RATS Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 11, 2020

H. Birkholz
Fraunhofer SIT
March 10, 2020

MUD-Based RATS Resources Discovery
draft-birkholz-rats-mud-00

Abstract

Manufacturer Usage Description (MUD) files and the MUD URI 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 an IEEE 802.1AR Secure Device Identifier (DevID). A DevID is a device specific pub-key identity document that can be presented to other entities, e.g. a network management system. If this entity is also a verifier as defined by the IETF Remote ATtestation procedureS (RATS) architecture, this verifier can use the references found in the MUD file specified in this document in order to discover appropriate Reference Integrity Measurements (RIM), Endorsement Documents, or even globally suitable Remote Attestation Services (RAS). All three types of theses resources are required to conduct RATS. Hence, the MUD file defined in this document enables remote attestation procedures by supporting the discovery of these required resources or services.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Verifiers, Endorsers, and Attesters are roles defined in the RATS Architecture [I-D.ietf-rats-architecture]. In the RATS architecture, the Attester role relies on the Verifier and Endorser roles to enable the appraisal of Attestation Evidence produced by said Attesters; and to create corresponding Attestation Results. 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 steer any future protocol interaction between the Attester and the remote Relying Party. To create these Attestation Results to be consumed by Relying Parties, the Attestation Evidence an Attester creates has to be processed by one or more appropriate Verifiers.

This document defines a procedure that enables the discovery of viable resources for RATS services in a local scope: 1.) Reference Integrity Measurements, and 2.) Endorsement documents.

Additionally, a third option is provided: this document defines the option to enable the discovery of remote Verfiers: 3.) Remote Attestation Services (RAS) in a global scope (if no local trusted authorities are available).

Attestation Policies and Endorsements are required to enable an appropriate appraisal of Attestation Evidence in a fashion that helps Relying Parties to digest the corresponding Attestation Results. This document defines the use of MUD URIs embedded in Secure Device Identifiers (IEEE 802.1AR DevIDs) as defined by [RFC8520]. These DevIDs are enrolled on the Attester by manufacturers or related supply chain entities with appropriate authority. The DevIDs can be presented to local Network Management Systems, AAA-services (e.g. via IEEE 802.1X), or other points of first contact (e.g. [RFC8071]) in a local scope. These local entities of authority can digest the DevID and conduct trust decisions based on the DevID by tracing associated certification paths and trust anchors [RFC4949]. If the DevID presented by the Attester is deemed to be trusted by the local trust authority, the MUD URI embedded is considered to be a trusted source of viable (and if their Identity Documents are also to be trusted - believable) Attestation Policies, Endorsements, and even globally available RAS.

In essence, the MUD file that is referenced by the DevID presented refers to sources of Attestation Policies and Endorsements recommended by the manufacturer or related supply chain entities with appropriate authority. These sources are required by appraisal procedures conducted by Verifiers in order to create well-founded Attestation Results. For example, trusted Endorses can enrich Attestation Results by vouching for the quality of hardware components, the composition of a Composite Attester, or other security characteristics of an Attester.

This specification does not define the format of Attestation Policies and Endorsement documents. A type of Attestation Policies and their representation is defined in [I-D.birkholz-rats-coswid-rim]. A specific format of Endorsements for hardware components based on [I-D.ietf-rats-eat] is defined in [I-D.birkholz-rats-endorsement-eat].

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 DevIDs

The MUD URI embedded in a DevID presented by an Attester points to a MUD file. [RFC8520] defines the format of how to embed MUD URIs in Secure Device Identifiers. This document uses this specification and does neither modify nor augment the definition about how to compose a MUD URI.

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 also include a reference to its MUD signature file via the 'mud-signature' statement. A MUD signature MAY be referenced in the DevID, but entities consuming this information must be aware that a MUD File can change. If MUD file changed (the MUD signature in the DevID does not match any more), a MUD signature file referenced in the MUD File itself MUST exist and MUST be available. If both the signature embedded in a DevID and referenced by a MUD File do not match, the MUD File SHOULD NOT be trusted.

4. Trusting MUD URIs and MUD Files

The level of assurance about the integrity of a MUD URI embedded in a DevID is based on the level of trust put into the corresponding trust anchor associated with the DevID. If you cannot establish a level of trust towards the entity that signed a DevID (the signer), the embedded MUD URI SHOULD NOT be trusted.

The level of assurance about the integrity of a MUD file is based on the level of trust put into the entity that created the corresponding MUD File Signature. If you cannot establish a level of trust put into the corresponding trust anchor associated with the MUD signature file, the referenced MUD File SHOULD NOT be trusted.

4.1. Trusting RATS Resources referenced by a MUD File

Reference Integrity Measurements and Endorsement documents that are referenced by a MUD File MUST be signed. 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 DevID presented by an Attester points to a MUD File. At the time of writing this -00 I-D, MUD URIs always 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@2019-03-09.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

Potentially

7. Security Considerations

Most likely a summary of the trust relationship corresponding to the RATS architecture

8. References

8.1. Normative References

[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>.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://www.rfc-editor.org/info/rfc6991>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8071] Watsen, K., "NETCONF Call Home and RESTCONF Call Home", RFC 8071, DOI 10.17487/RFC8071, February 2017, <https://www.rfc-editor.org/info/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://www.rfc-editor.org/info/rfc8174>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/info/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://www.rfc-editor.org/info/rfc8342>.

[RFC8520] Lear, E., Droms, R., and D. Romascanu, "Manufacturer Usage Description Specification", RFC 8520, DOI 10.17487/RFC8520, March 2019, <https://www.rfc-editor.org/info/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://www.rfc-editor.org/info/rfc8526>.

8.2. 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.

[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>.

Author's Address

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
Darmstadt 64295
Germany

Email: henk.birkholz@sit.fraunhofer.de