TRUSTED® COMPUTING GROUP

ERRATA

Errata for TCG Reference Integrity Manifest (RIM) Information Model Version 1.01 Revision 0.16

Version 1
Revision 4
November 12, 2020

Contact: admin@trustedcomputinggroup.org

PUBLISHED

DISCLAIMERS, NOTICES, AND LICENSE TERMS

CHANGE HISTORY

REVISION	DATE	DESCRIPTION
1.00/1.00	July 22, 2020	• Initial Release of Version 1.00.
1.00/1.01	August 18, 2020	• Added use of camel case for table 1 attributes
1.00/1.02	September 4, 2020	• Added informative note for Appendix A
1.00/1.03	October 9, 2020	• Removed Clarification section and folded description information into errata
1.00/1.04	November 2, 2020	• Minor Grammar fixes

CONTENTS

1 Introduction

This document describes errata and clarifications for the TCG Reference Integrity Manifest Information Model v1.0 as published. The information in this document is likely – but not certain – to be incorporated into a future version of the specification. Suggested fixes proposed in this document may be modified before being published in a later TCG Specification. Therefore, the contents of this document are not normative and only become normative when included in an updated version of the published specification. Note that since the errata in this document are non-normative, the patent licensing rights granted by Section 16.4 of the Bylaws do not apply.

.

.

.

.

2 Errata

2.1 Table 1

ISO 19770-2 adopts a convention of Pascal-case (ThisIsAnExample) for Elements and sub-Elements and camel-case (thisIsAnExample) for attributes. Table 1 is inconsistent with that convention. Attribute names should be camelCase.

Camel-case corrections for Table 1:

Element Name	Old attribute spelling	Corrected attribute spelling
SoftwareIdentity	Name	name
Entity	Name	name
	Regid	regid
	Role	role
Link	Href	href
Meta	PayloadType	payloadType
	PlatformManufacturerStr	platformManufacturerStr
	PlatformManufacturerId	platformManufacturerId
	PlatformModel	platformModel
	PlatformVersion	platformVersion
	FirmwareManufacturerStr	firmwareManufacturerStr
	FirmwareManufacturerId	firmwareManufacturerId
	FirmwareModel	firmwareModel
	FirmwareVersion	firmwareVersion
	BindingSpec	bindingSpec
	BindingSpecVersion	bindingSpecVersion
	RIMLinkHash	rimLinkHash
Payload	Name	name
	Size	size
	Hash	hash

2.2 versionScheme

versionScheme is defined by NISTIR8060 and should be included as an optional attribute of the SoftwareIdentity element in Table 1. The notes column entry in Table 1 for this attribute should be:

> As described in NISTIR 8060 section 5.1.2

2.3 corpus default value

The corpus attribute in the SoftwareEntity element as described in Table 1 is optional. If it is not present, the attribute should be considered false.

The SoftwareIdentity element corpus attribute Notes column in Table 1 should append the following sentence:

> The default value is false.

2.4 patch default value

The patch attribute within the SoftwareEntity element as described in Table 1 is optional. If it is not present it the attribute should be considered false.

The SoftwareIdentity element patch attribute Notes column in Table 1 should append the following sentence:

> The default value is false.

2.5 supplemental default value

The supplemental attribute within the SoftwareEntity Element as described in Table 1 is optional. If the supplemental attribute is not present it the attribute should be considered false.

The SoftwareIdentity element supplemental attribute Notes column in Table 1 should append the following sentence:

> The default value is false.

2.1 rimLinkHash

The Meta element's rimLinkHash in Table 1 is required, yet section 4.1.6 states the rimLinkHash is not required for Primary Base RIM. The RIMLinkHash is also defined in section 4.1.6 as the hash of the RIM referenced by the Link element. The rimLinkHash should be listed as optional in Table 1.

2.2 Payload attribute notes

The Payload element Notes column entry in Table 1 pertaining to the payload element's File, Directory, Process, and/or Resource attribute should be:

"see section 4.1.2 . "

2.3 Payload name

The Payload element's name attribute in Table 1 should be listed as optional and the note should be:

"MUST be present for File, Directory, and Process. MUST contain the name of the measurement target if PayloadType="Direct" or Support RIM if PayloadType="Indirect"."

2.4 Payload size

The Payload element's size attribute in Table 1 should be optional and the note should be:

"MUST be present for File and Directory. Should contain the size (in bytes) of the reference."

2.5 Payload hash

The Payload element's hash attribute note in Table 1 should be:

> MUST contain a Hash that holds the digest of the reference.

2.6 hashAlgorithm

The Signature element's hashAlgorithm attribute in Table 1 should be optional.

2.7 digest

The Signature element's digest attribute in Table 1 should be optional.

2.8 RIM Binding Specification Guidelines

Appendix A should read as informative:

Start of informative comment

In addition to the requirements detailed in this specification the Binding Specification should address the following requirements:

1. The Base RIM should be digitally signed using a TCG listed digital signing algorithm [16].

2. The binding specification should format the signature field of the Base RIM and define how signatures are to be applied.

3. The binding specification should define the value used for the BindingSpec attribute within the Meta field.

4. The Base and Supplemental RIMs should be formatted using XML (as described by NISTIR 8060) or CBOR (as described by the IEFT CoSWID specification [12]).

5. The Base RIM should hold a payload element for every support RIM Bundle specified in the Binding specification.

6. Delivery of the initial RIM Bundle to the Verifier should be addressed by the Binding specification. Delivery may include placement on the platform during manufacturing or a URI based retrieval mechanism. The LINK element in the Base RIM provides information about the location of updates and should be included a RIM Bundle.

7. The RIM Binding specification should define how the Certificate Path used for the Validation of the RIM Bundle is to be obtained by a Verifier.

8. The binding specification should specify the use of a Platform Certificate and populate the PlatformConfigurationURI attribute.

End of informative comment

