Workgroup: Remote ATtestation ProcedureS
Internet-Draft:
draft-wallace-rats-concise-ta-stores-00
Published: 22 June 2022
Intended Status: Standards Track
Expires: 24 December 2022
Authors: C. Wallace R. Housley
Red Hound Vigil Security

Concise TA Stores (CoTS)

Abstract

Trust anchor (TA) stores may be used for several purposes in the Remote Attestation Procedures (RATS) architecture including verifying endorsements, reference values, digital letters of approval, attestations, or public key certificates. This document describes a Concise Reference Integrity Manifest (CoRIM) extension that may be used to convey optionally constrained trust anchor stores containing optionally constrained trust anchors in support of these purposes.

About This Document

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

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-wallace-rats-concise-ta-stores/.

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

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 24 December 2022.

Table of Contents

1. Introduction

The RATS architecture [I-D.draft-ietf-rats-architecture] uses the definition of a trust anchor from [RFC6024]: "A trust anchor

represents an authoritative entity via a public key and associated data. The public key is used to verify digital signatures, and the associated data is used to constrain the types of information for which the trust anchor is authoritative." In the context of RATS, a trust anchor may be a public key or a symmetric key. This document focuses on trust anchors that are represented as public keys.

The Concise Reference Integrity Manifest (CoRIM) [I-D.draft-birkholz-rats-corim] specification defines a binary encoding for reference values using the Concise Binary Object Representation (CBOR) [RFC8949]. Amongst other information, a CoRIM may include key material for use in verifying evidence from an attesting environment (see section 3.11 in [I-D.draft-birkholz-rats-corim]). The extension in this document aims to enable public key material to be decoupled from reference data for several reasons, described below.

Trust anchor (TA) and certification authority (CA) public keys may be less dynamic than the reference data that comprises much of a reference integrity manifest (RIM). For example, TA and CA lifetimes are typically fairly long while software versions change frequently. Conveying keys less frequently and indepedent from reference data enables a reduction in size of RIMs used to convey dynamic information and may result in a reduction in the size of aggregated data transferred to a verifier. CoRIMs themselves are signed and some means of conveying CoRIM verification keys is required, though ultimately some out-of-band mechanism is required at least for bootstrapping purposes. Relying parties may verify attestations from both hardware and software sources and some trust anchors may be used to verify attestations from both hardware and software sources, as well. The verification information included in a CoRIM optionally includes a trust anchor, leaving trust anchor management to other mechanisms. Additionally, the CoRIM verification-map structure is tied to CoMIDs, leaving no simple means to convey verification information for CoSWIDs [I-D.draft-ietf-sacm-coswid].

This document defines means to decouple TAs and CAs from reference data and adds support for constraining the use of trust anchors, chiefly by limiting the environments to which a set of trust anchors is applicable. This constraints mechanism is similar to that in [fido-metadata] and [fido-service] and should align with existing attestation verification practices that tend to use per-vendor trust anchors. TA store instances may be further constrained using coarse-grained purpose values or a set of finer-grained permitted or excluded claims. The trust anchor formats supported by this draft allow for per-trust anchor constraints, if desired. Conveyance of trust anchors is the primary goal, CA certificates may optionally be included for convenience.

1.1. Constraints

This document aims to support different PKI architectures including scenarios with various combinations of the following characteristics:

- TA stores that contain a TA or set of TAs from a single organization
- TA stores that contain a set of TAs from multiple organizations
- TAs that issue certificates to CAs within the same organiation as the TA
- TAs that issue certificates to CAs from multiple organizations
- CAs that issue certificates that may be used to verify attestations or certificates from the same organization as the TA and CA
- CAs that issue certificates that may be used to verify attestations or certificates from multiple organizations

Subsequent specifications may define extensions to express constraints as well as processing rules for evaluating constraints expressed in TA stores, TAs, CA certificates and end entity (EE) certificates. Support for constraints is intended to enable misissued certificates to be rejected at verification time. Any public key that can be used to verify a certificate is assumed to also support verification of revocation information, subject to applicable constraints defined by the revocation mechanism.

2. Conventions and Definitions

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.

3. Trust anchor management for RATS

Within RATS, trust anchors may be used to verify digital signatures for a variety of objects, including entity attestation tokens (EATs), CoRIMs, X.509 CA certificates (possibly containing endorsement information), X.509 EE certificates (possibly containing endorsement or attestation information), other attestation data, digital letters of approval [dloa], revocation information, etc. Depending on context, a raw public key may suffice or additional information may be required, such as subject name or subject public

key identifier information found in an X.509 certificate. Trust anchors are usually aggregated into sets that are referred to as "trust anchor stores". Different trust anchor stores may serve different functional purposes.

Historically, trust anchors and trust anchor stores are not constrained other than by the context(s) in which a trust anchor store is used. The path validation algorithm in [RFC5280] only lists name, public key, public key algorithm and public key parameters as the elements of "trust anchor information". However, there are environments that do constrain trust anchor usage. The RPKI uses extensions from trust anchor certificates as defined in [RFC3779]. FIDO provides a type of constraint by grouping attestation verification root certificates by authenticator model in [fido-metadata].

This document aims to support each of these types of models by allowing constrained or unconstrained trust anchors to be grouped by abstract purpose, i.e., similar to traditional trust anchor stores, or grouped by a set of constraints, such as vendor name.

3.1. TA and CA conveyance

An unsigned concise TA stores object is a list of one or more TA stores, each represented below as a concise-ta-store-map element.

```
concise-ta-stores
  concise-ta-store-map #1
  ...
  concise-ta-store-map #n
```

Each TA store instance identifies a target environment and features one or more public keys. Optional constraints on usage may be defined as well.

```
concise-ta-store-map
  language
  store-identity
  target environment
  abstract coarse-grained constraints on TA store usage
  concrete fine-grained constraints on TA store usage
  public keys (possibly included per-instance constraints)
```

The following sections define the structures to support the concepts shown above.

3.1.1. The concise-ta-stores Container

The concise-ta-stores type is the root element for distrbuting sets of trust anchor stores. It contains one or more concise-ta-store-map

elements where each element in the list identifies the environments for which a given set of trust anchors is applicable, along with any constraints.

```
concise-ta-stores = [+ concise-ta-store]
```

The $concise-tag-type-choice [I-D.draft-birkholz-rats-corim] is extended to include the concise-ta-stores structure. As shown in Section 4 of [I-D.draft-birkholz-rats-corim], the $concise-tag-type-choice type is used within the unsigned-corim-map structure, which is used within COSE-Sign1-corim structure. The COSE-Sign1-corim provides for integrity of the CoTS data. CoTS structures are not intended for use as stand-alone, unsigned structures. The signature on a CoTS instance **SHOULD** be verified using a TA associated with the cots purpose (Section 3.3.1).

```
$concise-tag-type-choice /= #6.TBD(bytes .cbor concise-ta-stores)
```

3.1.2. The concise-ta-store-map Container

A concise-ta-store-map is a trust anchor store where the applicability of the store is established by the tastore.environment field with optional constraints on use of trust anchors found in the tastore.keys field defined by the tastore.purpose, tastore.perm_claims and tastore.excl_claims fields.

```
concise-ta-store-map = {
 ? tastore.language => language-type
 ? tastore.store-identity => tag-identity-map
 tastore.environments => environment-group-list
 ? tastore.purposes => [+ $$tas-list-purpose]
 ? tastore.perm_claims => [+ $$claims-set-claims]
 ? tastore.excl_claims => [+ $$claims-set-claims]
 tastore.keys => cas-and-tas-map
}

; concise-ta-store-map indices
tastore.language = 0
tastore.store-identity = 1
tastore.environment = 2
tastore.purpose = 3
tastore.perm_claims = 4
tastore.excl_claims = 5
tastore.keys = 6
```

The following describes each member of the concise-ta-store-map.

tastore.language: A textual language tag that conforms with the IANA Language Subtag Registry [IANA.language-subtag-registry].

tastore.store-identity:
A composite identifier containing identifying attributes that enable global unique identification of a TA store instance across versions and facilitate linking from other artifacts. The tag-identity-map type is defined in [I-D.draft-birkholz-rats-corim].

tastore.environment: A list of environment definitions that limit the contexts for which the tastore.keys list is applicable. If the tastore.environment is empty, TAs in the tastore.keys list may be used for any environment.

tastore.purpose: Contains a list of purposes (Section 3.3.1) for which the tastore.keys list may be used. When absent, TAs in the tastore.keys list may be used for any purpose. This field is simliar to the extendedKeyUsage extension defined in [RFC5280]. The initial list of purposes are: cots, corim, comid, coswid, eat, key-attestation, certificate

tastore.perm_claims: Contains a list of claim values (Section 3.3.2) [I-D.draft-ietf-rats-eat] for which tastore.keys list **MAY** be used to verify. When this field is absent, TAs in the tastore.keys list **MAY** be used to verify any claim subject to other restrictions.

tastore.excl_claims: Contains a list of claim values (Section 3.3.2) [I-D.draft-ietf-rats-eat] for which tastore.keys list **MUST NOT** be used to verify. When this field is absent, TAs in the tastore.keys list may be used to verify any claim subject to other restrictions.

tastore.keys: Contains a list of one or more TAs and an optional list of one or more CA certificates.

The perm_claims and excl_claims constraints **MAY** alternatively be expressed as extensions in a TA or CA. Inclusion of support here is intended as an aid for environments that find CBOR encoding support more readily available than DER encoding support.

3.1.3. The cas-and-tas-map Container

The cas-and-tas-map container provides the means of representing trust anchors and, optionally, CA certificates.

```
trust-anchor = [
  format => $pkix-ta-type
  data => bstr
]

cas-and-tas-map = {
 tastore.tas => [ + trust-anchor ]
 ? tastore.cas => [ + pkix-cert-data ]
}

; cas-and-tas-map indices
tastore.tas = 0
tastore.cas = 1

; format values
$pkix-ta-type /= tastore.pkix-cert-type
$pkix-ta-type /= tastore.pkix-tainfo-type
$pkix-ta-type /= tastore.pkix-spki-type

tastore.pkix-cert-type = 0
tastore.pkix-tainfo-type = 1
tastore.pkix-spki-type = 2

; certificate type
pkix-cert-data = bstr
```

The tastore.tas element is used to convey one or more trust anchors and an optional set of one or more CA certificates. TAs are implicitly trusted, i.e., no verification is required prior to use. However, limitations on the use of the TA may be asserted in the corresponding concise-ta-store-map or within the TA itself. The tastore.cas field provides certificates that may be useful in the context where the corresponding concise-ta-store-map is used. These certificates are not implicitly trusted and **MUST** be validated to a trust anchor before use. End entity certificates **SHOULD NOT** appear in the tastore.cas list.

The structure of the data contained in the data field of a trust-anchor is indicated by the format field. The pkix-cert-type is used to represent a binary, DER-encoded X.509 Certificate as defined in section 4.1 of [RFC5280]. The pkix-key-type is used to represent a binary, DER-encoded SubjectPublicKeyInfo as defined in section 4.1 of [RFC5280]. The pkix-tainfo-type is used to represent a binary, DER-encoded TrustAnchorInfo as defined in section 2 of [RFC5914].

The $pkix-ta-type provides an extensible means for representing trust anchor information. It is defined here as supporting the pkix-cert-type, pkix-spki-type or pkix-tainfo-type. The pkix-spki-type may be used where only a raw pubilc key is necessary. The pkix-cert-type may be used for most purposes, including scenarios where a raw

public key is sufficient and those where additional information from a certificate is required. The pkix-tainfo-type is included to support scenarios where constraints information is directly associated with a public key or certificate (vs. constraints for a TA set as provided by tastore.purpose, tastore.perm_claims and tastore.excl_claims).

The pkix-cert-data type is used to represent a binary, DER-encoded X.509 Certificate.

3.2. Environment definition

3.2.1. The environment-group-list Array

In CoRIM, "composite devices or systems are represented by a collection of Concise Module Identifiers (CoMID) and Concise Software Identifiers (CoSWID)". For trust anchor management purposes, targeting specific devices or systems may be too granular. For example, a trust anchor or set of trust anchors may apply to multiple device models or versions. The environment-map definition as used in a CoRIM is tightly bound to a CoMID. To allow for distribution of key material applicable to a specific or range of devices or software, the envrionment-group-list and environment-group-map are defined as below. These aim to enable use of coarse-grained naturally occurring values, like vendor, make, model, etc. to determine if a set of trust anchors is applicable to an environment.

```
environment-group-list = [* environment-group-list-map]

environment-group-list-map = {
  ? tastore.environment_map => environment-map,
  ? tastore.concise_swid_tag => abbreviated-swid-tag,
  ? tastore.named_ta_store => named-ta-store,
}

; environment-group-list-map indices
tastore.environment_map = 0
tastore.abbreviated_swid_tag = 1
tastore.named_ta_store = 2
```

An environment-group-list is a list of one or more environment-group-list-map elements that are used to determine if a given context is applicable. An empty list signifies all contexts **SHOULD** be considered as applicable.

An environment-group-list-map is one of environment-map[I-D.draft-birkholz-rats-corim], abbreviated-swid-tag-map (Section 3.2.2) or named-ta-store (Section 3.2.3).

As defined in [I-D.draft-birkholz-rats-corim], an envirionment-map may contain class-map, $instance-id-type-choice, $group-id-type-choice.

QUESTION: Should the above dispense with environment_map and concise_swid_tag and use or define some identity-focused structure with information common to both (possibly class-map from [I-D.draft-birkholz-rats-corim])? If not, should a more complete CoMID representation be used (instead of environment_map)?

3.2.2. The abbreviated-swid-tag-map Container

The abbreviated-swid-tag-map allows for expression of fields from a concise-swid-tag [I-D.draft-ietf-sacm-coswid] with all fields except entity designated as optional, compared to the concise-swid-tag definition that requires tag-id, tag-version and software-name to be present.

```
abbreviated-swid-tag-map = {
  ? tag-id => text / bstr .size 16,
  ? tag-version => integer,
  ? corpus => bool,
  ? patch => bool,
  ? supplemental => bool,
  ? software-name => text,
  ? software-version => text,
  ? version-scheme => $version-scheme,
  ? media => text,
  ? software-meta => one-or-more<software-meta-entry>,
  entity => one-or-more<entity-entry>,
  ? link => one-or-more<link-entry>,
  ? payload-or-evidence,
  * $$coswid-extension,
  global-attributes,
}
```

3.2.3. The named-ta-store Type

This specification allows for defining sets of trust anchors that are associated with an arbitrary name instead of relative to information typically expressed in a CoMID or CoSWID. Relying parties **MUST** be configured using the named-ta-store value to select a corresponding concise-ta-store-map for use.

```
named-ta-store = tstr
```

3.3. Constraints definition

3.3.1. The $$tas-list-purpose Type

The $$tas-list-purpose type provides an extensible means of expressions actions for which the corresponding keys are applicable. For example, trust anchors in a concise-ta-store-map with purpose field set to eat may not be used to verification certification paths. Extended key usage values corresponding to each purpose listed below (except for certificate) are defined in a companion specification.

```
$$tas-list-purpose /= "cots"
$$tas-list-purpose /= "corim"
$$tas-list-purpose /= "coswid"
$$tas-list-purpose /= "eat"
$$tas-list-purpose /= "key-attestation"
$$tas-list-purpose /= "certificate"
$$tas-list-purpose /= "dloa"
```

TODO - define verification targets for each purpose. QUESTION - should this have a registry?

3.3.2. Claims

A concise-ta-store-map may include lists of permitted and/or excluded claims [I-D.draft-ietf-rats-eat] that limit the applicability of trust anchors present in a cas-and-tas-map. A subsequent specification will define processing rules for evaluating constraints expressed in TA stores, TAs, CA certificates and end entity certificates.

3.4. Processing a concise-ta-stores RIM

When verifying a signature using a public key that chains back to a concise-ta-stores instance, elements in the concise-ta-stores array are processed beginning with the first element and proceeding until either a matching set is found that serves the desired purpose or no more elements are available. Each element is evaluated relative to the context, i.e., environment, purpose, artifact contents, etc.

For example, when verifying a CoRIM, each element in a triples-group **MUST** have an environment value that matches an environment-group-list-map element associated with the concise-ta-store-map containing the trust anchor used to verify the CoMID. Similarly, when verifying a CoSWID, the values in a abbreviated-swid-tag element from the concise-ta-store-map **MUST** match the CoSWID tag being verified. When verifying a certificate with DICE attestation extension, the information in each DiceTcbInfo element **MUST** be consistent with an environment-group-list-map associated with the concise-ta-store-map.

3.5. Verifying a concise-ta-stores RIM

[I-D.draft-birkholz-rats-corim] defers verification rules to [RFC8152] and this document follows suit with the additional recommendation that the public key used to verify the RIM **SHOULD** be present in or chain to a public key present in a concise-ta-store-map with purpose set to cots.

4. CDDL definitions

The CDDL definitions present in this document are provided below. Definitions from [I-D.draft-birkholz-rats-corim] are not repeated here.

```
concise-ta-stores = [+ concise-ta-store-map]
$concise-tag-type-choice /= #6.TBD(bytes .cbor concise-ta-stores)

concise-ta-store-map = {
 ? tastore.language => language-type
 ? tastore.store-identity => tag-identity-map
 tastore.environments => environment-group-list
 ? tastore.purposes => [+ $$tas-list-purpose]
 ? tastore.perm_claims => [+ $$claims-set-claims]
 ? tastore.excl_claims => [+ $$claims-set-claims]
 tastore.keys => cas-and-tas-map
}

; concise-ta-store-map indices
tastore.language = 0
tastore.store-identity = 1
tastore.environment = 2
tastore.purpose = 3
tastore.perm_claims = 4
tastore.excl_claims = 5
tastore.keys = 6

trust-anchor = [
  format => $pkix-ta-type
  data => bstr
]

cas-and-tas-map = {
 tastore.tas => [ + trust-anchor ]
 ? tastore.cas => [ + pkix-cert-type ]
}

; cas-and-tas-map indices
tastore.tas = 0
tastore.cas = 1

; format values
$pkix-ta-type /= tastore.pkix-cert-type
$pkix-ta-type /= tastore.pkix-tainfo-type
$pkix-ta-type /= tastore.pkix-spki-type

tastore.pkix-cert-type = 0
tastore.pkix-tainfo-type = 1
tastore.pkix-spki-type = 2

; certificate type
pkix-cert-data = bstr

environment-group-list = [* environment-group-list-map]
```

```
environment-group-list-map = {
  ? environment-map => environment-map,
  ? concise-swid-tag => abbreviated-swid-tag,
  ? named-ta-store => named-ta-store,
}

abbreviated-swid-tag = {
  ? tag-version => integer,
  ? corpus => bool,
  ? patch => bool,
  ? supplemental => bool,
  ? software-name => text,
  ? software-version => text,
  ? version-scheme => $version-scheme,
  ? media => text,
  ? software-meta => one-or-more<software-meta-entry>,
  ? entity => one-or-more<entity-entry>,
  ? link => one-or-more<link-entry>,
  ? payload-or-evidence,
  * $$coswid-extension,
  global-attributes,
}

named-ta-store = tstr

$tas-list-purpose /= "cots"
$tas-list-purpose /= "corim"
$tas-list-purpose /= "comid"
$tas-list-purpose /= "coswid"
$tas-list-purpose /= "eat"
$tas-list-purpose /= "key-attestation"
$tas-list-purpose /= "certificate"
$tas-list-purpose /= "dloa"
```

5. Examples

The following examples are isolated concise-ta-store-map instances shown as JSON for ease of reading. The final example is an ASCII hex representation of a CBOR-encoded concise-ta-stores instance containing each example below (and using a placeholder value for the concise-ta-stores tag).

The TA store below contains a TA from a single organization ("Zesty Hands, Inc,") that is used to verify CoRIMs for that organization. Because this TA does not verify certificates, a bare public key is appropriate.

```
{
  "environments": [
    {
      "environment": {
        "class": {
          "vendor": "Worthless Sea, Inc."
        }
      }
    }
  ],
  "purposes": [
    "corim"
  ],
  "keys": {
    "tas": [
      {
        "format": 2,
        "data":
"MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAErYoMAdqe2gJT3CvCcifZxyE9+
N8T6Jy5zbeo5LYtnOipmi1wXA9/gNtlwAbRCRQitH/GEcvUaGlzPZxIOITV/g=="
      }
    ]
  }
}
```

The TA store below features three TAs from different organizations grouped as a TA store with the name "Miscellaneous TA Store". The first TA is an X.509 certificate. The second and third TAs are TrustAnchorInfo objects containing X.509 certificates. Though not shown in this example, constraints could added to the TrustAnchorInfo elements, i.e., to restrict verification to attestations asserting a specific vendor name.

```
{
  "environments": [
    {
      "namedtastore": "Miscellaneous TA Store"
    }
  ],
  "keys": {
    "tas": [
      {
        "data":
"
MIIBvTCCAWSgAwIBAgIVANCdkL89UlzHc9Ui7XfVniK7pFuIMAoGCCqGSM49BAMCMD4
xCzAJBgNVBAYMAlVTMRAwDgYDVQQKDAdFeGFtcGxlMR0wGwYDVQQDDBRFeGFtcGxlIF
RydXN0IEFuY2hvcjAeFw0yMjA1MTkxNTEzMDdaFw0zMjA1MTYxNTEzMDdaMD4xCzAJB
gNVBAYMAlVTMRAwDgYDVQQKDAdFeGFtcGxlMR0wGwYDVQQDDBRFeGFtcGxlIFRydXN0
IEFuY2hvcjBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABONRqhA5JAekvQN8oLwRVND
nAfBnTznLLE+SEGks677sHSeXfcVhZXUeDiN7/
fsVNumaiEWRQpZh3zXPwL8rUMyjPzA9MB0GA1UdDgQWBBQBXEXJrLBGKnFd1xCgeMAV
SfEBPzALBgNVHQ8EBAMCAoQwDwYDVR0TAQH/BAUwAwEB/
zAKBggqhkjOPQQDAgNHADBEAiALBidABsfpzG0lTL9Eh9b6AUbqnzF+
koEZbgvppvvt9QIgVoE+bhEN0j6wSPzePjLrEdD+PEgyjHJ5rbA11SPq/1M="
      },
      {
        "format": 1,
        "data":
"
ooICtjCCArIwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASXz21w12owQAx58euratY
WiHEkhxDU9MEgetrvAtGYZxNnkfLCsp9vLcw8ISXC8tL97k9ZCUtnr0MzLw37XKRABB
T22tHlEou/DenpU0Ozccb3/+
fibjCCAj0wUjELMAkGA1UEBgwCVVMxGjAYBgNVBAoMEVplc3R5IEhhbmRzLCBJbmMuM
ScwJQYDVQQDDB5aZXN0eSBIYW5kcywgSW5jLiBUcnVzdCBBbmNob3KgggHlMIIBi6AD
AgECAhQL3EqgUXlQPljyddVSRnNHvK+
1MzAKBggqhkjOPQQDAjBSMQswCQYDVQQGDAJVUzEaMBgGA1UECgwRWmVzdHkgSGFuZH
MsIEluYy4xJzAlBgNVBAMMHlplc3R5IEhhbmRzLCBJbmMuIFRydXN0IEFuY2hvcjAeF
w0yMjA1MTkxNTEzMDdaFw0zMjA1MTYxNTEzMDdaMFIxCzAJBgNVBAYMAlVTMRowGAYD
VQQKDBFaZXN0eSBIYW5kcywgSW5jLjEnMCUGA1UEAwweWmVzdHkgSGFuZHMsIEluYy4
gVHJ1c3QgQW5jaG9yMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEl89tcNdqMEAMef
Hrq2rWFohxJIcQ1PTBIHra7wLRmGcTZ5HywrKfby3MPCElwvLS/e5PWQlLZ69DMy8N+
1ykQKM/MD0wHQYDVR0OBBYEFPba0eUSi78N6elTQ7Nxxvf/5+
JuMAsGA1UdDwQEAwIChDAPBgNVHRMBAf8EBTADAQH/
MAoGCCqGSM49BAMCA0gAMEUCIB2li+
f6RCxs2EnvNWciSpIDwiUViWayGv1A8xks80eYAiEAmCez4KGrolFKOZT6bvqf1sYQu
JBfvtk/y1JQdUvoqlg="
      },
      {
        "format": 1,
        "data":
"
ooIC1TCCAtEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATN0f5kzywEzZOYbaV23O3
```

```
N8cku39JoLNjlHPwECbXDDWp0LpAO1z248/hoy6UW/TZMTPPR/
93XwHsG16mSFy8XBBSKhM/
5gJWjvDbW7qUY1peNm9cfYDCCAlwwXDELMAkGA1UEBgwCVVMxHzAdBgNVBAoMFlNub2
JiaXNoIEFwcGFyZWwsIEluYy4xLDAqBgNVBAMMI1Nub2JiaXNoIEFwcGFyZWwsIEluY
y4gVHJ1c3QgQW5jaG9yoIIB+jCCAZ+gAwIBAgIUEBuTRGXAEEVEHhu4xafAnqm+
qYgwCgYIKoZIzj0EAwIwXDELMAkGA1UEBgwCVVMxHzAdBgNVBAoMFlNub2JiaXNoIEF
wcGFyZWwsIEluYy4xLDAqBgNVBAMMI1Nub2JiaXNoIEFwcGFyZWwsIEluYy4gVHJ1c3
QgQW5jaG9yMB4XDTIyMDUxOTE1MTMwOFoXDTMyMDUxNjE1MTMwOFowXDELMAkGA1UEB
gwCVVMxHzAdBgNVBAoMFlNub2JiaXNoIEFwcGFyZWwsIEluYy4xLDAqBgNVBAMMI1Nu
b2JiaXNoIEFwcGFyZWwsIEluYy4gVHJ1c3QgQW5jaG9yMFkwEwYHKoZIzj0CAQYIKoZ
Izj0DAQcDQgAEzdH+ZM8sBM2TmG2ldtztzfHJLt/
SaCzY5Rz8BAm1ww1qdC6QDtc9uPP4aMulFv02TEzz0f/d18B7BtepkhcvF6M/
MD0wHQYDVR0OBBYEFIqEz/
mAlaO8NtbupRjWl42b1x9gMAsGA1UdDwQEAwIChDAPBgNVHRMBAf8EBTADAQH/
MAoGCCqGSM49BAMCA0kAMEYCIQC2cf43f3PPlCO6/dxv40ftIgxxToKHF72UzENv7+
y4ygIhAIGtC/r6SGaFMaP7zD2EloBuIXTtyWu8Hwl+YGdXRY93"
      }
    ]
  }
}
```

The TA Store below features one TA with an environment targeting CoSWIDs with entity named "Zesty Hands, Inc," and one permitted EAT claim for software named "Bitter Paper".

```
{
  "environments": [
    {
      "swidtag": {
        "entity": [
          {
            "entity-name": "Zesty Hands, Inc.",
            "role": "softwareCreator"
          }
        ]
      }
    }
  ],
  "permclaims": [
    {
      "swname": "Bitter Paper"
    }
  ],
  "keys": {
    "tas": [
      {
        "data":
"
MIIB5TCCAYugAwIBAgIUC9xKoFF5UD5Y8nXVUkZzR7yvtTMwCgYIKoZIzj0EAwI
wUjELMAkGA1UEBgwCVVMxGjAYBgNVBAoMEVplc3R5IEhhbmRzLCBJbmMuMScwJQ
YDVQQDDB5aZXN0eSBIYW5kcywgSW5jLiBUcnVzdCBBbmNob3IwHhcNMjIwNTE5M
TUxMzA3WhcNMzIwNTE2MTUxMzA3WjBSMQswCQYDVQQGDAJVUzEaMBgGA1UECgwR
WmVzdHkgSGFuZHMsIEluYy4xJzAlBgNVBAMMHlplc3R5IEhhbmRzLCBJbmMuIFR
ydXN0IEFuY2hvcjBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABJfPbXDXajBADH
nx66tq1haIcSSHENT0wSB62u8C0ZhnE2eR8sKyn28tzDwhJcLy0v3uT1kJS2evQ
zMvDftcpECjPzA9MB0GA1UdDgQWBBT22tHlEou/DenpU0Ozccb3/+
fibjALBgNVHQ8EBAMCAoQwDwYDVR0TAQH/BAUwAwEB/
zAKBggqhkjOPQQDAgNIADBFAiAdpYvn+
kQsbNhJ7zVnIkqSA8IlFYlmshr9QPMZLPNHmAIhAJgns+Chq6JRSjmU+
m76n9bGELiQX77ZP8tSUHVL6KpY"
      }
    ]
  }
}
```

The ASCII hex below represents a signed CoRIM that features a concise-ta-stores containing the three examples shown above.

```
D2 84 58 5D A3 01 26 03 74 61 70 70 6C 69 63 61
74 69 6F 6E 2F 72 69 6D 2B 63 62 6F 72 08 58 41
A2 00 A2 00 74 41 43 4D 45 20 4C 74 64 20 73 69
67 6E 69 6E 67 20 6B 65 79 01 D8 20 74 68 74 74
70 73 3A 2F 2F 61 63 6D 65 2E 65 78 61 6D 70 6C
65 01 A2 00 C1 1A 61 CE 48 00 01 C1 1A 69 54 67
80 A0 59 0B 10 A3 00 50 70 2F 47 5D E6 6B 4F 61
A5 8E 3C EF 3C CD 6E 44 01 81 59 0A E8 D9 01 FB
83 A2 01 81 A1 01 A1 00 A1 01 73 57 6F 72 74 68
6C 65 73 73 20 53 65 61 2C 20 49 6E 63 2E 05 A1
00 81 82 02 58 5B 30 59 30 13 06 07 2A 86 48 CE
3D 02 01 06 08 2A 86 48 CE 3D 03 01 07 03 42 00
04 AD 8A 0C 01 DA 9E DA 02 53 DC 2B C2 72 27 D9
C7 21 3D F8 DF 13 E8 9C B9 CD B7 A8 E4 B6 2D 9C
E8 A9 9A 2D 70 5C 0F 7F 80 DB 65 C0 06 D1 09 14
22 B4 7F C6 11 CB D4 68 69 73 3D 9C 48 38 84 D5
FE A2 01 81 A1 03 76 4D 69 73 63 65 6C 6C 61 6E
65 6F 75 73 20 54 41 20 53 74 6F 72 65 05 A1 00
83 82 01 59 02 7E A2 82 02 7A 30 82 02 76 30 59
30 13 06 07 2A 86 48 CE 3D 02 01 06 08 2A 86 48
CE 3D 03 01 07 03 42 00 04 E3 51 AA 10 39 24 07
A4 BD 03 7C A0 BC 11 54 D0 E7 01 F0 67 4F 39 CB
2C 4F 92 10 69 2C EB BE EC 1D 27 97 7D C5 61 65
75 1E 0E 23 7B FD FB 15 36 E9 9A 88 45 91 42 96
61 DF 35 CF C0 BF 2B 50 CC 04 14 01 5C 45 C9 AC
B0 46 2A 71 5D D7 10 A0 78 C0 15 49 F1 01 3F 30
82 02 01 30 3E 31 0B 30 09 06 03 55 04 06 0C 02
55 53 31 10 30 0E 06 03 55 04 0A 0C 07 45 78 61
6D 70 6C 65 31 1D 30 1B 06 03 55 04 03 0C 14 45
78 61 6D 70 6C 65 20 54 72 75 73 74 20 41 6E 63
68 6F 72 A0 82 01 BD 30 82 01 64 A0 03 02 01 02
02 15 00 D0 9D 90 BF 3D 52 5C C7 73 D5 22 ED 77
D5 9E 22 BB A4 5B 88 30 0A 06 08 2A 86 48 CE 3D
04 03 02 30 3E 31 0B 30 09 06 03 55 04 06 0C 02
55 53 31 10 30 0E 06 03 55 04 0A 0C 07 45 78 61
6D 70 6C 65 31 1D 30 1B 06 03 55 04 03 0C 14 45
78 61 6D 70 6C 65 20 54 72 75 73 74 20 41 6E 63
68 6F 72 30 1E 17 0D 32 32 30 35 31 39 31 35 31
33 30 37 5A 17 0D 33 32 30 35 31 36 31 35 31 33
30 37 5A 30 3E 31 0B 30 09 06 03 55 04 06 0C 02
55 53 31 10 30 0E 06 03 55 04 0A 0C 07 45 78 61
6D 70 6C 65 31 1D 30 1B 06 03 55 04 03 0C 14 45
78 61 6D 70 6C 65 20 54 72 75 73 74 20 41 6E 63
68 6F 72 30 59 30 13 06 07 2A 86 48 CE 3D 02 01
06 08 2A 86 48 CE 3D 03 01 07 03 42 00 04 E3 51
AA 10 39 24 07 A4 BD 03 7C A0 BC 11 54 D0 E7 01
F0 67 4F 39 CB 2C 4F 92 10 69 2C EB BE EC 1D 27
97 7D C5 61 65 75 1E 0E 23 7B FD FB 15 36 E9 9A
88 45 91 42 96 61 DF 35 CF C0 BF 2B 50 CC A3 3F
```

30 3D 30 1D 06 03 55 1D 0E 04 16 04 14 01 5C 45
C9 AC B0 46 2A 71 5D D7 10 A0 78 C0 15 49 F1 01
3F 30 0B 06 03 55 1D 0F 04 04 03 02 02 84 30 0F
06 03 55 1D 13 01 01 FF 04 05 30 03 01 01 FF 30
0A 06 08 2A 86 48 CE 3D 04 03 02 03 47 00 30 44
02 20 0B 06 27 40 06 C7 E9 CC 6D 25 4C BF 44 87
D6 FA 01 46 EA 9F 31 7E 92 81 19 6E 0B E9 A6 FB
ED F5 02 20 56 81 3E 6E 11 0D D2 3E B0 48 FC DE
3E 32 EB 11 D0 FE 3C 48 32 8C 72 79 AD B0 35 D5
23 EA FF 53 82 01 59 02 BA A2 82 02 B6 30 82 02
B2 30 59 30 13 06 07 2A 86 48 CE 3D 02 01 06 08
2A 86 48 CE 3D 03 01 07 03 42 00 04 97 CF 6D 70
D7 6A 30 40 0C 79 F1 EB AB 6A D6 16 88 71 24 87
10 D4 F4 C1 20 7A DA EF 02 D1 98 67 13 67 91 F2
C2 B2 9F 6F 2D CC 3C 21 25 C2 F2 D2 FD EE 4F 59
09 4B 67 AF 43 33 2F 0D FB 5C A4 40 04 14 F6 DA
D1 E5 12 8B BF 0D E9 E9 53 43 B3 71 C6 F7 FF E7
E2 6E 30 82 02 3D 30 52 31 0B 30 09 06 03 55 04
06 0C 02 55 53 31 1A 30 18 06 03 55 04 0A 0C 11
5A 65 73 74 79 20 48 61 6E 64 73 2C 20 49 6E 63
2E 31 27 30 25 06 03 55 04 03 0C 1E 5A 65 73 74
79 20 48 61 6E 64 73 2C 20 49 6E 63 2E 20 54 72
75 73 74 20 41 6E 63 68 6F 72 A0 82 01 E5 30 82
01 8B A0 03 02 01 02 02 14 0B DC 4A A0 51 79 50
3E 58 F2 75 D5 52 46 73 47 BC AF B5 33 30 0A 06
08 2A 86 48 CE 3D 04 03 02 30 52 31 0B 30 09 06
03 55 04 06 0C 02 55 53 31 1A 30 18 06 03 55 04
0A 0C 11 5A 65 73 74 79 20 48 61 6E 64 73 2C 20
49 6E 63 2E 31 27 30 25 06 03 55 04 03 0C 1E 5A
65 73 74 79 20 48 61 6E 64 73 2C 20 49 6E 63 2E
20 54 72 75 73 74 20 41 6E 63 68 6F 72 30 1E 17
0D 32 32 30 35 31 39 31 35 31 33 30 37 5A 17 0D
33 32 30 35 31 36 31 35 31 33 30 37 5A 30 52 31
0B 30 09 06 03 55 04 06 0C 02 55 53 31 1A 30 18
06 03 55 04 0A 0C 11 5A 65 73 74 79 20 48 61 6E
64 73 2C 20 49 6E 63 2E 31 27 30 25 06 03 55 04
03 0C 1E 5A 65 73 74 79 20 48 61 6E 64 73 2C 20
49 6E 63 2E 20 54 72 75 73 74 20 41 6E 63 68 6F
72 30 59 30 13 06 07 2A 86 48 CE 3D 02 01 06 08
2A 86 48 CE 3D 03 01 07 03 42 00 04 97 CF 6D 70
D7 6A 30 40 0C 79 F1 EB AB 6A D6 16 88 71 24 87
10 D4 F4 C1 20 7A DA EF 02 D1 98 67 13 67 91 F2
C2 B2 9F 6F 2D CC 3C 21 25 C2 F2 D2 FD EE 4F 59
09 4B 67 AF 43 33 2F 0D FB 5C A4 40 A3 3F 30 3D
30 1D 06 03 55 1D 0E 04 16 04 14 F6 DA D1 E5 12
8B BF 0D E9 E9 53 43 B3 71 C6 F7 FF E7 E2 6E 30
0B 06 03 55 1D 0F 04 04 03 02 02 84 30 0F 06 03
55 1D 13 01 01 FF 04 05 30 03 01 01 FF 30 0A 06
08 2A 86 48 CE 3D 04 03 02 03 48 00 30 45 02 20

```
1D A5 8B E7 FA 44 2C 6C D8 49 EF 35 67 22 4A 92
03 C2 25 15 89 66 B2 1A FD 40 F3 19 2C F3 47 98
02 21 00 98 27 B3 E0 A1 AB A2 51 4A 39 94 FA 6E
FA 9F D6 C6 10 B8 90 5F BE D9 3F CB 52 50 75 4B
E8 AA 58 82 01 59 02 D9 A2 82 02 D5 30 82 02 D1
30 59 30 13 06 07 2A 86 48 CE 3D 02 01 06 08 2A
86 48 CE 3D 03 01 07 03 42 00 04 CD D1 FE 64 CF
2C 04 CD 93 98 6D A5 76 DC ED CD F1 C9 2E DF D2
68 2C D8 E5 1C FC 04 09 B5 C3 0D 6A 74 2E 90 0E
D7 3D B8 F3 F8 68 CB A5 16 FD 36 4C 4C F3 D1 FF
DD D7 C0 7B 06 D7 A9 92 17 2F 17 04 14 8A 84 CF
F9 80 95 A3 BC 36 D6 EE A5 18 D6 97 8D 9B D7 1F
60 30 82 02 5C 30 5C 31 0B 30 09 06 03 55 04 06
0C 02 55 53 31 1F 30 1D 06 03 55 04 0A 0C 16 53
6E 6F 62 62 69 73 68 20 41 70 70 61 72 65 6C 2C
20 49 6E 63 2E 31 2C 30 2A 06 03 55 04 03 0C 23
53 6E 6F 62 62 69 73 68 20 41 70 70 61 72 65 6C
2C 20 49 6E 63 2E 20 54 72 75 73 74 20 41 6E 63
68 6F 72 A0 82 01 FA 30 82 01 9F A0 03 02 01 02
02 14 10 1B 93 44 65 C0 10 45 44 1E 1B B8 C5 A7
C0 9E A9 BE A9 88 30 0A 06 08 2A 86 48 CE 3D 04
03 02 30 5C 31 0B 30 09 06 03 55 04 06 0C 02 55
53 31 1F 30 1D 06 03 55 04 0A 0C 16 53 6E 6F 62
62 69 73 68 20 41 70 70 61 72 65 6C 2C 20 49 6E
63 2E 31 2C 30 2A 06 03 55 04 03 0C 23 53 6E 6F
62 62 69 73 68 20 41 70 70 61 72 65 6C 2C 20 49
6E 63 2E 20 54 72 75 73 74 20 41 6E 63 68 6F 72
30 1E 17 0D 32 32 30 35 31 39 31 35 31 33 30 38
5A 17 0D 33 32 30 35 31 36 31 35 31 33 30 38 5A
30 5C 31 0B 30 09 06 03 55 04 06 0C 02 55 53 31
1F 30 1D 06 03 55 04 0A 0C 16 53 6E 6F 62 62 69
73 68 20 41 70 70 61 72 65 6C 2C 20 49 6E 63 2E
31 2C 30 2A 06 03 55 04 03 0C 23 53 6E 6F 62 62
69 73 68 20 41 70 70 61 72 65 6C 2C 20 49 6E 63
2E 20 54 72 75 73 74 20 41 6E 63 68 6F 72 30 59
30 13 06 07 2A 86 48 CE 3D 02 01 06 08 2A 86 48
CE 3D 03 01 07 03 42 00 04 CD D1 FE 64 CF 2C 04
CD 93 98 6D A5 76 DC ED CD F1 C9 2E DF D2 68 2C
D8 E5 1C FC 04 09 B5 C3 0D 6A 74 2E 90 0E D7 3D
B8 F3 F8 68 CB A5 16 FD 36 4C 4C F3 D1 FF DD D7
C0 7B 06 D7 A9 92 17 2F 17 A3 3F 30 3D 30 1D 06
03 55 1D 0E 04 16 04 14 8A 84 CF F9 80 95 A3 BC
36 D6 EE A5 18 D6 97 8D 9B D7 1F 60 30 0B 06 03
55 1D 0F 04 04 03 02 02 84 30 0F 06 03 55 1D 13
01 01 FF 04 05 30 03 01 01 FF 30 0A 06 08 2A 86
48 CE 3D 04 03 02 03 49 00 30 46 02 21 00 B6 71
FE 37 7F 73 CF 94 23 BA FD DC 6F E3 47 ED 22 0C
71 4E 82 87 17 BD 94 CC 43 6F EF EC B8 CA 02 21
00 81 AD 0B FA FA 48 66 85 31 A3 FB CC 3D 84 96
```

```
80 6E 21 74 ED C9 6B BC 1F 09 7E 60 67 57 45 8F
77 A3 01 81 A1 02 A1 02 A2 18 1F 71 5A 65 73 74
79 20 48 61 6E 64 73 2C 20 49 6E 63 2E 18 21 02
03 81 A1 19 03 E6 6C 42 69 74 74 65 72 20 50 61
70 65 72 05 A1 00 81 82 00 59 01 E9 30 82 01 E5
30 82 01 8B A0 03 02 01 02 02 14 0B DC 4A A0 51
79 50 3E 58 F2 75 D5 52 46 73 47 BC AF B5 33 30
0A 06 08 2A 86 48 CE 3D 04 03 02 30 52 31 0B 30
09 06 03 55 04 06 0C 02 55 53 31 1A 30 18 06 03
55 04 0A 0C 11 5A 65 73 74 79 20 48 61 6E 64 73
2C 20 49 6E 63 2E 31 27 30 25 06 03 55 04 03 0C
1E 5A 65 73 74 79 20 48 61 6E 64 73 2C 20 49 6E
63 2E 20 54 72 75 73 74 20 41 6E 63 68 6F 72 30
1E 17 0D 32 32 30 35 31 39 31 35 31 33 30 37 5A
17 0D 33 32 30 35 31 36 31 35 31 33 30 37 5A 30
52 31 0B 30 09 06 03 55 04 06 0C 02 55 53 31 1A
30 18 06 03 55 04 0A 0C 11 5A 65 73 74 79 20 48
61 6E 64 73 2C 20 49 6E 63 2E 31 27 30 25 06 03
55 04 03 0C 1E 5A 65 73 74 79 20 48 61 6E 64 73
2C 20 49 6E 63 2E 20 54 72 75 73 74 20 41 6E 63
68 6F 72 30 59 30 13 06 07 2A 86 48 CE 3D 02 01
06 08 2A 86 48 CE 3D 03 01 07 03 42 00 04 97 CF
6D 70 D7 6A 30 40 0C 79 F1 EB AB 6A D6 16 88 71
24 87 10 D4 F4 C1 20 7A DA EF 02 D1 98 67 13 67
91 F2 C2 B2 9F 6F 2D CC 3C 21 25 C2 F2 D2 FD EE
4F 59 09 4B 67 AF 43 33 2F 0D FB 5C A4 40 A3 3F
30 3D 30 1D 06 03 55 1D 0E 04 16 04 14 F6 DA D1
E5 12 8B BF 0D E9 E9 53 43 B3 71 C6 F7 FF E7 E2
6E 30 0B 06 03 55 1D 0F 04 04 03 02 02 84 30 0F
06 03 55 1D 13 01 01 FF 04 05 30 03 01 01 FF 30
0A 06 08 2A 86 48 CE 3D 04 03 02 03 48 00 30 45
02 20 1D A5 8B E7 FA 44 2C 6C D8 49 EF 35 67 22
4A 92 03 C2 25 15 89 66 B2 1A FD 40 F3 19 2C F3
47 98 02 21 00 98 27 B3 E0 A1 AB A2 51 4A 39 94
FA 6E FA 9F D6 C6 10 B8 90 5F BE D9 3F CB 52 50
75 4B E8 AA 58 04 A2 00 C1 1A 61 CE 48 00 01 C1
1A 69 54 67 80 58 40 84 64 A5 CC 98 98 9E 1F 72
CD 14 97 99 78 47 BE 03 E4 C8 61 34 A5 B4 43 91
AA D7 55 EC 31 3A 2E 15 41 EC E2 E4 58 7F 5A B3
59 C7 F4 FF 0C 27 61 A6 FB 90 75 F9 0E 9C CD 13
9A F1 F9 31 E7 01 06
```

6. Security Considerations

As a profile of CoRIM, the security considerations from [I-D.draft-birkholz-rats-corim] apply.

As a means of managing trust anchors, the security considerations from [RFC6024] and [RFC5934] apply. a CoTS signer is roughly analogous to a "management trust anchor" as described in [RFC5934].

7. IANA Considerations

7.1. CoRIM CBOR Tag Registration

IANA is requested to allocate tags in the "CBOR Tags" registry [IANA.cbor-tags], preferably with the specific value requested:

Tag	Data Item	Semantics
507	tagged array	Concise Trust Anchor Stores (CoTS)

Table 1

8. References

8.1. Normative References

[I-D.draft-birkholz-rats-corim] Birkholz, H., Fossati, T., Deshpande, Y., Smith, N., and W. Pan, "Concise Reference Integrity Manifest", Work in Progress, Internet-Draft, draft-birkholz-rats-corim-02, 26 January 2022, <https://datatracker.ietf.org/doc/html/draft-birkholz-rats-corim-02>.

[I-D.draft-ietf-rats-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>.

[I-D.draft-ietf-sacm-coswid] Birkholz, H., Fitzgerald-McKay, J., Schmidt, C., and D. Waltermire, "Concise Software Identification Tags", Work in Progress, Internet-Draft, draft-ietf-sacm-coswid-21, 7 March 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-sacm-coswid-21>.

[IANA.cbor-tags] IANA, "Concise Binary Object Representation (CBOR) Tags", <https://www.iana.org/assignments/cbor-tags>.

[IANA.language-subtag-registry] IANA, "Language Subtag Registry", <https://www.iana.org/assignments/language-subtag-registry>.

[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>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[RFC5914] Housley, R., Ashmore, S., and C. Wallace, "Trust Anchor Format", RFC 5914, DOI 10.17487/RFC5914, June 2010, <https://www.rfc-editor.org/rfc/rfc5914>.

[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>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

8.2. Informative References

[dloa] GlobalPlatform, "GlobalPlatform Card - Digital Letter of Approval Version 1.0", November 2015, <https://globalplatform.org/wp-content/uploads/2015/12/GPC_DigitalLetterOfApproval_v1.0.pdf>.

[fido-metadata] FIDO Alliance, "FIDO Metadata Statement", May 2021, <https://fidoalliance.org/specs/mds/fido-metadata-statement-v3.0-ps-20210518.html>.

[fido-service] FIDO Alliance, "FIDO Metadata Service", May 2021, <https://fidoalliance.org/specs/mds/fido-metadata-service-v3.0-ps-20210518.html>.

[I-D.draft-ietf-rats-architecture] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote Attestation Procedures Architecture", Work in Progress, Internet-Draft, draft-ietf-rats-architecture-18, 14 June 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-architecture-18>.

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, DOI 10.17487/

RFC3779, June 2004, <https://www.rfc-editor.org/rfc/rfc3779>.

[RFC5934] Housley, R., Ashmore, S., and C. Wallace, "Trust Anchor Management Protocol (TAMP)", RFC 5934, DOI 10.17487/RFC5934, August 2010, <https://www.rfc-editor.org/rfc/rfc5934>.

[RFC6024] Reddy, R. and C. Wallace, "Trust Anchor Management Requirements", RFC 6024, DOI 10.17487/RFC6024, October 2010, <https://www.rfc-editor.org/rfc/rfc6024>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/rfc/rfc8152>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Carl Wallace
Red Hound Software
United States of America

Email: carl@redhoundsoftware.com

Russ Housley
Vigil Security, LLC
516 Dranesville Road
Herndon, VA 20170
United States of America

Email: housley@vigilsec.com