Security Target

OPTIGA^{TM} Trusted Platform Module SLB9672_2.0 v16 SLB9673_2.0 v26

Common Criteria CCv3.1 EAL4 augmented (EAL4+)
Resistance to attackers with MODERATE attack potential

Version:	2.5
Date:	2025-08-21

PUBLIC

Author: Infineon Technologies AG, Connected Secure Systems S CERT

Edition 2.5

Published by

Infineon Technologies AG

81726 Munich, Germany

REVISION HISTORY

1.0	2021-02-22: Final version
1.8	2021-03-18: Recertification for TCG TPM v1.59 for IOT
2.0	2021-07-27: Final version for SLB9672_2.0 v16
2.2	2022-01-17: SLB9673_2.0 v26.10 with I2C added, reference to TPM PP 1.59 v1.3
2.3	2022-03-30: New TPM software version added
2.4	2023-04-24: New TPM software version added
2.5	2025-08-21: Recertification with scope reduction

TABLE OF CONTENTS

1 Security Target Introduction (ASE_INT)

This section contains the document management and provides an information overview. 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 and Target of Evaluation Reference

The title of the security target (ST) is Security Target OPTIGA^{TM} Trusted Platform Module SLB9672_2.0 v16 SLB9673_2.0 v26.
The security target has the version 2.5 and is dated 2025-08-11.

The Target of Evaluation (TOE) is a security IC (Security Controller) with integrated firmware (operating system) and guidance documentation, which is named OPTIGA^{TM} Trusted Platform Module SLB9672_2.0 v16 SLB9673_2.0 v26, is internally registered under the development code SLB9672_2.0 v16.10.16488.00 SLB9672_2.0 v16.12.16858.00 SLB9672_2.0 v16.13.17733.00 SLB9673_2.0 v26.10.16688.00 SLB9673_2.0 v26.13.17770.00.

The Security Target are built in accordance with Common Criteria V3.1.

The security functionality of the TOE is reduced to the FieldUpgrade process.

	Version	Date	Registration
Security Target	2.5	2025-08-21	Security Target OPTIGA^{TM} Trusted Platform Module SLB9672_2.0 v16 SLB9673_2.0 v26
Target of Evaluation	SLB9672_2.0 v16.10.16488.00 v16.12.16858.00 v16.13.17733.00 SLB9673_2.0 v26.10.16688.00 v26.13.17770.00		OPTIGA^{TM} Trusted Platform Module SLB9672_2.0 v16.10.16488.00 SLB9672_2.0 v16.12.16858.00 SLB9672_2.0 v16.13.17733.00 SLB9673_2.0 v26.10.16688.00 SLB9673_2.0 v26.13.17770.00 in the delivery format: as defined in section 2.2.4
Guidance Documentation	Rev. 01.59	November 8, 2019	Trusted Platform Module Library Part 1: Architecture, Family ”2.0” Level 00 Revision 01.59
	Rev. 01.59	November 8, 2019	Trusted Platform Module Library Part 2: Structures Family ”2.0” Level 00 Revision 01.59
	Rev. 01.59	November 8, 2019	Trusted Platform Module Library Part 3: Commands Family ”2.0” Level 00 Revision 01.59
	Rev. 01.59	November 8, 2019	Trusted Platform Module Library Part 4: Supporting Routines Family ”2.0” Level 00 Revision 01.59
	Version 1.1	June 18, 2020	Errata for TCG Trusted Platform Module Library, Family “2.0” Level 00 Revision 1.59 November 8, 2019
	Version 1.05 Rev. 14	2020-09-04	TCG PC Client Platform TPM Profile Specification for TPM 2.0
	Rev. 1.1	2021-07-22	OPTIGA^{TM} TPM SLB 9672 FW16.10 Databook
	Rev. 1.2	2022-03-09	OPTIGA^{TM} TPM SLB 9672 FW16.12 Databook
	Rev. 1.3	2023-04-12	OPTIGA^{TM} TPM SLB 9672 FW16.13 Databook
	Rev. 1.2	2022-03-09	OPTIGA^{TM} TPM SLB 9673 FW26.10 Databook
	Rev. 1.4	2023-04-14	OPTIGA^{TM} TPM SLB 9673 FW26.13 Databook
	Rev. 1.04	2021-10-06	OPTIGA^{TM} TPM SLB 9672 TPM2.0 Application Note User Guidance
	Rev. 1.5	2023-04-12	OPTIGA^{TM} TPM SLB 9672 TPM2.0 FW16.xx Errata and Updates
	Rev. 1.2	2023-04-17	OPTIGA^{TM} TPM SLB 9672 TPM2.0 FW26.xx Errata and Updates
			all documents in the delivery format: *.pdf

	3.1 Revision 5	April 2017	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2017-04-001 Part 2: Security functional requirements CCMB-2017-04-002 Part 3: Security Assurance Components CCMB-2017-04-003

Table 1: Identification

Remarks to the Target of Evaluation (TOE):

The TOE of this Security Target encloses the following versions:
SLB9672_2.0 v16.10.16488.00 SLB9672_2.0 v16.12.16858.00 SLB9672_2.0 v16.13.17733.00 SLB9673_2.0 v26.10.16688.00 SLB9673_2.0 v26.13.17770.00.

These versions may include different derivatives. The hardware and software of these derivatives are identical (related to one version), the only difference between the derivatives is the extended temperature range, the packaging and the own intermediated IFX certificate.

The derivatives are listed in the documents OPTIGA^{TM} TPM SLB 9672 TPM 2.0 FW16.xx Errata and Updates and in OPTIGA^{TM} TPM SLB 9673 TPM 2.0 FW26.xx Errata and Updates [13] in section 5 “Sales Order Code”. The documents OPTIGA^{TM} TPM SLB 967x FWxx.yy Databook listed in [14], gives in section 4.6.2 “TPM and vendor properties” a description to read out the version of the TOE.

1.2 Target of Evaluation Overview

This Security Target (ST) describes the target of evaluation (TOE) known as the OPTIGA^{TM} Trusted Platform Module SLB9672_2.0 v16 SLB9673_2.0 v26 and gives a summary product definition. In the following description the expressions SLB9672_2.0 or TOE stands for all the versions and derivatives of the TOE.

The OPTIGA^{TM} Trusted Platform Module SLB9672_2.0 v16.10.16488.00 SLB9672_2.0 v16.12.16858.00 SLB9672_2.0 v16.13.17733.00 SLB9673_2.0 v26.10.16688.00 SLB9673_2.0 v26.13.17770.00, called TOE or SLB9672_2.0 in the following text, is an integrated circuit and software platform that gives users the possibility to update the product OPTIGA^{TM} Trusted Platform Module SLB9672_2.0 v16.10.16488.00 SLB9672_2.0 v16.12.16858.00 SLB9672_2.0 v16.13.17733.00 SLB9673_2.0 v26.10.16688.00 SLB9673_2.0 v26.13.17770.00 to a new product version.

The SLB9672_2.0 uses the Serial Peripheral Interface (SPI) for the integration into existing PC mainboards. The SLB9672_2.0 is basically a secure controller with the following added functionality:

- Symmetric and asymmetric key procedures (AES encryption/decryption, ECDSA verification of digital signatures)
- Hash algorithms (SHA)

The security functionality of the TOE is reduced to the FieldUpgrade process.

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 must 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 constructed out 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 prove that the TOE meets these requirements. The functionality of the TOE to meet the requirements is described.

The TOE summary specification consisting of the security features, the assurance requirements and the security function policies are defined in the ST as property of this specific TOE, the SLB9672_2.0. 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.

2 Target of Evaluation Description

The TOE description helps to understand the specific security environment and the security policy. In this context the assets, threats, security objectives and security functional requirements can be employed.

2.1 TOE Definition

The Target of Evaluation (TOE) is the “OPTIGA^{TM} Trusted Platform Module SLB9672_2.0 v16.10.16488.00 SLB9672_2.0 v16.12.16858.00 SLB9672_2.0 v16.13.17733.00 SLB9673_2.0 v26.10.16688.00 SLB9673_2.0 v26.13.17770.00” of the Infineon Technologies AG called “SLB9672_2.0” or “TOE” in the following description. The TOE is an integrated circuit and software platform that provides computer manufacturers with the core components of a subsystem used to update the product OPTIGA^{TM} Trusted Platform Module SLB9672_2.0 v16.10.16488.00 SLB9672_2.0 v16.12.16858.00 SLB9672_2.0 v16.13.17733.00 SLB9673_2.0 v26.10.16688.00 SLB9673_2.0 v26.13.17770.00 to a new product version. For this FieldUpgrade process the SLB9672_2.0 provides several cryptographic services (e.g. AES in CTR, CMAC and KWP-AD mode, Hash algorithms, ECDSA signature verification). The trusted mechanism of the platform uses cryptographic processes, including secrets. The trusted mechanisms are required to be isolated from the platform order to protect secrets from disclosure and protect methods from subversion.

The security functionality of the TOE is reduced to the FieldUpgrade process.

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

To simplify system integration into existing PC mainboards, the SLB9672_2.0 uses the Serial Peripheral Interface (SPI).

The hardware of the SLB9672_2.0 is a secure controller based on the SLE90-Family architecture with additional components and is manufactured by the Infineon Technologies AG.

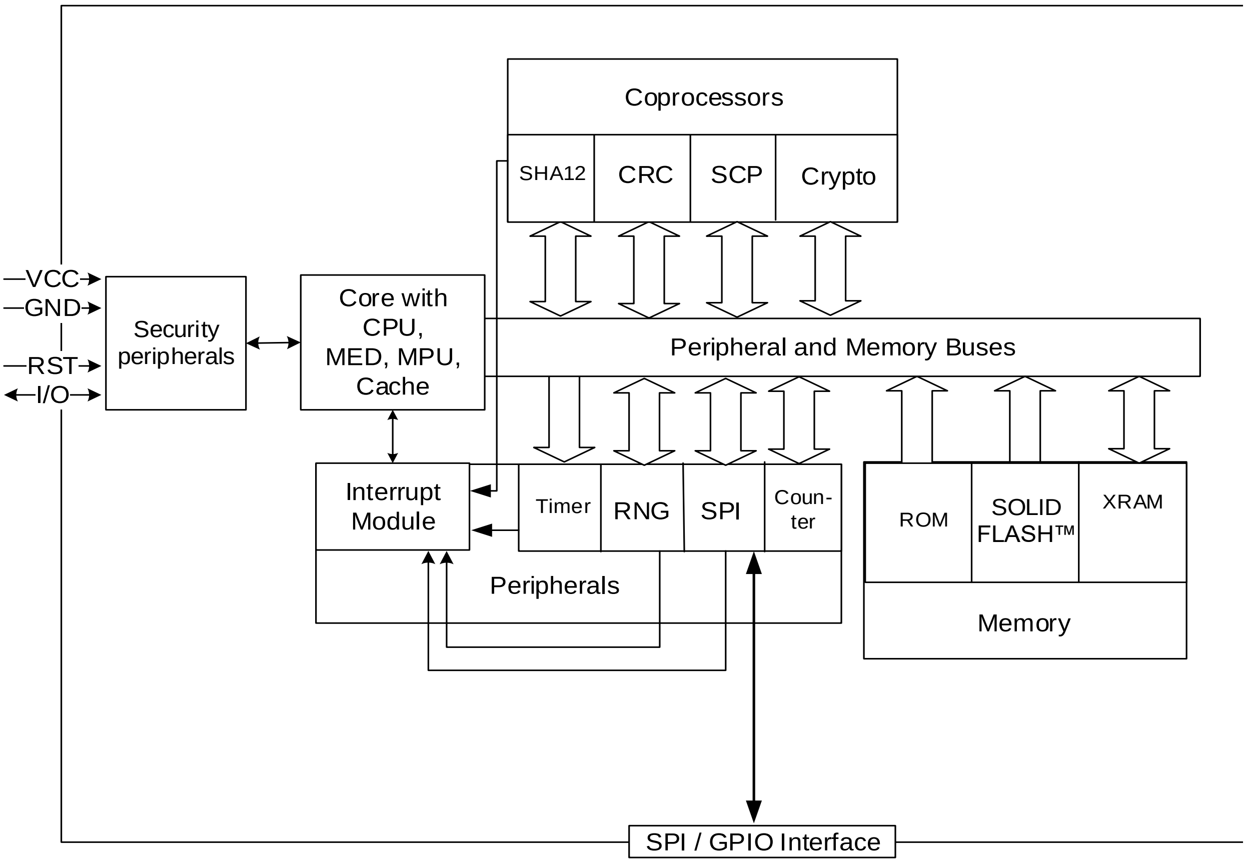
The IC, whose block diagram is shown in Figure 1, consists of a dedicated microprocessor (CPU) with a Memory Protection Unit (MPU), several Coprocessors, several different memories, security logic, shield, timer, an interrupt controlled I/O interface, a Random Number Generator (RNG), a hardware Hash Accelerator, a Counter and a Serial Peripheral Interface (SPI and an Inter-Integrated Circuit (I2C) interface. The SPI and I2C interfaces are the main interfaces of the chip. The SPI interface is only used by the SLB9672_2.0 v16 and the I2C interface is only used by the SLB9673_2.0 v26.

The CPU is a real 32-bit CPU-architecture and is compatible to the ARM Secure Core SC300 architecture. The major components of the core system is the CPU (Central Processing Unit), the MPU (Memory Protection Unit) and MED (Memory Encryption/Decryption Unit). The TOE implements a full 32-bit addressing with up to 2 GByte linear addressable memory space, a flexible Memory Management concept and stack. The flexible memory concept consists of ROM- and Flash-memory (SOLID FLASH^{TM} NVM[1]) as part of the non-volatile memory (NVM), respectively EEPROM.

The SLB9672_2.0 uses an internal generated clock of 100 MHz.
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 two cryptographic co-processors serve the need of modern cryptography: The symmetric co-processor (SCP) for AES hardware acceleration. The Asymmetric Crypto co-processor, called Crypto2304T in the following, is used for RSA and Elliptic Curve (ECC) cryptography. The third module the Hash accelerator named SHA12 provides Secure Hash Algorithms (SHA-256 and SHA-512).

[1] SOLID FLASH™ is an Infineon Trade Mark and stands for the Infineon EEPROM working as Flash memory. The abbreviation NVM is short for Non Volatile Memory.



Note: The SLB9672_2.0 v16 includes an SPI interface, the SLB9673_2.0 v26 includes an I2C interface

Figure 1: Block diagram of the TOE

The firmware required for operating the chip includes an operating system. 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 OPTIGA^{TM} TPM SLB 9672 TPM2.0 Databook listed in [14], which can be used by the host to load the actual version again in the case of a fatal error within the TOE. The field upgrade and recovery version can only be downloaded to the chip if it has been encrypted and signed by the manufacturer Infineon Technologies AG. The Figure 2 shows the firmware block diagram of the TOE.

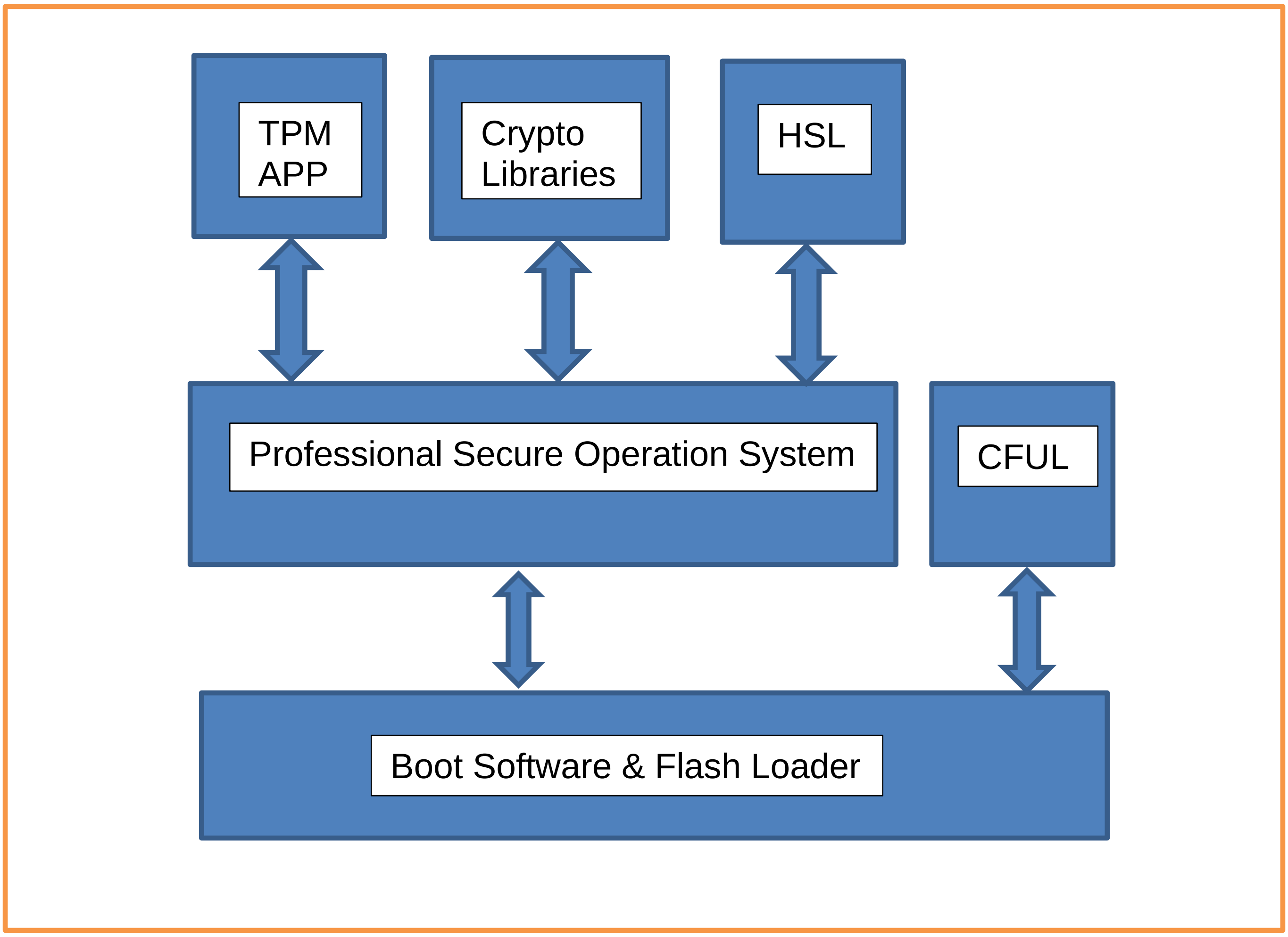

TPM APP
Crypto Libraries
HSL
Professional Secure Operation System
CFUL
Boot Software & Flash Loader

Figure 2: Firmware block diagram of the SLB9672_2.0

2.2 Scope of the TOE

The TOE manufactured by Infineon Technologies AG, comprises the hardware of the security controller, and the associated firmware required for operation provided in ROM and SOLID FLASH^{TM} NVM memory.

2.2.1 Hardware of the TOE

The *hardware part* of the TOE (cf. Figure 1) is comprised of:

- Security Peripherals (filters, sensors)
- Core System
  - with proprietary CPU implementation of the ARM Secure Core SC300 architecture from functional perspective
  - Cache
  - Memory Encryption/Decryption Unit (MED)
  - Memory Protection Unit (MPU)
- Memories
  - Read-Only Memory (ROM)
  - Random Access Memory (RAM)
  - SOLID FLASH^{TM} NVM
- Coprocessors
  - Crypto2304T for asymmetric algorithms like RSA and ECC
  - Symmetric Crypto Co-processor AES standard (SCP)
  - Hash accelerator for the SHA algorithms
- Random number generator (RNG)
- Checksum module (CRC)
- Interrupt module (INT)
- Timer (TIM)
- Buses (BUS)
  - Memory Bus
  - Peripheral Bus
- Serial Peripheral Interface (SPI – used by SLB9672_2.0 only)
- Inter-Integrated Circuit interface (I2C – used by SLB9673_2.0 v26 only)
- GPIO interface
- Tick Counter

2.2.2 Firmware/Software of the TOE

The entire firmware/software of the TOE consists of different parts. The firmware part includes the Boot Software providing the startup processing and the Flash Loader, which is only used for the production phase. The software part includes the Professional Secure Operating System used to operate the IC, the Cryptographic Libraries (ACL, SCL, HCL, RCL), the Hardware Support Library and the TPM2.0 Application. Additionally, the Endorsement Primary Seed (EPS), two ECC Endorsement Keys, two RSA Endorsement Keys (EK) and four EK credentials (Endorsement Certificate) are part of the TOE. The TOE provides also the FieldUpgrade and recovery functionality for updating the protected capabilities once the TOE is in the field, so that it is possible to update e.g. a certified TOE version v16.12.16858.00 to a newer certified version e.g. SLB9672_2.0 v16.15.zzzzz.00 or to download the actual TOE version again.
The BOS routines and a part of the FieldUpgrade routines are stored in especially protected memory areas.
The entire firmware of the TOE (cf. Figure 2) is comprised of:

- Boot Software (BOS)
- Professional Secure Operating System (PSOS)
- Cryptographic Libraries (ACL, SCL, HCL, RCL)
- Hardware Support Library (HSL)
- FieldUpgrade (CFUL)
- TPM2.0 Application (APP)

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 the guidance documentation is given in Table 1, section Guidance Documentation.

2.2.4 Forms of delivery

The TOE is finished, and the extended test features are removed.

The TOE is delivered in form of complete chips which include the hardware, the firmware, the Endorsement Primary Seed, two RSA Endorsement Key, two ECC Endorsement Keys and four Endorsement Certificates. The delivery of the TOE is done from a distribution center by postal transfer or delivery courier.

The TOE guidance documentation, as listed in Table 1 section Guidance Documentation, is provided as data file (all in *.pdf format) in a folder for the secured download by an authorised user. The secured download is a way of delivery of documentation using a secure ishare connected to Infineon customer portal. The TOE user needs a DMZ Account to login (authenticate) via the Internet.

2.2.5 Production sites

The TOE silicon is produced in the production site Tainan, Taiwan.

The delivery measures are described in the ALC_DVS aspect.

2.2.6 Life cycle of the TOE

The life cycle of the TOE as part of the evaluation covers phase 1 “Development” and phase 2 “Manufacturing and Delivery” as defined in the following description. The phase 1 includes the TOE development, the phase 2 includes the TOE manufacturing, the TOE conformance testing, the Platform Primary Seed and the TPM-Mfg EK credential issuance.

The TOE life cycle is described in four phases: Development, Manufacturing, Platform Integration and Operational usage. As the TOE supports the Field Upgrade process, the life cycle distinguishes two cases.

- Case 1: The TOE hardware and firmware are manufactured and delivered together.
- Case 2: The TOE firmware component is installed (as a replacement or an augmentation of the previously loaded TOE firmware) after delivery of the TOE hardware component to the platform vendor or the end user.

The Field Upgrade process, as described in OPTIGA^{TM} TPM SLB 9672 TPM2.0 Databook [14], changes the TOE to a new version.

Case 1 of the TOE life cycle can be summarized as follows.

- Development of the TOE (Phase 1)

  The Development of the TOE (Phase 1) comprises the development of the TOE hardware and the TOE firmware.

- Manufacturing and Delivery of the TOE (Phase 2)

  The Manufacturing Phase comprises the production of the integrated circuit implementing the TOE hardware and complete or parts of TOE firmware, the loading of TOE firmware parts stored in EEPROM or Flash memory, testing and delivery to the platform vendor.

  This phase ends with TOE delivery to the customer.

- Platform Integration (Phase 3)

  The TOE is installed in the platform, equipped with TOE and platform specific keys and certificates, and delivered to the customer of the platform.

- Operational usage (Phase 4)
  In the Operational Phase the TOE is prepared for operational usage and used in the environment of the end user. The preparative procedures for operational usage include secure acceptance of the delivered TOE, taking and releasing ownership.

In case 2 of the TOE life cycle the TOE hardware and parts of the TOE firmware of a previously certified TOE are used for access, integrity and authenticity control of the installation of the new firmware running on the same hardware and building a new TOE. The parts of the previously certified TOE may be run through the life cycle as in case 1 or in case 2.

The following steps describe the life cycle case 2 for the upgraded firmware parts only. The TOE hardware is as already delivered to the platform vendor or the end user.

- Development of the TOE (Phase 1)

  The Development of the TOE (Phase 1) comprises the development and testing of the TOE firmware upgrades to be installed on hardware of a previous TOE.

- Manufacturing of the TOE (Phase 2)

The TOE manufacturer delivers the field upgrade data for Field Upgrade to the platform vendor as their customer.

- Platform Integration (Phase 3)

  The platform vendor uses the Field Upgrade functionality to install the new TOE firmware on hardware of a previous TOE before delivery of the platform to the end user.

  Note the platform vendor may use different ways for delivery of the field upgrade data to the end user, e.g. using update mechanisms of operating systems running on the platform.

- Operational usage (Phase 4)

  The platform vendor or the end user may use the Field Upgrade functionality to install the new TOE firmware on hardware of a previous TOE after delivery of the platform to the end user. The preparative procedures for operational usage of the new certified TOE include secure acceptance procedures for use by the end user. After Field Upgrade the new TOE will be ready for operational use in the environment of the end user.

The installation of the new firmware may be performed in Phase 3 or Phase 4. The previous TOE verifies the integrity and authenticity of TOE field upgrade data as provided by the TOE firmware manufacturer. But the new TOE may or may not be a certified TOE depending on the TOE vendor or platform vendor certification policy. Thus, the user of the TOE shall be made aware of these changes, whether the installed firmware is certified, and which version of a certified TOE is installed.

3 Conformance Claims (ASE_CCL)

3.1 CC Conformance Claim

This Security Target (ST) and the TOE claim conformance to Common Criteria version v3.1 part 1 [1], part 2 [2] and part 3 [3].

Conformance of this ST is claimed for:
Common Criteria part 2 conformant and Common Criteria part 3 conformant.

3.2 PP Claim

This Security Target claims no conformance to a Protection Profile.

3.3 Package Claim

This Security Target claims no conformance to a package of a Protection Profile.

The assurance level for the TOE is EAL4 augmented with ALC_FLR.1 and AVA_VAN.4 defined in CC part 3 [3].

3.4 Conformance Claim Rationale

This security target claims no conformance to a Protection Profile.

3.5 Application Notes

None

4 Security Problem Definition (ASE_SPD)

4.1 Assets and Threats

This section of the security problem definition shows the assets of the TOE to be protected and the threats that are considered.

The assets are:

- Objects, operations and security attributes for the TOE state control SFP as defined in the Table 8.

These assets have to be protected while being executed as well as when the TOE is not in operation. The threats are directed against the assets.

The threats to security are defined in the following table.

Table 2: Threats

#	Threat	Description
1	T.Bypass	An unauthorised individual or user may tamper with TSF, security attributes or field upgrade data in order to bypass TOE security functions and gain access to TOE assets.
2	T. Hack_Crypto	Cryptographic operation may be incorrectly implemented, allowing an unauthorised individual or user to compromise or modify encrypted field upgrade data undetected.
3	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. The attacker may be a hostile user of the TOE.

4.2 Organisational Security Policies

The organisational security policies are defined in the following table.

Table 3: Organisational Security policies

#	OSP	Description
1	OSP.FieldUpgrade	The Platform software is allowed to perform Field Upgrade within the certified TOE or installing a new certified TOE before and after delivery to the end user. The end user shall be aware of the certification and the version of the TOE.

4.3 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 assumptions to the IT environment are defined in the following table:

Table 4:Assumptions to the IT Environment

#	Assumption	Description
1	A.Configuration	The TOE will be properly installed and configured based on AGD (user guidance documentations) instructions.

5 Security Objectives (ASE_OBJ)

This section shows the security objectives which are relevant for the TOE.

5.1 Security Objectives for the TOE

The security objectives of the TOE are defined in the following table.

Table 5: Objectives for the TOE

#	Objective	Description
1	O.Tamper_Resistance	The TOE must resist physical tampering of the TSF by hostile users. The TOE must protect assets against leakage.
2	O.Crypto_Key_Man	The TOE must manage FieldUpgrade cryptographic keys in a manner to protect their confidentiality and integrity.
3	O.FieldUpgradeControl	The TOE accepts only authentic update data provided by the TOE vendor for the Field Upgrade process.

5.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are described in the following table.

Table 6: Security Objective for the Operational Environment

#	Objective Name	Description
1	OE.FieldUpgradeInfo	The developer via AGD documentation will instruct the admin how to do the upgrade and that the admin should inform the end user regarding the Field Upgrade process, its result, whether the installed firmware is certified or not, and the version of the certified TOE.

5.3 Security Objectives Rationale

The following table gives an overview of the mapping between the security objectives for the TOE and the functional security requirements. The table shows and the rationale demonstrates that each security objective for the TOE is traced back to threats countered by that security objective and OSPs enforced by that security objective; each security objective for the operational environment is traced back to threats countered by that security objective, to OSPs enforced by that security objective, and to assumptions upheld by that security objective. All security objectives counter all threats, enforce all organisational security policies and uphold all assumptions.

	O.Tamper_Resistance	O.Crypto_KeyMan	O.FieldUpgradeControl	OE.FieldUpgradeInfo
T.Bypass	X			
T.Hack_Crypto		X		
T.Hack_Physical	X			
OSP.FieldUpgrade			X	X
A.Configuration				X

T.Bypass: An unauthorised individual or user may tamper with TSF, security attributes or other data in order to bypass TOE security functions and gain unauthorised access to TOE assets.

T.Bypass is countered by O.Tamper_Resistance. This objective allow the TOE to invoke the TSF in all actions and to counter the ability of unauthorised users to tamper with TSF, security attributes or other data.

- O.Tamper_Resistance: Requires the TOE to resist physical tampering of the TSF by hostile users. The TOE must protect assets against leakage.

T.Hack_Crypto: Cryptographic operation may be incorrectly implemented, allowing an unauthorized individual or user to compromise or modifying encrypted field upgrade data undetected.

T.Hack_Crypto is countered by O.Crypto_Key_Man. The security objective ensures secure key management and cryptographic operation.

- O.Crypto_Key_Man: Requires the TOE to manage cryptographic keys in a manner to protect their confidentiality and integrity.

T.Hack_Physical: An unauthorised individual or user of the TOE may cause unauthorized disclosure or modification of TOE assets by physically interacting with the TOE. The attacker may be a hostile user of the TOE.

T.Hack_Physical is countered by O.Tamper_Resistance.

- O.Tamper_Resistance requires the TOE to resist physical tampering of the TSF by hostile users. The TOE must protect assets against leakage.

OSP.FieldUpgrade: The Platform software is allowed to perform Field Upgrade within the certified TOE or install a new certified TOE before and after delivery to the end user. The end user shall be aware of the certification and the version of the TOE.

The OSP.FieldUpgrade is implemented by O.FieldUpgradeControl and OE.FieldUpgradeInfo.

- O.FieldUpgradeControl: Ensures that the TOE accepts only authentic update data provided by the TOE vendor for the Field Upgrade process.
- OE.FieldUpgradeInfo: Requires the developer via AGD documentation will instruct the admin how to do the upgrade and that the admin should inform the end user regarding the Field Upgrade process, its result, whether the installed firmware is certified or not, and the version of the certified TOE.

A.Configuration: The TOE will be properly installed and configured based on AGD (user guidance documentations) instructions).

The A.Configuration is directly covered by the objective for the TOE environment OE.FieldUpgradeInfo.

- OE.FieldUpgradeInfo: Requires the developer via AGD documentation will instruct the admin how to do the upgrade and that the admin should inform the end user regarding the Field Upgrade process, its result, whether the installed firmware is certified or not, and the version of the certified TOE.

6 Extended Components Definition (ASE_ECD)

There exist no extended components for this TOE

7 IT Security Requirements (ASE_REQ)

This section describes the security functional requirements (SFR) and the security assurance requirements (SAR) to be fulfilled by the TPE.

Table 7: Subjects

Subject	Description	TSF data
World	Entity not authenticated	(none)

The following table defines Protected Objects that are user data or TSF data depending on the context in which they are used, the operations applicable to these objects and their security attributes.

Table 8: Protected Objects, operations, security attributes

#	Protected Objects	Operations	Security attributes
1	Field upgrade data	Load/Install	Signature and Digest

7.1 Preface regarding Security Level related to Cryptography

The strength of the cryptographic algorithms was not rated in the course of the product certification (see [23] Section 9, Para.4, Clause 2). But cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functions it shall be checked whether the related cryptographic operations are appropriate for the intended system. Some further hints and guidelines can be derived from the "Technische Richtlinie BSI TR-02102", www.bsi.bund.de.

7.2 Security Functional Requirements for the TOE

The security functional requirements (SFR) for the TOE are defined in the following text.

In the following text the assignments are written in "italic style" and the selections are written "underlined".

FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles: *World*.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: *key zeroise method* that meets the following:

FIPS PUB 140-2 [F1402], section 4.7.6 (overwriting all bits with "0").

FCS_COP.1/AES Cryptographic operation (symmetric encryption/decryption)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/AES
The TSF shall perform *symmetric encryption and decryption* in accordance with a specified cryptographic algorithm *AES in the mode CTR, CMAC and KWP-AD* and cryptographic key sizes *256 bits* that meet the following:

- *ISO/IEC 18033-3: 2005, Information technology - Security techniques – Encryption algorithms -- Part 3: Block ciphers [18033]*
- *ISO/IEC 9797-1, Information technology -- Security techniques – Message authentication codes (MACs) -- Part 1: Mechanisms using a block cipher [97971]*
- *ISO/IEC 10116:2006, Information technology — Security techniques — Modes of operation for an n-bit block cipher [10116]*
- *NIST Special Publication 800-38F Recommendation for Block Cipher Modes for Key Wrapping [80038].*

FCS_COP.1/SHA Cryptographic operation (hash function)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/SHA The TSF shall perform *hash value calculation* in accordance with a specified cryptographic algorithm *SHA-256 and SHA-512* and cryptographic key sizes *none* that meet the following:

- *FIPS PUB 180-4, Federal Information Processing Standard 180-4 Secure Hash Standard (SHS) [F1804].*

FCS_COP.1/ECDSA Cryptographic operation (ECC signature verification)

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ECDSA The TSF shall perform *signature verification* in accordance with a specified cryptographic algorithm *ECDSA with curve TPM_ECC_NIST_P521* and cryptographic key sizes *521 bits* that meet the following:

ECDSA signature verification:

1. *According to section "6.4.4 Signature Verification Process" in ISO/IEC 14888-3:2006 [14888]:*
   - *6.4.4.2 not supported*
   - *6.4.4.3 not supported:* **–** *the hash-code H of the message is provided by the field update data as input to our function.*

   with curve
   - *ECC_NIST_P521 [F1864].*

FPT_FLS.1/FS Failure with preservation of secure state (fail state)

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_FLS.1.1/FS The TSF shall preserve a secure state when the following types of failures occur:
entering the fail state if
(1) during TPM Restart or TPM Resume, the TPM fails to restore the state saved at the last Shutdown(STATE), the TPM shall enter Failure Mode and return TPM_RC_FAILURE.
(2) failure detected by the module SysSec and hardware errors (traps)

Note: The module SysSec is a part of the TOE operating system, the module implements mechanisms to detect errors in the program flow.

FPT_FLS.1/SD Failure with preservation of secure state (shutdown)

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_FLS.1.1/SD The TSF shall preserve a secure state when the following types of failures occur:
shutdown if
(1) detection of a physical attack,
(2) detection of environmental condition out of spec values.

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist *physical manipulation and physical probing* to the *TSF* by responding automatically such that the SFRs are always enforced.

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.
Dependencies: No dependencies

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE.

Refinement: For this TOE the TSF data are the field upgrade data only.
Even for single chip implementations, the different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically-separated parts of the TOE.

The following table defines additional objects, operations and security attributes for the TPM state control SFP:

Table 9: Objects, operations and security attributes for the TPM state control SFP

#	Objects	Operations	Security attributes

1	**Field update data**
	Data provided by the vendor in order to replace the firmware or parts of the firmware.
		TPM2_FieldUpgradeStartVendor():
		Entering FUM and accepting the first data block of field update data
		TPM2_FieldUpgradeDataVendor()
		Read the following field update data blocks.
			Security attributes of field update data:
			Signature over the first or the complete digest of field update data, generated by the TOE manufacturer
			Digest over each block or the complete field update data

FDP_ACC.2/States Complete access control (operational states)

Hierarchical to: FDP_ACC.1 Subset access control
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1/States The TSF shall enforce the *TPM State Control SFP* on *all subjects and objects* and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/States The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1/States Security attribute based access control (operational states)

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/States The TSF shall enforce the *TPM State Control SFP* to objects based on the following

Subjects as defined in Table 7:

(1) all other subjects; their security attributes are irrelevant for this SFP,

Objects as defined in Table 8 and Table 9:

(1) Field update data with security attributes signature of the TOE manufacturer and digest,

(2) all other objects; their security attributes are irrelevant for this SFP.

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

(1) The world is authorized to change the TPM state to FUM if the authenticity of the first digest or the signature could be successfully verified.

(2) While in FUM state the world is authorized to import or activate field upgrade data only after successful verification of its integrity and authenticity.

(3) The FUM state shall only be left when the last data block has success fully been received by the TOE.

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

FDP_ACF.1.4/States The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*

FMT_MSA.1/States Management of security attributes (operational states)

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/StatesTSF shall enforce the *TPM state control SFP* to restrict the ability to modify the security attributes *TPM state* to *World*.

FMT_MSA.3/States Static attribute initialisation (operational states)

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

FMT_MSA.3.1/States The TSF shall enforce the *TPM state control SFP* to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/States The TSF shall allow the *nobody* to specify alternative initial values to override the default values when an object or information is created.

7.3 Security Assurance Requirements

The security assurance requirements (SAR) of the TOE are the assurance components of the Evaluation Assurance Level 4 (EAL4) as defined in the Common Criteria [1] [2] [3] and augmented with *ALC_FLR.1* and *AVA_VAN.4*. They are all drawn from the Common Criteria V3.1 part 3. The security assurance components are listed in Table 2.

Table 10: Assurance components

#	Assurance Class	Assurance Component	Assurance Components description
1	ADV: Development	ADV_ARC.1	Security architecture description
2		ADV_FSP.4	Complete functional specification
3		ADV_IMP.1	Implementation representation of the TSF
4		ADV_TDS.3	Basic modular design
5	AGD: Guidance documents	AGD_OPE.1	Operational user guidance
6		AGD_PRE.1	Preparative procedures
7	ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
8		ALC_CMS.4	Problem tracking CM coverage
9		ALC_DEL.1	Delivery procedures
10		ALC_DVS.1	Identification of security measures
11		ALC_LCD.1	Developer defined life-cycle model
12		ALC_FLR.1	Basic flow remediation -- augmented
13		ALC_TAT.1	Well-defined development tools
14	ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
15		ASE_ECD.1	Extended components definition
16		ASE_INT.1	ST introduction
17		ASE_OBJ.2	Security objectives
18		ASE_REQ.2	Derived security requirements
19		ASE_SPD.1	Security problem definition
20		ASE_TSS.1	TOE summary specification

21	ATE: Tests	ATE_COV.2	Analysis of coverage
22		ATE_DPT.1	Testing: basic design
23		ATE_FUN.1	Functional testing
24		ATE_IND.2	Independent testing – sample
25	AVA : Vulnerability assessment	AVA_VAN.4	Methodical vulnerability analysis -- augmented

7.4 Security Requirements and Assurance Rationale

The TOE is evaluated on Evaluation Assurance Level 4 (EAL4) as defined in CC [3] and augmented with ALC_FLR.1 and AVA_VAN.4.

EAL4 was selected because the objective of the TOE is to provide users with a moderate to high level of independently assured security to update the TOE to a new product version.

The developer and manufacturer ensure that the TOE is designed and fabricated so that the TSF achieves the desired properties, and it requires a combination of equipment, knowledge, skill, and time to be able to derive design information or affect the development and manufacturing process which could be used to compromise security through attack. This is addressed by the SAR of the class ALC especially by the component ALC_DVS.1

Further the AVA_VAN.4 requires the developer and the manufacturer to provide necessary evaluation evidence that the TOE fulfills its security objectives and is resistant to attack with Moderate potential. The component AVA_VAN.4 will analyze and assess the resistance of the TOE to attacks with Moderate attack potential.

EAL4 is also augmented with ALC_FLR.1 to track and correct the reported and found security flaws in the product.

All these components are contained in the EAL4 package. The component ALC_FLR.1 Basic flow remediation has no dependencies. Therefore, all these dependencies are satisfied by EAL4.

The following table demonstrates that each security objective for the TOE is covered by at least one SFR and each SFR is traced back to at least one security objective for the TOE.

Table 11: Security requirements rationale

TOE Security Functional Requirements Objective	O.Tamper_Resistance	O.Crypto_KeyMan	O.FieldUpgradeControl
FPT_PHP.3	X		
FPT_ITT.1	X		
FCS_CKM.4		X	
FCS_COP.1/AES		X	X
FCS_COP.1/SHA			X
FCS_COP.1/ECDSA		X	X
FMT_SMR.1			X
FDP_ACC.2/States			X
FDP_ACF.1/States			X
FMT_MSA.1/States			X
FMT_MSA.3/States			X

FPT_FLS.1/FS	X		
FPT_FLS.1/SD	X		

A detailed justification required for suitability of the security functional requirements to achieve the security objectives is given below.

The security objective **O.Crypto_Key_Man** requires that the TOE manage FieldUpgrade cryptographic keys in a manner to protect their confidentiality and integrity. This objective is addressed by the following SFR:

- FCS_CKM.4 requires the TSF to be able destroy cryptographic keys in accordance with a specific key destruction method.
- FCS_COP.1/AES requires that the TSF provides the ability to perform symmetric encryption and decryption of data.
- FCS_COP.1/ECDSA requires that the TSF provides the ability to perform signature verification of data.

The security objective **O.Tamper_Resistance** requires the TOE to resist physical tampering of the TSF by hostile users. This security objective is addressed by the following SFR:

- FPT_PHP.3 which requires that the TSF resists physical manipulation and physical probing.
- FPT_ITT.1 that require the TSF to prevent the disclosure of field update data when transmitted between physically separated parts of the TOE.
- FPT_FLS.1/FS and FPT_FLS.1/SD as the TSF preserve a secure state when the different types of failures are detected.

The security objective **O.FieldUpgradeControl** requires that the TOE accepts only authentic field update data provided by the TOE vendor. This objective is addressed by the following SFRs:

- FMT_SMR.1 defines a set of roles that the TSF shall maintain. Also, the association of users with these roles is required by this SFR.
- FDP_ACC.2/States requires that the TSF enforces the TPM State Control SFP on all subjects, objects and operations among subjects and objects covered by the SFP. The operations shall be covered by an access control SFP.
- FDP_ACF.1/States defines rules to enforce a policy regarding the TOE states, transitions between states and required authorisations to change the state of the TOE. This includes the state transition regarding the FUM state and the rules for the required authorisations.
- FMT_MSA.1/States requires that a TSF shall enforce a SFP to restrict the ability to modify the TOE state.
- FMT_MSA.3/States requires that the TSF shall enforce a SFP to provide restrictive default values for security attributes and nobody is authorised to specify alternative default initial values.
- FCS_COP.1/AES requires that the TSF provides the ability to perform symmetric encryption and decryption of data used to prove the authenticity of the field update data.
- FCS_COP.1/SHA requires that the TSF provides the ability to generate hash values used to prove the authenticity of the field update data.
- FCS_COP.1/ECDSA requires that the TSF provides the ability to perform signature verification of data used to prove the authenticity of the field update data.

7.5 Dependencies of Security Functional Requirements

The dependency rationale demonstrates that the dependencies of the SFR are fulfilled or provides an explanation in the case that the dependencies are not fulfilled.

Table 12: SRF Dependency rationale

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FPT_PHP.3	None	No dependency
FPT_ITT.1	None	No dependency
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes, see comment 1
FCS_COP.1/AES	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Yes, see comment 1
FCS_COP.1/SHA	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Yes, see comment 1
FCS_COP.1/ECDSA	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	Yes, see comment 1
FMT_SMR.1	FIA_UID.1	Yes, see comment 2
FDP_ACC.2/States	FDP_ACF.1	Yes, by FDP_ACF.1/States
FDP_ACF.1/States	FDP_ACC.1, FMT_MSA.3	Yes, by FDP_ACC.2/States and FMT_MSA.3/States
FMT_MSA.1/States	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1, FMT_SMF.1	Yes, by FDP_ACC.2/States and FMT_SMR.1, FMT_SMF.1 see comment 3
FMT_MSA.3/States	FMT_MSA.1, FMT_SMR.1	Yes, by FMT_MSA.1/States and FMT_SMR.1
FPT_FLS.1/FS	None	No dependency
FPT_FLS.1/SD	None	No dependency

Comment 1:

The requirement FCS_CKM.1 address the appropriate generation of cryptographic keys used by the specified cryptographic function and is not part of this Security Target. The required keys are imported during the production phase of the TOE. The requirements FDP_ITC.1 and FDP_ITC.2 address the secure import of user data, but no user data is imported into TOE in a secure manner.

End of comment.

Comment 2:

The requirement FIA_UID.1 address the identification of the user, but all users are allowed for the role World.

End of comment

Comment 3:

The requirement FMT_SMF.1 address management functions which are not necessary and used for the TOE.

End of comment.

8 TOE Summary Specification (ASE_TSS)

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

8.1 TOE Security Features

This section contains the definition and description of the security features (SF) of the TOE. The TOE provides five security features (SF) to meet the security functional requirements. The security features are:

SF_CRY:	Cryptographic Support
SF_G&T	General and Test
SF_OBH	Object Hierarchy

8.1.1 SF_CRY - Cryptographic Support

There are several functions within the TOE related to cryptographic support: ECDSA signature verification, AES data encryption and decryption, key destruction and the generation of hash values.

The TOE supports the destruction of cryptographic keys by erasure of memory areas containing cryptographic keys in accordance with FIPS PUB 140-2 [F1402], section 4.7.6.

The covered security functional requirement is FCS_CKM.4.

The TOE performs the encryption and decryption in accordance with the specified cryptographic algorithm AES in the CRT, CMAC and KWP_AD mode and cryptographic key size of 256 bits that meet [18033], [97971], [10116] and [80038].

The covered security functional requirement is FCS_COP.1/AES.

The TOE performs the hash value calculation in accordance with the specified cryptographic algorithm SHA-256 and SHA-512 (cryptographic key sizes not available) that meets [F1804].

The covered security functional requirement is FCS_COP.1/SHA.

The TOE performs signature verification in accordance with the specified cryptographic algorithm ECDSA with curve TPM_ECC_NIST_P521 and cryptographic key sizes 521 bits that meet [14888].

The covered security functional requirement is FCS_COP.1/ECDSA.

The SF_CRY “Cryptographic Support” covers the following security functional requirements:
FCS_CKM.4, FCS_COP.1/AES, FCS_COP.1/SHA and FCS_COP.1/ECDSA.

8.1.2 SF_G&T – General and Test

The TOE provides the role World and associates users with roles. The roles are enforced within the TOE because there are specific commands and specific keys bond to different token.

The covered security functional requirement is FMT_SMR.1.

The TOE preserves a secure state by entering the Fail state when a failure during TOE Restart or Resume occurs, a failure is detected by any crypto operations AES encryption, AES decryption, SHA, ECDSA signature verification or failure of any commands or internal operations and authorization occurs.

The covered security functional requirement is FPT_FLS.1/FS.

The TOE preserves a secure state by shutdown, when detecting a physical attack or an environmental condition which is out of spec value.

The covered security functional requirement is FPT_FLS.1/SD.

The TOE resists physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced.

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

- The correct function of the TOE is only given in the specific range of the environmental operating parameters. To prevent an attack exploiting those circumstances the external clock conditions, the temperature and electromagnetic radiation (e.g. light) are observed to detect if the specified range is left. The TOE falls into the defined secure state in case of a specified range violation. The defined secure state causes the chip internal reset process.
- 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 protection of security critical lines by specific intelligent and intrinsic shielding including secure wiring of security critical signals. The entire design is kept in a non-standard way to prevent attacks using standard analysis methods. A dedicated CPU with a non-public bus protocol is used which makes analysis complicated.
- The readout of data can be controlled with the use of encryption. An attacker cannot use the data obtained by espionage due to their encryption. The memory contents of the TOE are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data.
- The virtual physical address mapping together with the memory management unit **(**MMU) gives the operating system the possibility to define different access rights for memory areas. In case of an access violation the MMU will generate a non-maskable interrupt (NMI) and an interrupt service routine react on the access violation.

The covered security functional requirement is FPT_PHP.3.

The TOE protects TSF data from disclosure when it is transmitted between separate parts of the TOE.

The covered security functional requirement is FPT_ITT.1.

The SF_G&T “General and Test” covers the following security functional requirements:
FMT_SMR.1, FPT_FLS.1/FS, FPT_FLS.1/SD, FPT_PHP.3 and FPT_ITT.1.

8.1.3 SF_OBH - Object Hierarchy

The TOE supports different states during his life-cycle.

The TOE enforces the TPM State Control SFP on all subjects and objects and all operations among subjects and objects covered by the SFP. The TOE ensures that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP and enforces different access control rules on controlled subjects and objects.

The covered security functional requirements are FDP_ACC.2/States and FDP_ACF.1/States.

The TOE enforce the TPM state control SFP to receive field update data in a manner protected from errors and determines on receipt of field update data, whether error has occurred.

The covered security functional requirements are FMT_MSA.1/States and FMT_MSA.3/States.

The SF_OBH “Object Hierarchy” covers the following security functional requirements:
FDP_ACC.2/States, FDP_ACF.1/States, FMT_MSA.1/States and FMT_MSA.3/States.

8.1.4 Assignment of Security Functional Requirements

The justification of the mapping between security functional requirements and the security features is given in sections 8.1.1 – 8.1.3. The results are shown at following table.

Security Functional Requirement	SF_ CRY	SF_ G&T	SF_ OBH
FMT_SMR.1		X	
FCS_CKM.4	X		
FCS_COP.1/AES	X		
FCS_COP.1/SHA	X		
FCS_COP.1/ECDSA	X		
FPT_FLS.1/FS		X	
FPT_FLS.1/SD		X	
FPT_PHP.3		X	
FPT_ITT.1		X	
FDP_ACC.2/States			X
FDP_ACF.1/States			X
FMT_MSA.1/States			X
FMT_MSA.3/States			X

Table 13: Assignment security functional requirement to security features

8.2 Security Function Policy

The TOE enforces user access to cryptographic IT assets in accordance with the following security function policies (SFP)

- TPM State Control SFP

to meet the security functional requirements.

These policies include different subjects (roles), protected objects and operations which are described in the following. A detailed description is given of the subjects and the protected objects with their accompanying operations and security attributes are defined in Table 7 and Table 8.

The Table 8 lists the protected objects and the operation via reference to the used commands.

The policy “TPM State Control SFP” enforces the TOE to fulfill the requirements given in the following security enforcing functions: FDP_ACC.2/States, FDP_ACF.1/States, FMT_MSA.1/States and FMT_MSA.3/States.

9 Reference

9.1 Literature

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1,
Revision 5, CCMB-2017-04-001, April 2017

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1,
Revision 5, CCMB-2017-04-002, April 2017

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1,
Revision 5, CCMB-2017-04-003, April 2017

[4] Common Methodology for Information Technology Security Evaluation Methodology, Evaluation Methodology, Version 3.1,
Revision 5, CCMB-2017-04-004, April 2017

[5] Trusted Platform Module Library Part 1: Architecture, Family ”2.0” Level 00, Trusted Computing Group Revision 01.59, November 8, 2019

[6] Trusted Platform Module Library Part 2: Structures, Family ”2.0” Level 00 Trusted Computing Group Revision 01.59, November 8, 2019

[7] Trusted Platform Module Library Part 3: Commands, Family “2.0” Level 00 Trusted Computing Group Revision 01.59, November 8, 2019

[8] Protection Profile PC Client Specific TPM, TPM Library Specification Family “2.0” Level 0 Revision 1.59, Version 1.3, 29 September 2021
CERTIFICAT ANSSI-CC-PP-2021/02, dated 2021-11-30

[9] TCG PC Client Platform TPM Profile Specification for TPM 2.0, Version 01.05, Rev.14, September 4, 2020, Trusted Computing Group

[10] Trusted Platform Module Library Part 4: Supporting Routines, Family “2.0”, Level 00 Trusted Computing Group Revision 01.59, November 8, 2019

[12] OPTIGA^{TM} TPM SLB 9672 TPM2.0 Application Note User Guidance
Infineon Technologies AG, Revision 1.04, 2021-10-06

[13] OPTIGA^{TM} TPM SLB 9672 TPM 2.0 FW16.xx Errata and Updates,
Infineon Technologies AG, Revision 1.5, 2023-04-12 and
OPTIGA^{TM} TPM SLB 9672 TPM 2.0 FW26.xx Errata and Updates,
Infineon Technologies AG, Revision 1.2, 2023-04-17

[14] OPTIGA^{TM} TPM SLB 9672 FW16.10 Databook, Infineon Technologies AG,
Revision 1.1, 2021-07-22 and
OPTIGA^{TM} TPM SLB 9672 FW16.12 Databook, Infineon Technologies AG,
Revision 1.2, 2022-03-09 and
OPTIGA^{TM} TPM SLB 9672 FW16.13 Databook, Infineon Technologies AG,
Revision 1.3, 2023-04-12 and
OPTIGA^{TM} TPM SLB 9673 FW26.10 Databook, Infineon Technologies AG,
Revision 1.2, 2022-03-09 and
OPTIGA^{TM} TPM SLB 9673 FW26.13 Databook, Infineon Technologies AG,
Revision 1.4, 2023-04-14

[14888] ISO/IEC 14888-3, Information technology - Security techniques – Digital signature with appendix – Part 3: Discrete logarithm based mechanism

[18033] ISO/IEC 18033-3: 2005, Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers

[10116] ISO/IEC 10116:2006, Information technology — Security techniques — Modes of operation for an n-bit block cipher;
NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation. December 2001

[159465] ISO/IEC 15946-5: 2008; Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 5: Elliptic curve generation; Clause 7.3 (definition of ”Barreto-Naehrig (BN) elliptic curve)

[F1402] FIPS PUB 140-2, Security Requirements for Cryptographic Modules, Change Notices (12-03-2003), U.S. Department of Commerce, National Institute of Standards and Technology

[F1804] FIPS PUB 180-4, Federal Information Processing Standard 180-4 Secure Hash Standard (SHS), U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL);
ISO/IEC 10118-3, Information technology — Security techniques — Hashfunctions — Part 3: Dedicated hash functions

[F1864] FIPS PUB 186-4, Federal Information Processing Standards Publication Digital Signature Standard (DSS), National Institute of Standards and Technology

[97971] ISO/IEC 9797-1, Information technology -- Security techniques – Message authentication codes (MACs) -- Part 1: Mechanisms using a block cipher

[FUP] TPM-FieldUpgrade, DoxyGen Documentation, Infineon Technologies AG, 2015-02-20

[80038] NIST Special Publication 800-38F Recommendation for Block Cipher Modes for Key Wrapping, December 2021

9.2 List of Abbreviations

BOS	-	Boot Software
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
DRBG	-	Deterministic Random Number Generator
EAL	-	Evaluation Assurance Level
ECC	-	Error Correction Code
EDC	-	Error Detection Code
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
MPU	-	Memory Protection Unit
OS	-	Operating system
PLL	-	Phase Locked Loop
PP	-	Protection Profile
PSOS	-	Professional Secure Operating System
RMS	-	Resource Management System
RNG	-	Random Number Generator
RAM	-	Random Access Memory
ROM	-	Read Only Memory
SF	-	Security Feature
SFP	-	Security Function Policy
SFR	-	Special Function Register
SPA	-	Simple power analysis
ST	-	Security Target
STS	-	Self Test Software
SW	-	Software
TM	-	Test Mode (STS)
TOE	-	Target of Evaluation
TSF	-	TOE Security Functionality
TSP	-	TOE Security Policy
UM	-	User Mode (STS)
XRAM	-	eXtended Random Access Memory

9.3 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.

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.

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.

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.

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 authorization 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.

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.

Security Feature: 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.

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.

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 authorization 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.

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email: erratum@infineon.com

IMPORTANT NOTICE

The information contained in this Security Target is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this application note must verify any function and other technical information given herein in the real application. Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind (including without limitation warranties of non-infringement of intellectual property rights of any third party) with respect to any and all information given in this Security Target.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.