CERTIFICATION REPORT

Certification file:	**TUVIT-DSZ-CC-9205**
Product / system:	trusted platform module SLD9630TT1.1 / M2009
Product manufacturer:	Infineon Technologies AG St.-Martin-Straße 76 81609 München
Customer:	see above
Evaluation facility:	TÜViT, evaluation body for IT security
Evaluation report:	*Version 1.0 as of 2004-01-21* Document-number: *20468884_TÜV_040.01* Author: Dr. Patrick Bödeker
Result:	EAL3 augmented by 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, 2004-01-29

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

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

SLD9630TT1.1 / M2009
of
Infineon Technologies AG

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 1.0* for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.1* (ISO 15408) 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-9205-2004

Essen, 2004-01-29 sign. Dr. Gruschwitz
Certification Body

TÜV Informationstechnik GmbH - Subsidiary of the RWTÜV Group • Langemarckstraße 20 • 45141 Essen, Germany
☎ +49 201 8999-580 • 🖷 +49 201 8999-555 • tuvit@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] – a subsidiary of the RWTÜV 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-014/99-00 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 December 2nd, 1997 (renewed on the 20th of November 2002).
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, version 2.1, August 1999.
- 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 1.0, August 1999.
- 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. The CERTÜViT certificates are recognized by BSI – the national German certification body in international agreements – to be equivalent to its own certificates.

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, Finland, France, Germany, Greece, Hungary, Israel, Italy, Japan, The Netherlands, Norway, 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 SLD9630TT1.1 / M2009 has undergone the certification procedure at TÜViT certification body. It was an initial certification.

The evaluation of the security controller SLD9630TT1.1 / M2009 was conducted by the evaluation body for IT-security of TÜViT and concluded on January 21, 2004. The TÜViT evaluation facility is recognised by BSI.

The sponsor as well as the developer is Infineon Technologies AG. Distributor of the product is Infineon Technologies AG.

The certification was concluded with

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

This work was concluded on January 29, 2004. 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-18. The product SLD9630TT1.1 / M2009 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 security controller ***SLD9630TT1.1 / M2009***[3]*,* called within the TCPA TPM Protection Profile [TCPA TPM PP] a Trusted Platform Module (TPM). A 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 SLD9630TT1.1 is a complete solution implementing the version 1.1b of the Trusted Computing Platform Alliance (TCPA) specification. The SLD9630TT1.1 uses the LPC (Low Pin Count) interface as defined by Intel for the integration into existing PC mainboards. The SLD9630TT1.1 is basically a secure controller with the following added functionality:

- Random number generator
- Asymmetric key generation (RSA keys with key length up to 2048 bit)
- Symmetric and asymmetric key procedures (encryption/decryption, generation and verification of digital signatures)
- Hash algorithms (SHA-1, HMAC)
- Secure key and data storage
- Identification and Authentication mechanisms

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

The sponsor, vendor and distributor is “Infineon Technologies AG, St.-Martin-Straße 76, 81609 München“.

The TOE was evaluated against the claims of the Security Target[4] [ST] (attached in part D) by the “*evaluation body of TÜV Informationstechnik GmbH (TÜViT)*”. The evaluation was completed on January 21, 2004. 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 EAL3

[3] In the following shortly termed SLD9630TT1.1.

[4] hereinafter called ST

(Evaluation Assurance Level 3) 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).

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.

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

TSF	Short Description
Cryptographic Support	Provides generation of random numbers, generation of asymmetric key pairs, RSA digital signature, data encryption and decryption, key destruction, and the generation of hash values.
Authentication and Identification	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 TPM. The basic premise is to prove knowledge of a shared secret.
Access Control	Provides access control based on different attributes to protect the sensitive subjects (commands), objects (keys and user data) and operations (signature generation, encryption or decryption) of the TOE.
Origin	Provides 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.

TSF	Short Description
TSF Protection and Test	Provides a suite of tests (self-tests, hardware and firmware controlled) to check and demonstrate the correct operation of the TOE. The self-tests run during initial start-up, during normal operation, and at the request of the user. The user has the possibility to do a self-test and to sign the test result within the TPM.

A more detailed description of the TOE security functions can be found in section 6.1 of the 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 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.

All 17 threats are taken from the TCPA Trusted Platform Module Protection Profile, Version 1.9.7 [TCPA 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 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.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.

Threat	Description
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.Key_Gen_Destroy	Cryptographic keys may be generated or destroyed in an unsecure 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 unsecure 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”).
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 unsecure state or enter an unsecure state, allowing an attacker to obtain sensitive data or compromise the system.

Table 1: Threats

No organisational 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 assumptions and the assumptions for the IT environment are defined in the

section chapter 3.1 of the TCPA Trusted Platform Module Protection Profile, Version 1.9.7 [TCPA TPM PP] and are described in sections 4.1 and 4.2 of this report, respectively.

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 SLD9630TT1.1 / M2009 which comprises the hardware of the security controller and the associated firmware (operating system and Self Test Software).

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: administrator, entity owner, and entity user
- 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 6.2.1 of the 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 the TCPA Trusted Platform Module Protection Profile [TCPA TPM PP].

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The following usage assumption is defined in the TCPA Trusted Platform Module Protection Profile [TCPA 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 [TCPA 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) SLD9630TT1.1 / M2009. The TPM works together with a second module called the TCPA 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 comprised two major components: one hardware component with the 6 subcomponents: *Security Devices, Core, Peripherals, Memory, Coprocessors, Bus System* and one software/firmware component with the 10 subcomponents *Self-Test Software, I/O Interface, Manager Components, Memory Components, Authorization, Audit, Crypto Components, Archive, Security, Test*.

Subcomponent Name	Description
Security Devices	Collects all devices controlling the external environment. Malicious conditions of the TOE shall be prevented by either informing the software or driving the TOE in a secure state.
Core	Contains Central Processing Unit (CPU), Memory Management Unit (MMU), and Memory Encryption/Decryption Unit (MED)
Peripherals	Contains Random Number Generator (RNG), Timer, Interrupt module, LPC module, and Input logic.
Memory	Contains ROM, XRAM, and EEPROM.
Coprocessors	Contains the coprocessors for cryptographic operations: Advanced Crypto Engine (ACE), DDC accelerator, HASH, and Checksum module.
Bus System	Enables components and subcomponents to communicate with each another.
Self-Test Software	Contains the modes Start-up, user mode, chip ident mode, and test mode.
I/O Interface	Handles all access to the peripherals.
Manager Components	Contains modules TPM-Dispatcher, TPM-Command, and the State-Machine.
Memory Components	Manages the memory space.
Authorization	Implements different authorisation protocols.
Audit	Reports a log of audit events.
Crypto Components	Provides SHA-1, 3DES calculation and key management
Archive	Saves data in EEPROM which must be accessible after a powerless state.
Security	Supports the activation/deactivation of some HW security features and the interrupt service routine.
Test	Provides different test procedures to check the correct function of specific components of the TOE including the self-test.

More details of the architecture can be found in chapter 2 of the ST, which is attached as part D of this certification report.

6 Documentation

The following documentation is provided with the product by the developer to the consumer:

- SLD9630TT1.1 Preliminary Databook, V2.1, Feb 2003
- Trusted Computing Platform Alliance Main Specification, version 1.1b, 2002-02-22
- Low Pin Count (LPC) Interface Specification, version 1.0, 1997-09-29, by Intel
- SLD9630TT Specification of the LPC-I/O communication protocol, version 03.02, by Infineon Technologies AG

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 SLD9630TT1.1.

Testing approach:

- In the course of the development of the TOE the simulation tests are carried out. The HW simulation tests yield CRC sums, which are used in the further testing. Furthermore the software components undergo continuous testing by simulation and emulation.
- For each mask version a qualification/characterisation test is performed in order to decide, whether the TOE is released to production. Via the results of these tests a qualification/characterisation report is generated.
- As the qualification/characterisation testing is done in the test mode of the TOE an additional testing in user mode is necessary to verify the functionality of the final TOE with the integrated software (operating system). The tests in the test mode are designed with the goal to separate different functions and to show the root cause of a detected malfunction very fast. The verification in user mode tests the functionality of the software and tries to simulate the end user environment.
- Before delivery on every chip production tests are performed. These tests use the CRC sums attained by the simulation tests. The aim of these tests is to check whether each chip is functioning correctly.

- The software is developed in a software development environment using tools like software simulator, bond-out emulator and the final chip. The positive result of the software regression test suite is a prerequisite of the production release.

Amount of developer testing performed:

- The tests are performed on component level and therefore can be mapped to mechanisms and security function.

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. If one of the production tests (performed on every TOE) would fail, the TOE would not be delivered, but logically destroyed.

Tests of the evaluation body:

The independent testing of the evaluation body was partly performed in the developer's testing environment and partly at TÜViT GmbH, information security department, in Essen. 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 the whole campaign from the developer's tests and additionally add independent tests.

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 and at TÜViT premises. 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.

In the intended environment of use the TOE does not feature any exploitable vulnerabilities in the meaning of the security target for typical attackers possessing a low attack potential, if all the measures required are taken into consideration.

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

After delivery the TOE only features one fixed configuration (user mode), which cannot be altered by the user. 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].

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	n.a.[5]
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

[5] n.a. = not applicable

Assurance classes and components		Verdict
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 security requirements are taken from part 2 and part 3 [CC]. Thus, the component ADV_SRE.1 is not applicable. All other assurance components were 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.

All functional security requirements are taken from sections 2.2.6, 2.3, 5.2.3, 5.2.5 of the TCPA Trusted Platform Module Protection Profile [TCPA TPM PP].

All TOE security functional requirements are listed in section 5.1.1 or the security target [ST] and section 5.2 of the TCPA Trusted Platform Module Protection Profile [TCPA TPM PP]:

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

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

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.

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 "*SLD9630TT1.1 / M2009*". The validity can be extended to new versions and releases of the product, 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

There are no evaluation stipulations, comments, or recommendations.

11 Certification Stipulations and Notes

There are no stipulations.

12 Security Target

The security target [ST] for *SLD9630TT1.1 / M2009* is included in part D of this certification report.

13 Definitions

13.1 Acronyms

ACE	Advanced Crypto Engine
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
EAL	Evaluation Assurance Level
EEPROM	Electrical Erasable and Programmable Read Only Memory
ES	Embedded Software
FSP	Functional Specification
HLD	High-level Design
IC	Integrated Circuit
IGS	Installation, Generation and Start-up
OS	Operating System
OSP	Organisational Security Policy

PC	Personal Computer
PCCON	TCPA PC Connection Module
PP	Protection Profile
RAM	Random Access Memory
ROM	Read Only Memory
RSA	Signature Algorithm of Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SIF	Sub-interface
SOF	Strength of Function
SS	Sub-system
ST	Security Target
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
XRAM	Extended RAM

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from Part3 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

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

[CC] ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security,
ISO/IEC 15408-1:1999 (E), Part 1: Introduction and general model
ISO/IEC 15408-2:1999 (E), Part 2: Security functional requirements
ISO/IEC 15408-3:1999 (E), 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 1.0, revision August 1999

[ETR] Evaluation Technical Report, version 1.0, 2004-01-21, TÜV Informationstechnik GmbH, document-number: 20468884_TÜV_040.01

[ST] ASE - Security Target – Evaluation Documentation - SLD9630TT1.1 / M2009 - Security Target, Version 1.0, 2003-09-01

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

Part C

Excerpts from the Criteria

The excerpts from the criteria are dealing with

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

CC Part 1:

Conformance results (section 5.4 of CC part 1 with final interpretation 008)

„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.“

CC Part 3:

Assurance categorisation

The assurance classes, families, and the abbreviation for each family are shown in *Table 1*.

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 1: 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 2 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 2: 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 document: “Evaluation Documentation – SLD9630TT1.1 / M2009 - Security Target”

Author: Infineon Technologies AG

Date: 2003-09-01

Version: 1.0

Public

Infineon Technologies AG

Secure Mobile Solutions

Evaluation Documentation

SLD9630TT1.1 / M2009

Security Target

Version 1.0

Date 01.09.2003

Filename: SLD9630TT11_SecTar.doc
Autor: Jürgen Noller, SMS OP PS

Revision History:

Version	Date	Subject
0.1	02-07-2003	Initial revision
0.2	04-08-2003	FMT_SMF.1 added
1.0	01-09-2003	Comments from TüVIT added

List of Contents

List of Tables

List of Figures

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 profile 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 Security Target Identification

The title of the security target (ST) is SLD9630TT1.1 / M2009 Security Target. The security target has the revision 1.0 and is dated 01.09.2003.

The Target of Evaluation (TOE) is a security IC (Security Controller) with integrated firmware, which is named SLD9630TT1.1, is internally registered under the development code M2009B21 and has the version number B21.

The Security Target is based on the Protection Profile TCPA TPMPP v1.9.7 [PP].

The Protection Profile and the Security Target are built in accordance with Common Criteria V2.1.

	Version number	Date	Registration
Security Target	1.0	01.09.2003	SLD9630TT1.1/M2009B21 Security Target
Target of Evaluation			SLD9630TT1.1
Hardware	B21		M2009B21
Firmware	1.07		1.07
Protection Profile	1.9.7	01-07-2002	TCPA TPMPP v1.9.7
Common Criteria	2.1		

Table 1: Identification

1.2 Security Target Overview

This Security Target (ST) describes the target of evaluation (TOE) known as the Infineon SLD9630TT1.1 Trusted Platform Module (TPM) and gives a summary specification.

The SLD9630TT1.1 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 within a Trusted Computing Platform. The SLD9630TT1.1 is a complete solution implementing the version 1.1b of the Trusted Computing Platform Alliance specifications (TCPA). The SLD9630TT1.1 uses the LPC interface (Low Pin Count) as defined by Intel for the integration into existing PC mainboards. The SLD9630TT1.1 is basically a secure controller with the following added functionality:

- Random number generator
- Asymmetric key generation (RSA keys with key length up to 2048 bit)
- Symmetric and asymmetric key procedures (encryption/decryption, generation and verification of digital signatures)
- Hash algorithms (SHA-1, HMAC)
- Secure key and data storage
- Identification and Authentication mechanisms

In this security target the TOE (target of evaluation) is described and a summary specification is given. The security environment of the TOE is defined. The assets are identified which have to be protected through the security policy. The threats against these assets are described. The security objectives as the objectives of the security policy are defined as well as the security requirements. The applicable IT security requirements are taken from the Common Criteria, with appropriate refinements. The security requirements are build up of the security functional requirements as part of the security policy and the security assurance requirements as the steps during the evaluation and certification to show the TOE meets its requirements. The functionality of the TOE to meet the requirements is described.

The assets, threats, security objectives and the security functional requirements are defined in the Trusted Computing Platform Alliance (TCPA) Trusted Platform Module Protection Profile (TCPA TPMPP v1.9.7) and are referenced here.

The TOE summary specification consisting of the security enforced functions, the assurance measures and the security function policies are defined in the ST as property of this specific TOE, the SLD9630TT1.1. The rationale presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment.

The TPM works with a second module called the TCPA PC Connection (PCCON), which may include the PC system BIOS and other software. There is no coverage for the PCCON.

1.3 CC Conformance

This security target is conformant to chapter 5.4 of Common Criteria V2.1(ISO15408) part 1.

The TOE is conformant to Common Criteria V2.1 (ISO15408) part 2 and part 3.

The assurance level for the TOE is EAL 3 augmented with components ALC_FLR.1 and ADV_SPM.1.

The strength of function is basic.

This security target is in conformance to the protection profile TCPA TPMPP v1.9.7 [PP]. The certification of the protection profile TCPA TPMPP v1.9.7 is done from Security Evaluation Laboratory CygnaCom Solutions, Inc., Report CCEVS-VR-02-0022, Version 1.0, dated 10.Juli 2002.

The security assurance requirements of the TOE are according to the protection profile TCPA TPMPP v1.9.7. They are all drawn from Part 3 of the Common Criteria V2.1.

The assurance level of the [PP] is EAL3 augmented, the strength of function is basic.

Assurance-class	**Assurance components**	**Description**
Development	**ADV_SPM.1**	Informal TOE security policy model
Life cycle support	**ALC_FLR.1**	Basic flaw remediation

Table 2: Augmentations of the assurance level of the TOE

2 Description of the Target of Evaluation (TOE)

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. The following is a more detailed description of the TOE than in the TCPA TPMPP v1.9.7 as it belongs to the specific TOE.

2.1 Product Overview

The SLD9630TT1.1 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 [TCPA]. The SLD9630TT1.1 is a complete solution implementing the Trusted Computing Platform Alliance specification [TCPA] which is an industry group founded in 1999 by COMPAQ, HP, IBM, Intel, Microsoft and now including more than 160 companies.

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 TCPA subsystem is a trusted subsystem that is an integral part of a computing platform. The evaluated components that make up the TCPA 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 Trusted Platform Support Services (TSS) and the connection between them. 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 TSS is a set of functions and data that are common to all types of platforms, which are not required to be trustworthy.

The Target of Evaluation (TOE) of this security target is the “Infineon SLD9630TT1.1 Trusted Platform Module” called “SLD9630TT1.1” or “TPM” in the following description. The SLD9630TT1.1 is a complete solution implementing the TPM requirements of the Trusted Computing Platform Alliance Main Specifications version 1.1b [TCPA].

The SLD9630TT1.1 is basically a secure controller with the following added security capabilities, protocols and functions:

- Random number generation (RNG)

  The RNG capability is only accessible for 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.

- Algorithms: RSA, SHA-1, DES

  The SLD9630TT1.1 supports the RSA algorithm for encryption and digital signatures with key sizes of 512 to 2048 bits. The RSA implementation provides protection and detection of failures during the Chinese Remainder Theorem (CRT) process. The TPM storage keys and TPM identity keys are of strength equivalent to a 2048 bit RSA key. A storage key whose strength is less than that of a 2048 RSA key could not be stored in the SLD9630TT1.1. The TPM identity keys are RSA keys with key size of 2048 bits.

  The RSA algorithm is used for signature and verification operations according PKCS#1 V2 for the format and design of the signature output.

  The SLD9630TT1.1 supports the Secure Hash Algorithm-1 (SHA-1) hash algorithm as defined by United States Federal Information Processing Standard 180-1. The output of

the SHA-1 is a 160 bit hash value and all areas that expect a hash value are required to support the full 160 bits.

The SLD9630TT1.1 supports the DES and Tripple-DES algorithm with key sizes of 56, 112 and 168 bits for encryption and decryption. The function is used to support the temporary cashing of keys outside the TPM and for the personalisation of code and data.

Key Generation

The SLD9630TT1.1 generates asymmetric key pairs (algorithm RSA) in accordance with P1363. The generation function is a protected capability and the private key is held in a shielded location.

For the HMAC key generation and for the creation of all nonce values the next n bits are taken from the internal TPM RNG.

Key and Data Storage

The SLD9630TT1.1 has the capability of secure storage 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 cannot be any bigger than the key size used to encrypt it. The functionality of the SLD9630TT1.1 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. The keys may be migratable or non-migrateble. A migratable key is a key that may be transported outside a 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 the 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 to RSA encrypt and RSA decrypt 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.
- The Endorsement Key pair, which is an asymmetric key pair inserted in the SLD9630TT1.1 during the production phase, is used as proof that a TPM is a genuine TPM.
- Symmetric keys used for production, personalisation and key cashing.

- Self-Tests

  The SLD9630TT1.1 provides startup 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 (according FIPS 140-1).
  - Reading and extending the integrity registers.
  - Endorsement key pair integrity. This test verifies the RSA sign and verify engine by signing and verifying a known value with the endorsement key pair.
  - Integrity of the protected capabilities of the SLD9630TT1.1 by checking a hash value of the “microcode” (TPM firmware) to ensure that the microcode has not changed.
  - Test of the tamper-resistance markers.

  If a failure during any self-test is detected, the part experiencing the failure will enter a shutdown mode and an error code is returned.

- 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 TCPA specification calls the identification and authentication process and this data authorization.

  The identification and authentication (authorization) data for the TPM Owner and the owner of the Storage Root Key are held within the TPM itself. The identification and authentication (authorization) 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.

- Access control

Access control is enforced in the SLD9630TT1.1 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 different flags (TCPA_AUTH_DATA_USAGE, TCPA_KEY_FLAGS, TCPA_KEY_USAGE). The TCPA_AUTH_DATA_USAGE flag defines access as either owner or world. Owner must be authenticated with a shared secret. World means that usage of the key is permitted by anyone without authentication. The TCPA_KEY_FLAGS define whether a key is a migratable or a non-migratable key and whether the key is stored in volatile storage and must be unloaded at TPM startup. The TCPA_KEY_USAGE flag identifies the key type. Depending on the key type, certain operations may or may not be allowed using the particular key. Upon appropriate identification and authentication associated with the keys, users can use the key for the purposes permitted by the TCPA_KEY_USAGE flag.

- 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 TCPA_KEY_FLAGS.
  - TCPA_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 TCPA_KEY_USAGE, which indicates if the data is a key or key pair and the type of key.
  - Volatility attribute, which defines whether the data must be stored in volatile or non-volatile storage and if it is cleared at TPM startup. This security attribute is stored in TCP_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 the data originated at this TPM,
  - PCR values,
  - TPM owner/SRK 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.

Each SLD9630TT1.1 is identified and validated by its Endorsement Key. The Endorsement Key is an asymmetric key pair that is used as proof that an SLD9630TT1.1 is genuine. The Endorsement Key pair is generated and encrypted (using Tripple-DES algorithm) outside the SLD9630TT1.1 in a secure environment by the manufacturer Infineon Technologies and then

loaded encrypted into the SLD9630TT1.1 during the production phase. The Endorsement Key is transitively bound to the Platform via the SLD9630TT1.1 as follows:

1. An Endorsement Key is bound to one and only one SLD9630TT1.1 (i.e., that is a one to one correspondence between an Endorsement Key and a SLD9630TT1.1.)
2. A SLD9630TT1.1 is bound to one and only one Platform, (i.e., there is a one to one correspondence between a SLD9630TT1.1 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.

To simplify system integration into existing PC mainboards, the SLD9630TT1.1 uses the LPC interface (Low Pin Count) as defined by Intel.

With these capabilities, the SLD9630TT1.1 is able to realize the issue of [TCPA] to insert a trusted subsystem – called the “root of trust” – into the PC platform, which is able to extend its trust to other parts of the whole platform by building a “chain of trust”, where each link extends its trust to the next one. As a result, the TPM extends its trustworthiness, providing a Trusted PC for secure transactions. As an example the TPM is able to calculate hash-values of the BIOS at boot time as an integrity metric. Once this metric is available, it is saved in a secure memory location. Optionally, it could be compared to some predefined values and the boot process could be aborted on mismatch.

During the boot process, other integrity metrics are collected from the platform, e.g. the boot loader and the operating system itself. Device drivers may be hashed, even hardware like PCI cards can be detected and identified. Every metric obtained is concatenated to the already available metrics. This gives a final metric, which describes the operational state of the whole platform and the state of its system integrity.

A challenger may now ask the platform for these metrics and make informed decisions on whether to trust it based on the metric values obtained. To support the privacy issue, the user of the platform may restrict the SLD9630TT1.1 in answering to any challenge, but the user is never able to make the SLD9630TT1.1 report false metrics. Moreover, the user is able to create several identities for his interactions.

Offering these features to a system, the SLD9630TT1.1 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 SLD9630TT1.1 asymmetric encryption functionality. Regarding a network scenario, the client PCs equipped with an SLD9630TT1.1 are able to report their platform status to the server so that the network administration is aware of the their trustworthiness. In conclusion, the SLD9630TT1.1 acting as a service provider to a system helps to make transactions more secure and trustworthy.

The Target of Evaluation (TOE), the SLD9630TT1.1, consists of the following hardware and firmware components.

The hardware of the SLD9630TT1.1 is based on the SLE66CXXXXX architecture with additional components. The hardware is manufactured by the Infineon Technologies AG in a 0,22 µm CMOS technology. As a side effect of this porting the most components are unchanged.

The IC, whose block diagram is shown in Figure 1, consists of a dedicated microprocessor (CPU) with a MMU (Memory Management Unit), several different memories, security logic, shield, a timer, an interrupt-controlled I/O interface and a RNG (**R**andom **N**umber **G**enerator) are integrated on the chip. Additionally, a hardware hash accelerator and a specialized interface the Low Pin Count interface (LPC) have been added. This LPC interface is the main interface of the chip.

The CPU is compatible with the SAB 8051 instruction set and is 6 times faster than the standard processor. The memory comprises 256 bytes of internal RAM (IRAM), 8 kByte of extended RAM (XRAM), 64 kByte of user ROM, 8 kByte of test ROM and 64 kByte of EEPROM. It thus meets the requirements of the new generation of operating systems. The CPU accesses the memory via the integrated **M**emory **E**ncryption and **D**ecryption unit (MED). The access rights of the application to the memories can be controlled with the memory management unit (MMU). Security, sleep mode and interrupt logic as well as the RNG are specially designed for secure applications. The sleep mode logic is used to reduce the overall power consumption. The SLD9630TT1.1 uses an external clock of 33 MHz where is compliant to the definition of the LPC interface. The PLL unit allows to operate the core controller of the SLD9630TT1.1 with a multiplication factor over the divided external clock signal or free running with maximum frequency. The checksum module allows simple calculation of checksums per ISO 3309 (16 bit CRC).

Three modules for cryptographic operations are implemented on the TOE. The ACE (Advanced Crypto Engine) for calculation of asymmetric algorithms like RSA. This module is especially designed for high-performance applications with respect to the security and power consumption The DDC module provides the DES algorithm. This module computes the complete DES algorithm within a few clock cycles. The DDC is especially designed to counter attacks like DPA or EMA. The third module named HASH provides the Secure Hash Algorithm-1 (SHA-1).

To sum up, the TOE is a powerful security IC with a large amount of memory and special peripheral devices with both improved performance and optimised power consumption at minimal chip size.

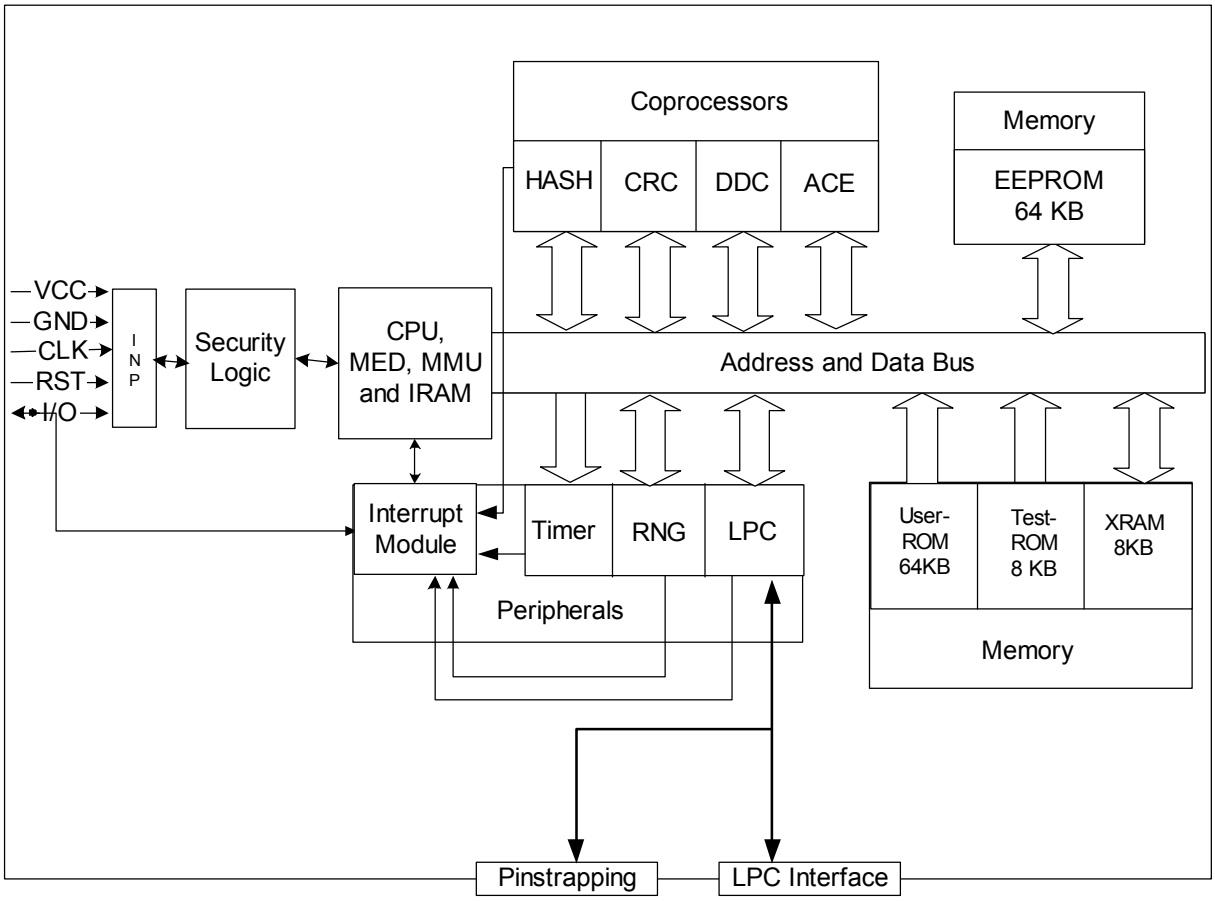

Figure 1: Block diagram of the SLD9630TT1.1

The firmware required for operating the chip includes an operating system which provides the TCPA functionality specified in the [TCPA]. The chip initialisation routine with security checks and identification mode as well as test routines for production testing are located in a separate test ROM. The firmware also provides the mechanism for updating the protected capabilities once the TOE is in the field as defined in the TPM_FieldUpgrade command of the [TCPA]. The field upgrade can only be downloaded to the chip if it has been encrypted and signed by the manufacturer Infineon Technologies AG. Figure 2 shows the firmware block diagram of the SLD9630TT1.1.

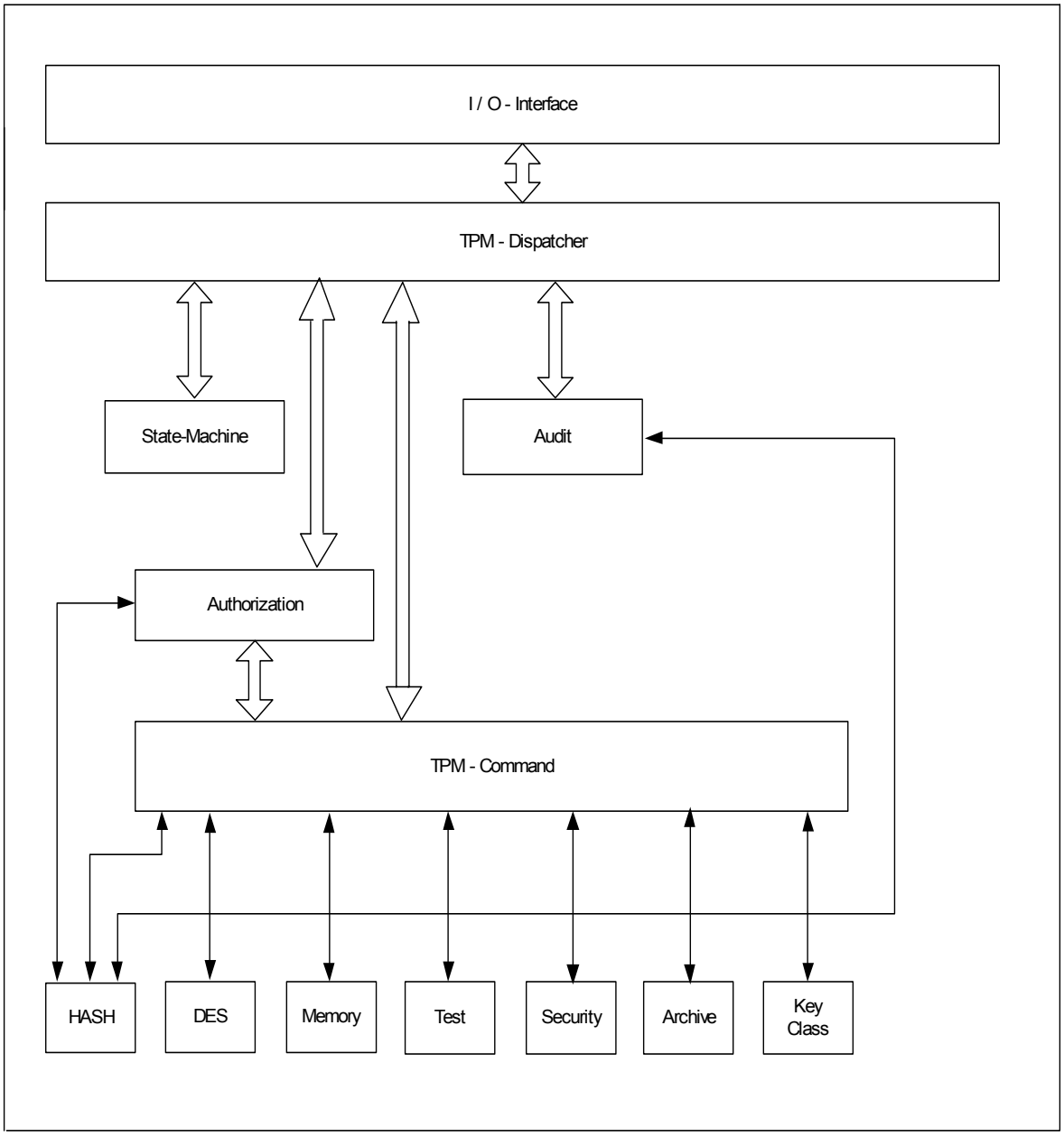

Figure 2: Firmware block diagram of the SLD9630TT1.1

2.2 Scope of the TOE

The TOE manufactured by Infineon Technologies, comprises the *hardware* of the security controller, type SLD9630TT1.1, and the associated *firmware* required for operation provided in ROM and EEPROM.

2.2.1 Hardware of the TOE

The *hardware part* of the TOE (cf. Figure 1) as defined in [PP] is comprised of:

- Security logic (SEC)
- Microcontroller type ECO 2000 (CPU) with the subcomponents memory encryption and decryption unit (MED), memory management unit (MMU) and 256 bytes of internal RAM (IRAM)
- External memory comprising:
  - 8 kByte extended RAM (XRAM)
  - 64 kByte user ROM, including the routines for chip management (RMS)
  - 8 KB test ROM containing the test routines (STS), and
  - a total of 64 kByte non-volatile memory (EEPROM)
- Random number generator (RNG)
- Checksum module (CRC)
- Interrupt module (INT)
- Timer (TIM)
- Address and data bus (BUS)
- ACE for long integer modulo calculations, which are used in asymmetric algorithms like RSA
- DES accelerator (DDC) used for fast calculations of the DES algorithm
- Low Pin Count interface (LPC)
- Hash accelerator (HASH) for the algorithms SHA-1

2.2.2 Firmware of the TOE

The entire *firmware* of the TOE consists of two different parts. The one is the operating system called firmware in the following document. The firmware includes operating system and the Endorsement Key and is used to operate the IC. The firmware includes also the capability for updating the protected capabilities once the TOE is in the field (TPM_FieldUpgrade). The other is the Self Test Software (STS). The STS routines are stored in the especially protected test ROM and are not accessible for the user software (application).
The entire *firmware* of the TOE (cf. Figure 2) as defined in [PP] is comprised of:

- I/O-Interface
- TPM-Dispatcher
- State-Machine
- Audit
- Authorization
- TPM-Command
- HASH
- DES
- Key Class
- Memory
- Security
- Archive
- Test

2.2.3 Guidance documentation

The guidance documentation consists of a set of information containing the description of all interfaces to operate the TOE. The list of guidance documentation is given in chapter 9.1.

2.2.4 Forms of delivery

The TOE is delivered in form of complete chips including the hardware, the firmware (operating system) and the Endorsement Key Pair. The TOE is finished and the extended test features are removed.

2.2.5 Production sites

The TOE may be produced in different production sites. The chip layout is not changed in this case and also the production testing does not differ. The delivery measures are described in the ALC_DVS aspect.

3 TOE Security Environment

3.1 Assets

The primary assets concern the TSF and the User Data that includes the data as well as program code (Embedded Firmware). This assets has to be protected while being executed as well as when the TOE is not in operation. This leads to the following primary assets:

- Embedded Firmware
- User Data
- TSF Data
- Hardware of TOE

3.2 Subjects and Objects

This chapter shows the subjects and objects where are relevant to the TOE.

The objects are:

Obj1 Embedded Firmware of the TOE

Obj2 User Data (user keys and data)

Obj3 Endorsement Key Pair

Obj4 Storage Root Key

Obj5 Keys

Obj6 Authentication Data

Obj7 Security Attributes

Obj8 Shielded Locations (contents)

The subjects are:

Sub1 Manufacturer (Infineon Technologies AG)

Sub2 Administrator

Sub3 User

Sub4 Attacker

3.3 Assumptions

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 assumptions and the assumptions for the IT environment are defined in the [PP] chapter 3.1.

The TCPA subsystem, in which the TPM is used, is a trusted subsystem that is an integral part of a computing platform. The evaluated components that make up the TCPA 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 TPM, the Connection module, and the Trusted Platform Support Services (TSS).

In general the TPM provides cryptographic capabilities and protected storage.

The Connection module (PCCON) provides the connection to the computing platform and the Root of Management Trust (RMT). The TPM relies on the PCCON module for all communication with the platform and for the 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 and therefore do not need to be part of the TPM.

3.4 Threats

The threats are directed against the assets.

The threats to security are defined in the [PP] chapter 3.2, no other threats are added.

3.5 Organisational Security Policies

No organisational security policies are defined.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives are defined and described in the [PP] chapter 4.1, no other security objectives are added.

4.2 Security Objectives for the Environment

The security objectives for the environment are described in the [PP] chapter 4.2, no other security objectives for the environment are added.

5 IT Security Requirements

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

The security functional requirements of the TOE are defined and described in the [PP] chapter 5.1 and 5.2. All assignments and selections of the security functional requirements are done in the [PP] with the exception of FDP_ACF.1.3, FDP_ACF.1.4, FDP_ETC.2.4, FDP_ITC.2.5, FMT_MOF.1.1 and FMT_SMF.1.

FDP_ACF.1.3: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

a) The execution of the commands TPM_ChangeAuthAsymStart, TPM_TakeOwnership, TPM_Seal, TPM_Unseal, TPM_LoadKey, TPM_CreateWrapKey and TPM_MakeIdentity depends on the values of the security attribute TCPA_KEY_FLAGS.

b) *The execution of the commands TPM_ChangeAuthAsymStart, TPM_MakeIdentity, TPM_TakeOwnership and TPM_CreateWrapKey depends on the values of the security attribute TCPA_KEY_USAGE.*

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

FDP_ETC.2.4: The TSF shall enforce the following rules when user data is exported from the TSC:

a) *A key may be encrypted for migration only if the migratable flag is set in TCPA_KEY_FLAGS.*

b) *A key may be exported to a key cash with the command TPM_SaveKeyContext.*

c) *An identity key may be exported with the command TPM_MakeIdentity.*

FDP_ITC.2.5: The TSF shall enforce the following rules when importing user data controlled under SFP from outside the TSC:

a) *A key may be imported from a key cash with the command TPM_LoadKeyContext.*

FMT_MOF.1.1: The TSF shall restrict the ability to disable or enable the functions: *prevent any entity from reading the PUBEK, enable/disable a TPM, disable the TPM_OwnerClear function and disable/enable auditing for a command to the TPM owner.*

FMT_SMF.1 Specification of management functions

Hirarchical to: No other components

FMT_SMF.1.1: The TSF shall be capable of performing the following security management functions: usage of the relevant firmware function calls as defined in [TCPA] to manage the security attributes, security functions and TSF data.

Dependencies: No dependences

5.1.2 TOE Security Assurance Requirements

The security assurance requirements of the TOE are the assurance components of the Evaluation Assurance Level 3 (EAL3) augmented with the components *ADV_SPM.1* and *ALC_FLR.1*. They are all drawn from the Common Criteria V2.1 (ISO15408) part 3. The assurance components are listed in Table 3.

#	Name	Description
1	ACM_CAP.3	Authorization controls
2	ACM_SCP.1	TOE CM coverage
3	ADO_DEL.1	Delivery procedures
4	ADO_IGS.1	Installation, generation and start-up procedures
5	ADV_FSP.1	Informal functional specification
6	ADV_HLD.2	Security enforcing high-level design
7	ADV_RCR.1	Informal corresponding demonstration
8	ADV_SPM.1	Informal TOE security policy model (augmented)
9	AGD_ADM.1	Administrator guidance (refined)
10	AGD_USR.1	User guidance (refined)
11	ALC_DVS.1	Identification of security measures
12	ALC_FLR.1	Basic flaw remediation (augmented)
13	ATE_COV.2	Analysis of coverage
14	ATE_DPT.1	Testing: high-level design
15	ATE_FUN.1	Functional testing
16	ATE_IND.2	Independent testing – sample
17	AVA_MSU.1	Examination of guidance
18	AVA_SOF.1	Strength of TOE security function evaluation
19	AVA_VLA.1	Developer vulnerability analysis

Table 3: Assurance components

The assurance requirements defined in Table 3 are defined in chapter 5.3 of the [PP].

The refinements regarding assurance requirements *AGD_ADM.1* and *AGD_USR.1* are refined in the text below.

Refinement regarding Administrator Guidance (AGD_ADM.1):
The guidance documents must not contain security relevant details that 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.

Refinement regarding User Guidance (AGD_USR.1):
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.

5.2 Security Requirements for the IT Environment

There are no security requirements for the IT environment defined.

5.3 Security Requirements for the Non-IT Environment

There are no security requirements for the non-IT environment defined.

5.4 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.

6 TOE Summary Specification

The product overview is given in chapter 2.1. In the following the security functionality and the assurance measures of the TOE are described.

6.1 TOE Security Enforced Functions

This chapter contains the definition and description of the security enforcing functions (SEF) of the TOE. The TOE provides five security enforcing functions (SEF) to meet the security functional requirements. The functions are:

SEF1: Cryptographic Support
SEF2: Authentication and Identification
SEF3: Access Control
SEF4: Origin
SEF5: TSF Protection and Test

6.1.1 SEF1 - Cryptographic Support

There are six functions within the TOE related to cryptographic support: generation of random numbers, generation of asymmetric key pairs, RSA digital signature, data encryption and decryption, key destruction and the generation of hash values.

The TOE supports the generation of random numbers with its internal random generator. The random numbers are generated from an analogue circuit and are undertaken a digital post-processing function.

The TOE supports the generation of cryptographic keys in accordance with the specified cryptographic key generation algorithm RSA and specified cryptographic key sizes RSA 512 to 1024, 1280 and 2048 bits. The source of randomness is the internal random generator (RNG).
The covered security functional requirement is FCS_CKM.1.

The TOE supports the destruction of cryptographic keys by erasure of volatile memory areas containing cryptographic keys in accordance with FIPS 140-1, Section 4.8.5.
The TOE supports the RSA encrypt and decrypt operation in accordance with the specified cryptographic algorithm RSA and cryptographic key sizes RSA 512 to 1024, 1280 and 2048 bits that meet PKCS#1 V2.
The TOE supports the encrypt and decrypt operation in accordance with the specified cryptographic algorithm DES and Tripple-DES and cryptographic key size of 56, 112 and 168 bits. The covered security functional requirement is FCS_COP.1.
The TOE supports the RSA signature generation and verification in accordance with the specified cryptographic algorithm RSA and cryptographic key sizes RSA 512 to 1024, 1280 and 2048 bits that meet PKCS#1 V2. The TOE uses the internal RNG as the source for any randomness that the process may require.

The TOE supports the secure hash in accordance with the specified cryptographic algorithm SHA-1 that meet FIPS 180-1 and the calculation of keyed-hashing message authentication code (HMAC) in accordance with the specified cryptographic algorithm SHA-1 and crypto-

graphic key sizes 160 bits that meet RFC 2104.
The covered security functional requirement is FCS_CKM.4.

The SEF1 covers the following security functional requirements: FCS_CKM.1, FCS_CKM.4 and FCS_COP.1. The SEF1 “Cryptographic Support” does not use probabilistic or permutational effects.

6.1.2 SEF2 - Authentication and Identification

The TPM 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 TPM. The basic premise is to prove knowledge of a shared secret. This shared secret is the identification and authentication data which is called authorization data in the [TCPA]. 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 first protocol is the “*Object-Independent Authorization Protocol*” (OI-AP), which allows the exchange of nonces with a specific TPM. Once an OI-AP session is established, its nonces can be used to authorize the use any entity managed by the TPM. The session can live indefinitely until either party request the session termination. The TPM_OIAP function starts the OI-AP session.

The second protocol is the “*Object Specific Authorization Protocol*” (OS-AP)”. The OS-AP allows establishment of an authentication session for a single entity. The session creates nonces that can authorize multiple commands without additional session-establishment overhead, but is bound to a specific entity. The TPM_OSAP command starts the OS-AP session. The TPM_OSAP specifies the entity to which the authorization is bound.

Any operational role can access all protected functions (i.e. commands) and shielded locations only through the authentication mechanism, i.e., by supplying the appropriate authentication token. The access-right of commands, data and keys are defined by different security attributes.
The covered security functional requirement is FIA_ATD.1.

The TOE prevents the reuse of authentication related to authorization data by using *nonces* for each message and response of all authorization protocols. The 20 bytes long *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.
The covered security functional requirements are FIA_UAU.4 and FIA_UAU.6.

The TOE 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. Each user has to be successfully authenticated/identified before allowing any other TSF-mediated actions on behalf of that user.
To control the TPM without conventional authentication information (e.g. there is no owner or the authentication information has been lost), the TPM supports the possibility of authentication with physical presence (of a person) at the platform by using a physical/electrical

method. This feature could be disabled by command.
The covered security functional requirements are FIA_UAU.1 and FIA_UID.1.

The SEF2 covers the following security functional requirements: FIA_ATD.1, FIA_UAU.1 FIA_UAU.4, FIA_UAU.6 and FIA_UID.1. The SEF2 “Authentication and Identification” uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF “basic”.

6.1.3 SEF3 – Access Control

The TOE provides the security function policy *Protected Operations Access Controls* (POAC) to protect the sensitive subjects, objects and operations of the TOE. The POAC is described in chapter 6.2.
The covered security functional requirement is FDP_ACC.1.

The TOE enforces the POAC on subjects (commands), objects (keys and user data) and operations (signature generation, encryption or decryption) based on different security attributes. The security attribute TCPA_AUTH_DATA_USAGE defines the access to key and data. The security attribute TCPA_KEY_USAGE defines the admitted cryptographic operations of keys and authorises the access to the following commands: TPM_CreateWrapKey, TPM_ChangeAuthAsymStart, TPM_MakeIdentity and TPM_TakeOwnership. The security attribute TCPA_KEY_FLAGS defines the indication of migration and volatile of keys and authorises the access to the following commands: TPM_TakeOwnership, TPM_Seal, TPM_Unseal, TPM_LoadKey, TPM_CreateWrapKey, TPM_SaveState and TPM_MakeIdentity.
The covered security functional requirement is FDP_ACF.1.

The export and import of user data, controlled under the SFP, is done under control of the POAC. The 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 following rules are enforced when exporting and importing keys:

- The encryption of a key for migration is only possible if the migratable flag for this key is set in TCPA_KEY_FLAGS.
- The TPM supports the capability of saving keys outside the TPM (key-cash). The TPM_SaveKeyContext command encrypts a key and the associated attributes within the TPM and exports them. The import from the key-cash into the TPM is done with the TPM_LoadKeyContext command. The command decrypts the key and its associated attributes within the TPM. The algorithm used for the key encryption/decryption is the Tripple-DES algorithm with a key size of 168 bits. The key is unique for each TPM and stored within the TPM.
- The TPM_MakeIdentity command exports an identity key encrypted with the public part of the SRK. The Import and decryption is done with the TPM_LoadKey command. Note that the decryption of the key outside the TPM is not possible because the private part of the SRK is a non-migratable key that never leaves the TPM.

The covered security functional requirement is FDP_ETC.2 and FDP_ITC.2.

The TOE 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

specific memory area.
The covered security functional requirement is FDP_RIP.2.

The SEF3 restrict the ability to disable or enable the following functions to the TPM owner:

- prevent any entity from reading the PUBEK
- enable/disable a TPM
- disable the TPM_OwnerClear function
- disable/enable auditing for a command

The covered security functional requirement is FMT_MOF.1.

The POAC restrict the ability to create the security attributes (TCPA_KEY_USAGE, TCPA_AUTH_DATA_USAGE, migratable flag and volatility flag) associated with a particular entity to the entity owner.
The covered security functional requirement is FMT_MSA.1.

The SEF3 ensures that only secure values are accepted for the security attributes.
The covered security functional requirement is FMT_MSA.2.

The POAC provides default values for security attributes for the associated key (SRC and identity key). The values are defined in Table 4. The change of this default values by the entity owner is not allowed.

Security attribute	Key	Default Value
TCPA_KEY_FLAGS->migratable	SRK	0x00000000[1]
TCPA_KEY_USAGE	SRK	TPM_KEY_STORAGE[2]
TCPA_KEY_FLAGS->migratable	Identity key	0x00000000[3]
TCPA_KEY_USAGE	Identity key	TPM_KEY_IDENTITY[4]

Table 4: Default values of security attributes

The covered security functional requirement is FMT_MSA.3.

The SEF3 restrict the ability to modify the following TSF data to the TPM owner:

- Identification and Authentication data associated with the Storage Root Key
- Migration authorization

The SEF3 restrict the ability to generate the following TSF data to the TPM owner:

- Storage Root Key
- tpmProof

The SEF3 restrict the ability to modify the following TSF data to the entity owner:

- Identification and Authentication data associated with entity

[1] See [TCPA] chapter 4.12

[2] See [TCPA] chapter 4.10, the value is 0x0011

[3] See [TCPA] chapter 4.12

[4] See [TCPA] chapter 4.10, the value is 0x0012

The SEF3 restrict the ability to generate the following TSF data to the TPM manufacturer Infineon Technologies AG:

- Endorsement Key Pair

The covered security functional requirement is FMT_MTD.1.

The TOE supports the roles: TPM owner and owners of entities. The role is bound always on specific authentication token, for the TPM owner it is the TPM ownership token and for the entity owner it is the entity token. The roles are enforced within the TOE because there are specific commands and specific keys bound to different token.
The TOE supports the role TPM manufacturer during the production phase of the TPM. The covered security functional requirement is FMT_SMR.2.

The SEF3 covers the following security functional requirements: FDP_ACC.1, FDP_ACF.1, FDP_ETC.2, FDP_ITC.2, RDP_RIP.2, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_SMR.2 and FMT_SMF.1
The SEF3 “Access Control” does not use probabilistic or permutational effects.

6.1.4 SEF4 – Origin

The SEF4 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. The identity keys used as signing key are always non-migratable keys generated within the TPM.

The covered security functional requirement is: FCO_NRO.2. The SEF4 “Origin” uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF “basic”.

6.1.5 SEF5 – TSF Protection and Test

The TOE supports a suite of tests (self-tests, hardware and firmware controlled) to check and demonstrate the correct operation of the security assumptions provided by the abstract machine, the RNG functioning, reading and extending the integrity registers, the testing of the endorsement key pair integrity, the RSA sign and verify engine, the hash functionality, any tamper-resistant markers and the integrity of the complete microcode (that includes the test of the protected capabilities).

The self-test runs during initial start-up, during normal operation, and at the request of the user. The user has the possibility to do a self-test and to sign the test result within the TPM. If any error occurs during the self-test, the TOE responds as defined in [TCPA] chapter 8.9 and chapter 10.8.3.

The covered security functional requirement is FPT_AMT1 and FPT_TST.1.

Upon the following types of failure occur, the TOE goes into a secure state. The failure types are:

- failure of any crypto operations including RSA encryption, RSA decryption, SHA, RNG, RSA signature generation, HMAC generation
- failure of any commands or internal operations.

The covered security functional requirement is FPT_FLS. 1.

The SEF5 supports replay detection for command requests that include the nonce parameter and performs the destroying of the session where replay is detected.
The covered security functional requirement is FPT_ RPL.1.

The TOE maintains all microcode (the TSF and all other code) in secure areas of the chip (ROM, EEPROM, XRAM) to protect the microcode for interference and tampering by untrusted subjects.
The covered security functional requirements are FPT_RVM.1 and FPT_SEP.1.

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

- Operating state checking: correct function of the TOE is only given in the specific range. To prevent an attack exploiting that circumstances it is necessary to detect if the specified range is left. All operating signals are filtered to prevent malfunctions. In addition the operating state is monitored with sensors for the operating voltage, clock signal frequency, temperature and electro magnetic radiation. The TOE falls into the defined secure state in case of a specified range violation[5]
- Protection against snooping: several mechanisms protect the TOE against snooping the design or the user data during operation and even if it is out of operation (power down). There are topological design measures for disguise, such as the use of the top metal layer with active signals for protecting critical data. The entire design is kept in a non standard way to prevent attacks using standard analysis methods.

[5] The operating state checking this function can only work when the TOE is running and can not prevent reverse engeniering.

- Notification of physical attack: the entire surface of the TOE is protected with the active shield. Attacks cover the surface are detected when the shield lines are cut or get contact. The notification of physical attack uses probabilistic or permutational effects.

The life cycle of the TOE is split-up in several phases as. The software development (phase 1), the chip development and production (phase 2, 3, 4) and the final use (phase 4-7) is a rough split-up from TOE point of view. These phases are implemented in the SLD9630TT1.1 as test mode (phase 2, 3, 4) and user mode (phase 1, 4-7). During start-up of the SLD9630TT1.1 the decision for the user mode or the test mode is taken dependent on several phase identifiers (phase management). If test mode is the active phase the SLD9630TT1.1 requests authentication before any action (test mode lock-out).

Memory Management Unit (MMU): the MMU of the TOE gives the internal firmware the possibility to define different access rights for memory areas. In case of an access violation the MMU will generate a non maskerable interrupt (NMI) and an interrupt service routine react on the access violation.

The covered security functional requirement is FPT_PHP.1.

The TOE supports the capability to consistently interpret TPM commands and responses when shared between the TSF and another trusted IT product as defined in [TCPA].
The covered security functional requirement is FPT_TDC.1.

The TOE supports a communication path between itself and local or remote users to protect the communicated data from modification or disclosure. 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.
The covered security functional requirement is FTP_TRP.1.

The covered security functional requirements are: FPT_AMT.1, FPT_FLS.1, FPT_PHP.1, FPT_RCV.4, FPT_RPL.1, FPT_RVM.1, FPT_SEP.1, FTP_TDC.1, FPT_TST.1 and FTP_TRP1. The SEF5 (“protection against snooping” and “test mode lock-out”) of “TSF Protection and Test” uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF “basic”.

6.1.6 Assignment of Security Functional Requirements

The justification of the mapping between security functional requirements and the Security Enforcing Functions is given in sections 6.1.1 – 6.1.5. The results are shown at Table 5.

#	Security Functional Requirement	SEF1	SEF2	SEF3	SEF4	SEF5
1	FCO_NRO.2				X	
2	FCS_CKM.1	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_SMR.2			X		
21	FMT_SMF.1			X		
22	FPT_AMT.1					X
23	FPT_FLS.1					X
24	FPT_PHP.1					X
25	FPT_RCV.4					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

Table 5: Assignment security functional requirement to SEF

6.2 Security Function Policy

6.2.1 Protected Operations Access Controls

The TOE enforces user access to cryptographic IT assets in accordance with the security function policy (SFP) "*Protected Operations Access Controls"* to meet the security functional requirements.

These policy include:

- Roles and services that can be accessed by those roles:
  Administrator, to perform any command related to system configuration the administrator must supply the TPM ownership token.
  Entity owner, 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.
  Entity users, to use loaded entities on the TPM using the entity use token associated with the 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
  DataIntegrityRegisters (Dir)
  Entities (the TPM can generate, store, use and destroy keys or identities)
  Security Attributes (e.g. Migration and Volatility attribute in TCPA_KEY_FLAGS, TCPA_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.

6.3 Assurance Measures

This chapter contains the definition and description of the assurance measures (AM) of the TOE. The assurance level selected for the TOE was EAL3 augmented because it provides appropriate assurance measures for the expected application of the product. The level EAL3 augmented ensures that the TOE gains maximum assurance from positive security engineering based on good commercial development practices. The TOE provides the following assurance measures to meet the TOE security assurance requirements. The measures are:

AM1: Configuration Management
AM2: Delivery Operation
AM3: Development
AM4: Guidance Documentation
AM5: Lifecycle Support
AM6: Tests
AM7: Vulnerability Assessment

The security target is the first document in the course of an evaluation. The exact references (version numbers and date) of the documents are not final during the evaluation of the security target. To avoid an update of the security target at the end of the evaluation the exact references are listed in the configuration list of the evaluation.

6.3.1 AM1 - Configuration Management

The document “SLD9630TT1.1_ConfigManagement.doc” describes the Configuration Management of the TOE.

The covered security assurance requirements are: ACM_CAP.3 and ACM_SCP.1.

6.3.2 AM2 - Delivery Operation

The document “SLD9630TT1.1_DeliveryOperation.doc” describes the delivery-, installation-, generation- and start-up-procedures of the TOE.

The covered security assurance requirements are: ADO_DEL.1 and ADO_IGS.1

6.3.3 AM3 - Development

The document “SLD9630TT1.1_Development.doc” describes the informal functional specification, the security enforcing high-level design, the informal correspondence demonstration and the informal security policy model of the TOE.

The covered security assurance requirements are: ADV_FSP.1, ADV_HLD.2, ADV_RCR.1 and ADV_SPM.1.

6.3.4 AM4 - Guidance Documentation

The document “SLD9630TT1.1_Guidance.doc” describes the administrator and user guidance of the TOE.

The covered security assurance requirements are: AGD_ADM.1 and AGD_USR.1.

6.3.5 AM5 - Lifecycle Support

The document “SLD9630TT1.1_LifeSup.doc” describes the identification of security measures, and the basic flaw remediation of the TOE.

The covered security assurance requirements are: ALC_DVS.1 and ALC_FLR.1.

6.3.6 AM6 - Tests

The document “SLD9630TT1.1_Tests.doc” describes the analysis of coverage, the testing of the high-level design, the functional testing and the independent testing (sample) of the TOE.

The covered security assurance requirements are: ATE_COV.2, ATE_DTP.1, ATE_FUN.1 and ATE_IND.2.

6.3.7 AM7 - Vulnerability Assessment

The document “SLD9630TT1.1_Vulnerability.doc” describes the examination of guidance, the strength of the TOE security function evaluation and the developer vulnerability analysis of the TOE.

The covered security assurance requirements are: AVA_MSU.1, AVA_SOF.1 and AVA_VLA.1.

6.3.8 Assignment Security Assurance Requirements to AM

#	Security assurance requirement	AM1	AM2	AM3	AM4	AM5	AM6	AM7
1	ACM_ CAP.3	X						
2	ACM_ SCP.1	X						
3	ADO_DEL.1		X					
4	ADO_IGS.1		X					
5	ADV_FSP.1			X				
6	ADV_HLD.2			X				
7	ADV_RCR.1			X				
8	ADV_SPM.1			X				
9	AGD_ADM.1				X			
10	AGD_USR.1				X			
11	ALC_DVS.1					X		
12	ALC_FLR.1					X		
13	ATE_COV.2						X	
14	ATE_DPT.1						X	
15	ATE_FUN.1						X	
16	ATE_IND.2						X	
17	AVA_MSU.1							X
18	AVA_SOF.1							X
19	AVA_VLA.1							X

Table 6: Assignment security assurance requirements to AM

7 PP Claims

7.1 PP Reference

This security target is in conformance to the protection profile TCPA TPMPP v1.9.7.

7.2 PP Tailoring

The assignments and selections foreseen in the TCPA TPMPP v1.9.7 are done here.

The assignments for FDP_ACF.1.3, FDP_ACF.1.4, FDT_ETC.2.4, FDP_ITC.2.5 and FMT_MOF.1.1 are specified in chapter 5.1.1 of this Security Target.

The assignments for FMT_MSA.3 (default values of security attributes) are specified in chapter 6.1.3 Table 4 of this Security Target.

7.3 PP Additions

The augmentation to the protection profile TCPA TPMPP v1.9.7 is the security functional requirements FMT_SMF.1 as defined in section 5.1.1 of this Security Target.
The refinements to the protection profile TCPA TPMPP v1.9.7 are defined in section 5.1.2 of this Security Target.

8 Rationale

This section provides the evidence used in the ST evaluation. This evidence supports the claims that the ST is a complete and cohesive set of requirements, that a conformant TOE would provide 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.

The chapter 6 of the [PP] can be applied completely.

8.1 Security Objective Rationale

The security objectives rationale are defined in the [PP] chapter 6.1.

Table 6.1 of the [PP] shows that all the identified Threats to Security, Secure Usage Assumptions and Secure Usage Assumptions for the IT Environment have been addressed by Security Objectives.

Table 6.2 of the [PP] shows that Security Objectives and the Security Objectives for the Environment are necessary, since each Security Objective addresses at least one Threat to Security, Secure Usage Assumption or Secure Usage Assumption for the IT Environment.

8.2 Security Requirements Rationale

8.2.1 Rationale for the Security Functional Requirements

The security requirements rationale are defined in the [PP] chapter 6.3, 6.4 and 6.5 and in the following for the requirement FMT_SMF.1. The Tables 7,8 and 9 including the necessary supplementations of the Tables 6.3, 6.4 and 6.5 of the [PP] for the requirement FMT_SMF.1.

The dependency FMT_SMR.1 introduced by the components FMT_MSA.1, FMT_MOF.1 and FMT_MTD.1 is considered to be satisfied because the access control specified for the intended TOE is rolebased for each subject as defined by the security functional requirement FMT_MTD.1. The requirement FMT_MTD.1 defines different roles to manage the access to security attributes, security functions and TSF.

The Table 6.3 of the [PP] and Table 7 shows that all security objectives met by at least one security functional requirement.

	Objective	Functional Component
4	O.DAC	FDP_ACC.1, FDP_ACF.1, FMT_MOF.1, FMT_MTD.1 (all iterations), FMT_SMF.1
18	O.Security_Attr_Mgt	FMT_MSA.3, FMT_MSA.1, FMT_SMF.1

Table 7: Supplementation of Table 6.3 of the [PP]

The security objective O.DAC is mapping additionally to the security functional requirement FMT_SMF.1, as FMT_SMF.1 encloses the security functional requirements FMT_MOF.1 and FMT_MTD.1. The security objective O.Security_Attr_Mgt is mapping additionally to the security functional requirement FMT_SMF.1, as FMT_SMF.1 encloses the security functional requirement FMT_MSA.1.

The Table 6.4 of the [PP] and Table 8 shows the dependencies between the security functional requirements.

#	Requirement	Dependencies
31	FMT_SMF.1	FMT_MOF.1, FMT_MTD.1

Table 8: Supplementation of Table 6.4 of the [PP]

The Table 6.5 of the [PP] and Table 9 shows that each security functional requirement is necessary, since it is used to address at least one of the Security Objectives.

#	Requirements	Objectives
31	FMT_SMF.1	O.DAC, O.Security_Attr_Mgt

Table 9: Supplementation of Table 6.5 of the [PP]

8.2.2 Rationale for the Assurance Requirements

The chosen assurance level EAL3 augmented determines the assurance requirements and is the same level as defined by the [PP]. In Table 3 the different assurance levels are shown as well as the augmentations.

The assurance level EAL3 and the augmentations with the requirements ADV_SPM.1 and ALC_FLR.1 were chosen in order to meet assurance expectations. An assurance level of EAL3 is chosen for this type of TOE since it is intended to defend against basic level attacks without a protected environment. This evaluation assurance level was selected since it provides even a formal evidence on the conducted vulnerability assessment. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defence against such attacks, the evaluators have access to all information regarding the TOE including the low level design.

8.2.3 Rationale for the Strength of Function

The strength of function “basic” is defined for the TOE and is the same level as defined by the [PP]. The strength of cryptographic algorithms is outside of the scope of the CC. Strength of function only applies to non-cryptographic, probabilistic or permutational mechanisms. The strength of function “basic” provides a sufficient protection of the product in its intended environment against attacker with a low attack potential.

8.2.4 Rationale for the Dependencies

The added security functional requirement FMT_SMF.1 has dependencies to the functional security requirements FMT_MOF.1, FMT_MSA.1 and FMT_MTD1.

8.3 TOE Summary Specification Rationale

This chapter shows that the TOE IT Security Functions and Assurance Measures are suitable to meet the TOE Security Requirements.

8.3.1 Security Enforced Functions Rationale

The Table 10 shows that the security enforced functions defined in the TOE Summary Specification address all of the TOE security functional requirements. The Table 10 shows that all security enforced functions work together to satisfy the TOE security functional requirements. All security enforced functions are necessary because there is at least one security functional requirement mapped to each security enforced function.

A discussion of the rationale for the mapping is provided for each security functional requirement below.

FCO_NRO.2 The TSF shall enforce proof of origin.

FCO_NRO.2 is mapped to SEF4 - Origin and Privacy. SEF4 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: The TSF shall provide the generation of cryptographic keys in accordance with specified cryptographic key generation algorithm RSA.

FCS_CKM.1 is mapped to SEF1 - Cryptographic Support. SEF1 supplies the generation of cryptographic RSA key pairs with key sizes of 512 to 2048 bit according PKCS#1 V2.

FCS_CKM.4 The TSF shall destroy cryptographic keys in accordance with a cryptographic key destruction method that meets FIPS 140-1, Section 4.8.5 or equivalent.

FCS_CKM.4 is mapped to SEF1 - Cryptographic Support. SEF1 supplies the destruction of cryptographic keys by erasure of volatile memory areas containing cryptographic keys in accordance with FIPS 140-1, Section 4.8.5.

FCS_COP.1 The TSF shall provide the following cryptographic operations: RSA encrypt and decrypt, RSA signature and signature verification, secure hash and keyed-hashing for message authentication.

FCS_COP.1 is mapped to SEF1 - Cryptographic Support. SEF1 supplies the RSA encrypt and decrypt operation and the RSA signature generation and signature verification in accordance with the specified cryptographic algorithm RSA and key sizes RSA 512 to 2048 bits that meet PKCS#1 V2. SEF1 supplies 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 and cryptographic key sizes 160 bits that meet RFC 2104.

FDP_ACC.1 The TSF shall provide a security function policy Protected Operations Access Controls (POAC) to specific objects and shall enforce rules to deter mine if an operation among controlled subjects and objects is allowed.

FDP_ACC.1 is mapped to SEF3 - User Data Protection. SEF3 enforces the security function policy POAC to protect sensitive subjects, objects and operations of the TSF.

FDP_ACF.1 The TSF shall enforce security attributes based on the protected operations access controls.

FDP_ACF.1 is mapped to SEF3 - User Data Protection. SEF3 supplies the security attributes TCPA_AUTH_DATA_USAGE, TCPA_KEY_FLAGS and TCPA_KEY_USAGE controlled from the Protected Operations Access Controls (POAC).

FDP_ETC.2 The TSF shall enforce the Protected Operations Access Controls for the export of user data with security attributes.

FDP_ETC.2 is mapped to SEF3 - User Data Protection. SEF3 enforce the POAC to control the export of user data with security attributes. The export is done with the users data´s unambiguously associated security attributes.

FDP_ITC.2 The TSF shall enforce the Protected Operations Access Controls for the import of user data with security attributes.

FDP_ITC.2 is mapped to SEF3 - User Data Protection. SEF3 enforce the POAC to control the import of user data with security attributes. The security attributes of the imported data are interpreted by the protocol and are unambiguously associated to the data.

FDP_RIP.2 The TSF shall enforce the full residual information protection.

FDP_RIP.2 is mapped to SEF3 - User Data Protection. SEF3 enforce 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 specific memory area.

FIA_ATD.1 The TSF enforces user attributes.

FIA_ATD.1 is mapped to SEF2 - Authentication and Identification. SEF2 supports the security attributes authentication data and role, belonging to individual users.

FIA_UAU.1 The TSF shall control the timing of authentication of each user.

FIA_UAU.1 is mapped to SEF2 - Authentication and Identification. SEF2 allows access to specific commands before the user is authenticated if the used key has the “world” access right. Each user require to be successfully authenticated before allowing any other TSF mediated actions on behalf of that user.

FIA_UAU.4 The TSF shall support single-use authentication mechanisms.

FIA_UAU.4 is mapped to SEF2 - Authentication and Identification. SEF2 provides the authentication protocols “Object-Independent Authorization Protocol” (OI-AP) and “Object Specific Authorization Protocol” (OS-AP).

FIA_UAU.6 The TSF shall support the re-authentication of users.

FIA_UAU.6 is mapped to SEF2 - Authentication and Identification. SEF2 provides the re-authentication of users by using the authorization protocol with a new nonce for each message and response to prevent the sneak of old authentication data.

FIA_UID.1 The TSF shall control the timing of identification of each user.

FIA_UID.1 is mapped to SEF2 - Authentication and Identification. SEF2 allows access to specific commands before the user is identified if the used key has the “world” access right. Each user require to be successfully identified before allowing any other TSF mediated actions on behalf of that user.

FMT_MOF.1 Management of security functions behaviour.

FMT_MOF.1 is mapped to SEF3 - Security Management. SEF3 allows the TPM owner to disable/enable the following functions to the TPM owner: prevent any entity from reading the PUBEK, enable/disable a TPM, disable the TPM_OwnerClear function and disable/enable auditing for a command.

FMT_MSA.1 Management of security attributes.

FMT_MSA.1 is mapped to SEF3 - Security Management. SEF3 supports the POAC to restrict the creation of security attributes (TCPA_AUTH_DATA_USAGE, TCPA_KEY_USAGE, migratable and volatility flag) to the TPM owner.

FMT_MSA.2 The TSF accepts only secure security attributes.

FMT_MSA.2 is mapped to SEF3 - Security Management. SEF3 ensure that only secure values are accepted for security attributes.

FMT_MSA.3 The TSF shall support static attribute initialisation.

FMT_MSA.3 is mapped to SEF3 - Security Management. SEF3 defines default values for specific security attributes of the SRK and the entity keys.

FMT_MTD.1 The TSF shall manage specific TSF data.

FMT_MTD.1 is mapped to SEF3 - Security Management. SEF3 restricts the ability to modify identification and authentication data associated with the SRK and migration authorization data to the TPM owner. SEF3 restrict the generation of the SRK and tpmProof to the TPM owner and the generation of the Endorsement Key Pair to the TPM manufacturer Infineon Technologies AG. SEF3

restricts the modification of the identification and authentication data associated with entity to the entity owner.

FMT_SMR.2 The TSF shall ensure security roles.

FMT_SMR.2 is mapped to SEF3 - Security Management. SEF3 supports the roles TPM owner and owner of entities. The role is bound always on a specific authentication token. The roles are enforced within the TOE because there are specific commands and specific keys bound to different token. The TOE supports the role TPM manufacturer during the production phase.

FMT_SMF.1 The TSF shall be capable of performing security management functions.

FMT_SMF.1 is mapped to SEF3 - Security Management. SEF3 supports the management of security functions, security attributes and TSF data.

FPT_AMT.1 The TSF shall support abstract machine testing.

FPT_AMT.1 is mapped to SEF5 – TSF Protection and Test. SEF5 supports a suite of tests (self-tests, hardware and firmware controlled) to check and demonstrate the correct operation of the security assumptions provided by the abstract machine.

FPT_FLS.1 The TSF shall preserve a secure state.

FPT_FLS.1 is mapped to SEF5 – TSF Protection and Test. SEF5 forces the TOE into a secure state upon the detection of defined failure types.

FPT_PHP.1 The TSF shall detect physical attacks.

FPT_PHP.1 is mapped to SEF5 – TSF Protection and Test. SEF5 protects the TOE against physical attacks with different features (e.g. operating state checking, protection against snooping, notification of physical attack).

FPT_RCV.4 The TSF shall support function recovery.

FPT_RCV.4 is mapped to SEF5 – TSF Protection and Test. All TPM commands have the property that the SF either completes successfully, or recovers to a consistent and secure state.

FPT_RPL.1 The TSF shall support replay detection.

FPT_RPL.1 is mapped to SEF5 – TSF Protection and Test. SEF5 supports replay detection for command requests that include the nonce parameter. The nonce parameter is a random number generated and/or stored in the TOE, each command request or answer includes a new nonce. If replay is detected the session is destroyed.

FPT_RVM.1 The TSF shall ensure the non-bypassability of the TSP.

FPT_RVM.1 is mapped to SEF5 – TSF Protection and Test. The TSF are programmed in a way that bypassing of TSF enforced functions is not possible.

FPT_SEP.1 Security domain for the TSF.

FPT_SEP.1 is mapped to SEF5 – TSF Protection and Test. The microcode of the TSF and all other functionality of the TOE are located in secure areas of the chip (e.g. ROM, EEPROM) to protect the microcode for interference and tampering by untrusted subjects.

FPT_TDC.1 The TSF shall ensure Inter-TSF TSF data consistency.

FPT_TDC.1 is mapped to SEF5 – TSF Protection and Test. SEF5 supports the capability to consistently interpret TPM commands and responses when shared between the TSF and other trusted IT product by the implementation of the firmware according the definitions of the TCPA Main Specification.

FPT_TST.1 The TSF shall provide a self-test.

FPT_TST.1 is mapped to SEF5 – TSF Protection and Test. SEF5 supports self-test during start-up or at the request of the user. The self-test of the TOE guarantees the demonstration of the correct operation of the TSF functions. The test includes the verification of the TSF executable code.

FTP_TRP.1 The TSF shall provide a trusted path.

FTP_TRP.1 is mapped to SEF5 – TSF Protection and Test. SEF5 supports a communication path between itself and local or remote users. The trusted path can be used from the TSF and local or remote users for initial user authentication, for all TPM commands, for all user commands and responses.

#	Security Functional Requirement	Security Enforced Function
1	FCO_NRO.2	SEF4 – Origin
2	FCS_CKM.1	SEF1 - Cryptographic Support
3	FCS_CKM.4	SEF1
4	FCS_COP.1	SEF1
5	FDP_ACC.1	SEF3 – Access Control
6	FDP_ACF.1	SEF3
7	FDP_ETC.2	SEF3
8	FDP_ITC.2	SEF3
9	FDP_RIP.2	SEF3
10	FIA_ATD.1	SEF2 - Authentication and Identification
11	FIA_UAU.1	SEF2
12	FIA_UAU.4	SEF2
13	FIA_UAU.6	SEF2
14	FIA_UID.1	SEF2
15	FMT_MOF.1	SEF3 – Access Control
16	FMT_MSA.1	SEF3
17	FMT_MSA.2	SEF3
18	FMT_MSA.3	SEF3
19	FMT_MTD.1	SEF3
20	FMT_SMR.2	SEF3
21	FMT_SMF.1	SEF3
22	FPT_AMT.1	SEF5 - TSF Protection and Testing
23	FPT_FLS.1	SEF5
24	FPT_PHP.1	SEF5
25	FPT_RCV.4	SEF5
26	FPT_RPL.1	SEF5
27	FPT_RVM.1	SEF5
28	FPT_SEP.1	SEF5
29	FPT_TDC.1	SEF5
30	FPT_TST.1	SEF5
31	FTP_TRP.1	SEF5

Table 10: Assignment security functional requirement to SEF

8.3.2 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 security functional requirements. This shows that the Security Enforcing Functions work together so as to satisfy the security functional requirements.

The Table 10 shows that all security functional requirements are satisfied by one Security Enforced 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 SFR´s and the assurance requirements supports each other and that there are no inconsistencies between these groups are shown in the sections above.

8.3.3 Assurance Measures Rationale

The rationale shows how all assurance requirements where satisfied. The Table 6 in chapter 6.3.8 shows that there is at least one Assurance Measure defined in the TOE Summary Specification to meet each of the Security Assurance Requirements.

8.4 PP Claims Rationale

This security target is in conformance to the protection profile [PP].

The assurance level of the [PP] is EAL 3 augmented. The Assurance Requirements of the TOE obtain the assurance level EAL 3 augmented for the TOE.

The augmentations are declared in chapter 5.1.1, 5.1.2, 5.1.3, 8.2.1 and 8.3.1. The security target adds in chapter 5.1.1 the security functional requirement FMT_SMF.1 to the security functional requirements of the [PP].

The strength of function level of the [PP] is basic. The strength of function level of the TOE is basic for the TOE.

9 References

9.1 Documents Guidance

[PP]	Trusted Computing Platform Alliance (TCPA) Trusted Platform Module Protection Profile	Version 1.9.7
[TCPA]	Trusted Computing Platform Alliance Main Specification	Version 1.1b

Table 11: Document guidance

9.2 Acronyms and Glossary

Acronyms

CC - Common Criteria
CI - Chip Identification mode (STS-CI)
CIM - Chip Identification Mode (STS-CI), same as CI
CRC - Cyclic Redundancy Check
DPA - Differential Power Analysis
DFA - Differential Failure Analysis
EAL - Evaluation Assurance Level
EEPROM - Electrically Erasable and Programmable Read Only Memory
EMA - Electro magnetic analysis
HW - Hardware
IC - Integrated Circuit
ID - Identification
IRAM - Internal Random Access Memory
IT - Information Technology
I/O - Input/Output
MED - Memory Encryption and Decryption
MMU - Memory Management Unit
OS - Operating system
PLL - Phase Locked Loop
PP - Protection Profile
RMS - Resource Management System
RNG - Random Number Generator
RAM - Random Access Memory
ROM - Read Only Memory
SF - Security Function
SEF - Security Enforced Function
SFP - Security Function Policy
SOF - Strength of Function
SPA - Simple power analysis

ST - Security Target
STS - Self Test Software
SW - Software
TM - Test Mode (STS)
TOE - Target of Evaluation
TSF - TOE Security Functions
TSP - TOE Security Policy
UM - User Mode (STS)
XRAM - eXtended Random Access Memory

Glossery

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

Central Processing Unit(CPU): Logic circuitry for digital information processing.

Chip → Integrated Circuit

Chip Identification Mode: Operational status phase of the TOE, in which actions for identifying the individual take place.

Controller: IC with integrated memory, CPU and peripheral devices.

CRC: Process for calculating checksums for error detection.

Challenger: An entity that requests and has the ability to interpret integrity metrics from a Subsystem.

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

EEPROM: Nonvolatile memory permitting electrical read and write operations.

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).

Firmware: Part of the software implemented as hardware.

Hardware: Physically present part of a functional system.

Hash value: Result of a hash calculation e.g. SHA-1.

HMAC: A mechanism for message authentication according RFC 2104 using the cryptographic hash function SHA-1.

Integrity metrics: Values that are the results of measurements on the identity for the TPM.

Integrated Circuit: Component comprising several electronic circuits implemented in a highly miniaturized device using semiconductor technology.

Internal Random Access Memory: RAM integrated in the CPU.

LPC Interface: Low Pin Count (LPC) Interface defined by Intel is a standardized interface used in PC mainboards.

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

Mechanism: Logic or algorithm which implements a specific security function in hardware or software.

Memory: Hardware part containing digital information (binary data).

Memory Encryption and Decryption: Method of encoding/decoding data transfer between CPU and memory.

Memory Management Unit (MMU): The MMU controls the different access rights of memory areas.

Microcontroller → Controller

Microprocessor → CPU

Migratable: A key that may be transported outside the specific TPM.

Nonce: A nonce is a random number value that provides protection from replay and other attacks.

Non-migratable: A key that cannot be transported outside the 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.

Platform Configuration Register (PCR): A PCR consists of a 160 bit field that holds a cumulatively updated hash value and a 4 byte status field.

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.

Protected function: Access to this function requires an authentication process.

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

Protection Profile: A document that defines all attacks and how they are resisted by the TPM, the RTM, and the methods by which these are incorporated into the platform.

Random Access Memory: Volatile memory which permits write and read operations.

Random Number Generator: Hardware part for generating random numbers.

Read Only Memory: Nonvolatile memory which permits read operations only.

Resource Management System: Part of the firmware containing EEPROM programming routines.

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.

Security Function: Part(s) of the TOE used to implement part(s) of the security objectives.

Security Target: Description of the intended state for countering threats.

Self Test Software: Part of the firmware with routines for controlling the operating state and testing the TOE hardware.

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

Shielded location: Storage location within the TPM with a protection against unauthorized access.

Smart Card: Plastic card in credit card format with built-in chip.

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.

Software: Information (non-physical part of the system) which is required to implement functionality in conjunction with the hardware (program).

Target of Evaluation: Product or system which is being subjected to an evaluation.

Test Mode: Operational status phase of the TOE in which actions to test the TOE hardware take place.

Threat: Action or event that might prejudice security.

Tripple-DES: Using DES three times with key of a size of 112 bit or 168 bit.

TpmProof: A random number stored within the TPM. The tpmProof is a unique secret for each TPM.

Trusted Building Block (TBB): A trusted platform is instantiated as a Trusted Building Block which is the evaluated component of a trusted system. The TBB is composed of the TPM, the TSS and the connection between them.

Trusted Platform Module: 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 which 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).

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

Trusted Set (TS): Subsystem capability that must be trustworthy for the subsystem.

TPM Identity:	One of the anonymous PKI identities belonging to a TPM; a TPM may have multiple identities.
User:	An entity that uses the platform in which a TPM is installed. The only rights that a User has over a TPM are 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 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.
User Mode:	Operational status phase of the TOE in which actions intended for the user take place.