TRUSTED® COMPUTING GROUP

SPECIFICATION

TCG PC Client Platform Firmware Integrity Measurement

Family 2.0
Version 1.0
Revision 24
December 4, 2019

Contact: admin@trustedcomputinggroup.org

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.

PUBLIC REVIEW

© TCG 2019

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.

This document is copyrighted by Trusted Computing Group (TCG), and no license, express or implied, is granted herein other than as follows: You may not copy or reproduce the document or distribute it to others without written permission from TCG, except that you may freely do so for the purposes of (a) examining or implementing TCG specifications or (b) developing, testing, or promoting information technology standards and best practices, so long as you distribute the document with these disclaimers, notices, and license terms.

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.

DRAFT

CONTENTS

DRAFT

 © TCG 2019

1 SCOPE

This document provides the requirements for a PC Client System in an enterprise computing environment to provide a solution complying with SP 800-155 BIOS Integrity Measurements. This document tailors optional requirements in other TCG specifications such as the TCG PC Client Platform Firmware Profile for TPM 2.0 Systems and the TCG Platform Certificate Profile Specification. Compliance with additional TCG specifications may be necessary for the full enterprise solution.

1.1 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.

1.2 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 statements.

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

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

 © TCG 2019

2 Background

Start of informative comment

Endpoint computers, desktops and laptops for instance, contain hardware, firmware, drivers, operating systems and application software that affect the integrity and security of the devices and the network within which they reside. For a network administrator, knowing the current posture of endpoints in their network can be a frustrating exercise. There are multiple problems at play: 1) are newly deployed machines built and configured as required and 2) what is the ongoing status of machines in the environment over the course of the lifetime of those machines. This specification provides the framework for determining the configuration of the hardware and what firmware has been run to initialize the system in a booted state in the form of Firmware Integrity Measurements (FIM). This specification works in conjunction with other TCG specifications to provide the full end-to-end solution for verification of the platforms in an enterprise environment and forms the basis for trust decisions made based on that verification.

Endpoint computers rely on platform OEM provided and 3rd party provided firmware to initialize and boot to a usable state. The firmware is stored in non-volatile memory and can be updated using utilities provided by the platform OEM. Some 3rd party provided firmware can be updated via utilities provided by the 3rd party, e.g. hard drive firmware updates. The firmware which runs during platform initialization and boot is measured and stored in the TPM, according to the TCG PC Client Platform Firmware Profile for TPM 2.0 Systems. These measurements provide the foundation for FIM but are an insufficient basis for a trust decision. These measurements tell a Network Administrator, or Verifier, *what is currently running*. What the Verifier needs to know is *what is supposed to be running*. How does a Verifier get from the current state to the required state? Reference Integrity Measurements , as specified in the TCG Reference Integrity Manifest Specification (RIM) [4] are the set of measurements which reflect a baseline, or golden, set of measurements against which a comparison can be made.

The FIM and RIM reflect the firmware which runs on an endpoint computer. What about the configuration? How does a Verifier know that any particular endpoint is properly configured? Functionality and devices currently enabled in an endpoint computer are also captured in FIM and RIM, but this is a subset of what a Verifier would like to know about an endpoint computer. What configuration changes can be made to the device to improve the security posture? What are the inherent attributes of the endpoint computer that allow a Verifier to better trust that endpoint? This information is not available in FIM, so it must be captured elsewhere. The Platform Certificate, defined in the TCG Platform Certificate Specification, captures this information. A platform OEM can provide a set of RIMs and a Platform Certificate to a Verifier for an endpoint delivered to the Verifier which allows the Verifier to establish a baseline for that computer. The scenarios enabled by this set of integrity and attribute information are detailed below.

End of informative comment

2.1 Platform Firmware Integrity Measurement Scenarios

Start of informative comment

The following scenarios are informative in nature and describe the sequence of events this specification is intended to address in combination with the other referenced TCG specifications in this document.

End of informative comment

1. Verification that an endpoint computer received by a customer matches what the customer ordered:
    a. A customer places an order for a computer with a specific configuration of hardware and firmware.
    b. The platform OEM builds the computer, generates the RIM and the Platform Certificate, and ships the computer to the customer.
    c. The platform OEM provides the customer the RIM and the Platform Certificate.
    d. The customer receives the computer, collects the FIM and compares it to the RIM.
    e. The customer compares the current Platform configuration to the Platform Certificate and the RIM.
    f. Using the information determined from steps d and e, the customer determines that the platform has been delivered without modification and establishes a baseline.
2. Verification that an endpoint computer is correctly configured to connect to a network

 © TCG 2019

a. An admin configures an endpoint computer to match the baseline security configuration based on the capabilities described in the Platform Certificate and delivers the computer to an end user.
b. The end user boots the system and attempts to connect to the network.
c. The network gatekeeper collects the FIM and Endorsement Key Certificate for the endpoint computer's TPM.
d. The network gatekeeper compares the FIM to the RIM and the Platform Certificate for that platform, as identified by the EK Cert and makes a decision that the platform is properly configured.
e. The endpoint computer is permitted to access the network.

3. Quarantine of an incorrectly configured endpoint computer, see Figure X.
    a. An admin configures an endpoint computer to match the baseline security configuration and delivers the computer to an end user.
    b. The end user boots the system and modifies the configuration by turning off a security feature, e.g. Secure Boot, and attempts to connect to the network.
    c. The network gatekeeper collects the FIM and the EK Certificate for the endpoint computer's TPM.
    d. The network gatekeeper compares the FIM to the RIM and the Platform Certificate for that platform, as identified by the EK Certificate and determines the security configuration has been modified from the baseline.
    e. The endpoint computer is quarantined from the network and remedial action is required to access the network.

2.2 Platform Firmware Integrity Measurement Flow

Start of informative comment

As a platform boots, each code module is measured by the previous code module prior to receiving control of host-computing resources. The chain starts at the S-CRTM and ends with the transition to the OS bootloader. The sequence and set of required measurements are defined in the TCG PC Client Platform Firmware Profile for TPM 2.0 Systems (PFP) [1]. Each measurement is created and extended into a TPM PCR. An event describing that measurement is recorded in an event log maintained by platform firmware through the end of the transition to the OS bootloader. When the OS bootloader gains control of the execution flow, it requests the event log from platform firmware and may make a copy of the event log within which the bootloader adds records of measurements it makes. The behavior of the bootloader is not specified by TCG. The call to request the event log is specified by TCG, but maintenance of the event log by an OS is not specified. Due to the potential for measurements to be made and recorded to the event log maintained by platform firmware between the call to retrieve the event log and delivery to the OS bootloader, the PFP [1] defines a secondary log available in memory which contains copies of events measured and recorded following the request for the log. OS bootloaders may retrieve this copy of the event log after EFI boot services drivers are unloaded and can use this copy to ensure it has a record of all measurements made to the TPM by platform firmware. This process is informatively illustrated in Figure 1 Overview of the Measurement Process.

 © TCG 2019

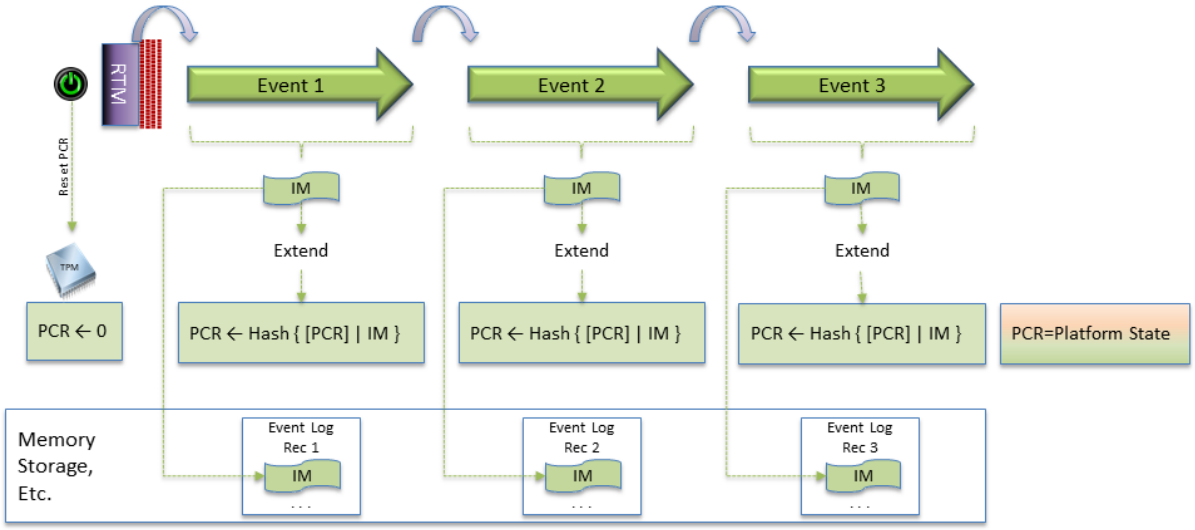

Figure 1 Overview of the Measurement Process

A platform manufacturer produces a Reference Integrity Manifest and signs it, as specified in the TCG Reference Integrity Manifest Information Model, which reflects the set of measurements made when the platform is configured as the platform manufacturer ships the system. This RIM may be stored in the system or may be delivered asynchronously. If a RIM exists, the platform manufacturer is expected to record a non-measured event in the event log which identifies the presence of the RIM with a GUID that can be matched to the RIM. The event, using the TCG_SP800-155-PlatformId_Event2, is specified in the PFP [1].

Verifying the RIM signature confirms for a verifier that it is indeed produced by the platform manufacturer. Once the RIM signature is verified, the values contained in the RIM can be stored in a database used for verification of platform measurements. The RIM and the TCG_SP800-155-PlatformId_Event2 element in the event log contain the same set of attributes which can be used to verify that the RIM and the Event log come from the same system with the same version of the firmware.

A Verifier compares an event log with the RIM attributes and then can parse an event log to extract the digests from the TCG_PCR_Event2 structure, defined in the PFP [1], for the PCR of interest. The event log is not inherently trusted until the PCR values are verified against the digests contained in the event log. These digests and the sequence thereof can be used to reconstruct the final value of the PCR. This final digest value can be compared to the actual PCR value by obtaining a Trusted Attestation Protocol (TAP) [5] report which maintains the integrity of the log using TPM signatures. Further, the verifier can compare the verified log digest values to those expected in the RIM. If nothing has been modified, the digests will match. If a mismatch occurs, the Verifier can decide that the system needs to be remediated.

The addition of a Platform Certificate can be used to provide another layer of verification. The Platform Certificate contains a signed set of assertions and configuration in addition to the attributes which are duplicated in the RIM and the TCG_SP800-155_PlatformId_Event2 element. The Platform Certificate reflects the state of the system as it was shipped to a customer. The ongoing maintenance of the system, including updates to the platform firmware is reflected only in the RIM. This additional layer is used to definitively associate the RIM and the system through the inclusion in the Certificate of the system's TPM Endorsement Key Certificate serial number, the BIOS revision, and the GUID of the RIM. The configuration elements contained in the Platform Certificate may additionally be captured

 © TCG 2019

as measurements in TPM PCRs, providing another set of cross-references for a verifier between the measurements made of the platform configuration on any given boot, the RIM, and the Platform Certificate.

End of informative comment

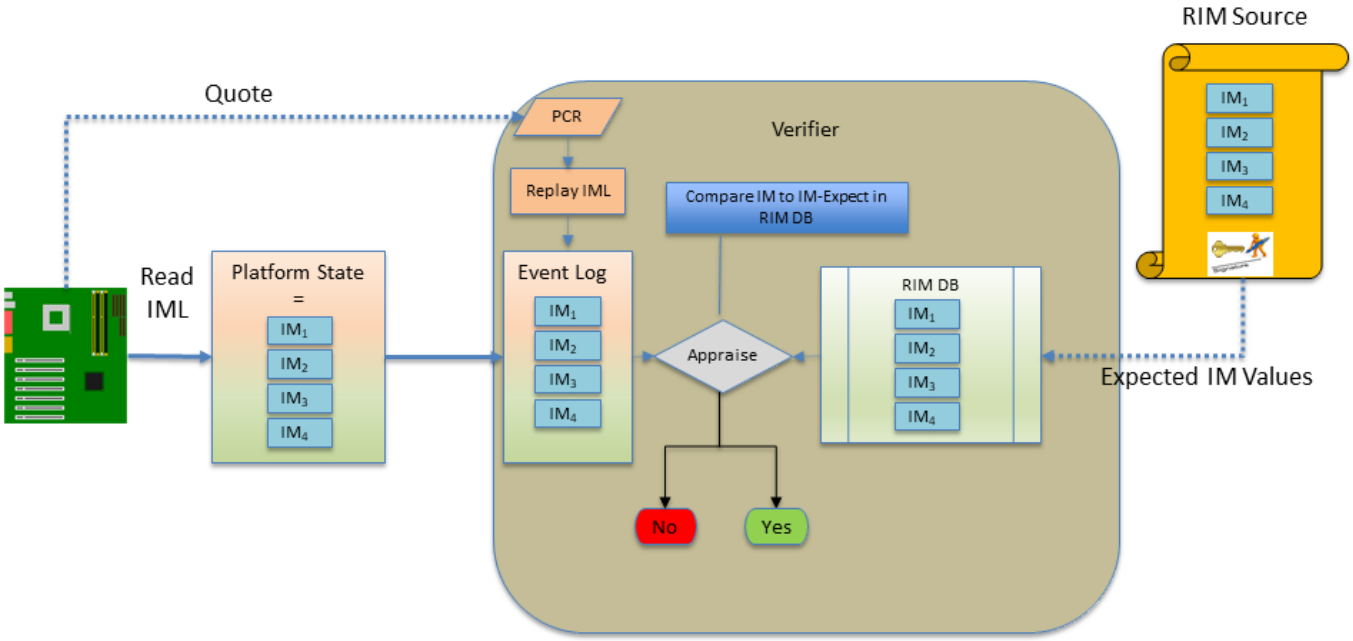

Figure 2 Verification of Measurements

 © TCG 2019

3 FIM Functional Components

Start of informative comment

There are multiple components necessary to provide a complete FIM solution. Many of these components are documented in other TCG specifications and are referenced informatively in this specification.

The following sections provide a description and associated requirement guidelines for the FIM functional components:

- Section 3.1 addresses Roots of Trust (RoTs) and the system requirements for compliance with this specification.

- Section 3.2 defines the necessary firmware integrity attributes and capabilities; references the PC Client Platform Firmware Profile [1] for measurement baselines.

- Section 3.3 informatively describes integrity reporting as specified in the TCG Trusted Attestation Protocol Information Model for TPM Families 1.2 and 2.0 and DICE Family 1.0 [5].

- Section 3.4 informatively describes the collection and transmission of FIMs to the Verifier, as specified the TCG Trusted Attestation Protocol Information Model for TPM Families 1.2 and 2.0 and DICE Family 1.0 [5].

- Section 3.5 informatively describes the Verifier itself.

End of informative comment

3.1 Roots of Trust (RoTs)

Start of informative comment

Roots of Trust (RoTs) are the foundation of any platform firmware integrity assurance. As defined by TCG “RoTs are components that perform one or more security specific functions, such as measurement, storage, and reporting…. A RoT is trusted always to behave in the expected manner because its misbehavior cannot be detected (such as by measurement) by attestation or by observation.” RoTs form the basis for firmware integrity measurements as defined in [1]. The RoTs and integrity measurements provide a record of the boot such that a Verifier can reliably determine what code ran on any given platform. Without the RoTs, a Verifier has no way to determine that the record of the boot is valid.

The trustworthiness of Software Agents that leverage one or more RoTs is dependent on the trustworthiness of the RoT itself and its attack surface. In a PC Client platform, the minimum set of RoTs comprises the Root of Trust for Measurement (RTM), the Root of Trust for Reporting (RTR) and the Root of Trust for Storage (RTS). The RTR and RTS as instantiated in the Trusted Platform Module (TPM).

The chain of trust starts at host platform reset. From the reset vector, the hardware is initialized, and firmware begins measuring code and extending it to the TPM Platform Configuration Registers (PCRs). The measurements contained in the TPM PCRs and the description of the measurements contained in the Event Log represent the platform boot process from reset through the OS Boot Manager code. Some platforms may instantiate the measurement process in a hardware element, e.g. the S-HCRTM or a DRTM. These elements provide an additional layer of assurance.

End of informative comment

3.1.1 Overview of Software Agents

Start of informative comment

FIM requires the coordination of the RTM and the Chain of Trust to perform measurements on an endpoint, a TPM to protect the measurements from modification until they can be reported, and a Reference Integrity Manifest (RIM) for comparison to the measurements of any individual boot process. A software agent, the Attestation Client, may be used to collect the measurements from the TPM and the record of the event logs. The information collected by the Attestation Client would minimally include the event log, the PCR quote results, and possibly a certificate for the signing key used to sign the quote. In some cases, the certificate for the signing key might be provided as part of an endpoint enrollment process. A comprehensive system for ensuring firmware integrity will also include some form of

 © TCG 2019

verification of the collected measurements, and correspondingly a Verifier is necessary to assess reported measurements. Such Verifiers generally reside externally in the network infrastructure. In addition, if any of the components of the measurement, reporting and/or verification process can be modified or updated, then the trustworthiness of such components depends upon the mechanism used to implement updates. Updates of the platform firmware are required to comply with NIST SP800-147. The Platform Certificate for the platform provides an assertion of the system's compliance to a signed firmware update process.

End of informative comment

3.1.2 Overview of Roots of Trust

Start of informative comment

The RoT for Measurement (RTM) is a RoT that makes the initial integrity measurement and adds it to a temper-resistant log. It is the root of the chain of transitive trust for subsequent Measurement Agents [TCG Glossary]. TCG specifies two major types of RTM: a Static- or S-RTM or a Dynamic or D-RTM. The S-RTM starts measuring at platform reset and cannot be re-initialized without a subsequent platform resent. The D-RTM, if supported by the platform, may start at any point after boot by initializing the state of the platform without requiring a reboot. In general, the D-RTM launches after an S-RTM, but the trust-chains anchored in each RTM are not co-dependent.

TCG defines the RoT for Storage (RTS) as the combination of a RoT for Confidentiality (RTC) and a RoT for Integrity (RTI) [TCG Glossary]. The RTS provides for confidentiality and integrity of data stored in TPM shielded locations. In the context of this specification, the RTS maintains a tamper-evident summary of the integrity measurement values and the sequence of those measurements. It does not include the details of the sequence of integrity measurements, but rather holds cumulative integrity results for those sequences. These cumulative integrity values can either be used to verify the integrity of a log containing the integrity measurement values and the sequence of those measurements, or it can be used as a proxy for that log.

The RoT for Reporting (RTR) is a RoT that reliably provides authenticity and non-repudiation services for the purpose of attesting to the origin and integrity of platform characteristics [TCG Glossary]. It necessarily leverages the RTM and RTS. A principle function of the RTR is to provide an unambiguous identity, statistically unique for the endpoint in the form of an Attestation Key (AK). The AK may be persistent or temporary. A typical usage of the AK in this instance involves a TPM2_Quote of the TPM PCRs signed by the AK that may be accompanied by a certificate.

End of informative comment

3.1.3 Agent Coordination

Start of informative comment

The trustworthiness and coordination of the RoTs, trust chain, and Agents in combination gives Verifiers the confidence to make a reliable assessment of the measured endpoint's firmware integrity. Evaluation of the trust properties afforded by the composed system is critical, and evaluation of an individual Agent's trust properties is only relevant in the context of the entire system.

Figure 2 informatively illustrates that the RoTs must act in concert to enable reliable and trustworthy measurement, reporting, and verification of FIMs. In addition, these RoTs must be combined in an endpoint that contains mechanisms for secure platform firmware updates, among other security functions.

End of informative comment

3.1.4 Platform Compliance with FIM

1. The platform manufacturer SHALL provide a system that complies with the TCG PC Client Platform Firmware Profile (PFP) [1] and includes a TPM compliant with the TCG PC Client Platform TPM Profile (PTP) [2].
2. The platform manufacturer platform manufacturer SHALL provide integrity-protected, non-bypassable authenticated platform firmware updates, as necessary to conform to [NIST-SP800-147].

 © TCG 2019

3. The platform manufacturer MAY provide hardware support for a dynamic RTM for post-boot-time measurements.
4. The platform manufacturer SHALL provide a RIM that complies with the TCG Reference Integrity Manifest Specification [4].
5. The platform manufacturer SHOULD provide a platform certificate that complies with the TCG Platform Certificate Profile Specification.

3.2 Platform Measurement Baselines

Start of informative comment

A key factor in a meaningful integrity measurement comparison scheme is establishing and maintaining, with confidence, a known baseline of assertions, configuration and measurements with which a Verifier can make decisions. The establishment of a baseline must consider two scenarios: platforms with platform firmware of unknown or questionable provenance, and platforms with a known and trusted (protected and signed) firmware. This section describes the required and optional assertions that are contained in the Platform Certificate provided by the platform manufacturer. The Platform Certificate provided by the platform manufacturer to a Verifier includes an unambiguous reference to the system TPM EK Certificate and a GUID and URI for obtaining the RIM.

An example scenario – a platform manufacturer generates the reference measurements based on the manufactured system, complete with code and configuration, and produces a RIM and a Platform Certificate. The platform manufacturer delivers the system and the Platform Certificate to a customer, who can take a snapshot of the PCRs prior to any configuration or firmware change. The customer can verify the snapshot against the RIM to verify no changes were made after manufacturing and prior to their receipt of the system. The customer can also verify the assertions contained in the Platform Certificate and compare them to the configuration in the snapshot. The customer can then make any firmware and configuration changes, interrogate the PCRs and take a new snapshot to establish their baseline. This would result in a Support RIM reflecting the customer's baseline, as defined in the TCG Reference Integrity Manifest Specification [4].

End of informative comment

3.2.1 Comparison of Terms

Start of informative comment

NIST SP800-155 uses terms different terms than those used by other TCG specification such as the TCG Platform Certificate Profile Specification. This specification aligns terminology with the other relevant TCG specifications, and so this informative comparison of terms is intended to clarify for a reader how TCG's terms relate to the NIST terminology.

End of informative comment

Table 1 Comparison of Terms

NIST SP800-155 draft	FIM Specification	Description
BIOS	Firmware	Platform Firmware used to initialize the system
Integrity Attribute	Assertions	Security Assertions about the Platform
	Configuration	Non-security related platform properties
Integrity Measurement	Measurement	A hash of code or configuration extended into a TPM Platform Configuration Register

 © TCG 2019

Measurement Assessment Authority	Verifier	The entity that verifies a measurement against a reference
Reference Integrity Measurement	Reference Measurement	The reference measurements provided by the platform firmware provider

3.2.2 Overview of Platform Assertions

Start of informative comment

In SP800-155, Integrity Attributes are used for assessing confidence in firmware integrity measurements. In this specification and in the TCG Platform Certificate Profile Specification, the Integrity Attributes defined in SP800-155 are mapped to Platform Assertions and Platform Configuration. Platform manufacturers have various ways to convey Integrity Attributes to customers. The platform manufacturer may provide this information in a Platform Certificate and a RIM to the customer in an out-of-band channel (i.e., not delivered with the endpoint itself, but through other means). The platform manufacturer may provide a tool to the customer to query the endpoint and extract the Platform Certificate and RIM from a known location. Alternatively, the platform manufacturer may allow the customer to present a serial number to a managed online service, which then responds with the Platform Certificate and RIM for the platform as it was delivered. Regardless of how the customer obtains the Platform Certificate for a particular endpoint, the purpose of the certificate and the RIM is to give the customer a means of assessing the validity of the assertions and measurements reported by the endpoint and developing a level of confidence in the reports it receives about the overall health status of the endpoint beyond only the RIMs.

End of informative comment

3.2.2.1 List of Platform Firmware Assertions

Platform Firmware assertions are defined in the Platform Certificate Profile Section 3.1. These attributes, as defined below, SHALL be reported in the Platform Certificate, as specified by the TCG Platform Credential Profile Specification.

1. `MeasurementRootType` – The valid values are defined in the Platform Certificate Profile Specification. For a PC Client Platform, the following values are permitted, and one SHALL be present:
    - `static (0)` - If the platform instantiates the RTM as part of the early platform firmware POST, an SRTM (Static Root of Trust for Measurement).
    - `Hardware static (6)` “S-HCRTM” if the endpoint utilizes a hardware-based root of trust for measurement (e.g. the platform firmware PEI code is measured by the RTM)
    - `dynamic (1)` - “DRTM” (Dynamic Root of Trust for Measurement) if the endpoint instantiates the RTM after the platform firmware POST.
    - `hybrid (3)` - Both an SRTM and DRTM are supported.

    NOTE: `MeasurementRootType` corresponds to the SP800-155 RTM attribute.
2. `TCGPlatformSpecification` – This attribute contains the platform class, version and revision of the platform-specific specification and the structure is defined in the Platform Certificate Profile Specification.
    - For a PC Client Platform:
        - `platformClass` SHALL be set to 0x 01 (PC Client).
        - `Version` SHALL correspond to the version and revision of the PC Client Platform Firmware Profile version and revision with which the platform firmware complies.

 © TCG 2019

3. `PlatformFirmwareSignature` - an indication of whether the Platform Firmware has been signed and the signatures are present with the platform firmware. If Platform Firmware is not signed, this assertion SHALL NOT be present. If platform firmware is signed, at least one of the following values SHALL be present:
    - `HardwareSRTM (0)` An H-CRTM is present and verifies the signature of the PEI code.
    - `SecureBoot (1)` UEFI Secure Boot is present.
4. `PlatformFirmwareUpdateCompliance` - This attribute provides an indication that the type of platform firmware update mechanism employed by the vendor verifies a signature in accordance with SP 800-147, SP 800-147B, or SP 800-193. A BIOS with an unreliable or nonexistent update mechanism may be held in suspicion. If the platform firmware cannot be updated, this attribute SHALL NOT be present. If platform firmware can be updated, this attribute SHALL contain one of the following values:
    - `sp800-147 (0)` – Update complies with SP 800-147
    - `sp800-147B (1)` – Update complies with SP 800-147B
    - `sp800-193 (2)` – Update complies with SP 800-193

Start of informative comment:

The importance of this attribute lies in the diligence exercised by the platform firmware provider in providing the latest update of the platform firmware code and data provided. In the context of security, the presence of a reliable update mechanism provides the end user with assurance that the platform firmware provider can safely remediate their products against threats should the need arise.

End of informative comment

5. `platformProperties` This attribute SHALL be present if any of the Properties in Tables 2 or 3 are provided by the platform. This attribute is an element of the `platformConfiguration` attribute, as defined in the TCG Platform Certificate Profile Specification.

    Table 2 contains the properties likely to be present in a PC Client platform. If any of these properties are present, they SHALL be enumerated in the `platformProperties` attribute in the Platform Certificate using the STRING / VALUE pairs defined in Tables 2. If none of these properties are present, this attribute SHALL NOT be present.

Table 2 PC Client platformProperties

`propertyName` (UTF8 String)	**`propertyValue` (UTF8 String)**	**`Status` (Integer)**	**Description**
`fwSetupAuth`	`n/a`	`1`	Present if the platform firmware supports authorization to enter firmware setup.
`fwSetupAuthTypes`	`Local` `Remote`	`1` `2`	SHALL be present if `fwSetupAuth` is present. The value 1 indicates a local, physically present user can supply authorization to enter platform firmware Setup. The value 2 indicates an IT

 © TCG 2019

			administrator can remotely supply authorization to enter platform firmware Setup.
IOMMUSupport	n/a	1	The platform provides IOMMU to protect the platform from DMA-based attacks
trustedExecutionEnvironment	n/a	1	The platform contains a Trusted Execution Environment.
physicalTamperProtection	n/a	1	The platform supports a method of physical tamper protection, e.g. a chassis lock.
physicalTamperDetection	n/a	1	The platform supports a method of physical tamper detection, e.g. a chassis intrusion switch
firmwareFlashWP	n/a	1	The platform supports firmware flash write protection, for example provided by the chipset or flash part.
SMMProtection	n/a	1	The platform supports System Management Mode memory protections.
externalDMA	n/a	1	The platform includes external ports capable of DMA.

6. `ComponentIdentifier` – This attribute SHOULD be present as defined in Section 3.1.8 of the Platform Certification Profile Specification. Table 4 informatively defines the components of interest in a PC Client platform. Table 5 informatively defines the components of interest in a Server Platform. The OIDs are defined in the TCG Component Class Registry and included here for convenience of the reader. The structure of this attribute is defined in Section 3.1.8 of the Platform Certificate Profile Specification and contains mandatory and optional elements.

    a. If the `componentIdentifier` is included, the following elements SHALL be present:

        i. `componentClass`, `componentManufacturer`, and `componentModel` elements, and

        ii. If the component is field replaceable, the optional `fieldReplaceable` element.

    b. If the `componentIdentifier` is included, the following elements SHOULD be present:

 © TCG 2019

i. `componentSerial` and `componentRevision`.

Table 3 PC Client Component to OID List

Component	**`componentClass` (UINT 32)**	**Notes**
CPU	00 01 00 02	Main CPU(s) – **Note** PC Client platforms may not include a CPU Serial Number, but should include a CPU Model
Service Processor	00 01 00 00	Embedded Controllers
Memory (DRAM)	00 06 00 04	DRAM based memory, if present should include the `fieldReplaceable` element
Memory (NVRAM)	00 06 00 1B	NV DIMM based memory, if present should include the `fieldReplaceable` element
Motherboard	00 03 00 03	Main motherboard
Network Controller (LAN)	00 09 00 02	Ethernet adapter if replaceable, should include the `fieldReplaceable` element
Network Controller (Wifi)	00 09 00 03	Wireless network adapter, if replaceable, should include the `fieldReplaceable` element
Network Controller (BT)	00 09 00 04	Bluetooth network adapter, if replaceable, should include the `fieldReplaceable` element
Fixed Storage (HDD)	00 07 00 05	Hard disk-based storage, if replaceable, should include the `fieldReplaceable` element
Fixed Storage (SSD)	00 07 00 03	Solid State-based storage, if replaceable, should include the `fieldReplaceable` element
Fixed Storage (M.2)	00 07 00 04	M.2 form factor SSD or NVME drive, if replaceable, should include the `fieldReplaceable` element
Removable Battery	00 0A 00 03	A removeable battery, e.g. for a notebook platform. If present should include the `fieldReplaceable`

DRAFT

		element
Chassis – Desktop	00 02 00 02	A Desktop system chassis
Chassis – Notebook	00 02 00 09	A Notebook system chassis

7. `PlatformConfigUri` – This attribute SHALL be present as defined in Section 3.1.9 of the Platform Certification Profile Specification if a Reference Integrity Manifest exists.

3.2.3 Platform Firmware Integrity Measurements

Start of informative comment

The PFP [1] provides a definition of the measurements a platform must perform and the format of how the measurements are required to be reported, in a TCG Event Log. The TCG TPM Library specification defines the basic mechanisms a TPM provides to serve as an RTS and RTR. The TCG EFI Specification defines the interface that firmware provides to continue reporting of measurements.

The properties and components defined in Section 3.2.2 are captured as part of measurements as defined in the PFP [1].

End of informative comment

1. A PC Client Platform compliant with this specification SHALL include a TCG_Sp800_155_PlatformId_Event2 structure in the TCG Event Log. Note: This event is defined in the PFP [1].

3.2.4 Platform Firmware Reference Integrity Manifest

Start of informative comment

The TCG Reference Integrity Manifest (RIM) Information Model Specification [4] defines an information model for a set of Reference Measurements for a platform. The platform manufacturer provides a Base RIM for the version of firmware shipped with the platform. For subsequent versions of the platform firmware, the platform manufacturer provides Patch RIMs.

End of informative comment

3.3 Platform Firmware Integrity Reporting

Start of informative comment

Reporting of the Platform Firmware integrity values stored in the RTS is performed by an Attestation Client. The format of the information provided by the reporting agent is defined in the TCG Trusted Attestation Protocol Information Model for TPM Families 1.2 and 2.0 and DICE Family 1.0. The Platform Firmware Integrity values may be signed by a TPM Attestation Key (AK) as part of a TPM2_Quote. To cryptographically verify the integrity values are linked to a platform, the AK might be linked to the TPM Endorsement Key (EK).

End of informative comment

3.3.1 Attestation Client

Start of informative comment

The Attestation Client is responsible for extracting the measurements stored in the TPM PCRs and formatting them as defined in the TAP Information Model Specification [5]. In addition to the information model defined in the TAP specification, methods of attestation are defined with the associated TPM commands required to support them. This includes the concepts of freshness, identity and time-based elements.

End of informative comment

 © TCG 2019

3.3.2 Endpoint Reports

Start of informative comment

System measurement reports may be generated and sent to a Verifier under several conditions: 1) on connection to a network, 2) on request of the Verifier, or 3) on request of a service. The Attestation Client might include the ability for a user or administrator to configure triggering events for measurement reporting. Report requests may be initiated by a user, an Attestation Client based on configuration, a Verifier or a service. Under certain circumstances, it might be advisable for an Attestation Client to ignore requests from unauthenticated services. See the TCG Trusted Attestation Protocol Use Cases.

End of informative comment

3.4 Platform Firmware Integrity Measurement Collection and Transmission

3.4.1 Overview of Measurement Collection and Transmission

Start of informative comment

Firmware Integrity Measurements are collected by a Client as a TAP Attester, then may be transmitted from the system to the Verifier.

Secure transmission of Integrity Measurements ensures that measurements are not disclosed in transit by malicious parties. Further, proper selection of transmission protocols can ensure maximum interoperability, freshness, and efficiency. Integrity protection and freshness is provided by TPM based signatures over TPM Platform Configuration Registers (PCRs) using one of the techniques described in the TAP [5] document. This ensures that even if the Collection Agent or other software becomes compromised, the measurements cannot be falsified.

End of informative comment

3.5 Verifier

3.5.1 Overview

Start of informative comment

The Verifier appraises the state of the client (acting as an Attester) using information about the client from the PCR values or Event Log. The Event Log and PCR values are passed from the client (i.e., the Attestor) using the protocols specified in the TAP [5] document. If the Event Log is used, the verifier first validates its integrity using the relevant PCR values. The Verifier appraises the Attester using a set of policies supplied by an administrator.

End of informative comment

 © TCG 2019

4 Normative References

Where a normative reference is undated, the latest available versions can be used.

[1] TCG PC Client Platform Firmware Profile (PFP) for TPM 2.0 Systems

[2] TCG PC Client Platform TPM Profile (PTP) for TPM 2.0

[3] TCG Platform Certificate Profile Specification

[4] TCG Reference Integrity Manifest Specification

[5] TCG Trusted Attestation Protocol Information Model for TPM Families 1.2 and 2.0 and DICE Family 1.0

DRAFT

 © TCG 2019