RATS Working Group H. Birkholz
Internet-Draft M. Eckel
Intended status: Standards Track Fraunhofer SIT
Expires: September 11, 2020 March 10, 2020

A CWT Claims Set Definition for RATS Endorsement Tokens
draft-birkholz-rats-endorsement-eat-00

Abstract

An Endorsement is defined by the RATS Architecture as a "secure statement that some entity (typically a manufacturer) vouches for the integrity of an Attester's signing capability". This documents defines Claims to be used in CBOR Web Tokens in the same fashion attestation Evidence can be represented via Entity Attestation Tokens (EAT). The defined Claims can be included in Endorsement Tokens. Endorsement Tokens can be provided by a manufacturer or a third party authority to vouch for the capabilities and characteristics of a hardware component a RATS Attester is not capable to create Evidence about.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Remote ATtestation procedureS (RATS) can be used to establish trust in the trustworthiness of a remote peer (the Attester). As a Relying Party typically cannot evaluate every kind of Attester by itself, the RATS architecture [I-D.ietf-rats-architecture] defines the Verifier role, to off-load the burden of appraisal to another entity than the Relying Party itself. The duty of a Verifier is to produce Attestation Results that are then easier to digest by a Relying Party in comparison to Evidence that can potentially be both large and/or esoteric for a generic Relying Party. Evidence are believable Claims about the Attester. Next to Evidence, a Verifier requires Endorsements. Endorsements are signed documents that include Claims about components of an Attester that an Attester cannot create Evidence about. Very prominent examples are Roots of Trust, such as a Static Code Root of Trust for Measurement as defined in the Trusted Computing Group (TCG) Glossary [TCGGLOSS]. These Endorsements of components of a composite device are typically provided by their manufacturer, a corresponding supply chain entity that assembles a composite device, or a certification authority.

This documents defines CBOR Web Token (CWT, [RFC8392]) Claims that can be assembled into a CWT Claims Set to compose Endorsement Tokens.

This is done in the same fashion as Claims are assembled into Entity Attestation Tokens [I-D.ietf-rats-eat] that can represent, for example, attestation Evidence for RATS.

1.1. Terminology

This document uses the terms Claims, Claims Set, and CBOR Web Token Claims set as defined in [RFC8392].

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. Endorsement Claims Definition

This section uses the same definition style for Claims as introduced in [I-D.ietf-rats-eat]. New Claims to be used in Endorsement Tokens are specified below. A JSON Web Token Claims (JWT, [RFC7519]) definition is out-of-scope of this document. Corresponding Claims are (to be) registered in the 'CWT Claims' subregistry of [IANA.cwt].

Each Claim definition is accompanied by a value definition using the Concise Data Definition Language (CDDL, [RFC8610]). An Endorsement Token that is using Claims that are defined in this document MUST include Claim values as specified in this document.

2.1. Component Manufacturer Claim

As a fall-back alternative to the more specific oemid Claim defined in [I-D.ietf-rats-eat], this Claim allows for byte strings representing entity identifiers that are not based on IEEE MA-L, MA-M, MA-S or an IEEE CID [IEEE.RA].

```
manufacturer-endorsement-claim = (
  manufacturer-endorsement => bytes,
)
```

2.2. Component Version Claim

A byte string representing a firmware version of a hardware component. Potentially, the value is derived from multiple version numbers, such as major and minor version number. The version represents the hardware component at the time the Endorsement Token was created, typically during manufacturing.

Note to the reader: in this -00 I-D there are only five exemplary Claims included yet. This list is far from complete or polished.

```
version-endorsement-claim = (
  version-endorsement => bytes,
)
```

2.3. Component Model Claim

A manufacturer-specific byte string that represents the part number or a similar model identifier as defined by the manufacturer.

```
model-endorsement-claim = (
  model-endorsement => bytes,
)
```

2.4. Field Upgradable Claim

A Claim that indicates if the firmware of a hardware component is mutable and therefore can be updated after manufacturing or not.

```
field-upgradable-claim = (
  field-upgradable => bool,
)
```

2.5. Shielded Secret Origination Claim

An indicator that shows if a securely stored secret key in the hardware component was generated by a function internal to the hardware component or if the secret key was enrolled in a secure and controlled environment by the manufacturer.

```
secret-origination-claim = (
  secret-origination => internal / external
)

internal = 0
external = 1
```

2.6. Common Criteria Claim

A reference to the specification document that includes evaluation results and parameters as defined by Common Criteria. This Claim value is a composite of an URI pointing to the specification document as well as a hash value specification document to ensure its authenticity. The hash entry is a composite of an algorithm ID as defined by the IANA "Named Information Hash Algorithm Registry" and the hash value as a byte string.

```
   common-criteria-claim =(
     common-criteria => [ any-uri,
                          hash,
                        ]
   )

   any-uri = text

   hash = [ hash-alg-id: int,
            hash-value: bytes,
          ]
```

3. Privacy Considerations

Potentially

4. Security Considerations

Most likely a sub-set of the trust relationships corresponding to the RATS architecture

5. IANA Considerations

In this section the Claim registration in [IANA.cwt] for the corresponding Claim definition above will be elaborated on.

6. References

6.1. Normative References

[IANA.cwt]
IANA, "CBOR Web Token (CWT) Claims", <http://www.iana.org/assignments/cwt>.

[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>.

[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>.

[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., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/info/rfc8610>.

6.2. Informative References

[I-D.ietf-rats-architecture] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote Attestation Procedures Architecture", draft-ietf-rats-architecture-02 (work in progress), March 2020.

[I-D.ietf-rats-eat] Mandyam, G., Lundblade, L., Ballesteros, M., and J. O'Donoghue, "The Entity Attestation Token (EAT)", draft-ietf-rats-eat-03 (work in progress), February 2020.

[IEEE.RA] "IEEE Registration Authority", <https://standards.ieee.org/products-services/regauth/index.html>.

[TCGGLOSS] TCG, "TCG Glossary Version 1.1 Revision 1.00", May 2017, <https://trustedcomputinggroup.org/wp-content/uploads/TCG-Glossary-V1.1-Rev-1.0.pdf>.

Authors' Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
Darmstadt 64295

Email: henk.birkholz@sit.fraunhofer.de

Michael Eckel
Fraunhofer SIT
Rheinstrasse 75
Darmstadt 64295
Germany

Email: michael.eckel@sit.fraunhofer.de