Remote ATtestation ProcedureS
Internet-Draft
Intended status: Standards Track
Expires: 28 November 2025

H. Birkholz
Fraunhofer SIT
M. Richardson
Sandelman Software Works
C. Liu
Huawei Technologies

27 May 2025

MUD-Based RATS Resources Discovery
draft-ietf-iotops-mud-rats-01

Abstract

Manufacturer Usage Description (MUD) files and the MUD URIs that point to them are defined in RFC 8520. This document introduces a new type of MUD file to be delivered in conjunction with a MUD file signature and/or to be referenced via a MUD URI embedded in other documents or messages, such as an IEEE 802.1AR Secure Device Identifier (DevID) or a CBOR Web Token (CWT). These signed documents can be presented to other entities, e.g., a network management system or network path orchestrator. If this entity also takes on the role of a verifier as defined by the IETF Remote ATtestation procedureS (RATS) architecture, this verifier can use the references included in the MUD file specified in this document to discover, for example, appropriate reference value providers, endorsement documents or endorsement distribution APIs, trust anchor stores, remote verifier services (sometimes referred to as Attestation Verification Services), or transparency logs. All theses references in the MUD file pointing to resources and auxiliary RATS services can satisfy general RATS prerequisite by enabling discovery or improve discovery resilience of corresponding resources or services.

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 28 November 2025.

Table of Contents

1. Introduction

Verifiers, Endorsers, and Attesters are roles defined in the RATS Architecture [RFC9334]. In the RATS architecture, the Relying Party roles depend on the Verifier to bear the burden of Evidence appraisal and to generate corresponding Attestation Results for them. Attestation Results compose a believable chunk of information that can be digested by Relying Parities in order to assess an Attester's trustworthiness. The assessment of a remote peer's trustworthiness is vital to determine whether any future protocol interaction between a Relying Party and a remote Attester can be considered secure. To create these Attestation Results to be consumed by Relying Parties, the Attestation Evidence an Attester generates has to be appraised by one or more appropriate Verifiers.

This document defines a procedure that enables the discovery of resources or services in support of RATS, including:

1. Reference Values,

2. Trust Anchors,

3. Endorsements and Endorsement Distribution APIs,

4. (remote) Verifier APIs,

5. Transparency Logs, or

6. Appraisal Policies.

MUD URIs can be embedded in any data item that was signed with trusted key material. One common way to establish trust in a signed data item is to associate the signing key material with a trust anchor via a certification path (see [RFC4949] for trust anchor and certification path). This document defines the use of MUD URIs embedded in two types of signed data items that typically are trusted via certification paths:

1. Secure Device Identifiers (IEEE 802.1AR DevIDs) as defined by [RFC8520] and

2. Entity Attestation Tokens (EAT) as defined by [I-D.ietf-rats-eat].

DevIDs and EATs (essentially CWTs) are two very prominent examples of "trustworthy documents" (TDs) with a binary format and the embedding of MUD URIs in theses TDs can be applied to other TD types, for example, Selective Disclosure CWTs [I-D.ietf-spice-sd-cwt].

Other TDs are out-of-scope of this specification, though. The TDs are typically enrolled on Attesters by manufacturers or provisioned by supply chain entities with appropriate authority. The TDs can be presented to local Network Management Systems, AAA-services (e.g., via IEEE 802.1X), or other points of first contact (POFC), for example, [RFC8071]. These POFC are typically trusted third parties (TTP) that can digest the TDs and then base trust decisions on the associated certification paths and trust anchors. If a TD presented by the Attester is deemed to be trusted by a local trust authority, the MUD URI embedded is considered to be a trusted source for viable resources and services in support of remote attestation of the Attester.

This specification does not define the shape or format of any resource or service that is referenced by the MUD file. In support of a unified mechanism to categorize the formats of referenced resources, a conceptual message wrapper (CMW, [I-D.ietf-rats-msg-wrap] is used for each type of resource. An example of a referenced resource is a CoRIM tag [I-D.ietf-rats-corim].

1.1. Requirements Notation

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. MUD URIs in Trusted Documents (TDs)

This document does neither modify nor augment the definition about how to compose a MUD URI. The two types of trusted documents (TDs) covered by this specification are Secure Device Identifiers and Entity Attestation Tokens.

2.1. MUD URIs in DevIDs

[RFC8520] defines the format of how to embed MUD URIs in DevIDs and that specification is used in this document.

2.2. MUD URIs in EATs

To embed a MUD URI in an EAT, the mud-uri claim specified in this document MUST be used.

3. MUD File Signatures

As the resources required by a Verifier's appraisal procedures have to be trustworthy, a MUD signature file for a corresponding MUD File MUST be available. The MUD File MUST include a reference to its MUD signature file via the 'mud-signature' statement. The MUD File Signature generation as specified in Section 13.1 of [RFC8520] applies. If a MUD file changed (i.e., the checking of the MUD File Signature fails) or the corresponding MUD File Signer certificate is expired (see Section 13.2 of [RFC8520], the reference in the changed MUD File MUST point to a new valid MUD Signature File and that new MUD File Signature MUST be available. If a corresponding MUD File Signer certificate is expired (see Section 13.2 of [RFC8520]) or a MUD File Signature referenced by a MUD File cannot be checked successfully, the MUD File MUST NOT be trusted.

3.1. MUD File Signer in DevIDs

[RFC8520] defines the format of how to embed a reference to the signing certificate in DevIDs and that specification applies to this specification.

3.2. MUD File Signer in EATs

To embed a reference to a MUD File Signer in an EAT, the mud-signer claim specified in this document MUST be used and the mud-uri claim MUST be present. The value of the mud-signer claim is a CBOR byte-wrapped subject field of the signing certificate of the MUD File as specified in Section 11 of [RFC8520].

4. Trusting MUD URIs and MUD Files

The level of assurance about the authenticity of a MUD URI embedded in a TD is based on the level of trust put into the corresponding trust anchor associated with the key material that signed the TD. If it is not possible to establish a level of trust towards the entity that signed a TD, the embedded MUD URI SHOULD NOT be trusted. In some usage scenarios it might suffice to trust a MUD File, if the referenced MUD File Signer's certificate is not expired, but that behavior is NOT RECOMMENDED.

The level of assurance about the authenticity of a MUD file is based on the level of trust put into the entity that created the corresponding MUD File Signer's certificate. If it is not possible to establish a level of trust into the corresponding trust anchor associated with the MUD Signer's certificate, the MUD File that references that MUD Signer MUST NOT be trusted.

4.1. Trusting RATS Resources Referenced by a MUD File

Resources, e.g., RATS Conceptual Messages, that are referenced by a MUD File MUST be signed (e.g., via a COSE_Sign1 envelope). The signing procedures, the format of corresponding identity documents, and the establishment of trust relationships associated with these resources are out-of-scope of this document.

5. Specification of RATS MUD Files Referenced by MUD URIs

The MUD URI embedded in a TD presented by an Attester points to a MUD File. MUD URIs typically point to a piece of data that is a YANG-modeled XML file with a structure specified in the style of a YANG module definition ([RFC7950] and corresponding updates: [RFC8342], [RFC8526]). This document specifies a YANG module augment definition for generic MUD files to create RATS MUD files. The following definition MUST be used, if a MUD URI points to a RATS MUD file.

5.1. Tree Diagram

The following tree diagram [RFC8340] provides an overview of the data model for the "ietf-mud-rats" module augment.

```
<CODE BEGINS>
module: ietf-mud-rats
  augment /mud:mud:
    +--rw ras
    |  +--rw ras-uris*   inet:uri
    +--rw rim
    |  +--rw rim-uris*   inet:uri
    +--rw edt
       +--rw edt-uris*   inet:uri
<CODE ENDS>
```

5.2. YANG Module

This YANG module has normative references to [RFC6991] and augments [RFC8520].

```
<CODE BEGINS> file ietf-mud-rats@2025-02-09.yang
module ietf-mud-rats {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-mud-rats";
  prefix "mud-rats";

  import ietf-mud {
    prefix "mud";
  }
```

```
     import ietf-inet-types {
       prefix "inet";
     }

     organization
       "IETF RATS (Remote ATtestation procedureS) Working Group";

     contact
       "WG Web: http://tools.ietf.org/wg/rats/
        WG List: rats@ietf.org
        Author: Eliot Lear <lear@cisco.com>
        Author: Henk Birkholz <henk.birkholz@sit.fraunhofer.de>";

     description
       "This YANG module augments the ietf-mud model to provide for three
        optional lists to enable Remote Attestation Procedures so that
        this device type may be used as a controller for other
        MUD-enabled devices.

        Copyright (c) 2020 IETF Trust and the persons identified as
        authors of the code.  All rights reserved.

        Redistribution and use in source and binary forms, with or
        without modification, is permitted pursuant to, and subject to
        the license terms contained in, the Simplified BSD License set
        forth in Section 4.c of the IETF Trust's Legal Provisions
        Relating to IETF Documents
        (https://trustee.ietf.org/license-info).

        This version of this YANG module is part of RFC XXXX
        (https://www.rfc-editor.org/info/rfcXXXX); see the RFC itself
         for full legal notices.

        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 (RFC 2119) (RFC 8174) when, and only when,
        they appear in all capitals, as shown here.";

     revision 2020-03-09 {
       description
         "Initial proposed standard.";
          reference "RFC XXXX: MUD Extension to find RATS supply chain
          entity resources: remote attestation services, endorsement
          documents, and reference integrity measurement";
     }

     grouping mud-rats-grouping {
```

```
      description
        "Grouping to locate RATS services";
      container ras {
        description
          "Lists of Remote Attestation Service
           (RAS/Verifiers) candidates.";
        leaf-list ras-uris {
          type inet:uri;
          description
            "A list of Verifiers that can appraise evidence produced by
             the entity that presents a DevID including this MUD URI.";
        }
      }
      container rim {
        description
          "Lists of Reference Integrity Measurement (RIM) candidates.";
        leaf-list rim-uris {
          type inet:uri;
          description
            "A list of RIM CoSWID that provide reference integrity
             measurements represented as signed CoSWID using
             the CoSWID RIM extension.";
        }
      }
      container edt {
        description
          "List of Endorsements for Roots of Trusts (e.g. Endorsement
           Key Certificates).";
        leaf-list edt-uris {
          type inet:uri;
          description
            "A list of Endorsements that vouch for the characteristics
             of Roots of Trusts the entity possesses.";
        }
      }
    }
    augment "/mud:mud" {
      uses mud-rats-grouping;
      description
        "add mud-rats URI resources";
    }
  }
  <CODE ENDS>
```

6. Privacy Considerations

The privacy considerations of RFC 9334 apply.

7. Security Considerations

The trust model and Security Considerations of RFC 8520 and RFC 9334 apply.

8. IANA Considerations

// RFC Editor: Please replace "RFCthis" with the RFC number assigned to this document.

// RFC Editor: This document uses the CPA (code point allocation) convention described in [I-D.bormann-cbor-draft-numbers]. For each usage of the term "CPA", please remove the prefix "CPA" from the indicated value and replace the residue with the value assigned by IANA; perform an analogous substitution for all other occurrences of the prefix "CPA" in the document. Finally, please remove this note.

8.1. CWT mud-uri Claim Registration

IANA is requested to add the new mud-uri CBOR Web Token claim to the "CBOR Web Token (CWT) Claims" registry [IANA.cwt] in the Standards Action Range as follows:

* Claim Name: mud-uri
* Claim Description: A CBOR byte-wrapped MUD URI as specified in [RFC8520]
* JWT Claim Name: mud-uri
* Claim Key: CPA109
* Claim Value Type(s): CBOR byte string
* Change Controller: IETF
* Specification Document(s): Section 2.2 of RFCthis

8.2. CWT mud-signer Claim Registration

IANA is requested to add the new mud-signer CBOR Web Token claim to the "CBOR Web Token (CWT) Claims" registry group [IANA.cwt] in the Standards Action Range as follows:

* Claim Name: mud-uri

* Claim Description: A CBOR byte-wrapped subject field of the signing certificate for a MUD file as specified in [RFC8520]

* JWT Claim Name: mud-signer

* Claim Key: CPA110

* Claim Value Type(s): CBOR byte string

* Change Controller: IETF

* Specification Document(s): Section 3.2 of RFCthis

8.3. JWT mud-uri Claim Registration

IANA is requested to add the new mud-signer JSON Web Token Claim to the "JSON Web Token (JWT)" registry group [IANA.jwt] as follows:

* Claim Name: mud-signer

* Claim Description: A MUD signer reference represented via a URI text string as defined by [RFC8520]

* Change Controller: IETF

* Specification Document(s): Section 2.2 of RFCthis

8.4. JWT mud-signer Claim Registration

IANA is requested to add the new mud-signer JSON Web Token Claim to the "JSON Web Token (JWT)" registry group [IANA.jwt] as follows:

* Claim Name: mud-signer

* Claim Description: A MUD signer reference represented via a URI text string as defined by [RFC8520]

* Change Controller: IETF

* Specification Document(s): Section 2.2 of RFCthis

9. References

9.1. Normative References

[I-D.ietf-rats-corim]
Birkholz, H., Fossati, T., Deshpande, Y., Smith, N., and W. Pan, "Concise Reference Integrity Manifest", Work in

Progress, Internet-Draft, draft-ietf-rats-corim-07, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-corim-07>.

[I-D.ietf-rats-eat] Lundblade, L., Mandyam, G., O'Donoghue, J., and C. Wallace, "The Entity Attestation Token (EAT)", Work in Progress, Internet-Draft, draft-ietf-rats-eat-31, 6 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-eat-31>.

[I-D.ietf-rats-msg-wrap] Birkholz, H., Smith, N., Fossati, T., Tschofenig, H., and D. Glaze, "RATS Conceptual Messages Wrapper (CMW)", Work in Progress, Internet-Draft, draft-ietf-rats-msg-wrap-14, 21 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-msg-wrap-14>.

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

[IANA.jwt] IANA, "JSON Web Token (JWT)", <https://www.iana.org/assignments/jwt>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://doi.org/10.17487/RFC2119>.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://doi.org/10.17487/RFC6991>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://doi.org/10.17487/RFC7950>.

[RFC8071] Watsen, K., "NETCONF Call Home and RESTCONF Call Home", RFC 8071, DOI 10.17487/RFC8071, February 2017, <https://doi.org/10.17487/RFC8071>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://doi.org/10.17487/RFC8174>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://doi.org/10.17487/RFC8340>.

[RFC8342] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "Network Management Datastore Architecture (NMDA)", RFC 8342, DOI 10.17487/RFC8342, March 2018, <https://doi.org/10.17487/RFC8342>.

[RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", RFC 8520, DOI 10.17487/RFC8520, March 2019, <https://doi.org/10.17487/RFC8520>.

[RFC8526] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "NETCONF Extensions to Support the Network Management Datastore Architecture", RFC 8526, DOI 10.17487/RFC8526, March 2019, <https://doi.org/10.17487/RFC8526>.

[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://doi.org/10.17487/RFC9334>.

9.2. Informative References

[I-D.bormann-cbor-draft-numbers] Bormann, C., "Managing CBOR codepoints in Internet-Drafts", Work in Progress, Internet-Draft, draft-bormann-cbor-draft-numbers-05, 1 March 2025, <https://datatracker.ietf.org/doc/html/draft-bormann-cbor-draft-numbers-05>.

[I-D.ietf-spice-sd-cwt] Prorock, M., Steele, O., Birkholz, H., and R. Mahy, "SPICE SD-CWT", Work in Progress, Internet-Draft, draft-ietf-spice-sd-cwt-03, 2 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-spice-sd-cwt-03>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://doi.org/10.17487/RFC4949>.

Authors' Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
Darmstadt
Email: henk.birkholz@ietf.contact

Michael Richardson
Sandelman Software Works
Canada
Email: mcr+ietf@sandelman.ca

Chunchi Liu
Huawei Technologies
Email: liuchunchi@huawei.com