Federal Office
for Information Security

Certification Report

BSI-CC-PP-0030-2008

for

PC Client Specific Trusted Platform Module Family 1.2; Level 2
Version 1.1

from

Trusted Computing Group

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-CC-PP-0030-2008

Common Criteria Protection Profile

PC Client Specific Trusted Platform Module Family 1.2; Level 2
Version 1.1

developed by Trusted Computing Group

Assurance Package claimed in the Protection Profile:
Common Criteria Part 3 conformant
EAL 4 augmented by
ALC_FLR.1
AVA_VAN.4

Common Criteria
Arrangement

Common Criteria

The Protection Profile identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the Protection Profile and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the Protection Profile by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 27 August 2008
For the Federal Office for Information Security

Bernd Kowalski
Head of Department

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products as well as for Protection Profiles (PP).

A PP defines an implementation-independent set of IT security requirements for a category of products which are intended to meet common consumer needs for IT security. The development and certification of a PP or the reference to an existent one gives consumers the possibility to express their IT security needs without referring to a special product. Product or system certifications can be based on Protection Profiles. For products which have been certified based on a Protection Profile an individual certificate will be issued.

Certification of the Protection Profile is carried out on the instigation of the BSI or a sponsor.

A part of the procedure is the technical examination (evaluation) of the Protection Profile according to Common Criteria [1].

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [2]
- Common Criteria for IT Security Evaluation (CC), Version 3.1 [1][5]
- Common Methodology for IT Security Evaluation, Version 3.1 [6]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [7]
- Procedure for the Issuance of a PP certificate by the BSI

2 Recognition Agreements

In order to avoid multiple certification of the same Protection Profile in different countries a mutual recognition of IT security certificates - as far as such certificates are based on CC - under certain conditions was agreed.

2.1 International Recognition of CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org.

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007

The Common Criteria Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The PP PC Client Specific Trusted Platform Module Family 1.2; Level 2 Version 1.1 has undergone the certification procedure at BSI.

The evaluation of the PP PC Client Specific Trusted Platform Module Family 1.2; Level 2 Version 1.1 was conducted by the ITSEF TÜV Informationstechnik GmbH. The evaluation was completed on 25 July 2008. The ITSEF TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Trusted Computing Group

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the certification result

This Certification Report only applies to the version of the Protection Profile as indicated.

In case of changes to the certified version of the Protection Profile, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified Protection Profile, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

5 Publication

The PP PC Client Specific Trusted Platform Module Family 1.2; Level 2 Version 1.1 has been included in the BSI list of the certified Protection Profiles, which is published regularly (see also Internet: http:// www.bsi.bund.de and [3]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the Protection Profile. The Certification Report may also be obtained in electronic form at the internet address stated above.

---

6 Information Technology Security Evaluation Facility

7 Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97006
USA

B Certification Results

The following results represent a summary of

- the certified Protection Profile,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Protection Profile Overview

This Protection Profile PC Client Specific Trusted Platform Module Family 1.2; Level 2 Version 1.1 [4] is established by Trusted Computing Group as a basis for the development of Security Targets in order to perform a certification of an IT-product (TOE).

The PP identifies the TOE as TCG (Trusted Computing Group) PC Client Specific Trusted Platform Module (PCCS TPM). The TOE is hardware, firmware and/or software that implements the functions defined in the TCG Trusted Platform Module Main Specification, version 1.2, [8] [9] [10] and the PC client specific interface specification [11].

Major security features are described by primitives and security services (which use the primitives). The following primitives (i.e. functionalities) are provided by the TOE:

- cryptographic algorithms (for key generation, digital signatures, random number generation),
- sealing data to system state,
- protected storage,
- binding information to the TPM,
- support of direct anonymous attestation (i.e. digital signing of specific internal TPM data by use of the Attestation Identity Key) and
- physical protection.

The TOE provides all security services based on the Main Specification, which are therefore mandatory, as well as optional services which are mandatory in the Interface Specification. The security services are based on the following TPM trust components:

- Root of Trust for Measurement RTM (computing engine for reliable integrity measurements),
- Root of Trust for Reporting RTP (computing engine capable of reliably reporting information held by the RTS) and
- Root of Trust for Storage RTS (computing engine capable of maintaining an accurate summary of values of integrity digests and the sequence of digests).

Other services are:

- SHA-1 Hashing,
- Digital Signing,
- Non-volatile storage as a shielded location for data of external entities (e.g. secret keys) with related access control,
- Key management: keys may be non-migratable or migratable or even certifiable migratable and
- Tick-counting.

The usage of the TOE is described in chapter 1.3.4 of the PP, where six operational roles of users (TPM owner, delegated entity, entity owner, entity user, user using operatorAuth and world) and the TOE internal subjects, objects and operations are described. The description details their relation and gives information on security attributes and authorisation data. By doing so, the description also refers to related standards.

The TPM life cycle has 7 phases from the protection profile prospective:

1. TPM development
2. TPM manufacturing
3. Platform manufacturing and delivery
4. Platform deployment phase
5. Platform identity registration
6. Platform operation
7. Platform recycling and retirement

The Figure 1 shows typical activities of the TPM life cycle Phase 1 to Phase 7. The functions in the white area are implemented (e.g. or at least supported) by the TOE (e.g. EK may be generated by the TOE or injected into the TOE). The grey area shows activities in the TOE environment. The Phase 1 and 2 are TOE development and manufacturing. They are subject of the evaluation of the development environment.

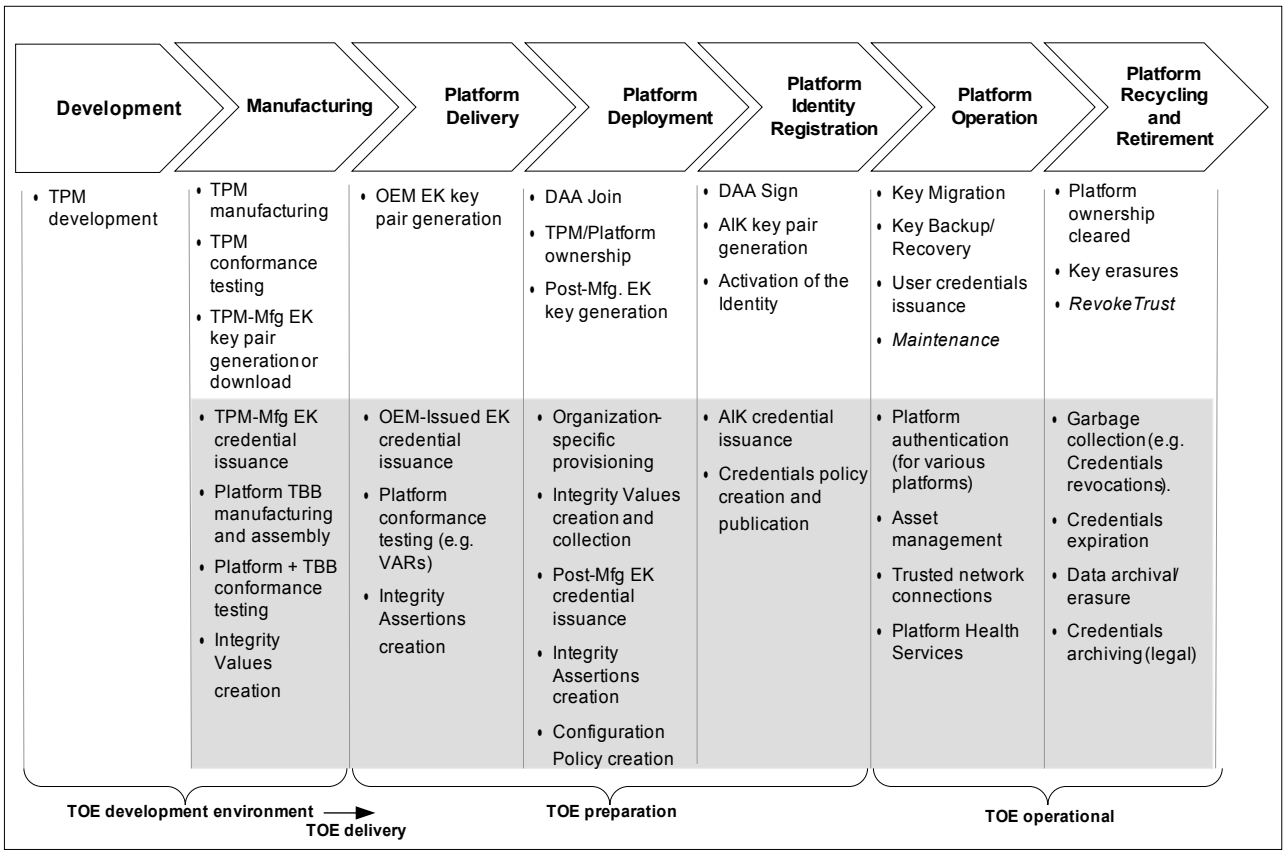

Figure 1: TOE life cycle

The whole life-cycle of the TPM will be considered during evaluations based on this Protection Profile as far as the developer/manufacturer of the TOE is directly involved.

The scope of the assurance components referring to the product's life-cycle is limited to Phases 1 and 2. These phases are under the control of the TPM developer and the TPM manufacturer. This includes the interfaces to the other phases where information and material is being exchanged with the partners of the developer/manufacturer of the TOE. The TPM manufacturer may use the TOE security functions like endorsement key generation described by security functional requirements.

The security functional requirements addressed in this protection profile are mainly used in the Phase 3 to Phase 7.

The assets to be protected by a TOE claiming conformance to this PP are defined in the Protection Profile [4], chapter 1.3.4, paragraph Objects and Operations. Based on these assets the security environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Protection Profile [4], chapter 4.

These Assumptions, Threats Organisational Security and Policies are split into Security Objectives to be fulfilled by a TOE claiming conformance to this PP and Security Objectives to be fulfilled by the IT-Environment of a TOE claiming conformance to this PP. The objectives are outlined in the PP [4], chapter 5.

The Protection Profile [4] requires a Security Target based on this PP or another PP claiming this PP, to be strictly conformant.

2 Security Functional Requirements

Based on the Security Objectives to be fulfilled by a TOE claiming conformance to this PP the security policy is expressed by the set of Security Functional Requirements to be implemented by a TOE. It covers the following issues:

- Security management,
- Cryptographic support,
- TPM Operational Modes,
- Identification, Authentication and Binding,
- Delegation,
- Key management,
- Key Migration,
- Measurement and Reporting,
- Non-volatile Storage,
- Counter,
- Data Import and Export,
- Direct Anonymous Attestation and
- TSF Protection.

The TOE Security Functional Requirements (SFR) are outlined in the PP [4], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the SFR claim is called:

Common Criteria Part 2 extended

3 Assurance Requirements

The TOE security assurance package claimed in the Protection Profile is based entirely on the assurance components defined in part 3 of the Common Criteria. Thus, this assurance package is called:

Common Criteria Part 3 conformant
EAL 4 augmented by
ALC_FLR.1
AVA_VAN.4

(for the definition and scope of assurance packages according to CC see part C or [1], part 3 for details).

4 Results of the PP-Evaluation

The Evaluation Technical Report (ETR) [5] was provided by the ITSEF according to the Common Criteria [1], the Methodology [6], the requirements of the Scheme [2] and all interpretations and guidelines of the Scheme (AIS) [7] as relevant for the TOE.

As a result of the evaluation the verdict PASS is confirmed for the assurance components of the class APE.

The following assurance components were used:

APE_INT.1 PP introduction
APE_CCL.1 Conformance claims
APE_SPD.1 Security problem definition
APE_OBJ.2 Security objectives
APE_ECD.1 Extended components definition
APE_REQ.2 Derived security requirements

The results of the evaluation are only applicable to the Protection Profile as defined in chapter 1.

5 Obligations and notes for the usage

The following aspects need to be fulfilled when using the Protection Profile:

none

6 Protection Profile Document

The Protection Profile PC Client Specific Trusted Platform Module Family 1.2; Level 2 Version 1.1 [4] is being provided within a separate document as Annex A of this report.

7 Definitions

7.1 Acronyms

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

cmd TPM command or commands as defined in [10]

DSAP Delegate-Specific Authorization Protocol

EAL Evaluation Assurance Level

EK Endorsement Key

HMAC Keyed-Hashing for Message Authentication (cf. RFC 2104)

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

Mfg Manufacturing (e.g. TPM-Mfg EK is the Endorsement key of the TPM generated during manufacturing)

NV	non-volatile (memory or area)
OIAP	Object-Independent Authorization Protocol
OSAP	Object-Specific Authorization Protocol
PCR	Platform Configuration Register
PP	Protection Profile
RTM	root of trust for measurement
RTR	root of trust for reporting
SAR	Security assurance requirement
SF	Security Function
SFP	Security Function Policy
SFR	security functional requirement
SRK	storage root key
ST	Security Target
TCG	Trusted Computing Group
TOE	Target of Evaluation
TPM	Trusted Platform Module
TSF	TOE Security Functions

7.2 Glossary

3DES DES - using a key of a size that is 3X the size that of a DES key. See DES.

AIK Credential - A credential issued by a Privacy Certification Authority (CA) that contains the public portion of an AIK key signed by a Privacy CA. The meaning and significance of the fields and the Privacy CA signature is a matter of policy. Typically it states that the public key is associated with a valid TPM. [12]

Attestation - The process of vouching for the accuracy of information. External entities can attest to shielded locations, protected capabilities, and Roots of Trust. A platform can attest to its description of platform characteristics that affect the integrity (trustworthiness) of a platform. Both forms of attestation require reliable evidence of the attesting entity. [12]

Attestation Identity - Key (AIK) An Attestation Identity Key (AIK) is an alias for the Endorsement Key. The AIK is an asymmetric key pair used for signing PCR data only. For interoperability, the AIK is an RSA 2048-bit key.

Augmentation - The addition of one or more requirement(s) to a package.

Authorization - In the TPM terminology: process of the identification, authentication and authorization of users by means of presented shared secrets (cf. [8], chapter 8).

Blob - Opaque data of fixed or variable size. The meaning and interpretation of the data is outside the scope and context of the Subsystem.

Context - A resource saved outside the TPM or loaded into the TPM (cf. [8], ch. 21, [9], ch. 18, [10], ch. 21)

Conformance Credential - A credential that vouches for the conformance of the TPM and the TBB to the TCG specifications.

Credential - Signed data containing information about public keys issued in the IT environment. Credential formats are expressed in ASN.1 notation and are expected to be able to leverage some elements of public key infrastructure. (cf. [14], sec. 4.2.5 for details).

DES - Symmetric key encryption using a key size of 56 bits defined by NIST as FIPS 46-3.

Direct Anonymous Attestation - A Protocol for vouching for an Attestation Identity Key (AIK) using zero-knowledge-proof technology. [12]

Endorsement Credential - A credential containing a public key (the endorsement public key) that was generated by a genuine TPM.

Endorsement Key (EK) - A term used ambiguously, depending on context, to mean a pair of keys, or the public key of that pair, or the private key of that pair; an asymmetric key pair generated by or inserted in a TPM that is used as proof that a TPM is a genuine TPM; the public endorsement key (PUBEK); the private endorsement key (PRIVEK).

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

HMAC - keyed-hashing message authentication code according to RFC 2104

Identity Credential - A credential for an Attestation Identity Key issued by a Privacy CA that provides an identity for the TPM.

Informal - Expressed in natural language.

Integrity metric(s) - Values that are the results of measurements on the integrity of the platform.

Man-in-the-middle attack - An attack by an entity intercepting communications between two others without their knowledge and by intercepting that communication is able to obtain or modify the information between them.

Migratable - A key which may be transported outside the specific TPM.

Nonce - A nonce is a random value that provides protection from replay and other attacks. Many of the commands and protocols in the specification require a nonce.

Non-Migratable - A key which cannot be transported outside a specific TPM; a key that is (statistically) unique to a particular TPM.

Object - An passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Operator - Anyone who has physical access to a platform [12].

Owner - The entity that owns the platform in which a TPM is installed. Since there is, by definition, a one-to-one relationship between the TPM and the platform, the Owner is also the Owner of the TPM. The Owner of the platform is not necessarily the “user” of the platform (e.g., in a corporation, the Owner of the platform might be the IT department while the user is an employee.) The Owner has administration rights over the TPM.

Payload of TPM command - In the context of transport protection: the data of a TPM command except the ordinal, the header information, keys, handles and authorizations which are encrypted in a wrapped transport command, cf. [8], sec. 8.1, for details.

PKI Identity Protocol - The protocol used to insert anonymous identities into the TPM.

Platform Credential - A credential that states that a specific platform contains a genuine TCG Subsystem.

Privacy CA - An entity that issues an Identity Credential for a TPM based on trust in the entities that vouch for the TPM via the Endorsement Credential, the Conformance Credential, and the Platform Credential.

Private Endorsement Key (PRIVEK) - The private key of the key pair that proves that a TPM is a genuine TPM. The PRIVEK is (statistically) unique to only one TPM.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Public Endorsement Key (PUBEK) - A public key that proves that a TPM is a genuine TPM. The PUBEK is (statistically) unique to only one TPM.

Random number generator (RNG) - A pseudo-random number generator that must be initialised with unpredictable data and provides, “random” numbers on demand.

Root of Trust for Measurement (RTM) - The point from which all trust in the measurement process is predicated.

Root of Trust for Reporting (RTR) - The point from which all trust in reporting of measured information is predicated.

Root of Trust for Storing (RTS) - The point from which all trust in Protected Storage is predicated.

RSA - An (asymmetric) encryption method using two keys a private key and a public key. Reference [22].

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

SHA-1 - A NIST defined hashing algorithm producing a 160-bit result from an arbitrary sized source as specified in FIPS 180-2.

Storage Root Key (SRK) - The root key of a hierarchy of keys associated with a TPM; generated within a TPM; a non-migratable key.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

TPM Identity - One of the anonymous PKI identities belonging to a TPM; a TPM may have multiple identities bound to an Attestation Identity Key.

TPM-protected capability - A function which is protected within the TPM, and has access to TPM secrets.

Transport log of commands - Hash value of command parameters of a transport session generated by the commands TPM_EstablishTransport, TPM_ExecuteTransport and TPM_ReleaseTransportSigned and is signed and returned by the command TPM_ReleaseTransportSigned.

Trusted Building Block (TBB) - The parts of the Root of Trust that do not have shielded locations or protected capabilities. Normally includes just the instructions for the RTM and the TPM initialization functions (reset, etc.). Typically platform-specific. One example of a 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. [12]

Trusted Platform Module (TPM) - The set of functions and data that are common to all types of platform, which must be trustworthy if the Subsystem is to be trustworthy; a logical definition in terms of protected capabilities and shielded locations.

Trusted Platform Support Services - The set of functions and data that are common to all types of platform, which are not required to be trustworthy (and therefore do not need to be part of the TPM).

User - An entity that uses the platform in which a TPM is installed. The only rights that a User has over a TPM are the rights given to the User by the Owner. These rights are expressed in the form of authentication data, given by the Owner to the User, that permits access to entities protected by the TPM. The User of the platform is not necessarily the "owner" of the platform (e.g., in a corporation, the owner of the platform might be the IT department while the User is an employee). There can be multiple Users.

Validation Credential - A credential that states values of measurements that should be obtained when measuring a particular part of the platform when the part is functioning as expected.

Validation Data - Data inside a Validation Credential; the values that the integrity measurements should produce when the part of a platform described by the Validation Credential is working correctly.

Validation Entity - An entity that issues a Validation Certificate for a component; the manufacturer of that component; an agent of the manufacturer of that component.

8 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 1, September 2006
Part 2: Security functional components, Revision 2, September 2007
Part 3: Security assurance components, Revision 2, September 2007

[2] BSI certification: Procedural Description (BSI 7125)

[3] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[4] Common Criteria Protection Profile PC Client Specific Trusted Platform Module Family 1.2; Level 2, Version 1.1, July 10, 2008, Trusted Computing Group

[5] Evaluation Technical Report, Version 1, July 21, 2008, TÜV Informationstechnik GmbH (confidential document)

[6] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 2, September 2007

[7] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

[8] TPM Main Part 1 Design Principles, Specification Version 1.2, Revision 94, 29 March 2005, Trusted Computing Group, Incorporated

[9] TPM Main Part 2 TPM Structures, Specification Version 1.2, Revision 94, 29 March 2005, Trusted Computing Group, Incorporated

[8] specifically

- AIS 14, Version 4, 2 April 2007, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 3, 2 April 2007, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC

[10] TPM Main Part 3 Commands, Specification Version 1.2, Revision 94, 29 March 2005, Trusted Computing Group, Incorporated

[11] TCG PC Client Specific TPM Interface Specification (TIS) for TPM Family 1.2; Level 2, Version 1.2 FINAL, Revision 1.00, July 11, 2005

[12] TCG Glossary of Technical Terms, https://www.trustedcomputinggroup.org/groups/glossary/

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

[14] TCG Specification Architecture Overview, Specification, Revision 1.4, 2nd August 2007

[15] IEEE P1363-2000, Standard Specifications for Public Key Cryptography, Institute of Electrical and Electronics Engineers, Inc. (note reaffirmation PAR is actual running)

[16] FIPS PUB 180-2 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SECURE HASH STANDARD, National Institute of Standards and Technology, 2002 August 1

[17] RFC 2104: HMAC: Keyed-Hashing for Message Authentication, http://www.ietf.org/rfc/rfc2104.txt

[18] PKCS #1 v2.0: RSA Cryptography Standard, RSA Laboratories, October 1, 1998

[19] Federal Information Processing Standards Publication 197: Specification for the ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001

[20] FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION DATA ENCRYPTION STANDARD (DES) Reaffirmed 1999 October 25

[21] NIST Special Publication 800-17: Modes of Operation Validation System (MOVS): Requirements and Procedures, February 1998

[22] RSA, The Security Division of EMC, http//www.rsa.com

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (Security Functional Requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see annex A.

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.”

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools

Assurance Class	Assurance Components
	ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

This page is intentionally left blank.

D Annexes

List of annexes of this certification report

Annex A: Protection Profile PC Client Specific Trusted Platform Module Family 1.2; Level 2 Version 1.1 [4] provided within a separate document.

This page is intentionally left blank.