National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

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

Report Number: CCEVS-VR-04-0070

Dated: 18 August 2004

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
Directorate
100 Bureau Drive
Gaithersburg, MD 20899
20755-6740

National Security Agency
Information Assurance
9800 Savage Road STE 6740
Fort George G. Meade, MD

ACKNOWLEDGEMENTS

Validation Team

Louise Huang, Lead Validator, Mitretek Systems

Common Criteria Testing Laboratory

CygnaCom Solutions

McLean, Virginia

Table of Contents

1. Executive Summary

This report documents the NIAP validators' assessment of the evaluation of 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. It presents the evaluation results, their justifications, and the conformance results.

An evaluation of the 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 was completed during July 2004. The evaluation was performed by CygnaCom Solutions, the Common Criteria Testing Laboratory (CCTL) in the United States. The evaluation was conducted in accordance with the requirements drawn from the Common Criteria CC v2.1, Part 3, CEM v1.0 Class APE: Protection Profile Evaluation. The assurance activities in this CC class offer confidence that the TCG PC Specific TBB PP and TCG PC Specific TBB With Maintenance PP contain security requirements that are justifiably included to counter stated threats and meet realistic security objectives. The CC class also offers confidence that the Protection Profiles are internally consistent, coherent and technically sound. The evaluation team determined these Protection Profiles to be Part 2 extended, Part 3 conformant, and to meet Evaluation Assurance Level 3 with Augmentation (EAL3 Augmented) with ADV_SPM.1, Informal TOE security policy model.

The TCG has defined in the PC Specific Specification the specific Building Block that performs the initial platform reset to anchor the chain of the Transitive Trust at the Trusted Building Block or TBB. TCG defines its concept of "measurement" which provides the information about the platform's configuration for a determination of trustworthiness. The measurement is sent to the TPM. The TPM protects this value per the TCG Main Specification and TPM Protection Profile. After the measurement is sent to the TPM, 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. The chain of the Transitive Trust on a computing platform relies on a Root Of Trust established during platform reset to ensure the platform begin its execution in trusted components, which are within the Core Root of Trust for Measurement (CRTM). The trust model for the TCG architecture relies on entities, called "challengers", outside the TBB to determine the validity or trustworthiness of a platform, which is determined by analyzing an unbroken chain of measurements. These chains of measurements are rooted in the TBB, therefore, is called the Root of Trust. The TBB contains a Core Root of Trust for Measurement (CRTM), a Trusted Platform Module (TPM), connection of the CRTM to the motherboard, and the connection of the TPM to the motherboard. The connection of the CRTM to the TPM is done through transitive trust of the CRTM connection and the TPM connection. The CRTM and the TPM are the only trusted components of the motherboard and indication of physical presence requires a trusted mechanism to be activated by the platform owner, the indication of physical presence must also be contained within the TBB. This TCG PC

Specific TBB PP describes the IT security requirements on a TBB except the TPM, which has its own CC evaluated Protection Profile (TCPA TPM PP). The TBB PP compliant TOE is required to provide 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.

The TCG PC Specific TBB With Maintenance Protection Profile contains the security requirements for the TBB and the security requirements for Security Maintenance. Maintenance of the TBB is a capability for defect management, upgrade, or other reasons that may be provided by the platform manufacturer. The BIOS architecture falls under two main categories: CRTM within the BIOS Boot Block and monolithic. In the 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.

For the first category of BIOS architecture, 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. The maintenance requirements apply only to the BIOS Boot Block portion of the BIOS.

The validation team followed the procedures outlined in the Common Criteria Evaluation and Validation Scheme [CCEVS] publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed that the evaluation and all of its activities were in accordance with the CC, the CEM, and CCEVS policy. The validation team concludes that the evaluation has completed and the evaluation team's results are valid. Therefore, the CCEVS grants a Common Criteria Certificate to the sponsor, acknowledging the successful completion of the evaluation and the validity of this Common Criteria Protection Profile.

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List. Table 1: Evaluation Identifiers provides information needed to completely identify the product.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product	Trusted Computing Group (TCG) Personal Computer (PC) Specific Trusted Building Block (TBB) Protection Profile (PP), Version 2.5, dated 20 July 2004 and TCG PC Specific TBB With Maintenance Protection Profile, Version 2.5, dated 20 July 2004.
Evaluation Technical Report	Trusted Computing Group (TCG) Personal Computer (PC) Specific Trusted Building Block (TBB) Protection Profile and TCG PC Specific TBB With Maintenance Protection Profile Evaluation Technical Report, Version 1.4, 20 July 2004
Conformance Result	CC Version 2.1, Part 2 extended CC Part 3 conformant, at EAL3 with ADV_SPM.1, Informal TOE security policy model, Augmentation
Sponsor	Trusted Computing Group (TCG)
PP Authors	TCG Conformance Workgroup

Item	Identifier
Common Criteria Testing Lab (CCTL)	CygnaCom Solutions
CCEVS Validator(s)	Louise Huang, Mitretek Systems

3. Protection Profile Summary

These Protection Profiles specify the functional and assurance security requirements for the Root of Trust for Measurement components within the TCG architecture of Trusted Building Block providing the Root of Trust.   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 TCG Personal Computer (PC) Specific Trusted Building Block (TBB) Protection Profile describes the IT security requirements for a Root of Trust module known as the Trusted Building Block (TBB) in PC specific architecture. 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. The challengers make use of the measurements for making the decisions about the validity or trustworthiness of the platform or its components.

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 in TCG architecture. The TOE always contains the following:

- A Core Root of Trust for Measurement (CRTM)
- A Connection to a Trusted Platform Module (TPM)
- A Connection to the PC motherboard
- A Connection to the PC motherboard’s reset signal
- A Connection to the PC motherboard’s physical presence signal

The TBB provides the Core Root of Trust for Measurement (CRTM) via attestation of the platform’s configuration, hardware, software, or both, for a determination of trustworthiness. A measurement begins by performing a SHA-1 hash on the next

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

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 sent to the TPM, 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.

The TCG PC Specific TBB With Maintenance Protection Profile contains the security requirements for the TBB and the security requirements for Security Maintenance. Maintenance of the TBB is a capability for defect management, upgrade, or other functionalities that may be provided by the platform manufacturer. 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.

4. TOE Security Environment

4.1 Threats to Security

Threats to TOE security are defined in Table 4.1, below. These threats are included in both the TCG PC Specific TBB PP and the TCG PC Specific TBB With Maintenance PP.

Table 4.1 – 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.

#	Name	Threat
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.

4.2 Threats for the Maintenance Package

Threats applicable to the Maintenance package are defined in Table 4.2, below. These threats are included in the TCG PC Specific TBB With Maintenance PP only.

Table 4.2 – 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.

4.3 Threats for the IT Environment

Threats to TOE security environment are defined in Table 4.3, 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 4.3 – 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.

4.4 Environmental Assumptions

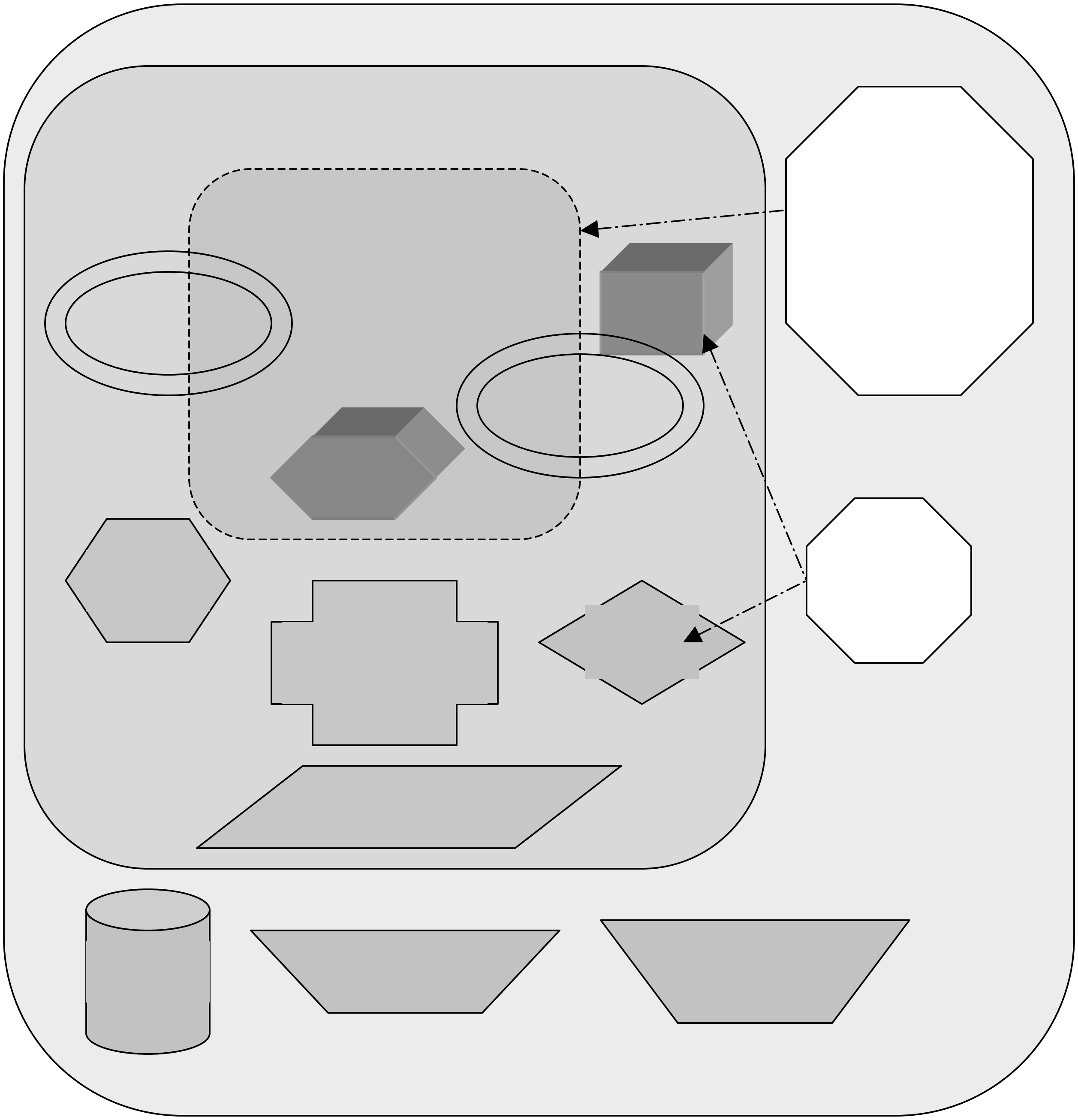
Assumptions for the IT environment are defined in Table 4.4, below. The assumptions are included in the TCG PC Specific TBB PP and the TCG PC Specific TBB With Maintenance PP.

Table 4.4 – Usage Assumptions for the IT Environment

#	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.

5. Architectural Information

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.



6. Security Content of PP

The TBB PP conformant TOE is required to provide the following security features:

- 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.

The TBB With Maintenance PP conformant TOE is required to provide the following additional 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.

7. Documentation

The evaluation evidence is: 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, dated July 20, 2004.

8. Results of the Evaluation

The Common Criteria Testing Laboratory [CCTL] Evaluation Team conducted the evaluation in accordance with the APE section of the CC and the CEM. The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of the APE assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the Security Target authors of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence. The evaluation team accomplished this by providing evaluation observation reports (EORs), or rationale in the draft ETR sections for an evaluation activity (e.g., APE) that recorded the evaluation team's evaluation results and provided them to the developer. The evaluation team also communicated with the developer by telephone, electronic mail, and holding meetings for technical discussion. The evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. No constraints or assumptions were identified in performing this evaluation.

9. Validation Comments/Recommendations

9.1 Recommendations

The Validation team observed that the evaluation and all of its activities were in accordance with the CC, the CEM, and CCEVS practices. The Validator agrees that the CCTL presented appropriate CEM work units and rationale to support a **pass** verdict. The validation team therefore concludes that the evaluation, and results of **pass** for the 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., is complete and correct. The validation team recommends that this evaluation be approved by the CCEVS.

9.2 Comments

The Validation Team would like to note that this Protection Profile author, the Trusted Computing Group (TCG), is a not-for-profit industry-standards organization with the aim of enhancing the security of the computing environment in disparate computer platforms. TCG has adopted the specifications developed by the Trusted Computing Platform Alliance (TCPA). The PC Specific Trusted Building Blocks (TBB) Protection Profile defines a portion of the security requirements for a trustworthiness computer platform. The TBB are the parts of the Roots of Trust. The PC specific TBB is the combination of the CRTM, connection of the CRTM storage to a motherboard, the connection of the TPM to a motherboard, and mechanisms for determining Physical Presence. Normally these include just the instructions for the RTM and TPM initialization functions (reset, etc.).

In TCG systems *roots of trust* are components that must be *trusted* because misbehavior might not be detected. A complete set of Roots of Trust has at least the minimum functionality necessary to describe the platform characteristics that affect the trustworthiness of the platform. The Validation Team would like to note that the TBB Target of Evaluation (TOE) and the Trusted Platform Module (TPM) are the trusted components on the motherboard to form the roots of trust. There are commonly three *Roots of Trust* in a TCG trusted platform:

- A root of trust for measurement (RTM),

- A root of trust for storage (RTS) and
- A root of trust for reporting (RTR).

The RTM is a computing engine capable of making inherently reliable integrity measurements. The CRTM is the instructions executed by the platform when it acts as the RTM. The RTM is also the root of the chain of *transitive trust*.

The RTS is a computing engine capable of maintaining an accurate summary of values of integrity digests and the sequence of digests. The RTR is a computing engine capable of reliably reporting information held by the RTS.

The RTM is provided by a TBB PP conformance TOE and the RTS and the RTR are provided by a TPM PP conformance TOE. Each root is trusted to function correctly without external oversight. Trusting “roots of trust” may be achieved through a variety of ways but is anticipated to include Common Criteria Test Laboratory (CCTL) for technical evaluation by competent experts. A TOE, which is under CC evaluation and claims conformant to the TBB PP, must be tested with a CC evaluated TPM that is conformant with the Trusted Computing Group Trusted Platform Module Protection Profile (TPM PP).

10. Abbreviations

CC - Common Criteria

CRTM – Core Root of Trust for Measurement

EAL - Evaluation Assurance Level

IT - Information Technology

PP - Protection Profile

RTM - Root of Trust for Measurement

SF - Security Function

SFP - Security Function Policy

SOF - Strength of Function

ST - Security Target

TBB – Trusted Building Block

TOE - Target of Evaluation

TPM - Trusted Platform Module

TSC - TSF Scope of Control

TSF - TOE Security Functions

TSFI - TSF Interface

TSP - TOE Security Policy