TRUSTED® COMPUTING GROUP

SPECIFICATION

TCG PC Client Reference Integrity Manifest Specification

Version 1.1
Revision 11
April 26, 2024

Contact: admin@trustedcomputinggroup.org

PUBLISHED

DISCLAIMERS, NOTICES, AND LICENSE TERMS

Acknowledgement

The TCG wishes to thank those who contributed to this specification. This document builds on considerable work done in the various working groups in the TCG.

Special thanks to the members of the IWG group and others contributing to this document:

A.J. Stein	United States Government
Adonay Behre	AMI
Adrian Shaw	HP Inc.
Alberto Munoz	Intel Corporation
Amit Kapoor	Integrity Security Services, LLC
Amy Nelson	Dell, Inc.
Anas Arif	Intel Corporation
Antonio Javier Cabrera Gutierrez	Infineon Technologies
Bill Keown	Lenovo (United States) INC
Bill Sulzen	Cisco Systems
Brad Litterell	Microsoft
Brandon Weeks	Google Inc.
Carolin Baumgartner	Carolin Baumgartner
Chris Fenner	Google Inc.
Dan Morav	Nuvoton Technology Corporation
Dana Amsalem Cohen	Nuvoton Technology Corporation
Daniel Wong	Google Inc.
David Challener	David Challener
David Koplos	Micron Technology, Inc
David Safford	David Safford
Dennis Mattoon	Microsoft
Dick Wilkins	Phoenix Technologies
Donna Yu	Microsoft
Doug Ambrisko	Cisco Systems
Endrigo Pinheiro	HP Inc.
Eoin Carroll	Toyota Motor Corporation
Eric Hibbard	Samsung Semiconductor Inc.
Fabien Arrive	STMicroelectronics
Ferdinand Nolscher	Google Inc.
Fernando Tavares	Positivo Tecnologia S.A.
Florian Schweiger	Infineon Technologies
Frederick Otumfuor	AMI
Ga-Wai Chin	Infineon Technologies
Gongyuan Zhuang	Advanced Micro Devices, Inc.
Graeme Proudler	Graeme Proudler
Greg Kazmierczak	Greg Kazmierczak
Guy Fedorkow	Juniper Networks, Inc.
Henk Birkholz	Fraunhofer Institute for Secure Information Technology (SIT)
Isaac Asay	Advanced Micro Devices, Inc.
Jason Kolodziej	Dell, Inc.

Jason Young	Dell, Inc.
Jean Fioretti	WISeKey Semiconductors
Jeff Andersen	Google Inc.
Jen ye	Advanced Micro Devices, Inc.
Jerry Vacek	United States Government
Jesse Pool	Broadcom
Jiewen Yao	Intel Corporation
Joe Pennisi	NVIDIA Corporation
Jonathan Wilbur	Wildboar Software
Joshua Schiffman	HP Inc.
Ken Goldman	IBM
Lawrence Reinert	United States Government
Liqun Chen	University of Surrey
Ludovic Jacquin	NVIDIA Corporation
Michael Eckel	Fraunhofer Institute for Secure Information Technology (SIT)
Mike Boyle	United States Government
Monty Wiseman	Beyond Identity
Mukund Khatri	Dell, Inc.
Ned Smith	Intel Corporation
Nick Grobelny	Dell, Inc.
Patrick Debaenst	WISeKey Semiconductors
Patrick Gallo	United States Government
Paul England	Microsoft
Paul Stonelake	Micron Technology, Inc
Qi Huang	Advanced Micro Devices, Inc.
Rony Michaely	Lenovo (United States) INC
Silviu Vlasceanu	Huawei Technologies Co., Ltd.
Steve Clark	WISeKey Semiconductors
Subramanian Swaminathan	Juniper Networks, Inc.
Sven Schuch	Infineon Technologies
Theo Koulouris	Hewlett Packard Enterprise
Thomas Bowen	Intel Corporation
Thomas Deleuran	Huawei Technologies Co., Ltd.
Thomas Hardjono	MIT Connection Science
Thorsten Stremlau	NVIDIA Corporation
Todd Johnson	Cisco Systems
Tom Brostrom	Cyber Pack Ventures
Tom Dodson	Intel Corporation
Tom Laffey	Hewlett Packard Enterprise
Toru Tomita	NEC Corporation
Travis Gilbert	Dell, Inc.
Trevor Conn	Dell, Inc.
Vick Wei	Google Inc.
William Bellingrath	Juniper Networks, Inc.
Yucong Tao	Microsoft

Zachary Blum	United States Government
Zachary Halvorsen	Google Inc.
Zhang Li	Huawei Technologies Co., Ltd.
Zhoucan Gu	Google Inc.
Zhuo Liu	Huawei Technologies Co., Ltd.

CONTENTS

1 Scope and Context

Attester integrity and corresponding attestation evidence are critical to many use cases. DICE [21], TPM [22] and platform specifications [7] were designed to provide information - evidence helpful for Verifiers to determine the state of a platform - the Attester. To that end the TCG Trusted Attestation Protocol (TAP) Information Model specification [1] was created to outline the information presented by the Attester device to the Verifier. The TCG Reference Integrity Manifest (RIM) Information Model (IM) specification [12] compliments the TAP by providing common information elements used by the Verifier to validate the identity of the RIM's creator and the integrity of the support files used to provide the integrity reference information.

This PC Client RIM specification complies with the RIM Information Model and provides additional requirements for PC Client platforms that adhere to the TCG PC Client Platform Firmware Profile [7]. This specification describes the RIM file formats, RIM storage locations within the PC Client, and provides references for the content of the RIM support files.

This PC Client RIM is limited to the integrity reference information necessary for TPM Quote validation by a Verifier for measurements taken during the Attester's boot cycle. Other integrity processes, such as Integrity Measurement Architecture (IMA) [23] are beyond the scope of this specification.

1.1 Audience

This specification is intended to be used by: firmware developers that create firmware compatible with the PC Client Firmware Profile [7]; Verifier developers who need to know the formatting, structure, and usage guidelines for creating and processing a RIM Bundle; and platform developers that need to understand how to create and distribute RIM Bundles. This specification may also be beneficial to OS developers who manage TPM PCRs 8-15.

1.2 SCOPE

1. To describe the formatting for the common set information elements described by the TCG Reference Integrity Manifest (RIM) Information Model specification
2. To describe the RIM support files for PC Client platforms as required by the RIM Information Model specification.
3. To define default storage locations for RIM Bundles.

1.3 Relationships to other Documents

1.3.1 TCG Documents

There are many TCG documents that use the terminology of Reference Manifest (RM) and Reference Integrity Manifest (RIM). This specification defines the RIM for PC Client platforms.

1.3.1.1 RIM IM

The Reference Integrity Measurement (RIM) Information Model (IM) specification defines an abstract structure for assembling reference measurements (Assertions) that manufacturers and other supply chain entities assert as expected values. The RIM IM requires that a binding specification (this specification) defines a realization of RIM information model expressions.

1.3.1.2 TAP

The TCG Trusted Attestation Protocol (TAP) Information Model specification provides the information elements used by Verifiers. Not all of the information is required by every Verifier. The RIM is essential for TAP based attestation [1]. The TAP Information Model provides the reference material needed by the Verifier in order to implement the TAP Information Model. Future versions of the TAP Information Model specification may include gathering RIM information from the Attester.

1.3.1.3 FIM

The PC Client Firmware Integrity Measurement (FIM) specification [11] outlines the basic process for collecting, reporting, and processing (attestation) of PC Client firmware.

1.3.1.4 Platform Certificate Profile

The TCG Platform Certificate Profile specification [10] 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 PlatformConfigurationURI attribute that contains "URI where the reference integrity measurements could be obtained by the verifier". The RIM Information Model specification discusses options for the PlatformConfigurationURI attribute.

1.3.2 Non TCG Documents

1.3.2.1 NISTIR 8060

The National Institute for Standards and Technology Interagency Report (NISTIR) 8060 [3], "Guidelines for the Creation of Interoperable Software Identification (SWID) Tags" is the primary reference for the elements described in this specification. NIST IR 8060 uses definitions from ISO-IEC 19770-2 and is accessible on the NIST website. Because this specification is focused on integrity there are further restrictions and additional requirements for the information elements that are above and beyond the guidelines found in NISTIR 8060. Compliance with NISTIR 8060 is optional for this specification.

1.3.2.2 ISO-IEC 19770-2 (SWID)

ISO-IEC 19770-2 [4] 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.

1.3.2.3 XML Signature Syntax and Processing

The XML Signature Syntax and Processing Version 2.0 [8] 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.

1.4 Terms and Definitions

Asserter: A supply chain entity, manufacturer, vendor, or reseller that produces reference values.

Assertions: Reference values.

Attester: A platform or platform component that provides evidence to a Verifier as to its state.

Base RIM: The Base RIM is a RIM Bundle that provides a verifiable identity of the RIM creator and integrity information of support RIMs. The Base RIM contains a digest of each support RIM. The Base RIM also contains a signature.

Component RIM: A RIM bundle that applies to Firmware of a distinct make or model of a device that is integrated into a device that complies with the TCG PC Client RIM.

Composite RIM: A RIM Bundle that includes or references other Base RIM Instances in its payload element.

Endorsements: A protected statement from an entity (typically in a supply chain) that vouches for the trustworthiness of an Attester device.

Endorser: An entity that creates Endorsements that can be used to help evaluate the trustworthiness of Attesters.

GUID: Globally Unique IDentifier that is referenced by ISO 19970-2 and is technically identical to the UUID as specified by RFC 4122 [24].

Reference Integrity Manifest (RIM): A Reference Integrity Manifest contains structures that a Verifier uses to validate expected values (Assertions) against actual values (Evidence).

RIM Binding / Binding Specification: A specification that defines conventions for RIM (and RIM Bundle) formatting, marshalling, serialization, digesting, signing, encryption, realization, location, discovery, or storage. A RIM Binding / Binding Specification also describes how the information contained in a RIM Bundle is transmitted between Attesters and Verifiers. For example, a RIM Bundle may be marshalled for conveyance over an IP-based communication protocol or instantiated as a file or collection of files in a file system.

RIM Bundle: A collection of a single Base RIM and one or more Support RIMs. A Bundle is created by a single entity at a single point in time.

RIM Bundle Collection: A collection of RIM Bundles typically consisting of a Primary RIM Bundle and one or more Supplemental RIM Bundles.

RIM Creator: Manufacturer, System Integrators, Value Added Resellers, Information Technology (IT) support organizations, or endpoint platform owners that create a RIM instance for an Endpoint platform.

RIM GUID: A GUID created as a reference to a specific RIM Bundle. The RIM GUID can be used to link a RIM Bundle to multiple other RIM Bundles.

Supplemental RIM Bundle: Additional RIM Bundles added to a RIM Bundle Collection.

Support RIM: A Support RIM contains assertions about the state or configuration of the device to which the RIM applies (a.k.a., Reference Integrity Measurements).

SWID: Software ID tags as defined by ISO-IEC 19770-2.

SWID Schema: An XML schema that describes the structure of the SWID tag.

TCG Event Log: A log file created by the Core Base of Trust for Measurement (CRTM) that is defined in the TCG PC Client Platform Firmware Profile Specification [7].

TCG Event Log Expected Values: A TCG Event Log file, as defined by the PC Client Firmware Profile Specification [7], that is captured by a RIM creator and used as a RIM support file.

TPM PCR Expected Values: A TPM PCR structure that is saved to a file captured by the Primary RIM creator and used as a RIM support file (see section 3.2.1).

Verifier: A system that analyzes evidence from an Attester to determine the Attester's state.

1.5 Key Words

The key words "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" in this document's normative statements are to be interpreted as described in RFC-2119[2]. Key words for use in RFCs to Indicate Requirement Levels.

1.6 Statement Type

Please note a very important distinction between different sections of text throughout this specification. 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 Background

Start of informative comment

The TCG TPM 2.0 Provisioning Guidance [5] describes a set of Golden Measurements that “represent the expected default values of the integrity measurements which the boot firmware and subsequent code generates and extends into TPM PCRs”. The Provisioning Guidance document further states that Platform Manufacturers should deliver a list of expected integrity measurements of the platform BIOS, firmware, and other binaries they provide “as shipped”. Golden Measurements should be included in boot firmware updates, in order to support a given devices lifecycle.

The TCG PC Client Platform Firmware Profile [7] defines a TCG Event Log that captures hashes of firmware and software, firmware configuration settings, and events that are critical to boot operations of the device that extend into the TPM’s Platform Configuration Registers (PCRs). The TCG Event Log can be used by an Attester to serve as the “PCR Log Values” described in the TAP Model that is sent to the Verifier as part of an attestation request. The Verifier needs reference information in order to validate the log information being sent by the Attester.

The Verifier is also responsible for validating the Quote information sent by the Attester. The reference information is critical in terms of creating values that can be used to validate the TPM Quote.

A check of the PCR values from a TPM is necessary to ensure that the firmware and firmware configuration has not been altered during post processing and delivery of the Attester device. Once the Attester owner takes possession of the device, they can elect to create RIM bundles to track modifications made to the configuration of the device, if such modifications are required.

End of informative comment

3 PC Client Reference Integrity Measurement (PCRIM)

Start of informative comment

The TCG RIM Information Model specification describes a RIM Bundle that consists of a Base RIM and one or more Support RIM (files). The combination of Base and Support RIM represents a RIM Bundle. There may be many RIM Bundles (referred to a RIM Bundle Collection) depending upon the production cycle of a device and the device's associated distribution model.

A RIM Bundle is used by a Verifier as a reference for the appraisal process. To perform the appraisal process, the Verifier also needs an Event Log and a TPM Quote from an Attester (as described by the TAP). The values from the Attester are appraised against the PCRIM during a verification process.

The PCRIM adopts guidance as described by the TCG RIM IM (the information model). The following section assumes familiarity with the RIM IM and provides additional requirements for PC Clients.

End of informative comment

3.1 The PC Client Base RIM

Start of informative comment

The Base RIM for PC clients is instantiated as a File. The File contains elements as defined by the RIM IM with the additions or restrictions as noted in this section.

End of informative comment

3.1.1 Base RIM Format

The format of a Base RIM file for PC Clients MUST be compliant with the ISO/IEC19770-2 (SWID) specification [4] and follow the guidelines presented by NIST IR 8060 (the SWID guidance specification).

3.1.2 RIM Information Model Elements

This specification uses the definitions from Table 1 of the Reference Integrity Information Model specification except for the Elements shown in Table 1 of this specification:

Element	Attribute	Required	Notes
SoftwareIdentity	tagId	Yes	MUST be a GUID that is the same as the ReferenceManifestGuid created for the TCG Event Log's TCG_Sp800-155-PlatformId_Event field (refer to the TCG PC Client Platform Firmware Profile specification [7] for the definition of the TCG_Sp800-155-PlatformId_Event). The tagID MUST meet the requirements specified by RFC 4122 [13]
	version	Yes	MUST be set to the platform firmware version
Meta	bindingSpec	Yes	MUST be a String set to "PC Client RIM". "PC Client RIM" indicates that the RIM Bundle complies with the TCG PC Client RIM Binding specification (this specification)
	bindingSpecVersion	Yes	MUST be in the form of X.Y.Z where X is the major and Y is the minor revision of this specification and Z is the revision of the Errata. The default for errata version is 0
	pcUriGlobal	Yes	MUST be a URI equivalent to the URI found in the platformConfigURI attribute within the Attester's Platform certificate. The platformConfigURI attribute is defined in the TCG Platform Certificate Profile specification [10] and referenced in the TCG Firmware Integrity Measurement [11]
	pcUriLocal	Yes	SHOULD be set if the tagCreator stores the RIM bundle on the device
	payloadType	Yes	MUST be set to "Indirect"
Payload	supportRimFormat	Yes	As specified in section 3.2
	supportRimType	Yes	As specified in section 3.2
	supportRimUriGlobal	Optional	MAY be set to a URI to retrieve a copy of the Support RIM

Table 1: Changes to the RIM IM information elements

3.1.3 Base RIM Signatures

All RIMs MUST be digitally signed in compliance with W3C XML Signature Syntax and Processing Version 1.1 [8] with the following requirements:

1. The Base RIM MUST use the **Enveloped** signature.
    - **a.** The **KeyInfoReference** element (that provides details on where to get the information to validate the signature) MUST be populated. **KeyInfoReference** MUST use either **KeyName** or the **X509Data** element.
    - **b.** If the **KeyName** is used then **KeyName** SHOULD be set to the subjectKeyIdentifier of the signing certificate**.**
    - c. If the **X509Data** sub element is used to hold a signing certificate then a corresponding Link element MAY exist with a rel attribute set to "signing certificate". The corresponding href value MUST be set to "embedded". Self signed certificates MUST NOT be used in this field.
2. The Base RIM MUST use a TCG listed algorithm as a **hashAlgorithm**.
3. The Base RIM MUST use a TCG listed algorithm as a **sigAlgorithm**.

3.1.3.1 Layered Endorsements

Start of informative comment

In some cases, there may be a need for an entity that is not the tag creator to provide a secondary signature for the RIM (e.g., a layered endorsement). The PC Client RIM utilizes the W3C defined "Detached Signature" for providing secondary signatures to be applied to an existing signed PC Client RIM. The initial Base RIM uses the enveloped signature provided by the tagCreator. Each secondary signature will be a sibling element of the BaseRIMs SoftwareIdentity element. The secondary signature uses the Base RIM's tagId as the SignedInfo Reference. In this way, multiple signatures can be appended to the BaseRIM as illustrated by the following example:

Company_A Base RIM with signature element (tagId=2345)

Company_B_Signature (ID=2345)

Company_C_Signature (ID=2345)

End of informative comment

1. When applying a secondary signature, the secondary signing entity MUST use the W3C detached signature [26].
2. Each detached signature's SignedInfo Reference MUST identify the BASE RIM by its SoftwareEntity tagId.
3. Each subsequent signature MUST add a signature as a sibling element.

3.1.3.2 Timestamps

Start of informative comment

This PC Client RIM optionally supports a simple timestamp or a countersignature timestamp. Time stamp services are typically provided by a commercial Time Stamp Authority (TSA). Most TSAs support the RFC 3161 Time-Stamp Protocol [27] but the time stamp itself may be encoded using a number of methods.

End of informative comment

3.1.3.2.1 Simple Timestamp

Start of informative comment

A simple timestamp is an optional way of capturing the exact time a PC Client Base RIM was signed.

The following is an example of a snippet of a Base RIM with a timestamp within a SignatureProperties:

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id=RimSignatureId>
...
<SignedInfo>
   <Reference URI="#SimpleTimeStamp">
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>nIn57kPcBgVTPJuE+KfPqiqnjT6EwR+BAGBbeZgZdyc=</DigestValue>
   </Reference>
</SignedInfo>
…
 <SignatureProperties>
   <SignatureProperty Id="SimpleTimeStamp" Target="RimSignatureId">
     <timestamp xmlns:rfc3339=https://www.ietf.org/rfc/rfc3339.txt dateTime= “2022-09-15T23:20:50.52Z /> 
```



```
    </SignatureProperty>
  </SignatureProperties>
...
</Signature>
```

Note that the inclusion of a Reference element within the SignedInfo element pointing to the timestamp object provides integrity protection by the Base RIMs signature.

End of informative comment

1. The PC Client RIM MUST use the timestamp tag within the signature properties element to encapsulate a Simple timestamp
2. The namespace of the simple timestamp MUST be https://www.ietf.org/rfc/rfc3339.txt
3. When using a simple timestamp, the timestamp value MUST be in the “Internet Date/Time” format as specified in RFC 3339.
4. The target of the SignatureProperties MUST be set to the ID of the Signature element.
5. The PC Client RIM MUST use a Reference Element that includes a digest of the SignatureProperty element used for the simple timestamp.

3.1.3.2.2 Countersignatures

Start of informative comment

There may be a need to provide a countersignature that can be used to validate the base RIM when the signing certificate of the BaseRIM has expired. A countersigning service can provide that facility. The format for a countersignature typically meets the countersignature definition found within RFC 3852 (Cryptographic Message Syntax) or is packaged as described in RFC 2315 (PKCS 7) [28] to meet Authenticode countersignature requirements.

The countersignature data, typically contained within the “Time Stamp Response" of the time stamp protocol, is base64 encoded and embedded in the Timestamp attribute within the SignatureProperties element. Creation of the timestamp and verification of the countersignature timestamp is outside the scope of this specification.

The following is an example of a snippet from a Base RIM with a countersignature within a SignatureProperties element:

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id=RimSignatureId>
...
<SignedInfo>
   <Reference URI="# CountersignedTimeStamp ">
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <DigestValue>nIn57kPcBgVTPJuE+KfPqiqnjT6EwR+BAGBbeZgZdyc=</DigestValue>
   </Reference>
</SignedInfo>
…
 <SignatureProperties>
   <SignatureProperty Id="CountersignedTimeStamp" Target="RimSignatureId">
   <timestamp xmlns:rfc3852=https://www.ietf.org/rfc/rfc3852.txt dateTime=“V5lIY4Cdqk2UH6W246hlz16hBv=” />
  </SignatureProperty>
 </SignatureProperties>
```


...

</Signature>

Where the countersignature data is base64 encoded and placed in the timestamp block. The inclusion of a Reference element within the SignedInfo element pointing to the timestamp object provides integrity protection by the Base RIM's signature.

End of informative comment

3.1.3.2.2.1 CMS (RFC 3852) Countersignatures

1. A PC Client RIM MUST use the timestamp tag within the SignatureProperties element to encapsulate an RFC 3852 countersignature timestamp.
2. When using RFC 3852 timestamps, the namespace used MUST be "https://www.ietf.org/rfc/rfc3852.txt".
3. The RFC 3852 countersignature data MUST be base 64 encoded prior to embedding in the Base RIM.
4. A PC Client RIM MUST use a Reference Element that includes a digest of the SignatureProperty element used for the Countersignature timestamp.

3.1.3.2.2.2 PKCS 7 (Authenticode) Countersignatures

1. The PC Client RIM MUST use the timestamp tag within the Signature element to encapsulate an Authenticode countersignature timestamp [9]
2. When using Authenticode countersignature timestamps the namespace used MUST be "https://www.ietf.org/rfc/rfc2315.txt"
3. The Authenticode countersignature data MUST be base 64 encoded prior to embedding in the Base RIM.
4. The PC Client RIM MUST use a Reference Element that includes a digest of the SignatureProperty element used for the Countersignature timestamp.

3.1.4 Base RIM signing certificates

Start of informative comment

The signer of the Base RIM needs to make the set of Certificates (aka the "Certificate path" used to validate the Base RIM) accessible to Verifiers.

End of informative comment

1. Signing Certificates MUST use TCG listed algorithms.
2. The Authority Information Access (AIA) extension SHOULD be used to define the location of all of the issuer certificates and the URI of the Online Certificate Status Protocol (OCSP) [20] responder (if supported by the Issuer's Certificate Authority).
3. The Validity period of the Issuing certificates SHOULD be longer than the expected service life of the device.

3.2 PC Client Support RIM

Start of informative comment

A Support RIM is a binary file containing the Events captured by the S-CRTM as specified by the PC Client Platform Firmware Profile [7] that correspond to the particular PCR the Support RIM covers, as determined by the pcrIndex value of the TCG_PCR_EVENT2 structure.

The Support RIM concept allows for multiple types of support RIM as specified by the supportRIMFormat attribute. This concept enables new formats to be defined in future versions of this specification. The current set of support RIM formats are by no means a comprehensive set of measurements possible for a specific device. Rather they are a snapshot of values as collected within the Event Logs or PCR values taken at the time of the production or modification of the equipment.

There are currently three formats defined for a PC Client support RIM: TPM PCR Assertion, TCG Event Log Assertions, and Partial TCG Event Log Assertions. The supportRimFormat attribute within the File attribute of the Payload element is used to determine the format being used for the support RIM.

The following section defines the currently defined support RIM formats and how the Support RIM are identified. Support RIM generation is outside the scope of this specification.

End of informative comment

The PC Client RIM Bundle:

1. MUST contain at least one Support RIM file.
2. MUST use the supportRimFormat attribute within the Payload File element within the Base RIM to note the support format(s) being specified.
3. The default value is for the supportRimFormat is “TCG_EventLog_Assertion”.

3.2.1 TPM PCR Assertions

Start of informative comment

TPM PCR Assertions are optional for those RIM Bundle creators that cannot utilize the Event Log Assertions due to device limitations or other restrictive conditions. TPM PCR Assertions lack the detail provided by the Event Log Assertions that are useful for diagnostic purposes. When possible, the Event Log Assertions are recommended to be used.

TPM PCR Assertions that are created by the Platform creator should include at least PCRs 0-7 if the Platform Manufacturer does not include an Operating System. The Platform Manufacturer may include other PCRs as appropriate.

TPM PCR Assertions that are created by entities other than the Platform creator (e.g., a Value Added Reseller) should include all PCRs whose values are different from those stated by the Platform Manufacturer. The Value Added Reseller may, however, include all PCRs.

One illustrative example is a Platform Manufacturer that installs firmware but not an Operating system. If the Platform Manufacturer is utilizing the TPM PCR Assertion support RIM then only PCRs 0-7 are included in the TPM PCR Assertion. If a Value Added Reseller adds a NIC card that changes only the value for PCR 2, and no other PCR values are affected, then the VAR should create a supplemental RIM Bundle that contains at least the new value for PCR 2. If the VAR installs an Operating System, the PCR 8-15 should be included as well.

End of informative comment

1. If the TPM PCR Assertions are used then the supportRimFormat attribute within the Base RIM MUST be set to “TPM_PCR_Assertion.”
2. TPM PCR Assertions MUST utilize the data from the output of the TPM2_PCR_Read command as defined in the Trusted Platform Module Library Part 3 [19]. The data is equivalent to TPM 2.0 PCR Values defined in the TCG Trusted Attestation Protocol (TAP) Information Model specification. According to the Trusted Platform Module Library Part 3 this information contains:

Type	Name	Description
UINT32	pcrUpdateCounter	The current value of the PCR update counter
TPML_PCR_SELECTION	pcrSelectionOut	The PCR in the returned list
TPML_DIGEST	pcrValues	The contents of the PCR indicated in pcrSelect as tagged digests

Table 2: TPM2_PCR_Read command output

3. The TPM PCR Assertion for a primary RIM Bundle MUST contain (at a minimum) values for the first eight PCRs (PCR 0-7). As an example, a Platform Manufacturer that does not install an Operating System would create a Support RIM of type TPM PCR Assertion that includes only PCRs 0-7.

4. The TPM PCR Assertions MUST include all supported TPM hash algorithms supported by the platform firmware and the TPM.

The Platform Manufacturer, System Integrator, or Value Added Reseller that adds an OS is recommended to create RIM Bundles that include new support RIM covering PCRs 8-15 at a minimum.

3.2.2 TCG Event Log Assertions

Start of informative comment

The TCG Event Log Assertion Support RIM is a binary file (no formatting) containing the Events captured by the S-CRTM as specified by the PC Client Platform Firmware Profile [7]. An example of the event log can be found in Appendix A: PC Client Base RIM Example.

End of informative comment

1. The TCG Event Log Assertions MUST use a supportRIMFormat attribute set to “TCG_Event_Log_Assertion”.
2. The support RIM MUST be a TCG Event Log as defined by the PC Client Platform.
3. The TCG Event Log Assertions for a primary RIM Bundle MUST contain (at a minimum) events corresponding to the first eight PCRs (PCR 0-7). As an example, a Platform Manufacturer that does not install an Operating System would create a Support RIM of type “TCG Event Log Assertion” that includes only events extended to PCRs 0-7.

3.2.3 Partial TCG Event Log Assertions

Start of informative comment

TPM Event Log Assertions effectively make the entity signing the RIM bundle the sole endorser of all the reference values contained therein. This may be restrictive in environments where responsibility for endorsing different parts of a platform’s overall state falls on separate entities (such as different manufacturers), or when management events (such as a boot order change) cause some reference measurements to change but not others. In such environments, using TCG Event Log Assertions forces the RIM Bundle creator to create a new Bundle after every event that results in a change to the contents of the current TCG Event Log, and in the process assume responsibility and endorse reference measurements it may not be in a position to verify.

Partial TCG Event Log Assertions address this problem by allowing different entities to assume responsibility for endorsing different parts of a platform’s overall state. This is accomplished by having each Support RIM in a RIM Bundle provide reference values for events that correspond to a particular PCR. Specifically, where in the TCG Event Log Assertions format the single Support RIM contains the entire binary event log, in the Partial TCG Event Log Assertions format the RIM Bundle contains multiple Support RIM files – one for each PCR covered. Each Support RIM file contains in binary form a list of Events (captured by the S-CRTM as specified by the PC Client Platform Firmware Profile [7]) that correspond to the appropriate PCR. A Support RIM for Partial TCG Event Log Assertions does not have to include all Events for a particular PCR that are present in the Event Log, only the subset endorsed by the creator of the RIM Bundle. Furthermore, a RIM Bundle of the Partial TCG Event Log Assertions type does not have to contain Support RIMs for all PCRs, only those endorsed by the creator of the RIM Bundle. Supplemental RIM Bundles may be used to extend the coverage provided by the primary RIM Bundle.

Partial TCG Event Log Assertions that are created by the Platform creator should consist of a Primary RIM bundle with a Base RIM and at least one Support RIM, typically for Events extended to PCR0. The Platform Manufacturer may include Support RIMs for other PCRs in the Primary RIM Bundle as appropriate.

Partial TCG Event Log Assertions that are created by entities other than the Platform creator (e.g., a VAR) should consist of Supplemental RIM Bundles that contain Support RIMs for Events not endorsed by the Primary RIM Bundle. The VAR may, however, provide reference values for Events for which the creator of the Primary Bundle has already provided assertions. A verifier should decide which reference values are authoritative according to local policy.

One illustrative example is a Platform Manufacturer that installs firmware but not an Operating system. If the Platform Manufacturer is utilizing the Partial TCG Event Log Assertions Support RIM format then it might create a Primary RIM Bundle with three Support RIMs for PCRs 0, 6 and 7. If a Value Added Reseller adds a NIC card that only changes

the value of PCR 2, and no other PCR values are affected, then the VAR should create a supplemental RIM Bundle that contains a new Base RIM and a new Support RIM for events corresponding to PCR2. If the VAR additionally installs an Operating System, new Support RIMs for PCRs 1,4,5 and 8-15 should be included as well.

End of informative comment

1. If the Partial TCG Event Log Assertions type is used then the supportRimFormat attribute within the Base RIM MUST be set to ”Partial_TCG_EventLog_Assertion.”
2. The RIM Bundle MAY include a separate Support RIM for each of the PCRs whose values are included in the bundle.
3. The primary RIM Bundle MUST contain (at a minimum) one Support RIM with values corresponding to one PCR.
4. Each Support RIM file MAY contain only Events extended to the PCR it corresponds to, as determined by the pcrIndex value of the TCG_PCR_EVENT2 structure.
5. The first event of every Support RIM MUST be the informational event TCG_EfiSpecIdEvent that identifies the version of the Event Log.

3.3 PC Client RIM Discovery

Start of informative comment

There are several TCG defined objects that provide optional information that describes the identity and location of the RIM bundle after its creation:

1. The TCG Event log:

The PC Client Platform Firmware Profile [7] defines the Firmware Integrity Measurement Reference Manifest Event that contains a TCG_Sp800_155_PlatformId_Event2 structure. The TCG_Sp800_155_PlatformId_Event2 structure contains a ReferenceManifestGuid, FirmwareManufacturerStr, FirmwareManufacturer and Firmware Version attributes that can be used to identify the RIM.

2. TCG defined UEFI Variable

The PC Client Platform Firmware Profile also defines a Base/OEM Platform RIM EFI Variable. The Base/OEM Platform RIM EFI Variable contains a Platform RIM Variable Data Structure that provides location options that include Local UEFI Device, Local UEFI Device Path, UEFI Variable options. Refer to the PC Client Platform Firmware Profile for details.

3. The TCG Platform Certificate Profile

The TCG Platform Certificate Profile [10] defines an optional Platform Configuration URI attribute that provides a location where a verifier can obtain the RIM Bundle for the device.

End of informative comment

3.3.1 EFI System Partition Storage

Start of informative comment

Storage for PC Client RIM Bundles is defined in this section as a convenience for the end user. OEMs, System Integrators, and Value Added Resellers should use the platformConfigUri attribute within the Platform Certificate in order to provide a flexible, agile, and security centered approach for Verifiers to obtain RIM Bundles.

End of informative comment

The Primary RIM Creator (the entity that creates the initial RIM Bundle) MUST place the RIM Bundle on the Attester device within a tcg/manifest directory located on the EFI System Partition (ESP). Per the SWID guidance document [3], a subdirectory named “swidtag” is used to hold the Base RIM file. Another subdirectory of the tcg directory named “rim” holds the RIM support files. The directories used by a PC Client for storing RIM files MUST be:

Directory	Files
efi_path/EFI/tcg/manifest/swidtag	Base RIM Files
efi_path/EFI/tcg/manifest/rim	Support RIM Files

Table 3: Directory Structure for RIM Files

Example: If a system mounts the ESP to /boot/efi the full path for the base RIM would be /boot/efi/EFI/tcg/manifest/swidtag

3.3.2 File naming conventions

Start of informative comment

Since there can be multiple organizations creating RIM Bundles for a given device, a naming convention is required ensure the uniqueness of each RIM file.

End of informative comment

3.3.2.1 The Base RIM file name

Per the NISTIR 8060 SWID guidance document [3], the following naming convention MUST be used for the Base RIM file:

<name of the tag creator> + <product name> + <RIM version>.swidtag

Where:

1. “name of the tag creator” is the “name” attribute of the Entity element defined in the RIM Information Model specification
2. “product name” is the “name” attribute of the SoftwareIdentity element defined in the RIM Information Model specification.
3. “RIM version” is the “version” attribute of the SoftwareIdentity element defined in the RIM Information Model specification . Note that version attribute is set to BIOS version as specified in section 3.1.2.

Example: acme.com.BigProduct.3.swidtag

3.3.3 RIM Support File names

The TCG Event Log Assertions files MUST use the following naming convention:

<name of the tag creator> + <product name> + <product version>.rimel

The TPM PCR Assertions files MUST use the following naming convention:

<name of the tag creator> + <product name> + <product version>.rimpcr

The Partial TCG Event Log Assertions files MUST use the following naming convention if the file only contains references to a single PCR:

<name of the tag creator> + <product name> + <product version>.rimpcr + <PCR number>

Examples:

acme.com.BigProduct.3.rimel

acme.com. BigProduct.3.rimpcr

acme.com.BigProduct.3.rimpcr0

4 RIM Lifecycle

Start of informative comment

The RIM Information Model specification describes a lifecycle that allows for multiple organizations to participate in the production, distribution, and maintenance of the Attester Device. For PC Clients the RIM Bundle is inherently bound to the Firmware lifecycle. The RIM Bundle should be updated during the process of updating the Firmware.

End of informative comment

4.1 RIM Bundle Creation

Start of informative comment

The Primary RIM Bundle is installed by the Platform Supplier (the tagCreator). The RIM Bundle is installed in the EFI partition in accordance with section 3.3.

End of informative comment

4.2 Pre Delivery RIM Bundles

Start of informative comment

When a System Integrator or Value Added Reseller make modifications that require a new RIM Bundle, the RIM Bundle is installed in the EFI partition in accordance with section 3.3 **Error! Reference source not found.** The RIM B undle is considered “supplemental” to the Primary RIM Bundle created by the Attester Device Manufacturer.

End of informative comment

4.2.1 Supplemental RIM Bundles

Start of informative comment

The RIM Information Model specification allows for pre-delivery modifications by System Integrator and Value Added Resellers as well as post-delivery modifications by IT organizations. A modification will require the creation of a supplemental RIM Bundle if the modification changes any reference value contained within the existing RIM Bundle collection. Examples of modifications that require a new RIM Bundle include:

- Firmware updates that occurred after the device has completed the production cycle.
- Modification of a system component that contains Option ROMs (e.g., NIC or Graphic cards).
- Installation of an Operating System.
- Installation of an EFI user application (e.g., system diagnostic applications).
- Modification of the firmware configuration that may change measured settings (e.g., boot order, secure boot enable, etc.).

As discussed in the RIM information Model specification, a VAR sets the VAR specific information in the entity element of the Base RIM. The VAR also needs to provide either a TCG Event Log Assertions or a TPM PCR Assertions File(s) along with payload file hashes in the Base RIM file. Each VAR should create only a single RIM Bundle.

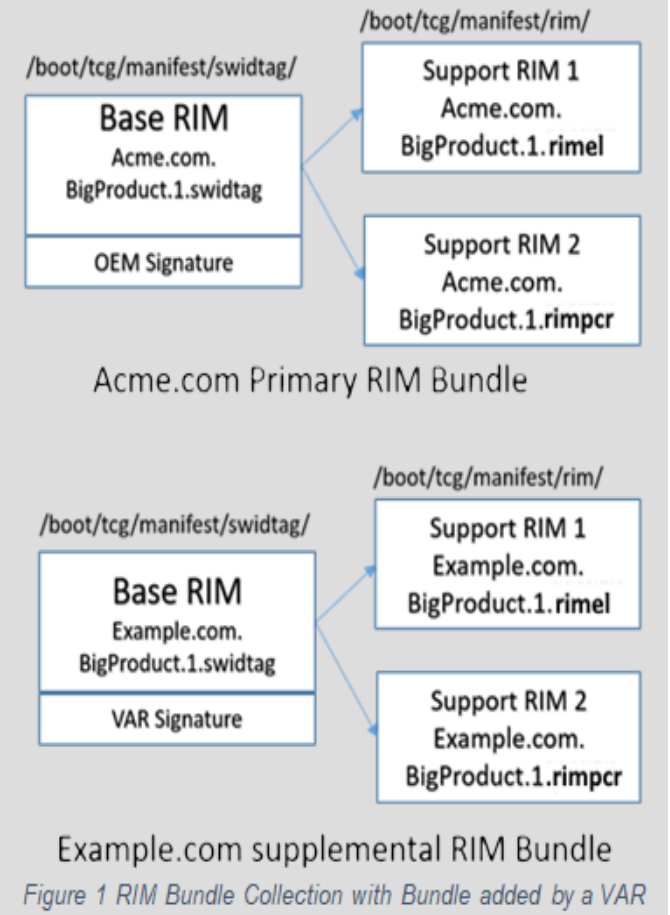

Figure 1 RIM Bundle Collection with Bundle added by a VAR

End of informative comment

A System integrator or Value Added Reseller can make a supplemental RIM Bundle that provides a new set of RIM files, as illustrated by the example in figure 1.

1. Supplemental RIM bundles MUST have the supplemental attribute within the Base RIMs SoftwareIdentity element be set to “true.”
2. The Supplemental RIM Bundle file names are unique and MUST not conflict with the Primary RIM Bundle. A System Integrator or Value Added Reseller MUST NOT remove any RIM Bundle as the information in RIM Bundles may provide valuable information in an investigation attempting to track down unauthorized modification detected by a Verifier.

As an example, the following listing illustrates a Linux based directory structure:

```
/boot/efi/EFI/tcg/manifest/
                    |--- /rim/
                          | -- Acme.com.BigProduct.1.rimel
                          | -- Acme.com.BigProduct.1.rimpcr
                          | -- Example.com.BigProduct.1.rimel
                          | -- Example.com.BigProduct.1.rimpcr0
                    |--swidtag/
                          | -- Acme.com.BigProduct.1.swidtag
                          | -- Example.com.BigProduct.1.swidtag
```

4.3 Supply Chain Processing using the RIM

Start of informative comment

An organization procuring a new device (an Attester Device owner or designated Maintenance Organization) that applies this specification may choose to use the RIM as a means of verifying the Firmware and Boot Manager installed on the device. That process involves the use of a Verifier to perform either PCR Composite or Event Log Verification. Part of the process involves the transfer of all RIMs on the devices to the Verifier. The Verifier is responsible for obtaining the Trust Anchors/Certificate paths used for validating the signatures on the RIMs prior to performing the validation.

End of informative comment

4.3.1 Optional Reimaging

Start of informative comment

Some organizations may choose to reimage the device for security or maintenance reasons. This generally involves using an OS specific installer that will remove any existing OS and install an approved OS (not necessarily the newest available version) as well as performing some initial configuration and setup that the device needs to meet local organizational policies and guidelines. This may invalidate some or all of the RIM Bundle Collection(s). The reimaging may also (optionally) include reflashing the firmware to a known revision. If the organization chooses to perform PCR Composite Event Log Verification after reimaging then the guidance for this case is:

1. Backup the RIM delivered with the device as it may be destroyed when the device is re-imaged.
2. Create a new RIM when the device is reimaged. This includes signing the RIM with a signing key that has an Organization-approved Certificate.
3. Verify that the new RIM Bundle contains correct measurements for each device using an OEM provided, commercially available, or open source tool (if available). These tools may require the RIM Bundle as a prerequisite or require internet access to obtain RIM Bundles associated with the newly installed OS and or firmware.
4. Import the new RIMs into the Verifier for future verifications.

End of informative comment

4.4 Maintenance updates

Start of informative comment

As described in the RIM Information Model, an IT Organization (an Attester Device owner or designated Maintenance Organization) may decide to manage configuration changes by creating RIM Bundles. The new RIM Bundle is considered a supplemental RIM as described in section 4.2.1. Refer to the Maintenance update section (section 5.3) of the TCG Reference Integrity Manifest (RIM) Information Model specification for further details.

End of informative comment

4.5 Firmware Updates

Start of informative comment

Firmware updates require an updated RIM to be created by the Platform Manufacturer (or delegated representative). The updated RIM should follow the guidance given in the TCG Reference Integrity Manifest (RIM) Information Model specification section 5.4.

End of informative comment

Appendix A: PC Client Base RIM Example

The PC Client RIM examples can be found on Github under the following URL:

https://github.com/TrustedComputingGroup/PCClient/PCClientRIM/

This PC Client RIM example uses a 2048 bit RSA key pair with an associated self-signed certificate representing the Example.com corporation. The following parameters are used:

Software Identity Name: Example.com BIOS
 version : 01
 tagId: 94f6b457-9ac9-4d35-9b3f-78804173b65as
 tagVersion:0
Entity (tagCreator) Name
 Regid: http://Example.com
 Role: softwareCreator tagCreator
Links:
 installation media url: https://Example.com/support/ProductA/firmware/installfiles
Meta:
 colloquialVersion: Firmware_2019
 Edition: 12
 Product: ProductA
 Revision: r2
 PayloadType: Indirect
 PlatformManufacturerStr: Example.com
 PlatformManufacturerId: 00201234
 PlatformModel: ProductA
 PlatformVersion:01
 FirmwareManufacturerStr: BIOSVendorA
 FirmwareManufacturerId: 00213022
 FirmwareModel:A0
 FirmwareVersion: 12
 BindingSpec: PC Client RIM
 BindingSpecVersion: 1.2
Payload:
 Directory: /boot/tcg/manifest/swidtag
 File1: Example.com.iotBase.bin
 Version: 01.00
 size= 15400

Please refer to Github for the specific test patterns.

Appendix B: RIM Guidance for OS developers

Operating systems that manage a TPM's PCRs 8-15 need to provide RIM Bundles during OS installation and updates to those PCR values that change when OS updates are distributed. RIM Bundle distribution can be accommodated by the OS packaging or installation/update services by including a RIM Bundle to be installed on the EFI partition.

An Operating System that manages a TPM's PCRs 8-15 should provide PC Client RIM Bundles and include the instance in any OS installation or update process that effects any of the PCR values. This may or may not be practical, depending on how the OS loads and measures drivers (in parallel).

The OS RIM should follow the requirements for Supplemental RIMs as defined in section 4.2.1.

The Event Log Assertions file should exclude any PCRs not measured into by the OS.

For the TPM PCR Log Assertions the TPML_PCR_SELECTION (as defined in the Trusted Platform Module Library Part 3 [19]) should be set to contain only PCRs 8-15 that are applicable to the OS.

Most Operating Systems provide package management subsystems that utilize publicly accessible mirrors to assist in the installation and update processes. These systems should provide RIM Bundles that are specific to the device configuration.

Any packaging of Firmware updates (e.g., rpm, deb, msi, etc.) should include the associated RIM Bundle. Any installation/update of OS packages that include firmware updates should include placement of the RIM Bundle in accordance with the EFI System Partition Storage section. The definition of the packaging is out of scope for this specification.

Appendix C: References

[1] Trusted Computing Group, “Trusted Attestation Protocol (TAP) Information Model for TPM Families 1.2 and 2.0 and DICE Family 1.0”, https://trustedcomputinggroup.org/wp-content/uploads/TNC_TAP_Information_Model_v1.00_r0.29A_publicreview.pdf

[2] IEFT RFC-2119, "Key words for use in RFCs to Indicate Requirement Levels", https://tools.ietf.org/html/rfc2119

[3] NISTIR-8660, “Guidelines for the Creation of Interoperable Software ID (SWID) Tags”, April 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8060.pdf

[4] 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. http://www.iso.org/iso/catalogue_detail?csnumber=65666

[5] TCG TPM 2.0 Provisioning Guidance, March 2017, https://trustedcomputinggroup.org/wp-content/uploads/TCG-TPM-v2.0-Provisioning-Guidance-Published-v1r1.pdf

[6] TCG Infrastructure Working Group Reference Manifest (RM) Schema Specification, November 2006, https://trustedcomputinggroup.org/wp-content/uploads/IWG-Reference_Manifest_Schema_Specification_v1.pdf

[7] TCG PC Client Platform Firmware Profile, October 2018, https://trustedcomputinggroup.org/wp-content/uploads/TCG_PCClient_Specific_Platform_Profile_for_TPM_2p0_1p04_PUBLIC.pdf

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

[9] Time Stamping Authenticode Signatures, https://learn.microsoft.com/en-us/windows/win32/seccrypto/time-stamping-authenticode-signatures

[10] TCG Platform Certificate Profile, Version 1.1 Revision 1 5 13 Feb 2019, https://trustedcomputinggroup.org/wp-content/uploads/IWG_Platform_Certificate_Profile_v1p1_r15_pubrev.pdf

[11] TCG PC Client Platform Firmware Integrity Measurement (FIM) specification, Version1 Revision 24, https://trustedcomputinggroup.org/wp-content/uploads/TCG_PC_Client-FIM_v1r24_3feb20.pdf

[12] TCG Reference Integrity Manifest Information Model, https://trustedcomputinggroup.org/wp-content/uploads/TCG_RIM_Model_v1-r13_2feb20.pdf

[13] IETF RFC-4122 , “A Universally Unique IDentifier (UUID) URN Namespace”, https://tools.ietf.org/html/rfc4122

[15] IANA Private Enterprise Numbers, http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers

[16] TCG Algorithm Registry,Family “2.0", Level 00 Revision 01.22,February 9, 2015,https://trustedcomputinggroup.org/wp-content/uploads/TCG_Algorithm_Registry_Rev_1.22.pdf

[17] NIST, The SWID Tag Validation (SWIDVal) Tool Version 0.5.0, https://csrc.nist.gov/CSRC/media/Projects/Software-Identification-SWID/tools/swidval-0.5.0-swidval.zip

[18] NIST SWID Tag extensions from NIST IR 8060, https://csrc.nist.gov/schema/swid/2015-extensions/swid-2015-extensions-1.0.xsd

[19] Trusted Platform Module Library Part 3: Commands, Family “2.0” Level 00 Revision 01.38 September 29, 2016 https://www.trustedcomputinggroup.org/wp-content/uploads/TPM-Rev-2.0-Part-3-Commands-01.38.pdf

[20] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, RFC 6960, https://tools.ietf.org/html/rfc6960

[21] Foundational Trust for IOT and Resource Constrained Devices https://trustedcomputinggroup.org/work-groups/dice-architectures/

[22] Trusted Platform Module (TPM) https://trustedcomputinggroup.org/work-groups/trusted-platform-module/

[23] Integrity Measurement Architecture, https://sourceforge.net/p/linux-ima/wiki/Home/

[24] RFC 4122 A Universally Unique IDentifier (UUID) URN Namespace, https://tools.ietf.org/html/rfc4122

[25] EFI System Partition Subdirectory Registry, Unified Extensible Firmware Interface Forum, https://uefi.org/registry

[26] XML Signatures Scenarios FAQ, https://www.w3.org/Signature/Drafts/PROP-xmldsig-faq-20000218/Overview.html

[27] Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), rfc#3161, https://www.ietf.org/rfc/rfc3161.txt

[28] PKCS #7: Cryptographic Message Syntax Version 1.5, https://www.ietf.org/rfc/rfc2315.txt

