

RATS
Internet-Draft
Intended status: Standards Track
Expires: 27 November 2022

L. Lundblade
Security Theory LLC
H. Birkholz
Fraunhofer SIT
T. Fossati
arm
26 May 2022

EAT Media Types
draft-lundblade-rats-eat-media-type-00

Abstract

Payloads used in Remote Attestation Procedures may require an associated media type for their conveyance, for example when used in RESTful APIs.

This memo defines media types to be used for Entity Attestation Tokens (EAT).

Discussion Venues

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

Discussion of this document takes place on the Remote Attestation Procedures Working Group mailing list (rats@ietf.org), which is archived at <https://mailarchive.ietf.org/arch/browse/rats/>.

Source for this draft and an issue tracker can be found at <https://github.com/thomas-fossati/draft-eat-mt>.

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 2022.

Copyright Notice

Copyright (c) 2022 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	2
1.1. Requirements Language	3
2. EAT Types	3
3. A Media Type Parameter for EAT Profiles	4
4. Examples	5
5. Security Considerations	5
6. IANA Considerations	5
6.1. Media Types	6
6.2. application/eat-cwt Registration	6
6.3. application/eat-jwt Registration	7
6.4. application/eat-deb+cbor Registration	7
6.5. application/eat-deb+json Registration	8
6.6. application/eat-ucs+cbor Registration	8
6.7. application/eat-ucs+json Registration	9
6.8. Content-Format	9
7. References	10
7.1. Normative References	10
7.2. Informative References	11
Acknowledgments	11
Authors' Addresses	11

1. Introduction

Payloads used in Remote Attestation Procedures [RATS-Arch] may require an associated media type for their conveyance, for example when used in RESTful APIs (Figure 1).

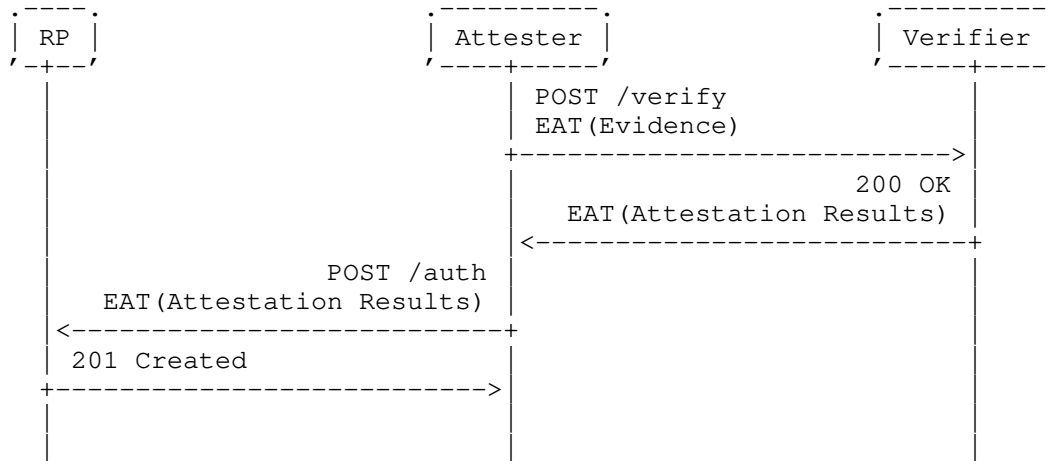


Figure 1: Conveying RATS conceptual messages in REST APIs using EAT

This memo defines media types to be used for Entity Attestation Token (EAT) [EAT] payloads independently of the RATS Conceptual Message in which they manifest themselves.

1.1. Requirements Language

This document uses the terms and concepts defined in [RATS-Arch].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. EAT Types

Figure 2 illustrates the six EAT wire formats and how they relate to each other. [EAT] defines four of them (CWT, JWT and DEB in its JSON and CBOR flavours), whilst [UCCS] defines the remaining two: UCCS and UJCS.

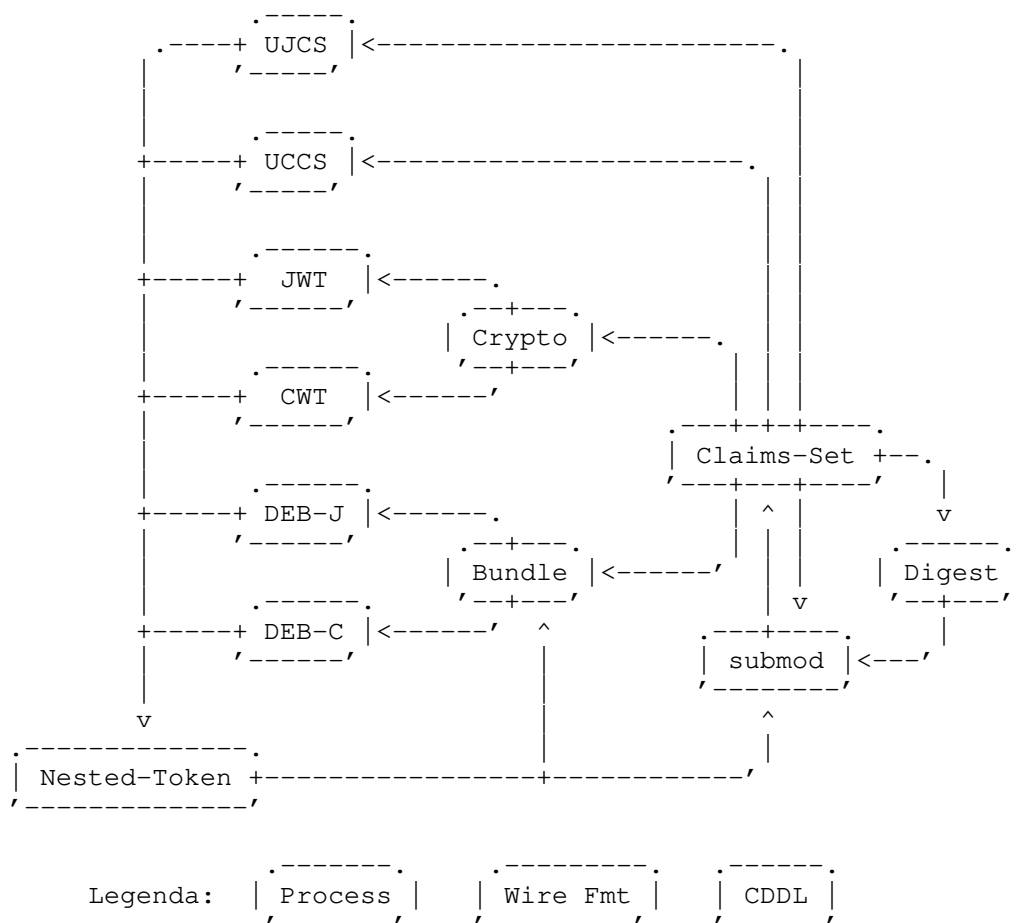


Figure 2: EAT Types

3. A Media Type Parameter for EAT Profiles

EAT is an open and flexible format. To improve interoperability, Section 7 of [EAT] defines the concept of EAT profiles. Profiles are used to constrain the parameters that producers and consumers of a specific EAT profile need to understand in order to interoperate. For example: the number and type of claims, which serialisation format, the supported signature schemes, etc. EATs carry an in-band profile identifier using the `eat_profile` claim (see Section 4.3.3 of [EAT]). The value of the `eat_profile` claim is either an OID or a URI.

The media types defined in this document include an optional profile parameter that can be used to mirror the `eat_profile` claim of the transported EAT. Exposing the EAT profile at the API layer allows API routers to dispatch payloads directly to the profile-specific processor without having to snoop into the request bodies. This design also provides a finer-grained and scalable type system that matches the inherent extensibility of EAT. The expectation being that a certain EAT profile automatically obtains a media type derived from the base (e.g., `application/eat-cwt`) by populating the profile parameter with the corresponding OID or URL.

4. Examples

The example in Figure 3 illustrates the usage of EAT media types for transporting attestation evidence.

```
POST /challenge-response/v1/session/1234567890 HTTP/1.1
Host: verifier.example
Accept: application/eat-cwt; profile=tag:ar4si.example,2021
Content-Type: application/eat-cwt; profile=tag:evidence.example,2022

[ CBOR-encoded EAT w/ profile=tag:evidence.example,2022 ]
```

Figure 3: Example REST Verification API (request)

The example in Figure 4 illustrates the usage of EAT media types for transporting attestation results.

```
HTTP/1.1 200 OK
Content-Type: application/eat-cwt; profile=tag:ar4si.example,2021

[ CBOR-encoded EAT w/ profile=tag:ar4si.example,2021 ]
```

Figure 4: Example REST Verification API (response)

In both cases the profile is carried as an explicit parameter.

5. Security Considerations

The security consideration of [EAT] and [UCCS] apply in full.

6. IANA Considerations

```
// RFC Editor: please replace RFCthis with this RFC number and remove
// this note.
```

6.1. Media Types

IANA is requested to add the following media types to the "Media Types" registry [IANA.media-types].

Name	Template	Reference
EAT CWT	application/eat-cwt	RFCthis, Section 6.2
EAT JWT	application/eat-jwt	RFCthis, Section 6.3
EAT CBOR DEB	application/eat-deb+cbor	RFCthis, Section 6.4
EAT JSON DEB	application/eat-deb+json	RFCthis, Section 6.5
EAT UCCS	application/eat-ucs+cbor	RFCthis, Section 6.6
EAT UJCS	application/eat-ucs+json	RFCthis, Section 6.7

Table 1: New Media Types

6.2. application/eat-cwt Registration

Type name: application
 Subtype name: eat-cwt
 Required parameters: n/a
 Optional parameters: "profile" (EAT profile in string format. OIDs MUST use the dotted-decimal notation. The parameter value is case-insensitive.)
 Encoding considerations: binary
 Security considerations: Section 5 of RFCthis
 Interoperability considerations: n/a
 Published specification: Section 6.1 of RFCthis
 Applications that use this media type: Attesters, Verifiers, Endorsers and Reference-Value providers, Relying Parties that need to transfer EAT payloads over HTTP(S), CoAP(S), and other transports.
 Fragment identifier considerations: n/a
 Person & email address to contact for further information: RATS WG mailing list (rats@ietf.org)
 Intended usage: COMMON
 Restrictions on usage: none
 Author/Change controller: IETF
 Provisional registration:
 // maybe

6.3. application/eat-jwt Registration

Type name: application
Subtype name: eat-jwt
Required parameters: n/a
Optional parameters: "profile" (EAT profile in string format. OIDs MUST use the dotted-decimal notation. The parameter value is case-insensitive.)
Encoding considerations: 8bit
Security considerations: Section 5 of RFCthis
Interoperability considerations: n/a
Published specification: Section 6.1 of RFCthis
Applications that use this media type: Attesters, Verifiers, Endorsers and Reference-Value providers, Relying Parties that need to transfer EAT payloads over HTTP(S), CoAP(S), and other transports.
Fragment identifier considerations: n/a
Person & email address to contact for further information: RATS WG mailing list (rats@ietf.org)
Intended usage: COMMON
Restrictions on usage: none
Author/Change controller: IETF
Provisional registration:
// maybe

6.4. application/eat-deb+cbor Registration

Type name: application
Subtype name: eat-deb+cbor
Required parameters: n/a
Optional parameters: "profile" (EAT profile in string format. OIDs MUST use the dotted-decimal notation. The parameter value is case-insensitive.)
Encoding considerations: binary
Security considerations: Section 5 of RFCthis
Interoperability considerations: n/a
Published specification: Section 6.1 of RFCthis
Applications that use this media type: Attesters, Verifiers, Endorsers and Reference-Value providers, Relying Parties that need to transfer EAT payloads over HTTP(S), CoAP(S), and other transports.
Fragment identifier considerations: n/a
Person & email address to contact for further information: RATS WG mailing list (rats@ietf.org)
Intended usage: COMMON
Restrictions on usage: none
Author/Change controller: IETF
Provisional registration:

// maybe

6.5. application/eat-deb+json Registration

Type name: application
Subtype name: eat-deb+json
Required parameters: n/a
Optional parameters: "profile" (EAT profile in string format. OIDs MUST use the dotted-decimal notation. The parameter value is case-insensitive.)
Encoding considerations: Same as [RFC7159]
Security considerations: Section 5 of RFCthis
Interoperability considerations: n/a
Published specification: Section 6.1 of RFCthis
Applications that use this media type: Attesters, Verifiers, Endorsers and Reference-Value providers, Relying Parties that need to transfer EAT payloads over HTTP(S), CoAP(S), and other transports.
Fragment identifier considerations: n/a
Person & email address to contact for further information: RATS WG mailing list (rats@ietf.org)
Intended usage: COMMON
Restrictions on usage: none
Author/Change controller: IETF
Provisional registration:
// maybe

6.6. application/eat-ucs+cbor Registration

Type name: application
Subtype name: eat-ucs+cbor
Required parameters: n/a
Optional parameters: "profile" (EAT profile in string format. OIDs MUST use the dotted-decimal notation. The parameter value is case-insensitive.)
Encoding considerations: binary
Security considerations: Section 5 of RFCthis
Interoperability considerations: n/a
Published specification: Section 6.1 of RFCthis
Applications that use this media type: Attesters, Verifiers, Endorsers and Reference-Value providers, Relying Parties that need to transfer EAT payloads over HTTP(S), CoAP(S), and other transports.
Fragment identifier considerations: n/a
Person & email address to contact for further information: RATS WG mailing list (rats@ietf.org)
Intended usage: COMMON
Restrictions on usage: none

Author/Change controller: IETF
Provisional registration:
// maybe

6.7. application/eat-ucs+json Registration

Type name: application
Subtype name: eat-ucs+json
Required parameters: n/a
Optional parameters: "profile" (EAT profile in string format. OIDs MUST use the dotted-decimal notation. The parameter value is case-insensitive.)
Encoding considerations: Same as [RFC7159]
Security considerations: Section 5 of RFCthis
Interoperability considerations: n/a
Published specification: Section 6.1 of RFCthis
Applications that use this media type Attesters, Verifiers, Endorsers and Reference-Value providers, Relying Parties that need to transfer EAT payloads over HTTP(S), CoAP(S), and other transports.
Fragment identifier considerations: n/a
Person & email address to contact for further information: RATS WG mailing list (rats@ietf.org)
Intended usage: COMMON
Restrictions on usage: none
Author/Change controller: IETF
Provisional registration:
// maybe

6.8. Content-Format

| (*Issue*: need a way to pass the profile information when using
| content formats. A new CoAP option?)

IANA is requested to register a Content-Format number in the "CoAP Content-Formats" sub-registry, within the "Constrained RESTful Environments (CoRE) Parameters" Registry [IANA.core-parameters], as follows:

Content-Type	Content Coding	ID	Reference
application/eat-cwt	-	TBD1	RFcthis
application/eat-jwt	-	TBD2	RFcthis
application/eat-deb+cbor	-	TBD3	RFcthis
application/eat-deb+json	-	TBD4	RFcthis
application/eat-ucs+cbor	-	TBD5	RFcthis
application/eat-ucs+json	-	TBD6	RFcthis

Table 2: New Content-Formats

TBD1..6 are to be assigned from the space 256..999.

In the registry as defined by Section 12.3 of [CoAP] at the time of writing, the column "Content-Type" is called "Media type" and the column "Content Coding" is called "Encoding".

// RFC editor: please remove this paragraph.

7. References

7.1. Normative References

- [CoAP] 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/rfc/rfc7252>>.
- [EAT] Lundblade, L., Mandyam, G., and J. O'Donoghue, "The Entity Attestation Token (EAT)", Work in Progress, Internet-Draft, draft-ietf-rats-eat-13, 20 May 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-rats-eat-13>>.
- [IANA.core-parameters] IANA, "Constrained RESTful Environments (CoRE) Parameters", <<https://www.iana.org/assignments/core-parameters>>.
- [IANA.media-types] IANA, "Media Types", <<https://www.iana.org/assignments/media-types>>.

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/rfc/rfc2119>>.
- [RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, <<https://www.rfc-editor.org/rfc/rfc7159>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/rfc/rfc8174>>.
- [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-02, 12 January 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-rats-uccs-02>>.

7.2. Informative References

- [RATS-Arch] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote Attestation Procedures Architecture", Work in Progress, Internet-Draft, draft-ietf-rats-architecture-16, 24 May 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-rats-architecture-16>>.

Acknowledgments

TODO

Authors' Addresses

Laurence Lundblade
Security Theory LLC
Email: lg1@securitytheory.com

Henk Birkholz
Fraunhofer Institute for Secure Information Technology
Rheinstrasse 75
64295 Darmstadt
Germany
Email: henk.birkholz@sit.fraunhofer.de

Thomas Fossati
arm
Email: thomas.fossati@arm.com