Editors Response to AUTH48 Questions on RFC 9711 from the RFC Editor

The editors thank the RFC Editor for all of their efforts in pulling this draft together. This response is divided into two sections: (a) changes that the editors require that were not cited by the RFC Editor, and (b) responses to the recommended changes by the RFC Editor.

Contents

[Editors Required Changes: 1](#_Toc188192995)

[Editors Response to RFC Editors Questions 2](#_Toc188192996)

# Editors Required Changes:

1. Original, Informative References:

**[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>>.

New:

**[IEEE.802-2014]** "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>>.

1. Original, Sec. 4.2.10:

If the entity is stationary, the heading is NaN (floating-point not-a-number).

New:

If the entity is stationary, the heading is NULL.

1. Original, Sec. 4.2.10:

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 >

New:

location-type = {

latitude => number,

longitude => number,

? altitude => number,

? accuracy => number,

? altitude-accuracy => number,

? heading => number / null,

? 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 >

# Editors Response to RFC Editors Questions

Please note that Editors’ responses will be preceded with “EDITORS’ RESPONSE: “.

1) <!--[rfced] Section 1. FYI - We expanded the first mentions of "ueid"  
and "oemid" as shown below. Please let us know if this is not accurate.  
  
Original:  
   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].  
  
Current:  
   The ueid (Universal Entity ID) is  
   effectively a serial number uniquely identifying the device.  This  
   ueid is the base64url encoding of a 48-bit Media Access Control (MAC)  
   address preceded by the type byte 0x02.  The oemid (Hardware OEM ID)  
   identifies the manufacturer using a Private Enterprise Number (PEN) [PEN].  
-->     

EDITORS’ RESPONSE: Current is acceptable.  
  
2) <!--[rfced] Section 1.2. Please clarify the latter part of this  
sentence. Is the intended meaning that EAT is not used for  
specific token definition as shown below?  
  
Original:  
   EAT is a framework for defining attestation tokens for specific use  
   cases, not a specific token definition.  
  
Perhaps:  
   EAT is a framework that is used for defining attestation tokens for  
   specific use cases; it is not used for specific token definition.  
-->

EDITORS’ RESPONSE: Perhaps suggestion is acceptable.  
  
3) <!--[rfced] Sections 1.2 and 4.2.18. The term "follow-on documents"  
hasn't been used since early RFCs. Would it be clearer to say  
"subsequent documents" as shown below? Note that there are 2 instances.  
  
Original:  
   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.   
   [...]  
  
   Nested tokens can be one of three types as defined in this document or  
   types standardized in follow-on documents (e.g., [UCCS]).  
  
Perhaps:  
   Finally, this document introduces the notion of an EAT profile that  
   facilitates the creation of narrowed definitions of EATs for  
   specific use cases in subsequent documents.   
   [...]  
  
   Nested tokens can be one of three types as defined in this document or  
   types that are standardized in subsequent documents (e.g., [UCCS]).  
-->  
  
EDITORS’ RESPONSE: Both Perhaps suggestions are acceptable.

4) <!--[rfced] Section 2. We note that RFC 7515 (Section 2) defines  
"base64url encoding" rather than "base64url encoded". Would you  
like to update the terminology list to match RFC 7515, or is this  
variance okay?  
  
Original:  
   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.  
  
Perhaps:  
   base64url encoding:  As defined in [RFC7515], base64 encoding  
      uses a 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.  
-->

EDITORS’ RESPONSE: Perhaps suggestion is acceptable.  
  
5) <!--[rfced] Section 2. We added a citation to RFC 9052 for "COSE" for easy  
reference. If that is not correct or desired, please let us know.  
  
Original:  
   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.)  
  
Current:  
   Claim Key:  The CBOR map key used to identify a claim.  (The term  
      "Claim Key" comes from CWT.  This document, like COSE [RFC9052],  
      uses the term "label" to refer to CBOR map keys to avoid  
      confusion with cryptographic keys.)  
-->

EDITORS’ RESPONSE: Current is acceptable.  
  
6) <!--[rfced] Section 4. Can "of most of what is defined" be rephrased  
for clarity as shown below?  
  
Original:  
   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].  
  
Perhaps:  
   This specification includes a CDDL definition that is based on the  
   CDDL definitions in [RFC8392] and [RFC7519].  
-->

EDITORS’ RESPONSE: Please modify using the following text: “This specification includes a CDDL definition that is derived from normative text in [RFC8392] and [RFC7519].”  
  
7) <!--[rfced] Section Titles  
  
a) Should the title of Section 4.2.2 be updated as shown  
below (i.e., remove "(SUEIDs)") for consistency with the  
other section titles? (See the separate question re: removing  
the hyphen in 'semipermanent'.)  
  
Original:  
   4.2.1.  ueid (Universal Entity ID) Claim  
   4.2.2.  sueids (Semi-permanent UEIDs) Claim (SUEIDs)  
  
Perhaps:  
   4.2.1.  ueid (Universal Entity ID) Claim  
   4.2.2.  sueids (Semipermanent UEIDs) Claim  
  
...

EDITORS’ RESPONSE: Perhaps suggestion is acceptable.

b) Should the title of Section 4.2.18 contain "Claim" for  
consistency?  
  
Original:  
   4.2.16. measurements (Measurements) Claim  
   4.2.17. measres (Software Measurement Results) Claim  
   4.2.18  submods (Submodules)  
  
Perhaps:  
   4.2.16. measurements (Measurements) Claim  
   4.2.17. measres (Software Measurement Results) Claim  
   4.2.18  submods (Submodules) Claim  
-->

EDITORS’ RESPONSE: Perhaps suggestion is acceptable.  
  
8) <!--[rfced] Section 4.2.3.2. Please clarify what "these" refers to in  
"Many companies already have purchased one of these" (last sentence).  
  
Original:  
   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 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.  Similarly, MA-M is a 28-bit  
   value used as the first part of a MAC address, and MA-S, formerly  
   known as OUI-36, is a 36-bit value.  Many companies already have  
   purchased one of these.  
-->  
  
EDITORS’ RESPONSE: Please modify the last sentence using the following text: “Many companies have already obtained an OEM ID from the IEEE registry”.

9) <!--[rfced] Section 4.2.3.3. This sentence cites the application  
for PENs (<https://pen.iana.org/pen/PenApplication.page>), so it seems  
either the text or the reference should be updated. Which do you prefer?  
  
Original:  
   IANA maintains a registry for Private Enterprise Numbers [PEN].  
  
where  
   [PEN]      "Private Enterprise Number (PEN) Request", n.d.,  
              <<https://pen.iana.org/pen/PenApplication.page>>.  
  
  
Option A (if the reference remains the same):  
   IANA maintains the application for Private Enterprise  
   Numbers [PEN].  
  
Option B (if the reference is changed to the registry itself):  
  
   IANA maintains a registry for Private Enterprise Numbers [PEN].  
  
where:  
   [PEN]  IANA, "Private Enterprise Numbers (PENs)",     
          <<https://www.iana.org/assignments/enterprise-numbers/>>.  
-->

EDITORS’ RESPONSE: Option B is acceptable.  
  
10) <!--[rfced] Section 4.2.7. A word is missing after "may be". Please  
confirm if "used" is the correct word as shown below.  
  
Original:  
   The "manifests" claim Section 4.2.15 may be instead if this is too  
   simple.  
  
Current:  
   The "manifests" claim (Section 4.2.15) may be used instead if this  
   is too simple.  
-->

EDITORS’ RESPONSE: Current is acceptable.  
  
11) <!-- [rfced] Section 4.2.10. We notice that [W3C.GeoLoc] is listed as  
an informative reference, whereas [WGS84] is a normative  
reference.  Considering the key word "MUST" in this sentence,  
should [W3C.GeoLoc] be listed as a normative reference?  
  
Original:  
   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]).  
 -->  
  
EDITORS’ RESPONSE: The W3C.Geoloc should be made normative.

12) <!--[rfced] Section 4.2.10. With the expansion of "GNSS",  
should this be rephrased?  
  
Original:  
   For example, it might have been minutes or hours or more  
   since the last contact with a GNSS satellite.  
  
Current:  
   For example, it might have been minutes, hours, or more  
   since the last contact with a Global Navigation Satellite  
   System (GNSS) satellite.  
  
Perhaps:  
   For example, it might have been minutes, hours, or more  
   since the last contact with a satellite in the Global  
   Navigation Satellite System (GNSS).  
-->

EDITORS’ RESPONSE: Perhaps suggestion is acceptable.  
  
13) <!--[rfced] Section 4.2.15. Should the word 'tag' be added here,  
as the term 'SWID tag' is used in RFC 9393?  
  
Original:  
   For example, the manifest may be a CBOR-encoded CoSWID, an  
   XML-encoded SWID or other.  
  
Current:  
   For example, the manifest may be a CBOR-encoded CoSWID, an  
   XML-encoded Software Identification (SWID), or other.  
  
Perhaps:  
   For example, the manifest may be a CBOR-encoded CoSWID, an  
   XML-encoded Software Identification (SWID) tag, or other.  
-->

EDITORS’ RESPONSE: Perhaps suggestion is acceptable.  
  
14) <!--[rfced] Sections 4.2.15 and 4.2.16. RFC 7252 uses Content-Format  
"identifier" rather than "integer". Given this, should "integer"  
be removed or replaced with "identifier" as shown below for  
consistency (3 instances)?  
  
Original:  
   Identification of the type of manifest is always by a Constrained  
   Application Protocol (CoAP) Content-Format integer [RFC7252].  
  
   The first item in the array of two MUST be an integer CoAP  
   Content-Format identifier.  
  
   The identification of format is by CoAP Content Format, the same as  
   the "manifests" claim in Section 4.2.15.  
  
Perhaps:  
   Identification of the type of manifest is always by a Constrained  
   Application Protocol (CoAP) Content-Format identifier [RFC7252].  
  
   The first item in the array of two MUST be a CoAP Content-Format  
   identifier.  
  
   The format is identified by a CoAP Content-Format identifier, which  
   is the same for the "manifests" claim in Section 4.2.15.  
-->

EDITORS’ RESPONSE: Perhaps suggestion is acceptable.  
  
15) <!--[rfced] Section 4.2.16. What words are missing after "a"?  
  
Original:  
   This claim can be a [RFC9393].  
  
Perhaps:  
   This claim can be a CoSWID [RFC9393].  
-->  
  
EDITORS’ RESPONSE: Perhaps suggestion is acceptable.  
  
16) <!--[rfced] Section 4.2.17. Should the terms/values listed in these  
two paragraphs match for consistency as shown below?  
  
Also, 'success/fail' or 'success/failure' is a corresponding pair  
rather than 'successful/fail'. (If this is updated, seemingly the  
CDDL below and in Section 7.3.1 would also need an update, e.g.,  
'comparison-successful'.)  
  
Current:  
   This claim provides a simple standard way to report the result  
   of a comparison as success, failure, fail to run, and absence.  
  
  
   1 - comparison successful:  The comparison to reference values was  
       successful.  
  
   2 - comparison fail:  The comparison was completed but 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.  
  
Perhaps:  
   This claim provides a simple standard way to report the result  
   of a comparison as a success, a failure, not run, or absent.  
  
  
   1 - comparison success:  The comparison to reference values was  
       successful.  
  
   2 - comparison failure:  The comparison was completed but 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.  
-->

EDITORS’ RESPONSE: Perhaps suggestion is acceptable. Please update the CDDL instances accordingly.  
  
  
17) <!--[rfced] Sections 4.2.18.1 and 4.2.18.3. Would it be correct to say  
that the keys (or no keys) are distinct from the surrounding  
token produced by the attester?  
  
Original:  
   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.  
  
   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.   
  
Perhaps:  
   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 that are distinct from the surrounding token produced by  
   the attester.  
  
   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 that are distinct from the  
   surrounding token produced by the attester.   
-->

EDITORS’ RESPONSE: Original text should not be changed. Please revert.  
  
18) <!--[rfced] Section 4.2.18.2. We updated this sentence to clarify  
"is directly". If it changes the intended meaning, please let us know.  
  
Original:  
   The input to the digest algorithm is directly the CBOR or  
   JSON-encoded Claims-Set for the submodule.  
  
Current:  
   The direct input to the digest algorithm is either the  
   CBOR-encoded or the JSON-encoded Claims-Set for the  
   submodule.  
-->

EDITORS’ RESPONSE: Please modify using the following text: “The input to the digest algorithm is the CBOR or JSON-encoded Claims-Set for the submodule.”  
  
19) <!--[rfced] Section 6.3.9. FYI, "end-end" has been updated to "end-to-end".  
(This is similar to a change that was made in version 31 of the original.)  
  
Original:  
   While not always possible, a profile should specify or make reference  
   to, a full end-end specification for key identification.  
  
Current:  
   While not always possible, a profile should specify, or make reference  
   to, a full end-to-end specification for key identification.  
-->

EDITORS’ RESPONSE: Current text is acceptable.  
  
20) <!--[rfced] Section 6.3.12. The text mentions the measurement and  
measurements claims; however, Section 4.2.16 only refers to the  
"measurements" claim. Should "claims" perhaps be singular, or  
should "measurement" be removed or updated (perhaps "measres"  
claim was intended)?  
  
Original:  
   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.  
  
Perhaps:  
   The "manifests" claim (Section 4.2.15) along with the  
   "measurements" claim (Section 4.2.16) and "measres" claim (Section 4.2.17)  
   are examples of this, allowing the use of CoSWID and other formats.  
-->

EDITORS’ RESPONSE: Please change using the following text:

*The "manifests" claim (Section 4.2.15) and "measurements" claim (Section 4.2.16) are examples of this, allowing the use of CoSWID and other formats.*

Justification: “measres” isn’t meant to be pluggable, but the original text needs to be modified.

21) <!--[rfced] Section 6.3.12. FYI - We updated the following text as the  
second sentence is a fragment. If this changes the intended  
meaning, please let us know.  
  
Original:  
   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.  
  
Current:  
   For example, there are variations in the CoSWID format, such as a profile  
   that requires the receiver to accept all variations that are allowed  
   to be sent.  
-->

EDITORS’ RESPONSE: Current text is acceptable.  
  
22) <!--[rfced] Section 7.1. This sentence mentions that CDDL for the  
seven claims is included "here". Please clarify what "here"  
refers to - is it referring to Section 7.1 or to one of the  
subsections?  
  
Original:  
   CDDL for the seven claims defined by [RFC8392] and [RFC7519] is  
   included here.  
  
Perhaps:  
   CDDL for the seven claims defined by [RFC8392] and [RFC7519] is  
   also specified in this document.  
-->

EDITORS’ RESPONSE: Perhaps suggestion is acceptable.  
  
23) <!--[rfced] Section 7.2. What does "This" refer to - is it "The  
following subsections" as shown below?  
  
Current:  
7.2.  Encoding Data Types  
  
   This makes use of the types defined in "Standard Prelude"  
   (Appendix D of [RFC8610]).  
  
Perhaps:  
7.2.  Encoding Data Types  
  
   The following subsections use the types defined in  
   "Standard Prelude" (Appendix D of [RFC8610]).  
-->

EDITORS’ RESPONSE: Perhaps suggestion is acceptable.  
  
24) <!--[rfced] Section 7.3.1. This sentence does not parse - is "use"  
perhaps missing after the comma? Please let us know how we may  
update for clarity.  
  
Original:  
   When there is variation between CBOR and JSON, the  
   JC<> CDDL generic defined in Appendix D.   
  
Perhaps:  
   When there is variation between CBOR and JSON, use the  
   JC<> CDDL generic defined in Appendix D.   
-->

EDITORS’ RESPONSE: Please modify using the following text: “When there is variation between CBOR and JSON, the JC<> CDDL generic defined in Appendix D is used.”  ﻿  
  
25) <!--[rfced] Section 9.1. The following text does not parse  
(specifically, the latter part after the comma). Please let us  
know how we may update for clarity.  
  
Original:  
   For example, this document says that a UEID is permanent and that it  
   must not change, but it does not say what degree of attack to change  
   it must be defended.  
  
Perhaps:  
   For example, this document states that a UEID is permanent and that it  
   must not change, but it does not state if change is needed to defend  
   against a certain degree of attack.  
-->

EDITORS’ RESPONSE: Please modify using the following text: “For example, this document states that a UEID is permanent and that it must not change, but it does not describe any security requirements or a level of defense to prevent an attacker from changing the UEID.”  
  
26) <!--[rfced] Section 10.2. Is this sentence necessary?  
  
Original:  
   The "Claim Value                           
   Type(s)" here all name CDDL definitions and are only for the CWT  
   registry.  
  
It seems redundant with this text in the preceding paragraph:  
  
   The "Claim Key" and "Claim Value Types(s)" are for the CWT registry  
   only.  
-->

EDITORS’ RESPONSE: Please delete the original text and do not replace it.  
  
27) <!--[rfced] Below are questions about the IANA-related text.  
In addition to responding to these questions, please review  
all of the IANA-related updates carefully and let us know  
if any further updates are needed.  
  
a) Section 4.2.18.2. Please clarify which IANA registry is  
being referred to in the last sentence (i.e., the "JOSE Algorithm  
registry"). Is it the "JSON Web Signature and Encryption  
Algorithms" registry <<https://www.iana.org/assignments/jose/>>?  
  
Original:  
   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.  
  
Perhaps:  
   The hash algorithm identifier is always from the "COSE Algorithms"  
   registry [IANA.COSE.Algorithms].  Either the integer or  
   the string identifier may be used.  The hash algorithm identifier is  
   never from the "JSON Web Signature and Encryption Algorithms" registry.

EDITORS’ RESPONSE: Please modify using the following text: “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 any other algorithm registry.”  
  
b) Section 10.2. May we remove all quote marks from the JWT Claim Name  
fields? We note that quote marks are not used in the "CBOR Web Token  
(CWT) Claims" registry <<https://www.iana.org/assignments/cwt>>.  
For example:  
OLD: JWT Claim Name: "eat\_nonce"  
NEW: JWT Claim Name: eat\_nonce

EDITORS’ RESPONSE: Original text should not be changed. Please revert.  
  
c) Section 10.2. In the "CBOR Web Token (CWT) Claims" registry  
for eat\_nonce (Claim Key 10), the Reference field includes "OpenID  
Connect Core 1.0" (<https://openid.net/specs/openid-connect-core-1_0.html>),  
but the Reference field in the draft did not. FYI, this document  
has been updated to match the registry, and "OpenID Connect Core 1.0"  
has been added as an informative reference.  
  
In the JWT Claims registry, should "eat\_nonce" have a matching  
Reference field? (This document states the Reference fields are  
"common and equivalent".) If so, we will ask IANA to update the registry  
as follows.  
  
Old: eat\_nonce  Nonce   [IETF]  [RFC-ietf-rats-eat-30]  
New: eat\_nonce  Nonce   [IETF]  [OpenID Connect Core 1.0][RFC-ietf-rats-eat-30]  
  
EDITORS’ RESPONSE: Original text should not be changed. Please revert. The change that should be made is to remove the OpenID Connect reference from the CWT registry. The defintion of this claim rests entirely in EAT. I believe the reason that OpenID mentions this claim is because OpenID was revised after the EAT claim was allocated early. Also see EAT section 4.1.

d) Section 10.2. Regarding "Claim Description" (in both the CWT and JWT  
Claims registries), would you like to update these to remove 'Indicates'  
so they are similar to other descriptions? If so, we will ask IANA to  
update the registries accordingly with any changes made.  
  
Original:  
   ueid          The Universal Entity ID  
  
   sueids        Semi-permanent UEIDs  
  
   hwmodel       Model identifier for hardware  
  
   dbgstat       Indicates status of debug facilities  
  
   eat\_profile   Indicates the EAT profile followed  
  
   intuse        Indicates intended use of the EAT  
  
Perhaps:  
   ueid          Universal Entity ID  
  
   sueids        Semipermanent UEIDs  
  
   hwmodel       Model identifier for hardware  
  
   dbgstat       The status of debug facilities  
  
   eat\_profile   The EAT profile followed  
  
   intuse        The intended use of the EAT

EDITORS’ RESPONSE: Perhaps suggestion is acceptable.

e) Section 10.3. In the "DEV URN Subtypes" registry, may we  
update the descriptions as follows?  
- change "Identifier" to "ID" to match the "JSON Web Token Claims"  
registry, "CBOR Web Token (CWT) Claims" registry, and the running text in  
this document.  
- change "Semi-permanent" to "Semipermanent" per Merriam-Webster  
(throughout this document and in the two other registries).  
  
Original:  
   ueid    Universal Entity Identifier  
   sueid   Semi-permanent Universal Entity Identifier  
  
Perhaps:  
   ueid    Universal Entity ID  
   sueid   Semipermanent Universal Entity ID

EDITORS’ RESPONSE: Perhaps suggestion is acceptable.  
  
f) Section 10.4. FYI - In the "CBOR Tags" registry at  
<https://www.iana.org/assignments/cbor-tags/>, the reference to Section 5  
of this document is included under the Semantics column. We will ask  
IANA to update the registry so that "RFC 9711, Section 5" is only  
in the Reference column.  
  
Original:  
           +=====+============+===============================+  
           | Tag | Data Items | Semantics                     |  
           +=====+============+===============================+  
           | 602 | array      | Detached EAT Bundle Section 5 |  
  
Current:  
   +=====+===========+=====================+=====================+  
   | Tag | Data Item | Semantics           | Reference           |  
   +=====+===========+=====================+=====================+  
   | 602 | array     | Detached EAT Bundle | RFC 9711, Section 5 |

EDITORS’ RESPONSE: Current text is acceptable.  
  
g) Section 10.5. The columns for the "Entity Attestation Token  
(EAT) Intended Uses" registry are "Integer", "Name", and  
"Description" in this document, but "Value", "Description", and  
"Reference" in the IANA registry <<https://www.iana.org/assignments/rats>>.  
Which one is correct?  If the IANA registry is correct, please provide  
updated text for Section 10.5 where it describes the three columns.  
-->

EDITORS’ RESPONSE: Please make change as below to synchronize the EAT text with the IANA registry:

ORIGINAL:

  Integer: This is a unique integer used to identify the intended use in CBOR-encoded tokens.

NEW:

  Value: This is a unique integer used to identify the intended use in CBOR-encoded tokens.

28) <!-- [rfced] FYI, a normative reference to RFC 5234 has been added because  
this document contains ABNF. See the IESG statement on "Guidelines for  
the Use of Formal Languages in IETF Specifications"  
(<https://ietf.org/blog/guidelines-use-formal-languages-ietf-specifications/>) -  
specifically "The use of a language requires a reference to the  
specification for that language. This reference is normative ..."  
  
Please review where RFC 5234 is cited and let us know if you prefer  
otherwise. Also, RFC 7405 has been added because "%s" is used.  
  
Current:  
   The ABNF [RFC5234] [RFC7405] 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  
-->

EDITORS’ RESPONSE: Current text is acceptable.  
  
29) <!--[rfced] FYI, we updated the URL for this reference because it  
was a direct download of the PDF file. The updated URL points to  
a landing page with more information and the option to download  
the file instead. Please let us know if you prefer otherwise.  
  
Original:  
   [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>>.  
  
Current:  
   [WGS84]  National Geospatial-Intelligence Agency (NGA), "Department  
            of Defense World Geodetic System 1984: Its Definition and  
            Relationships with Local Geodetic Systems",  
            NGA.STND.0036\_1.0.0\_WGS84, July 2014,  
            <<https://nsgreg.nga.mil/doc/view?i=4085>>.  
-->

EDITORS’ RESPONSE: Current text is acceptable.  
  
30) <!--[rfced] FYI, we updated this reference to reflect the most current  
version (September 2024). Please let us know if you prefer otherwise.  
  
Original:  
  [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>.  
  
Current:  
   [ThreeGPP.IMEI]  
      3GPP, "Numbering, addressing and identification", 3GPP  
      TS 23.003, Version 19, September 2024,  
      <<https://portal.3gpp.org/desktopmodules/Specifications/>  
      SpecificationDetails.aspx?specificationId=729>.  
-->     

EDITORS’ RESPONSE: Current text is acceptable.  
  
31) <!--[rfced] There is a more recent version of this reference  
(September 2024). May we point to that version instead, or do you  
prefer the 2013 (outdated) version?  
  
Current:  
   [W3C.GeoLoc]  
       Popescu, A., Ed., "Geolocation API Specification", W3C  
       Recommendation, 24 October 2013,  
       <<https://www.w3.org/TR/2013/REC-geolocation-API->  
       20131024/>.  
  
Perhaps:  
   [W3C.GeoLoc]  
       Cáceres, M. and R. Grant, "Geolocation", W3C  
       Recommendation, September 2024,  
       <<https://www.w3.org/TR/geolocation/>>.  
-->  
  
EDITORS’ RESPONSE: Perhaps suggestion is acceptable. Please bear in mind that this reference will become normative as per RFC Editors comment no. 11 above.

32) <!--[rfced] Appendix A. Please review this note and let us know if  
there are any outstanding actions regarding regenerating the examples.  
  
AUTHOR NOTE:  
   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.  
-->  
  
EDITORS’ RESPONSE: Examples were successfully regenerated.

33) <!--[rfced] Questions about the sourcecode  
  
a) We updated <artwork> to <sourcecode> in Sections 1 and 10.3 as  
well as Appendices A.1.1 - A.2.3 and D. Please confirm that this is  
correct.  
  
In addition, please consider whether the "type" attribute of any sourcecode  
element should be set and/or has been set correctly.  
  
The current list of preferred values for "type" is available at  
<<https://www.rfc-editor.org/rpc/wiki/doku.php?id=sourcecode-types>>.  
If the current list does not contain an applicable type, feel free to  
suggest additions for consideration. Note that it is also acceptable  
to leave the "type" attribute not set.  
  
...  
Sourcecode in the Appendices

EDITORS’ RESPONSE: These changes were confirmed to be correct.  
  
b) We notice that each sourcecode element in the appendices contains  
introductory text, formatted as a comment within the sourcecode. Should this  
text be moved outside of the sourcecode? If not, please consider the questions  
that follow.

EDITORS’ RESPONSE: As a blanket guideline, no. However there is a specific example below where this is necessary.  
  
c) Appendix A.2.1. The text below refers to a section that is  
outside of the sourcecode. Should a pointer to "Appendix A.1.7  
of RFC 9711" be added?  
  
Original:  
   / 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.                    /  
  
Perhaps:  
   / This is a full CWT-format token. The payload is the   /  
   / attestation hardware block in Appendix A.1.7 of       /  
   / RFC 9711. The main structure that is visible is       /  
   / that of the COSE\_Sign1.                               /

EDITORS’ RESPONSE: Perhaps suggestion is acceptable.

d) Appendix A.2.2. The text below refers to "the next section".  
Should a pointer be added to Appendix A.2.3?  
  
Original:  
  / Most importantly, it includes a submodule that is a     /  
  / detached digest which is the hash of the "TEE" claims   /  
  / set in the next section.

EDITORS’ RESPONSE: Please add the pointer.  
  
e) Appendix D. The text below refers to the I-D  
"draft-ietf-rats-uccs". May we move this sentence outside of  
the sourcecode so that a citation can be added for the I-D?  
  
Original:  
   ; This is replicated from draft-ietf-rats-uccs  
  
   Claims-Set = {  
       \* $$Claims-Set-Claims  
       \* Claim-Label .feature "extended-claims-label" => any...  
  
Perhaps:  
   The following example is replicated from [UCCS].  
  
   Claims-Set = {  
       \* $$Claims-Set-Claims  
       \* Claim-Label .feature "extended-claims-label" => any...

EDITORS’ RESPONSE: Perhaps suggestion is acceptable with one change. Editors do not want a normative reference to UCCS. Rather, the editors prefer the following text in the main draft (i.e. not part of the CDDL description): “See also [UCCS].”

f) Appendix D. Please clarify where a reader can find "claims-set.cddl"  
as this is the only mention of it in this document.  
  
Original:  
   ; Note that the payload of a JWT is defined in claims-set.cddl. That  
   ; definition is common to CBOR and JSON.  
-->

EDITOR RESPONSE:   Please change to "is defined in the CDDL description of claims-set."  
  
34) <!--[rfced] Appendix A.1.2. To avoid repetition, we updated "with the  
CPU" to "containing the CPU". Please review.  
  
Original:  
   The main attestation is associated with the chip with the  
   CPU and running the main OS.  
  
Current:  
   The main attestation is associated with the chip containing  
   the CPU and running the main OS.  
-->

EDITORS’ RESPONSE: Current text is acceptable.  
  
35) <!--[rfced] Appendix A.1.3. Is the intention to say that 47 bytes are  
encoded in CBOR "including" an 8-byte nonce and 16-byte UEID as  
shown below? Please let us know how we may update for clarity.  
  
Original:  
   47 bytes encoded in CBOR (8-byte nonce, 16-byte UEID).  
  
Perhaps:  
   47 bytes are encoded in CBOR (including an 8-byte nonce and  
   a 16-byte UEID).  
-->

EDITORS’ RESPONSE: Please modify using the following text: “T he entire encoded token is 47 bytes, 8 of which are the nonce and 16 of which are the UEID”

36) <!--[rfced] Appendix A.1.4. Within the sourcecode, may we update  
"eliptic" to "elliptic" as shown below? If different spacing is  
desired, please let us know.  
  
Original:  
   / kty /       1: 2, / EC2, eliptic curve with x & y /  
  
Perhaps:  
   / kty /       1: 2, / EC2, elliptic curve with x & y/  
-->  
  
EDITORS’ RESPONSE: Perhaps suggestion is acceptable.

37) <!--[rfced] Appendix A.1.6. We believe "Trustus Verifications" is a  
service (rather than multiple services) that verifies the  
software component measures, so we have updated accordingly. If  
what is shown below is not correct, please let us know.  
  
Original:  
   "Trustus Verifications" is the name of the services that verifies the  
   software component measurements.  
  
Current:  
   "Trustus Verifications" is the name of the service that verifies the  
   software component measurements.  
-->

EDITORS’ RESPONSE: Current text is acceptable.  
  
38) <!--[rfced] Appendix B.2. How can "UEID takes the view" be reworded  
to avoid personification? Also, it is not clear what "It" refers to  
in the second sentence - is it also "UEID"? Please clarify.  
  
Original:  
   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 processes implement UEID in a simple and  
   direct way.  
-->

EDITORS’ RESPONSE: Please make change:

“The design philosophy underlying UEID assumes that this construction is no longer needed, in particular because cryptographic-quality random number generators are readily available. Therefore hardware, software, and/or manufacturing processes can implement UEID in a simple and direct way. “  
  
39) <!--[rfced] Appendix C.4. We are having trouble parsing the first  
sentence below. Please let us know how we may update for clarity.  
  
Original:  
   EAT thus cannot be defined permanence in terms of defense against  
   attack. EAT's definition of permanence is in terms of operations and  
   device lifecycle.  
  
Perhaps:  
   Thus, EAT's permanence cannot be defined in terms of defense against  
   attack; it can be defined in terms of operations and device life cycle.  
-->

EDITORS’ RESPONSE: Please make change:

“For EAT, permanence is not defined in terms of resistance to attacks. Instead, it is defined in the context of operational functionality and the device lifecycle.”  
  
40) <!--[rfced] Appendix E.3. May we rephrase this text for clarity?  
Please let us know if this conveys the intended meaning.  
  
Original:  
   However, EAT is intended for use in low-security use cases  
   the same as high-security use case.  
  
Perhaps:  
   However, EAT is intended for use in both low-security and  
   high-security use cases.  
-->

EDITORS’ RESPONSE: Original text should not be changed.   
  
41) <!-- [rfced] In the html and pdf outputs, the text enclosed in <tt> is output  
in fixed-width font. In the txt output, there are no changes to the font,  
and the quotation marks have been removed.  
  
Please review carefully and let us know if the output is acceptable or if any  
updates are needed.  
-->

EDITORS’ RESPONSE: These changes were confirmed to be correct.  
  
42) <!-- [rfced] Please review whether any of the notes in this document  
should be in the <aside> element. It is defined as "a container for  
content that is semantically less important or tangential to the  
content that surrounds it" (<https://authors.ietf.org/en/rfcxml-vocabulary#aside>).  
-->

EDITORS’ RESPONSE: Editors do not feel this change is necessary.  
  
43) <!-- [rfced] Throughout the text, the following terminology appears to be used  
inconsistently. Please review these occurrences and let us know if/how they  
may be made consistent.   
  
  Claims-Set (34) vs. claims set (8)  
  Claims-Sets (3) vs. claims-sets (1) vs. claims sets (11)

EDITORS’ RESPONSE: Please change claims-sets to Claims-sets in the text, not in sourcecode elements.  Claimes-set is meant to refer to a CDDL construct, while claims set is the term-of-art.  
  
  Detached EAT Bundle vs. detached EAT bundle  
   [Note: should all instances be capitalized to match how it  
   appears in the "CBOR Tags" registry  
   (<https://www.iana.org/assignments/cbor-tags)>?]  
  
EDITORS’ RESPONSE: It is fine to change this to the capitalized version if this is the RFC Ed preference.  The capitalization in the editors' draft is based on whether the term comes at the beginning of a sentence or table entry.

EAT nonce claim vs. "eat\_nonce" claim  
   [Note: are these different or should they be consistent? One instance  
   mentions "EAT nonce claim" but points to Section 4.1, which discusses  
   the "eat\_nonce" claim:  
     One option to provide freshness is the EAT nonce claim (Section 4.1).

EDITORS’ RESPONSE: "nonce" is a term-of-art.  "EAT nonce" refers to the use of a nonce in the EAT context.  eat\_nonce is the actual claim label.  The document is consistent in this regard.  No need to change.

  "Nonce" claim vs. "nonce" claim vs. nonce claim  
  Key ID vs. key ID vs. key identifier  
  Simple TEE vs. simple TEE  
  Submodule claim vs. submodule claim

EDITORS’ RESPONSE: This was meant to be based on the appearance of the term in the sentence itself.  For instance, if "submodule claim" appeared at the beginning it would be capitalized.  In order to improve readability, editors suggest adopting that rule.  There is one instance however of "submodule claim" that was inadvertently capitalized (last sentence in 4.2.18), and the editors request RFC Ed to fix this in the revised XML.

b) FYI - We updated the following terms for consistency. Please let us know  
if any further updates are needed.  
  
  base-64 and base 64 -> base64  
  Canonical -> canonical  
  CWT Tag -> CWT tag (per RFC 8392)  
  Collision Probability -> collision probability  
  EAT Claims -> EAT claims  
  eco-system -> ecosystem  
  Simple TEE -> simple TEE  
  standards-action -> Standards Action (per RFC 8126)  
  Hexadecimal Representation -> hexadecimal representation (per other RFCs)  
  
The following terms are capitalized in RFC 9334; however, they were  
typically lowercased outside Section 2 of this document.  
  
  Attester (1 instance) -> attester  
  Endorser (1 instance) -> endorser  
  Evidence (1 instance) -> evidence

EDITORS’ RESPONSE: Changes are acceptable.  
  
c) Should "nested token" be "Nested-Token" in the following since the text  
seems to be referring to the type, or is it correct per the context?  
  
Current:  
   This CDDL uses, but does not define, Submodule or nested tokens  
   because the definition for these types varies between CBOR and JSON  
   and the JC<> generic cannot be used to define it.  
  
   The value of each entry in a submodule may be a Claims-Set, nested token,  
   or Detached-Submodule-Digest.  
-->

EDITORS’ RESPONSE: Please leave text as it stands. No change is required.  
  
44) <!-- [rfced] Abbreviations  
  
a) We have added expansions for the following abbreviations  
per Section 3.6 of RFC 7322 ("RFC Style Guide"). Please review each  
expansion in the document carefully to ensure correctness.  
  
  Company ID (CID)  
  Concise Software Identification (CoSWID)  
  Certificate Revocation List (CRL)  
  Elliptic Curve Digital Signature Algorithm (ECDSA)  
  Extended Unique Identifier (EUI)  
  Global Navigation Satellite System (GNSS)  
  Global System for Mobile Communications Association (GSMA)  
  Hashed Message Authentication Code (HMAC)  
  hardware (HW)  
  Initial Device Identifier (IDevID)  
  Internet of Things (IoT)  
  JSON Web Encryption (JWE)  
  JSON Web Signature (JWS)  
  Local Device Identifier (LDevID) (per IEEE.802.1AR)  
  Media Access Control (MAC)  
  Not a Number (NaN)  
  Organizationally Unique Identifier (OUI)  
  Software Version Number (SVN)  
  software (SW)  
  Software Identification (SWID)

EDITORS’ RESPONSE: Changes are acceptable.  
  
b) FYI, we updated this expansion to match use in past RFCs.  
  
  JavaScript Object Signing and Encryption (JOSE) (this document) vs.  
  JSON Object Signing and Encryption (JOSE) (in RFC 9052 and many other RFCs)  
-->

EDITORS’ RESPONSE: Changes are acceptable.  
  
45) <!-- [rfced] Please review the "Inclusive Language" portion of the online  
Style Guide <<https://www.rfc-editor.org/styleguide/part2/#inclusive_language>>  
and let us know if any changes are needed.  
  
For example, please consider whether the following terms should be updated:  
 - whitespace  
 - master  
 - Native  
-->

EDITORS’ RESPONSE: Editors do not see a need to change terminology as the candidate replacement terms would negatively impact the technical interpretation of the document.