Trusted Computing Group (TCG) Personal Computer (PC) Specific Trusted Building Block (TBB) Protection Profile

and

TCG PC Specific TBB With Maintenance Protection Profile

Version 2.5

July 20, 2004

Prepared By: David Grawrock / Monty Wiseman

Prepared For: TCG Conformance Workgroup

Preface

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

Contact the Trusted Computing Group at [website link] for information on specification licensing through membership agreements.

Foreword

This document contains two Protection Profiles, which are written to support the development of trusted subsystems that may be integrated into a computing platform.

The majority of the requirements used in these Protection Profiles are taken from the “Common Criteria for Information Technology Security Evaluations,” Version 2.1. Some extended functional requirements are also included.

Comments on this document should be sent to the Trusted Computing Group at http://www.trustedcomputinggroup.org.

A revision history is provided below.

Revision History

Version Number	Date	Revisions/Comments
0.91	10/22/02	Initial Version
0.92	10/29/02	Version for Workgroup review with Maintenance package integrated.
0.93	11/05/02	Integrated Maintenance PP into the document. Responded to EORs.
0.94	11/12/02	Responded to EORs.
0.95	11/18/02	Responded to EORs.
1.0	12/09/02	Responded to EORs.
1.1	12/19/02	Updated with comments from the TCG Workgroup.
1.2	12/23/02	Responded to EORs.
1.3	1/14/03	Revised functional requirements.
1.4	1/21/03	Responded to EORs.
1.5	1/27/03	Responded to EORs and comments from TCG Workgroup.
1.6	7/5/03	Responded to EORs and comments from version 1.5. Extensive re-edit of section 2. Changed references from TCPA to TCG. Make changes per 7/1/2003 telecon.
1.7	7/10/03	Made final edits per 7/8/2003 telecon.
1.7.1	7/28/03	Made wording change to FPT_ITM.1.1
1.7.2	7/28/03	Added to section 2: Description of trust model and description of one-to-one connection. Added FPT_ENV_RST.1.
1.7.3	7/29/03	Make this PP specific to TCG document versions in section 1.3. Wording changes to section 2.1.4. Added wording to FPT_ENV_RST.
1.8	8/4/03	Made final edits in preparation for evaluation.
1.9	10/31/03	Updated the PP based on comments from the Validator.
1.91	11/8/03	Edits per 11/4/03 concall with Validator.
2.0	1/11/04	Final edits for submission to validator and evaluator.
2.1	1/19/04	Fixed minor typo.
2.2	1/27/04	Final edits for submission to validator and evaluator.
2.3	3/15/04	Additional edits for submission to validator and evaluator.
2.4	6/24/04	Update based on validator comments.
2.5	7/20/04	Made minor updates based on validator recommendations.

Table Of Contents

Page

List of Figures and Tables

1 - Introduction

1.1 - Identification

This document contains two PPs entitled:

- Trusted Computing Group (TCG) Personal Computer (PC) Specific Trusted Building Block (TBB) Protection Profile (PP), and
- TCG PC Specific TBB With Maintenance PP.

Assurance Level: The assurance level for both of these Protection Profiles is EAL3 augmented with ADV_SPM.1.

Document Version Number: 2.5

Document Publication Date: July 20, 2004

Authors: TCG Conformance Workgroup, David Grawrock, Monty Wiseman

Sponsoring Organization: TCG

Registration: <To be filled in upon registration>

Keywords: TCG, SmartCard, TPM, TBB

1.2 - Protection Profile Overview

Evaluating trust in a PC is difficult and expensive. The two Protection Profiles (PP) contained in this document define a "Root of Trust" as a building block of the Trusted Computing Group (TCG) architecture. The TCG architecture is defined in the TCG Main Specification. The Root of Trust provides the foundation for "Transitive Trust" which makes and reports trust measurements of components of the TCG Architecture external to the Root of Trust. One of the PPs in this document contains the Root of Trust and connections used as a building block for the TCG architecture; the other PP contains both the Root of Trust and connections and also a maintenance capability. The two PPs are defined as 1) a TBB and 2) a TBB with the addition of a maintenance package.

1.3 - Related Protection Profiles and Documents

The Protection Profiles in this document reference the "Trusted Computing Group Trusted Platform Module Protection Profile.” (See: http://niap.nist.gov/cc-scheme/PPRegistry.html. File number: CCEVS-020016).

Related documents:

Trusted Computing Group PC Specific Implementation Specification 1.1 (See: http://www.trustedcomputinggroup.org) hence forward referenced in this PP as Trusted Computing Group PC Specific Implementation Specification.

Trusted Computing Group Main Specification 1.1b (See: http://www.trustedcomputinggroup.org) hence forward referenced in the PP as Trusted Computing Group Main Specification.

1.4 - PP Organization

Section 1 provides the introductory material for this document.

Section 2 provides the TOE description for both PPs. An introduction is provided in 2.1. Section 2.2 provides the TBB description for the TCG PC Specific TBB; the TCG PC Specific TBB with Maintenance TOE Description is defined as the combination of Section 2.2 and Section 2.3, which provides the description of the maintenance package. Finally, in Section 2.4, the IT environment is described.

Section 3 provides a discussion of the expected environment for the TOE, including assumptions and threats. As in the previous section, threats and assumptions are first defined for the TCG PC Specific TBB TOE and then threats and assumptions are defined for the maintenance package. The combination of the threats and assumptions for the TCG PC Specific TBB TOE and for the maintenance package are the threats and assumptions for the TCG PC Specific TBB with Maintenance TOE.

Section 4 defines the security objectives for both the TOE and the TOE environment. As in the previous section, objectives are first defined for the TCG PC Specific TBB TOE and then objectives are defined for the maintenance package. The combination of the objectives for the TCG PC Specific TBB TOE and for the maintenance package is the objectives for the TCG PC Specific TBB with Maintenance TOE.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively, plus extended functional requirements, which must be satisfied by the TOE. As in the previous section, functional requirements are first defined for the TCG PC Specific TBB TOE and then functional requirements are defined for the maintenance package. The combination of the functional requirements for the TCG PC Specific TBB TOE and for the maintenance package is the functional requirements for the TCG PC Specific TBB with Maintenance TOE. The assurance requirements (CC Part 3 requirements) are identical for both PPs in this document.

Section 6 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the threats. Arguments are provided for the coverage of each threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next, Section 6 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements

Appendix A provides an acronym list and a list terminology specific to the PPs.

1.5 - Common Criteria Conformance

These PPs have been built with Common Criteria (CC) Version 2.1 (ISO/IEC 15408 Evaluation Criteria for Information Technology Security; Part 1: Introduction and general model, Part 2: Security functional requirements, and Part 3: Security assurance requirements).

These PPs are Common Criteria Version 2.1, Part 2 extended, and Part 3 conformant, at Evaluation Assurance Level 3 with Augmentation. The definition of Part 2 extended is found in the CC Part 3, section 5.4, “Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2.”

2 - TOE Description

2.1 - Introduction

2.1.1 - TCG Fundamentals

There are two entities in the TCG architecture: the client and the challenger. For the purpose of illustrating this Protection Profile, the client is the entity that contains the TOE. The challenger is an entity the client has requested a service from, however, the challenger may want to have assurance of the platform's configuration using authentication or attestation. Platform Authentication is the CC-defined concept of authentication applied to the platform as the subject. The platform may have one or more identities associated with it. Platform Attestation is using the Platform Authentication to provide additional assurance in the platform by providing an attestation of the platform's configuration – hardware, software, or both.

Platform Authentication and Platform Attestation rely on the platform's ability to provide either authentication of an identity or attest to its configuration or both. Protected storage relies on the storage capabilities within the TPM itself optionally along with the platform's configuration. All of these features require that the platform have a root of trust. The root of trust provides assurance to the challenger or user (in the case of protected storage) that the authentication or configuration is trustworthy. This trust is established by having the platform begin its execution in trusted components. Those components are within the Core Root of Trust for Measurement (CRTM) as described within this Protection Profile.

Providing the information about the platform's configuration for a determination of trustworthiness involves a TCG concept called "measurement". A measurement begins by performing a hash (in TCG this is using SHA-1 resulting in a 160 bit value) on the next component to be executed. The resulting hash is sent to the TPM using an "Extend" function. The TPM protects this value per the TCG Main Specification and TPM Protection Profile. After the measurement is Extended, control of the platform is transferred to the component that was measured. By progressively performing these measurements starting from the first instruction executed after the platform is reset through the boot process, a "chain" of measurements results in a trust in the boot process. In the TCG Architecture the result of this chain is called Transitive Trust.

2.1.2 - PC Architecture Overview

A Personal Computer (PC) is usually a general purpose-computing platform executing either commonly available Operating Systems and applications or dedicated Operating Systems and applications. Each PC contains one "host" component called a motherboard. It is the motherboard that is associated with the PC. It typically contains the main CPU, primary memory, some common IO ports and connectors for daughter cards. Motherboards are designed in a modular approach using components that may be common (or at least with little modification) across several motherboard designs. The PC industry calls these components Building Blocks.

2.1.3 - TCG's addition of trust to the PC Architecture

The TCG architecture and these Protection Profiles take advantage of this modularization by separating and simplifying the components that implement the TCG features. The chain of measurements described above that result in Transitive Trust must begin at some point and that point must be trusted *a priori*. TCG relies on a Root Of Trust that is established during platform reset to anchor the chain of the Transitive Trust. TCG has therefore defined in the PC Specific Specification the specific Building Block that performs the initial platform boot at the Trusted Building Block or TBB[1]. This is the component that embodies the trust associated with the TCG architecture.

2.1.4 - Trust Model

The trust model for the TCG architecture relies on entities that are outside the trust boundary (i.e., the TOE) to determine the validity or trustworthiness of a platform. These entities are called "challengers" in the TCG architecture. The validity or trustworthiness of a platform is determined by analyzing an unbroken chain of measurements. These chains of measurements are rooted in the TBB. The TCG architecture calls this the Root of Trust. Challengers must first decide to trust the Root of Trust before analyzing the chain of trust because without a trusted root the chain cannot be trusted. It is the challengers that make use of the measurements and make the decisions about the validity or trustworthiness of the platform or its components. Therefore, it is outside the scope of the TCG architecture for the TOE as specified in this Protection Profile to make any validity or trustworthiness decisions regarding the value of the measurements.

2.1.5 - Connections

Building blocks attach either to other building blocks or to the motherboard using “connections”. The CC defines connectivity as the property that allows communication between the TOE and external IT entities, which is an appropriate definition for this architecture. Each connection must provide assurance that the TOE is communicating with the specified Building Block or IT entity. Note: the connection does not provide confidentially.

2.1.6 - One-to-one Connection

This term denotes a specific relationship between entities on each side of a specific connection. Once established (via any method such as physical attachment, logical cryptographic binding, etc.) a one-to-one connection is always established between the same two entities. For example, once a TPM is bound (i.e., attached) to a TBB, the TBB will not allow a connection to any other TPM.

2.1.7 - Description of the TOE

The target of evaluation (TOE) for both the TCG PC Specific TBB PP and the TCG PC Specific TBB With Maintenance PP is a subsystem within a PC with TCG architecture. The TOE always contains the following:

- A Core Root of Trust for Measurement (CRTM)

  Note: This is not a “connection” as it is wholly contained within the TOE.

- A Connection to a Trusted Platform Module (TPM)
- A Connection to the PC motherboard
- A Connection to the PC motherboard’s reset signal

[1] For a complete definition of the TBB see the "TCG PC Specific Implementation Specification"

- A Connection to the PC motherboard's physical presence signal

The TCG PC Specific TBB TOE contains only the TBB. The TCG PC Specific TBB With Maintenance TOE contains the TBB and the maintenance package. In both PPs, the TOE operates within the defined IT environment.

In both PPs, the TOE assumes the TPM is a CC evaluated TPM, which is conformant with the Trusted Computing Group Trusted Platform Module Protection Profile (TPM PP); the TPM is not addressed herein except to define its connection to the CRTM and PC motherboard. The IT environment is the TCG architecture including the TPM as defined by the TCG Main Specification and compliant with the TPM PP. The TPM is required to be present in the environment and the TOE cannot conform to the TCG PC Specific TBB PP or the TCG PC Specific TBB With Maintenance PP unless an evaluated TPM is present in the environment.

Many security relevant functions can be implemented in hardware or software or a combination of the two. These protection profiles do not mandate how functionality is to be implemented. A Security Target claiming compliance with either of these protection profiles must indicate how the required functionality is met.

The security requirements in this document apply to the TOE from the final manufacture of the TOE to its inclusion in the TCG architecture on a PC that is operated by the end user.

2.1.8 - TBB Overview

The TCG PC Specific TBB TOE contains only the TBB. The TBB consists of hardware and/or software that establishes trust (provides an integrity measurement) and provides connectivity between a CRTM, the TPM, the PC motherboard, the platform reset, and the physical presence signal. The TOE provides functionality that permits an entity to believe measurements that describe the current computing environment in the platform. An entity can assess those measurement results and compare them with values that are expected if the platform is operating as expected. If there is a match between the measurement results and the expected values, the entity can trust computations within the platform to execute as expected.

The CRTM measures the state of the hardware and software environment in a platform. Three data components are involved in an integrity metric. The first component is the method used to gather that data. The second component is predicted values of measured data in a platform. The third component is the actual values of measured data in a platform. Any integrity challenger needs to know about all of these components in order to make a decision about the integrity of the platform.

Measurements must be done in ways that ensure the validity of the collected data. Hence, the TOE provides a root of trust for the process of measuring integrity data. This is the purpose of the CRTM. The TOE's connections to the TPM, and PC motherboard provide secure pathways for information to flow between these components.

The terms PC motherboard and platform are defined in the TCG PC Specific Implementation Specification. As an environmental consideration, the PC motherboard and platform are bound into one entity and are used synonymously in this document.

Figure 1, below, depicts the TOE and the environment. The TPM is outside the TOE, but the connection of the TPM to the TOE is included within the TOE. The TOE is only conformant with these PPs if there is a TPM connected to the PC motherboard and to the TOE; this is an environmental assumption.

Figure 1 depicts the "one-to-one" relationships between the TOE, the TPM and the PC motherboard. The components within the heavy-dashed lines are within the TOE, i.e., the CRTM and the connections to the TPM and the platform are part of the TOE while the TPM itself is within the IT environment. Note that the HD, Keyboard, Output device, CPU, remaining portion of the BIOS, and Supporting H/W are not part of the TOE. The Supporting H/W includes components to connect memory and I/O controllers to the PC motherboard.

2.1.9 - TBB Functionality

The TBB must provide a CRTM and the assurances that the connections between the TPM, the PC motherboard, the platform reset, and the physical presence signal are properly established and maintained and that at least one physical attack, specified by the ST author, on the TPM connection can be detected. Ensuring that connections are properly established and maintained includes ensuring secure function recovery in case of failure and non-bypassability of the TOE Security Policy.

There is a one-to-one relationship between the TPM and the platform, which is maintained by the connection that is part of the TOE. The TPM may be removable from the PC motherboard, but must not be movable to another PC motherboard and still be operational. The meaning of a one-to-one relationship is that the TPM connection shall ensure that one and only one specific TPM may be connected to a platform. The ST author will specify the means of enforcement of the one-to-one relationship.

The TBB has no users as such; it provides the following security functionality:

- The TBB is reset upon the CPU receiving platform reset signal
- The CRTM code is the first code executed within the TBB
- Preserves a secure state in the event of a failure of the TPM connection,
- Provides a means to detect at least one physical attack on the TPM Connection,
- Provides a root of trust for measurement, the CRTM, which measures certain platform characteristics.

There are no required probabilistic or permutational mechanisms included in the TOE; therefore a strength of function analysis is not possible. The TOE is designed to protect against a “low” attack potential overall.

2.1.10 - TBB Reset

The TBB is reset when the CPU is reset after receiving the reset signal from the platform. Because the TBB includes the reset vector this causes the execution of the CPU to begin within the CRTM, thus the TBB. The platform reset signal resets the CPU, which, in turn, executes the CRTM code. As described in Section 2.3, IT Environment and in the objective for the IT Environment, OE.Reset, upon reset of the CPU (causing the beginning of the CRTM’s execution) the IT Environment will also reset the TPM.

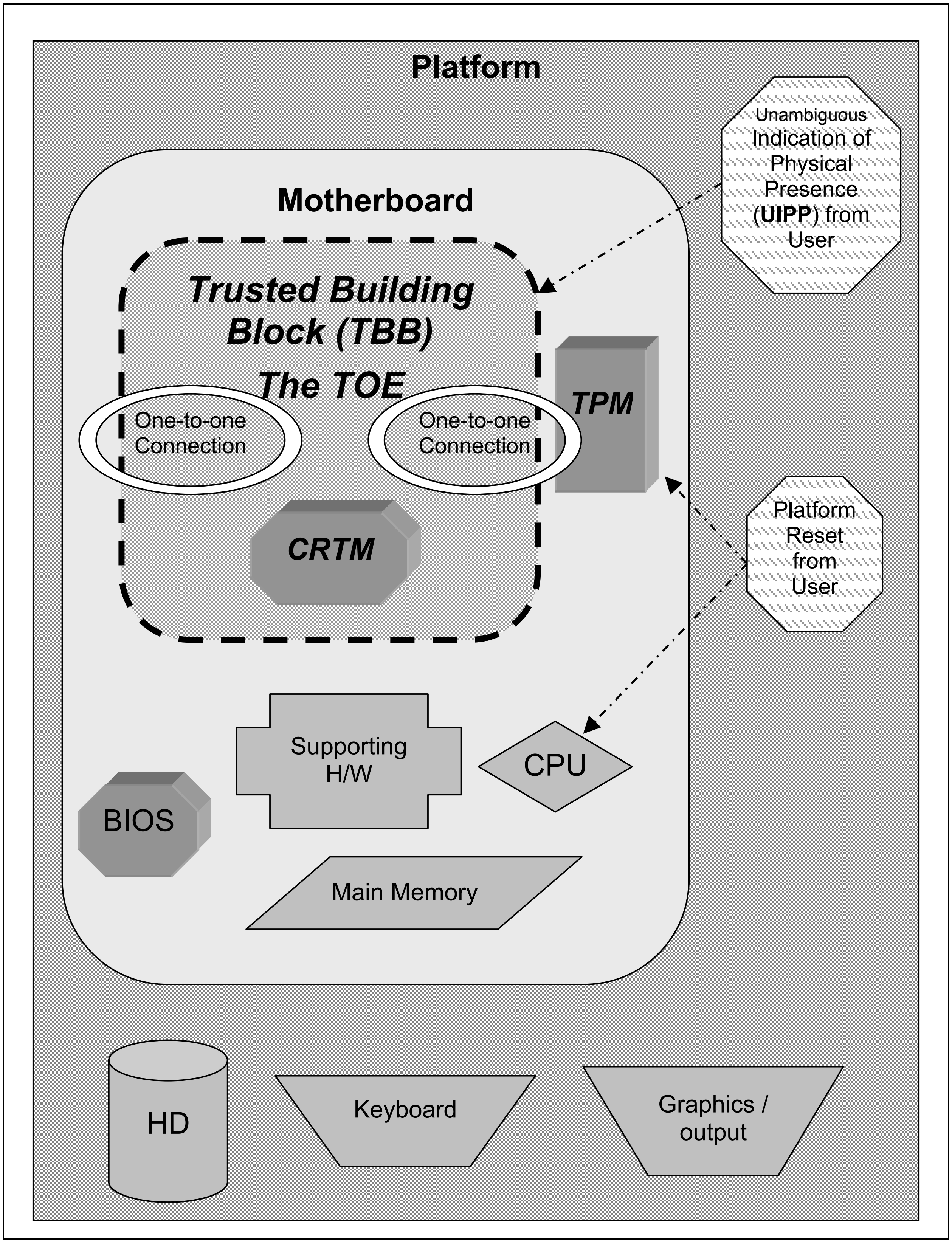

Figure 1. Overview of the TOE and TOE Environment

2.2 - Maintenance Package Description

2.2.1 - Introduction

The TCG PC Specific TBB With Maintenance TOE contains the TBB, as defined in Section 2.1, above, and a Maintenance Package, described in this section. Maintenance of the TBB is a capability that may be provided by the platform manufacturer. Some environments will require that the TBB provide a maintenance capability for defect management, upgrade, or other reasons. This document contains two PPs: one that defines only TBB security functionality and one that defines both TBB and maintenance of the TBB security functionality. The approach used to define the two PPs was to declare the maintenance functionality as a "package." A package, as defined by the CC, is an intermediate combination of functional or assurance components that define requirements that meet an identifiable set of security objectives. A package may be thought of as a set of defined security requirements.

The following maintenance package description is included, in addition to the TOE description in Section 2.1, in the TCG PC Specific TBB With Maintenance PP.

2.2.2 - Maintenance Package Overview

The objectives and requirements of the TBB makes designing a maintenance-free implementation desirable because of its simplicity, however, some environments will require the TBB to provide for maintenance to accommodate defect management, upgrade, or other functionality.

If maintenance features are implemented for any TOE, the maintenance threats, objectives and requirements specified in TCG PC Specific TBB With Maintenance PP are requisite.

Maintenance will generally apply to updating, replacing, etc. of the CRTM. For example, the CRTM is typically wholly contained within the BIOS Boot Block. The BIOS architecture falls under two main categories: CRTM within the BIOS Boot Block and monolithic.

In the CRTM within the BIOS Boot Block category, the BIOS is actually divided into two parts. The first part, called the BIOS Boot Block, contains only the initialization code necessary to boot the platform to an operational state. This part is controlled by the platform manufacturer and is specifically designed to be small and perform as few functions as possible. The second part of this category of BIOS is upgradeable by anyone with proper authorization and usually allows 3rd party developers access to modify it and update it with patches. In this type of BIOS, the CRTM is contained in the BIOS Boot Block and can only be updated, modified, etc. by the manufacturer or their agents. For this category of BIOS architecture, the maintenance requirements apply only to the BIOS Boot Block portion of the BIOS.

In the second type, monolithic, all of the BIOS is contained and maintained within one unit having the same security protection in all components or areas within that unit. In this category of BIOS, while the actual executable portion of the CRTM may only occupy a small portion of it, the entire BIOS must be protected as if the CRTM occupied all of it. For this category of BIOS architecture, the maintenance requirements apply to the entire BIOS.

Some platforms provide protection of the connections via "soft" or cryptographic methods. These methods also may need to be updated, maintained, etc. While this connection method is optional, if used and maintainable, the threats, objectives, and requirements pertaining to the maintenance of these connections apply to those components as well.

Maintenance of the TOE components requires the following functionality:

- Identification and authentication of the administrator, manufacturer or other authorized maintenance provider, including the assignment and enforcement of roles assigned by the ST author,
- Access control on the TOE that enforces controls on subjects, objects and operations within the TOE,
- Consistency checking and defined interpretation rules for data imported from outside the TOE,
- Replay detection for TBB maintenance requests and user authentication,
- Security domain separation to protect the TOE from interference and tampering by untrusted subjects

When the TOE includes the maintenance package, a strength of function analysis may be performed on the identification and authentication function. Due to the difficulty in providing protections for remote maintenance and the level of potential harm possible from a successful attack, the attack potential for the maintenance identification and authentication function is assumed to be high.

2.3 - IT Environment

The IT Environment is the same for the TCG PC Specific TBB TOE and for the TCG PC Specific TBB With Maintenance TOE. The IT environment, depicted in Figure 1 as surrounding the TOE, is assumed to contain a CC evaluated TPM, which is conformant with the Trusted Computing Group Trusted Platform Module Protection Profile (TPM PP). The TPM must be present for the TOE to operate.

The IT environment provides signals to reset the CPU, and thus the TOE, and to the TPM. A reset is performed in the case of a platform reset or upon request by the platform user. A platform reset causes a CPU reset forcing the next instruction to be executed to be from the CRTM.

Certain operations may be performed by the TPM if a user is physically present at the system. The TOE accepts an indication of physical presence from the IT environment and provides the indication of physical presence to the TPM; the TPM, which is in the IT environment, limits access to certain commands if the indication of physical presence is not set.

3 - TOE Security Environment

3.1 - Threats to Security

Threats to TOE security are defined in Table 3.1, below. These threats are included in both the TCG PC Specific TBB PP and the TCG PC Specific TBB With Maintenance PP.

Table 3.1 – Threats to Security

#	Name	Threat
1	T.CRTM_Not_First	An attacker may cause other code to be executed prior to executing the CRTM code upon platform reset, thereby compromising the CRTM and causing the CRTM to become untrusted.
2	T.Failure	An attacker may gain access to secrets by causing the connection to the TPM to fail.
3	T.Incorrect_CRTM	An attacker may substitute a CRTM in the TOE, causing the CRTM to be invalidated and compromising the security of the data within the TPM.
4	T.Malfunction	A malfunction of the TOE may cause modification of TOE assets or cause TOE assets to be disclosed.
5	T.Measure_Integrity	The CRTM may fail to measure the integrity of the next component to execute and thereby cause a denial of service or a compromise of the security of data.
6	T.Physical	An attacker may cause disclosure or modification of TOE assets by physically interacting with the TOE to exploit vulnerabilities in the physical environment.
7	T.Protect	An operation external to the TOE may interfere with TOE security functions or resources, causing disclosure of TSF data or other errors to occur.
8	T.TPM_One_To_Many	An attacker may disconnect the TPM from the platform and successfully reconnect the TPM with another platform, thereby compromising the security of the data within the TPM and invalidating the CRTM.

3.2 - Threats for the Maintenance Package

Threats applicable to the Maintenance package are defined in Table 3.2, below. These threats are included in the TCG PC Specific TBB With Maintenance PP only.

Table 3.2 – Threats to Security for the Maintenance Package

#	Name	Threat
1	T.Attack	An undetected compromise of the TOE assets may occur as a result of an attacker (whether an insider or outsider) attempting to perform actions that the individual is not authorized to perform.
2	T.I&A_Bypass	An unauthorized individual or user may gain unauthorized access to TOE assets.
3	T.Imperson	An unauthorized individual may impersonate an authorized user of the TOE and thereby gain access to TOE data and operations.
4	T.Inconsistent	The TOE may fail to consistently interpret and share data with another trusted IT product, such as the manufacturer's maintenance data distribution facility or update/maintenance functions, causing security breaches or erroneous data in the TOE.
5	T.Modify	An attacker may modify TOE or user data, e.g., file permissions, in order to gain access to the TOE and its assets.
6	T.Object_Init	An attacker may gain unauthorized access to an object upon its creation if the security attributes are not assigned to the object or an unauthorized individual can assign the security attributes upon object creation.
7	T.Roles	A user may assume a more privileged role than permitted and use the enhanced privilege to take unauthorized actions.
8	T.Replay	An unauthorized individual may gain access to the system and sensitive data through a "replay" attack that allows the individual to capture identification and authentication.

3.3 - Secure Usage Assumptions and Threats for the IT Environment

Secure usage assumptions for the environment are defined in Table 3.3, below. These assumptions are included in the TCG PC Specific TBB PP and the TCG PC Specific TBB With Maintenance PP. Threats to TOE security environment are defined in Table 3.4, below. These threats apply to the environment in both the TCG PC Specific TBB PP and the TCG PC Specific TBB With Maintenance PP.

Table 3.3 – Secure Usage Assumptions

#	Name	Assumption
1	AE.Certified_TPM	The TPM connected to the TOE is a CC certified component, compliant with the TCG TPM PP, and is present during any operation of the TOE.

Table 3.4 – Threats to the IT Environment

#	Name	Assumption
1	TE.Bypass	An attacker may bypass IT Environmental security functions and gain unauthorized access to TOE assets.
2	TE.Presence	A remote attacker may cause the IT environment to pass an indication of physical presence to the TOE, thereby allowing the attacker to perform operations on the TPM that may only be performed when physically present at the platform.
3	TE.Reset	The CPU may reset without the TPM reset, resulting in a set of invalid PCR values and denial of service or the TPM may reset without a CPU reset, resulting in a TPM with PCRs set to their initial state (i.e., the value 0), resulting in an untrusted root of trust.

4 - Security Objectives

4.1 - Security Objectives for the TOE

The security objectives in Table 4.1 are included in both the TCG PC Specific TBB PP and the TCG PC Specific TBB With Maintenance PP.

Table 4.1 – Security Objectives for the TOE

#	Name	Objective
1	O.Correct_CRTM	The TSF shall unambiguously associate the CRTM with the TOE and the TSF shall enforce that the CRTM is the correct CRTM for the TOE.
2	O.CRTM_First	The TOE shall ensure that the CRTM code is the first code executed upon platform reset.
3	O.Detect_Physical	The TOE shall provide features that permit a human to detect at least one method of physical tampering with the TPM connection.
4	O.Fail_Secure	The TOE shall preserve a secure state in the event of failure of the TPM connection.
5	O.Integrity	The CRTM shall measure the integrity of the next component to execute and pass integrity data to the TPM.
6	O.One_To_One	The TOE shall enforce a one-to-one relationship between the TPM and the Platform.
7	O.Secure_State	The TOE shall maintain and recover to a secure state without security compromise after system error or other interruption of system operation.
8	O.Self_Protect	The TSF shall maintain a domain for its own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure.

4.2 - Security Objectives for the Maintenance Package

The security objectives in Table 4.2 apply to the Maintenance Package. The security objectives apply to the TCG PC Specific TBB With Maintenance PP only.

Table 4.2 – Security Objectives for the TOE

#	Name	Objective
1	O.DAC	The TOE shall control and limit access to the objects and resources on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the discretionary security policy.
2	O.Data_Consistency	The TOE shall operate under a set of defined rules when interpreting TBB maintenance information shared between or received from another trusted IT product.
3	O.I&A	The TOE shall uniquely identify all users, and must authenticate the claimed identity before granting a user access to TOE protected objects, except those explicitly defined by the ST author.
4	O.Init_Secure	The TOE shall assign valid default security attributes to an object when an object is initialized and shall allow only authorized users to change default security attributes.
5	O.Limit_Actions	The TOE shall restrict the actions a user may perform before the TSF verifies the identity of the user.
6	O.Security_Mgt	The TOE shall enforce access control to ensure that only authorized users with specific, managed roles may change security attributes.
7	O.Security_Roles	The TOE shall maintain security-relevant roles and associations of users with those roles.
8	O.Single_Auth	The TOE shall provide a single use authentication mechanism and require re-authentication to prevent “replay” attacks.

4.3 - Security Objectives for the IT Environment

The security objectives in Table 4.3 are included in both the TCG PC Specific TBB PP and the TCG PC Specific TBB With Maintenance PP.

Table 4.3 – Security Objectives for the IT Environment

#	Name	Assumption
1	OE.Certified_TPM	The TPM included in the IT environment shall be a CC certified component, compliant with the TCG TPM PP and shall be present during any operation of the TOE.
2	OE.Invoke	The IT Environment shall invoke IT Environmental security functions defined by the ST author to support the TOE Security Policy.
3	OE.Presence	The IT Environment shall pass an unambiguous indication of physical presence to the TOE.
4	OE.Reset	The IT Environment shall ensure that the CPU and TPM are reset simultaneously and that the reset signal shall be derived from or initiated by the platform reset or power-on signal.

5 - IT Security Requirements

This section defines the TOE security functional requirements, assurance requirements and environmental requirements for both of the PPs defined in this document. Security requirements are defined as follows:

- TBB Security Functional Requirements in Section 5.1 apply to both the TCG PC Specific TBB Protection Profile and the Trusted Computing Group PC Specific TBB with Maintenance Protection Profile.
- Maintenance Package Security Functional Requirements in Section 5.2, which apply only to the Trusted Computing Group PC Specific TBB with Maintenance Protection Profile.
- Requirements for the IT environment in Section 5.3, which apply to both the Trusted Computing Group PC Specific TBB Protection Profile and the Trusted Computing Group PC Specific TBB with Maintenance Protection Profile.
- TOE Security Assurance Requirements in Section 5.5, which apply to both the Trusted Computing Group PC Specific TBB Protection Profile and the Trusted Computing Group PC Specific TBB with Maintenance Protection Profile.

Strength of function is discussed in Section 5.4 for both PPs.

Requirements are drawn from the CC Parts 2 and 3 and have been written as required as Part 2 extended requirements. Selections and assignments to be made by the ST author in Part 2 and Part 2 extended requirements are enclosed in [square brackets] and text is in *italics*. A list of selections, identified as “Selection by the ST author,” allow the ST author to select one or more of the items listed as indicated. Assignments, identified as “Assignment by the ST author,” provide the ST author with the opportunity to insert specific information. The refinements in Part 2 requirements are indicated by *italics*. Assignments and selections in Part 2 requirements are indicated by *italics*.

The TOE SFRs for both of the PPs defined in this document are Part 2 Extended and the TOE SARs are Part 3 Conformant. The SFRs are Part 2 Extended, because there are explicitly stated requirements as well as requirements drawn from Part 2.

The definition of Part 2 extended is found in the CC Part 3, section 5.4, “Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2. All functional requirements included these PPs are listed in Table 5.1, below. Part 2 extended requirements are explicitly identified as “Part 2 extended.”

Table 5.1 – Part 2 or Part 2 Extended Requirements

Requirement	**Part 2 or extended**
TBB PC PP Requirements	
FPT_CIC.1	Part 2 Extended
FPT_FLS.1	Part 2
FPT_FST.1	Part 2 Extended
FPT_ITM.1	Part 2 Extended
FPT_OTO.1	Part 2 Extended
FPT_PHP_TPM.1	Part 2 Extended
FPT_RCV.4	Part 2
FPT_SEP.1	Part 2
Additional Requirements for the TBB PC PP With Maintenance	
FDP_ACC.1	Part 2
FDP_ACF.1	Part 2
FIA_UAU.1	Part 2
FIA_UID.1	Part 2
FMT_MOF.1	Part 2
FMT_MSA.1	Part 2
FMT_MSA.3	Part 2
FMT_SMF.1	Part 2
FMT_SMR.1	Part 2
FPT_RPL.1	Part 2
FPT_TDC.1	Part 2
Requirements for the IT Environment	
FDP_IPP.1	Part 2 Extended
FPT_ENV_RST.1	Part 2 Extended
FPT_RVM_ENV.1	Part 2 Extended

5.1 - TOE Security Functional Requirements

The security functional requirements for the TBB are provided in Table 5.2. The full text of the security functional requirements is contained below. These functional requirements are included in both the TCG PC Specific TBB PP and the TCG PC Specific TBB with Maintenance PP.

Table 5.2 – TBB Security Functional Requirements

#	Functional Requirement	Title
1	FPT_CIC.1	CRTM is the correct CRTM
2	FPT_FLS.1	Failure with preservation of a secure state
3	FPT_FST.1	CRTM first to execute
4	FPT_ITM.1	Measures integrity of next component
5	FPT_OTO.1	TPM associated one-to-one with platform
6	FPT_PHP_TPM.1	Indication of physical attack on the TPM connection
7	FPT_RCV.4	Function recovery
8	FPT_SEP.1	TSF domain separation

5.1.1 - FPT – Protection of the TOE Security Functions

FPT_CIC.1 CRTM is the correct CRTM

Hierarchical to: No other components.

FPT_CIC.1.1 The TSF shall unambiguously associate a CRTM with the TOE.

FPT_CIC.1.2 The TSF shall enforce that the CRTM is the correct CRTM for the TOE by the following means: *[Assignment by the ST author: means of enforcing that the CRTM is the correct CRTM].*

Dependencies: No dependencies.

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *TPM connection failure, [Assignment by the ST author: other failures defined]*.

Dependencies: ADV_SPM.1 Informal TOE security policy model

Application Note: *CRTM failure is not included in this requirement because such a failure cannot be checked. TPM operation failure is not included because the TPM has its own fail-safe mechanisms that are not included in the TOE. The intention of this requirement is if the initial measurement cannot be made, the TOE must take some action so that components executing outside and after the TOE cannot establish or otherwise use the TPM. A connection failure can be detected by the CRTM not receiving a response from the TPM or receiving a communication failure from the communication bus that the TPM is on.*

FPT_FST.1 CRTM first to execute

Hierarchical to: No other components.

FPT_FST.1.1 The CRTM shall be the first code executed upon reset of the platform.

Dependencies: FPT_ENV_RST.1 Simultaneous reset of CPU and TPM

Application Note: *The TCG PC Specific Implementation Specification states, " The CRTM MUST be an immutable portion of the Platform's initialization code that executes upon Platform Reset. The Platform's execution MUST begin at the CRTM upon any Platform Reset." This requirement implements that portion of the specification.*

FPT_ITM.1 Measures integrity of next component

Hierarchical to: no other requirement

FPT_ITM.1.1 The CRTM shall measure the BIOS code and data not part of the TOE to which control will next be passed.

FPT_ITM.1.2 The CRTM shall incorporate via an extend operation the results of the measurement to the TPM prior to passing control to the next component.

Application note: *Once determining which is the next component that the CRTM will pass control of the platform to, the CRTM calculates a hash of that component. After calculating the hash of the next component the CRTM executes a TPM_Extend operation per the TCG PC Specific Specification. Once this operation is complete, the CRTM does not pass control to any other component except the one it hashed and extended as described in the requirement.*

Dependencies: No dependencies.

FPT_OTO.1 TPM associated one-to-one with platform

Hierarchical to: no other components

FPT_OTO.1.1 The TOE shall enforce a one-to-one relationship between the TPM and the platform by the following means: *[Assignment by the ST author: means of enforcing a one-to-one relationship between the TPM and the platform].*

Dependencies: No dependencies.

Application Note: *There is a one-to-one relationship between the TPM and the platform, which is maintained by the connection that is part of the TOE. The TPM may be removable from the PC motherboard, but must not be movable to another PC motherboard and still be operational. The meaning of a one-to-one relationship is that the TPM connection shall ensure that one and only one specific TPM may be connected to a platform. The ST author will specify the means of enforcement of the one-to-one relationship. Some examples of enforcement are: cryptographic techniques, data erasure, and fixing the TPM to the TOE with solder or glue.*

FPT_PHP_TPM.1 Indication of physical attack on the TPM Connection

Hierarchical to: No other components.

FPT_PHP_TPM.1.1 The TSF shall provide the specified unambiguous attack indication of at least one method or methods of physical tampering with the TPM connection that might compromise the TSF: *[Assignment by the ST author: specification of unambiguous indication of at least one method or methods of physical tampering].*

FPT_PHP_TPM.1.2 The TSF shall provide the specified capability to determine whether at least one method or methods of physical tampering with the TPM connection has occurred: *[Assignment by the ST author: specification of capability to determine whether at least one method or methods of physical tampering with the TPM connection has occurred].*

Dependencies: No dependencies.

Application Note: *Examples of physical tampering include removal or replacement of the TPM.*

FPT_RCV.4 Function recovery

Hierarchical to: No other components.

FPT_RCV.4.1 The TSF shall ensure that *the following security functions: communication to the TPM, [Assignment by the ST author: other security functions]; and the following failure scenarios: failure of communication to the TPM, [Assignment by the ST author: other failure scenarios]* have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

Dependencies: ADV_SPM.1 Informal TOE security policy model

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.2 - Security Functional Requirements for the Maintenance Package

The security functional requirements for the Maintenance Package are listed in Table 5.3. The full text of the functional requirements is provided below. These functional requirements are included only in the TCG PC Specific TBB with Maintenance PP.

Table 5.3 – Maintenance Package Security Functional Requirements

#	Functional Requirement	Title
1	FDP_ACC.1	Subset access control
2	FDP_ACF.1	Security attribute based access control
3	FIA_UAU.1	Timing of authentication
4	FIA_UID.1	Timing of identification
5	FMT_MOF.1	Management of security functions behavior
6	FMT_MSA.1	Management of security attributes
7	FMT_MSA.3	Static attribute initialisation
8	FMT_SMF.1	Specification of management functions
9	FMT_SMR.1	Security roles
10	FPT_RPL.1	Replay detection
11	FPT_TDC.1	Inter-TSF basic TSF data consistency

5.2.1 - FDP – User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the *TBB Security Policy* on

a) Subjects: commands executing on behalf of users.

b) Objects: keys and user data.

c) [*Assignment by the ST author: access control operations*].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components

FDP_ACF.1.1 The TSF shall enforce the *TBB Security Policy* to objects based on [*Assignment by the ST author: security attributes*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*Assignment by the ST author: rules*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [A*ssignment by the ST author: rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on: [*Assignment by the ST author: rules, based on security attributes, that explicitly deny access of subjects to objects*].

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialisation

5.2.2 - FIA – Identification and authentication

Application Note: The identification and authentication capability is used to authenticate a manufacturer or other maintenance provider and to authorize the performance of maintenance. The method selected for identification and authentication is selected by the manufacturer and is defined in the ST. In all cases, the term "user" is understood as the manufacturer or other authorized maintenance provider.

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components

FIA_UAU.1.1 The TSF shall allow [*Assignment by the ST author: list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

Application Note: The assignment "no actions" is valid.

FIA_UID.1 Timing of identification

Hierarchical to: No other components

FIA_UID.1.1 The TSF shall allow [*Assignment by the ST author: list of TSF mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: None.

Application Note: The assignment “no actions” is valid.

5.2.3 - FMT – Security management

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components

FMT_MOF.1.1 The TSF shall restrict the ability to *disable or enable* the functions *CRTM connection, TPM connection, CRTM maintenance* to [*Selection of one or more by the ST author: TBB administrator, TBB manufacturer,* [*Assignment by the ST author: other roles named in FMT_SMR.1*]].

Dependencies: FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components

FMT_MSA.1.1 The TSF shall enforce the *TBB Security Policy* to restrict the ability to [*Selection of one or more by the ST author: change_default, query, modify, delete,* [*Assignment by the ST author: other operations*]] the security attributes [Assignment by the ST author: *list of security attributes associated with maintenance*] to [*Selection of one or more by the ST author: TBB administrator, TBB manufacturer,* [*Assignment by the ST author: other roles*]].

Dependencies: FMT_SMR.1 Security roles, FDP_ACC.1 Subset access control, FMT_SMF.1 Specification of Management Functions

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components

FMT_MSA.3.1 The TSF shall enforce the *TBB Security Policy* to provide *specific* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*Selection of one or more by the ST author: TBB administrator, TBB manufacturer,* [*Assignment by the ST author: other roles named in FMT_SMR.1*]] to specify alternative initial values to override the default values when an object or information is created.

Application Note: *The security attribute default values are set by the manufacturer and must be specified in the ST.*

Dependencies: FMT_SMR.1 Security roles, FMT_MSA.1 Management of security attributes

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: *managing the group of roles that can interact with the TSF; managing the group of roles that can interact with security attributes,* [*Assignment by the ST author: other management functions defined*].

Dependencies: No dependencies.

FMT_SMR.1 Security roles

Hierarchical to: No other components

FMT_SMR.1.1 The TSF shall maintain the roles: [*Selection of one or more by the ST author: TBB administrator, TBB manufacturer,* [*Assignment by the ST author: other roles*]].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification.

Application Note: *The ST author must ensure that roles defined in FMT_SMR.1, FMT_MSA.1, FMT_MSA.3, and FMT_MOF.1 agree.*

5.2.4 - FPT – Protection of the TOE Security Functions

FPT_RPL.1 Replay detection

Hierarchical to: No other components.

FPT_RPL.1.1 The TSF shall detect replay for the following entities: *command, TBB maintenance request, TBB administrator authorization.*

FPT_RPL.1.2 The TSF shall perform *shutdown of TBB* when replay is detected.

Dependencies: No dependencies.

FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret *TBB maintenance information* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [*Assignment by the ST author: interpretation* rules] when interpreting the TSF data from another trusted IT product.

Dependencies: No dependencies.

5.3 - Functional Security Requirements for the IT Environment

The functional security requirements for the IT Environment are provided below. These functional requirements are included in both the TCG PC Specific TBB PP and the TCG PC Specific TBB with Maintenance PP.

5.3.1 - FDP – User data protection

FDP_IPP.1 Indication of physical presence

Hierarchical to: No other components.

FDP_IPP.1.1 The IT environment shall provide unambiguous indication of physical presence to the TOE.

FDP_IPP.1.2 The indication of physical presence shall come from the physical presence connection.

Dependencies: No dependencies.

Application Note: *Indication of physical presence can be achieved using either a hardware or software mechanism that provides an indication of physical presence to the TOE.*

5.3.2 - FPT – Protection of the TOE Security Functions

FPT_ENV_RST.1 Simultaneous reset of CPU and TPM

Hierarchical to: No other components.

FPT_ENV_RST.1.1 The IT Environment shall provide a reset signal and ensure that the reset signal causes the CPU and TPM to be reset simultaneously.

FPT_ENV_RST.1.2 The reset signal shall be derived or initiated by the platform reset or power-on signal.

Dependencies: No dependencies.

FPT_RVM_ENV.1 Non-bypassability of the SP for the IT environment

Hierarchical to: No other components.

FPT_RVM_ENV.1.1 The IT Environment SF shall ensure that IT Environment SP enforcement functions *[Selection by the ST Author: [Assignment* *by the ST author: functions], none]* are invoked and succeed before each function within the IT Environment SC is allowed to proceed.

Dependencies: No dependencies.

Application Note: This explicitly stated requirement allows the ST author to specify SP enforcement functions performed by the IT environment. "None" is a valid selection.

5.4 - Strength of Function Requirement

The strength of function claim for the TOE authentication function, included only in the Maintenance Package is SOF-high. Strength of function only applies to non-cryptographic, probabilistic or permutational mechanisms with respect to a CC evaluation. Other than the authentication function, there are no other mechanisms to which a SOF requirement applies. The SOF requirement applies to the identification and authentication functionality within the TOE. A minimum strength of function level for both PPs is SOF-basic.

5.5 - TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 3 (EAL3) augmented with ADV_SPM.1, Informal TOE security policy model. All requirements are drawn from Part 3 of the Common Criteria and are therefore not provided in total, but are only listed in Table 5.4, below. EAL3 was selected because the TOE requires a moderate level of independently assured security and requires a thorough investigation of the TOE and its development without substantial re-engineering. ADV_SPM.1 was added because it is a dependency of functional security requirement FPT_FLS.1 and FPT_RCV.4.

Table 5.4 - EAL3 Assurance Requirements, augmented

ACM_CAP.3	Authorisation controls
ACM_SCP.1	TOE CM coverage
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.2	Security enforcing high-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model [Augmentation of EAL 3]
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of security measures
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
AVA_MSU.1	Examination of guidance
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

6 - Rationale

This section provides further evidence and explanation to support the certification of these PPs.

6.1 - Security Objectives Rationale

6.1.1 - Security Objectives Rationale for the TBB

Table 6.1 maps threats to objectives, demonstrating that all threats are mapped to at least one objective. Table 6.2 maps objectives to threats, demonstrating that all objectives are mapped to at least one threat. A discussion of the rationale for threat mappings is provided below. The mappings and rationale below are included in both the TCG PC Specific TBB PP and the TCG PC Specific TBB With Maintenance PP.

Table 6.1 – Mapping the TOE Security Environment to Objectives for the TBB

	Assumption/Threat	Objectives
1	T.CRTM_Not_First	O.CRTM_First
2	T.Failure	O.Fail_Secure
3	T.Incorrect_CRTM	O.Correct_CRTM
4	T.Malfunction	O.Secure_State
5	T.Measure_Integrity	O.Integrity
6	T.Physical	O.Detect_Physical
7	T.Protect	O.Self_Protect
8	T.TPM_One_To_Many	O.One_To_One

T.CRTM_Not_First states that an attacker may cause other code to be executed prior to executing the CRTM code upon platform reset, thereby compromising the CRTM and causing the CRTM to become untrusted. This threat is countered O.CRTM_First, which ensures that the CRTM code is the first code executed upon platform reset.

T.Failure states that an attacker may gain access to secrets by causing the connection to the TPM to fail. This threat is countered by O.Fail_Secure, which ensures that the TOE preserves a secure state in the event of failure of the TPM connection.

T.Incorrect_CRTM states that an attacker may substitute a CRTM in the TOE, causing the CRTM to be invalidated and compromising the security of the data within the TPM. This threat is countered by O.Correct_CRTM, which ensures that the TSF unambiguously associates the CRTM with the TOE and that the TSF enforces that the CRTM is the correct CRTM for the TOE.

T.Malfunction states that a malfunction of the TOE may cause modification of TOE assets or cause TOE assets to be disclosed. This threat is countered by O.Secure_State, which ensures that the TOE maintains and recovers to a secure state without security compromise after system error or other interruption of system operation.

T.Measure_Integrity states that the CRTM may fail to measure the integrity of the next component to execute and thereby cause a denial of service or a compromise of the security of data. This threat is countered by O.Integrity, which ensures that the CRTM measures the integrity of the next component to execute and passes integrity data to the TPM.

T.Physical states that an attacker may cause disclosure or modification of TOE assets by physically interacting with the TOE to exploit vulnerabilities in the physical environment. This threat is countered by O.Detect_Physical, which ensures that the TOE provides features that permit a human to detect at least one method of physical tampering with the TPM connection.

T.Protect states that an operation external to the TOE may interfere with TOE security functions or resources, causing disclosure of TSF data or other errors to occur. This threat is countered by O.Self_Protect, which ensures that the TSF maintains a domain for its own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure.

T.TPM_One_To_Many states that an attacker may disconnect the TPM from the platform and successfully reconnect the TPM with another platform, thereby compromising the security of the data within the TPM and invalidating the CRTM. This threat is countered by O.One_To_One, which ensures that the TOE enforces a one-to-one relationship between the TPM and the Platform.

Table 6.2 – Tracing of Security Objectives to Threats for the TBB

	Objectives	**Threat**
1	O.Correct_CRTM	T.Incorrect_CRTM
2	O.CRTM_First	T.CRTM_Not_First
3	O.Detect_Physical	T.Physical
4	O.Fail_Secure	T.Failure
5	O.Integrity	T.Measure_Integrity
6	O.One_To_One	T.TPM_One_To_Many
7	O.Secure_State	T.Malfunction
8	O.Self_Protect	T.Protect

6.1.2 - Security Objectives Rationale for the Maintenance Package

For the Maintenance Package, Table 6.3 maps threats to objectives, demonstrating that all threats are mapped to at least one objective. Table 6.4 maps objectives to threats, demonstrating that all objectives are mapped to at least one threat. A discussion of the rationale for threat mappings is provided below. The mappings and rationale below are included only in the TCG PC Specific TBB With Maintenance PP.

Table 6.3 – Mapping the Threats to Objectives for the Maintenance Package

#	Threats	Objectives
1	T.Attack	O.DAC
2	T.I&A_Bypass	O.Limit_Actions
3	T.Imperson	O.I&A
4	T.Inconsistent	O.Data_Consistency
5	T.Modify	O.Security_Mgt
6	T.Object_Init	O.Init_Secure
7	T.Roles	O.Security_Roles
8	T.Replay	O.Single_Auth

T.Attack states that an undetected compromise of the TOE assets may occur as a result of an attacker (whether an insider or outsider) attempting to perform actions that the individual is not authorized to perform. This threat is countered by O.DAC, which ensures that the TOE controls and limits access to its objects and resources on the basis of individual users or identified groups of users, as defined by a set of managed roles, and in accordance with the set of rules defined by the discretionary security policy.

T.I&A_Bypass states that an unauthorized individual or user may gain unauthorized access to TOE assets. This threat is countered by O.Limit_Actions, which ensures that the TOE restricts the actions a user may perform before the TSF verifies the identity of the user.

T.Imperson states that an unauthorized individual may impersonate an authorized user of the TOE and thereby gain access to TOE data and operations. This threat is countered by O.I&A, which ensures that the TOE uniquely identifies all users and authenticates the claimed identity before granting a user access to the TOE facilities, except those explicitly defined by the ST author.

T.Inconsistent states that the TOE may fail to consistently interpret and share data with another trusted IT product, such as the manufacturer's maintenance data distribution facility or update/maintenance functions, causing security breaches or erroneous data in the TOE. This threat is countered by O.Data_Consistency, which ensures that the TOE operates under a set of defined rules when interpreting TBB maintenance information shared between or received from another trusted IT product.

T.Modify states that an attacker may modify TOE or user data, e.g., file permissions, in order to gain access to the TOE and its assets. This threat is countered by

O.Security_Mgt, which ensures that the TOE enforces access control to ensure that only authorized users with specific, managed roles may change security attributes.

T.Object_Init states that an attacker may gain unauthorized access to an object upon its creation if the security attributes are not assigned to the object or an unauthorized individual can assign the security attributes upon object creation. This threat is countered by O.Init_Secure, which ensures that the TOE assigns valid default security attributes to an object when an object is initialized and shall allow only authorized users to change default security attributes.

T.Roles states that a user may assume a more privileged role than permitted and use the enhanced privilege to take unauthorized actions. This threat is countered by O.Security_Roles, which ensures that the TSF maintains security-relevant roles and associations of users with those roles.

T.Replay states that an unauthorized individual may gain access to the system and sensitive data through a "replay" attack that allows the individual to capture identification and authentication data. This threat is countered by O.Single_Auth, which ensures that the TOE provides a single use authentication mechanism and requires re-authentication to prevent "replay" attacks.

Table 6.4 – Mapping the Objectives to Threats for the Maintenance Package

#	Objectives	Threats
1	O.DAC	T.Attack
2	O.Data_Consistency	T.Inconsistent
3	O.I&A	T.Imperson
4	O.Init_Secure	T.Object_Init
5	O.Limit_Actions	T.I&A_Bypass
6	O.Security_Mgt	T.Modify
7	O.Security_Roles	T.Roles
8	O.Single_Auth	T.Replay

6.1.3 - Security Objectives Rationale for the IT Environment

The assumptions for and threats to the IT environment are mapped to security objectives in Table 6.5, demonstrating that all assumptions and threats are mapped to at least one objective. Table 6.6 maps objectives to threats and assumptions, demonstrating that all objectives are mapped to at least one threat or assumption. A discussion of the rationale for threat mappings is provided below. The mappings and rationale below are included both in the TCG PC Specific TBB PP and in the TCG PC Specific TBB with Maintenance PP.

Table 6.5 – Mapping the Assumptions and Threats to Objectives for the IT Environment

#	Assumptions and Threats	Objectives
1	AE.Certified_TPM	OE.Certified_TPM
2	TE.Bypass	OE.Invoke
3	TE.Presence	OE.Presence
4	TE.Reset	OE.Reset

AE.Certified_TPM makes the assumption that the TPM connected to the TOE is a CC certified component, compliant with the TCG TPM PP, and that the TPM is present during the operation of the TOE. The objective for the IT environment, OE.Certified_TPM, states that the TPM connected to the TOE shall be a CC certified component, compliant with the TCG TPM PP and that the TPM must be present during the operation of the TOE.

TE.Bypass states that an attacker may bypass IT Environmental security functions and gain unauthorized access to TOE assets. This threat is countered by OE.Invoke, which ensures that the IT Environment invokes IT Environmental security functions defined by the ST author to support the TOE Security Policy.

TE.Presence states that a remote attacker may cause the IT environment to pass an indication of physical presence to the TOE, thereby allowing the attacker to perform operations on the TPM that may only be performed when physically present at the platform. This threat is countered by OE.Presence, which ensures that the IT Environment shall pass an unambiguous indication of physical presence to the TOE.

TE.Reset states that the CPU may reset without the TPM reset, resulting in a set of invalid PCR values and denial of service or the TPM may reset without a CPU reset, resulting in a TPM with PCRs set to their initial state (i.e., the value 0), resulting in an untrusted root of trust. This threat is countered by OE.Reset, which ensures that the CPU and TPM are reset simultaneously and that the reset signal shall be derived from or initiated by the platform reset or power-on signal.

Table 6.6 – Mapping Objectives to Threats and Assumptions for the IT Environment

#	Objectives	Assumptions and Threats
1	OE.Certified_TPM	AE.Certified_TPM
2	OE.Invoke	TE.Bypass
3	OE.Presence	TE.Presence
4	OE.Reset	TE.Reset

6.2 - Security Requirements Rationale

6.2.1 - Functional Security Requirements Rationale for the TBB

The requirements rationale for the security functional requirements is provided in this section. First, in subsection 6.2.1.1, TBB Security Objectives are mapped to functional requirements, rationale is provided, and functional requirements are mapped to TBB security objectives. Next, in subsection 6.2.1.2, rationale is provided to show that functional requirements are mutually supportive.

6.2.1.1 - Functional Security Requirements Mapping and Rationale

The TBB Security Objectives are mapped to functional requirements in Table 6.7, showing that all objectives are necessary. Rationale for the mappings is provided below. Table 6.8 maps requirements to objectives, showing that all functional security requirements are necessary. The mappings and rationale below are included in both the TCG PC Specific TBB PP and the TCG PC Specific TBB with Maintenance PP.

Table 6.7 – TBB Security Objectives Mapped to Functional Requirements

#	Objective	Functional Requirement
1	O.Correct_CRTM	FPT_CIC.1
2	O.CRTM_First	FPT_FST.1
3	O.Detect_Physical	FPT_PHP_TPM.1
4	O.Fail_Secure	FPT_FLS.1
5	O.Integrity	FPT_ITM.1
6	O.One_To_One	FPT_OTO.1
7	O.Secure_State	FPT_RCV.4
8	O.Self_Protect	FPT_SEP.1

O.Correct_CRTM states that the TSF unambiguously associates the CRTM with the TOE and that the TSF enforces that the CRTM is the correct CRTM for the TOE. This objective is mapped to FPT_CIC.1, which requires that the TSF unambiguously associate a CRTM with the TOE and that the TSF enforces that the CRTM is the correct CRTM for the TOE by the means specified by the ST author.

O.CRTM_First states that the TOE shall ensure that the CRTM code is the first code executed upon platform reset. This objective is mapped to FPT_FST.1, which requires that the CRTM be the first code executed upon platform reset.

O.Detect_Physical states that the TOE shall provide features that permit a human to detect at least one method of physical tampering with the TPM connection. This objective is mapped to FPT_PHP_TPM.1, which requires that the TSF provide the specified unambiguous attack indication of at least one method or methods of physical tampering with the TPM connection that might compromise the TSF, such as removal or replacement of the TPM, and that TSF provide a specified capability to determine whether at least one method or methods of physical tampering with the TPM connection has occurred.

O.Fail_Secure states that the TOE shall preserve a secure state in the event of failure of the TPM connection. This objective is mapped to FPT_FLS.1, which requires that the TSF shall preserve a secure state when TPM connection failure occurs.

O.Integrity states that the CRTM shall measure the integrity of the next component to execute and pass integrity data to the TPM. This objective is mapped to FPT_ITM.1, which requires that the CRTM make a measure of the next component to which control will be passed and that CRTM use the results of the measurement to perform TPM_Extend to the TPM.

O.One_To_One states that the TOE shall enforce a one-to-one relationship between the TPM and the Platform. This objective is mapped to FPT_OTO.1, which requires that the TOE enforce a one-to-one relationship between the TPM and the platform.

O.Secure_State states that the TOE shall maintain and recover to a secure state without security compromise after system error or other interruption of system operation. This objective is mapped to FPT_RCV.4, which requires that the TSF ensure that the following security functions: communication to the TPM and other functions specified and the following failure scenarios: failure of communication to the TPM and other failure scenarios specified have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

O.Self_Protect states that he TSF shall maintain a domain for its own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure. This objective is mapped to FPT_SEP.1, TSP domain separation which requires the TSF to protect itself.

Table 6.8 – TBB Functional Requirements mapped to Security Objectives

#	Functional Requirement	Objective
1	FPT_CIC.1	O.Correct_CRTM
2	FPT_FLS.1	O.Fail_Secure
3	FPT_FST.1	O.CRTM_First
4	FPT_ITM.1	O.Integrity
5	FPT_OTO.1	O.One_To_One
6	FPT_PHP_TPM.1	O.Detect_Physical
7	FPT_RCV.4	O.Secure_State
8	FPT_SEP.1	O.Self_Protect

6.2.1.2 - Rationale For Mutually Supportive Functional Requirements

TBB functional requirements are mutually supportive in defining a secure CRTM and secure connections from the CRTM, TPM, and the platform. FPT_CIC.1, FPT_ITM.1, and FPT_FST.1 ensure that the CRTM is the correct CRTM for the platform and that the CRTM operates correctly, i.e., it is the first component to execute, it measures the integrity of the next component, and it passes the integrity measurement data to the TPM. The TPM connection and its relationship to the CRTM are defined by FPT_OTO, which ensures one to one association of the platform with the TPM. FPT_PHP_TPM.1, FPT_RCV.4, and FPT_FLS.1 define protections for the TPM connection. Finally, the entire TOE is protected by FPT_SEP.1, TSF domain separation.

6.2.2 - Functional Security Requirements Rationale for the Maintenance Package

The requirements rationale for the Maintenance Package security functional requirements is provided in this section. First, in subsection 6.2.2.1, Maintenance Package Security Objectives are mapped to functional requirements, rationale is provided, and functional requirements are mapped to Maintenance Package security objectives. Next, in subsection 6.2.2.2, rationale is provided to show that functional requirements are mutually supportive.

6.2.2.1 - Functional Security Requirements Mapping and Rationale

The Maintenance Package Security Objectives are mapped to functional requirements in Table 6.9, showing that all objectives are necessary. Rationale for the mappings is provided below. Table 6.10 maps requirements to objectives, showing that all functional security requirements are necessary. The mappings and rationale below are included only in the TCG PC Specific TBB with Maintenance PP.

Table 6.9 – Maintenance Package Security Objectives Mapped to Functional Requirements

#	Objective	Functional Requirement(s)
1	O.DAC	FDP_ACC.1, FDP_ACF.1, FMT_MOF.1, FMT_MSA.3, FMT_SMF.1
2	O.Data_Consistency	FPT_TDC.1
3	O.I&A	FIA_UAU.1, FIA_UID.1
4	O.Init_Secure	FMT_MSA.3
5	O.Limit_Actions	FIA_UAU.1, FIA_UID.1
6	O.Security_Mgt	FMT_MSA.1, FMT_MSA.3, FMT_SMF.1
7	O.Security_Roles	FMT_SMR.1
8	O.Single_Auth	FPT_RPL.1

O.DAC states that the TOE shall control and limit access to the objects and resources on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the discretionary security policy. This objective is met by :

- FDP_ACC.1, Subset access control, which requires that the TSF enforce the TBB Security Policy.
- FDP_ACF.1, Security attribute based access control, which requires that access controls be applied to enforce specific access control rules defined by the ST author.
- FMT_MOF.1, Management of security functions behavior, which requires that the TSF restrict, according to roles selected by the ST author, the ability to disable or enable the CRTM connection, TPM connection, CRTM maintenance functions. The roles selected by the ST author, include, but are not limited to the TBB administrator, TBB manufacturer, or another specified role.

- FMT_MSA.3, Static attribute initialization, which restricts setting initial values to override the default values to certain specified roles.
- FMT_SMF.1, Specification of management functions, which requires that the TSF be capable of managing the group of roles that can interact with security attributes and the TSF.

O.Data_Consistency states that the TOE shall operate under a set of defined rules when interpreting TBB maintenance information shared between or received from another trusted IT product. This objective is met by FPT_TDC.1, Inter-TSF basic TSF data consistency, which requires that the TSF provides the capability to consistently interpret TBB maintenance information when shared between the TSF and another trusted IT product, such as the manufacturer's maintenance facility. It also requires that the TOE follow interpretation rules as defined by the ST author.

O.I&A states that the TOE shall uniquely identify all users, and must authenticate the claimed identify before granting a user access to the TOE facilities, except those explicitly defined by the ST author. This objective is met by:

- FIA_UAU.1, Timing of authentication, requires that a user be successfully authenticated before performing all actions except those explicitly defined.
- FIA_UID.1, Timing of identification, requires that a user be successfully identified before performing all actions except those explicitly defined by the ST author.

O.Init_Secure states that the TOE shall provide valid default security attributes when an object is initialized and shall allow only authorized users to change default security attributes. This objective is met by FMT_MSA.3, Static attribute initialisation, which requires that the TSF provide specific default values for security attributes and that only ST specified roles be allowed to override the default values when an object or information is created. These security attribute values will be specified in the ST.

O.Limit_Actions states that the security environment shall restrict the actions a user may perform before the TSF verifies the identity of the user. This objective is met by:

- FIA_UAU.1, Timing of authentication, requires that a user be successfully authenticated before performing all actions except those explicitly defined.
- FIA_UID.1, Timing of identification, requires that a user be successfully identified before performing all actions except those explicitly defined by the ST author.

O.Security_Mgt states that the TOE shall enforce access control to ensure that only authorized users with specific, managed roles may change security attributes. This objective is met by:

- FMT_MSA.1, Management of security attributes, which requires that the TSF restrict the ability to create the security attributes associated with maintenance.
- FMT_MSA.3, Static attribute initialization, which restricts setting initial values to override the default values to certain specified roles.
- FMT_SMF.1, Specification of management functions, which requires that the TSF be capable of managing the group of roles that can interact with security attributes.

O.Security_Roles states that the TOE shall maintain security-relevant roles and associations of users with those roles. This objective is met by FMT_SMR.1, Security roles, which requires that the TSF maintain roles including TBB administrator, TBB manufacturer, and other roles as assigned by the ST author, and that the TSF shall associate users with roles.

O.Single_Auth states that the TOE shall provide a single use authentication mechanism and require re-authentication to prevent “replay” attacks. This objective is met by FPT_RPL.1, Replay detection, which requires that the TSF detect replay for TBB maintenance requests for the entities command, TBB maintenance request, and TBB administrator authorization. FPT_RPL.1 requires the TSF to perform a shutdown of the TBB when replay is detected.

Table 6.10 – Maintenance Package Functional Requirements Mapped to Security Objectives

#	Functional Requirement	Objective
1	FDP_ACC.1	O.DAC
2	FDP_ACF.1	O.DAC
3	FIA_UAU.1	O.I&A, O.Limit_Actions
4	FIA_UID.1	O.I&A, O.Limit_Actions
5	FMT_MOF.1	O.DAC
6	FMT_MSA.1	O.Security_Mgt
7	FMT_MSA.3	O.DAC, O.Init_Secure, O.Security_Mgt
8	FMT_SMF.1	O.DAC, O.Security_Mgt
9	FMT_SMR.1	O.Security_Roles
10	FPT_RPL.1	O.Single_Auth
11	FPT_TDC.1	O.Data_Consistency

6.2.2.2 - Rationale For Mutually Supportive Functional Requirements

The functional requirements in the Maintenance Package are mutually supportive in defining a method for identifying and authenticating users and then allowing those users to perform updates to the TBB. Access controls, which are essential to prevent unauthorized access and potential unauthorized modification of the TBB, are provided by FDP_ACC.1 and FDP_ACF.1. Identification and authentication is provided by FIA_UAU.1 and FIA_UID.1 and is supported by FMT_SMR.1, which defines roles, FMT_SMF.1, which requires that the TSF be capable of managing the group of roles that can interact with the TSF, and FPT_RPL.1, which prevents replay attacks. Security management for all of these functions is provided by FMT_MOF.1, FMT_MSA.1, and FMT_MSA.3. Finally, protection and ensuring consistency in the interpretation of the data passed to the TOE to perform maintenance is addressed by FPT_TDC.1.

6.2.3 - Functional Security Requirements Rationale for the IT Environment

The requirements rationale for the security functional requirements for the IT Environment is provided in this section. There are three objectives for the IT Environment mapped to functional requirements, i.e., OE.Invoke, OE.Presence and OE.Reset. The other objective for the IT environment, OE.Certified_TPM, is mapped to an assumption, AE.Certified_TPM. Objectives are mapped to functional requirements for the IT environment in Table 6.11 and rationale is provided below.

Table 6.11 – Security Objectives for the IT Environment Mapped to Functional Requirements

#	Objective	Functional Requirement(s)
1	OE.Invoke	FPT_RVM_ENV.1
2	OE.Presence	FDP_IPP.1
3	OE.Reset	FPT_ENV_RST.1

OE.Invoke states that the IT Environment shall invoke IT Environmental security functions defined by the ST author to support the TOE Security Policy. This objective is mapped to FPT_RVM_ENV.1, which requires that the IT environment of the TOE ensure that security policy enforcement functions defined by the ST author are invoked and succeed before each defined function within the scope of control of the IT environmental SF is allowed to proceed.

OE.Presence states that the IT Environment shall pass an unambiguous indication of physical presence to the TOE. This objective is mapped to FDP_IPP.1, Indication of physical presence, which requires that the TOE environment provide unambiguous indication of physical presence to the TOE.

OE.Reset states that the IT Environment shall ensure that the CPU and TPM are reset simultaneously and that the reset signal shall be derived from or initiated by the platform reset or power-on signal. This objective is mapped to FPT_ENV_RST.1, Simultaneous reset of CPU and TPM, which requires that the IT environment ensures that the CPU and TPM are reset simultaneously and that the reset signal be derived or initiated by the platform reset or power-on signal.

6.2.4 - Assurance Security Requirements Rationale

EAL3 was selected because the TOE requires a moderate level of independently assured security and requires a thorough investigation of the TOE and its development without substantial re-engineering. EAL3 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation, and the high-level design of the TOE to understand the security behaviour. The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, examination of guidance documentation to ensure there is no misleading, unreasonable, and conflicting guidance, and evidence of a developer search for obvious vulnerabilities. EAL3 assurance requirements are applicable and appropriate to support the explicitly stated TOE security functional requirements.

EAL 3 is augmented with ADV_SPM.1 because ADV_SPM.1 is a dependency of functional security requirements FPT_FLS.1 and FPT_RCV.4.

6.2.5 - Strength of Function Rationale

The TOE is assumed to be designed to protect against “low” attack potential overall. Thus, based on the CEM Annex B, Table B.2, the minimum strength of function is SOF Basic. The identification and authentication functionality for the TOE is assumed to be designed to protect against a “high” attack potential. Note that the I&A mechanism used in the TOE is application-specific and SOF analysis must be performed as part of ST development. The TCG PC Specific TBB PP requires a SOF rating of SOF Basic or higher. The TCG PC Specific TBB With Maintenance PP requires a SOF rating overall of SOF Basic or higher and a SOF rating of High for identification and authentication functionality.

A SOF rating reflects the attacker, described in terms of attack potential, against which the probabilistic or permutational security function is designed to protect. To determine a SOF rating for the I&A functionality provided in the TOE, the developer of the ST must calculate the attack potential. One way to calculate the attack potential is to use Table B.3 from the CEM Annex B to calculate a numerical score for attack potential and then use Table B.4 from the CEM Annex B to translate the number into a qualitative attack potential and an SOF rating. For example, using Table B.3, assuming a layman with no knowledge of the TOE and no equipment, with > 1 month elapsed time, and > 1 month access to the TOE results in a score of 17 for attack potential. Note that a brute force attack on the I&A mechanism is obvious and hence the corresponding identifying values are all zero.

Using Table B.4 (duplicated below), the resistance to attack with attack potential score translates to an attack potential of “low”. Again, using Table B.2 or B.4, a SOF rating of SOF Basic is required for attack potential of “low”.

Table B.4 from CEM Annex B

Range of Values	Resistant to attack with attack potential of:	SOF rating
<10	No rating	No rating
10 – 17	Low	Basic
18 – 24	Moderate	Medium
>25	High	High

6.3 - Dependency Rationale

Table 6.12 – Functional Requirements Dependencies

#	Requirement	Dependencies
TBB Requirements		
1	FPT_CIC.1	None
2	FPT_FLS.1	ADV_SPM.1 (Augmentation of EAL 3)
3	FPT_FST.1	FPT_ENV_RST.1 (Item 21)
4	FPT_ITM.1	None
5	FPT_OTO.1	None
6	FPT_PHP_TPM.1	None
7	FPT_RCV.4	ADV_SPM.1 (Augmentation of EAL 3)
8	FPT_SEP.1	None
Maintenance Package Requirements		
9	FDP_ACC.1	FDP_ACF.1 (Item 10)
10	FDP_ACF.1	FDP_ACC.1 (Item 9), FMT_MSA.3 (Item 15)
11	FIA_UAU.1	FIA_UID.1 (Item 12)
12	FIA_UID.1	None
13	FMT_MOF.1	FMT_SMF.1 (Item 16), FMT_SMR.1 (Item 17)
14	FMT_MSA.1	FDP_ACC.1 (Item 9), FMT_SMR.1 (Item 17), FMT_SMF.1 (Item 16)
15	FMT_MSA.3	FMT_MSA.1 (Item 14), FMT_SMR.1 (Item 17)
16	FMT_SMF.1	None
17	FMT_SMR.1	FIA_UID.1 (Item 12)
18	FPT_RPL.1	None
19	FPT_TDC.1	None
Requirements for the IT Environment		
20	FDP_IPP.1	None
21	FPT_ENV_RST.1	None
22	FPT_RVM_ENV.1	None

6.4 - Rationale for Extensions

6.4.1 - Rationale for Extension FPT_CIC.1

FPT_CIC.1, CRTM is the correct CRTM, is included to define the requirement for the CRTM to be unambiguously associated with the TOE and for the TSF to enforce that the CRTM is the correct CRTM for the TOE. Since the CRTM is the basis for trust for the security of the TOE and components in the TOE IT environment, i.e., the TPM, it is essential that the CRTM be associated with the TOE. No such requirement is available in the Common Criteria.

6.4.2 - Rationale for Extension FPT_FST.1

FPT_FST.1, CRTM First to execute, is included to define the requirement that the CRTM must be the first code to execute upon platform reset. This ensures that other code is not executed prior to CRTM code, which could compromise the security of the CRTM. This is a fundamental property of the reporting of the integrity metrics. This allows formation of the root of trust for reporting. No such requirement is available in the Common Criteria.

6.4.3 - Rationale for Extension FPT_ITM.1

FPT_ITM.1, Measures integrity of next component, is included to define the requirements for developing the chain of trust in the CRTM as each component is executed. A fundamental property of TCG is the establishment of a "chain of trust" where the chain is anchored to a trusted point, which is the CRTM. No such requirement is available in the Common Criteria.

6.4.4 - Rationale for Extension FPT_OTO.1

FPT_OTO.1, TPM associated one-to-one with platform, is included to define the requirement for a one-to-one relationship between the TPM and the platform. Note that the meaning of a one-to-one relationship is that the TPM may be removable, but the TPM connection shall ensure that one and only one specific TPM may be connected to the platform at any given time. This provides assurance that the reporting of the chain of trust comes from a single and valid TPM and not a forged one. If one is forged and the forgery is detected, the TPM can be invalidated (or revoked) without changing the security of the other TPMs in operation. This also provides a way to bind data to the particular platform, which contains the TPM. If the TPM were allowed to be moved to another platform, the data could also be moved. This would be a violation of a basic feature of a TCG platform. No such requirement is available in the Common Criteria.

6.4.5 - Rationale for Extension FPT_PHP_TPM.1

FPT_PHP_TPM.1, Indication of physical attack on the TPM connection, is included to define the requirement for physical evidence if the TPM connection is tampered with. This supports the requirements for one-to-one association of the TPM to the TOE. No such requirement is available in the Common Criteria.

6.4.6 - Rationale for Extension FDP_IPP.1

FDP_IPP.1, FDP_IPP.1 Indication of physical presence, is included to define the requirement for the IT environment to provide unambiguous indication of physical presence to the TOE and to require that the indication of physical presence come from the physical presence connection. This requirement supports the TOE's ability to trust an indication of physical presence from the IT environment. No such requirement is available in the Common Criteria.

6.4.7 - Rationale for Extension FPT_ENV_RST.1

FPT_ENV_RST.1, Simultaneous reset of CPU and TPM is included to define the requirement for the IT environment that the CPU and TPM are reset simultaneously and that the reset signal shall be derived or initiated by the platform reset or power-on signal. No such requirement is available in the Common Criteria.

6.4.8 - Rationale for Extension FPT_RVM_ENV.1

FPT_RVM_ENV.1, Non-bypassability of the TSP for the IT environment, are included to allow the ST author to specify TSP functions outside the TOE. No such requirement is available in the Common Criteria.

Appendix A – Acronyms and Terminology

Acronyms

CC - Common Criteria

CRTM – Core Root of Trust for Measurement

EAL - Evaluation Assurance Level

IT - Information Technology

PP - Protection Profile

SF - Security Function

SFP - Security Function Policy

SOF - Strength of Function

ST - Security Target

TBB – Trusted Building Block

TOE - Target of Evaluation

TSC - TSF Scope of Control

TSF - TOE Security Functions

TSFI - TSF Interface

TSP - TOE Security Policy

Terminology

Core Root of Trust for Measurement (CRTM)

See TCG Main Specification

Extend operation or just Extend

See the TCG Main Specification

Measurement

The function of a currently executing component as follows:

1. Prior to branching outside the currently executing block the code, the currently executing code performs a hash function on the entire block of code that is to be executed next.
2. Using the above hash value, perform an Extend operation on the appropriate PCR as defined by the TCG PC Specific Implementation Specification.
3. Optionally create a TCG Log entry as defined by the TCG PC Specific Implementation Specification.

PC motherboard

See TCG PC Specific Implementation Specification of motherboard.

Owner

This is the TCG term, which is equivalent to administrator

Platform

See TCG PC Specific Implementation Specification

Platform Reset

See TCG PC Specific Implementation Specification

Root of Trust for Measurement (RTM)

See TCG Main Specification

Trusted Building Block (TBB)

See TCG PC Specific Implementation Specification

Trusted Platform Module (TPM)

See TCG Main Specification