# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme
# Validation Report

# Trusted Computing Platform Alliance (TCPA)
# Trusted Platform Module
# Protection Profile, Version 1.9.7

|  |  |
|---|---|
| **Report Number:** | **CCEVS-VR-02-0022** |
| **Dated:** | **10 July 2002** |
| **Version:** | **1.0** |

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 20899**

**National Security Agency**
**Information Assurance Directorate**
**9800 Savage Road STE 6740**
**Fort George G. Meade, MD 20755-6740**

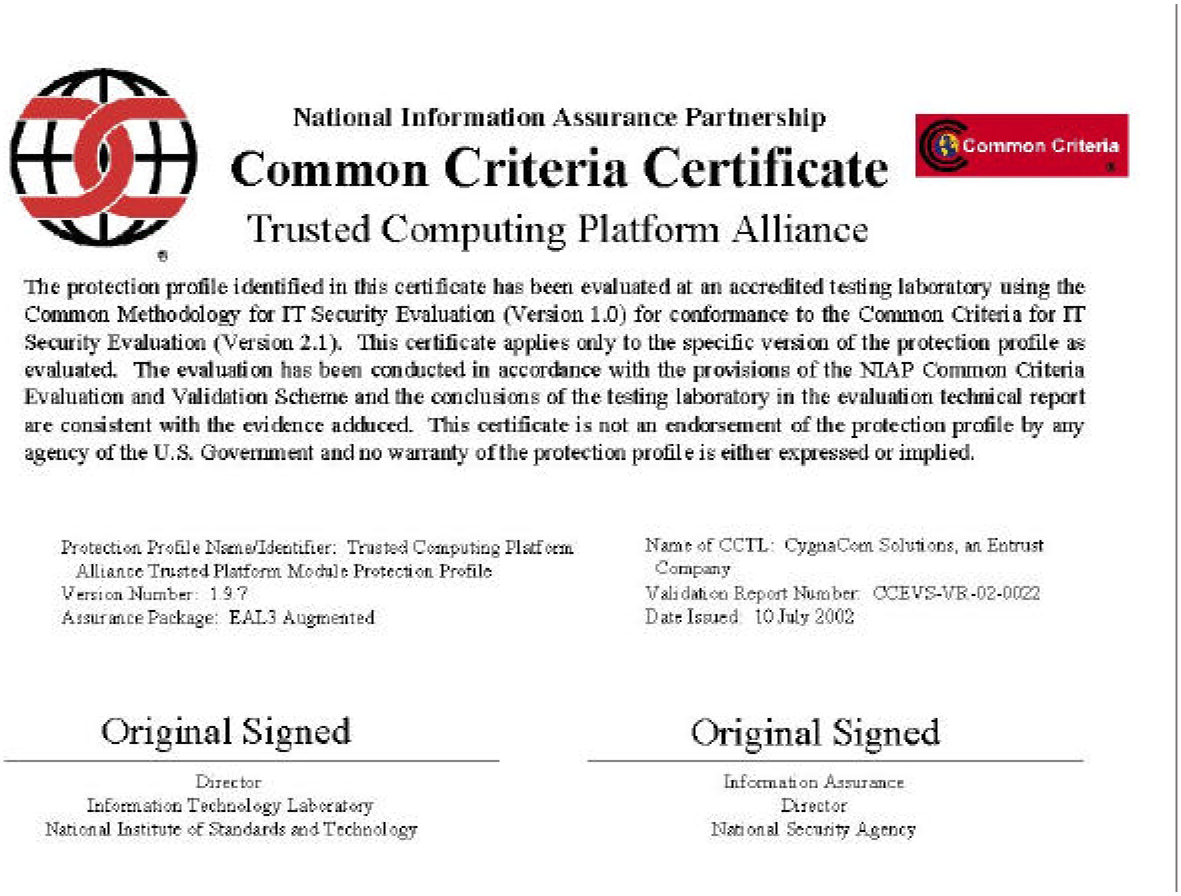
# ACKNOWLEDGEMENTS

## Validation Team

Jeffrey Gilliatt
Mitretek Systems Inc.,
McLean, VA

## Common Criteria Testing Laboratory

CygnaCom Solutions
McLean, Virginia



National Information Assurance Partnership

**Common Criteria Certificate**

Trusted Computing Platform Alliance

The protection profile identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This certificate applies only to the specific version of the protection profile as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the protection profile by any agency of the U.S. Government and no warranty of the protection profile is either expressed or implied.

Protection Profile Name/Identifier: Trusted Computing Platform Alliance Trusted Platform Module Protection Profile
Version Number: 1.9.7
Assurance Package: EAL3 Augmented

Name of CCTL: CygnaCom Solutions, an Entrust Company
Validation Report Number: CCEVS-VR-02-0022
Date Issued: 10 July 2002

Original Signed
Director
Information Technology Laboratory
National Institute of Standards and Technology

Original Signed
Information Assurance
Director
National Security Agency

# Table of Contents

# Executive Summary

The Trusted Computing Alliance (TCPA) Trusted Platform Module (TPM), Protection Profile (PP), Version 1.9.7 evaluation completed on 10 July 2002. The TCPA Trusted Platform Module, Protection Profile evaluation was performed by CygnaCom Solutions in the United Sates. The evaluation was conducted in accordance with the requirements drawn from the Common Criteria CCv2.1, Part 3, Class APE: Protection Profile Evaluation. The assurance activities in this CC class offer confidence that the TCPA Trusted Platform Module PP contains security requirements that are justifiably included to meet realistic security objectives and counter stated threats. The assurance activities in this CC class also offer confidence that the Protection Profile is internally consistent, coherent and technically sound.

The evaluation was also conducted in accordance with CCEVS Policy Letter #2, dated 4 March 2002, which permits the reuse of previous evaluation results. Consequently, the results from the evaluation of the TPM PP version 1.9.4 served as the basis for the evaluation, while the evaluation focused primarily on the incremental changes contained in TPM PP version 1.9.7.

The protection profile identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This Validation Report applies only to the specific version of the protection profile as evaluated. The evaluation has been conducted in accordance with the provision of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the protection profile by any agency of the U.S. Government and no warranty of the protection profile is either expressed or implied.

CygnaCom Solutions, the Common Criteria Testing Laboratory [CCTL], is accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Common Criteria Evaluation and Validation Scheme to conduct security evaluations. The CCTL has presented CEM work units and rationale that are consistent with the CC [Common Criteria], the CEM [Common Evaluation Methodology] and CCEVS publication number 4 Guidance to CCEVS Approved Common Criteria Testing Laboratories. The CCTL evaluation team concluded the requirements of the APE class have been met. Therefore, a **pass** verdict has been issued, by the CCTL, for the protection profile assurance family.

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

## Evaluation Details

| | |
|---|---|
| **Evaluation Completion:** | 10 July 2002 |
| **Evaluated Product:** | Trusted Computing Alliance (TCPA) Trusted Platform Module Protection Profile, Version 1.9.7, 1 July 2002. |
| **Developer:** | CygnaCom Solutions, 7927 Jones Branch Drive, Suite 100 West, McLean, VA 22102-3305 |
| **CCTL:** | CygnaCom Solutions, 7927 Jones Branch Drive, Suite 100 West McLean, VA 22102-3305 |
| **Validation Team:** | Jeffrey Gilliatt, Mitretek Systems, Inc., 3150 Fairview Park South, Falls Church, VA 22042-4519 |
| **Evaluation Class:** | EAL3 augmented with ADV_SPM.1 and ALC_FLR.1 |

## Protection Profile Identification

Trusted Computing Platform Alliance (TCPA) Trusted Platform Module Protection Profile, Version 1.9.7, dated 1 July 2002

## Protection Profile Overview

This PP describes the IT security requirements for a security module known as the Trusted Platform Module (TPM). The TPM provides security primitives in a secure environment. The primitives include digital signatures, random number generation, protected storage and binding information to the TPM. The TCPA TPM is described in detail in the TCPA Main Specification.

## Interpretations

The following NIAP and CCIMB Interpretations were applied during this evaluation:

NIAP Interpretations:

I-0421: Application Notes in Protection Profiles Are Informative Only

CCIMB Interpretations:

CCIMB Interp 080: Work unit does not use `shall examine...to determine'
CCIMB Interp 084: Aspects of objectives in TOE and environment
CCIMB Interp 038: Use of 'as a minimum' in C&P elements
CCIMB Interp 43: Meaning of "clearly stated" in APE/ASE_OBJ.1
CCIMB Interp 51: Use of documentation without C & P elements
CCIMB Interp 64: Apparent higher standard for explicitly stated requirements
CCIMB Interp 85: SOF Claims additional to the overall claim
CCIMB Interp 95: SCP Dependency in ACM_CAP

## Threats to Security

| # | Threat | Description |
|---|---|---|
| 1 | T.Attack | An undetected compromise of the cryptography-related IT assets may occur as a result of an attacker (whether an insider or outsider) attempting to perform actions that the individual is not authorised to perform. |
| 2 | T.Bypass | An unauthorized individual or user may tamper with security attributes or other data in order to bypass TOE security functions and gain unauthorized access to TOE assets. |
| 3 | T.Export | A user or an attacker may export data without security attributes or with unsecure security attributes, causing the data exported to be erroneous and unusable, to allow erroneous data to be added or substituted for the original data, and/or to reveal secrets. |
| 4 | T.Hack_Crypto | Cryptographic algorithms may be incorrectly implemented, allowing an unauthorized individual or user to decipher keys generated within the TPM and thereby gain unauthorised access to encrypted data. |
| 5 | T.Hack_Physical | An unauthorised individual or user of the TOE may cause unauthorised disclosure or modification of TOE assets by physically interacting with the TOE to exploit vulnerabilities in the physical environment. |
| 6 | T.Imperson | An unauthorized individual may impersonate an authorised user of the TOE and thereby gain access to TOE data, keys, and operations. |
| 7 | T.Import | A user or attacker may import data or keys without security attributes or with erroneous security attributes, causing key ownership and authorization to be uncertain or erroneous and the system to malfunction or operate in an unsecure manner. |
| 8 | T.Key_Gen_Destroy | Cryptographic keys may be generated or destroyed in an unsecure manner, causing key compromise. |

| # | Threat | Description |
|---|---|---|
| 9 | T.Malfunction | TOE assets may be modified or disclosed to an unauthorised individual or user of the TOE, through malfunction of the TOE. |
| 10 | T.Modify | An attacker may modify TSF or user data, e.g., stored security attributes or keys, in order to gain access to the TOE and its assets. |
| 11 | T. Object_Attr_Default | A user may create an object with no security attribute values. |
| 12 | T.Object_Attr_Change | A user or attacker may make unauthorized changes to security attribute values for an object. |
| 13 | T.Object_SecureValues | A user may set unsecure values for object security attributes. |
| 14 | T.Residual_Info | A user may obtain information that the user is not authorized to have when the data is no longer actively managed by the TOE (“data scavenging”). |
| 15 | T.Replay | An unauthorized individual may gain access to the system and sensitive data through a “replay” or “man-in-the-middle” attack that allows the individual to capture identification and authentication data. |
| 16 | T.Repudiate_Transact | An originator of data may deny originating the data to avoid accountability. |
| 17 | T.Test | The TOE may start-up in an unsecure state or enter an unsecure state, allowing an attacker to obtain sensitive data or compromise the system. |

## Security Policy

Policy statements whose enforcement must be provided by the [TCPA TPM PP] security mechanisms: None

## Secure Usage Assumptions

Assumptions about the use of the TPM TOE:

| | |
|---|---|
| A.Configuration | The TOE will be properly installed and configured. |

Assumptions about the Operating Environment of the TPM:

| | |
|---|---|
| AE.Physical_Protection | The TOE provides tamper evidence only. It provides no protection against physical threats such as simple power |

analysis, differential power analysis, external signals, or extreme temperature. Physical protection is assumed to be provided by the environment.

## Security Content of PP

- Communication by enforced proof of origin.
- Cryptographic Support employing cryptographic functionality and addressing key management and operational use of cryptographic keys.
- User Data Protection relating to the subset and security attribute(s) based access control, import/export of user data with security attributes, and full residual information protection.
- Identification and Authentication supporting user attribute definitions, timing of authentication data, single-use authentication mechanisms to prevent reuse of authentication data, re-authentication mechanisms, and timing of identification.
- Security Management covering aspects of management of security functions including management of behavior, security attributes, secure security attributes, static attribute initialization, management of TSF data, restrictions on security roles (TPM owner and entity owner, and manufacturer).
- Protection of the TOE Security Functions by protecting the functions that manage and protect the integrity of confidential TSF data from disclosure and modification. This is accomplished through the use of abstract machine testing, failure with the preservation of a secure state, passive detection of physical attack, function recovery, replay detection, non-bypassability of the TSP, TSF domain separation, Inter-TSF basic TSF data consistency and TSF testing.
- Trusted Path/Channels providing protection from modification and disclosure of transmitted data by means of a secure communications trusted path between the TOE and local and remote users.

## Assurance Content of PP

The [TCPA TPM PP] provides for Assurance at the EAL3 – augmented with assurance components as shown in the table below:

| | |
|---|---|
| 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<br>[**Augmented**] |
| AGD_ADM.1 | Administrator guidance |
| AGD_USR.1 | User guidance |
| ALC_DVS.1 | Identification of security measures |
| ALC_FLR.1 | Basic flaw remediation |
| | [**Augmented**] |
| 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 |

## Documentation

The evidence used in this evaluation is based solely upon:

[TCPA TPM PP] Trusted Computing Platform Alliance Trusted Platform Protection Profile, Version 1.9.7, 1 July 2002.

The evaluation and validation methodology was drawn from the following:

[CC_Part 1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_Part 2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_Part 2A] Common Criteria for Information Technology Security Evaluation Part 2: Annexes, dated August 1999, version 2.1.

[CC_Part 3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_Part 1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_Part 2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CCEVS_PUB 1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0, May 1999.

[CCEVS_PUB2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Operating Procedures, Scheme Publication #2, Version 1.5, May 2000.

[CCEVS_PUB3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Validators of IT Security Evaluations, Scheme Publication #3, Version 0.5, February 2001 and version 1.0, February 2002.

[CCEVS_PUB4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, 20 March 2001.

[CCEVS_PUB5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, August 2000.

[CCEVS_POLICY2] Reuse of Previous Evaluation Results & Evidence, CCEVS Policy Letter #2, 4 March 2002.

## Results of the Evaluation

The Common Criteria Testing Laboratory [CCTL] team conducted the evaluation according to the CC and the CEM and concluded that the requirements of the APE class were met. Therefore, a **pass** verdict has been issued for the protection profile assurance family.

## Validator Comments/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 Validation Team 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 result of **pass** for the Trusted Computing Platform Alliance Trusted Platform Module Protection Profile, is complete and correct.