TRUSTED® COMPUTING GROUP

SPECIFICATION

TCG Component Reference Integrity Manifest Information Model

Version 1.0
Revision 38
February 15, 2024

Contact: admin@trustedcomputinggroup.org

Public Review

Work in Progress

This document is an intermediate draft for comment only and is subject to change without notice. Readers should not design products based on this document.

DISCLAIMERS, NOTICES, AND LICENSE TERMS

THIS SPECIFICATION IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

Contact the Trusted Computing Group at www.trustedcomputinggroup.org for information on specification licensing through membership agreements.

Any marks and brands contained herein are the property of their respective owners.

CHANGE HISTORY

VERSION / REVISION	DATE	DESCRIPTION
1.0 / 0.36	10/24/23	• Draft for IWG Review
		•

CONTENTS

DISCLAIMERS, NOTICES, AND LICENSE TERMS 1
CHANGE HISTORY 2
Table of Figures 4
Table of Tables 5
1 SCOPE and Context 6
1.1 Audience 6
1.2 Key Words 6
1.3 Statement Type 6
2 Introduction 8
2.1 Glossary 8
2.2 Relationships to Other Documents 9
2.2.1 TCG Specifications 9
2.2.2 Non TCG Documents 10
2.3 Background 11
2.4 Composite RIMs 12
3 Requirements 14
3.1 Component RIM Information Model 14
3.1.1 Component RIM 14
3.1.2 TAG Roles 18
3.1.3 Requirements 19
Appendix A: References 22

Table of Figures

Figure 1 Representative Platform Composition 13

Table of Tables

Table 1 Glossary 8
Table 2 Component RIM Information Model 14
Table 3 Component RIM IM to SWID/CoSWID Mapping 15
Table 4 Component RIM IM to CoRIM/CoMID Mapping 17
Table 5 RIM Roles 18

1 SCOPE and Context

This Component Reference Integrity Manifest Information Model Specification (This Specification or This IM) complements information models for attestation (see section 2.2.1.1) by defining a Component Reference Integrity Manifest (RIM) Information Model (IM) for components of a platform, e.g., a PC Client or Server platform. Components of a platform may include microprocessors, integrated circuits, or might include printed circuit assemblies, such as a graphics adapter or a backplane for a server. This IM provides a basis for refinement in platform specific binding specifications. This RIM IM leverages the TCG Reference Integrity Manifest Information Model[3].

Attestation is a critical element of endpoint assessment and integrity management capability. Generation of Attestation evidence is a foundational element of several Trusted Computing use cases that rely on a Root of Trust such as DICE and TPM. Attestation evidence is used by Verifiers to determine the state of a platform. Evidence is presented to a Verifier by an Attester. The Verifier evaluates evidence using Reference Values asserted by Endorsers (aka supply chain entities).

This IM defines an abstract structure for assembling reference measurements that may be asserted by component manufacturers as expected values. Because component reference measurements may be provided to a platform manufacturer for inclusion in a platform RIM bundle or may be in a RIM provided by the component manufacturer directly to a Verifier, This Specification accommodates various schemas and encoding options (SWID[1] and [2], CoSWID [16], CoRIM [17]). This document does not specify a deployment model.

A Component RIM has several characteristics. These characteristics include:

- The entity or organization that created the RIM instance
- The entity or organization that produces reference values
- Inclusion of reference measurements, for example mutable component firmware and configuration, or immutable component code (e.g. ROM)
- What component and what attesting environment are associated with the RIM
- Integrity protection

This IM contains a superset of attributes and assertions to address a broad set of use cases. Inclusion of these attributes and assertions helps ensure semantic interoperability and promote good security practice.

1.1 Audience

This document aids in the creation of RIM binding specifications that define the formatting, structure, and usage guidelines for a given family of platforms. Verifier developers and component developers working with Component RIM binding specifications may need to refer to This Specification for Component RIM element definitions. RIM binding specifications define a realization of RIM information model definitions, including definition of formats, protocols, storage, and delivery methods used to instantiate and convey reference information to a Verifier. RIM binding specifications may define how RIMs are stored and retrieved, e.g., from a location on an Attester's platform. They may also need to refer to the TCG Reference Integrity Manifest Specification[3].

1.2 Key Words

The key words "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" in this document normative statements are to be interpreted as described in RFC-2119, Key words for use in RFCs to Indicate Requirement Levels.

1.3 Statement Type

Please note a very important distinction between different sections of text throughout this document. There are two distinctive kinds of text: informative comment and normative statements. Because most of the text in This Specification

will be of the kind normative statements, the authors have informally defined it as the default and, as such, have specifically called out text of the kind informative comment. They have done this by flagging the beginning and end of each informative comment and highlighting its text in gray. This means that unless text is specifically marked as of the kind informative comment, it can be considered a kind of normative statement.

EXAMPLE: Start of informative comment

This is the first paragraph of 1–n paragraphs containing text of the kind *informative comment* ...

This is the second paragraph of text of the kind *informative comment* ...

This is the nth paragraph of text of the kind *informative comment* ...

To understand the TCG specification the user must read the specification. (This use of MUST does not require any action).

End of informative comment

2 Introduction

This Specification extends the scope of attestation and endorsement from platforms to include components. The TCG Reference Integrity Manifest Information Model Specification[3] and TCG PC Client Reference Integrity Manifest Specification [4] define the contents and structure of endorsements for PC Client platform firmware. PC Client platforms embed components from third parties that contain firmware. The PC Client Platform Firmware Profile [22] defines component firmware measurements made by platform firmware and the method of measurement.

The purpose of This Specification is to:

1. Define an information model that provides a foundation for Component RIM binding specifications.
2. Describe an Information Model baseline with common elements that a Verifier can support:
    a. Verifiable cryptographic identities used by a RIM creator identity.
    b. Verifiable cryptographic integrity verification of RIM structures.
    c. Support for references to the RIM Binding specification used to realize a RIM structure.
3. Describe the lifecycle of a Component RIM.
4. Support endorsement of measurements embedded in a platform, such as DICE or SPDM [19] based measurements.
5. Support the definition of separable and composable elements that can be assembled to form a coherent description of the integrity posture of a platform.
6. Support multiple types of platforms from simple IoT devices to complex servers.
7. Support TCG Firmware Integrity Measurement (FIM) [5] requirements.
8. Enable Verifiers to determine the type of RIM data (DICE, SPDM or other), the Target Environment and allow correlation between References, measurements, and the target environment.

2.1 Glossary

This Specification uses the following terms as defined below in Table 1 Glossary.

Table 1 Glossary

Term	Definition
Component	An element of a platform that comprises one or more integrated circuits with firmware and ROM, each of which may be supplied by different vendors and have different configurations of firmware and/or ROM.
Platform	A platform is comprised of one or more components assembled and working together to deliver a specific computing function but does not include any software other than the firmware that is part of the components in the platform. Examples of platforms include a notebook, a desktop, a server, a network switch, a blade, etc. See NIST SP 800-193 [23]
RIM	Reference Integrity Manifest, an Endorsement of a set of Reference Values and meta data associated with the Attesting Environment.
Assertions	See the TCG Reference Integrity Manifest (RIM) Information Model [3]
Evidence	See Section TCG Attestation Framework and the TCG Attestation Framework [10]
Verifiers	See Section TCG Attestation Framework and the TCG Attestation Framework [10]
Tag	Defined in the SWID ISO specification [1]
Primary Tag	Defined in the SWID ISO specification [1]
Patch Tag	Defined in the SWID ISO specification [1]
Supplemental Tag	Defined in the SWID ISO specification [1]

Security Version Number (SVN)	The version number of a component that indicates which security relevant updates have been applied to the component.
Globally Unique Identifier (GUID)	Defined in the SWID ISO specification [1]
Object Identifier (OID)	Defined by IETF RFC 5280 [14]
Universal Unique Identifier (UUID)	Defined by IETF RFC 4122 [15]
Binding Specification	A TCG specification that tailors the requirements in an Information Model for specific use cases. A binding spec does not loosen requirements of the Information Model but might further constrain the Information Model, define encoding requirements, and possibly standardized values for specific fields.
Support File	See the TCG Reference Integrity Manifest (RIM) Information Model [3]

2.2 Relationships to Other Documents

2.2.1 TCG Specifications

Start of informative comment

The following sections summarize some TCG specifications that define or use assertion.

End of informative comment

2.2.1.1 TAP

Start of informative comment

TCG's Trusted Attestation Protocol (TAP) Information Model specification [9] defines the information elements used by Verifiers of platform RIMs. Not all information elements are required by every Verifier.

End of informative comment

2.2.1.2 TCG RIM Information Model

Start of informative comment

The Reference Integrity Measurement (RIM) Information Model (IM) specification [3] defines an abstract structure for assembling reference measurements (Assertions) asserted by manufacturers and other supply chain entities as expected values. The RIM IM requires a binding specification to define a realization of a RIM information model definitions.

End of informative comment

2.2.1.3 TCG PC Client RIM

Start of informative comment

This PC Client RIM specification [4] complies with the RIM Information Model and is a binding specification for the RIM IM on PC Client and Server platforms. It describes the RIM file formats, RIM storage locations within the PC Client, and provides references for the content of the RIM support files.

End of informative comment

2.2.1.4 TCG FIM

Start of informative comment

The PC Client Firmware Integrity Measurement (FIM) specification [5] outlines the basic process for collecting, reporting, and processing (attestation) of PC Client firmware. It also provides requirements for and a mechanism to relate a Platform Certificate compliant with the TCG Platform Certificate Profile Specification [5].

End of informative comment

2.2.1.5 TCG Attestation Framework

Start of informative comment

TCG Attestation Framework Part 1 [10] is a common reference for attestation terminology and concepts, to enable designers of attestation solutions to better specify, describe, and standardize interoperable systems. It contains a description of the TCG attestation framework and associated properties. This document is not yet published.

End of informative comment

2.2.1.6 TCG Platform Certificate

Start of informative comment

The TCG Platform Certificate Profile specification [5] contains assertions about trust made by a platform manufacturer. The certificate asserts the platform's security properties and configuration as shipped. The Platform Certificate Profile defines a mechanism that can be used to incorporate a Component Certificate that might be coupled with a Component RIM.

End of informative comment

2.2.1.7 DICE Attestation Architecture

Start of informative comment

The DICE Attestation Architecture [5] defines an attestation architecture for DICE layering architectures.

End of informative comment

2.2.1.8 DICE Endorsement Architecture for Devices

Start of informative comment

The DICE Endorsement Architecture for Devices [5] describes the role of endorsement structures in attestation, the composition of an endorsement manifest schema that describes hardware (devices and components), how vendors might define relevant Claim sets, and how those Claim sets can be represented in an interoperable, machine-readable format. It further describes how to construct manifests that describe devices having multiple components and multiple component vendors that each might issue endorsement manifests.

End of informative comment

2.2.2 Non TCG Documents

Start of informative comment

This section identifies industry (non-TCG) information model specifications for manifest structures.

End of informative comment

2.2.2.1 DMTF Security Protocol and Data Model Specification (SPDM)

Start of informative comment

DTMF DSP0274 Security Protocol and Data Model Specification (SPDM) [19] defines the data structures and mechanisms for a caller to authenticate the identity of an SPDM device and/or obtain a measurement of the device's state for the purposes of attestation.

End of informative comment

2.2.2.2 NISTIR 8060

Start of informative comment

The National Institute for Standards and Technology Interagency Report (NISTIR) 8060 [2], "Guidelines for the Creation of Interoperable Software Identification (SWID) Tags" is one of the references for the elements described in This IM. NIST IR 8060 pulls its definitions from ISO-IEC 19770-2 [1] which is accessible on the NIST website. Because This Specification is focused on integrity of component firmware, there are further restrictions and additional requirements for the information elements above and beyond the guidelines found in NISTIR 8060.

End of informative comment

2.2.2.3 ISO-IEC 19770-2 (SWID)

Start of informative comment

ISO-IEC 19770-2 [1] International Organization for Standardization/International Electrotechnical Commission "Software identification tag" is known as the "SWID Specification" and is the main reference source for NIST IR 8060.

End of informative comment

2.2.2.4 CoSWID

Start of informative comment

Concise Software Identifiers (CoSWID) [16] defines a concise representation of ISO/IEC 19770-2:2015 Software Identification (SWID) tags that are interoperable with the XML schema definition of ISO/IEC 19770-2:2015 and augmented for application in Constrained-Node Networks.

End of informative comment

2.2.2.5 CoRIM

Start of informative comment

Concise Reference Integrity Manifest (CoRIM) [17] represent Endorsements and Reference Values in CBOR [12] format. Composite devices or systems are represented by a collection of Concise Model Identifier (CoMID) and Concise Software Identifiers (CoSWID) bundled in a CoRIM document.

End of informative comment

2.2.2.6 XML Signature Syntax and Processing

Start of informative comment

XML Signature Syntax and Processing Version 2.0 [18] is an informative W3C Working Group Note that describes XML digital signature processing rules and syntax. XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.

End of informative comment

2.2.2.7 CBOR Object Signing (COSE)

Start of informative comment

CBOR Object Signing [13] describes how to create and process signatures, message authentication codes, and encryption using CBOR for serialization. The signature format is used by CoSWID [16] and CoRIM [17].

End of informative comment

2.2.2.8 IANA CBOR Tags Registry

Start of informative comment

CBOR Tags are defined in the IANA registry [21]. That registry assigns identifiers that are used by Component RIMs.

End of informative comment

2.3 Background

Start of Informative Comment

There are different types of component assemblies, ranging from a simple integrated circuit with firmware and some ROM to printed circuit board assemblies consisting of multiple integrated circuits, each of which may be supplied by different vendors and have different configurations of firmware and/or ROM. This Specification supports these different types of components, which vary in complexity. To help a Verifier, This Specification defines Component RIMs as composable elements. Figure 1 provides an example of platform composition in relation to the various RIMs that may be available.

A Component RIM contains identifying information that describes the composition of the component, its Attesting Environment, an endorsement by one or more authorities or Endorsers, and potentially references to related RIMs. A Component RIM also contains one or more reference measurements that the Endorser asserts are “correct” for that class of component and firmware.

There are various schemas and encoding methods for RIMs. A Component RIM may use the schema for a SWID or CoSWID tag, as defined in the TCG RIM Information Model [3], or it may use the schema for a CoRIM, as defined in [17]. This Specification defines a RIM IM with each of these schemas in mind. Platform binding specifications may limit the format of the Component RIM.

End of informative comment

2.4 Composite RIMs

Start of informative comment

A Composite RIM is a Base RIM that includes or references other Base RIMs. As defined in [3], there may be scenarios in which multiple entities participate in the supply chain of a given device. That in turn may lead the Verifier to retrieve multiple RIM Bundles to verify the device. Such a scenario may require a RIM Bundle associated with the device to include or provide references to other RIM Bundle(s) being managed by other entities.

Consider a modern PC or Server manufacturer that includes components from various component vendors (e.g., disk drive, memory, CPU’s, etc.). Each component vendor may have its own RIM that corresponds to Firmware running on the component. The PC or Server manufacturer may wish to include or reference a component RIM in its own RIM without corrupting the original component RIM’s signature. The PC or Server Manufacturer may also want its own signature on the RIM to include coverage of all the component RIMs. As exemplified below in the text and in Figure 1 Representative Platform Composition, the inclusion of Component RIM reference within a PC manufacturer’s RIM is illustrated as follows:

```
PC_BaseRIM
 |-------> PC_Support RIM
 |-------> Component1_BaseRIM
 |            |-------->Component1_Support RIM
 |-------> Component2_BaseRIM
 |            |-------->Component2_Support RIM
 |            |-------->SubComponentA_BaseRIM
 |                          |-------->SubComponentA_Support RIM
End
```

The Composite RIM payload would include the PC Manufacturer Support RIM and a set of Base/Support RIMs for each component Manufacturer.

This Specification enables component RIMs of various encoding schemes such as CoMID, CoRIM, CoSWID, or SWID schemas, thus resulting in the following:

```
PC_BaseRIM
 |-------> PC_Support RIM (SWID Tag)
 |------> Component1_BaseRIM (SWID Tag)
 |            |-------->Component1_Support RIM
 |-------> Component2_BaseRIM (SWID Tag)
```



```
|            |------->Component2_Support RIM (CoRIM/CoMid)
|            |------->SubComponentA_BaseRIM (SWID Tag)
|                          |-------->SubComponentA_Support RIM
|-------> Component3_RIM (CoSWID)
|-------> Component4_RIM (CoRIM/CoSWID)
End
```

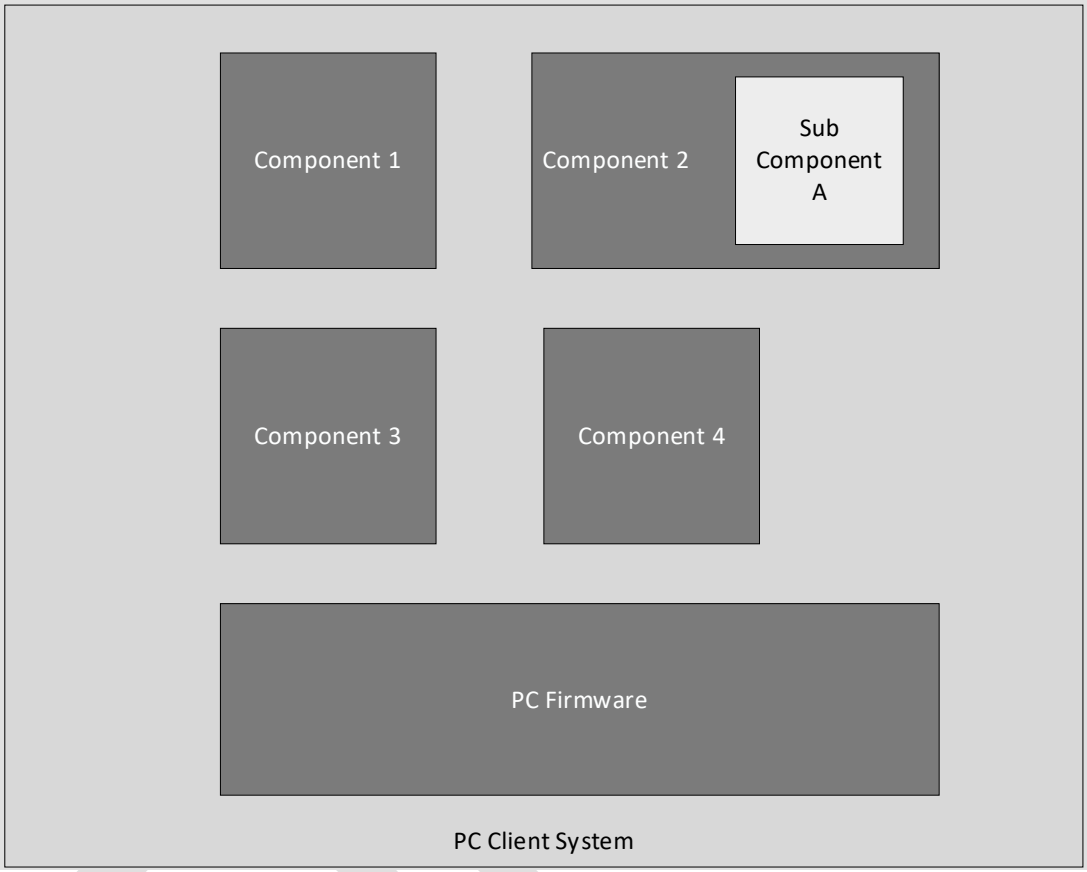

Figure 1 Representative Platform Composition

End of informative comment

3 Requirements

3.1 Component RIM Information Model

Start of informative comment

This section defines the mandatory and optional attributes of a Component RIM. Optional attributes may be made mandatory by a platform binding specification such as the TCG PC Client Firmware Integrity Measurement Specification [5].

End of informative comment

3.1.1 Component RIM

Start of informative comment

This IM contains a set of schema-agnostic elements defined in Table 2 Component RIM Information ModelTable *3* Component RIM and the following sections. The elements are further mapped to schema-specific names in Table 3 Component RIM IM to SWID/CoSWID Mapping and Table 4 Component RIM IM to CoRIM/CoMID Mapping. The Required column in Table 2 Component RIM Information Model indicates whether the attribute is required for compatibility with This Specification. Table 1 groups the elements by their Attestation Category. The order defined in Table 1 does not necessarily correspond to any order allowed or required by a RIM's schema. Note that the SWID and CoSWID schemas mandate a particular order of elements, while CoRIM and CoMID do not, but that order is not defined in This Specification.

The RIM Lifecycle types include initial, patch, and supplemental. An Initial RIM or Primary RIM is provided with the first firmware revision available for the Component. Primary RIMs are also provided when all measurements change based on the revision of firmware applied to the Component, or when a RIM issuer wishes to endorse all measurements anew instead of issuing a Patch RIM to be used alongside a particular Primary RIM. A Patch RIM can be used when a subset of the reference values is modified by a firmware update and thus includes only the modified values.

A Supplemental RIM is recommended for use when a VAR or Owner adds components to a system or makes configuration changes that result in additional measurements. In this case, the Supplemental RIM contains the reference values for the additional components.

Both Patch RIMs and Supplemental RIMs are used with a Primary RIM: but where a Patch RIM replaces values present in the Primary RIM, a Supplemental RIM adds values to those contained in the Primary RIM.

End of informative comment

Table 2 Component RIM Information Model

Attestation Category	General Name	Description	Mandatory / Optional
Endorsement Identity	Tag Identity	Unique Identifier of the RIM	M
	Tag Version	Version of the RIM **Note:** This version represents the version of the RIM or the patch or supplemental RIM, not the Component firmware version	M
Tag Lifecycle	Tag Lifecycle Type	Information indicating whether this is an initial RIM or a patch or supplement to an initial RIM	O1
	Previous Tag Hash	Hash of any related tag in the Tag lifecycle	O
	Previous Tag URI	Link to a repository of a related Tag in the lifecycle	O
	URI for FW Package	Link to a repository of the installation package for the firmware that corresponds to reference values encompassed by this RIM	O
	Endorser	Name of the Entity endorsing this tag	M

Endorser Identity	Endorser URI	URI of the Endorser	O
	Endorser Role	Role of the Endorser. See section 3.1.2 TAG Roles	M
Attesting Environment	Attesting component model	Model Number or Name of the Component that provides Evidence corresponding to the RIM	M
	Attesting component version	Version Number of the Component that provides Evidence corresponding to the RIM	O
	Attesting Component Manufacturer	Manufacturer of the Component that provides Evidence corresponding to the RIM	O
	Attesting Component FW version	Version of the firmware corresponding to the RIM	M
	Attesting Component FW SVN	Security Version of the firmware corresponding to the RIM	O
Additional Info	Component Identity or Attribute Cert URI	URI to obtain an Attribute or Identity Certificate for the Attesting Component	O
	Binding Spec Name	Name of the Binding Specification with which the RIM complies	M
	Binding Spec Version	Version of the Binding Specification with which the RIM complies	O
Reference Values	Reference Value Location	Indicates whether the Reference Values are included in the Tag directly or by reference	M
	Reference Value Collection Type	If included by reference, indicates the format of the reference value artifact. If included directly, indicates the Reference Value or Reference Value Collections.	O1
	Reference Value Name	If included by reference, this is the Name of the Reference Value artifact	O1
	Reference Value or Reference Value Collection size	If included by reference, this is the size of the Reference Value artifact	O1
	Reference Value or Reference Value Collection Hash	If included by reference, this is the hash of the Reference Value artifact	O1
	Reference Value Attributes	If included by reference, provides information about the referenced object	O1
Endorsement	Signature	The Endorsement over the Tag	M

Note: O1 indicates the element is conditionally optional

Table 3 Component RIM IM to SWID/CoSWID Mapping

Attestation Category	General Name	SWID Elements	CoSWID Elements
Endorsement Identity	Tag Identity	tagID	tag-id
	Tag Version	tagVersion	tag-version
Tag Lifecycle	Tag Lifecycle Type	patch	patch
		supplemental	supplemental
	Previous Tag Hash	rimLinkHash	N/A

	Previous Tag URI	previousTagURI	Link-entry.href, link-entry. rel=supersedes
	URI for FW Package	installationMediaURI	Link-entry.href; link-entry. Rel=installationmedia
Endorser Identity	Endorser	Name	Entity-entry.entity-name
	Endorser URI	regID	Entity-entry.reg-id
	Endorser Role	Role	Entity-entry.role
Attesting Environment	Attesting component model	componentModel	Software-name
	Attesting component version	componentVersion	Software-version
		colloquialVersion	Software-meta-entry.colloquial-version
		Edition	Software-meta-entry.edition
		Product	Software-meta-entry.product
	Attesting Component Manufacturer	componentManufacturerStr	N/A
		componentManufacturerID	N/A
	Attesting Component FW version	firmwareVersion (Revision in RIM IM)	Software-meta-entry.revision
		firmwareSVN (firmwareVersion in RIM IM)	N/A
Additional Info	Component Identity or Attribute Cert URI	componentLocator (pcURIglobal in RIM IM))	Software-meta-entry.persistent_id
	Binding Spec Name	bindingSpec	N/A
	Binding Spec Version	bindingSpecVersion	N/A
Reference Values	Reference Value Location	payloadType	N/A
	Reference Value Collection Type	file, directory, process and/or resource	Payload-entry.resource-collection.path-elements-group, process-entry, resource-entry
	Reference Value Name	Name	File-entry.filesystem-item.fs-name
	Reference Value or Reference Value Collection size	Size	File-entry.size
	Reference Value or Reference Value Collection Hash	Hash	File-entry.hash
	Reference value Collection Link	supportFileLink	N/A
	Reference Value Collection Hash	supportFileHash	N/A
	Reference Value Attributes	supportRimType	N/A
		supportRimFormat	N/A
		supportRimUriGlobal	N/A
Endorsement	Signature	sigAlgorithm	sigAlgorithm
		hashAlgorithm	hashAlgorithm

		keyInfoReference	keyInfoReference
		digest	Digest
		timestamp	N/A
		signature	N/A

Start of Informative Comment

CoRIM, as defined in [17], is a signed encapsulation of other elements that can be CoMID or CoSWID elements. CoMID elements are not signed and cannot exist without a CoRIM encapsutation. CoSWID elements are signed and can be provided as a RIM without a CoRIM, but when included as elements in a CoRIM encapsulation, their signature is removed.

CoRIM does not stand on its own, and thus does not fulfil the requirements of the Component RIM IM without a CoMID or CoSWID element.

End of Informative Comment.

Table 4 Component RIM IM to CoRIM/CoMID Mapping

Attestation Category	General Name	CoRIM elements	CoMID elements
Endorsement Identity	Tag Identity	corim-map.id	tag-identity-map.tag-id
	Tag Version	N/A	tag-identity-map.tag-version
Tag Lifecycle	Tag Lifecycle Type	N/A	linked-tag-map.tag-rel (tag-rel-type-choice=supplements)
	Previous Tag Hash	N/A	N/A
	Previous Tag URI	N/A	concise-mid-tag.linked-tags
	URI for FW Package	corim-map.corim-locator-map	N/A
Endorser Identity	Endorser	N/A	entity-entry.entity-name
	Endorser URI	N/A	entity-entry.reg-id
	Endorser Role	corim-entity-map.corim-role-type- choice	comid-entity-map.comid-role-type-choice
Attesting Environment	Attesting component model	N/A	class-map.model
	Attesting component version	N/A	measurement-values-map.version
	Attesting Component Manufacturer	N/A	class-map.vendor
	Attesting Component FW version	N/A	class-map.class-id
		N/A	measurement-values-map.version
	Attesting Component FW SVN	N/A	measurement-values-map.svn
Additional Info	Component Identity or Attribute Cert URI	corim-locator-map	N/A
	Binding Spec Name	N/A	N/A
	Binding Spec Version	N/A	N/A

Reference Values	Reference Value Location	N/A	CBOR Tags (for CoRIM and CoMID)
	Reference Value Collection Type	N/A	N/A
	Reference Value Name	N/A	measurement-values-map.name
	Reference Value or Reference Value Collection size	N/A	N/A
	Reference Value or Reference Value Collection Hash	N/A	measurement-values-map.digests
	Reference Value Attributes	N/A	corim-locator-map
		N/A	N/A
		N/A	N/A
		N/A	N/A
		N/A	corim-map.corim-locator-map
Endorsement	signature	AlgorithmIdentifier	n/a
		KeyID	n/a
		IV (Optional)	n/a
		PartialIV (Optional)	n/a
		Signature	n/a

3.1.2 TAG Roles

Start of informative comment

Different roles may exist, depending on the encoding chosen for the RIM. Table 5 RIM Roles maps the roles for the encoding options to the roles defined for This Specification.

This Specification normatively defines the roles in the column labeled “Component RIM IM”, in Table 5 RIM Roles. The other roles in Table 5 RIM Roles are normatively defined in the specifications stated in the column heading.

Note: This IM mandates a minimum set of Roles. Binding specifications may require additional Roles.

End of informative comment

Table 5 RIM Roles

RIM Roles	**Component RIM IM**	**SWID** [1]	**CoSWID** [16]	**CoMID** [17]	**CoRIM** [17]
Tag Creator	tagCreator	tagCreator	tagCreator	tag-creator	n/a
SW/FW Creator	softwareCreator	softwareCreator	softwareCreator	creator	n/a
Manifest Creator	tagCreator	tagCreator	tagCreator	n/a	manifest-creator
Tag Endorser	tagSigner	tagSigner	TagSigner	n/a	corim-signer

A Component RIM SHALL support the following RIM Roles:

1. Tag Creator (Tag or Manifest)
2. Tag Endorser

3.1.3 Requirements

3.1.3.1 Endorsement Identity and Life Cycle Elements

Start of informative comment

The Endorsement Identity and Life Cycle Elements provide a Verifier with the information necessary to correlate a RIM to its associated version of firmware or ROM and the measurements collected that version of firmware or ROM within its Attesting Environment.

End of informative comment

1. The componentModel attribute value SHALL be unique to a class of component from a given component manufacturer.
2. The Tag Identity SHALL be universally unique within the component vendor name space, e.g., a GUID, OID or string.
3. If a RIM is a patch RIM, the patch flag SHALL be present and set to TRUE.
4. If a RIM is a supplemental RIM, the supplemental flag SHALL be present and set to TRUE.
5. The patch flag SHALL NOT be set if the supplemental flag is set.

3.1.3.2 Endorser Identity Element

Start of informative comment

The Endorser Identity Element contains the information about the entities that play a role in the development of the component and the creation of the Component RIM. Each role is associated with an Endorser Identity. The simplest case is a single Endorser that fulfils the roles of tagCreator, tagSigner, and softwareCreator. To enable a broad set of platform and component types, this information model provides for, but does not require, multiple Endorser Identities to be represented in the RIM.

End of informative comment

1. A RIM SHALL contain at least one Endorser Identity corresponding to the creator of the Tag. See section 3.1.2 TAG Roles.
2. The Endorser and Endorser Role attributes for the Endorser Identity SHALL be populated.

3.1.3.3 Attesting Environment Element

Start of informative comment

The Attesting Environment Element contains additional information useful for a Verifier to associate a RIM with a particular Attesting Environment, as well as the binding specification information with which the RIM complies.

End of informative comment

1. The Attesting Component Model attribute SHALL be present.

3.1.3.4 Additional Information Element

Start of informative comment

The Additional Information Element contains information that a Verifier might use to enable correlation of the RIM to a particular component, such as a reference to a Component Identity Certificate, and enable understanding the schema of the RIM, such as the Binding Specification element, which might define the schema.

The Binding Spec Name attribute SHALL be present.

3.1.3.5 Reference Values Element

Start of informative comment

The Reference Value Element contains the Reference Values or a link to the support files. Additional constraints may be applied by binding specifications.

End of informative comment

1. The Reference Value Location Attribute SHALL be present.
2. If the Reference Value Location Attribute is present and contains a CBOR Tag:
    a. The CBOR Tag SHALL be a valid IANA registered Tag, see [21].
3. If the Reference Value Location Attribute is present and contains a reference to a file containing the Reference Values:
    a. The Reference Value Collection Type attribute SHALL be present and SHALL contain a schema specific value describing the Reference Value Collection.
    b. The Reference Value Name attribute SHALL be present and include the name of the file containing the Reference Values.
    c. The Reference Value Size attribute SHALL be present and include the size of the file containing the Reference Values.
    d. The Reference Value Hash SHALL be present and SHALL contain a Hash of the Reference Value file.
4. If the Reference Value Location Attribute is present and contains the string “Direct”:
    a. The Reference Value Hash SHALL be present and SHALL contain one or more Reference Values.

3.1.3.6 Signature Element

Start of informative comment

The Signature element constitutes a single “endorsement”.

It is helpful if the binding specification can include test sample(s) that illustrate how the signature element is applied.

The binding specification is responsible for defining the encoding of the Signature element and defining the various attributes contained within the signature element necessary for a verifier to be able to verify the signature.

End of informative comment

3.1.3.7 Layered Endorsements

Start of informative comment

Multiple entities may provide more than one independent signature on a single Base RIM. Binding specifications may include descriptions of how multiple signature elements from multiple parties can be applied to the Base RIM.

The addition of multiple signature elements is optional and does not preclude the use of Base RIM signed by a single tagCreator.

End of informative comment.

3.1.3.8 Timestamps

Start of informative comment

A RIM signer can include a timestamp to note the time that the Base RIM was signed by the tagCreator. There exist two timestamp scenarios of interest:

Countersignatures: Allowing a Trusted Third Party (TTP) authority to create a timestamp that can vouch for the fact that the RIM was signed at the specified time by the signer of the RIM. The countersignature is typically valid for a longer time than the RIM signature, which allows for validation of the RIM after the signer's certificate has expired.

Verifier RIM Policy: The Verifier may have policies that take into the account the time the RIM was created for determining the validity of the measurements within the RIM. For instance, a Verifier might impose an expiration date on a RIM.

The binding specification provides a definition of a timestamp to be included as part of the Base RIM's signature if it is permitted or required by the binding specification.

End of informative comment

Appendix A: References

[1] ISO/IEC 19770-2:2015 International Organization for Standardization/International Electrotechnical Commission, Information technology -- Software asset management -- Part 2: Software identification tag, ISO/IEC 19770-2:2009, November 2009. https://www.iso.org/standard/65666.html

[2] NISTIR-8660, “Guidelines for the Creation of Interoperable Software ID (SWID) Tags”, April 2016, https://csrc.nist.gov/publications/detail/nistir/8060/final

[3] TCG, “TCG Reference Integrity Manifest (RIM) Information Model”, version 1.00 Revision 0.16, November 2020, https://trustedcomputinggroup.org/resource/tcg-reference-integrity-manifest-rim-information-model/

[4] TCG, “TCG PC Client Reference Integrity Manifest”, version 1.4, November 2020, https://trustedcomputinggroup.org/resource/tcg-pc-client-reference-integrity-manifest-specification/

[5] TCG, “TCG PC Client Platform Firmware Integrity Measurement”, Version 1.0, Revision 43, May 2021, https://trustedcomputinggroup.org/resource/tcg-pc-client-platform-firmware-integrity-measurement/

[6] TCG, “TCG Platform Certificate Profile”, Version 1.1 Revision 19, April 2020, https://trustedcomputinggroup.org/resource/tcg-platform-certificate-profile/

[7] TCG, “DICE Attestation Architecture”, Version 1.0 Revision 0.23, March 2021, https://trustedcomputinggroup.org/resource/dice-attestation-architecture/

[8] TCG, “DICE Endorsement Architecture for Devices”, Version 1.0 Revision 0.38, November 2022, https://trustedcomputinggroup.org/resource/dice-endorsement-architecture-for-devices-v1-0-r0-38/

[9] TCG, “TCG Trusted Attestation Protocol (TAP) Information Model for TPM families 1.2 and 2.0 and DICE family 1.0”, Version 1.0 Revision 0.36, September 2019, https://trustedcomputinggroup.org/resource/tcg-tap-information-model/

[10] TCG draft, “TCG Attestation Framework Part 1: Terminology, Concepts, and Requirements”, TBD

[11] IETF RFC-9334, “Remote ATtestation ProcedureS (RATS) Architecture”, January 2023, https://datatracker.ietf.org/doc/rfc9334/

[12] IETF RFC-8949, “Concise Binary Object Representation (CBOR)”, December 2020, https://datatracker.ietf.org/doc/rfc8949/

[13] IETF RFC-8152, “CBOR Object Signing and Encryption (COSE)”, July 2017, https://datatracker.ietf.org/doc/rfc8152/

[14] IETF RFC-5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, May 2008, https://datatracker.ietf.org/doc/rfc5280/

[15] IETF RFC-4122, “A Universally Unique IDentifier (UUID) URN Namespace”, July 2005, https://datatracker.ietf.org/doc/rfc4122/

[16] IETF RFC-9393, “Concise Software Identification Tags”, draft-ietf-sacm-coswid-23, February 2023, https://datatracker.ietf.org/doc/rfc9393/

[17] IETF draft, “Concise Reference Integrity Manifest”, draft-ietf-rats-corim-00, September 2022, https://datatracker.ietf.org/doc/draft-ietf-rats-corim/

[18] W3C Working Group Note, "XML Signature Syntax and Processing Version 2.0", 23 July 2015, https://www.w3.org/TR/xmldsig-core2/

[19] DMTF DSP0274, “Security Protocol and Data Model (SPDM) Specification”, Version 1.2.1, June 2022, https://www.dmtf.org/dsp/DSP0274

[21] IANA CBOR Tag Registry, https://www.iana.org/assignments/cbor-tags/cbor-tags.xhtml

[22] TCG PC Client Platform Firmware Profile for TPM 2.0 Systems Version 1.06 or later https://trustedcomputinggroup.org/resource/pc-client-specific-platform-firmware-profile-specification/

[23] NIST SP800-193 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

