CERTIFICATION REPORT

Certification file:	**TUVIT-DSZ-CC-9214**
Product / system:	trusted platform module PC8375T with HW A4, FW SK4.11
Product manufacturers:	Winbond Electronics Corporation No. 9, Li-Shin Rd. Science-Based Industrial Park Hsinchu, 300, Taiwan *and* National Semiconductor Corporation 2900 Semiconductor Dr. Santa Clara, California, USA 95052-8090
Customer:	Winbond Electronics Corporation
Evaluation facility:	TÜViT, evaluation body for IT security
Evaluation report:	*Version 1.2 as of 2005-11-21* Document-number: *20574959_TÜV_034.03* Author: Dr. Karsten Grans, Wolfgang Peter
Result:	EAL3 augmented ADV_SPM.1, ALC_FLR.1 Compliance to TCPA Trusted Platform Module Protection Profile, Version 1.9.7
Evaluation stipulations:	none
Certifier:	Dr. Christoph Sutter
Certification stipulations:	none

Essen, 2005-11-28

Dr. Ernst-Hermann Gruschwitz Dr. Christoph Sutter

Contents

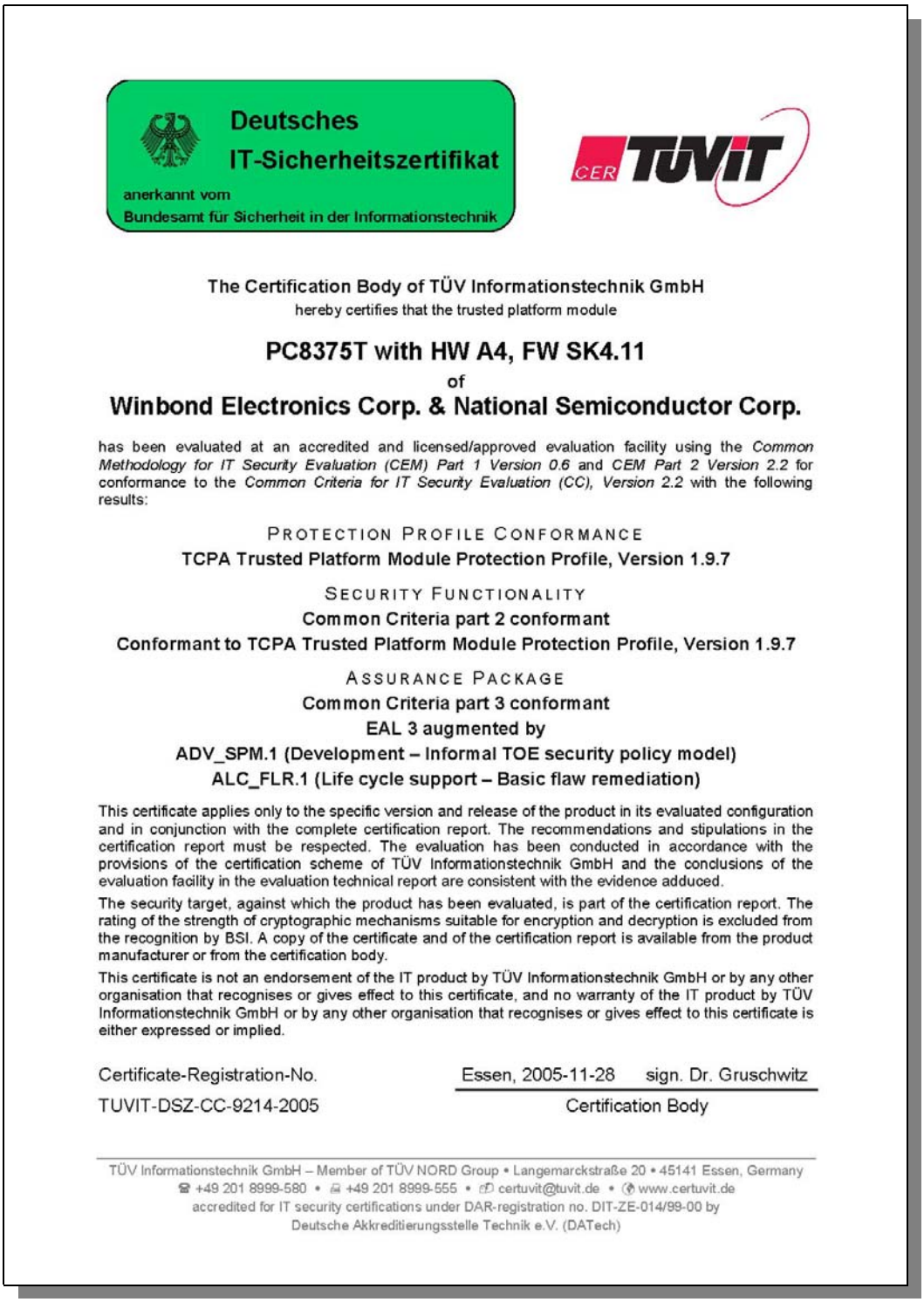
Part A

Certificate and Background of the Certification

Part A presents a copy of the issued certificate and summarizes

- information about the certification body,
- the certification procedure, and
- the performance of evaluation and certification.

1 The Certificate



Deutsches
IT-Sicherheitszertifikat
anerkannt vom
Bundesamt für Sicherheit in der Informationstechnik

CER TÜViT

The Certification Body of TÜV Informationstechnik GmbH
hereby certifies that the trusted platform module

PC8375T with HW A4, FW SK4.11
of
Winbond Electronics Corp. & National Semiconductor Corp.

has been evaluated at an accredited and licensed/approved evaluation facility using the *Common Methodology for IT Security Evaluation (CEM) Part 1 Version 0.6* and *CEM Part 2 Version 2.2* for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.2* with the following results:

PROTECTION PROFILE CONFORMANCE
TCPA Trusted Platform Module Protection Profile, Version 1.9.7

SECURITY FUNCTIONALITY
Common Criteria part 2 conformant
Conformant to TCPA Trusted Platform Module Protection Profile, Version 1.9.7

ASSURANCE PACKAGE
Common Criteria part 3 conformant
EAL 3 augmented by
ADV_SPM.1 (Development – Informal TOE security policy model)
ALC_FLR.1 (Life cycle support – Basic flaw remediation)

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The recommendations and stipulations in the certification report must be respected. The evaluation has been conducted in accordance with the provisions of the certification scheme of TÜV Informationstechnik GmbH and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The security target, against which the product has been evaluated, is part of the certification report. The rating of the strength of cryptographic mechanisms suitable for encryption and decryption is excluded from the recognition by BSI. A copy of the certificate and of the certification report is available from the product manufacturer or from the certification body.

This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate is either expressed or implied.

Certificate-Registration-No.
TUVIT-DSZ-CC-9214-2005

Essen, 2005-11-28 sign. Dr. Gruschwitz
Certification Body

TÜV Informationstechnik GmbH – Member of TÜV NORD Group • Langemarckstraße 20 • 45141 Essen, Germany
☎ +49 201 8999-580 • 🖷 +49 201 8999-555 • certuvit@tuvit.de • www.certuvit.de
accredited for IT security certifications under DAR-registration no. DIT-ZE-014/99-00 by
Deutsche Akkreditierungsstelle Technik e.V. (DATech)

2 Certification Body – CERTÜVIT

CERTÜVIT, the Certification Body of *TÜV Informationstechnik GmbH*[1] – Member of TÜV NORD Group – was established in 1998 and offers a variety of services in the context of security evaluation and validation.

CERTÜVIT was accredited in September 1999 for certification of IT security products according to ITSEC and Common Criteria by *Deutsche Akkreditierungsstelle für Informations- und Telekommunikationstechnik (Dekitz)* now *Deutsche Akkreditierungsstelle Technik e.V. (DATech), Frankfurt/Main* under DAR-registration no. DAT-ZE-014/99-01 and performs its projects under a quality management system certified against ISO 9001 by *Germanischer Lloyd, Hamburg*.

CERTÜVIT is accredited by *Bundesamt für Sicherheit in der Informationstechnik*[2] to issue the "German IT Security Certificate" which is recognised by BSI as equivalent to the "German IT Security Certificate" of BSI.

3 Specifications of the Certification Procedure

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

- DIN EN 45011
- TÜVIT Certification Scheme
- TÜVIT Certification Conditions
- Regulations on the "German IT Security Certificate" issued by the BSI and accepted in the contract of BSI and TÜVIT as of November 20, 2002.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, version 2.2, January 2004.
- Common Methodology for Information Technology Security Evaluation (CEM) part 1, version 0.6, January 1997.
- Common Methodology for Information Technology Security Evaluation (CEM) part 2, version 2.2, January 2004.
- Application Notes and Interpretations of the Scheme (AIS), published by BSI.

[1] in the following termed shortly TÜVIT

[2] in the following termed shortly BSI

4 Recognition Agreements

In order to avoid multiple certification of the same product by different certification bodies a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC – under certain conditions was agreed. CERTÜViT certificates are German IT Security Certificates recognized by BSI – the national German certification body in international agreements – to be equivalent to its own certificates but they are not part of these international agreements.

4.1 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4 was signed between the national participants of Australia and New Zealand, Austria, Canada, Czech Republic, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, The Netherlands, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

4.2 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. The arrangement on the mutual recognition of IT security certificates based on the CC was extended by these participants up to and including the evaluation assurance level EAL7.

5 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The trusted platform module *PC8375T with HW A4, FW SK4.11* has undergone the certification procedure at TÜViT certification body. It was an initial certification.

The evaluation of the trusted platform module PC8375T with HW A4, FW SK4.11 was conducted by the evaluation body for IT-security of TÜViT and concluded on November 21, 2005. The TÜViT evaluation facility is recognised by BSI.

The sponsor and distributor of PC8375T with HW A4, FW SK4.11 is Winbond Electronics Corporation and the developers are Winbond Electronics Corporation and National Semiconductor Corporation.

The certification was concluded with

- the comparability check and
- the preparation of this certification report.

This work was concluded on November 28, 2005. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stipulations regarding generation, configuration and operation, as given in part B of this report, are observed,
- the product is operated – where indicated – in the environment described.

This certification report applies only to the version of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

With regard to the meaning of the evaluation assurance levels (EAL) and the strength of function (SoF), please refer to part C of this report.

6 Publication

The following Certification Results consist of pages B-1 to B-21. The product PC8375T with HW A4, FW SK4.11 will be included in the BSI list of certified products which is published at regular intervals (e. g. in the Internet at http://www.bsi.bund.de) and the TÜViT certification lists (http://www.certuvit.de).

Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form at the internet address of CERTÜViT as stated above.

Part B

Certification Result

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the Certification Result

1 Executive Summary

1.1 Target of Evaluation and Evaluation Background

The target of evaluation (TOE) is the trusted platform module ***PC8375T with HW A4, FW SK4.11***[3]. The PC8375T is a single-chip device, comprising besides the Trusted Platform Module (TPM) for PC security based on the TCG standard, a "Super I/O" module and additional system functions, all together representing the physical scope of the TOE. Within the evaluation the evaluator checked that the additional functionality of the Super I/O and system functions, which are not part of this certification, cannot violate the TSP.

A trusted platform module (TPM) is an integrated circuit and software platform that provides computer manufacturers with the core components of a subsystem used to assure authenticity, integrity and confidentiality within a Trusted Computing Platform. The PC8375T is a complete solution implementing the version 1.1b of the Trusted Computing Group specifications [TCG]. The PC8375T uses the Low Pin Count interface (LPC) as defined by Intel for the integration into existing PC main boards.

The PC8375T TPM module is basically a secure processor supporting the following security features:

- Random number generation
- Algorithm: RSA, SHA-1, HMAC
- Key generation
- Key management
- Key and data storage
- Identification and Authentication mechanisms
- Self Tests
- Access control
- Hacking and physical tampering protection/detection.

The PC8375T TPM module works with a second module called the TCG PC Connection (PCCON), which may include the PC system BIOS and other software. The PCCON module is not part of the certification.

[3] In the following shortly termed PC8375T.

The TOE is conformant to the Trusted Computing Platform Alliance (TCPA) Trusted Platform Module Protection Profile (TPM PP), version 1.9.7 [TPM-PP] and was evaluated against the claims of the Security Target[4] [ST] (attached in part D) by "*evaluation body of TÜV Informationstechnik GmbH*" (TÜViT). The evaluation was completed on November 21, 2005. TÜViT's evaluation body is recognised by BSI.

1.2 Assurance Package

The TOE security assurance requirements are based entirely on the assurance components and classes defined in Part 3 of the Common Criteria (see part C of this report or [CC] Part 3 for details). The TOE meets the assurance requirements of assurance level EAL 3 (Evaluation Assurance Level 3 – methodically tested and checked) augmented by ADV_SPM.1 (Development – Informal TOE security policy model) and ALC_FLR.1 (Life cycle support – Basic flaw remediation).

1.3 Strength of Functions

The TOE's strength of functions is rated "basic" (SOF-basic). The strength of functions rating does not include cryptographic algorithms for encryption and decryption. For more details see also chapter 9 of this report.

1.4 Functionality

All of the TOE's security functional requirements were taken from CC part 2 (i. e. the set is CC part 2 conformant) [CC]. They can be categorized in the following seven categories:

1. communication
2. cryptographic support,
3. user data protection,
4. identification and authentication,
5. security management,
6. protection of the TSF, and
7. trusted path/channels.

[4] hereinafter called ST

Chapter 9 lists the security functional requirements in more detail. They are met by seven suitable TOE security functions (TSF):

TSF	Short Description
1. Cryptographic Operations	Provides RSA digital signature generation and verification, RSA encryption and decryption and generation of SHA-1 hash values.
2. Self-Test	Provides a suite of self tests to check and demonstrate the correct operation of the TOE security functions with regard to RNG functionality, reading and extending the integrity registers, endorsement key pair integrity, RSA sign and verify engine, hash functionality, any tamper-resistance markers and integrity of the complete TPM microcode.
3. Access Control	Enforces the security function policy *Protected Operations Access Controls* (POAC) to protect sensitive subjects (commands), objects (keys and user data) and operations (signature generation/verification, encryption or decryption)
4. Hacking and physical tampering protection/ detection	Provides tamper evidence of the housing, snooping protection/ detection during operation and domain separation for all microcode (TSF code as well as other code) to protect it from interference and tampering by untrusted subjects. In addition, the TOE firmware maintains a total separation between the TPM non-volatile data and the non-TPM data.
5. Key Management	Provides secure generation, storing, and destruction of asymmetric (RSA) cryptographic key pairs.
6. Random Number Generation	Provides generation of random numbers using true hardware random number module according to class P1 of [AIS31].
7. Identification and Authentication	Provides two protocols for authentication and identification to authenticate an entity owner and to authorize use of an entity. The basic premise is to prove knowledge of a shared secret.

Table 1: TOE Security Functions

A more detailed description of the TOE security functions can be found in chapter 6 of the public ST, which is attached as part D of this certification report.

1.5 Summary of Threats and Organisational Security Policies (OSPs)

The asset under attack is the information transiting the TOE. The threat agents include, but are not limited to: 1) people with TOE access who are expected to possess “average” expertise, few resources, and moderate motivation, or 2) failure of the TOE.

All 17 threats are taken from the TCPA Trusted Platform Module Protection Profile, Version 1.9.7 [TPM-PP]:

Threat	Description
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.
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.
T.Export	A user or an attacker may export data without security attributes or with insecure 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.
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.
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.
T.Imperson	An unauthorized individual may impersonate an authorised user of the TOE and thereby gain access to TOE data, keys, and operations.
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 insecure manner.
T.Key_Gen_Destroy	Cryptographic keys may be generated or destroyed in an insecure manner, causing key compromise.
T.Malfunction	TOE assets may be modified or disclosed to an unauthorised individual or user of the TOE, through malfunction of the TOE.
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.
T.Object_Attr_Default	A user may create an object with no security attribute values.
T.Object_Attr_Change	A user or attacker may make unauthorized changes to security attribute values for an object.
T.Object_SecureValues	A user may set insecure values for object security attributes.
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”).

Threat	Description
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.
T.Repudiate_Transact	An originator of data may deny originating the data to avoid accountability.
T.Test	The TOE may start-up in an insecure state or enter an insecure state, allowing an attacker to obtain sensitive data or compromise the system.

Table 2: Threats

No organisational security policies are defined.

1.6 Special Configuration Requirements

The TOE is delivered in one fixed configuration and no further generation takes place after delivery to the customer.

1.7 Assumptions about the Operating Environment

The TOE environment is highly variable. In general, the TOE is assumed to be in an uncontrolled environment with no guarantee of the TOE’s physical security. The TOE secure usage assumption and the assumption for the IT environment are defined in the section chapter 3.1 of the TCPA Trusted Platform Module Protection Profile, Version 1.9.7 [TPM-PP] and are described in chapter 4 of this report.

1.8 Independence of the Certifier

Within the last two years, the certifier did not render any consulting- or other services for the company ordering the certification and there was no relationship between them that might have an influence on his assessment.

The certifier did not participate at any time in test procedures for the product, which forms the basis of the certification.

1.9 Disclaimers

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept with regard to generation, configuration and operation as detailed in this certification report. This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is the trusted platform module PC8375T with HW A4, FW SK4.11 which comprises the hardware of the security controller and the associated firmware.

The TOE delivery comprised the TOE itself in form of a module and the guidance ([AGD], [APN], [DSH]) in form of pdf-files as indicated in the table below.

No	Type	Identifier	Form of delivery
1	HW	**PC8375T with HW A4, FW SK4.11**	module
2	DOC	PC8374T and PC8375T, Guidance, version 1.2, 2005-02-24	pdf-file
3	DOC	TPM Initialization and Configuration for PC8375T and PC8394T, application note, version 07'2004	pdf-file
4	DOC	PC8375T, Datasheet (incl. Errata sheet revision 1.0), version 1.1, 04'2004	pdf-file

Table 3: Deliverables of the TOE

The TOE (item 1) is securely delivered in sealed caged trolley directly to the customer, in general the PC manufacturer. The TOE can be identified by the device marking on the module: **PC8375T0IBM/VLA A3D2**

The guidance documentation (items 2-4) must be downloaded from a secure ftp-server (address: ftp.winbond.co.il). This guidance documentation is additionally dedicated to application software developers.

3 Security Policy

The TOE provides the security function policy *Protected Operations Access Controls* (POAC) to protect the sensitive subjects (commands executed on behalf of users), objects (keys and user data) and operations (signature generation, encryption, decryption, and export and import of user data) of the TOE.

This policy includes:

- roles: TPM owner, entity owner, and TPM manufacturer
- critical security parameters: authentication token, endorsement key pair, storage root key, platform configuration register (PCR) values, DataIntegrityRegisters (Dir), entities, and security attributes
- Modes of access (read, write, execute, and delete) to services, user and TSF data and cryptographic security parameters.

A more detailed description of the security policy can be found in section 5.2.3 of the public ST, which is attached as part D of this certification report and in sections 2.2.6, 2.3, 5.2.3, 5.2.5 of [TPM-PP].

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The following usage assumption is defined in [TPM-PP] and must be regarded when using the TOE:

Assumption	Description
A.Configuration	The TOE will be properly installed and configured.

4.2 Environmental Assumptions

The following usage assumption is defined in [TPM-PP] and must be regarded when using the TOE:

Assumption	Description
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.

4.3 Clarification of Scope

The Target of Evaluation (TOE) is the trusted platform module (TPM) PC8375T with HW A4, FW SK4.11. The TPM works together with a second module called the TCG PC Connection (PCCON), which may include the PC system BIOS and other software. This second module is not part of the TOE and therefore not part of this certification.

5 Architectural Information

The TOE comprises two major components: the hardware (including subcomponents: Core, Memory, Peripherals, Cryptographic Accelerator, Bus interface, and TRNG) and the firmware (including subcomponents: Global Control, Global Services, Security Services, Reset & Init, Commands) as indicated in the following tables:

HW-Subcomponents	Description
Core	central processing unit (CPU)
Memory	contains RAM and non-volatile memory
Peripherals	timers, watchdog, power management and others
Cryptographic Accelerator	accelerators for SHA1 and RSA
Bus Interface	LPC bus interface
TRNG	hardware true random number generator

Table 4: Hardware Subcomponents

FW-Components	Description
Global Control	controls the flow of events handled by the FW
Global Services	volatile and non-volatile memory managers
Security Services	cryptography, key generation, RNG, self-test
Reset & Init	firmware initialization tasks
Commands	handles all TPM commands

Table 5: Firmware Subcomponents

6 Documentation

The following documentation is provided with the product by the developer to the consumer as indicated in chapter 2 above:

- PC8374T and PC8375T, Guidance, version 1.2, 2005-02-24 [AGD]
- TPM Initialization and Configuration for PC8375T and PC8394T, application note, version 07’2004 [APN]
- PC8375T, Datasheet (incl. Errata sheet revision 1.0), version 1.1, 04’2004 [DSH]

7 IT Product Testing

The developer tested the TOE with the overall objectives to verify that the TOE satisfies all requirements specified in Functional Specification (FSP) and that it is a correct and complete implementation of the High Level Design (HLD) description.

The developers testing effort can be summarised in the following four aspects: [ETR]

TOE test configuration:

- The tests are performed with the chip PC8375T with HW A4, FW SK4.11.

Testing approach:

- In the course of the development of the TOE, hardware simulation tests are carried out.
- After successful completion of the hardware simulation tests, the hardware of all TOE subsystems is verified using automatic functional testing.
- The firmware developed for the TOE is tested in a way that will enable to evaluate the level and coverage of security functions and subsystem testing.

Amount of developer testing performed:

- The tests are performed on subsystem level and can be mapped to security functions.

Testing result:

- Overall the TSF have been tested systematically against the Functional Specification and the High Level Design.
- The developer tests demonstrate that the security functions perform as specified.
- All test results are positive and none is failed.

Tests of the evaluation body:

The independent testing of the evaluation body was performed in the developer's testing environment. The specification of the tests was done by the evaluator and implemented by the developer. Employees of the developer performed the actual testing under the supervision of the evaluator. The same platforms and tools as for the developer tests were used.

The evaluator's objective regarding this aspect was to test the functionality of the TOE as described in the Functional Specification and the High Level Design, and to verify the developer's test results by conducting about 30% of the developer's tests and additionally add independent tests. The tests include all security functions.

The results of the specified and conducted independent evaluator tests confirm the TOE functionality as described in the functional specification and the high level design. The TOE security functions were found to behave as specified.

The results of the developer tests, which have been repeated by the evaluator, matched the results of the developer.

The penetration testing according to AVA_VLA.1 was performed in the developer's testing environment considering all obvious vulnerabilities. The same platforms and tools as for the developer tests were used.

The TOE is resistant against all attacks based on the level of a low attack potential.

The penetration testing conducted confirms that all the obvious vulnerabilities were considered and that the vulnerabilities identified are non-exploitable in the intended operational environment of the TOE, if taking into consideration all the measures the user is informed about.

8 Evaluated Configuration

The TOE *PC8375T with HW A4, FW SK4.11* is delivered in one fixed configuration and no further generation takes place. Therefore, the evaluated configuration is identical to the TOE, which can be identified as described in chapter 2 of this certification report.

9 Results of the Evaluation

The Evaluation Technical Report [ETR] was provided by TÜViT's evaluation body according to the requirements of the Scheme, the Common Criteria [CC], the Methodology [CEM] and the Application Notes and Interpretations of the Scheme [AIS]. Especially, the following Application Notes and Interpretations of the Scheme were used in the present certification:

- [AIS 25], [AIS 26], and [AIS 37] for smart card IC specific methodology and
- [AIS 31] for the assessment of the random number generator.

The verdicts for the CC, part 3 assurance classes and components (according to EAL3 augmented by ADV_SPM.1 and ALC_FLR.1 and the class ASE for the Security Target Evaluation) are summarised in the following table:

Assurance classes and components		Verdict
Security Target evaluation	**CC Class ASE**	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration Management	**CC Class ACM**	PASS
Authorisation controls	ACM_CAP.3	PASS
TOE CM coverage	ACM_SCP.1	PASS
Delivery and operation	**CC Class ADO**	PASS
Delivery procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	**CC Class ADV**	PASS
Informal functional specification	ADV_FSP.1	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	**CC Class AGD**	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	**CC Class ALC**	PASS
Identification of security measures	ALC_DVS.1	PASS
Basic flaw remediation	ALC_FLR.1	PASS
Tests	**CC Class ATE**	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	**CC Class AVA**	PASS
Examination of guidance	AVA_MSU.1	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

All assurance components were taken from [CC] part 3 and assessed with the verdict PASS. This includes that all evaluator action elements being part of the assurance components are also assessed with PASS. Therefore, the TOE as defined in the security target is considered to be Part 3 conformant.

Section 5.2 of the public ST, which is attached as part D of this certification report, lists the following TOE security functional requirements.

ID	**Class**/Component
FCO	**Communication**
FCO_NRO.2	Enforced proof of origin

ID	**Class**/Component
FCS	**Cryptographic support**
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP	**User data protection**
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_ETC.2	Export of user data with security attributes
FDP_ITC.2	Import of user data with security attributes
FDP_RIP.2	Full residual information protection
FIA	**Identification and authentication**
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UAU.4	Single-use authentication mechanism
FIA_UAU.6	Re-authenticating
FIA_UID.1	Timing of identification
FMT	**Security management**
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMR.2	Restrictions on security roles
FPT	**Protection of the TSF**
FPT_AMT.1	Abstract machine testing
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.1	Passive detection of physical attack
FPT_RCV.4	Function recovery
FPT_RPL.1	Replay detection
FPT_RVM.1	Non-bypassability of the TSF
FPT_SEP.1	TSF domain separation
FPT_TDC.1	Inter-TSF basic TSF data consistency
FPT_TST.1	TSF testing

ID	**Class**/Component
FTP	**Trusted path/channels**
FTP_TRP.1	Trusted path

All security functional requirements were taken from [CC] part 2, i. e. the TOE is [CC] part 2 conformant.

The TOE is conformant to the TCPA Trusted Platform Module Protection Profile, Version 1.9.7 [TPM-PP].

The evaluation performed in accordance to EAL3 augmented by ADV_SPM.1 and ALC_FLR.1 has shown that the TOE security functional requirements are correctly realised by the TOE security functions. Thus, in realising these functional requirements, it is assured that the TOE will meet the security objectives claimed in the ST.

TSF2 (Self-Test), TSF4 (Hacking and physical tampering protection/detection), TSF5 (Key Management), TSF6 (Random number generation) and TSF7 (Identification and Authentication) fulfil the SOF-rating basic (SOF-basic). The strength of function rating for the RNG was performed according to class P1 of [AIS 31]. The strength of functions rating does not include cryptographic algorithms for encryption and decryption, like RSA in TSF1 (Cryptographic Operations).

The sponsor must advise the certification authority about any modification of the TOE or its guidance documentation. The certification authority will then check whether the certification results are still valid and, if necessary, initiate all further steps concerning a re-evaluation. The results of the evaluation are only applicable to the product "*PC8375T with HW A4, FW SK4.11*". The validity can be extended to new versions and releases of the product or to chips from other production and manufacturing sites, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

10 Evaluation Stipulations, Comments, and Recommendations

The Evaluation Technical Report [ETR] contains the following recommendations and hints:

The TOE is delivered exclusively to the PC manufacturer who is called manufacturer in the following (corresponding to the system administrator in Common Criteria). In a subsequent phase of the TOE's life cycle the so called application software developer, called developer in the following, is responsible for implementing the application software for the TOE. The developer is defined as user (corresponding to the user in Common Criteria). The actual end user of the TOE obtains the TOE from the manufacturer together with the PC on which

the TOE is running. It is the developer responsibility to supply guidance documents to the end user of the TOE.

For this reason only one set of operational documentation [AGD] is provided by the manufacturer. It deals with the two Common Criteria aspects together (user and system administrator documentation) and is of relevance for the manufacturer as well for the developer. The documentation for the manufacturer mainly takes the form of the PC8374T/PC8375T Guidance [AGD], the Datasheet [DSH] and the TPM Initialization and Configuration application note [APN]. The documentation delivered to the developer are only [AGD] and [DSH]. As mentioned above the documents [AGD], [DSH] and [APN] are supplied as guidance documents for the TOE. In addition the referenced documents [TCPA] and [PCS] are publicly available. In [AGD] all security functions relevant for the manufacturer and developer are discussed and exact references to [DSH, APN, TCPA, PCS] are provided where detailed information about these functions can be found.

The guidance [AGD, DSH, APN] encloses the following elements:

- Description of the administrative functions, non-administrative functions and interfaces available to the administrator and the non-administrative users of the TOE (in [AGD] chapter 2).
- Describes assumptions regarding user behaviour that are relevant to secure operation of the TOE and all security parameters, indicates secure values as appropriate (in [AGD] chapter 3 , refined in [APN] chapter 3).
- Description how to administer the TOE in a secure manner and to use the security functions of the TOE (in [AGD] chapter 5 and 8, refined in [APN] chapter 3).
- Describes each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TOE (in [AGD] chapter 6).
- Description of all security requirements for the IT environment that are relevant to the administrator and/or the user (in [AGD] chapter 7).
- Presents all responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of the TOE security requirement (in [DSH] chapter 10 – 13)

With these descriptions the administrator and user receives all information concerning the realisation of the security functions. The purpose and the behaviour of the security functions are described to the administrator and user. It is described by which methods the interfaces of the SF could be invoked and every influence of the security behaviour is explained. In the above cited documents the parameters (and defaults) to be set by the administrator are given.

11 Certification Stipulations and Notes

There are no stipulations or notes resulting from the certification report.

12 Security Target

The public version of the security target [ST-lite] for the trusted platform module *PC8375T with HW A4, FW SK4.11* is included in part D of this certification report.

13 Definitions

13.1 Acronyms

ADM	Administrator Guidance
CC	Common Criteria for Information Technology Security Evaluation (referenced to as [CC])
CEM	Common Methodology for Information Technology Security Evaluation (referenced to as [CEM])
CM	Configuration Management
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DOC	Documentation
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EEPROM	Electrical Erasable and Programmable Read Only Memory
FSP	Functional Specification
HLD	High-level Design
HW	Hardware
IC	Integrated Circuit
IF	Interface
IGS	Installation, Generation and Start-up
LPC	Low Pin Count Interface
OSP	Organisational Security Policy
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SIF	Sub-interface
SOF	Strength of Function
SPA	Simple Power Analysis
SS	Sub-system
ST	Security Target
SW	Software
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Alliance

TOE	Target of Evaluation
TPM	Trusted Platform Module
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Function Interfaces
TSP	TOE Security Policy
USR	User Guidance
VLA	Vulnerability Analysis

13.2 Glossary

Augmentation – The addition of one or more assurance component(s) from Part 3 to an EAL or assurance package.

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.

Informal – Expressed in natural language.

Object – An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile – An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function – A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target – A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

Strength of Function – A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic – A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium – A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high – A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject – An entity within the TSC that causes operations to be performed.

Target of Evaluation – An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions – A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy – A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control – The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[AGD] PC8374T and PC8375T, Guidance, version 1.2, 2005-02-24

[AIS] Application Notes and Interpretations of the Scheme (AIS), published by BSI

[AIS 25] AIS 25, Version 2, as of 2002-07-29 including the CC supporting document: “The Application of CC to Integrated Circuits”, Version 1.2, 07’2002

[AIS 26] AIS 26, Version 2, as of 2002-08-06 including the CC supporting document: “Application of Attack Potential to Smartcards”, Version 1.1, 07’2002

[AIS 31] AIS 31, Version 1, 2001-09-25 “Functionality classes and evaluation methodology for physical random number generators”

[AIS 37] AIS 37, Version 1, as of 2002-07-29 including the CC supporting document: “Guidance for smartcard evaluation”, Version 1.1, 03’2002

[APN] TPM Initialization and Configuration for PC8375T and PC8394T, application note, version 07’2004

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004,
Part 1: Introduction and general model
Part 2: Security functional requirements
Part 3: Security assurance requirements

[CEM] Common Methodology for Information Technology Security Evaluation,
Part 1: Introduction and general model, version 0.6, revision 11.01.1997,
Part 2: Evaluation Methodology, Version 2.2, January 2004

[DSH] PC8375T, Datasheet (incl. Errata sheet revision 1.0), version 1.1, 04'2004

[ETR] Evaluation Technical Report (ETR), TÜV Informationstechnik GmbH, version 1.2, 2005-11-21, document-number: 20574959_TÜV_034.03

[PCS] Trusted Computing Group PC Specific Specification, version 1.0.

[ST] Security Target – NSC SIO with integrated TPM PC8375T, Version 1.4, 2005-11-21
confidential document

[ST-lite] Security Target "Lite" – NSC SIO with integrated TPM PC8375T, Version Version 1.4, 2005-11-21
public version of the Security Target [ST]

[TCG] Trusted Computing Platform Alliance (TCPA) – Main Specification, Version 1.1b, 2002-02-22

[TCPA] Trusted Computing Platform Alliance Main Specification, version 1.1b, 2002-02-22

[TPM-PP] Trusted Computing Platform Alliance (TCPA) – Trusted Platform Module Protection Profile, Version 1.9.7, 2002-07-01
(certified on 2002-07-10 by NIAP under certification ID: CCEVS-VR-02-0022)

Part C

Excerpts from the Criteria

The excerpts from the criteria are dealing with

- conformance results
- assurance categorization
- evaluation assurance levels
- strength of security function
- vulnerability analysis

CC Part 1:

Conformance results

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

> **Part 2 conformant** - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2.
>
> **Part 2 extended** - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2.

plus one of the following:

> **Part 3 conformant** - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3.
>
> **Part 3 extended** - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

> ***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
>
> ***Package name* Augmented** - A PP or TOE is an augmentation of a predefined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

> ***PP Conformant*** - A TOE meets specific PP(s), which are listed as part of the conformance result."

CC Part 3:

Assurance categorisation

The assurance classes, families, and the abbreviation for each family are shown in *Table 6*.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 6: Assurance family breakdown and mapping

Evaluation assurance levels (chapter 6)

“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 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

„Table 7 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 2 of 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 CC 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 extended with explicitly stated assurance requirements."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration Management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Delivery and Operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_IMT					**1**	**2**	***3***
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Guidance Documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Life Cycle Support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability Assessment	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Table 7: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested

“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 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, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested

"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 practice. 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

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

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

"EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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

"EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices 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

“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

“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.“

Strength of TOE security functions (AVA_SOF)

AVA_SOF Strength of TOE security functions

“Strength of function analysis addresses TOE security functions that are realised by a probabilistic or permutational mechanism (e.g. a password or hash function). Even if such functions cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat them by direct attack. A level or a specific metric may be claimed for the strength of each of these functions. Strength of function analysis is performed to determine whether such functions meet or exceed the claim. For example, strength of function analysis of a password mechanism can demonstrate that the password function meets the strength claim by showing that the password space is sufficiently large.”

Three levels exist: SOF-basic, SOF-medium, and SOF-high.

Vulnerability analysis (AVA_VLA)

AVA_VLA Vulnerability analysis

"Vulnerability analysis consists of the identification of flaws potentially introduced in the different refinement steps of the development. It results in the definition of penetration tests through the collection of the necessary information concerning: (1) the completeness of the TSF (does the TSF counter all the postulated threats?) and (2) the dependencies between all security functions. These potential vulnerabilities are assessed through penetration testing to determine whether they could, in practice, be exploitable to compromise the security of the TOE."

Application notes

"A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.

The intent of the developer analysis is to confirm that no identified security vulnerabilities can be exploited in the intended environment for the TOE and that the TOE is resistant to obvious penetration attacks.

Obvious vulnerabilities are considered to be those that are open to exploitation that requires a minimum of understanding of the TOE, skill, technical sophistication, and resources. These might be suggested by the TSF interface description. Obvious vulnerabilities include those in the public domain, details of which should be known to a developer or available from an evaluation authority.

Performing a search for vulnerabilities in a systematic way requires that the developer identify those vulnerabilities in a structured and repeatable way, as opposed to identifying them in an ad-hoc fashion. The associated evidence that the search for vulnerabilities was systematic should include identification of all TOE documentation upon which the search for flaws was based.

Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential. To accomplish this intent, the evaluator first assesses the exploitability of all identified vulnerabilities. This is accomplished by conducting penetration testing. The evaluator

should assume the role of an attacker with a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential when attempting to penetrate the TOE. Any exploitation of vulnerabilities by such an attacker should be considered by the evaluator to be “obvious penetration attacks” (with respect to the AVA_VLA.*.2C elements) in the context of the components AVA_VLA.2 through AVA_VLA.4.”

Part D

Security Target

Attached is the public version of the Security Target: "*Security Target "Lite" – NSC SIO with integrated TPM PC8375T*"

Author: Winbond Electronics Corporation

Date: 2005-11-21

Version: 1.4

NATIONAL SEMICONDUCTOR/WINBOND

Security Target “Lite”

Version:	**1.4**
Date:	**21-Nov-2005**
Product:	**NSC SIO with integrated TPM PC8375T**
Manufacturer:	**Winbond Electronics Corporation (WEC) and National Semiconductor (NSC)**
Certification ID:	**TUVIT-DSZ-CC-9214**
Author:	**Abraham Mizrahi**

Revision History

Version	Date	Description
1.2	7-Feb, 2005	Initial revision based on full ST v1.2
1.3	September 8, 2005	Updated revision
1.4	November 21, 2005	Final revision

Table of Contents

List of Tables

Page

1 Introduction

This section contains document management and overview information. The Security Target (ST) identification provides the labelling and descriptive information necessary to identify, catalogue, register, and cross-reference a ST. The ST overview summarizes the ST in narrative form and provides sufficient information for a potential user to determine whether the ST is of interest. The overview can also be used as a standalone abstract for ST catalogues and registers.

1.1 Identification

The title of this ST is “NSC SIO with integrated TPM PC8375T revision 1.4, dated 21-Nov - 2005”.

The Target of Evaluation (PC8375T with HW A4, FW SK4.11) is a TPM (Trusted Platform Module), a TCG 1.1b compliant security processor with embedded firmware and a “Super I/O” module. The “Super I/O” includes legacy SuperI/O functions, system glue functions, health monitoring and control, commonly used functions such as GPIO, and Power Management support. It includes just one internal bus that connects all the internal subsystems with the LPC interface. In the following the TOE is called PC8375T.

The Security Target is based on the Trusted Computing Group (TCG) Trusted Platform Module Protection Profile (TPM PP) v1.9.7 [PP].

The Protection Profile and the Security Target are built with Common Criteria V2.1. The ST takes into account all relevant current final interpretations.

The assurance level for this protection profile is **EAL3, augmented**. The strength of function is **SOF Basic**.

1.2 Overview

This security target describes the TOE, which is called PC8375T and gives a short summary specification.

The PC8375T is an integrated device, comprising a TPM module, a *SuperIO*, and several other functions.

The TPM module is a separated logical entity from the other functions, and all security functionality is comprised in the TPM module. It provides computer manufacturers with the core components of a subsystem used to assure authenticity, integrity and confidentiality within a Trusted Computing Platform. The PC8375T is a complete solution implementing the version 1.1b of the Trusted Computing Group specifications (TCG). The PC8375T uses the Low Pin Count interface (LPC) as defined by Intel for the integration into existing PC

mainboards. The PC8375T TPM module is basically a secure processor supporting the following protocols and algorithms:

- Random number generation
- Algorithm: RSA, SHA-1, HMAC
- Key generation
- Key management
- Key and data storage
- Identification and Authentication mechanisms
- Self Tests
- Access control
- Hacking and physical tampering protection/detection.

The PC8375T TPM module works with a second module called the TCG PC Connection (PCCON), which may include the PC system BIOS and other software. The PCCON is not part of this evaluation.

1.3 Related Documents

- Trusted Computing Group (TCG) Main Specification, Version 1.1b [TCG]
- Trusted Computing Platform Alliance (TCPA) Trusted Platform Module Protection Profile (TPM PP), Version 1.9.7 [PP]
- Common Criteria (CC) for Information Technology Security Evaluation, Version 2.1 (ISO 15408) [CC]
- Common Methodology (CEM) for Information Technology Security Evaluation [CEM]

1.4 Organization

The main sections of the ST are the TOE Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, PP Claims and Rationale.

Section 2, the TOE Description, provides general information about a Trusted Platform Module and the TOE itself, serves as an aid to understanding the TOE's security requirements, and provides context for the ST's evaluation.

The TOE Security Environment in Section 3 describes security aspects of the environment in which the TOE is to be used and the manner in which it is to be employed. The TOE security environment includes:

a) Assumptions regarding the TOE's intended usage and environment of use

b) Threats relevant to secure TOE operation

c) Organizational security policies with which the TOE must comply

Section 4 contains the security objectives that reflect the stated intent of the ST. The objectives define how the TOE will counter identified threats and how it will cover identified organizational security policies and assumptions. Each security objective is categorized as being for the TOE or for the environment.

Section 5 contains the applicable Security Requirements taken from the Common Criteria, with appropriate refinements. The requirements are provided in separate subsections for the TOE and its environment. The IT security requirements are subdivided as follows:

a) TOE Security Functional Requirements

b) TOE Security Assurance Requirements

The TOE summary specification in chapter 6 consisting of the security functions, the assurance measures and the security function policies is defined in the ST as property of this specific TOE, the PC8375T.

The PP Claims are given in chapter 7 in form of PP reference, PP tailoring and PP additions.

The Rationale in Section 8 presents evidence that the ST is a complete and cohesive set of requirements and that the TOE provides an effective set of IT security countermeasures within the security environment. The Rationale is in three main parts. First, a Security Objectives Rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them. Then, a Security Requirements Rationale demonstrates that the security requirements (TOE and environment) are traceable to the security objectives and are suitable to meet them. Finally the TOE summary specification rationale consists of a TOE security functions rationale and an assurance measures rationale.

A glossary of acronyms and terms used in the ST as well as references are provided in the Appendix in chapter 9.

1.5 Common Criteria Conformance

This ST has 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). The TOE itself is conformant with Common Criteria Version 2.1, part 2 and part 3. Furthermore it is conformant with the protection profile TCG TPMPP version 1.9.7 [PP].

The assurance level for the TOE is **EAL 3 augmented** by ADV_SPM.1 and ALC_FLR.1.

The strength of function is **SOF Basic**.

2 TOE Description

The TOE description helps to understand the specific security environment and the security policy. In this context the assets, threats, security objectives and security functional requirements can be employed. After some general remarks about the Trusted Platform Module in chapters 2.1 and 2.2, chapter 2.3 presents a more detailed description of the TOE than in the [PP] as it refers to this particular TOE implementation.

2.1 TPM - Some general remarks

The Trusted Platform Module is an integrated circuit and software platform that provides computer manufacturers with the core components of a subsystem used to assure authenticity, integrity and confidentiality in e-commerce and Internet communications within a Trusted Computing Platform as defined in [TCG]. The TPM is a complete solution implementing the Trusted Computing Group specification [TCG] which is an industry group originally founded in 1999 by COMPAQ, HP, IBM, Intel, Microsoft as “TCPA”, and later changed to the current TCG organization.

A Trusted Platform is a platform that can be trusted by local users and by remote entities. The basis for trusting a platform is a declaration by a known authority that a platform with a given identity can be trusted to measure and report the way it is operating. That operating information can be associated with data stored on the platform, to prevent the release of that data if the platform is not operating as expected. Other authorities provide declarations that describe the operating information the platform ought to produce when it is operating properly. The local user and remote entities trust the judgment of the authorities; so, when they receive proof of the identity of the platform, information about the current platform environment, and proof about the expected platform environment, they can decide whether to trust the platform to behave in a sufficiently trustworthy and predictable manner. The local user and/or remote entities must take this decision themselves because the level of trust in a platform can vary with the intended use of that platform, and only the local user and/or remote entities know that intended purpose.

The trusted mechanism of the platform uses cryptographic processes, including secrets. The trusted mechanisms are required to be isolated from the platform in order to protect secrets from disclosure and protect methods from subversion.

The subsystem protects itself against physical and software attacks to provide protection against attacks to the platform.

Some, but not all, subsystem capabilities must be trustworthy for the subsystem to be trustworthy. These are called the “Trusted Set” (TS). Other capabilities must work properly if the subsystem is to work properly, but they do not affect the level of trust in a Subsystem. These are called the “Trusted platform Support Set” (TSS).

The Trusted Set of capabilities can be partitioned into measurement capabilities, reporting capabilities, and storage capabilities. The trusted measurement capabilities are called the

"Root of Trust for Measurement" (RTM). The trusted reporting capabilities are called the "Root of Trust for Reporting" (RTR). The trusted storage capabilities are called the "Root of Trust for Storage" (RTS). The RTM makes reliable measurements about the platform and puts the measurement results into the RTR. The RTR prevents unauthorized changes to the measurement results, and reliably reports those measurement results. The RTS provides methods to minimize the amount of trusted storage that is required. The "Root of Trust for Measurement" and the "Root of Trust for Reporting" cooperate to permit 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 to be expected if the platform is operating as expected. If there is sufficient match between the measurement results and the expected values, the entity can trust computations within the platform (not just within the TS) to execute as expected.

The RTR have a cryptographic identity in order to prove to a remote entity that RTR messages come from genuine trusted capabilities, and not from bogus trusted capabilities.

The TCG subsystem is a trusted subsystem that is an integral part of a computing platform. The evaluated components that make up the TCG subsystem are called the Trusted Building Blocks (TBB). The TBB provide useful trust and security capabilities, while minimizing the number of functions that must be trusted. The TBB consists of logical components including the Trusted Platform Module (TPM), the Connection module (PCCON) and the Trusted Platform Support Services (TSS). In general the TPM contains all trusted capabilities except for the RTM, so a TPM is common to all types of trusted platforms. The TPM uses cryptographic techniques to reliably report its identity and the measurement results. Since this raises privacy issues, the Subsystem includes features that provide privacy controls to the Owner. The PCCON provides the connection to the computing platform and the Root of Management Trust (RMT). The TSS is a set of functions and data that are common to all types of platforms, which are not required to be trustworthy.

The TPM is a collection of hardware, firmware and/or software that among others support the following security features:

- Algorithms: RSA, SHA-1, HMAC
- Random number generation
- Key generation
- Self Tests

The TPM may be used to provide secure storage for an unlimited number of private keys or other data by using RSA key technology to encrypt data and keys. The resulting encrypted file, which contains header information in addition to the data or key, is called a blob and is output by the TPM and can be loaded in the TPM when needed. The functionality of the TPM can also be used so that private keys generated on the TPM can be stored outside the TPM (encrypted) in a way that allows the TPM to use them later without ever exposing such keys in the clear outside the TPM.

The functionality used to provide secure storage is:

- Seal and Unseal, which perform RSA encrypt and decrypt, respectively, on data that is externally generated. The sealing operation encrypts not only the data, but also the platform configuration values that are stored in the platform configuration registers (PCRs) in the TPM and tpmProof, which is a unique identifier for that TPM. To unseal the data, three conditions must exist: 1) the appropriate key must be available for unseal, 2) the TPM PCRs must contain the same values that existed at the time of the seal operation, and 3) the value of tpmProof must be the same as that encrypted during the seal operation. By requiring the PCR values to be duplicated at unseal and the tpmProof value to be checked, the seal operation allows software to explicitly state the future "trusted" configuration that the platform must be in for the decrypted key to be used and for decrypt to only occur on the specified TPM.
- Unbind, which RSA decrypts a blob created outside the TPM that has been encrypted using a public key where the associated private key is stored in the TPM.

A number of key types are defined within the TPM. Keys may be migratable or non-migratable. A migratable key is a key that may be transported outside the specific TPM. A non-migratable key is a key that cannot be transported outside a specific TPM. Key types include:

- The Storage Root key (SRK), which is the root key of a hierarchy of keys associated with a TPM; it is generated within a TPM and is a non-migratable key. Each TPM contains a SRK, generated by the TPM at the request of the Owner. Under that SRK are two trees: one dealing with migratable data and the other dealing with non-migratable data
- Signing Keys, which must be a leaf of the Storage Root Key hierarchy. The private key of the key pair is used for signing operations only.
- Storage keys, which are used for RSA encrypt and RSA decrypt of other keys in the Protected Storage hierarchy only.
- Identity Keys, which are used for operations that require a TPM identity, only.
- Binding Keys, which are used for TPM_Unbind operations only. A bind operation (performed outside the TPM) associates identification and authentication data with a particular data set and the entire data blob is encrypted outside the TPM using a binding key, which is an RSA key. The TPM_Unbind operation uses a private key stored in the TPM to decrypt the blob so that the data (often a key pair) stored in the blob may be used.
- The Endorsement key pair, which is an asymmetric key pair generated by or inserted in a TPM that is used as proof that a TPM is a genuine TPM.

Each TPM is identified and validated by its Endorsement Key. A TPM has only one endorsement key pair. The Endorsement Key is transitively bound to the Platform via the TPM as follows:

1. An Endorsement Key is bound to one and only one TPM (i.e., there is a one to one correspondence between an Endorsement Key and a TPM.)
2. A TPM is bound to one and only one Platform, (i.e., there is a one to one correspondence between a TPM and a Platform.)
3. Therefore, an Endorsement Key is bound to a Platform, (i.e., there is a one to one correspondence between an Endorsement Key and a Platform.

TPM algorithms, protocols, identification and authentication, and access control functions are described in the subsections below.

2.1.1 Algorithms

The TPM supports the RSA algorithm and must use the RSA algorithm for encryption and digital signatures. The TPM supports RSA key sizes of 512, 1024, and 2048 bits. The RSA public exponent must be e, where e = 2^{16}+1. TPM devices that use the Chinese Remainder Theorem (CRT) as the RSA implementation must provide protection and detection of failures during the CRT process to avoid attacks on the private key. All TPM Storage keys are of strength equivalent to a 2048 bit RSA key. The TPM does not load a Storage key whose strength is less than that of a 2048 bit RSA key. All TPM identity keys are of strength equivalent to a 2048 bit RSA key or greater.

The TPM supports the Secure Hash Algorithm (SHA)-1 hash algorithm as defined by United States Federal Information Processing Standard 180-1. The output of SHA-1 is 160 bits and all areas that expect a hash value are required to support the full 160 bits. A SHA-1 digest is used in the early stages of a boot process, before more sophisticated computing resources are available. Secure Hash is also used in the process of preparing data for signature or signature verification.

The TPM uses the RSA algorithm for signature and verification operations. The TPM must use PKCS #1 V2 for the format and design of the signature output.

2.1.2 Random Number Generator (RNG)

The RNG capability is only accessible to valid TPM commands. Intermediate results from the RNG are not available to any user. When the data is for internal use by the TPM (e.g., asymmetric key generation) the data is held in a shielded location and is not accessible to any user.

2.1.3 Key Generation

The TPM generates asymmetric key pairs. The generate function is a protected capability and the private key is held in a shielded location.

The TPM generates the HMAC key by taking the next *n* bits from the TPM RNG.

The creation of all nonce values uses the next *n* bits from the TPM RNG.

2.1.4 Self Tests

The TPM provides start-up self-tests and a mechanism to allow the self-tests to be run on demand. The response from the self-tests is pass or fail. Self-tests include checks of the following:

- RNG functionality, as defined by United Stated Federal Information Processing Standard 140-2.
- Reading and extending the integrity registers. The self-test for the integrity registers will leave the integrity registers in a known state.
- Endorsement key pair integrity, if the key pair exists. This test will verify that the Endorsement key pair can sign and verify a known value. This test will also test the RSA sign and verify engine. If the Endorsement key has not yet been generated, the TPM action is manufacturer specific.
- Integrity of the protected capabilities of the TPM. This consists of checks that ensure that the TPM “microcode” or equivalent has not changed.
- Any tamper-resistance markers. The tests on the tamper-resistance or tamper-evident markers are under programmable control. There is no requirement to check tamper-evident tape or the status of epoxy surrounding the case.
- When the TPM detects a failure during any self-test, the part experiencing the failure will enter a shutdown mode and an error code is returned.

2.1.5 Identification and Authentication

The TPM identification and authentication capability is used to authenticate an entity owner and to authorize use of an entity. The basic premise is to prove knowledge of a shared secret. This shared secret is the identification and authentication data. The TCG Specification calls the identification and authentication process and this data authorization.

The identification and authentication data for the TPM Owner and the owner of the Storage Root Key are held within the TPM itself. The identification and authentication data for other owners of entities are held and protected with the entity.

The identification and authentication protocols use a random nonce. This requires that a nonce from one side be in use only for a message and its reply. For instance, the TPM would create a nonce and send that on a reply. The requestor would receive that nonce and then include it in the next request. The TPM would validate that the correct nonce was in the request and then create a new nonce for the reply. This mechanism is in place to prevent replay attacks and man-in-the-middle attacks.

2.1.6 Access Control

Access control is enforced in the TPM on all data and operations performed on that data. The TPM provides access control by denying access to some data and operations and

allowing access to other data and operations based on the value of the TCG_AUTH_DATA_USAGE flag TCG_KEY_FLAGS and the TCG_KEY_USAGE flag. The TCG_AUTH_DATA_USAGE flag defines access as either owner or world. Owner must be authenticated with a shared secret as described in Section 2.2.5, above. World means that usage of the key is permitted by anyone without authentication. The TCG_KEY_FLAGS define whether a key is migratable or non-migratable and whether the key is stored in volatile storage and must be unloaded at TPM start-up. The TCG_KEY_USAGE flag identifies the key type, as defined in Section 2.2 above. Depending on the key type, certain operations may or may not be allowed using the particular key, as described above.

Upon appropriate identification and authentication associated with the keys, users can use the key for the purposes permitted by the TCG_KEY_USAGE flag.

2.2 Security Attributes and Data

All data, including user key pairs, user data, and TSF data, have associated security attributes, stored as flags in the TPM or associated with the data in an encrypted blob. The following security attributes are defined:

- Migration attribute, which determines if the data (or key pair) can migrate from one TPM to another. This security attribute is stored in TCG_KEY_FLAGS.
- TCG_AUTHDATA_USAGE flag is used to define whether the data can be access only by the owner or by the world.
- Attribute key type, stored in TCG_ KEY_USAGE, which indicates if the data is a key or key pair and the type of key (e.g., storage, binding, etc., as defined in section 2.2, above).
- Volatility attribute, which defines whether the data must be stored in volatile or non-volatile storage and if it is cleared at TPM start-up. This security attribute is stored in TCG_KEY_FLAGS.

Within the TPM, for the purposes of Common Criteria evaluation, TSF data is defined as:

- The Endorsement Key Pair,
- The Storage Root Key (SRK),
- TPMProof, i.e., the random number (nonce) that each TPM maintains to validate that the data originated at this TPM.
- PCR values,
- TPM owner identification and authentication data,
- Entity owner identification and authentication data,
- Migration authorization data, which is used in creating migratable key blobs,
- Security attributes as defined above.

User data is defined as all user keys and other data that may be passed to the TPM for signature, decryption, etc.

2.3 TOE overview

The Target of Evaluation (TOE), the PC8375T with HW A4 and FW SK4.11, is based on National Semiconductor's SafeKeeper™ technology, which provides TCG-compliant security functionality.

The PC8375T is a single-chip device, comprising a Trusted Platform Module (TPM) for PC security based on the TCG standard, a "Super I/O" module, and additional system functions, all together representing the physical scope of the TOE. The Super I/O and system functions can be rated not security-relevant and therefore will be excluded from this evaluation. Detailed information can be found in the high-level design.

The PC8375T TPM module complies with TCG specifications (main specification V1.1b [TCG] and PC specific specification V1.0 [TCG_PC]).

The PC8375T TPM module provides desktop PC platforms with:

- System integrity checks: Enables checking of the TOE integrity;
- Authentication: Provides assurance that the source of the data is valid and as expected;
- Data integrity checks: Provides assurance that received data is exactly as sent;
- Secure storage: supplies shielded location and protected storage mechanism to protect sensitive and confidential data, such as credit card numbers, passwords and keys.
- Additional proprietary functions

The **firmware part of the TOE** provides an API set that matches the TCG specification [TCG], at which the API represents the logical scope of the TOE. TCG capabilities that must be trustworthy can be accessed only through the authentication mechanism or by supplying physical presence proof.

The TOE also supplies an area for secure storage. The shielded locations are accessible only for protected functions (it is stated in [TCG] at the beginning of each command definition if a command is a protected function/capability). The following data is stored in shielded locations:

- The private keys of the Endorsement-Key and Store-Root-Key remain in shielded location and never leave the TPM;

- Platform secrets;
- TPM Owner secret;
- Imported protected data (e.g. keys) is stored only in a shielded location;
- Platform Configuration Registers (PCRs) and Data Integrity Registers (DIRs).

The TOE TPM module supplies the following cryptographic services for the user:

- Hardware True-Random generator to generate random numbers also for entities outside of the TPM. Keys generation: generation of 2048, 1024 and 512-bit asymmetric key pairs.
- Performing RSA encryption and decryption on externally generated data using keys stored in the shielded location.
- Digital signature using the RSA algorithm.
- Integrity metrics.
- SHA1 hashing.

The PC8375T can be used in a wide field of applications, e.g. in a remote access network to authenticate platforms to a server and vice versa. Concerning e-commerce transactions, contracts can be signed with digital signatures using the PC8375T asymmetric encryption functionality. Regarding a network scenario, the client PCs equipped with an PC8375T are able to report their platform status to the server so that the network administration is aware of the their trustworthiness. In conclusion, the PC8375T acting as a service provider to a system helps to make transactions more secure and trustworthy.

(Hardware interface): The device interfaces with the host though the LPC interface.

(Software interface): The device SW interface is the TCG 1.1 command API.

(Guidance documentation): The guidance documentation consists of

- The device datasheet [Datasheet], which details the specific vendor software commands and the drivers protocols

- The AGD document used during this evaluation [AGD], which details all the aspects relevant for the user and administrator of the TOE.

- The PC8375T Initialization and Configuration application note [Init].

- The TCG main specification [TCG], which details all the standard TCG commands, and the protocols for device initialisation, starting from endorsement key-pair generation.

The guidance documents [Datasheet], [AGD] and [Init] are delivered to the customer by NSC, whereas the TCG main specification [TCG] is publicly available.

(Forms of delivery): The PC8375T is delivered as a complete unit, with the firmware already programmed in the chip non-volatile memory.

3 TOE Security Environment

3.1 Secure Usage Assumptions

TOE secure usage assumptions are defined in Table 3.1, below.

Table 3.1 – Secure Usage Assumptions

#	Assumption	Description
1	A.Configuration	The TOE will be properly installed and configured.

Table 3.2 lists the Secure Usage Assumptions for the IT environment.

Table 3.2 – Assumptions for the IT Environment

#	Assumption Name	Description
1	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.

3.2 Organizational Security Policies

There are no organizational security policies defined.

3.3 Threats to Security

Threats to the TOE are defined in Table 3.3, below. The asset under attack is the information transiting the TOE. In general, the threat agent includes, but is not limited to: 1) people with TOE access who are expected to possess “average” expertise, few resources, and moderate motivation, or 2) failure of the TOE.

Table 3.3 – Threats

#	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.

#	Threat	Description
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.
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.

4 Security Objectives

4.1 Security Objectives for the TOE

TOE security objectives are defined in Table 4.1, below.

Table 4.1 – Security Objectives for the TOE

#	Objective	Description
1	O.Crypto_Key_Man	The TOE shall generate and destroy cryptographic keys in a secure manner.
2	O.Crypto_Op	The TOE shall perform cryptographic operations, including secure hash, HMAC, RSA digital signature and signature verification, RSA encryption and decryption, and RSA key generation in accordance with specified algorithms and key size; key size must be sufficient size to protect private/public key pairs from deciphering.
3	O.Crypto_Self_Test	The TOE shall provide the ability to verify that the cryptographic functions operate as designed.
4	O.DAC	The TOE shall control and restrict user access to the TOE assets in accordance with a specified access control policy.
5	O.Export	When data are exported outside the TPM, the TOE shall ensure that the data security attributes being exported are unambiguously associated with the data.
6	O.Fail_Secure	The TOE shall preserve the secure state of the system in the event of a cryptographic or other failure.
7	O.General_Integ_Checks	The TOE shall provide periodic checks on system integrity and user data integrity.
8	O.HMAC	The TOE shall provide the ability to detect the modification of security attributes and other data.
9	O.I&A	The TOE shall uniquely identify all users, and shall authenticate the claimed identify before granting a user access to the TOE facilities.
10	O.Import	When data are being imported into the TOE, the TOE shall ensure that the data security attributes are being imported with the data and the data is from authorized source. In addition, the TOE shall verify those security attributes according to the TSF access control rules.
11	O.Invoke	The TSF shall be invoked for all actions.
12	O.Limit_Actions_Auth	The TOE shall restrict the actions a user may perform before the TOE verifies the identity of the user.
13	O.MessageNR	The TOE shall provide user data integrity, source authentication, and the basis for source non-repudiation when exchanging data with a remote system.

#	Objective	Description
14	O.No_Residual_Info	The TOE shall ensure there is no “object reuse,” i.e., ensure that there is no residual information in information containers or system resources upon their reallocation to different users.
15	O.Object_Attr_Default	The TOE shall require default security attributes for the object when the object is created.
16	O.Object_Attr_DefaultOver	The TOE shall permit authorised users to override defaulted values for security attributes for an object.
17	O.Obj_Attr_SecureValues	The TOE shall maintain object security attributes by permitting only secure values.
18	O.Security_Attr_Mgt	The TOE shall allow only authorised users to initialise and change object security attributes.
19	O.Security_Roles	The TOE shall maintain security-relevant roles and association of users with those roles.
20	O.Self_Protect	The TSF will maintain a domain for its own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure.
21	O.Single_Auth	The TOE shall provide a single use authentication mechanism and require re-authentication to prevent “replay” and “man-in-the-middle” attacks.
22	O.Tamper_ID	The TOE shall provide features that permit a human to detect physical tampering of a system component.

4.2 Security Objectives for the Environment

Table 4.2 lists security objectives for the environment.

Table 4.2 – Security Objectives for the Environment

#	Objective Name	Objective Description
1	OE.Configuration	The TOE shall be installed and configured properly for starting up the TOE in a secure state.
2	OE.PhysSecurity	The environment shall provide an acceptable level of physical security so that the TPM cannot be tampered with or be subject to side channel attacks such as the various forms of power analysis and timing analysis.

5 IT Security Requirements

5.1 Introduction

This section defines the TOE security functional requirements and assurance requirements. All requirements are from the CC Parts 2 and 3. Selections, assignments, and refinements performed in the [PP] yet are indicated by *italics*; unperformed operations from the [PP] and refinements which are performed within this ST first are indicated by *underlined italics*.

5.2 TOE Security Functional Requirements

This section defines the TOE security functional requirements. A list of the requirements is provided in Table 5.1. The full text of the security functional requirements is contained below. Certain security functional requirements have multiple iterations in the text. Iterations are indicated by the use of a ":" in the component identification and by a ";" in the component name. All assignments and selections of the security functional requirements not done in the [PP] yet (FDP_ACF.1.3, FDP_ACF.1.4, FDP_ETC.2.4, FDP_ITC.2.5 and FMT_MOF.1.1) are performed here as well. Furthermore in addition to [PP] one refinement is supplemented for the functional requirement FCS_CKM.4 as defined in the text below. Moreover the security functional requirement FMT_SMF.1 is added here according to CC final interpretation 065.

Table 5.1 – TOE Security Functional Requirements

#	Functional Requirement	Title
1	FCO_NRO.2	Enforced proof of origin
2	FCS_CKM.1	Cryptographic key generation
3	FCS_CKM.4	Cryptographic key destruction
4	FCS_COP.1	Cryptographic operation
5	FDP_ACC.1	Subset access control
6	FDP_ACF.1	Security attribute based access control
7	FDP_ETC.2	Export of user data with security attributes
8	FDP_ITC.2	Import of user data with security attributes
9	FDP_RIP.2	Full residual information protection
10	FIA_ATD.1	User attribute definition
11	FIA_UAU.1	Timing of authentication
12	FIA_UAU.4	Single-use authentication mechanism
13	FIA_UAU.6	Re-authenticating
14	FIA_UID.1	Timing of identification
15	FMT_MOF.1	Management of security functions behaviour
16	FMT_MSA.1	Management of security attributes

#	Functional Requirement	Title
17	FMT_MSA.2	Secure security attributes
18	FMT_MSA.3	Static attribute initialisation
19	FMT_MTD.1	Management of TSF data
20	FMT_SMF.1	Specification of management functions
21	FMT_SMR.2	Restrictions on security roles
22	FPT_AMT.1	Abstract machine testing
23	FPT_FLS.1	Failure with preservation of secure state
24	FPT_PHP.1	Passive detection of physical attack
25	FPT_RCV.4	Function recovery
26	FPT_RPL.1	Replay detection
27	FPT_RVM.1	Non-bypassability of the TSP
28	FPT_SEP.1	TSF domain separation
29	FPT_TDC.1	Inter-TSF basic TSF data consistency
30	FPT_TST.1	TSF testing
31	FTP_TRP.1	Trusted path

5.2.1 Class FCO – Communication

FCO_NRO.2 Enforced proof of origin

Hierarchical to: FCO_NRO.1

FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted *TPM data signed using identity keys* at all times.

FCO_NRO.2.2 The TSF shall be able to relate the *identity* of the originator of the information, and the *TPM data* of the information to which the evidence applies.

FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to *recipient* given *evidence only available when requestor properly authenticates*.

Dependencies: FIA_UID.1 Timing of identification

5.2.2 Class FCS – Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA* and specified cryptographic key sizes *RSA 512, 1024, 2048* that meet the following: *PKCS#1 V2*.
Dependencies:	FCS_COP.1 Cryptographic operation, FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *erasure of memory areas containing cryptographic keys* that meets the following: *FIPS 140-2, Section 4.7.6, Key Zeroization*.
Dependencies:	FCS_CKM.1 Cryptographic key generation, FMT_MSA.2 Secure security attributes

FCS_COP.1:1 Cryptographic operation; RSA encrypt and decrypt

Hierarchical to: No other components.

FCS_COP.1.1;1	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *RSA* and cryptographic key sizes *RSA 512, 1024, 2048* that meet the following: *PKCS#1 V2*.

FCS_COP.1:2 Cryptographic operation; RSA signature and signature verification

Hierarchical to: No other components.

FCS_COP.1.1;2	The TSF shall perform *signature generation and signature verification* in accordance with a specified cryptographic algorithm *RSA* and cryptographic key sizes *RSA 512, 1024, 2048* that meet the following: *PKCS#1 V2*.

FCS_COP.1:3 Cryptographic operation; SHA

Hierarchical to: No other components.

FCS_COP.1.1; 3	The TSF shall perform *secure hash* in accordance with a specified cryptographic algorithm *SHA-1* and cryptographic key sizes *not applicable* that meet the following: *FIPS 180-1*.

FCS_COP.1:4 Cryptographic operation; Keyed-Hashing for Message Authentication

Hierarchical to: No other components.

FCS_COP.1.1; 4 The TSF shall perform *keyed-hashing message authentication code (HMAC)* in accordance with a specified cryptographic algorithm *SHA-1* and cryptographic key sizes *160 bits* that meet the following: *RFC 2104*.

Dependencies: FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes

5.2.3 Class FDP – User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the *Protected Operations Access Controls* on

a) Subjects: commands executing on behalf of users.
b) Objects: keys and user data.
c) Operations: signature generation, encryption, or decryption;

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 *Protected Operations Access Controls* to objects based on *security attributes TCG_AUTH_DATA_USAGE, TCG_KEY_FLAGS and TCG_KEY_USAGE*.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) Key and data access is defined as "owner" access or "world" based on the value of TCG_AUTH_DATA_USAGE

b) Cryptographic operations for each key are limited based on the specification of the TCG_KEY_USAGE value.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on: *none*.

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

FDP_ETC.2 Export of user data with security attributes

Hierarchical to: No other components

FDP_ETC.2.1 The TSF shall enforce the *Protected Operations Access Controls* when exporting user data, controlled under the SFP, outside of the TSC.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC: *A key may be encrypted for migration only if the migratable flag is set in TCG_KEY_FLAGS, none*.

Application note: *Security attributes are encrypted in a blob prior to export. As part of the blob that has been encrypted, the security attributes are unambiguously associated with the data.*

Dependencies: FDP_ACC.1 Subset access control

FDP_ITC.2 Import of user data with security attributes

Hierarchical to: No other components

FDP_ITC.2.1 The TSF shall enforce the *Protected Operations Access Controls* when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: *none*.

Application note: *Security attributes are imported with data as part of the encrypted blob. As part of the blob that has been encrypted, the security attributes are unambiguously associated with the data.*

Dependencies: FDP_ACC.1 Subset access control, FTP_TRP.1 Trusted path, FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_RIP.2 Full residual information protection

Hierarchical to: FDP_RIP.1

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *de-allocation of the resource from* all objects.

Dependencies: None.

5.2.4 Class FIA – Identification and Authentication

Application Note: The TPM identification and authentication capability is used to authenticate an entity owner and to authorize use of an entity. The basic premise is to prove knowledge of a shared secret. This shared secret is the identification and authentication data. Note that the *TCG* Main Specification document refers to the identification and authentication process and this data as *authorization*.

FIA_ATD.1 User attribute definition

Hierarchical to: No other components

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: *authentication data, role.*

Dependencies: None

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components

FIA_UAU.1.1 The TSF shall allow *access to data and keys where entity owner has given the "world" access based on the value of TCG_AUTH_DATA_USAGE; access to the following commands: TPM_SelfTestFull, TPM_ContinueSelfTest, TPM_GetTestResult, TPM_PcrRead, TPM_DirRead, and TPM_EvictKey* 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

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to *the use of the "Object-Independent Authorization Protocol" (OI-AP) and the "Object-Specific Authorization Protocol" (OS-AP) protocols.*

Dependencies: None.

FIA_UAU.6 Re authenticating

Hierarchical to: No other components

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions: *for every command that requires user authentication*.

Dependencies: None.

FIA_UID.1 Timing of identification

Hierarchical to: No other components

FIA_UID.1.1 The TSF shall allow *access to data and keys where entity owner has given the "world" access based on the value of TCG_AUTH_DATA_USAGE; access to the following commands: TPM_SelfTestFull, TPM_ContinueSelfTest, TPM_GetTestResult, TPM_PcrRead, TPM_DirRead, and TPM_EvictKey* 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.

5.2.5 Class 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

TPM_DisablePubekRead (prevent any entity from reading the PUBEK),

TPM_OwnerSetDisable (enable/disable a TPM),

TPM_DisableOwnerClear (disable the TPM_OwnerClear function)

to *the TPM owner*.

Dependencies: FMT_SMR.1 Security roles, FMT_SMF.1 Specification of management functions (added here according to CC final interpretation 065)

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components

FMT_MSA.1.1 The TSF shall enforce the *Protected Operations Access Controls* to restrict the ability to *create* the security attributes *associated with a particular entity, including TCG_KEY_USAGE, TCG_AUTH_DATA_USAGE, migratable flag, and volatility flag* to *the entity owner.*

Dependencies: FMT_SMR.1 Security roles, FDP_ACC.1 Subset access control, FMT_SMF.1 Specification of management functions (added here according to CC final interpretation 065)

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model, FMT_SMR.1 Security roles, FDP_ACC.1 Subset access control, FMT_MSA.1 Management of security attributes

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components

FMT_MSA.3.1 The TSF shall enforce the *Protected Operations Access Controls* to provide *specific* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *entity owner* to specify alternative initial values to override the default values when an object or information is created.

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

FMT_MTD.1:1 Management of TSF data – TPM Owner modify

Hierarchical to: No other components

FMT_MTD.1.1;1 The TSF shall restrict the ability to *modify* the *TSF data: Identification and authentication data associated with the Endorsement Key and SRK; Migration authorization data* to *the TPM Owner*.

FMT_MTD.1:2 Management of TSF data – TPM Owner create

Hierarchical to: No other components

FMT_MTD.1.1;2 The TSF shall restrict the ability to *generate* the *TSF data: Storage Root Key and TPMProof* to *the TPM Owner*.

FMT_MTD.1:3 Management of TSF data – Entity Owner

Hierarchical to: No other components

FMT_MTD.1.1;3 The TSF shall restrict the ability to *modify* the *TSF data: Identification and Authentication data associated with entity;* to the *entity Owner*.

FMT_MTD.1:4 Management of TSF data – Manufacturer

Hierarchical to: No other components

FMT_MTD.1.1;4 The TSF shall restrict the ability to *generate* the *TSF* data: *Endorsement Key Pair* to the *TPM manufacturer or designee*.

Dependencies: FMT_SMR.1 Security roles, FMT_SMF.1 Specification of management functions (added here according to CC final interpretation 065)

FMT_SMF.1 Specification of management functions (added here according to CC final interpretation 065)

Hierarchical to: No other components

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: *Disabling/enabling of security functions behavior, Creation of POAC security attributes, Modification and generation of TSF data.*

Dependencies: No Dependencies

FMT_SMR.2 Restrictions on security roles

Hierarchical to: FMT_SMR.1

FMT_SMR.2.1 The TSF shall maintain the roles: *TPM owner, owners of entities, and TPM manufacturer or designee*.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the condition: *successful presentation of correct authentication data* is satisfied.

Dependencies: FIA_UID.1 Timing of identification.

5.2.6 Class FPT – Protection of the TOE Security Functions

FPT_AMT.1 Abstract machine testing

Hierarchical to: No other components

FPT_AMT.1.1	The TSF shall run a suite of tests *during initial start-up and at the request of an authorised user* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.
Dependencies:	None.
Application note:	*The term "authorised user" in FPT_AMT.1 should be interpreted as any user. Authentication is NOT required for a user to run tests.*

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: *failure of any crypto operations including RSA encryption, RSA decryption, SHA, RNG, RSA signature generation, HMAC generation; failure of any commands or internal operations*.
Dependencies:	ADV_SPM.1 Informal TOE security policy model

FPT_PHP.1 Passive detection of physical attack

Hierarchical to: No other components

FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
Dependencies:	FMT_MOF.1 Management of security functions behavior

FPT_RCV.4 Function recovery

Hierarchical to: No other components

FPT_RCV.4.1	The TSF shall ensure that *all TPM Commands* 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_RPL.1 Replay detection

Hierarchical to: No other components.

FPT_RPL.1.1	The TSF shall detect replay for the following entities: *command requests that include the nonce parameter.*
FPT_RPL.1.2	The TSF shall perform *destroy session* when replay is detected.
Dependencies:	None.

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components

FPT_RVM.1.1	The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
Dependencies:	None.

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:	None.

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 *TPM commands and responses* when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use *the TCG Main Specification* when interpreting the TSF data from another trusted IT product.
Dependencies:	None.

FPT_TST.1 TSF testing

Hierarchical to: No other components

FPT_TST.1.1	The TSF shall run a suite of self tests *during initial start-up and periodically during normal operation, at the request of the authorized user, and at the condition: prior to execution of the first call to a capability that uses those functions* to demonstrate the correct operation of the TSF.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.
Application note:	*The term "authorised user" in FPT_TST.1 should be interpreted as a user. Authentication is NOT required for a user to run self tests or to verify correct system operation based on self tests.*
Application Note:	*The self-test capabilities are designed to enable the creation of a TCG platform with minimum latency due to TPM self-test. It might be possible to avoid wasting time, waiting for a TPM to do self-test, by designing a platform where TPM self-testing is done in parallel with other system functions, at a time when TPM capabilities are not required.* *Tests will include: at start-up, a TPM automatically tests just those internal functions that are used by critical TPM capabilities. This permits the use of those critical TPM capabilities as soon as possible after start-up. Remaining TPM capabilities use additional internal functions that must be tested before the remaining TPM capabilities can execute. A test of the additional functions can be explicitly called. Alternatively, those functions will automatically be tested prior to execution of the first call to a capability that uses those functions. At any time, other self-test commands will explicitly cause the TPM to do a full self-test.* *TPM_SelfTestFull causes the TPM to do a full self-test.* *TPM_ContinueSelfTest causes the TPM to test the TPM internal functions that were not tested at start-up. TPM_ContinueSelfTest is unusual, in that it returns a result code to the caller before execution of the command and does not return a result code to the caller after execution of the command. If the functions used by a capability have not been tested, TPM_ContinueSelfTest is executed automatically after that capability is called and before it is executed. It is anticipated that the caller or TPM driver software is preprogrammed with knowledge of the time that the TPM will require to complete TPM_ContinueSelfTest. It is anticipated that a call to a TPM that is executing TPM_ContinueSelfTest would result in a "busy" indication.*

The tests themselves only return a TCG_SUCCESS or TCG_FAIL answer. TPM_GetTestResult must be used to discover why self-test failed. Upon the failure of a self-test the TPM goes into failure mode and does not allow most other operations to continue. [These self-tests] demonstrate the correct operation of the TSF.

Dependencies: FPT_AMT.1 Abstract machine testing

5.2.7 Class FTP – Trusted Path/Channels

FTP_TRP.1 Trusted path

Hierarchical to: No other components

FTP_TRP.1.1	The TSF shall provide a communication path between itself and *local or remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2	The TSF shall permit *the TSF, local or remote users* to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the user of the trusted path for *initial user authentication, for all TPM commands, all user commands, and TSF responses.*

Dependencies: None

5.2.8 Strength of Function Requirement

The threat level for the TOE authentication function is assumed to be SOF-basic. The strength of cryptographic algorithms is outside the scope of the CC. Strength of function only applies to non-cryptographic, probabilistic or permutational mechanisms. The SOF requirement applies to the identification and authentication functionality within the TOE.

5.3 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 3 (EAL3) augmented by ADV_SPM.1 and ALC_FLR.1. They are all drawn from Part 3 of the Common Criteria. The assurance components are listed in Table 5.2. EAL 3 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 requirements FMT_MSA.2. ALC_FLR.1 was added to provide basic flaw remediation. Moreover in addition to [PP] two refinements are

supplemented for the assurance requirements AGD_ADM.1 and AGD_USR.1 as defined in the text below.

Table 5.2 - 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)
AGD_ADM.1	Administrator guidance (refined)
AGD_USR.1	User guidance (refined)
ALC_DVS.1	Identification of security measures
ALC_FLR.1	Basic flaw remediation (augmentation)
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

5.3.1 Class ACM: Configuration Management

ACM_CAP.3 Authorisation controls

Dependencies: ALC_DVS.1 Identification of security measures

Developer action elements:

ACM_CAP.3.1D The developer shall provide a reference for the TOE.

ACM_CAP.3.2D The developer shall use a CM system.

ACM_CAP.3.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The TOE shall be labeled with its reference.

ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.

ACM_CAP.3.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.3.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.3.7C The CM plan shall describe how the CM system is used.

ACM_CAP.3.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

Evaluator action elements:

ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.1 TOE CM Coverage

Dependencies: ACM_CAP.3 Authorisation controls

Developer action elements:

The following element is changed as a result of Interpretation 004.

ACM_SCP.1.1D The developer shall provide a list of configuration items for the TOE..

Content and presentation of evidence elements:

The Content and presentation of evidence elements are replaced as a result of Interpretations 004 and 038.

ACM_SCP.1.1C The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.

Evaluator action elements:

ACM_SCP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Class ADO: Delivery and Operation

ADO_DEL.1 Delivery Procedures

Dependencies: No dependencies.

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, Generation, and Start-up Procedures

Dependencies: AGD_ADM.1 Administrator guidance

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Class ADV: Development

ADV_FSP.1 Informal functional specification

Dependencies: ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.2 Security enforcing high-level design

Dependencies: ADV_FSP.1 Informal functional specification, ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action elements:

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal correspondence demonstration

Dependencies: No dependencies.

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more

abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_SPM.1 Informal TOE security policy model

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Class AGD: Guidance Documents

AGD_USR.1 User guidance

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_USR.1.1D	The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C	The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2C	The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3C	The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C	The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5C	The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6C	The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinement regarding User Guidance (AGD_USR.1)

Introduction

The Common Criteria assurance components of the families AGD_USR (user guidance) and AGD_ADM (administrator guidance) “describe all relevant aspects for the secure application of the TOE.“ The terms “user” and “administrator” are used.

In the case of a TPM the meaning of the terms “user” and “administrator” are not obvious. Therefore, the following refinements are given regarding guidance.

User guidance refers to material that is intended to be used by non-administrative human users of the TOE, and by others (e.g. programmers) using the TOE’s external interfaces. User guidance describes the security functions provided by the TSF and provides instructions and guidelines, including warnings, for its secure use.

Refinement

The TOE can only be used via the application software. Therefore, the "user" of the TOE (as used in the Common Criteria assurance class AGD: guidance) is the application software developer.
Guidance document (refers to the Common Criteria assurance component of the family AGD_USR) must be given to the developer of the application software to ensure that the application software properly uses the TOE.

The guidance documents should provide only the information that is necessary for using the TOE. Depending on the recipient of that guidance documentation User and Administrator Guidance can be given in the same document.

AGD_ADM.1 Administrator guidance

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinement regarding Administrator Guidance (AGD_ADM.1)

Introduction

Administrator guidance refers to written material that is intended to be used by those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security.

Refinement

The TOE provides security functions which can or need to be administrated by the entity who handles the TOE before it is delivered to the PC users. This entity is a PC manufacturer and his responsibilities are to configure the TOE and to create the endorsement key.
Guidance document (refers to the Common Criteria assurance component of the family AGD_ADM) must be given to the PC manufacturer to ensure that it properly handles the TOE.
.

Guidance documents must not contain security relevant details which are not absolutely necessary for the administration actually to be done. Depending on the recipient of that guidance documentation User and Administrator Guidance can be given in the same document.

5.3.5 Class ALC: Life Cycle Support

ALC_DVS.1 Identification of security measures

Dependencies:	No dependencies.

Developer action elements:

ALC_DVS.1.1D	The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C	The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2C	The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_FLR.1 Basic flaw remediation

Dependencies: No dependencies.

Developer action elements:

The following element is changed as a result of Interpretation 094.

ALC_FLR.1.1D The developer shall provide the flaw remediation procedures addressed to TOE developers.

Content and presentation of evidence elements:

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

Evaluator action elements:

ALC_FLR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6 Class ATE: Tests

ATE_COV.2 Analysis of coverage

Dependencies: ADV_FSP.1 Informal functional specification, ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.1 Testing: high-level design

Dependencies: ADV_HLD.1 Descriptive high-level design, ATE_FUN.1 Functional testing

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements:

ATE_DPT.1.2E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Dependencies: No dependencies.

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C	The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3C	The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5C	The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent Testing - Sample

Dependencies:	ADV_FSP.1 Informal functional specification, AGD_ADM.1 Administrator guidance, AGD_USR.1 User guidance, ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D	The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C	The TOE shall be suitable for testing.
ATE_IND.2.2C	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E	The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3E	The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Class AVA: Vulnerability Assessment

AVA_MSU.1 Examination of guidance

Dependencies: ADO_IGS.1 Installation, generation, and start-up procedures, ADV_FSP.1 Informal functional specification, AGD_ADM.1 Administrator guidance, AGD_USR.1 User guidance

Developer action elements:

AVA_MSU.1.1D The developer shall provide guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.1.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

Evaluator action elements:

AVA_MSU.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.1.2E The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_SOF.1 Strength of TOE security function evaluation

Dependencies: ADV_FSP.1 Informal functional specification, ADV_HLD.1 Descriptive high-level design

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

AVA_VLA.1 Developer vulnerability analysis

Dependencies: ADV_FSP.1 Informal functional specification, ADV_HLD.1 Descriptive high-level design, AGD_ADM.1 Administrator guidance, AGD_USR.1 User guidance

Developer action elements:

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2E	The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.4 Security Requirements for the IT Environment

No security requirements for the IT environment are defined.

5.5 Security Requirements for the Non-IT Environment

No security requirements for the Non-IT environment are defined.

6 TOE Summary Specification

The TOE summary specification in the following specifies the security functionality in form of security functions as well as the assurance measures of the TOE.

6.1 TOE Security Functions

The TOE consists of seven security functions (SF), which are described more detailed in the following chapters. These security functions are:

SF1: Cryptographic Operations
SF2: Self-Test
SF3: Access Control
SF4: Hacking and physical tampering protection/detection
SF5: Key Management
SF6: Random Number Generation
SF7: Identification and Authentication

6.1.1 SF1 – Cryptographic Operations

There are three functions within the PC8375T TPM module related to cryptographic operations: RSA digital signature generation and verification, RSA encryption and decryption and the generation of hash and HMAC values.

The PC8375T TPM module supports the RSA signature generation and verification (SHA-1 is used for signature generation; data is stored DER encrypted) in accordance with the specified cryptographic algorithm RSA and cryptographic key sizes of 512, 1024 and 2048 bits as defined by PKCS#1 V2.0.

The TOE supports the RSA encryption and decryption (OAEP or PKCS V15 encoding) in accordance with the specified cryptographic algorithm RSA and cryptographic key sizes of 512, 1024 and 2048 bits as defined by PKCS#1 V2.0.

The PC8375T TPM module support the secure hash in accordance with the specified cryptographic algorithm SHA-1 that meets FIPS 180-1 and the calculation of keyed-hashing message authentication code (HMAC) in accordance with the specified cryptographic algorithm SHA-1 using a key length of 20 bytes and a block size of 64 bytes as defined by RFC 2104. The SHA-1 hash algorithm is used for checksums, tie public data to a private protected data (the public information is hashed and stored inside the private protected data), extending the PCRs, auditing and XOR encryption. The HMAC hash algorithm is used by the authorization and authentication process for proving knowledge of the authorization data and to proof that no modifications are made to the command input/output.

The covered security functional requirements are: FCS_COP.1, FPT_FLS.1 and FPT_RCV.4.

The SF1 “Cryptographic Operations” does not use probabilistic or permutational effects.

6.1.2 SF2 – Self Test

The TOE supports a suite of self tests to check and demonstrate the correct operation of the TOE security functions with regard to RNG functionality, reading and extending the integrity registers, endorsement key pair integrity, RSA sign and verify engine, hash functionality, any tamper-resistance markers and integrity of the complete TPM microcode (that includes the test of the protected capabilities). The self-tests run during initial *start-up*, at the *explicit* request of a user, and *automatically* prior to execution of the first call to a capability that uses corresponding functions. Authentication is NOT required for a user to run self-tests or to verify correct system operation based on self-tests. The response from the self-tests is pass or fail.

At *start-up*, the default is that a TPM automatically tests just those internal functions that are used by critical TPM capabilities. This permits the use of those critical TPM capabilities as soon as possible after *start-up*. Remaining TPM capabilities use additional internal functions that must be tested before the remaining TPM capabilities can execute. A test of the additional functions can be *explicitly* called. Alternatively, those functions will *automatically* be tested prior to execution of the first call to a capability that uses those functions. At any time, other self-test commands will *explicitly* cause the TPM to do a full self-test (TPM_SelfTestFull) or to test the TPM internal functions that were not tested at start-up (TPM_ContinueSelfTest).

The *start-up* self tests whose default is described in the former paragraph are configurable, i.e. the default can be changed so that all the functionality will be tested at start-up.

The following functionality is tested on start-up and explicitly:

- Hash functionality;
- Reading and extending the integrity registers. The self-test for the integrity registers will leave them in a known state.

The following additional functionality is tested on start-up, explicitly and automatically:

- RNG functionality, as defined by FIPS 140-2.
- Endorsement Key pair integrity, if the key pair exists. This test will verify that the Endorsement key pair can sign and verify a known value.
- RSA algorithm using known data.

- Integrity of the protected capabilities of the TOE. This consists of checks that ensure that the TOE “microcode” or equivalent has not changed.

When the TPM detects a failure during any self-test, the part experiencing the failure will enter a shutdown/failure mode, an error code is returned and the TPM does not allow most other operations to continue. If any error occurs during the self-test, the TOE responds as defined in [TCG] chapter 8.9 and chapter 10.8.3. The TOE may recover from a failure mode by a system reset which leads to TPM initialization.

The covered security functional requirements are: FPT_AMT.1, FPT_FLS.1, FPT_RCV.4 and FPT_TST.1.

The SF2 “Self Test” uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF “basic”.

6.1.3 SF3 – Access Control

The TOE provides the security function policy *Protected Operations Access Controls* (POAC, described in chapter 6.3) to protect the sensitive subjects, objects and operations of the PC8375T.

The TOE enforces the POAC policy on subjects (commands), objects (keys and user data) and operations (signature generation/verification, encryption or decryption). The TOE provides access control by denying access to some subjects, objects and operations and allowing access to other subjects, objects and operations based on three different security attributes, stored as flags in the TPM or associated with the data in an encrypted blob.

- The security attribute *TCG*_AUTH_DATA_USAGE defines the access to key and data. The *TCG*_AUTH_DATA_USAGE flag defines access as either “owner” or “world”. An owner must be authenticated with a shared secret as described in SF7, “world” means that usage of the key is permitted by anyone without authentication.
- The security attribute *TCG*_KEY_FLAGS defines the indication of migration and volatility of keys. It determines if the data (or key pair) can be migrated from one TPM to another, it defines whether the data (or key pair) must be stored in volatile or non-volatile storage and if the data (or key pair) is cleared at TPM start-up.
- The third security attribute called *TCG*_KEY_USAGE indicates if the data is a key or key pair and the type of key (e.g., storage, signing, binding, etc., as defined in chapter 2.1). Depending on the key type, certain cryptographic operations may or may not be allowed using the particular key, as described in chapter 2.1.

The POAC provides default values for the security attributes mentioned above. As required by FMT_MSA.3 in the [PP] these default values are defined in the following table.

Table 6.1 – Default values of security attributes

Security attribute	Key	Default value
*TCG*_KEY_FLAGS->migratable	SRK	0x00000000, see [TCG] chapter 4.12
*TCG*_KEY_USAGE	SRK	0x0011 (TPM_KEY_STORAGE), see [TCG] chapter 4.10
*TCG*_KEY_FLAGS->migratable	Identity key	0x00000000, see [TCG] chapter 4.12
*TCG*_KEY_USAGE	Identity key	0x0012 (TPM_KEY_IDENTITY), see [TCG] chapter 4.10

Access to some trustworthy TPM and NSC commands is based on:

- State locking: Configuration commands cannot be run after the device has been locked.
- Authentication mechanism or on proving physical presence on the platform.

Besides the aspects mentioned above the export and import of user data, controlled under the SFP, is also done under control of the POAC security policy. POAC enforces the export of the associated security attributes with the data and enforces the interpretation and use of the imported associated security attributes.

The covered security functional requirements are: FDP_ACC.1, FDP_ACF.1, FDP_ETC.2, FDP_ITC.2, FDP_RIP.2, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.2 and FPT_TDC.1.

The SF3 “Access Control” does not use probabilistic or permutational effects.

6.1.4 SF4 – Hacking and physical tampering protection/detection

The TOE supports the following functionality for protection against and detection of hacking and physical tampering:

- Tamper evidence: The TOE is provide in a monolithic package. Any intent to gain physical access to the TPM protected areas will result in evident damage to the TOE enclosure.

- Snooping protection/detection: The TOE is equipped with a mechanism for protection against snooping the user data or the design during operation

- Domain separation: The TOE maintains all microcode (TSF code as well as other code) in secure areas of the chip for its own execution to protect the microcode from interference and tampering by untrusted subjects. In addition, the TOE firmware maintains a total separation between the TPM non-volatile data and the non-TPM data.

The covered security functional requirements are: FPT_PHP.1, FPT_RVM.1 and FPT_SEP.1.

The SF4 “Hacking and physical tampering protection/detection” uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF “basic”.

6.1.5 SF5 – Key Management

There are three functions within the PC8375T TPM module related to key management: generation of asymmetric key pairs, key storing and key destruction.

The TOE supports the generation of asymmetric cryptographic key pairs in accordance with the specified cryptographic key generation algorithm RSA and specified cryptographic key sizes RSA 512, 1024 and 2048 bits as defined by PKCS#1 V2.0. The source of randomness is the TOE random number generator (RNG). The generate function is a protected capability and the private key is held in a shielded location.

The TOE supports the storing of cryptographic keys by storing them in a randomized location inside the shielded location.

The PC8375T TPM module supports the destruction of cryptographic keys by invalidating the keys in accordance with FIPS 140-2.

The covered security functional requirements are: FCS_CKM.1 and FCS_CKM.4.

The SF5 “Key Management” uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF “basic”.

6.1.6 SF6 – Random Number Generation

The PC8375T TPM module supports the generation of random numbers using true HW RNG module.

The true HW random number generator is based on physical probabilistic controlled effects.

The covered security functional requirement is: FCS_CKM.1.

The SF6 “Random Number Generation” uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF “basic” and functionality class P1 of [AIS31].

6.1.7 SF7 – Identification and Authentication

The TOE identification and authentication capability is used to authenticate an entity owner and to authorize use of an entity. The basic premise is to prove knowledge of a shared secret. This shared secret is the identification and authentication data. The TCG Specification [TCG] calls the identification and authentication process and this data authorization. In both cases, the protocol exchanges nonce-data so that both sides of the transaction can compute a HMAC using secrets or shared secrets and nonce-data. Each side generates the hash value and can compare to the value transmitted. Network listeners cannot directly infer the authorization data from the hashed objects sent over the network. The identification and authentication data for the TOE Owner and the owner of the Storage Root Key are held within the TOE itself. The identification and authentication data for other owners of entities are held and protected with the entity.

The PC8375T TPM module provides two protocols for authentication and identification to authenticate an entity owner and to authorize use of an entity without revealing the authorization data on the network or the connection to the TOE. The first protocol is the “*Object-Independent Authorization Protocol*” (OI-AP), which allows the exchange of nonces with a specific TPM. The second protocol is the “*Object Specific Authorization Protocol*” (OS-AP)” allowing establishment of an authentication session for a single entity. Both identification and authentication protocols use a random nonce. This requires that a nonce from one side be in use only for a message and its reply. For instance, the TOE would create a nonce and send that on a reply. The requestor would receive that nonce and then include it in the next request. The TOE would validate that the correct nonce was in the request and then create a new nonce for the reply. This mechanism is in place to prevent replay attacks and man-in-the-middle attacks.

The TOE prevents the reuse of authentication related to authorization data by using *nonces* for each message and response of all authorization protocols. The *nonce* values from the TOE use the internal RNG. A re-authentication of users is done by using the authorization protocol with a new *nonce* for each message and response.

Any operational role can access all protected commands and shielded locations only through the authentication mechanism. The access-right of commands, user data, keys and operations are defined by different security attributes as defined in chapter 6.1.3. The PC8375T TPM module allows access to data and keys with the “world” access and access

to different commands on behalf of the user to be performed before the user is authenticated/identified. In contrast to this each user has to be successfully authenticated/identified before allowing any other TSF-mediated action on behalf of that user.

Furthermore the SF7 supplies the generation and verification of evidence of origin for transmitted data signed using identity keys, by using RSA algorithm for the signature operation at all times.

The covered security functional requirements are: FCO_NRO.2, FIA_ATD.1, FIA_UAU.1 FIA_UAU.4, FIA_UAU.6, FIA_UID.1, FPT_RPL.1 and FTP_TRP.1.

The SF7 “Identification and Authentication” uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF “basic”.

6.1.8 Assignment of SFs to security functional requirements

The justification of the mapping between security functional requirements and security functions is given in sections 6.1.1 – 6.1.7 as well as in this chapter 6.1.8. The results are summarized in table 6.2.

Table 6.2 – Assignment of security functional requirements to security functions

#	SFR	SF1	SF2	SF3	SF4	SF5	SF6	SF7
1	FCO_NRO.2							X
2	FCS_CKM.1					X	X	
3	FCS_CKM.4					X		
4	FCS_COP.1	X						
5	FDP_ACC.1			X				
6	FDP_ACF.1			X				
7	FDP_ETC.2			X				
8	FDP_ITC.2			X				
9	FDP_RIP.2			X				
10	FIA_ATD.1							X
11	FIA_UAU.1							X
12	FIA_UAU.4							X
13	FIA_UAU.6							X
14	FIA_UID.1							X
15	FMT_MOF.1			X				
16	FMT_MSA.1			X				
17	FMT_MSA.2			X				
18	FMT_MSA.3			X				
19	FMT_MTD.1			X				
20	FMT_SMF.1			X				

#	SFR	SF1	SF2	SF3	SF4	SF5	SF6	SF7
21	FMT_SMR.2			X				
22	FPT_AMT.1		X					
23	FPT_FLS.1	X	X					
24	FPT_PHP.1				X			
25	FPT_RCV.4	X	X					
26	FPT_RPL.1							X
27	FPT_RVM.1				X			
28	FPT_SEP.1				X			
29	FPT_TDC.1			X				
30	FPT_TST.1		X					
31	FTP_TRP.1							X

FCO_NRO.2 (Enforced proof of origin) is mapped to SF7. SF7 supplies the generation and verification of evidence of origin for transmitted data signed using identity keys, by using RSA algorithm for the signature operation (signing the hash value generated over the transmitted data) at all times.

FCS_CKM.1 (Cryptographic key generation) is mapped to SF5 and SF6. SF5 and SF6 support the generation of asymmetric cryptographic key pairs in accordance with the specified cryptographic key generation algorithm RSA and specified cryptographic key sizes RSA 512, 1024 and 2048 bits. The source of randomness is the TOE random number generator (RNG) as defined in SF6

FCS_CKM.4 (Cryptographic key destruction) is mapped to SF5. SF5 supports the destruction of cryptographic keys by invalidating the keys in accordance with FIPS 140-2.

FCS_COP.1 (Cryptographic operation) is mapped to SF1. SF1 supports the RSA encryption and decryption (OAEP or PKCS V15 encoding) as well as the RSA signature generation and verification (DER or SHA1 encoding) in accordance with the specified cryptographic algorithm RSA and cryptographic key sizes of 512, 1024 and 2048 bits as defined by PKCS#1 V2.0. Furthermore SF1 supports the secure hash in accordance with the specified cryptographic algorithm SHA-1 that meets FIPS 180-1 and the calculation of keyed-hashing message authentication code (HMAC) in accordance with the cryptographic algorithm SHA-1 using a key length of 20 bytes and a block size of 64 bytes as defined by RFC 2104.

FDP_ACC.1 (Subset access control) and FDP_ACF.1 (Security attribute based access control) are mapped to SF3. SF3 enforces the security function policy POAC (cf. chapter 6.3) to protect the sensitive subjects (commands), objects (keys and user data) and

operations (signature generation/verification, encryption or decryption) of the PC8375T TPM MODULE. The TOE provides access control by denying access to some subjects, objects and operations and allowing access to other subjects, objects and operations based on the security attributes TCG_AUTH_DATA_USAGE, TCG_KEY_FLAGS and TCG_KEY_USAGE.

FDP_ETC.2 (Export of user data with security attributes) and FDP_ITC.2 (Import of user data with security attributes) are mapped to SF3. SF3 enforces the POAC to control the export and import of user data with security attributes. POAC enforces the export of the associated security attributes with the data and enforces the interpretation and use of the imported associated security attributes.

FDP_RIP.2 (Full residual information protection) is mapped to SF3. SF3 enforces that the previous information content of resources is made unavailable upon the de-allocation of the resource from all objects by overwriting or de-allocation of the corresponding memory area.

FIA_ATD.1 (User attribute definition) is mapped to SF7. SF7 supports the security attributes authentication data and role, belonging to individual users, with regard to identification and authentication. Any operational role can access all protected commands and shielded locations only through the authentication mechanism. The access-right of commands, user data, keys and operations are defined by different security attributes as defined in chapter 6.1.3. The PC8375T TPM module allows access to data and keys with the “world” access and access to different commands on behalf of the user to be performed before the user is authenticated/identified. In contrast to this each user has to be successfully authenticated/identified before allowing any other TSF-mediated action on behalf of that user.

FIA_UAU.1 (Timing of authentication) and FIA_UID.1 (Timing of identification) are mapped to SF7. SF7 allows access to data and keys with the “world” access and access to different commands on behalf of the user to be performed before the user is authenticated/identified. In contrast to this each user has to be successfully authenticated/identified before allowing any other TSF-mediated action on behalf of that user.

FIA_UAU.4 (Single-use authentication mechanism) and FIA_UAU.6 (Re-authenticating) is mapped to SF7. SF7 provides two protocols for authentication and identification to authenticate an entity owner and to authorize use of an entity without revealing the authorization data on the network or the connection to the TOE. The first protocol is the “*Object-Independent Authorization Protocol*” (OI-AP), which allows the exchange of nonces with a specific TPM. The second protocol is the “*Object Specific Authorization Protocol*” (OS-AP)” allowing establishment of an authentication session for a single entity. Both

identification and authentication protocols use a random nonce. Users re-authentication by the authorisation protocols is realized with a new nonce for each message and response to prevent sneaking of old authentication data.

FMT_MOF.1 (Management of security functions behaviour) is mapped to SF3. SF3 supports the TPM owner in disabling/enabling the following three functions: TPM_DisablePubekRead (prevent any entity from reading the PUBEK), TPM_OwnerSetDisable (enable/disable a TPM) and TPM_DisableOwnerClear (disable the TPM_OwnerClear function).

FMT_MSA.1 (Management of security attributes), FMT_MSA.2 (Secure security attributes) and FMT_MSA.3 (Static attribute initialisation) are mapped to SF3. SF3 enforces the POAC to restrict the ability to create the security attributes associated with a particular entity (TCG_AUTH_DATA_USAGE, TCG_KEY_USAGE, migratable and volatility flag) to the entity owner. Only secure values are accepted for the security attributes of SF3. Moreover the POAC provides specific default values for security attributes, whereby the entity owner is allowed to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 (Management of TSF data) and FMT_SMR.2 (Restrictions on security roles) are mapped to SF3. SF3 supports the roles TPM owner, owners of entities and TPM manufacturer (NSC), which are associated with users by means of SF3. SF3 restricts the ability to modify identification and authentication data associated with the EK and SRK as well as migration authorization data to the TPM owner. Moreover SF3 restricts the generation of the SRK and TPM_Proof to the TPM owner and the modification of the identification and authentication data associated with entity to the entity owner. Furthermore SF3 restricts the generation of the Endorsement Key Pair to NSC or the PC manufacturer. The Endorsement Key Pair is created as part of the chip initialization process at the factory, and can not be changed/removed for the entire TOE's life time.

FMT_SMF.1 (Specification of management functions) is mapped to SF3. SF3 supports the specification of the following management functions to be provided by the TOE: Disabling/enabling of security functions behavior, creation of POAC security attributes, modification and generation of TSF data.

FPT_AMT.1 (Abstract machine testing) and FPT_TST.1 (TSF testing) are mapped to SF2. SF2 supports a suite of self-tests to check and demonstrate the correct operation of both the security assumptions provided by the abstract machine that underlies the TSF and the TOE security functions. The self-tests run during initial start-up, periodically during normal

operation, at the explicit request of the authorized user, and automatically prior to execution of the first call to a capability that uses corresponding functions.

FPT_FLS.1 (Failure with preservation of secure state) and FPT_RCV.4 (Function recovery) are mapped to SF1 and SF2. SF1 and SF2 force the TOE into a secure state upon detection of any failure during self-test, crypto operation and commands (RSA encryption, RSA decryption, SHA, RNG, RSA signature generation, HMAC generation) or internal operations. All TPM commands including those ones mentioned above have the property that the SF either completes successfully, or recovers to a consistent and secure state.

FPT_PHP.1 (Passive detection of physical attack) is mapped to SF4. SF4 provides several measures for detecting physical tampering and protecting the TOE against corresponding attacks that might compromise the TOE security functions (e.g. tamper evident package, snooping protection/detection).

FPT_RPL.1 (Replay detection) is mapped to SF7. SF7 supports replay detection for command requests that include the nonce parameter. The nonce parameter is a random number generated by the TOE's random number generator, whereby each command request includes a new nonce. In case of detected replay for such a request the corresponding session is destroyed. The "replay detection" mechanism is in place to prevent replay attacks and man-in-the-middle attacks.

FPT_RVM.1 (Non-bypassability of the TSP) is mapped to SF4. SF4 supports TSF implementation in a way that bypassing of TSP enforcement functions is not possible. The TOE maintains all microcode (TSF code as well as other code) in secure areas of the chip for its own execution to protect the microcode from interference and tampering by untrusted subjects. In addition, the TOE firmware maintains a total separation between the TPM non-volatile data and the non-TPM data.

FPT_SEP.1 (TSF domain separation) is mapped to SF4. SF4 provides maintenance of all microcode (TSF code as well as other code) in secure areas of the chip for its own execution to protect the microcode from interference and tampering by untrusted subjects.

FPT_TDC.1 (Inter-TSF basic TSF data consistency) is mapped to SF3. SF3 supports the capability to consistently interpret TPM commands and responses when shared between the TSF and other trusted IT product. The TSF use the TCG Main Specification [TCG] when interpreting the TSF data from such another trusted IT product.

FTP_TRP.1 (Trusted path) is mapped to SF7. SF7 supports a communication path between itself and local or remote users to protect the communicated data from modification or disclosure. The communications path, which is logically distinct from other communication paths, is capable of providing assurance that the user is communicating with the correct TSF, and that the TSF is communicating with the correct user. The trusted path can be used from the TSF and local or remote users for initial user authentication, for all TPM commands, all user commands and TSF responses.

6.2 Assurance Measures

In Table 6.3 the TOE specific assurance measures are listed. These measures, mainly consisting of providing appropriate documentation, are fulfilling the requirements from table 5.2:

Table 6.3 - Assurance requirements and assurance measures

Assurance requirements according to EAL3+	Assurance measures of the developer
Configuration management ACM_CAP.3 (Authorisation control) ACM_SCP.1 (TOE CM coverage)	Application of a CM System including configuration control
Delivery and operation ADO_DEL.1 (Delivery procedures) ADO_IGS.1 (Installation, generation and start-up procedures)	Documentation of the TOE's protection mechanisms with regard to delivery, installation and start-up
Development ADV_FSP.1 (Informal functional specification) ADV_HLD.2 (Security enforcing high-level design) ADV_RCR.1 (Informal corresponding demonstration) ADV_SPM.1 (Informal TOE security policy model)	Definition of CC requirements with regard to development procedures and documentation
Guidance documents AGD_ADM.1 (Administrator guidance) AGD_USR.1 (User guidance)	Creating and delivery of administrator and user guidance
Life cycle support ALC_DVS.1 (Identification of security measures) ALC_FLR.1 (Basic flaw remediation)	Ensuring the development processes by physical, personal and other security measures as well as ensuring the maintenance process by tracking and correcting flaws in the TOE

Assurance requirements according to EAL3+	Assurance measures of the developer
Tests ATE_COV.2 (Analysis of coverage) ATE_DPT.1 (Testing: high-level design) ATE_FUN.1 (Functional Testing) ATE_IND.2 (Independent Testing – sample)	Usage of a tool-based and automated test system for testing the security functions, high-level testing and testing the functional specification. Documenting the results and independent testing by the evaluator
Vulnerability assessment AVA_MSU.1 (Examination of guidance) AVA_SOF.1 (Strength of TOE security function evaluation) AVA_VLA.1 (Developer vulnerability analysis)	Analysing the security-relevant mechanisms with regard to SOF Basic and vulnerability analysis of obvious TOE vulnerabilities

6.3 Security Function Policy

The TOE enforces user access to cryptographic IT assets in accordance with the security function policy "*Protected Operations Access Controls (POAC)"* (cf. chapter 5.2.3 of this document) to meet the security functional requirements.

This policy includes:

- Roles and services that can be accessed by those roles:
  PC Manufacturer (corresponds to the role "TPM manufacturer or designee" of FMT_SMR.2.1): Has free access to all the functionality and data that the [TCG] permits before owner is installed.

  Administrator (represents a subset of the role "TPM owner" of FMT_SMR.2.1): To perform any command related to system configuration the administrator must supply the TPM ownership token.

  Entity owner (corresponds to the role "owners of entitites" of FMT_SMR.2.1): To load their entities into the TPM using the entity parent token associated with the entity. Loading of an entity does not include the usage of the loaded entity.
- Critical security parameters such as:
  Authentication token (a 20-byte blob of data)
  Endorsement Key Pair (2048 bit RSA key pair, imported into the TPM during the production phase, the private key never leaves the TPM)
  Storage Root Key (2048 RSA key pair, generated by the TPM, the private key never leaves the TPM)
  Platform Configuration Register (PCR) values
  Data Integrity Registers (Dir)
  Entities (the TPM can generate, store, use and destroy keys or identities)
  Security Attributes (e.g. Migration and Volatility attribute in TCG_KEY_FLAGS, TCG_AUTHDATA_USAGE, Key type attribute in TCP_KEY_FLAGS)

- Modes of access (read, write, execute, and delete) to services, user and TSF data and cryptographic security parameters.

A detailed description of the POAC policy will be given later on during the evaluation process within the document corresponding to the assurance component ADV_SPM.1 (Informal TOE security policy model).

7 PP Claims

7.1 PP Reference

This security target is in compliance with the protection profile TCG TPMPP version 1.9.7 [PP].

7.2 PP Tailoring

The assignments foreseen in the TCG TPMPP version 1.9.7 [PP] are done here. They are specified for FDP_ACF.1.3, FDP_ACF.1.4, FDT_ETC.2.4, FDP_ITC.2.5 and FMT_MOF.1.1 in chapter 5.2 of this security target, indicated by *underlined italics*. Moreover in addition to [PP] two refinements are supplemented for the assurance requirements AGD_ADM.1 and AGD_USR.1 as defined in chapter 5.3.4 of this ST and one refinement is supplemented for the functional requirement FCS_CKM.4 as defined in chapter 5.2.2 of this ST. Furthermore ACM_SCP.1 was modified here due to CC final interpretations 004 and 038, and in addition ALC_FLR.1 was modified due to CC final interpretations 094.

7.3 PP Additions

There are no additional assumptions, threats, security objectives and IT security requirements included in this ST compared to that ones contained in TCPA TPMPP version 1.9.7 [PP] with the exception of the security functional requirement FMT_SMF.1. FMT_SMF.1 is added here due to CC final interpretation 065 as mentioned in the introduction of chapter 5.2.

8 Rationale

This section provides the evidence used in the ST evaluation, at which chapters 8.1 – 8.4 are taken from the [PP] and chapters 8.5 – 8.6 are added compared with [PP]. This evidence supports the claims that the ST is a complete and cohesive set of requirements, that the TOE would provides an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements. The rationale also demonstrates that the [PP] conformance claims are valid.

8.1 Security Objectives Rationale

Table 8.1 maps assumptions and threats to objectives, demonstrating that all assumptions and threats are mapped to at least one objective. Table 8.2 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.

Table 8.1 – Mapping the TOE Security Environment to Objectives

#	Assumption/Threat	Objectives
1E	A.Configuration	OE.Configuration
2E	AE.Physical_Protection	OE.PhysSecurity
1	T.Attack	O.DAC, O.I&A, O.Security_Roles, O.Self_Protect
2	T.Bypass	O.HMAC, O.Security_Attr_Mgt, O.Invoke
3	T.Export	O.Export
4	T.Hack_Crypto	O.Crypto_Op
5	T.Hack_Physical	O.Tamper_ID
6	T.Imperson	O.I&A, O.Security_Roles, O.Import
7	T.Import	O.Import
8	T.Key_Gen_Destroy	O.Crypto_Key_Man
9	T.Malfunction	O.Fail_Secure
10	T.Modify	O.Limit_Actions_Auth, O.Security_Attr_Mgt, O.Security_Roles, O.Crypto_Key_Man
11	T.Object_Attr_Default	O.Object_Attr_Default
12	T.Object_Attr_Change	O.Object_Attr_DefaultOver
13	T.Object_SecureValues	O.Obj_Attr_SecureValues
14	T.Residual_Info	O.No_Residual_Info, O.Cryto_Key_Man
15	T.Replay	O.Single_Auth
16	T.Repudiate_Transact	O.MessageNR
17	T.Test	O.Crypto_Self_Test, O.General_Integ_Checks

Table 8.2 – Tracing of Security Objectives to Threats and Assumptions

#	Objectives	Threat/Assumptions
1E	OE.Configuration	A.Configuration
2E	OE.PhysSecurity	AE.Physical_Protection
1	O.Crypto_Key_Man	T.Residual_Info, T.Key_Gen_Destroy
2	O.Crypto_Op	T.Hack_Crypto
3	O.Crypto_Self_Test	T.Test
4	O.DAC	T.Attack
5	O.Export	T.Export
6	O.Fail_Secure	T.Malfunction
7	O.General_Integ_Checks	T.Test
8	O.HMAC	T.Bypass
9	O.I&A	T.Attack, T.Imperson
10	O.Import	T.Import, T.Imperson
11	O.Invoke	T.Bypass
12	O.Limit_Actions_Auth	T.Modify
13	O.MessageNR	T.Repudiate_Transact
14	O.No_Residual_Info	T.Residual_Info
15	O.Object_Attr_Default	T.Object_Attr_Default
16	O.Object_Attr_DefaultOver	T.Object_Attr_Change
17	O.Obj_Attr_SecureValues	T.Object_SecureValues
18	O.Security_Attr_Mgt	T.Modify, T.Bypass
19	O.Security_Roles	T.Attack, T.Modify, T.Imperson
20	O.Self_Protect	T.Attack
21	O.Single_Auth	T.Replay
22	O.Tamper_ID	T.Hack_Physical

8.1.1 Threats

This section describes each threat and enumerates and discusses the security objectives that counter the threat.

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.

T.Attack is countered by O.DAC, O.I&A, O.Security_Roles, and O.Self_Protect. These objectives limit the ability of a user to the performance of only those actions that the user is authorized to perform:

- O.DAC: The TOE shall provide its users with the means of controlling and limiting access to the TOE assets in accordance with a specified access control policy. This objective limits an attacker from performing unauthorized actions through a defined access control policy.
- O.I&A: The TOE shall uniquely identify all users, and shall authenticate the claimed identify before granting a user access to the TOE facilities. This objective supports the access control policy by uniquely identifying users (key pairs within the TOE) so that specific access control rules can be applied for each user role.
- O.Security_Roles: The TOE shall maintain security-relevant roles and association of users with those roles. This objective further supports the access control policy by associating each user with a role, which then can be assigned a specific access control policy.
- O.Self_Protect: The TSF will maintain a domain for its own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure.

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.

T.Bypass is countered by O.HMAC, O.Security_Attr_Mgt, and O.Invoke. These three objectives allow the TOE to detect tampering with data and to counter the ability of unauthorized users from tampering with security attributes or other data:

- O.HMAC: The TOE shall provide the ability to detect the modification of security attributes and other data. This objective provides the capability for the system to detect tampering with data.
- O.Security_Attr_Mgt: The TOE shall allow only authorised users to initialise and change object security attributes. This objective requires that only authorized users be allowed to initialise and change security attributes, which counters the threat of an unauthorized user making such changes.
- O.Invoke: The TSF shall be invoked for all actions. This objective assists in the protection of the system from tampering by unauthorised users, since it requires the TSF to be invoked for all actions and does not allow it to be bypassed by any user.

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.

T.Export I countered by O.Export. O.Export states: When data are exported outside the TPM, the TOE shall ensure that the data security attributes being exported are unambiguously associated with the data.

T.Hack_Crypto: Cryptographic algorithms may by incorrectly implemented, allowing an unauthorized individual or user to decipher keys generated within the TPM and thereby gain unauthorised access to encrypted data.

T.Hack_Crypto is countered by O.Crypto_Op, which states: The TOE shall perform cryptographic operations, including secure hash, HMAC, RSA digital signature and signature verification, RSA encryption and decryption, and RSA key generation in accordance with specified algorithms and key size; key size must be sufficient size to protect private/public key pairs from deciphering.

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.

T.Hack_Physical is countered by O.Tamper_ID, which states: The TOE shall provide features that permit a human to detect physical tampering of a system component. Although this objective does not prevent physical tampering, it allows physical tampering to be detected if the TOE is physically examined.

T.Imperson: An unauthorized individual may impersonate an authorised user of the TOE and thereby gain access to TOE data, keys, and operations.

T.Imperson is countered by O.I&A, O.Security_Roles, and O.Import. These objectives require a user to be identified and authenticated and to function under a predefined role with specified access control policy:

- O.I&A: The TOE shall uniquely identify all users, and shall authenticate the claimed identify before granting a user access to the TOE facilities. This objective requires identification and authentication of users (key pairs within the TOE) so that specific access control rules can be applied for each user role.
- O.Security_Roles: The TOE shall maintain security-relevant roles and association of users with those roles. This objective further requires the association of each user with a role, which then can be assigned a specific access control policy.
- O.Import: When data are being imported into the TOE, the TOE shall ensure that the data security attributes are being imported with the data and the data is from authorized source. In addition, the TOE shall verify those security attributes according to the TSF access control rules.

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.

T.Import is countered by O.Import, which states: When data are being imported into the TOE, the TOE shall ensure that the data security attributes are being imported with the data and the data is from authorized source. In addition, the TOE shall verify those security attributes according to the TSF access control rules.

T.Key_Gen_Destroy: Cryptographic keys may be generated or destroyed in an unsecure manner, causing key compromise.

T.Key_Gen_Destroy is countered by O.Crypto_Key_Man, which states: The TOE shall generate and destroy cryptographic keys in a secure manner.

T.Malfunction: TOE assets may be modified or disclosed to an unauthorised individual or user of the TOE, through malfunction of the TOE.

T.Malfunction is countered by O.Fail_Secure, which states: The TOE shall preserve the secure state of the system in the event of a cryptographic or other failure.

T.Modify: An attacker may modify data, e.g., stored security attributes or keys, in order to impersonate an authorised user or to gain access to the TOE and its assets. The integrity of the information may be compromised due to the unauthorised modification or destruction of the information by an attacker.

T.Modify is countered by O.Limit_Actions_Auth, O.Security_Attr_Mgt, O.Security_Roles, and O.Crypto_Key_Man. These objectives support the ability of the TOE to limit unauthorized user access and to maintain data and system integrity through appropriate management of cryptographic data in particular:

- O.Limit_Actions_Auth: The TOE shall restrict the actions a user may perform before the TOE verifies the identity of the user.
- O.Security_Attr_Mgt: The TOE shall allow only authorised users to initialise and change object security attributes.
- O.Security_Roles: The TOE shall maintain security-relevant roles and association of users with those roles.
- O.DAC: The TOE shall control and restrict user access to the TOE assets in accordance with a specified access control policy.

T. Object_Attr_Default: An attacker may create an object with no security attribute values.

T.Object_Attr_Default is countered by O.Object_Attr_Default, which states: The TOE shall require default security attributes for the object when the object is created.

T.Object_Attr_Change: A user or attacker may make unauthorized changes to security attribute values for an object.

T.Object_Attr_Change is countered by O.Object_Attr_DefaultOver, which states: The TOE shall permit authorised users to override defaulted values for security attributes for an object.

T.Object_SecureValues: An attacker or user may set unsecure values for object security attributes.

T.Object_SecureValues is countered by O.Obj_Attr_SecureValues, which states: The TOE shall maintain object security attributes by permitting only secure values.

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”).

T.Residual_Info is countered by O.No_Residual_Info and O.Crypto_Key_Man. O.No_Residual_Info ensure that no residual data is left in buffers or system locations. O.Crypto_Key_Man specifies that cryptographic key destruction must be performed:

- O.No_Residual_Info: The TOE shall ensure there is no “object reuse,” i.e., ensure that there is no residual information in information containers or system resources upon their reallocation to different users.
- O.Crypto_Key_Man: The TOE shall generate and destroy cryptographic keys in a secure manner.

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.

T.Replay is countered by O.Single_Auth, which states: The TOE shall provide a single use authentication mechanism and require re-authentication to prevent “replay” and “man-in-the-middle” attacks.

T.Repudiate_Transact: An originator of data may deny originating the data to avoid accountability.

T.Repudiate_Transact is countered by O.MessageNR, which states: The TOE shall provide user data integrity, source authentication, and the basis for source non-repudiation when exchanging data with a remote system.

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.

T.Test is countered by O.Crypto_Self_Test and O.General_Integ_Checks. These objectives require the TOE to provide self-test and integrity checking functionality in order to detect unsecure states either at start-up or during normal operation:

- O.Crypto_Self_Test: The TOE shall provide the ability to verify that the cryptographic functions operate as designed.
- O.General_Integ_Checks: The TOE shall provide periodic integrity checks on both system and user data.

8.2 Security Requirements Rationale

In this section, the objectives are mapped to the functional requirements and rationale is provided for the selected EAL and its components and augmentation.

8.2.1 Security Functional Requirements Rationale

The mapping of security objectives to functional requirements (components) is provided in Table 8.3.

Table 8.3 – Functional Component to Security Objective Mapping

#	Objectives	Functional Component
1	O.Crypto_Key_Man	FCS_CKM.1, FCS_CKM.4
2	O.Crypto_Op	FCS_COP.1, all iterations
3	O.Crypto_Self_Test	FPT_AMT.1, FPT_TST.1
4	O.DAC	FDP_ACC.1, FDP_ACF.1, FMT_MOF.1, FMT.MTD.1 (all iterations), FMT_SMF.1
5	O.Export	FDP_ETC.2
6	O.Fail_Secure	FPT_FLS.1, FPT_RCV.4
7	O.General_Integ_Checks	FPT_AMT.1, FPT_TST.1
8	O.HMAC	FCS_COP.1:4
9	O.I&A	FIA_UAU.1, FIA_UID.1, FIA_ATD.1
10	O.Import	FDP_ITC.2, FPT_TDC.1, FTP_TRP.1
11	O.Invoke	FPT_RVM.1
12	O.Limit_Actions_Auth	FIA_UAU.1, FIA_UID.1
13	O.MessageNR	FCO_NRO.2, FDP_ETC.2
14	O.No_Residual_Info	FDP_RIP.2
15	O.Object_Attr_Default	FMT_MSA.3
16	O.Object_Attr_DefaultOver	FMT_MSA.3
17	O.Obj_Attr_SecureValues	FMT_MSA.2, FPT_TDC.1
18	O.Security_Attr_Mgt	FMT_MSA.3, FMT_MSA.1, FMT_SMF.1
19	O.Security_Roles	FMT_SMR.2, FIA_ATD.1
20	O.Self_Protect	FPT_SEP.1
21	O.Single_Auth	FIA_UAU.4, FIA_UAU.6, FPT_RPL.1
22	O.Tamper_ID	FPT_PHP.1

A discussion of the rationale for the mapping is provided for each objective below.

O.Crypto_Key_Man: The TOE shall generate and destroy cryptographic keys in a secure manner.

O.Crypto_Key_Man is mapped to:

- FCS_CKM.1, Cryptographic key generation, which requires that cryptographic keys be generated in accordance with the RSA algorithm with specified cryptographic sizes that meet PKCS #1 V.2 standard.
- FCS_CKM.4, Cryptographic key destruction, which requires that cryptographic keys be destroyed in accordance with a specified secure key destruction method.

O.Crypto_Op: The TOE shall perform cryptographic operations, including secure hash, HMAC, RSA digital signature and signature verification, RSA encryption and decryption,

and RSA key generation in accordance with specified algorithms and key size; key size must be sufficient size to protect private/public key pairs from deciphering.

O.Crypto_Op is mapped to:

- FCS_COP.1, Cryptographic operations. There are four iterations of this component, including RSA encrypt and decrypt, RSA signature and signature verification, SHA, and Keyed-Hashing for Message Authentication. The iterations cover all cryptographic operations and specify key sizes and standards that must be met.

O.Crypto_Self_Test: The TOE shall provide the ability to verify that the cryptographic functions operate as designed.

O.Crypto_Self_Test is mapped to:

- FPT_AMT.1: Abstract machine testing. This component tests the cryptographic portion of the underlying abstract state machine.

- FPT_TST.1: TSF testing. This component defines self-tests to ensure that the cryptographic functions are operating correctly. Tests conducted during start-up and/or periodically may include known-answer tests of cryptographic operations, as well as statistical tests on random number generators. Additional tests may involve generation of private / public key pairs, pair-wise consistency tests of encryption and decryption, key-entry tests, and key integrity tests.

O.DAC: The TOE shall provide its users with the means of controlling and limiting access to the TOE assets in accordance with a specified access control policy.

O.DAC is mapped to:

- FDP_ACC.1, Subset access control, which requires that Protected Operations Access Controls by enforced on subjects, objects and operations.
- FDP_ACF.1, Security attribute based access control, which defines access controls based on TCG_AUTH_DATA_USAGE and TCG_KEY_USAGE values.
- FMT_MOF.1, Management of security functions behaviour, which specifies the list of functions (TPM_DisablePubekRead, TPM_OwnerSetDisable, TPM_DisableOwnerClear) that are restricted to the TPM owner.
- FMT_MTD.1, Management of TSF Data, ensures that the TSF data is accessible to authorized users.
- FMT_SMF.1, Specification of management functions defines the specification of the following management functions to be provided by the TOE: Disabling/enabling of security functions behavior, creation of POAC security attributes, modification and generation of TSF data.

O.Export: When data are exported outside the TPM, the TOE shall ensure that the data security attributes being exported are unambiguously associated with the data.

O.Export is mapped to:

- FDP_ETC.2, Export of user data with security attributes, which requires that data exported outside the TSF have security attributes that are unambiguously associated with the data exported.

O.Fail_Secure: The TOE shall preserve the secure state of the system in the event of a cryptographic or other failure.

O.Fail_Secure is mapped to:

- FPT_FLS.1, Failure with preservation of secure state, which requires that the TSF preserve a secure state in the event of a failure.
- FPT_RCV.4, Function recovery, which requires that all TPM Commands either complete successfully or fail and recover to a secure state.

O.General_Integ_Checks: The TOE shall provide periodic integrity checks on both system and user data.

O.General_Integ_Checks is mapped to:

- FPT_AMT.1: Abstract machine testing. This component tests the cryptographic portion of the underlying abstract state machine.

- FPT_TST.1: TSF testing. This component defines self-tests to ensure that the cryptographic functions are operating correctly. Tests conducted during start-up and/or periodically may include known-answer tests of cryptographic operations, as well as statistical tests on random number generators. Additional tests may involve generation of private / public key pairs, pair-wise consistency tests of encryption and decryption, key-entry tests, and key integrity tests.

O.HMAC: The TOE shall provide the ability to detect the modification of security attributes and other data.

O.HMAC is mapped to:

- FCS_COP.1.1;4, which requires that the TOE provide HMAC capability in conformance with the referenced standard to provide the ability to detect the modification of security attributes and other data.

O.I&A: The TOE shall uniquely identify all users, and shall authenticate the claimed identify before granting a user access to the TOE facilities. The TPM identification and authentication capability is used to authenticate an entity owner and to authorize use of an entity. The basic premise is to prove knowledge of a shared secret. This shared secret is the identification and authentication data. Note that the TCG Main Specification document refers to the identification and authentication process and this data as *authorization*.

O.I&A is mapped to:

- FIA_UAU.1, Timing of authentication, which states that a user shall be successfully authenticated before performing all actions except those explicitly defined.

- FIA_UID.1, Timing of identification, which states that a user shall be successfully identified before performing all actions except those explicitly defined.
- FIA_ATD.1, User attribute definition, which supports FIA_UAU.1 and FIA_UID.1 by providing a requirement for user attributes. Authentication data is defined as a user attribute. Authentication data in this case is associated with a specific key, which is analogous to a user.

O.Import: When data are being imported into the TOE, the TOE shall ensure that the data security attributes are being imported with the data and the data is from authorized source. In addition, the TOE shall verify those security attributes according to the TSF access control rules.

O.Import is mapped to:

- FDP_ITC.2, Import of user data with security attributes, which states that data imported into the TOE must have security attributes. These include authentication data on user keys.
- FPT_TDC.1, Inter-TSF basic TSF data consistency, defines security attributes and requires that they be consistently interpreted when importing data.
- FTP_TRP.1, Trusted path ensures that the data is being received from an authorized source. Trusted path is also a dependency of FDP_ITC.2, requiring a trusted path for data import.

O.Invoke: The TSF shall be invoked for all actions.

O.Invoke is mapped to:

- FPT_RVM.1, Non-bypassability of the TSP, which ensures that TSP functions are invoked and succeed before each function within the TSC is allowed to proceed.

O.Limit_Actions_Auth: The TOE shall restrict the actions a user may perform before the TOE verifies the identity of the user.

O.Limit_Actions_Auth is mapped to:

- FIA_UAU.1, Timing of authentication, which states that a user shall be successfully authenticated before performing all actions except those explicitly defined.
- FIA_UID.1, Timing of identification, which states that a user shall be successfully identified before performing all actions except those explicitly defined.

O.MessageNR: The TOE shall provide user data integrity, source authentication, and the basis for source non-repudiation when exchanging data with a remote system.

O.MessageNR is mapped to:

- FCP_NRO.2, Enforced proof of origin, which requires that the TSF enforce generation of data that provides evidence of origin for data transmitted.
- FDP_ETC.2, Export of user data with security attributes, ensures that access control SFPs and security attributes are associated with exported data, thereby providing user data integrity.

O.No_Residual_Info: The TOE shall ensure there is no "object reuse," i.e., ensure that there is no residual information in information containers or system resources upon their reallocation to different users.

O.No_Residual_Info is mapped to:

- FDP_RIP.2, Full residual information protection, which requires that any previous information content of a resource be made unavailable.

O.Object_Attr_Default: The TOE shall require default security attributes for the object when the object is created.

O.Object_Attr_Default is mapped to:

- FMT_MSA.3, Static attribute initialisation, which requires that security attributes be specified and that certain defaults be in place.

O.Object_Attr_DefaultOver: The TOE shall permit authorised users to override defaulted values for security attributes for an object.

O.Object_Attr_DefaultOver is mapped to:

- FMT_MSA.3, Static attribute initialisation, which requires that security attributes be specified, that certain defaults be defined, and that authorised users have the capability to override the defaults.

O.Obj_Attr_SecureValues: The TOE shall maintain object security attributes by permitting only secure values.

O.Obj_Attr_SecureValues is mapped to:

- FMT_MSA.2, Secure security attributes, which requires that only secure values be accepted for security attributes.
- FPT_TDC.1, Inter-TSF basic TSF data consistency, defines security attributes.

O.Security_Attr_Mgt: The TOE shall allow only authorised users to initialise and change object security attributes.

O.Security_Attr_Mgt is mapped to:

- FMT_MSA.3, Static attribute initialisation, which requires that security attributes be specified.
- FMT_MSA.1, Management of security attributes, which specifies that access controls, requiring security attributes for objects be enforced.
- FMT_SMF.1, Specification of management functions defines the specification of the following management functions to be provided by the TOE: Disabling/enabling of security functions behavior, creation of POAC security attributes, modification and generation of TSF data.

O.Security_Roles: The TOE shall maintain security-relevant roles and association of users with those roles.

O.Security_Roles is mapped to:

- FMT_SMR.2, Restrictions on security roles, which requires that the TSF maintain roles and that the roles be associated with users.
- FIA_ATD.1, User attribute definition, which provides a requirement for user attributes. Authentication data is defined as a user attribute. Authentication data in this case is associated with a specific key, which is analogous to a user. Note that the TPM identification and authentication capability is used to authenticate an entity owner and to authorize use of an entity. The basic premise is to prove knowledge of a shared secret. This shared secret is the identification and authentication data. Note that the TCG Main Specification document refers to the identification and authentication process and this data as *authorization*.

O.Self_Protect: The TSF will maintain a domain for its own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure.

O.Self_Protect is mapped to FPT_SEP.1, TSP domain separation which requires the TSF to protect itself.

O.Single_Auth: The TOE shall provide a single use authentication mechanism and require re-authentication to prevent “replay” and “man-in-the-middle” attacks.

O.Single_Auth is mapped to:

- FIA_UAU.4, Single-use authentication mechanisms, which prevents the reuse of authentication data.
- FIA_UAU.6, Re authenticating, which requires that a user be re authenticated for every command that requires user authentication.
- FPT_RPL.1, Replay detection, prevents replay attacks.

O.Tamper_ID: The TOE shall provide features that permit a human to detect physical tampering of a system component.

O.Tamper_ID is mapped to:

- FPT_PHP.1, Passive detection of physical attack, which requires that physical tampering with the TOE be detectable.

8.2.2 Security Assurance Requirements Rationale

EAL 3 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. EAL 3 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, and evidence of a developer search for obvious vulnerabilities.

EAL 3 is augmented with ADV_SPM.1 because ADV_SPM.1 is a dependency of functional security requirements FMT_MSA.2. EAL 3 is also augmented with ALC_FLR.1 to track and correct the reported and found security flaws in the product.

8.2.3 Strength of Function Rationale

The TOE is expected to be designed to protect against “low” attack potential. Thus, based on the CEM Annex B, Table B.2, the strength of function is SOF Basic. The strength of cryptographic algorithms is outside the scope of the CC. Strength of function only applies to non-cryptographic, probabilistic or permutational mechanisms. The SOF requirement applies to the identification and authentication functionality for the TPM.

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 TPM, the developer of this 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 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. Using Table B.4 (duplicated below), this number translates to 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

The threat level for the TOE authentication function is assumed to be SOF-basic. This defines a level of authentication strength of function where analysis shows that the function provides basic protection against straightforward or intentional breach of TOE security by attackers possessing a minimum attack potential.

The hardware and FAILRSTPWD passwords are 64 bits each. In compliance with the Administrator’s Guide, the passwords:

- Must be exactly 8 characters long and must not be zeros.
- Must contain alphanumeric characters only.

- Must not be a common word, a word in any existing password dictionaries, or a word easily guessed (such as “password”).

User passwords are discretionary, however, in compliance with the User’s Guide, users must use passwords and follow the same guidelines for selecting passwords as those of the administrator, listed above.

Analysis was performed using the following assumptions:

- It is assumed that the SOF analysis is limited to users who choose to specify passwords, i.e., user passwords are discretionary and if a user decides not to use a password as an authentication mechanism, than no SOF claims are made. Note that the hardware password and FAILRSTPWD must be supplied as part of chip initialization; these passwords are not discretionary.
- It is assumed that the administrators and the users will follow password guidelines listed above.
- It is assumed that attackers would have access to commonly available password crackers, particularly those that use dictionary and exhaustive search attacks.
- It is assumed that the environment provides protections such that passwords could not be captured en route to the chip, therefore the analysis covers only those attacks that guess passwords or retrieve them from the TOE through some vulnerability; the scope of the SOF analysis is the TOE.
- Although words easily guessed or those in a known password dictionary are not supposed to be used, in order to present the worst-case scenario, it is assumed that users will select natural language passwords, thereby greatly reducing the possible passwords that could be used.
- It is assumed that users would clear their keys from the system after user to avoid an exhaustive attack on user key passwords. This is recommended in the user guide. User passwords are therefore not considered in the analysis.
- It is assumed that natural language passwords number no greater than 100,000.
- It is assumed that the attacker would first use a dictionary attack that would include common strategies for guessing passwords such as selecting a user login name, pAsSwOrD, simple transformations for common words, etc.
- Motivation of the attacker is not considered as part of this analysis because the system is multi-purpose and there is no way of knowing the value of the assets

protected by the TOE. It is assumed that the value of the assets is low and therefore motivation on the part of the attacker is moderate to low.

- It is assumed that there are no time limitations on the attacker.

The chip does not allow reads to the registers that hold the Hardware, FAILRSTPWD, and user passwords. Based on the vulnerability analysis, there is no obvious vulnerability such as buffer overflow, etc, that would allow an attacker access to these registers. Therefore, the SOF analysis focused on password "cracker" attacks. With 100,000 password possibilities, on average, the cracker would guess the password in 50,000 tries.

If there were no other protections, it would be relatively simple to break the password mechanism in a short time with 50,000 tries. However, the TOE has authentication failure protection on the hardware and FAILRSTPWD, which locks the attacker out of the system on the 10th incorrect password supplied for a period of one hour and 17 minutes. Thereafter, every single subsequent failed attempt causes the lockout period to double. The lockouts do not stop until a correct Hardware or FAILRSTPWD is entered.

Given the authentication failure protection mechanism, it would take months to crack the password, given that the attacker on average must try 50,000 passwords and the lockout periods double with each lockout, i.e., the first lockout after 10 tries is one hour and 17 minutes, the next password try lockout period would be two hours and 34 minutes, etc.

The attack potential for the TOE authentication mechanism was scored using Table B.3 in Annex B.8 of the CEM. The attack potential was scored as 17, i.e., a layman with no equipment (score of 0) would take more than a month to guess the password, with the score of 8 for elapsed time and 9 for Access to the TOE (total of 17). The calculated attack potential is therefore a 17, which corresponds to SOF-basic.

Note that the I&A mechanism used in the TPM is manufacturer-specific and SOF analysis must be performed as part of ST development. Note that the SOF rating is required by this ST to be SOF Basic or higher.

8.3 Dependency Rationale

Table 8.4 – Functional Requirements Dependencies

#	Requirement	Dependencies
1	FCO_NRO.2	FIA_UID.1
2	FCS_CKM.1	FCS_COP.1, FCS_CKM.4, FMT_MSA.2

#	Requirement	Dependencies
3	FCS_CKM.4	FCS_CKM.1, FMT_MSA.2
4	FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
5	FDP_ACC.1	FDP_ACF.1
6	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
7	FDP_ETC.2	FDP_ACC.1
8	FDP_ITC.2	FDP_ACC.1, FTP_TRP.1, FPT_TDC.1
9	FDP_RIP.2	None
10	FIA_ATD.1	None
11	FIA_UAU.1	FIA_UID.1
12	FIA_UAU.4	None
13	FIA_UAU.6	None
14	FIA_UID.1	None
15	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1
16	FMT_MSA.1	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1
17	FMT_MSA.2	ADV_SPM.1, FDP_ACC.1, FMT_MSA.1, FMT_SMR.1
18	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
19	FMT_MTD.1	FMT_SMF.1, FMT_SMR.1
20	FMT_SMF.1	None
21	FMT_SMR.2	None
22	FPT_AMT.1	None
23	FPT_FLS.1	ADV_SPM.1
24	FPT_PHP.1	FMT_MOF.1
25	FPT_RCV.4	ADV_SPM.1
26	FPT_RPL.1	None
27	FPT_RVM.1	None
28	FPT_SEP.1	None
29	FPT_TDC.1	None
30	FPT_TST.1	FPT_AMT.1
31	FPT_TRP.1	None

8.4 Security Functional Requirements Grounding in Objectives

Table 8.5 – Requirements to Objectives Mapping

#	Requirements	Objectives

#	Requirements	Objectives
1	FCO_NRO.2	O.MessageNR
2	FCS_CKM.1	O.Crypto_Key_Man
3	FCS_CKM.4	O.Crypto_Key_Man
4-1	FCS_COP.1; 1	O.Crypto_Op
4-2	FCS_COP.1; 2	O.Crypto_Op
4-3	FCS_COP.1; 3	O.Crypto_Op
4-4	FCS_COP.1; 4	O.Crypto_Op, O.HMAC
5	FDP_ACC.1	O.DAC
6	FDP_ACF.1	O.DAC
7	FDP_ETC.2	O.Export, O.MessageNR
8	FDP_ITC.2	O.Import
9	FDP_RIP.2	O.No_Residual_Info
10	FIA_ATD.1	O.I&A, O.Security_Roles
11	FIA_UAU.1	O.I&A, O.Limit_Actions_Auth
12	FIA_UAU.4	O.Single_Auth
13	FIA_UAU.6	O.Single_Auth
14	FIA_UID.1	O.I&A, O.Limit_Actions_Auth
15	FMT_MOF.1	O.DAC
16	FMT_MSA.1	O.Security_Attr_Mgt
17	FMT_MSA.2	O.Obj_Attr_SecureValues
18	FMT_MSA.3	O.Security_Attr_Mgt, O.Object_Attr_Default, O.Object_Attr_DefaultOver
19	FMT_MTD.1	O.DAC (all iterations of FMT_MTD.1)
20	FMT_SMF.1	O.DAC, O.Security_Attr_Mgt
21	FMT_SMR.2	O.Security_Roles
22	FPT_AMT.1	O.Crypto_Self_Test, O.General_Integ_Checks
23	FPT_FLS.1	O.Fail_Secure
24	FPT_PHP.1	O.Tamper_ID
25	FPT_RCV.4	O.Fail_Secure
26	FPT_RPL.1	O.Single_Auth
27	FPT_RVM.1	O.Invoke
28	FPT_SEP.1	O.Self_Protect
29	FPT_TDC.1	O.Obj_Attr_SecureValues, O.Import
30	FPT_TST.1	O.Crypto_Self_Test, O.General_Integ_Checks

#	Requirements	Objectives
31	FTP_TRP.1	O.Import

8.5 TOE Summary Specification Rationale

This chapter shows that the TOE security functions and assurance measures are suitable to meet the TOE Security Requirements.

8.5.1 TOE Security Functions Rationale

Table 6.2 in chapter 6 shows that the security functions defined in the TOE Summary Specification address all of the TOE security functional requirements. All security functions are necessary because there is at least one security functional requirement mapped to each security function. The corresponding rationale for each mapping is provided for each security functional requirement within chapter 6.1.

8.5.2 Security Requirements are mutually supportive and internally consistent

All security functional requirements are taken from the Common Criteria part 2. The TOE fulfils all the dependencies defined in the selected SFRs. This shows that the security functions work together so as to satisfy the security functional requirements.

The Table 6.2 shows that all security functional requirements are satisfied by at least one security function. The definitions of the security functional requirements and the assurance components in the preceding chapters demonstrate that mutual support and consistency are given for both groups of requirements. The fact that the SFRs and the assurance requirements support each other and that there are no inconsistencies between these groups is shown in the sections above.

8.5.3 Assurance Measures Rationale

The rationale shows how all assurance requirements were satisfied. The Table 6.3 in chapter 6 shows that there is at least one assurance measure defined in the TOE Summary Specification to meet each of the security assurance requirements.

8.6 PP Claims Rationale

This security target is in compliance with the protection profile TCPA TPMPP version 1.9.7 [PP].

The assignments foreseen in the TCPA TPMPP version 1.9.7 [PP] are done here. They are specified for FDP_ACF.1.3, FDP_ACF.1.4, FDT_ETC.2.4, FDP_ITC.2.5 and

FMT_MOF.1.1 in chapter 5.2 of this security target, indicated by *underlined italics*. Moreover in addition to [PP] two refinements are supplemented for the assurance requirements AGD_ADM.1 and AGD_USR.1 as defined in chapter 5.3.4 of this ST. These refinements are not in contradiction to any assumption in [PP].

There are no additional security objectives and IT security requirements included in this ST compared to that ones contained in TCPA TPMPP version 1.9.7 [PP] with the exception of the security functional requirement FMT_SMF.1. FMT_SMF.1 is added here due to CC final interpretation 065 as mentioned in the introduction of chapter 5.2.

9 Appendix

9.1 References

[AGD] *PC8374T/PC8375T Guidance document*, February 2004, Rev.1.2 by NSC

[AIS31] *A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators1 Version 3.1 25.09.20*01

[CC] *Common Criteria for Information Technology Security Evaluation*, version 2.1, revision August 1999
Part 1: Introduction and general model, CCIMB-99-031,
Part 2: Security functional requirements, CCIMB-99-032,
Part 3: Security Assurance Requirements, CCIMB-99-033
Incorporated with interpretations as of 2002-02-28

[CEM] *Common Methodology for Information Technology Security Evaluation, Part 1: Introduction and general model*, version 0.6, revision 11.01.1997,
Part 2: Evaluation Methodology, version 1.0, revision August 1999
Incorporated with interpretations as of 2002-02-28

[Datasheet] *PC8374T/PC8375T Datasheet*, April 2004, Rev 1.1 by NSC

[Init] *TPM Initialization and Configuration for PC8375T and PC8394T* application note, July 2004, by NSC

[PP] *Trusted Computing Platform Alliance (TCPA) Trusted Platform Module Protection Profile (TPM PP)*, version 1.9.7, revision July 1,2002
http://niap.nist.gov/cc-scheme/pp/index.html

[TCG] *Trusted Computing Group Main Specification*, version 1.1b, revision February 22, 2002, https://www.trustedcomputinggroup.org/home)

[TCG_PC] *Trusted Computing Group PC Specific Implementation Specification*, version 1.0, revision 2001-09-09, https://www.trustedcomputinggroup.org/home)

[AIS31] *A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators1 Version 3.1 25.09.20*01

9.2 Acronyms and Glossary

Acronyms

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
NSC	National Semiconductor Ltd.
PP	Protection Profile

SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

Glossary

3DES:	DES using a key of a size that is 3X the size that of a DES key. See DES.
Blob:	Opaque data of fixed or variable size. The meaning and interpretation of the data is outside the scope and context of the Subsystem.
Challenger:	An entity that requests and has the ability to interpret integrity metrics from a Subsystem.
Conformance Credential:	A credential that states the conformance to the TCG specification of: the TPM; the method of incorporation of the TPM into the platform; the RTM; and the method of incorporation of the RTM into the platform.
Denial-of-service attack:	An attack on a system (or subsystem) which has no affect on information except to prevent its use.
DES:	Symmetric key encryption using a key size of 56 bits defined by NIST as FIPS 46-3.
Endorsement Credential:	A credential containing a public key (the endorsement public key) that was generated by a genuine TPM.
Endorsement Key:	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).
Identity Credential:	A credential issued by a Privacy CA that provides an identity for the TPM.
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.
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.
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.

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: http://www.rsa.com.
SHA-1:	A NIST defined hashing algorithm producing a 160-bit result from an arbitrary sized source as specified in FIPS 180-1.
Storage Root Key (SRK):	The root key of a hierarchy of keys associated with a TPM; generated within a TPM; a non-migratable key.
Subsystem:	The combination of the TSS and the TPM.
Support Services (TSS):	Services to support the TPM but which do not need the protection of the TPM. The same as Trusted Platform Support Services.
TCG-protected capability:	A function which is protected within the TPM, and has access to TPM secrets.
TPM Identity:	One of the anonymous PKI identities belonging to a TPM; a TPM may have multiple identities.

Trusted Platform Agent (TPA): Trusted Platform Agent; the component within the platform that reports integrity metrics, logs, Validation Data, etc. to a Challenger; outside the scope of this specification.

Trusted Platform Measurement Store (TPMS): Storage locations within the Subsystem, which contain unprotected logs of measurement process.

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 (TSS): 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.