measurements of the software that exists on the entity or any other measurable subsystem of the entity (e.g. hash of sections of a file system or non-volatile memory). The defining characteristic of this claim is that its contents are created by processes on the entity that inventory, measure or otherwise characterize the software on the entity. The contents of this claim do not originate from the manufacturer of the measurable subsystem (e.g. developer of a software library).

This claim can be a [\[RFC9393\]](#). When the CoSWID format is used, it **MUST** be an evidence CoSWID, not a payload CoSWID.

Formats other than CoSWID **MAY** be used. The identification of format is by CoAP Content Format, the same as the "manifests" claim in [Section 4.2.15](#).

```

$$Claims-Set-Claims // = (
    measurements-label => measurements-type
)

measurements-type = [+ measurements-format]

measurements-format = [
    content-type: coap-content-format,
    content-format: JC< $measurements-body-json,
                    $measurements-body-cbor >
]

$measurements-body-cbor /= bytes .cbor untagged-coswid
$measurements-body-json /= base64-url-text

```

#### 4.2.17. measres (Software Measurement Results) Claim

The "measres" claim is a general-purpose structure for reporting comparison of measurements to expected reference values. This claim provides a simple standard way to report the result of a comparison as success, failure, fail to run, and absence.

It is the nature of measurement systems that they are specific to the operating system, software and hardware of the entity that is being measured. It is not possible to standardize what is measured and how it is measured across platforms, OS's, software and hardware. The recipient must obtain the information about what was measured and what it indicates for the characterization of the security of the entity from the provider of the measurement system. What this claim provides is a standard way to report basic success or failure of the measurement. In some use cases it is valuable to know if measurements succeeded or failed in a general way even if the details of what was measured is not characterized.

This claim **MAY** be generated by the verifier and sent to the relying party. For example, it could be the results of the verifier comparing the contents of the "measurements" claim, [Section 4.2.16](#), to reference values.

This claim **MAY** also be generated on the entity if the entity has the ability for one subsystem to measure and evaluate another subsystem. For example, a TEE might have the ability to measure the software of the rich OS and may have the reference values for the rich OS.

Within an entity, attestation target or submodule, multiple results can be reported. For example, it may be desirable to report the results for measurements of the file system, chip configuration, installed software, running software and so on.

Note that this claim is not for reporting the overall result of a verifier. It is solely for reporting the result of comparison to reference values.

An individual measurement result (individual-result) is an array consisting of two elements, an identifier of the measurement (result-id) and an enumerated type of the result (result). Different measurement systems will measure different things and perhaps measure the same thing in different ways. It is up to each measurement system to define identifiers (result-id) for the measurements it reports.

Each individual measurement result is part of a group that may contain many individual results. Each group has a text string that names it, typically the name of the measurement scheme or system.

The claim itself consists of one or more groups.

The values for the results enumerated type are as follows:

- 1 -- comparison successful:** Indicates successful comparison to reference values.
- 2 -- comparison fail:** The comparison was completed and did not compare correctly to the reference values.
- 3 -- comparison not run:** The comparison was not run. This includes error conditions such as running out of memory.
- 4 -- measurement absent:** The particular measurement was not available for comparison.

```

$$Claims-Set-Claims // = (
    measurement-results-label =>
        [ + measurement-results-group ] )

measurement-results-group = [
    measurement-system: tstr,
    measurement-results: [ + individual-result ]
]

individual-result = [
    result-id: tstr / binary-data,
    result: result-type,
]

result-type = comparison-successful /
    comparison-fail /
    comparison-not-run /
    measurement-absent

comparison-successful    = JC< "success",        1 >
comparison-fail          = JC< "fail",           2 >
comparison-not-run       = JC< "not-run",        3 >
measurement-absent       = JC< "absent",         4 >

```

#### 4.2.18. submods (Submodules)

Some devices are complex and have many subsystems. A mobile phone is a good example. It may have subsystems for communications (e.g., Wi-Fi and cellular), low-power audio and video playback, multiple security-oriented subsystems like a TEE and a Secure Element, and etc. The claims for a subsystem can be grouped together in a submodule.

Submodules may be used in either evidence or attestation results.

Because system architecture will vary greatly from use case to use case, there are no set requirements for what a submodule represents either in evidence or in attestation results. Profiles, [Section 6](#), may wish to impose requirements. An attester that outputs evidence with submodules should document the semantics it associates with particular submodules for the verifier. Likewise, a verifier that outputs attestation results with submodules should document the semantics it associates with the submodules for the relying party.

A submodule claim is a map that holds some number of submodules. Each submodule is named by its label in the submodule claim map. The value of each entry in a submodule may be a Claims-Set, nested token or Detached-Submodule-Digest. This allows for the submodule to serve as

its own attester or not and allows for claims for each submodule to be represented directly or indirectly, i.e., detached.

A submodule may include a submodule, allowing for arbitrary levels of nesting. However, submodules do not inherit anything from the containing token and must explicitly include all claims. Submodules may contain claims that are present in any surrounding token or submodule. For example, the top-level of the token may have a UEID, a submodule may have a different UEID and a further subordinate submodule may also have a UEID.

The following sub-sections define the three types for representing submodules:

\*A submodule Claims-Set

\*The digest of a detached Claims-Set

\*A nested token, which can be any EAT

The Submodule type definition and Nested-Token type definition vary with the type of encoding. The definitions for CBOR-encoded EATs are as follows:

Nested-Token = CBOR-Nested-Token

CBOR-Nested-Token =  
JSON-Token-Inside-CBOR-Token /  
CBOR-Token-Inside-CBOR-Token

CBOR-Token-Inside-CBOR-Token = bstr .cbor \$EAT-CBOR-Tagged-Token

JSON-Token-Inside-CBOR-Token = tstr

\$\$Claims-Set-Claims // = (submods-label => { + text => Submodule })

Submodule = Claims-Set / CBOR-Nested-Token /  
Detached-Submodule-Digest

The Submodule and Nested-Token definitions for JSON-encoded EATs is as below. This difference in definitions vs. CBOR is necessary because JSON has no tag mechanism and no byte string type to help indicate the nested token is CBOR.

Nested-Token = JSON-Selector

JSON-Selector = \$JSON-Selector

\$JSON-Selector /= [type: "JWT", nested-token: JWT-Message]

\$JSON-Selector /= [type: "CBOR", nested-token:  
CBOR-Token-Inside-JSON-Token]

\$JSON-Selector /= [type: "BUNDLE", nested-token: Detached-EAT-Bundle]

\$JSON-Selector /= [type: "DIGEST", nested-token:  
Detached-Submodule-Digest]

CBOR-Token-Inside-JSON-Token = base64-url-text

\$\$Claims-Set-Claims // = (submods-label => { + text => Submodule })

Submodule = Claims-Set / JSON-Selector

The Detached-Submodule-Digest type is defined as follows:

```
Detached-Submodule-Digest = [  
  hash-algorithm : text / int,  
  digest          : binary-data  
]
```

Nested tokens can be one of three types as defined in this document or types standardized in follow-on documents (e.g., [[UCCS](#)]). Nested tokens are the only mechanism by which JSON can be embedded in CBOR and vice versa.

The addition of further types is accomplished by augmenting the \$EAT-CBOR-Tagged-Token socket or the \$JSON-Selector socket.

When decoding a JSON-encoded EAT, the type of submodule is determined as follows. A JSON object indicates the submodule is a Claims-Set. In all other cases, it is a JSON-Selector, which is an array of two elements that indicates whether the submodule is a nested token or a Detached-Submodule-Digest. The first element in the array indicates the type present in the second element. If the value is "JWT", "CBOR", "BUNDLE" or a future-standardized token types, e.g., [[UCCS](#)], the submodule is a nested token of the indicated type, i.e., JWT-Message, CBOR-Token-Inside-JSON-Token, Detached-EAT-Bundle, or a future type. If the value is "DIGEST", the submodule is a Detached-Submodule-Digest. Any other value indicates a standardized extension to this specification.

When decoding a CBOR-encoded EAT, the CBOR item type indicates the type of the submodule as follows. A map indicates a CBOR-encoded submodule Claims-Set. An array indicates a CBOR-encoded Detached-Submodule-Digest. A byte string indicates a CBOR-encoded CBOR-Nested-Token. A text string indicates a JSON-encoded JSON-Selector. Where



JSON-Selector is used in a CBOR-encoded EAT, the "DIGEST" type and corresponding Detached-Submodule-Digest type **MUST NOT** be used.

The type of a CBOR-encoded nested token is always determined by the CBOR tag encountered after the byte string wrapping is removed in a CBOR-encoded enclosing token or after the base64 wrapping is removed in JSON-encoded enclosing token.

The type of a JSON-encoded nested token is always determined by the string name in JSON-Selector and is always "JWT", "BUNDLE" or a new name standardized outside this document for a further type (e.g., "UCCS"). This string name may also be "CBOR" to indicate the nested token is CBOR-encoded.

"**JWT**": The second array item **MUST** be a JWT formatted according to [\[RFC7519\]](#)

"**CBOR**": The second array item **MUST** be some base64url-encoded CBOR that is a tag, typically a CWT or CBOR-encoded detached EAT bundle

"**BUNDLE**": The second array item **MUST** be a JSON-encoded Detached EAT Bundle as defined in this document.

"**DIGEST**": The second array item **MUST** be a JSON-encoded Detached-Submodule-Digest as defined in this document.

As noted elsewhere, additional EAT types may be defined by a standards action. New type specifications **MUST** address the integration of the new type into the Submodule claim type for submodules.

#### 4.2.18.1. Submodule Claims-Set

The Claims-Set type provides a means of representing claims from a submodule that does not have its own attesting environment, i.e., it has no keys distinct from the attester producing the surrounding token. Claims are represented as a Claims-Set. Submodule claims represented in this way are secured by the same mechanism as the enclosing token (e.g., it is signed by the same attestation key).

The encoding of a submodule Claims-Set **MUST** be the same as the encoding as the surrounding EAT, e.g., all submodule Claims-Sets in a CBOR-encoded token must be CBOR-encoded.

#### 4.2.18.2. Detached Submodule Digest

The Detached-Submodule-Digest type is similar to a submodule Claims-Set, except a digest of the Claims-Set is included in the claim with the Claims-Set contents conveyed separately. The separately-conveyed Claims-Set is called a detached claims set. The input to the digest

algorithm is directly the CBOR or JSON-encoded Claims-Set for the submodule. There is no byte-string wrapping or base 64 encoding.

The data type for this type of submodule is an array consisting of two data items: an algorithm identifier and a byte string containing the digest. The hash algorithm identifier is always from the COSE Algorithm registry, [[IANA.COSE.Algorithms](#)]. Either the integer or string identifier may be used. The hash algorithm identifier is never from the JOSE Algorithm registry.

A detached EAT bundle, described in [Section 5](#), may be used to convey detached claims sets and the EAT containing the corresponding detached digests. EAT, however, doesn't require use of a detached EAT bundle. Any other protocols may be used to convey detached claims sets and the EAT containing the corresponding detached digests. Detached Claims-Sets must not be modified in transit, else validation will fail.

#### **4.2.18.3. Nested Tokens**

The CBOR-Nested-Token and JSON-Selector types provide a means of representing claims from a submodule that has its own attesting environment, i.e., it has keys distinct from the attester producing the surrounding token. Claims are represented in a signed EAT token.

Inclusion of a signed EAT as a claim cryptographically binds the EAT to the surrounding token. If it was conveyed in parallel with the surrounding token, there would be no such binding and attackers could substitute a good attestation from another device for the attestation of an errant subsystem.

A nested token need not use the same encoding as the enclosing token. This enables composite devices to be built without regards to the encoding used by components. Thus, a CBOR-encoded EAT can have a JSON-encoded EAT as a nested token and vice versa.

### **4.3. Claims Describing the Token**

The claims in this section provide meta data about the token they occur in. They do not describe the entity. They may appear in evidence or attestation results.

#### **4.3.1. iat (Timestamp) Claim**

The "iat" claim defined in CWT and JWT is used to indicate the date-of-creation of the token, the time at which the claims are collected and the token is composed and signed.

The data for some claims may be held or cached for some period of time before the token is created. This period may be long, even days.

Examples are measurements taken at boot or a geographic position fix taken the last time a satellite signal was received. There are individual timestamps associated with these claims to indicate their age is older than the "iat" timestamp.

CWT allows the use of floating-point for this claim. EAT disallows the use of floating-point. An EAT token **MUST NOT** contain an "iat" claim in floating-point format. Any recipient of a token with a floating-point format "iat" claim **MUST** consider it an error.

A 64-bit integer representation of the CBOR epoch-based time [RFC8949] used by this claim can represent a range of +/- 500 billion years, so the only point of a floating-point timestamp is to have precession greater than one second. This is not needed for EAT.

#### 4.3.2. eat\_profile (EAT Profile) Claim

See [Section 6](#) for the detailed description of an EAT profile.

The "eat\_profile" claim identifies an EAT profile by either a Uniform Resource Identifier (URI) or an Object Identifier (OID). Typically, the URI will reference a document describing the profile. An OID is just a unique identifier for the profile. It may exist anywhere in the OID tree. There is no requirement that the named document be publicly accessible. The primary purpose of the "eat\_profile" claim is to uniquely identify the profile even if it is a private profile.

The OID is always absolute and never relative.

See [Section 7.2.1](#) for OID and URI encoding.

```
$$Claims-Set-Claims // = (profile-label => general-uri / general-oid)
```

#### 4.3.3. intuse (Intended Use) Claim

EATs may be employed in the context of several different applications. The "intuse" claim provides an indication to an EAT consumer about the intended usage of the token. This claim can be used as a way for an application using EAT to internally distinguish between different ways it utilizes EAT. 5 possible values for "intuse" are currently defined, but an IANA registry can be created in the future to extend these values based on new use cases of EAT.

**1 -- Generic:** Generic attestation describes an application where the EAT consumer requires the most up-to-date security assessment of the attesting entity. It is expected that this is the most commonly-used application of EAT.

**2-- Registration:** Entities that are registering for a new service may be expected to provide an attestation as part of the

registration process. This "intuse" setting indicates that the attestation is not intended for any use but registration.

- 3 -- **Provisioning:** Entities may be provisioned with different values or settings by an EAT consumer. Examples include key material or device management trees. The consumer may require an EAT to assess entity security state of the entity prior to provisioning.
- 4 -- **Certificate Issuance:** Certification Authorities (CAs) may require attestation results (which in a background check model might require receiving evidence to be passed to a verifier) to make decisions about the issuance of certificates. An EAT may be used as part of the certificate signing request (CSR).
- 5 -- **Proof-of-Possession:** An EAT consumer may require an attestation as part of an accompanying proof-of-possession (PoP) application. More precisely, a PoP transaction is intended to provide to the recipient cryptographically-verifiable proof that the sender has possession of a key. This kind of attestation may be necessary to verify the security state of the entity storing the private key used in a PoP application.

```
$$Claims-Set-Claims // = ( intended-use-label => intended-use-type )
```

```
intended-use-type = generic /  
                  registration /  
                  provisioning /  
                  csr /  
                  pop
```

```
generic          = JC< "generic",      1 >  
registration     = JC< "registration", 2 >  
provisioning     = JC< "provisioning", 3 >  
csr              = JC< "csr",          4 >  
pop              = JC< "pop",          5 >
```

## 5. Detached EAT Bundles

A detached EAT bundle is a message to convey an EAT plus detached claims sets secured by that EAT. It is a top-level message like a CWT or JWT. It can occur in any place that a CWT or JWT occurs, for example as a submodule nested token as defined in [Section 4.2.18.3](#).

A detached EAT bundle may be either CBOR or JSON-encoded.

A detached EAT bundle consists of two parts.

The first part is an encoded EAT as follows:

- \***MUST** have at least one submodule that is a detached submodule digest as defined in [Section 4.2.18.2](#)
- \***MAY** be either CBOR or JSON-encoded and doesn't have to be the same as the encoding of the bundle
- \***MAY** be a CWT, or JWT or some future-defined token type, but **MUST NOT** be a detached EAT bundle
- \***MUST** be authenticity and integrity protected

The same mechanism for distinguishing the type for nested token submodules is employed here.

The second part is a map/object as follows:

- \***MUST** be a Claims-Set
- \***MUST** use the same encoding as the bundle
- \***MUST** be wrapped in a byte string when the encoding is CBOR and be base64url-encoded when the encoding is JSON

For CBOR-encoded detached EAT bundles, tag 602 can be used to identify it. The standard rules apply for use or non-use of a tag. When it is sent as a submodule, it is always sent as a tag to distinguish it from the other types of nested tokens.

The digests of the detached claims sets are associated with detached Claims-Sets by label/name. It is up to the constructor of the detached EAT bundle to ensure the names uniquely identify the detached claims sets. Since the names are used only in the detached EAT bundle, they can be very short, perhaps one byte.

BUNDLE-Messages = BUNDLE-Tagged-Message / BUNDLE-Untagged-Message

BUNDLE-Tagged-Message = #6.602(BUNDLE-Untagged-Message)

BUNDLE-Untagged-Message = Detached-EAT-Bundle

```
Detached-EAT-Bundle = [  
  main-token : Nested-Token,  
  detached-claims-sets: {  
    + tstr => JC-NEST-SAFE<json-wrapped-claims-set,  
                                     cbor-wrapped-claims-set>  
  }  
]
```

json-wrapped-claims-set = base64-url-text

cbor-wrapped-claims-set = bstr .cbor Claims-Set

## 6. Profiles

EAT makes normative use of CBOR, JSON, COSE, JOSE, CWT and JWT. Most of these have implementation options to accommodate a range of use cases.

For example, COSE doesn't require a particular set of cryptographic algorithms so as to accommodate different usage scenarios and evolution of algorithms over time. Section 10 of [\[RFC9052\]](#) describes the profiling considerations for COSE.

The use of encryption is optional for both CWT and JWT. Section 8 of [\[RFC7519\]](#) describes implementation requirement and recommendations for JWT.

Similarly, CBOR provides indefinite length encoding, which is not commonly used, but valuable for very constrained devices. For EAT itself, in a particular use case some claims will be used and others will not. Section 4 of [\[RFC8949\]](#) describes serialization considerations for CBOR.

For example a mobile phone use case may require the device make and model, and prohibit UEID and location for privacy reasons. The general EAT standard retains all this flexibility because it too is aimed to accommodate a broad range of use cases.

It is necessary to explicitly narrow these implementation options to guarantee interoperability. EAT chooses one general and explicit mechanism, the profile, to indicate the choices made for these implementation options for all aspects of the token.

Below is a list of the various issues that should be addressed by a profile.

The "eat\_profile" claim in [Section 4.3.2](#) provides a unique identifier for the profile a particular token uses.

A profile can apply to evidence or to attestation results or both.

### 6.1. Format of a Profile Document

A profile document doesn't have to be in any particular format. It may be simple text, something more formal or a combination.

A profile may define, and possibly register, one or more new claims if needed. A profile may also reuse one or more already defined claims, either as-is or with values constrained to a subset or subrange.

### 6.2. Full and Partial Profiles

For a "full" profile, the receiver will be able to decode and verify every possible EAT sent when a sender and receiver both adhere to it. For a "partial" profile, there are still some protocol options left undecided.

For example, a profile that allows the use of signing algorithms by the sender that the receiver is not required to support is a partial profile. The sender might choose a signing algorithm that some receivers don't support.

Full profiles **MUST** be complete such that a complying receiver can decode, verify and check for freshness every EAT created by a complying sender. Full profiles do not need to require the receiver fully handle every claim in an EAT from a complying sender. Profile specifications may assume the receiver has access to the necessary verification keys or may go into specific detail on the means to access verification keys.

The "eat\_profile" claim **MUST NOT** be used to identify partial profiles.

While fewer profiles are preferable, sometimes several may be needed for a use case. One approach to handling variation in devices might be to define several full profiles that are variants of each other. It is relatively easy and inexpensive to define profiles as they don't have to be standards track and don't have to be registered anywhere. For example, flexibility for post-quantum algorithms can be handled as follows. First, define a full profile for a set of non-post-quantum algorithms for current use. Then, when post-quantum

algorithms are settled, define another full profile derived from the first.

### **6.3. List of Profile Issues**

The following is a list of EAT, CWT, JWT, COSE, JOSE and CBOR options that a profile should address.

#### **6.3.1. Use of JSON, CBOR or both**

A profile should specify whether CBOR, JSON or both may be sent. A profile should specify that the receiver can accept all encodings that the sender is allowed to send.

This should be specified for the top-level and all nested tokens. For example, a profile might require all nested tokens to be of the same encoding of the top level token.

#### **6.3.2. CBOR Map and Array Encoding**

A profile should specify whether definite-length arrays/maps, indefinite-length arrays/maps or both may be sent. A profile should specify that the receiver be able to accept all length encodings that the sender is allowed to send.

This applies to individual EAT claims, CWT and COSE parts of the implementation.

For most use cases, specifying that only definite-length arrays/maps may be sent is suitable.

#### **6.3.3. CBOR String Encoding**

A profile should specify whether definite-length strings, indefinite-length strings or both may be sent. A profile should specify that the receiver be able to accept all types of string encodings that the sender is allowed to send.

For most use cases, specifying that only definite-length strings may be sent is suitable.

#### **6.3.4. CBOR Preferred Serialization**

A profile should specify whether or not CBOR preferred serialization must be sent or not. A profile should specify the receiver be able to accept preferred and/or non-preferred serialization so it will be able to accept anything sent by the sender.



### 6.3.5. CBOR Tags

The profile should specify whether the token should be a CWT Tag or not.

When COSE protection is used, the profile should specify whether COSE tags are used or not. Note that RFC 8392 requires COSE tags be used in a CWT tag.

Often a tag is unnecessary because the surrounding or carrying protocol identifies the object as an EAT.

### 6.3.6. COSE/JOSE Protection

COSE and JOSE have several options for signed, MACed and encrypted messages. JWT may use the JOSE NULL protection option. It is possible to implement no protection, sign only, MAC only, sign then encrypt and so on. All combinations allowed by COSE, JOSE, JWT, and CWT are allowed by EAT.

A profile should specify all signing, encryption and MAC message formats that may be sent. For example, a profile might allow only COSE\_Sign1 to be sent. For another example, a profile might allow COSE\_Sign and COSE\_Encrypt to be sent to carry multiple signatures for post quantum cryptography and to use encryption to provide confidentiality.

A profile should specify the receiver accepts all message formats that are allowed to be sent.

When both signing and encryption are allowed, a profile should specify which is applied first.

### 6.3.7. COSE/JOSE Algorithms

See the section on "Application Profiling Considerations" in [[RFC9052](#)] for a discussion on selection of cryptographic algorithms and related issues.

The profile **MAY** require the protocol or system using EAT to provide an algorithm negotiation mechanism.

If not, the profile document should list a set of algorithms for each COSE and JOSE message type allowed by the profile per [Section 6.3.6](#). The verifier should implement all of them. The attester may implement any of them it wishes, possibly just one for each message type.

If detached submodule digests are used the profile should address the determination of the hash algorithm(s) for the digests.

### 6.3.8. Detached EAT Bundle Support

A profile should specify whether or not a detached EAT bundle ([Section 5](#)) can be sent. A profile should specify that a receiver be able to accept a detached EAT bundle if the sender is allowed to send it.

### 6.3.9. Key Identification

A profile should specify what must be sent to identify the verification, decryption or MAC key or keys. If multiple methods of key identification may be sent, a profile should require the receiver support them all.

[Appendix F](#) describes a number of methods for identifying verification keys. When encryption is used, there are further considerations. In some cases key identification may be very simple and in others involve multiple components. For example, it may be simple through use of COSE key ID or it may be complex through use of an X.509 certificate hierarchy.

While not always possible, a profile should specify or make reference to, a full end-end specification for key identification. For example, a profile should specify in full detail how COSE key IDs are to be created, their lifecycle and such rather than just specifying that a COSE key ID be used. For example, a profile should specify the full details of an X.509 hierarchy including extension processing, algorithms allowed and so on rather than just saying X.509 certificates are used.

### 6.3.10. Endorsement Identification

Similar to, or perhaps the same as verification key identification, the profile may wish to specify how endorsements are to be identified. However note that endorsement identification is optional, whereas key identification is not.

### 6.3.11. Freshness

Security considerations, see [Section 9.3](#), require a mechanism to provide freshness. This may be the EAT nonce claim in [Section 4.1](#), or some claim or mechanism defined outside this document. The section on freshness in [[RFC9334](#)] describes several options. A profile should specify which freshness mechanism or mechanisms can be used.

If the EAT nonce claim is used, a profile should specify whether multiple nonces may be sent. If a profile allows multiple nonces to be sent, it should require the receiver to process multiple nonces.

### 6.3.12. Claims Requirements

A profile may define new claims that are not defined in this document.

This document requires an EAT receiver must accept tokens with claims it does not understand. A profile for a specific use case may reverse this and allow a receiver to reject tokens with claims it does not understand. A profile for a specific use case may specify that specific claims are prohibited.

A profile for a specific use case may modify this and specify that some claims are required.

A profile may constrain the definition of claims that are defined in this document or elsewhere. For example, a profile may require the EAT nonce be a certain length or the "location" claim always include the altitude.

Some claims are "pluggable" in that they allow different formats for their content. The "manifests" claim ([Section 4.2.15](#)) along with the measurement and "measurements" ([Section 4.2.16](#)) claims are examples of this, allowing the use of CoSWID and other formats. A profile should specify which formats are allowed to be sent, with the assumption that the corresponding CoAP content types have been registered. A profile should require the receiver to accept all formats that are allowed to be sent.

Further, if there is variation within a format that is allowed, the profile should specify which variations can be sent. For example, there are variations in the CoSWID format. A profile that require the receiver to accept all variations that are allowed to be sent.

### 6.4. The Constrained Device Standard Profile

It is anticipated that there will be many profiles defined for EAT for many different use cases. This section gives a normative definition of one profile that is good for many constrained device use cases.

The identifier for this profile is "urn:ietf:rfc:rfcTBD".

RFC Editor: please replace rfcTBD with this RFC number and remove this note.

Issue	Profile Definition
CBOR/JSON	CBOR <b>MUST</b> be used
CBOR Encoding	Definite length maps and arrays <b>MUST</b> be used
CBOR Encoding	Definite length strings <b>MUST</b> be used

Issue	Profile Definition
CBOR Serialization	Preferred serialization <b>MUST</b> be used
COSE Protection	COSE_Sign1 <b>MUST</b> be used
Algorithms	The receiver <b>MUST</b> accept ES256, ES384 and ES512; the sender <b>MUST</b> send one of these
Detached EAT Bundle Usage	Detached EAT bundles <b>MUST NOT</b> be sent with this profile
Verification Key Identification	Either the COSE kid or the UEID <b>MUST</b> be used to identify the verification key. If both are present, the kid takes precedence. (It is assumed the receiver has access to a database of trusted verification keys which allows lookup of the verification key ID; the key format and means of distribution are beyond the scope of this profile)
Endorsements	This profile contains no endorsement identifier
Freshness	A new single unique nonce <b>MUST</b> be used for every token request
Claims	No requirement is made on the presence or absence of claims other than requiring an EAT nonce. As per general EAT rules, the receiver <b>MUST NOT</b> error out on claims it doesn't understand.

Table 2: Constrained Device Profile Definition

Any profile with different requirements than those above **MUST** have a different profile identifier.

Note that many claims can be present for tokens conforming to this profile, even claims not defined in this document. Note also that even slight deviation from the above requirements is considered a different profile that **MUST** have a different identifier. For example, if a kid (key identifier) or UEID is not used for key identification, it is not in conformance with this profile. For another example, requiring the presence of some claim is also not in conformance and requires another profile.

Derivations of this profile are encouraged. For example another profile may be simply defined as The Constrained Device Standard Profile plus the requirement for the presence of claim xxxx and claim yyyy.

## 7. Encoding and Collected CDDL

An EAT is fundamentally defined using CDDL. This document specifies how to encode the CDDL in CBOR or JSON. Since CBOR can express some things that JSON can't (e.g., tags) or that are expressed differently (e.g., labels) there is some CDDL that is specific to the encoding.

## 7.1. Claims-Set and CDDL for CWT and JWT

CDDL was not used to define CWT or JWT. It was not available at the time.

This document defines CDDL for both CWT and JWT. This document does not change the encoding or semantics of anything in a CWT or JWT.

A Claims-Set is the central data structure for EAT, CWT and JWT. It holds all the claims and is the structure that is secured by signing or other means. It is not possible to define EAT, CWT, or JWT in CDDL without it. The CDDL definition of Claims-Set here is applicable to EAT, CWT and JWT.

This document specifies how to encode a Claims-Set in CBOR or JSON.

With the exception of nested tokens and some other externally defined structures (e.g., SWIDs) an entire Claims-Set must be in encoded in either CBOR or JSON, never a mixture.

CDDL for the seven claims defined by [\[RFC8392\]](#) and [\[RFC7519\]](#) is included here.

## 7.2. Encoding Data Types

This makes use of the types defined in [\[RFC8610\]](#) Appendix D, Standard Prelude.

### 7.2.1. Common Data Types

time-int is identical to the epoch-based time, but disallows floating-point representation.

For CBOR-encoded tokens, OIDs are specified using the CDDL type name "oid" from [\[RFC9090\]](#). They are encoded without the tag number. For JSON-encoded tokens, OIDs are a text string in the common form of "nn.nn.nn...".

Unless explicitly indicated, URIs are not the URI tag defined in [\[RFC8949\]](#). They are just text strings that contain a URI conforming to the format defined in [\[RFC3986\]](#).

```
time-int = #6.1(int)

binary-data = JC< base64-url-text, bstr>

base64-url-text = tstr .regexp "[A-Za-z0-9_-]+"

general-oid = JC< json-oid, ~oid >

json-oid = tstr .regexp "([0-2])((\\\.0)|(\\\. [1-9][0-9]*))*"

general-uri = JC< text, ~uri >

coap-content-format = uint .le 65535
```

### 7.2.2. JSON Interoperability

JSON should be encoded per [[RFC8610](#)], Appendix E. In addition, the following CDDL types are encoded in JSON as follows:

- \*bstr -- **MUST** be base64url-encoded
- \*time -- **MUST** be encoded as NumericDate as described in Section 2 of [[RFC7519](#)].
- \*string-or-uri -- **MUST** be encoded as StringOrURI as described in Section 2 of [[RFC7519](#)].
- \*uri -- **MUST** be a URI [[RFC3986](#)].
- \*oid -- **MUST** be encoded as a string using the well established dotted-decimal notation (e.g., the text "1.2.250.1") [[RFC4517](#)].

The CDDL generic "JC<>" is used in most places where there is a variance between CBOR and JSON. The first argument is the CDDL for JSON and the second is CDDL for CBOR.

### 7.2.3. Labels

Most map labels, Claims-Keys, Claim-Names and enumerated-type values are integers for CBOR-encoded tokens and strings for JSON-encoded tokens. When this is the case the "JC<>" CDDL construct is used to give both the integer and string values.

### 7.2.4. CBOR Interoperability

CBOR allows data items to be serialized in more than one form to accommodate a variety of use cases. This is addressed in [Section 6](#).

### 7.3. Collected CDDL

#### 7.3.1. Payload CDDL

This CDDL defines all the EAT Claims that are added to the main definition of a Claim-Set in [Appendix D](#). Claims-Set is the payload for CWT, JWT and potentially other token types. This is for both CBOR and JSON. When there is variation between CBOR and JSON, the JC<> CDDL generic defined in [Appendix D](#). Note that the JC<> generic uses the CDDL ".feature" control operator defined in [[RFC9165](#)].

This CDDL uses, but doesn't define Submodule or nested tokens because the definition for these types varies between CBOR and JSON and the JC<> generic can't be used to define it. The submodule claim is the one place where a CBOR token can be nested inside a JSON token and vice versa. Encoding-specific definitions are provided in the following sections.

```

time-int = #6.1(int)

binary-data = JC< base64-url-text, bstr>

base64-url-text = tstr .regexp "[A-Za-z0-9_-]+"

general-oid = JC< json-oid, ~oid >

json-oid = tstr .regexp "([0-2])((\\\.0)|(\\\. [1-9][0-9]*))*"

general-uri = JC< text, ~uri >

coap-content-format = uint .le 65535

$$Claims-Set-Claims //=
    (nonce-label => nonce-type / [ 2* nonce-type ])

nonce-type = JC< tstr .size (8..88), bstr .size (8..64)>

$$Claims-Set-Claims //= (ueid-label => ueid-type)

ueid-type = JC<base64-url-text .size (10..44) , bstr .size (7..33)>

$$Claims-Set-Claims //= (sueids-label => sueids-type)

sueids-type = {
    + tstr => ueid-type
}

$$Claims-Set-Claims //= (
    oemid-label => oemid-pen / oemid-ieee / oemid-random
)

oemid-pen = int

oemid-ieee = JC<oemid-ieee-json, oemid-ieee-cbor>
oemid-ieee-cbor = bstr .size 3
oemid-ieee-json = base64-url-text .size 4

oemid-random = JC<oemid-random-json, oemid-random-cbor>
oemid-random-cbor = bstr .size 16
oemid-random-json = base64-url-text .size 24

$$Claims-Set-Claims //= (
    hardware-version-label => hardware-version-type
)

hardware-version-type = [

```



```

    version: tstr,
    ? scheme: $version-scheme
]

$$Claims-Set-Claims //= (
    hardware-model-label => hardware-model-type
)

hardware-model-type = JC<base64-url-text .size (4..44),
    bytes .size (1..32)>

$$Claims-Set-Claims //= ( sw-name-label => tstr )

$$Claims-Set-Claims //= (sw-version-label => sw-version-type)

sw-version-type = [
    version: tstr
    ? scheme: $version-scheme
]

$$Claims-Set-Claims //= (oem-boot-label => bool)

$$Claims-Set-Claims //= ( debug-status-label => debug-status-type )

debug-status-type = ds-enabled /
    disabled /
    disabled-since-boot /
    disabled-permanently /
    disabled-fully-and-permanently

ds-enabled                = JC< "enabled", 0 >
disabled                  = JC< "disabled", 1 >
disabled-since-boot       = JC< "disabled-since-boot", 2 >
disabled-permanently      = JC< "disabled-permanently", 3 >
disabled-fully-and-permanently =
    JC< "disabled-fully-and-permanently", 4 >

$$Claims-Set-Claims //= (location-label => location-type)

location-type = {
    latitude => number,
    longitude => number,
    ? altitude => number,
    ? accuracy => number,
    ? altitude-accuracy => number,
    ? heading => number,
    ? speed => number,
    ? timestamp => ~time-int,
    ? age => uint
}

```

```

latitude      = JC< "latitude",      1 >
longitude     = JC< "longitude",     2 >
altitude      = JC< "altitude",      3 >
accuracy      = JC< "accuracy",      4 >
altitude-accuracy = JC< "altitude-accuracy", 5 >
heading       = JC< "heading",       6 >
speed         = JC< "speed",         7 >
timestamp     = JC< "timestamp",     8 >
age           = JC< "age",           9 >

$$Claims-Set-Claims // = (uptime-label => uint)

$$Claims-Set-Claims // = (boot-seed-label => binary-data)

$$Claims-Set-Claims // = (boot-count-label => uint)

$$Claims-Set-Claims // = ( intended-use-label => intended-use-type )

intended-use-type = generic /
                  registration /
                  provisioning /
                  csr /
                  pop

generic          = JC< "generic",      1 >
registration     = JC< "registration", 2 >
provisioning     = JC< "provisioning", 3 >
csr              = JC< "csr",         4 >
pop              = JC< "pop",         5 >

$$Claims-Set-Claims // = (
    dloa-label => [ + dloa-type ]
)

dloa-type = [
    dloa_registrar: general-uri
    dloa_platform_label: text
    ? dloa_application_label: text
]

$$Claims-Set-Claims // = (profile-label => general-uri / general-oid)

$$Claims-Set-Claims // = (
    manifests-label => manifests-type
)

manifests-type = [+ manifest-format]

manifest-format = [

```

```

    content-type:  coap-content-format,
    content-format: JC< $manifest-body-json,
                    $manifest-body-cbor >
]

$manifest-body-cbor /= bytes .cbor untagged-coswid
$manifest-body-json /= base64-url-text

$$Claims-Set-Claims // = (
    measurements-label => measurements-type
)

measurements-type = [+ measurements-format]

measurements-format = [
    content-type:  coap-content-format,
    content-format: JC< $measurements-body-json,
                    $measurements-body-cbor >
]

$measurements-body-cbor /= bytes .cbor untagged-coswid
$measurements-body-json /= base64-url-text

$$Claims-Set-Claims // = (
    measurement-results-label =>
        [ + measurement-results-group ] )

measurement-results-group = [
    measurement-system: tstr,
    measurement-results: [ + individual-result ]
]

individual-result = [
    result-id:  tstr / binary-data,
    result:    result-type,
]

result-type = comparison-successful /
              comparison-fail /
              comparison-not-run /
              measurement-absent

comparison-successful = JC< "success",      1 >
comparison-fail       = JC< "fail",         2 >
comparison-not-run    = JC< "not-run",     3 >
measurement-absent    = JC< "absent",      4 >

```

```
Detached-Submodule-Digest = [  
  hash-algorithm : text / int,  
  digest         : binary-data  
]
```

```
BUNDLE-Messages = BUNDLE-Tagged-Message / BUNDLE-Untagged-Message
```

```
BUNDLE-Tagged-Message = #6.602(BUNDLE-Untagged-Message)  
BUNDLE-Untagged-Message = Detached-EAT-Bundle
```

```
Detached-EAT-Bundle = [  
  main-token : Nested-Token,  
  detached-claims-sets: {  
    + tstr => JC-NEST-SAFE<json-wrapped-claims-set,  
                                     cbor-wrapped-claims-set>  
  }  
]
```

```
json-wrapped-claims-set = base64-url-text
```

```
cbor-wrapped-claims-set = bstr .cbor Claims-Set
```

```
nonce-label           = JC< "eat_nonce",    10 >  
ueid-label            = JC< "ueid",         256 >  
sueids-label         = JC< "sueids",        257 >  
oemid-label          = JC< "oemid",         258 >  
hardware-model-label = JC< "hwmodel",       259 >  
hardware-version-label = JC< "hwversion",   260 >  
uptime-label         = JC< "uptime",       261 >  
oem-boot-label       = JC< "oemboot",      262 >  
debug-status-label  = JC< "dbgstat",       263 >  
location-label       = JC< "location",     264 >  
profile-label        = JC< "eat_profile",  265 >  
submods-label        = JC< "submods",      266 >  
boot-count-label     = JC< "bootcount",    267 >  
boot-seed-label      = JC< "bootseed",     268 >  
dloas-label          = JC< "dloas",        269 >  
sw-name-label        = JC< "swname",       270 >  
sw-version-label     = JC< "swversion",    271 >  
manifests-label      = JC< "manifests",    272 >  
measurements-label  = JC< "measurements",  273 >  
measurement-results-label = JC< "measres" , 274 >  
intended-use-label   = JC< "intuse",       275 >
```

### 7.3.2. CBOR-Specific CDDL

EAT-CBOR-Token = \$EAT-CBOR-Tagged-Token / \$EAT-CBOR-Untagged-Token

\$EAT-CBOR-Tagged-Token /= CWT-Tagged-Message

\$EAT-CBOR-Tagged-Token /= BUNDLE-Tagged-Message

\$EAT-CBOR-Untagged-Token /= CWT-Untagged-Message

\$EAT-CBOR-Untagged-Token /= BUNDLE-Untagged-Message

Nested-Token = CBOR-Nested-Token

CBOR-Nested-Token =

    JSON-Token-Inside-CBOR-Token /

    CBOR-Token-Inside-CBOR-Token

CBOR-Token-Inside-CBOR-Token = bstr .cbor \$EAT-CBOR-Tagged-Token

JSON-Token-Inside-CBOR-Token = tstr

\$\$Claims-Set-Claims // = (submods-label => { + text => Submodule })

Submodule = Claims-Set / CBOR-Nested-Token /

    Detached-Submodule-Digest

### 7.3.3. JSON-Specific CDDL

EAT-JSON-Token = \$EAT-JSON-Token-Formats

\$EAT-JSON-Token-Formats /= JWT-Message

\$EAT-JSON-Token-Formats /= BUNDLE-Untagged-Message

Nested-Token = JSON-Selector

JSON-Selector = \$JSON-Selector

\$JSON-Selector /= [type: "JWT", nested-token: JWT-Message]

\$JSON-Selector /= [type: "CBOR", nested-token:

    CBOR-Token-Inside-JSON-Token]

\$JSON-Selector /= [type: "BUNDLE", nested-token: Detached-EAT-Bundle]

\$JSON-Selector /= [type: "DIGEST", nested-token:

    Detached-Submodule-Digest]

CBOR-Token-Inside-JSON-Token = base64-url-text

\$\$Claims-Set-Claims // = (submods-label => { + text => Submodule })

Submodule = Claims-Set / JSON-Selector

## 8. Privacy Considerations

Certain EAT claims can be used to track the owner of an entity; therefore, implementations should consider privacy-preserving options dependent on the usage of the EAT. For example, the location claim might be suppressed in EATs sent to unauthenticated consumers.

### 8.1. UEID and SUEID Privacy Considerations

A UEID is usually not privacy-preserving. Relying parties receiving tokens that happen to be from a particular entity will be able to know the tokens are from the same entity and be able to identify the entity issuing those tokens.

Thus the use of the claim may violate privacy policies. In other usage situations a UEID will not be allowed for certain products like browsers that give privacy for the end user. It will often be the case that tokens will not have a UEID for these reasons.

An SUEID is also usually not privacy-preserving. In some cases it may have fewer privacy issues than a UEID depending on when and how and when it is generated.

There are several strategies that can be used to still be able to put UEIDs and SUEIDs in tokens:

\*The entity obtains explicit permission from the user of the entity to use the UEID/SUEID. This may be through a prompt. It may also be through a license agreement. For example, agreements for some online banking and brokerage services might already cover use of a UEID/SUEID.

\*The UEID/SUEID is used only in a particular context or particular use case. It is used only by one relying party.

\*The entity authenticates the relying party and generates a derived UEID/SUEID just for that particular relying party. For example, the relying party could prove their identity cryptographically to the entity, then the entity generates a UEID just for that relying party by hashing a proofed relying party ID with the main entity UEID/SUEID.

Note that some of these privacy preservation strategies result in multiple UEIDs and SUEIDs per entity. Each UEID/SUEID is used in a different context, use case or system on the entity. However, from the view of the relying party, there is just one UEID and it is still globally universal across manufacturers.

## **8.2. Location Privacy Considerations**

Geographic location is most always considered personally identifiable information. Implementers should consider laws and regulations governing the transmission of location data from end user devices to servers and services. Implementers should consider using location management facilities offered by the operating system on the entity generating the attestation. For example, many mobile phones prompt the user for permission before sending location data.

## **8.3. Boot Seed Privacy Considerations**

The "bootseed" claim is effectively a stable entity identifier within a given boot epoch. Therefore, it is not suitable for use in attestation schemes that are privacy-preserving.

## **8.4. Replay Protection and Privacy**

EAT defines the EAT nonce claim for replay protection and token freshness. The nonce claim is based on a value usually derived remotely (outside of the entity). This claim might be used to extract and convey personally identifying information either inadvertently or by intention. For instance, an implementor may choose a nonce equivalent to a username associated with the device (e.g., account login). If the token is inspected by a 3rd-party then this

information could be used to identify the source of the token or an account associated with the token. To avoid the conveyance of privacy-related information in the nonce claim, it should be derived using a salt that originates from a true and reliable random number generator or any other source of randomness that would still meet the target system requirements for replay protection and token freshness.

## 9. Security Considerations

The security considerations provided in Section 8 of [[RFC8392](#)] and Section 11 of [[RFC7519](#)] apply to EAT in its CWT and JWT form, respectively. Moreover, Chapter 12 of [[RFC9334](#)] is also applicable to implementations of EAT. In addition, implementors should consider the following.

### 9.1. Claim Trustworthiness

This specification defines semantics for each claim. It does not require any particular level of security in the implementation of the claims or even the attester itself. Such specification is far beyond the scope of this document which is about a message format not the security level of an implementation.

The receiver of an EAT comes to know the trustworthiness of the claims in it by understanding the implementation made by the attester vendor and/or understanding the checks and processing performed by the verifier.

For example, this document says that a UEID is permanent and that it must not change, but it doesn't say what degree of attack to change it must be defended.

The degree of security will vary from use case to use case. In some cases the receiver may only need to know something of the implementation such as that it was implemented in a TEE. In other cases the receiver may require the attester be certified by a particular certification program. Or perhaps the receiver is content with very little security.

### 9.2. Key Provisioning

Private key material can be used to sign and/or encrypt the EAT, or can be used to derive the keys used for signing and/or encryption. In some instances, the manufacturer of the entity may create the key material separately and provision the key material in the entity itself. The manufacturer of any entity that is capable of producing an EAT should take care to ensure that any private key material be suitably protected prior to provisioning the key material in the entity itself. This can require creation of key material in an enclave (see [[RFC4949](#)] for definition of "enclave"), secure



transmission of the key material from the enclave to the entity using an appropriate protocol, and persistence of the private key material in some form of secure storage to which (preferably) only the entity has access.

### 9.2.1. Transmission of Key Material

Regarding transmission of key material from the enclave to the entity, the key material may pass through one or more intermediaries. Therefore some form of protection ("key wrapping") may be necessary. The transmission itself may be performed electronically, but can also be done by human courier. In the latter case, there should be minimal to no exposure of the key material to the human (e.g. encrypted portable memory). Moreover, the human should transport the key material directly from the secure enclave where it was created to a destination secure enclave where it can be provisioned.

### 9.3. Freshness

All EAT use **MUST** provide a freshness mechanism to prevent replay and related attacks. The extensive discussions on freshness in [\[RFC9334\]](#) including security considerations apply here. The EAT nonce claim, in [Section 4.1](#), is one option to provide freshness.

### 9.4. Multiple EAT Consumers

In many cases, more than one EAT consumer may be required to fully verify the entity attestation. Examples include individual consumers for nested EATs, or consumers for individual claims with an EAT. When multiple consumers are required for verification of an EAT, it is important to minimize information exposure to each consumer. In addition, the communication between multiple consumers should be secure.

For instance, consider the example of an encrypted and signed EAT with multiple claims. A consumer may receive the EAT (denoted as the "receiving consumer"), decrypt its payload, verify its signature, but then pass specific subsets of claims to other consumers for evaluation ("downstream consumers"). Since any COSE encryption will be removed by the receiving consumer, the communication of claim subsets to any downstream consumer **MUST** leverage an equivalent communication security protocol (e.g. Transport Layer Security).

However, assume the EAT of the previous example is hierarchical and each claim subset for a downstream consumer is created in the form of a nested EAT. Then the nested EAT is itself encrypted and cryptographically verifiable (due to its COSE envelope) by a downstream consumer (unlike the previous example where a claims set without a COSE envelope is sent to a downstream consumer). Therefore, Transport Layer Security between the receiving and downstream

consumers is not strictly required. Nevertheless, downstream consumers of a nested EAT should provide a nonce unique to the EAT they are consuming.

### **9.5. Detached EAT Bundle Digest Security Considerations**

A detached EAT bundle is composed of a nested EAT and a claims set as per [Section 5](#). Although the attached claims set is vulnerable to modification in transit, any modification can be detected by the receiver through the associated digest, which is a claim fully contained within an EAT. Moreover, the digest itself can only be derived using an appropriate COSE hash algorithm, implying that an attacker cannot induce false detection of modified detached claims because the algorithms in the COSE registry are assumed to be of sufficient cryptographic strength.

### **9.6. Verification Keys**

In all cases there must be some way that the verification key is itself verified or determined to be trustworthy. The key identification itself is never enough. This will always be by some out-of-band mechanism that is not described here. For example, the verifier may be configured with a root certificate or a master key by the verifier system administrator.

Often an X.509 certificate or an endorsement carries more than just the verification key. For example, an X.509 certificate might have key usage constraints, and an endorsement might have reference values. When this is the case, the key identifier must be either a protected header or in the payload, such that it is cryptographically bound to the EAT. This is in line with the requirements in section 6 on Key Identification in JSON Web Signature [[RFC7515](#)].

## **10. IANA Considerations**

### **10.1. Reuse of CBOR and JSON Web Token (CWT and JWT) Claims Registries**

Claims defined for EAT are compatible with those of CWT and JWT so the CWT and JWT Claims Registries, [[IANA.CWT.Claims](#)] and [[IANA.JWT.Claims](#)], are re-used. No new IANA registry is created.

All EAT claims defined in this document are placed in both registries. All new EAT claims defined subsequently should be placed in both registries.

[Appendix E](#) describes some considerations when defining new claims.

## 10.2. CWT and JWT Claims Registered by This Document

This specification adds the following values to the "JSON Web Token Claims" registry established by [RFC7519] and the "CBOR Web Token Claims Registry" established by [RFC8392]. Each entry below is an addition to both registries.

The "Claim Description", "Change Controller" and "Specification Documents" are common and equivalent for the JWT and CWT registries. The "Claim Key" and "Claim Value Type(s)" are for the CWT registry only. The "Claim Name" is as defined for the CWT registry, not the JWT registry. The "JWT Claim Name" is equivalent to the "Claim Name" in the JWT registry.

IANA is requested to register the following claims. The "Claim Value Type(s)" here all name CDDL definitions and are only for the CWT registry.

RFC editor: please see instructions in followg paragraph and remove for final publication

RFC Editor: Please make the following adjustments and remove this paragraph. Replace "**this document**" with this RFC number. In the following, the claims with "Claim Key: TBD" need to be assigned a value in the Specification Required Range, preferably starting around 267. Those below already with a Claim Key number were given early assignment. No change is requested for them except for Claim Key 262. Claim 262 should be renamed from "secboot" to "oemboot" in the JWT registry and its description changed in both the CWT and JWT registries.

\*Claim Name: Nonce

\*Claim Description: Nonce

\*JWT Claim Name: "eat\_nonce"

\*Claim Key: 10

\*Claim Value Type(s): bstr or array

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: UEID

\*Claim Description: The Universal Entity ID

\*JWT Claim Name: "ueid"

\*CWT Claim Key: 256

\*Claim Value Type(s): bstr

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: SUEIDS

\*Claim Description: Semi-permanent UEIDs

\*JWT Claim Name: "sueids"

\*CWT Claim Key: 257

\*Claim Value Type(s): map

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Hardware OEM ID

\*Claim Description: Hardware OEM ID

\*JWT Claim Name: "oemid"

\*Claim Key: 258

\*Claim Value Type(s): bstr or int

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Hardware Model

\*Claim Description: Model identifier for hardware

\*JWT Claim Name: "hwmodel"

\*Claim Key: 259

\*Claim Value Type(s): bstr

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Hardware Version

\*Claim Description: Hardware Version Identifier

\*JWT Claim Name: "hwversion"

\*Claim Key: 260

\*Claim Value Type(s): array

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: OEM Authorized Boot

\*Claim Description: Indicates whether the software booted was OEM authorized

\*JWT Claim Name: "oemboot"

\*Claim Key: 262

\*Claim Value Type(s): bool

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Debug Status

\*Claim Description: Indicates status of debug facilities

\*JWT Claim Name: "dbgstat"

\*Claim Key: 263

\*Claim Value Type(s): uint

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Location

\*Claim Description: The geographic location

\*JWT Claim Name: "location"

\*Claim Key: 264

\*Claim Value Type(s): map

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: EAT Profile

\*Claim Description: Indicates the EAT profile followed

\*JWT Claim Name: "eat\_profile"

\*Claim Key: 265

\*Claim Value Type(s): uri or oid

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Submodules Section

\*Claim Description: The section containing submodules

\*JWT Claim Name: "submods"

\*Claim Key: 266

\*Claim Value Type(s): map

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Uptime

\*Claim Description: Uptime

\*JWT Claim Name: "uptime"

\*Claim Key: 261

\*Claim Value Type(s): uint

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Boot Count

\*Claim Description: The number times the entity or submodule has been booted

\*JWT Claim Name: "bootcount"

\*Claim Key: 267

\*Claim Value Type(s): uint

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Boot Seed

\*Claim Description: Identifies a boot cycle

\*JWT Claim Name: "bootseed"

\*Claim Key: 268

\*Claim Value Type(s): bstr

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: DLOAs

\*Claim Description: Certifications received as Digital Letters of Approval

\*JWT Claim Name: "dloas"

\*Claim Key: 269

\*Claim Value Type(s): array

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Software Name

\*Claim Description: The name of the software running in the entity

\*JWT Claim Name: "swname"

\*Claim Key: 270

\*Claim Value Type(s): tstr

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Software Version

\*Claim Description: The version of software running in the entity

\*JWT Claim Name: "swversion"

\*Claim Key: 271

\*Claim Value Type(s): array

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Software Manifests

\*Claim Description: Manifests describing the software installed on the entity

\*JWT Claim Name: "manifests"

\*Claim Key: 272

\*Claim Value Type(s): array

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Measurements

\*Claim Description: Measurements of the software, memory configuration and such on the entity

\*JWT Claim Name: "measurements"

\*Claim Key: 273

\*Claim Value Type(s): array

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Software Measurement Results

\*Claim Description: The results of comparing software measurements to reference values



\*JWT Claim Name: "measres"

\*Claim Key: 274

\*Claim Value Type(s): array

\*Change Controller: IETF

\*Specification Document(s): **this document**

\*Claim Name: Intended Use

\*Claim Description: Indicates intended use of the EAT

\*JWT Claim Name: "intuse"

\*Claim Key: 275

\*Claim Value Type(s): uint

\*Change Controller: IETF

\*Specification Document(s): **this document**

### 10.3. UEID URN Registered by this Document

IANA is requested to register the following new subtypes in the "DEV URN Subtypes" registry under "Device Identification". See [[RFC9039](#)].

Subtype	Description	Reference
ueid	Universal Entity Identifier	This document
sueid	Semi-permanent Universal Entity Identifier	This document

Table 3: UEID URN Registration

ABNF for these two URNs is as follows where b64ueid is the base64url-encoded binary byte-string for the UEID or SUEID:

```
body =/ ueidbody
ueidbody = %s"ueid:" b64ueid
```

### 10.4. CBOR Tag for Detached EAT Bundle Registered by this Document

In the registry [[IANA.cbor-tags](#)], IANA is requested to allocate the following tag from the Specification Required space, with the present document as the specification reference.

Tag	Data Items	Semantics
602	array	Detached EAT Bundle <a href="#">Section 5</a>

Table 4: Detached EAT Bundle Tag Registration

## 11. References

### 11.1. Normative References

- [DLOA] "Digital Letter of Approval", November 2015, <[https://globalplatform.org/wp-content/uploads/2015/12/GPC\\_DigitalLetterOfApproval\\_v1.0.pdf](https://globalplatform.org/wp-content/uploads/2015/12/GPC_DigitalLetterOfApproval_v1.0.pdf)>.
- [IANA.cbor-tags] IANA, "Concise Binary Object Representation (CBOR) Tags", <<https://www.iana.org/assignments/cbor-tags>>.
- [IANA.COSE.Algorithms] IANA, "CBOR Object Signing and Encryption (COSE)", <<https://www.iana.org/assignments/cose>>.
- [IANA.CWT.Claims] IANA, "CBOR Web Token (CWT) Claims", <<https://www.iana.org/assignments/cwt>>.
- [IANA.JWT.Claims] IANA, "JSON Web Token (JWT)", <<https://www.iana.org/assignments/jwt>>.
- [PEN] "Private Enterprise Number (PEN) Request", n.d., <<https://pen.iana.org/pen/PenApplication.page>>.
- [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>>.
- [RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <<https://www.rfc-editor.org/info/rfc3986>>.
- [RFC4517] Legg, S., Ed., "Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules", RFC 4517, DOI 10.17487/RFC4517, June 2006, <<https://www.rfc-editor.org/info/rfc4517>>.
- [RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <<https://www.rfc-editor.org/info/rfc4648>>.
- [RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/

RFC7252, June 2014, <<https://www.rfc-editor.org/info/rfc7252>>.

- [RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <<https://www.rfc-editor.org/info/rfc7515>>.
- [RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <<https://www.rfc-editor.org/info/rfc7519>>.
- [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>>.
- [RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <<https://www.rfc-editor.org/info/rfc8259>>.
- [RFC8392] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <<https://www.rfc-editor.org/info/rfc8392>>.
- [RFC8610] Birkholz, H., Viganò, 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>>.
- [RFC8792] Watsen, K., Auerswald, E., Farrel, A., and Q. Wu, "Handling Long Lines in Content of Internet-Drafts and RFCs", RFC 8792, DOI 10.17487/RFC8792, June 2020, <<https://www.rfc-editor.org/info/rfc8792>>.
- [RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <<https://www.rfc-editor.org/info/rfc8949>>.
- [RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <<https://www.rfc-editor.org/info/rfc9052>>.
- [RFC9090] Bormann, C., "Concise Binary Object Representation (CBOR) Tags for Object Identifiers", RFC 9090, DOI 10.17487/RFC9090, July 2021, <<https://www.rfc-editor.org/info/rfc9090>>.

- [RFC9165] Bormann, C., "Additional Control Operators for the Concise Data Definition Language (CDDL)", RFC 9165, DOI 10.17487/RFC9165, December 2021, <<https://www.rfc-editor.org/info/rfc9165>>.
- [RFC9334] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote ATtestation procedures (RATS) Architecture", RFC 9334, DOI 10.17487/RFC9334, January 2023, <<https://www.rfc-editor.org/info/rfc9334>>.
- [RFC9393] Birkholz, H., Fitzgerald-McKay, J., Schmidt, C., and D. Waltermire, "Concise Software Identification Tags", RFC 9393, DOI 10.17487/RFC9393, June 2023, <<https://www.rfc-editor.org/info/rfc9393>>.
- [ThreeGPP.IMEI] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification", 2019, <<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729>>.
- [WGS84] National Geospatial-Intelligence Agency (NGA), "WORLD GEODETIC SYSTEM 1984, NGA.STND.0036\_1.0.0\_WGS84", 8 July 2014, <<https://earth-info.nga.mil/php/download.php?file=coord-wgs84>>.

## 11.2. Informative References

- [BirthdayAttack] "Birthday attack", <[https://en.wikipedia.org/wiki/Birthday\\_attack](https://en.wikipedia.org/wiki/Birthday_attack)>.
- [CBOR.Cert.Draft] Mattsson, J. P., Selander, G., Raza, S., Höglund, J., and M. Furuheid, "CBOR Encoded X.509 Certificates (C509 Certificates)", Work in Progress, Internet-Draft, draft-ietf-cose-cbor-encoded-cert-09, 4 March 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-cose-cbor-encoded-cert-09>>.
- [COSE.X509.Draft] Schaad, J., "CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates", Work in Progress, Internet-Draft, draft-ietf-cose-x509-09, 13 October 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-cose-x509-09>>.
- [EAT.media-types] Lundblade, L., Birkholz, H., and T. Fossati, "EAT Media Types", Work in Progress, Internet-Draft, draft-ietf-rats-eat-media-type-07, 2 April 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-rats-eat-media-type-07>>.

- [IEEE-RA] "IEEE Registration Authority", <<https://standards.ieee.org/products-services/regauth/index.html>>.
- [IEEE.802-2001] "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture", IEEE standard, DOI 10.1109/ieeestd.2014.6847097, July 2014, <<https://doi.org/10.1109/ieeestd.2014.6847097>>.
- [IEEE.802.1AR] "IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity", IEEE standard, DOI 10.1109/ieeestd.2018.8423794, July 2018, <<https://doi.org/10.1109/ieeestd.2018.8423794>>.
- [JTAG] "IEEE Standard for Reduced-Pin and Enhanced-Functionality Test Access Port and Boundary-Scan Architecture", February 2010, <<https://ieeexplore.ieee.org/document/5412866>>.
- [OUI.Guide] "Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)", August 2017, <<https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/eui.pdf>>.
- [OUI.Lookup] "IEEE Registration Authority Assignments", <<https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries>>.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <<https://www.rfc-editor.org/info/rfc4949>>.
- [RFC9039] Arkko, J., Jennings, C., and Z. Shelby, "Uniform Resource Names for Device Identifiers", RFC 9039, DOI 10.17487/RFC9039, June 2021, <<https://www.rfc-editor.org/info/rfc9039>>.
- [RFC9562] Davis, K., Peabody, B., and P. Leach, "Universally Unique Identifiers (UUIDs)", RFC 9562, DOI 10.17487/RFC9562, May 2024, <<https://www.rfc-editor.org/info/rfc9562>>.
- [UCCS] Birkholz, H., O'Donoghue, J., Cam-Winget, N., and C. Bormann, "A CBOR Tag for Unprotected CWT Claims Sets", Work in Progress, Internet-Draft, draft-ietf-rats-uccs-09, 4 March 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-rats-uccs-09>>.
- [W3C.GeoLoc] Popescu, A., Ed., "Geolocation API Specification", W3C REC REC-geolocation-API-20131024, W3C REC-geolocation-

## **Appendix A. Examples**

Most examples are shown as just a Claims-Set that would be a payload for a CWT, JWT, detached EAT bundle or future token types. The signing is left off so the Claims-Set is easier to see. Some examples of signed tokens are also given.

RFC Editor: When the IANA values are permanently assigned, please contact the authors so the examples can be regenerated. Regeneration is required because IANA-assigned values are inside hex and based-64 encoded data and some of these are signed.

### **A.1. Claims Set Examples**

#### **A.1.1. Simple TEE Attestation**

This is a simple attestation of a TEE that includes a manifest that is a payload CoSWID to describe the TEE's software.

```

/ This is an EAT payload that describes a simple TEE. /

{
  / eat_nonce /      10: h'48df7b172d70b5a18935d0460a73dd71',
  / oemboot /       262: true,
  / dbgstat /      263: 2, / disabled-since-boot /
  / manifests /    272: [
                        [
                          258, / CoAP Content ID for CoSWID /

                          / This is byte-string wrapped /
                          / payload CoSWID. It gives the TEE /
                          / software name, the version and /
                          / the name of the file it is in. /
                          / {0: "3a24", /
                          / 12: 1, /
                          / 1: "Acme TEE OS", /
                          / 13: "3.1.4", /
                          / 2: [{31: "Acme TEE OS", 33: 1}, /
                          /      {31: "Acme TEE OS", 33: 2}], /
                          / 6: { /
                          /   17: { /
                          /     24: "acme_tee_3.exe" /
                          /   } /
                          / } /
                          / } /
                          / } /
                        h' a60064336132340c01016b
                          41636d6520544545204f530d65332e31
                          2e340282a2181f6b41636d6520544545
                          204f53182101a2181f6b41636d652054
                          4545204f5318210206a111a118186e61
                          636d655f7465655f332e657865'
                        ]
                      ]
}

```

```
/ A payload CoSWID created by the SW vendor. All this really does /
/ is name the TEE SW, its version and lists the one file that /
/ makes up the TEE. /
```

```
1398229316({
  / Unique CoSWID ID /      0: "3a24",
  / tag-version /          12: 1,
  / software-name /        1: "Acme TEE OS",
  / software-version /     13: "3.1.4",
  / entity /               2: [
    {
      / entity-name /      31: "Acme TEE OS",
      / role /              33: 1 / tag-creator /
    },
    {
      / entity-name /      31: "Acme TEE OS",
      / role /              33: 2 / software-creator /
    }
  ],
  / payload /              6: {
    / ...file /            17: {
      / ...fs-name /       24: "acme_tee_3.exe"
    }
  }
})
```



### A.1.2. Submodules for Board and Device

```
/ This example shows use of submodules to give information /
/ about the chip, board and overall device. /
/ /
/ The main attestation is associated with the chip with the /
/ CPU and running the main OS. It is what has the keys and /
/ produces the token. /
/ /
/ The board is made by a different vendor than the chip. /
/ Perhaps it is some generic IoT board. /
/ /
/ The device is some specific appliance that is made by a /
/ different vendor than either the chip or the board. /
/ /
/ Here the board and device submodules aren't the typical /
/ target environments as described by the RATS architecture /
/ document, but they are a valid use of submodules. /

{
  / eat_nonce /      10: h'e253cabedc9eec24ac4e25bcbeaf7765',
  / ueid /          256: h'0198f50a4ff6c05861c8860d13a638ea',
  / oemid /         258: h'894823', / IEEE OUI format OEM ID /
  / hwmodel /      259: h'549dcecc8b987c737b44e40f7c635ce8'
                    / Hash of chip model name /,
  / hwversion /    260: ["1.3.4", 1], / Multipartnumeric /
  / swname /       270: "Acme OS",
  / swversion /    271: ["3.5.5", 1],
  / oemboot /      262: true,
  / dbgstat /      263: 3, / permanent-disable /
  / timestamp (iat) / 6: 1526542894,
  / submods / 266: {
    / A submodule to hold some claims about the circuit board /
    "board" : {
      / oemid /      258: h'9bef8787eba13e2c8f6e7cb4b1f4619a',
      / hwmodel /    259: h'ee80f5a66c1fb9742999a8fdab930893'
                    / Hash of board module name /,
      / hwversion / 260: ["2.0a", 2] / multipartnumeric+suffix /
    },

    / A submodule to hold claims about the overall device /
    "device" : {
      / oemid /      258: 61234, / PEN Format OEM ID /
      / hwversion / 260: ["4.0", 1] / Multipartnumeric /
    }
  }
}
```

### A.1.3. EAT Produced by Attestation Hardware Block

```
/ This is an example of a token produced by a HW block           /
/ purpose-built for attestation. Only the nonce claim changes   /
/ from one attestation to the next as the rest either come     /
/ directly from the hardware or from one-time-programmable memory /
/ (e.g. a fuse). 47 bytes encoded in CBOR (8 byte nonce, 16 byte /
/ UEID). /

{
  / eat_nonce /          10: h'd79b964ddd5471c1393c8888',
  / ueid /              256: h'0198f50a4ff6c05861c8860d13a638ea',
  / oemid /             258: 64242, / Private Enterprise Number /
  / oemboot /           262: true,
  / dbgstat /           263: 3, / disabled-permanently /
  / hwversion /         260: [ "3.1", 1 ] / Type is multipartnumeric /
}
```

#### A.1.4. Key / Key Store Attestation

```

/ This is an attestation of a public key and the key store /
/ implementation that protects and manages it. The key store /
/ implementation is in a security-oriented execution /
/ environment separate from the high-level OS (HLOS), for /
/ example a Trusted Execution Environment (TEE). The key store /
/ is the Attester. /
/ /
/ There is some attestation of the high-level OS, just version /
/ and boot & debug status. It is a Claims-Set submodule because /
/ it has lower security level than the key store. The key /
/ store's implementation has access to info about the HLOS, so /
/ it is able to include it. /
/ /
/ A key and an indication of the user authentication given to /
/ allow access to the key is given. The labels for these are /
/ in the private space since this is just a hypothetical /
/ example, not part of a standard protocol. /

{
  / eat_nonce /      10: h'99b67438dba40743266f70bf75feb1026d5134
                    97a229bfe8',
  / oemboot /       262: true,
  / dbgstat /       263: 2, / disabled-since-boot /
  / manifests /     272: [
                    [ 258, / CoAP Content ID. /
                    h'a600683762623334383766
                    0c000169436172626f6e6974650d6331
                    2e320e0102a2181f75496e6475737472
                    69616c204175746f6d6174696f6e1821
                    02'
                    ]
                    / Above is an encoded CoSWID /
                    / with the following data /
                    / SW Name: "Carbonite" /
                    / SW Vers: "1.2" /
                    / SW Creator: /
                    / "Industrial Automation" /
                    ],
  / exp /           4: 1634324274, / 2021-10-15T18:57:54Z /
  / iat /           6: 1634317080, / 2021-10-15T16:58:00Z /
                    -80000 : "fingerprint",
                    -80001 : { / The key -- A COSE_Key /
                    / kty /      1: 2, / EC2, elliptic curve with x & y /
                    / kid /      2: h'36675c206f96236c3f51f54637b94ced',
                    / curve /    -1: 2, / curve is P-256 /
                    / x-coord /  -2: h'65eda5a12577c2bae829437fe338701a
                    10aaa375e1bb5b5de108de439c08551d',
                    / y-coord /  -3: h'1e52ed75701163f7f9e40ddf9f341b3d

```

```

c9ba860af7e0ca7ca7e9eecd0084d19c'
},
/ submods /      266 : {
                    "HLOS" : { / submod for high-level OS /
/ eat_nonce /    10: h'8b0b28782a23d3f6',
/ oemboot /      262: true,
/ manifests /    272: [
                    [ 258, / CoAP Content ID. /
                      h'a600687337
                      6537346b78380c000168
                      44726f6964204f530d65
                      52322e44320e0302a218
                      1F75496E647573747269
                      616c204175746f6d6174
                      696f6e182102'
                    ]
                    / Above is an encoded CoSWID /
                    / with the following data: /
                    /   SW Name: "Droid OS" /
                    /   SW Vers: "R2.D2" /
                    /   SW Creator: /
                    /     "Industrial Automation"/
                    ]
                }
            }
}

```

#### A.1.5. Software Measurements of an IoT Device

This is a simple token that might be for an IoT device. It includes CoSWID format measurements of the SW. The CoSWID is in byte-string wrapped in the token and also shown in diagnostic form.

```
/ This EAT payload is for an IoT device with a TEE. The attestation /
/ is produced by the TEE. There is a submodule for the IoT OS (the /
/ main OS of the IoT device that is not as secure as the TEE). The /
/ submodule contains claims for the IoT OS. The TEE also measures /
/ the IoT OS and puts the measurements in the submodule. /
```

```
{
  / eat_nonce / 10: h'5e19fba4483c7896',
  / oemboot / 262: true,
  / dbgstat / 263: 2, / disabled-since-boot /
  / oemid / 258: h'8945ad', / IEEE CID based /
  / ueid / 256: h'0198f50a4ff6c05861c8860d13a638ea',
  / submods / 266: {
    "OS" : {
      / oemboot / 262: true,
      / dbgstat / 263: 2, / disabled-since-boot /
      / measurements / 273: [
        [
          258, / CoAP Content ID /

          / This is a byte-string wrapped /
          / evidence CoSWID. It has /
          / hashes of the main files of /
          / the IoT OS. /
          h'a600663463613234350c
          17016d41636d6520522d496f542d4f
          530d65332e312e3402a2181f724163
          6d6520426173652041747465737465
          7218210103a11183a318187161636d
          655f725f696f745f6f732e65786514
          1a0044b349078201582005f6b327c1
          73b4192bd2c3ec248a292215eab456
          611bf7a783e25c1782479905a31818
          6d7265736f75726365732e72736314
          1a000c38b10782015820c142b9aba4
          280c4bb8c75f716a43c99526694caa
          be529571f5569bb7dc542f98a31818
          6a636f6d6d6f6e2e6c6962141a0023
          3d3b0782015820a6a9dcdfb3884da5
          f884e4e1e8e8629958c2dbc7027414
          43a913e34de9333be6'
        ]
      ]
    }
  }
}
```

/ An evidence CoSWID created for the "Acme R-IoT-OS" created by /  
/ the "Acme Base Attester" (both fictitious names). It provides /  
/ measurements of the SW (other than the attester SW) on the /  
/ device. /

```
1398229316({
  / Unique CoSWID ID /      0: "4ca245",
  / tag-version /          12: 23, / Attester-maintained counter /
  / software-name /        1: "Acme R-IoT-OS",
  / software-version /     13: "3.1.4",
  / entity /               2: {
    / entity-name /        31: "Acme Base Attester",
    / role /                33: 1 / tag-creator /
  },
  / evidence /             3: {
    / ...file /            17: [
      {
        / ...fs-name /      24: "acme_r_iot_os.exe",
        / ...size /         20: 4502345,
        / ...hash /         7: [
          1, / SHA-256 /
          h'05f6b327c173b419
          2bd2c3ec248a2922
          15eab456611bf7a7
          83e25c1782479905'
        ]
      },
      {
        / ...fs-name /      24: "resources.rsc",
        / ...size /         20: 800945,
        / ...hash /         7: [
          1, / SHA-256 /
          h'c142b9aba4280c4b
          b8c75f716a43c995
          26694caabe529571
          f5569bb7dc542f98'
        ]
      },
      {
        / ...fs-name /      24: "common.lib",
        / ...size /         20: 2309435,
        / ...hash /         7: [
          1, / SHA-256 /
          h'a6a9dcdffb3884da5
          f884e4e1e8e86299
          58c2dbc702741443
          a913e34de9333be6'
        ]
      }
    ]
  }
}
```

```
    ]
  }
})
```

#### A.1.6. Attestation Results in JSON

This is a JSON-encoded payload that might be the output of a verifier that evaluated the IoT Attestation example immediately above.

This particular verifier knows enough about the TEE attester to be able to pass claims like debug status directly through to the relying party. The verifier also knows the reference values for the measured software components and is able to check them. It informs the relying party that they were correct in the "measres" claim. "Trustus Verifications" is the name of the services that verifies the software component measurements.

```
{
  "eat_nonce": "jkd8KL-8xQk",
  "oemboot": true,
  "dbgstat": "disabled-since-boot",
  "oemid": "iUWt",
  "ueid": "AZj1Ck_2wFhhyIYNE6Y4",
  "swname": "Acme R-IoT-OS",
  "swversion": [
    "3.1.4"
  ],
  "measres": [
    [
      "Trustus Measurements",
      [
        [
          "all",
          "success"
        ]
      ]
    ]
  ]
}
```

#### A.1.7. JSON-encoded Token with Submodules

This example has its lines wrapped per [\[RFC8792\]](#).



```

{
  "eat_nonce": "lI-IYNE6Rj60",
  "ueid": "AJj1Ck_2wFhhyIYNE6Y46g==",
  "secboot": true,
  "dbgstat": "disabled-permanently",
  "iat": 1526542894,
  "submods": {
    "Android App Foo": {
      "swname": "Foo.app"
    },
    "Secure Element Eat": [
      "CBOR",
      "2D3ShEOhASagWGaoCkiUj4hg0TpGPhkBAFABmPUKT_bAWGHIhg0TpjjqGQ\
ECGfryGQEFBBkBBvUZAQcDGQEEgmMzLjEBGQEKoWNURUWCL1gg5c-V_ST6txRGdC3VjU\
Pa4XjLX-K5QpGpKRCC_8JjWgtYQPaQyw0IZ3-mJKN3X9fLx0hAnsmBa-MvpHRz0w-Ywn\
-67bvJljuctezAPD41s6_At7NbSV3qwJlxIuqGfwe41es="
    ],
    "Linux Android": {
      "swname": "Android"
    },
    "Subsystem J": [
      "JWT",
      "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJKLUF0dGVzd\
GVyIiwiaWF0IjoxNjUxNzY4MjY4LjleHAiOiM1bGwsImF1ZCI6IiIsInN1YiI6IiJ9.\
gjw4nFMhLpJUuPXvMPzK1GMjhyJq2vWXg1416XKszwQ"
    ]
  }
}

```

## A.2. Signed Token Examples

### A.2.1. Basic CWT Example

This is a simple CWT-format token signed with the ECDSA algorithm.

```
/ This is a full CWT-format token. The payload is the /
/ attestation hardware block above. The main structure /
/ visible is that of the COSE_Sign1. /
```

```
61( 18( [
  h'A10126', / protected headers /
  {}, / empty unprotected headers /
  h'A60A4CD79B964DDD5471C1393C88881901005001
  98F50A4FF6C05861C8860D13A638EA19010219FA
  F2190106F5190107031901048263332E3101', / payload /
  h'9B9B2F5E470000F6A20C8A4157B5763FC45BE759
  9A5334028517768C21AFFB845A56AB557E0C8973
  A07417391243A79C478562D285612E292C622162
  AB233787' / signature /
] ) )
```

### A.2.2. CBOR-encoded Detached EAT Bundle

In this detached EAT bundle, the main token is produced by a HW attestation block. The detached Claims-Set is produced by a TEE and is largely identical to the Simple TEE examples above. The TEE digests its Claims-Set and feeds that digest to the HW block.

In a better example the attestation produced by the HW block would be a CWT and thus signed and secured by the HW block. Since the signature covers the digest from the TEE that Claims-Set is also secured.

The detached EAT bundle itself can be assembled by untrusted software.

/ This is a detached EAT bundle tag. /

602([

/ First part is a full EAT token with claims like nonce and /  
/ UEID. Most importantly, it includes a submodule that is a /  
/ detached digest which is the hash of the "TEE" claims set /  
/ in the next section. The COSE payload follows: /

/ { /

/ 10: h'948F8860D13A463E', /

/ 256: h'0198F50A4FF6C05861C8860D13A638EA', /

/ 258: 64242, /

/ 262: true, /

/ 263: 3, /

/ 260: ["3.1", 1], /

/ 266: { /

/ "TEE": [ /

/ -16, /

/ h'8DEF652F47000710D9F466A4C666E209 /

/ DD74F927A1CEA352B03143E188838ABE' /

/ ] /

/ } /

/ } /

h'D83DD28443A10126A05866A80A48948F8860D13A463E1901  
00500198F50A4FF6C05861C8860D13A638EA19010219FAF2  
19010504190106F5190107031901048263332E310119010A  
A163544545822F58208DEF652F47000710D9F466A4C666E2  
09DD74F927A1CEA352B03143E188838ABE5840F690CB0388  
677FA624A3775FD7CBC4E8409EC9816BE32FA474733B0F98  
C27FBAEDBBC9963B9CB5ECC03C3E35B3AFC0B7B35B495DEA  
C0997122EA867F07B8D5EB',

{

/ A CBOR-encoded byte-string wrapped EAT claims-set. It /  
/ contains claims suitable for a TEE. /

"TEE" : h'a40a48948f8860d13a463e190106f519010702  
190111818218795858a60064336132340c0101  
6b41636d6520544545204f530d65332e312e34  
0282a2181f6b41636d6520544545204f531821  
01a2181f6b41636d6520544545204f53182102  
06a111a118186e61636d655f7465655f332e65  
7865'

}

])

```

/ This example contains submodule that is a detached digest, /
/ which is the hash of a Claims-Set convey outside this token. /
/ Other than that is is the other example of a token from an /
/ attestation HW block. /

{
  / eat_nonce /      10: h'3515744961254b41a6cf9c02',
  / ueid /           256: h'0198f50a4ff6c05861c8860d13a638ea',
  / oemid /          258: 64242, / Private Enterprise Number /
  / oemboot /        262: true,
  / dbgstat /        263: 3, / disabled-permanently /
  / hwversion /      260: [ "3.1", 1 ], / multipartnumeric /
  / submods/         266: {
                        "TEE": [ / detached digest submod /
                                  -16, / SHA-256 /
                                  h'e5cf95fd24fab7144674
                                  2dd58d43dae178e55fe2
                                  b94291a9291082ffc263
                                  5a0b'
                                ]
                      }
}

```

### A.2.3. JSON-encoded Detached EAT Bundle

In this bundle there are two detached Claims-Sets, "Audio Subsystem" and "Graphics Subsystem". The JWT at the start of the bundle has detached signature submodules with hashes that cover these two Claims-Sets. The JWT itself is protected using HMAC with a key of "xxxxxx".

This example has its lines wrapped per [\[RFC8792\]](#).

```
[
  [
    "JWT",
    "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJYXRFbm9uY2UiOiJ5dT\
c2Tk44SXVWnmUiLCJzdWJtb2RzIjp7IkF1ZGlvIFN1YnN5c3RlbSI6WyJESUdFU1QiLF\
siU0hBLTI1NiIsIkZSRW4yVlR3aTk5cWNNRVFzYmxtTVFnM2I1b2ZYUG50M1BJYW5CME\
5RT3MiXV0sIkdyYXBoaWNzIFN1YnN5c3RlbSI6WyJESUdFU1QiLFsiU0hBLTI1NiIsIk\
52M3NqUVU3Q1Z0RFRka0RTUlhWcFZDNUNMVFBwVQWWhTLUhoVlZWXMmXV19fQ.FYs\
7R-TKhgAk85NyCOPQlbtGGjFM_3chnhBE0uM6qCo"
  ],
  {
    "Audio Subsystem" : "ewogICAgImVhdF9ub25jZSI6ICJsSStJWU5FNlJ\
qNk8iLAogICAgInVlawQi0iAiQWROSlU0b1lYdFVwQStIeDNqQTcvRFEiCiAgICAib2V\
tawQi0iAiaVVXdCIsCiAgICAib2VtYm9vdCI6IHRYdWUsIAogICAgInN3bmFtZSI6ICJ\
BdWRpbyBQcm9jZXRzIjogT1MiCn0K",
    "Graphics Subsystem" : "ewogICAgImVhdF9ub25jZSI6ICJZWStJWU5F\
NlJqNk8iLAogICAgInVlawQi0iAiQWVUTUlRQ1NVMnhwQmtVdGlnHU3bGUiCiAgIC\
ib2VtawQi0iA3NTAwMwKICAgICJvZW1ib290IjogdHJ1ZSwgCiAgICAic3duYW1lIjog\
IkdyYXBoaWNzIE9TIgp9Cg"
  }
]
```

**Appendix B. UEID Design Rationale**

**B.1. Collision Probability**

This calculation is to determine the probability of a collision of type 0x01 UEIDs given the total possible entity population and the number of entities in a particular entity management database.

Three different sized databases are considered. The number of devices per person roughly models non-personal devices such as traffic lights, devices in stores they shop in, facilities they work in and so on, even considering individual light bulbs. A device may have individually attested subsystems, for example parts of a car or a mobile phone. It is assumed that the largest database will have at most 10% of the world's population of devices. Note that databases that handle more than a trillion records exist today.

The trillion-record database size models an easy-to-imagine reality over the next decades. The quadrillion-record database is roughly at the limit of what is imaginable and should probably be accommodated. The 100 quadrillion database is highly speculative perhaps involving nanorobots for every person, livestock animal and domesticated bird. It is included to round out the analysis.

Note that the items counted here certainly do not have IP address and are not individually connected to the network. They may be connected

to internal buses, via serial links, Bluetooth and so on. This is not the same problem as sizing IP addresses.

People	Devices / Person	Subsystems / Device	Database Portion	Database Size
10 billion	100	10	10%	trillion (10 <sup>12</sup> )
10 billion	100,000	10	10%	quadrillion (10 <sup>15</sup> )
100 billion	1,000,000	10	10%	100 quadrillion (10 <sup>17</sup> )

Table 5: Entity Database Size Examples

This is conceptually similar to the Birthday Problem where m is the number of possible birthdays, always 365, and k is the number of people. It is also conceptually similar to the Birthday Attack where collisions of the output of hash functions are considered.

The proper formula for the collision calculation is

$$p = 1 - e^{-k^2/(2n)}$$

- p Collision Probability
- n Total possible population
- k Actual population

However, for the very large values involved here, this formula requires floating point precision higher than commonly available in calculators and software so this simple approximation is used. See [[BirthdayAttack](#)].

$$p = k^2 / 2n$$

For this calculation:

- p Collision Probability
- n Total population based on number of bits in UEID
- k Population in a database

Database Size	128-bit UEID	192-bit UEID	256-bit UEID
trillion (10 <sup>12</sup> )	2 * 10 <sup>-15</sup>	8 * 10 <sup>-35</sup>	5 * 10 <sup>-55</sup>
quadrillion (10 <sup>15</sup> )	2 * 10 <sup>-09</sup>	8 * 10 <sup>-29</sup>	5 * 10 <sup>-49</sup>
100 quadrillion (10 <sup>17</sup> )	2 * 10 <sup>-05</sup>	8 * 10 <sup>-25</sup>	5 * 10 <sup>-45</sup>

Table 6: UEID Size Options

Next, to calculate the probability of a collision occurring in one year's operation of a database, it is assumed that the database size

is in a steady state and that 10% of the database changes per year. For example, a trillion record database would have 100 billion states per year. Each of those states has the above calculated probability of a collision.

This assumption is a worst-case since it assumes that each state of the database is completely independent from the previous state. In reality this is unlikely as state changes will be the addition or deletion of a few records.

The following tables gives the time interval until there is a probability of a collision based on there being one tenth the number of states per year as the number of records in the database.

$$t = 1 / ((k / 10) * p)$$

t Time until a collision

p Collision probability for UEID size

k Database size

Database Size	128-bit UEID	192-bit UEID	256-bit UEID
trillion (10 <sup>12</sup> )	60,000 years	10 <sup>24</sup> years	10 <sup>44</sup> years
quadrillion (10 <sup>15</sup> )	8 seconds	10 <sup>14</sup> years	10 <sup>34</sup> years
100 quadrillion (10 <sup>17</sup> )	8 microseconds	10 <sup>11</sup> years	10 <sup>31</sup> years

Table 7: UEID Collision Probability

Clearly, 128 bits is enough for the near future thus the requirement that type 0x01 UEIDs be a minimum of 128 bits.

There is no requirement for 256 bits today as quadrillion-record databases are not expected in the near future and because this time-to-collision calculation is a very worst case. A future update of the standard may increase the requirement to 256 bits, so there is a requirement that implementations be able to receive 256-bit UEIDs.

## B.2. No Use of UUID

A UEID is not a Universally Unique Identifier (UUID) [[RFC9562](#)] by conscious choice for the following reasons.

UUIDs are limited to 128 bits which may not be enough for some future use cases.

Today, cryptographic-quality random numbers are available from common CPUs and hardware. This hardware was introduced between 2010 and 2015. Operating systems and cryptographic libraries give access to this hardware. Consequently, there is little need for implementations to construct such random values from multiple sources on their own.

Version 4 UUIDs do allow for use of such cryptographic-quality random numbers, but do so by mapping into the overall UUID structure of time and clock values. This structure is of no value here yet adds complexity. It also slightly reduces the number of actual bits with entropy.

The design of UUID accommodates the construction of a unique identifier by combination of several identifiers that separately do not provide sufficient uniqueness. UEID takes the view that this construction is no longer needed, in particular because cryptographic-quality random number generators are readily available. It takes the view that hardware, software and/or manufacturing process implement UEID in a simple and direct way.

Note also that that a type 2 UEID (EUI/MAC) is only 7 bytes compared to 16 for a UUID.

## **Appendix C. EAT Relation to IEEE.802.1AR Secure Device Identity (DevID)**

This section describes several distinct ways in which an IEEE IDevID [[IEEE.802.1AR](#)] relates to EAT, particularly to UEID and SUEID.

[[IEEE.802.1AR](#)] orients around the definition of an implementation called a "DevID Module." It describes how IDevIDs and LDevIDs are stored, protected and accessed using a DevID Module. A particular level of defense against attack that should be achieved to be a DevID is defined. The intent is that IDevIDs and LDevIDs can be used with any network protocol or message format. In these protocols and message formats the DevID secret is used to sign a nonce or similar to prove the association of the DevID certificates with the device.

By contrast, EAT standardizes a message format that is sent to a relying party, the very thing that is not defined in [[IEEE.802.1AR](#)]. Nor does EAT give details on how keys, data and such are stored protected and accessed. EAT is intended to work with a variety of different on-device implementations ranging from minimal protection of assets to the highest levels of asset protection. It does not define any particular level of defense against attack, instead providing a set of security considerations.

EAT and DevID can be viewed as complimentary when used together or as competing to provide a device identity service.

### **C.1. DevID Used With EAT**

As just described, EAT standardizes a message format and [[IEEE.802.1AR](#)] doesn't. Vice versa, EAT doesn't define a an device implementation, but DevID does.



Hence, EAT can be the message format that a DevID is used with. The DevID secret becomes the attestation key used to sign EATs. The DevID and its certificate chain become the endorsement sent to the verifier.

In this case, the EAT and the DevID are likely to both provide a device identifier (e.g. a serial number). In the EAT it is the UEID (or SUEID). In the DevID (used as an endorsement), it is a device serial number included in the subject field of the DevID certificate. It is probably a good idea in this use for them to be the same serial number or for the UEID to be a hash of the DevID serial number.

## **C.2. How EAT Provides an Equivalent Secure Device Identity**

The UEID, SUEID and other claims like OEM ID are equivalent to the secure device identity put into the subject field of a DevID certificate. These EAT claims can represent all the same fields and values that can be put in a DevID certificate subject. EAT explicitly and carefully defines a variety of useful claims.

EAT secures the conveyance of these claims by having them signed on the device by the attestation key when the EAT is generated. EAT also signs the nonce that gives freshness at this time. Since these claims are signed for every EAT generated, they can include things that vary over time like GPS location.

DevID secures the device identity fields by having them signed by the manufacturer of the device sign them into a certificate. That certificate is created once during the manufacturing of the device and never changes so the fields cannot change.

So in one case the signing of the identity happens on the device and the other in a manufacturing facility, but in both cases the signing of the nonce that proves the binding to the actual device happens on the device.

While EAT does not specify how the signing keys, signature process and storage of the identity values should be secured against attack, an EAT implementation may have equal defenses against attack. One reason EAT uses CBOR is because it is simple enough that a basic EAT implementation can be constructed entirely in hardware. This allows EAT to be implemented with the strongest defenses possible.

## **C.3. An X.509 Format EAT**

It is possible to define a way to encode EAT claims in an X.509 certificate. For example, the EAT claims might be mapped to X.509 v3 extensions. It is even possible to stuff a whole CBOR-encoded unsigned EAT token into a X.509 certificate.

If that X.509 certificate is an IDevID or LDevID, this becomes another way to use EAT and DevID together.

Note that the DevID must still be used with an authentication protocol that has a nonce or equivalent. The EAT here is not being used as the protocol to interact with the rely party.

#### C.4. Device Identifier Permanence

In terms of permanence, an IDevID is similar to a UEID in that they do not change over the life of the device. They cease to exist only when the device is destroyed.

An SUEID is similar to an LDevID. They change on device life-cycle events.

[[IEEE.802.1AR](#)] describes much of this permanence as resistant to attacks that seek to change the ID. IDevID permanence can be described this way because [[IEEE.802.1AR](#)] is oriented around the definition of an implementation with a particular level of defense against attack.

EAT is not defined around a particular implementation and must work on a range of devices that have a range of defenses against attack. EAT thus can't be defined permanence in terms of defense against attack. EAT's definition of permanence is in terms of operations and device lifecycle.

#### Appendix D. CDDL for CWT and JWT

[[RFC8392](#)] was published before CDDL was available and thus is specified in prose, not CDDL. Following is CDDL specifying CWT as it is needed to complete this specification. This CDDL also covers the Claims-Set for JWT.

Note that [Section 4.3.1](#) requires that the iat claim be the type ~time-int ([Section 7.2.1](#)), not the type ~time when it is used in an EAT as floating-point values are not allowed for the "iat" claim in EAT.

The COSE-related types in this CDDL are defined in [[RFC9052](#)].

This however is NOT a normative or standard definition of CWT or JWT in CDDL. The prose in CWT and JWT remain the normative definition.

```

; This is replicated from draft-ietf-rats-uccs

Claims-Set = {
    * $$Claims-Set-Claims
    * Claim-Label .feature "extended-claims-label" => any
}
Claim-Label = int / text
string-or-uri = text

$$Claims-Set-Claims // = ( iss-claim-label => string-or-uri )
$$Claims-Set-Claims // = ( sub-claim-label => string-or-uri )
$$Claims-Set-Claims // = ( aud-claim-label => string-or-uri )
$$Claims-Set-Claims // = ( exp-claim-label => ~time )
$$Claims-Set-Claims // = ( nbf-claim-label => ~time )
$$Claims-Set-Claims // = ( iat-claim-label => ~time )
$$Claims-Set-Claims // = ( cti-claim-label => bytes )

iss-claim-label = JC<"iss", 1>
sub-claim-label = JC<"sub", 2>
aud-claim-label = JC<"aud", 3>
exp-claim-label = JC<"exp", 4>
nbf-claim-label = JC<"nbf", 5>
iat-claim-label = JC<"iat", 6>
cti-claim-label = CBOR-ONLY<7> ; jti in JWT: different name and text

JSON-ONLY<J> = J .feature "json"
CBOR-ONLY<C> = C .feature "cbor"

JC<J,C> = JSON-ONLY<J> / CBOR-ONLY<C>

; Same as JC<> but with unwound generic nesting as it seems to cause
; problems. Perhaps this is the nesting problem described in RFC
; 8610.
JC-NEST-SAFE<J,C> = J .feature "json" / C .feature "cbor"

; A JWT message is either a JWS or JWE in compact serialization form
; with the payload a Claims-Set. Compact serialization is the
; protected headers, payload and signature, each b64url encoded and
; separated by a ".". This CDDL simply matches top-level syntax of of
; a JWS or JWE since it is not possible to do more in CDDL.

JWT-Message =
    text .regexp "[A-Za-z0-9_-]+\.\.[A-Za-z0-9_-]+\.\.[A-Za-z0-9_-]+"

; Note that the payload of a JWT is defined in claims-set.cddl. That
; definition is common to CBOR and JSON.

```

; This is some CDDL describing a CWT at the top level This is  
; not normative. RFC 8392 is the normative definition of CWT.

CWT-Message = CWT-Tagged-Message / CWT-Untagged-Message

; The payload of the COSE\_Message is always a Claims-Set

; The contents of a CWT Tag must always be a COSE tag

CWT-Tagged-Message = #6.61(COSE\_Tagged\_Message)

; An untagged CWT may be a COSE tag or not

CWT-Untagged-Message = COSE\_Messages

## **Appendix E. New Claim Design Considerations**

The following are design considerations that may be helpful to take into account when creating new EAT claims. It is the product of discussion in the working group.

EAT reuses the CWT and JWT claims registries. There is no registry exclusively for EAT claims. This is not an update to the expert review criteria for the JWT and CWT claims registries as that would be an overreach for this document.

### **E.1. Interoperability and Relying Party Orientation**

It is a broad goal that EATs can be processed by relying parties in a general way regardless of the type, manufacturer or technology of the device from which they originate. It is a goal that there be general-purpose verification implementations that can verify tokens for large numbers of use cases with special cases and configurations for different device types. This is a goal of interoperability of the semantics of claims themselves, not just of the signing, encoding and serialization formats.

This is a lofty goal and difficult to achieve broadly requiring careful definition of claims in a technology neutral way. Sometimes it will be difficult to design a claim that can represent the semantics of data from very different device types. However, the goal remains even when difficult.

### **E.2. Operating System and Technology Neutral**

Claims should be defined such that they are not specific to an operating system. They should be applicable to multiple large high-level operating systems from different vendors. They should also be applicable to multiple small embedded operating systems from multiple vendors and everything in between.

Claims should not be defined such that they are specific to a software environment or programming language.

Claims should not be defined such that they are specific to a chip or particular hardware. For example, they should not just be the contents of some HW status register as it is unlikely that the same HW status register with the same bits exists on a chip of a different manufacturer.

The boot and debug state claims in this document are an example of a claim that has been defined in this neutral way.

### **E.3. Security Level Neutral**

Many use cases will have EATs generated by some of the most secure hardware and software that exists. Secure Elements and smart cards are examples of this. However, EAT is intended for use in low-security use cases the same as high-security use case. For example, an app on a mobile device may generate EATs on its own.

Claims should be defined and registered on the basis of whether they are useful and interoperable, not based on security level. In particular, there should be no exclusion of claims because they are just used only in low-security environments.

### **E.4. Reuse of Extant Data Formats**

Where possible, claims should use already standardized data items, identifiers and formats. This takes advantage of the expertise put into creating those formats and improves interoperability.

Often extant claims will not be defined in an encoding or serialization format used by EAT. It is preferred to define a CBOR and JSON encoding for them so that EAT implementations do not require a plethora of encoders and decoders for serialization formats.

In some cases, it may be better to use the encoding and serialization as is. For example, signed X.509 certificates and CRLs can be carried as-is in a byte string. This retains interoperability with the extensive infrastructure for creating and processing X.509 certificates and CRLs.

### **E.5. Proprietary Claims**

It is not always possible or convenient to achieve the above goals, so the definition and use of proprietary claims is an option.

For example, a device manufacturer may generate a token with proprietary claims intended only for verification by a service offered by that device manufacturer. This is a supported use case.

In many cases proprietary claims will be the easiest and most obvious way to proceed, however for better interoperability, use of general standardized claims is preferred.

## **Appendix F. Endorsements and Verification Keys**

The verifier must possess the correct key when it performs the cryptographic part of an EAT verification (e.g., verifying the COSE/JOSE signature). This section describes several ways to identify the verification key. There is not one standard method.

The verification key itself may be a public key, a symmetric key or something complicated in the case of a scheme like Direct Anonymous Attestation (DAA).

RATS Architecture [[RFC9334](#)] describes what is called an endorsement. This is an input to the verifier that is usually the basis of the trust placed in an EAT and the attester that generated it. It may contain the public key for verification of the signature on the EAT. It may contain implied claims, those that are passed on to the relying party in attestation results.

There is not yet any standard format(s) for an endorsement. One format that may be used for an endorsement is an X.509 certificate. Endorsement data like reference values and implied claims can be carried in X.509 v3 extensions. In this use, the public key in the X.509 certificate becomes the verification key, so identification of the endorsement is also identification of the verification key.

The verification key identification and establishment of trust in the EAT and the attester may also be by some other means than an endorsement.

For the components (attester, verifier, relying party,...) of a particular end-end attestation system to reliably interoperate, its definition should specify how the verification key is identified. Usually, this will be in the profile document for a particular attestation system.

See also security consideration in [Section 9.6](#).

### **F.1. Identification Methods**

Following is a list of possible methods of key identification. A specific attestation system may employ any one of these or one not listed here.

The following assumes endorsements are X.509 certificates or equivalent and thus does not mention or define any identifier for

endorsements in other formats. If such an endorsement format is created, new identifiers for them will also need to be created.

#### **F.1.1. COSE/JWS Key ID**

The COSE standard header parameter for Key ID (kid) may be used. See [\[RFC9052\]](#) and [\[RFC7515\]](#)

COSE leaves the semantics of the key ID open-ended. It could be a record locator in a database, a hash of a public key, an input to a Key Derivation Function (KDF), an Authority Key Identifier (AKI) for an X.509 certificate or other. The profile document should specify what the key ID's semantics are.

#### **F.1.2. JWS and COSE X.509 Header Parameters**

COSE X.509 [\[COSE.X509.Draft\]](#) and JSON Web Signature [\[RFC7515\]](#) define several header parameters (x5t, x5u,...) for referencing or carrying X.509 certificates any of which may be used.

The X.509 certificate may be an endorsement and thus carrying additional input to the verifier. It may be just an X.509 certificate, not an endorsement. The same header parameters are used in both cases. It is up to the attestation system design and the verifier to determine which.

#### **F.1.3. CBOR Certificate COSE Header Parameters**

Compressed X.509 and CBOR Native certificates are defined by CBOR Certificates [\[CBOR.Cert.Draft\]](#). These are semantically compatible with X.509 and therefore can be used as an equivalent to X.509 as described above.

These are identified by their own header parameters (c5t, c5u,...).

#### **F.1.4. Claim-Based Key Identification**

For some attestation systems, a claim may be re-used as a key identifier. For example, the UEID uniquely identifies the entity and therefore can work well as a key identifier or endorsement identifier.

This has the advantage that key identification requires no additional bytes in the EAT and makes the EAT smaller.

This has the disadvantage that the unverified EAT must be substantially decoded to obtain the identifier since the identifier is in the COSE/JOSE payload, not in the headers.

## Appendix G. Changes from Previous Drafts

RFC editor: please remove this paragraph.

The following is a list of known changes since the immediately previous drafts. This list is non-authoritative. It is meant to help reviewers see the significant differences. A comprehensive history is available via the IETF Datatracker's record for this document.

### G.1. From draft-ietf-rats-eat-24

The changes from draft-24, not draft 25, are listed here as draft-24 is what was accepted after IETF last call and draft-25 was kind of a false start.

- \*Address some small claim data type naming issues that came to light when IANA completed the registrations requested by this document. In particular, the CDDL type names are used.
- \*Remove all dependence on SUIT Manifest to break schedule interlock with RFC Editor. Use of SUIT-Manifest is peripheral to the core of EAT. It was mostly a content type pre-registration. The modification consisted of the removal of one sentence, a few more words and two lines of CDDL.
- \*Reworded full profiles description to convey intent without using "may not"
- \*Upated references for UUIDs and LDAP to non-obsolete documents.
- \*Removed some non-ascii quote marks
- \*"MAY not" -> "MAY NOT"

### Contributors

Many thanks to the following contributors to draft versions of this document:

Henk Birkholz  
Fraunhofer SIT

Email: [henk.birkholz@sit.fraunhofer.de](mailto:henk.birkholz@sit.fraunhofer.de)

Thomas Fossati  
Arm Limited

Email: [thomas.fossati@arm.com](mailto:thomas.fossati@arm.com)

Miguel Ballesteros



Michael Richardson  
Sandelman Software Works

Email: [mcr+ietf@sandelman.ca](mailto:mcr+ietf@sandelman.ca)

Patrick Uiterwijk

Mathias Brossard

Hannes Tschofenig  
Arm Limited

Email: [hannes.tschofenig@arm.com](mailto:hannes.tschofenig@arm.com)

Paul Crowley

### **Authors' Addresses**

Laurence Lundblade  
Security Theory LLC

Email: [lgl@securitytheory.com](mailto:lgl@securitytheory.com)

Giridhar Mandyam  
Mediatek USA

Email: [giridhar.mandyam@gmail.com](mailto:giridhar.mandyam@gmail.com)

Jeremy O'Donoghue  
Qualcomm Technologies Inc.  
279 Farnborough Road  
Farnborough  
GU14 7LS  
United Kingdom

Phone: [+44 1252 363189](tel:+441252363189)

Email: [jodonogh@qti.qualcomm.com](mailto:jodonogh@qti.qualcomm.com)

Carl Wallace  
Red Hound Software, Inc.

Email: [carl@redhoundsoftware.com](mailto:carl@redhoundsoftware.com)