Security Target

OPTIGA™ Trusted Platform Module SLB9672_2.0 v16 SLB9673_2.0 v26

Common Criteria CC:2022 EAL4 augmented (EAL4+)
Resistance to attackers with MODERATE attack potential

Version: 2.7
Date: 2026-02-02

PUBLIC

Author: Infineon Technologies AG, Connected Secure Systems S CERT

Version 2.7

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	2024-03-11: New FW15.xx Errata and Updates added
2.6	2024-08-27: New TPM software version added, old versions removed
2.7	2026-02-02: Change to CC:2022 and new TPM software versions added

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™ Trusted Platform Module SLB9672_2.0 v16 SLB9673_2.0 v26.
The security target has the version 2.7 and is dated 2026-02-02.

The Target of Evaluation (TOE) is a security IC (Security Controller) with integrated firmware (operating system) and guidance documentation, which is named OPTIGA™ Trusted Platform Module SLB9672_2.0 v16.25.19774.00 SLB9673_2.0 v26.25.19812.00, is internally registered under the development code SLB9672_2.0 v16.25.19774.00 SLB9673_2.0 v26.25.19812.00.

The Security Target is based on the Trusted Computing Group
“Protection Profile PC Client Specific TPM
TPM Library Specification Family “2.0” Level 0 Revision 1.59” (PP, [8]).

The Security Target is built in compliance with Common Criteria CC:2022.

The Security Target considers all relevant current final interpretations.

The certification body of this process is the German BSI, whereas the abbreviation stands for Bundesamt für Sicherheit in der Informationstechnik.

.

	Version	Date	Registration
Security Target	2.7	2026-02-02	Security Target OPTIGA™ Trusted Platform Module SLB9672_2.0 v16 SLB9673_2.0 v26
Target of Evaluation	SLB9672_2.0 v16.25.19774.00 SLB9673_2.0 v26.25.19812.00		OPTIGA™ Trusted Platform Module SLB9672_2.0 v16.25.19774.00 SLB9673_2.0 v26.25.19812.00 in the delivery format: as defined in section 2.2.4
Protection Profile	Version 1.3	2021-09-29	Protection Profile PC Client Specific TPM TPM Library Specification Family “2.0” Level 0 Revision 1.59 CERTIFICAT ANSSI-CC-PP-2021/02
Guidance Documentation	Rev. 01.59 Rev. 01.59 Rev. 01.59 Rev. 01.59 Version 1.1 Version 1.05 Revision 14 Rev. 1.8 Rev. 1.8 Rev. 1.04 Rev. 1.8 Rev. 1.4	November 8, 2019 November 8, 2019 November 8, 2019 November 8, 2019 June 18, 2020 September 4, 2020 2026-01-07 2026-01-07 2021-10-06 2026-01-13 2026-01-21	Trusted Platform Module Library Part 1: Architecture, Family ”2.0” Level 00 Revision 01.59 Trusted Platform Module Library Part 2: Structures Family ”2.0” Level 00 Revision 01.59 Trusted Platform Module Library Part 3: Commands Family ”2.0” Level 00 Revision 01.59 Trusted Platform Module Library Part 4: Supporting Routines Family ”2.0” Level 00 Revision 01.59 Errata for TCG Trusted Platform Module Library, Family “2.0” Level 00 Revision 1.59 November 8, 2019 TCG PC Client Platform TPM Profile Specification for TPM 2.0 OPTIGA™ TPM SLB 9672 TPM2.0 Extended datasheet for v16.25.19774.00 OPTIGA™ TPM SLB 9673 TPM2.0 Extended datasheet for v26.25.19812.00 OPTIGA™ TPM 2.0 Application Note User Guidance OPTIGA™ TPM SLB 9672 TPM 2.0 FW16.xx Errata and Updates OPTIGA™ TPM SLB 9673 TPM 2.0 FW26.xx Errata and Updates all documents in the delivery format: *.pdf

	CC:2022 Revision 1	November 2022	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2022-11-001 Part 2: Security functional requirements CCMB-2022-11-002 Part 3: Security assurance components CCMB-2022-11-003 Part 4: Framework for the specification of evaluation methods and activities CCMB-2022-11-004 Part 5: Pre-defined packages of security requirements CCMB-2022-11-005 Common Methodology for Information Technology Security Evaluation Part 6:, Evaluation methodology CCMB-2022-11-006
	Version 1.1	2024-07-22	Common Criteria Maintenance Board CC Errata and Interpretation, Errata and Interpretation for CC:2022 (release 1) and CEM:2022 (release 1), Version 1.1, 2024-07-22

Table 1: Identification

Remarks to the Target of Evaluation (TOE):

The TOE of this Security Target encloses the following versions:
SLB9672_2.0 v16.25.19774.00 SLB9673_2.0 v26.25.19812.00.

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 are the extended temperature range, the packaging and the own intermediated IFX certificate.

The derivatives are listed in the documents OPTIGA™ TPM SLB 9672 TPM 2.0 FW16.xx Errata and Updates and in OPTIGA™ TPM SLB 9673 TPM 2.0 FW26.xx Errata and Updates [13] in section 5 “Sales Order Code”. The documents OPTIGA™ TPM SLB 967x TPM2.0 Extended datasheet 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™ Trusted Platform Module SLB9672_2.0 v16.25.19774.00 SLB9673_2.0 v26.25.19812.00and gives a summary product definition. The following description is valid for all the versions and derivatives of the target of evaluation.

The OPTIGA™ Trusted Platform Module SLB9672_2.0 SLB9672_2.0 v16.25.19774.00 SLB9673_2.0 v26.25.19812.00, called “TPM” or “TOE” in the following text, 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. The TPM is a complete solution implementing the version 2.0 of the TCG Trusted Platform Module Library, Family “2.0” Level 00, [TPM] and the TCG PC Client Platform TPM Profile Specification for TPM 2.0, [9] and fulfills the requirements for an evaluation according [F1402].

The SLB9672_2.0 v16.25.19774.00 uses the Serial Peripheral Interface (SPI) for the integration into existing mainboards. The SLB9673_2.0 v26.25.19812.00 uses the Inter-Integrated Circuit (I2C) interface for the integration into existing mainboards. The SLB9672_2.0 v16 and SLB9673_2.0 v26 are basically secure controller with the following added functionality:

- Random number generator (DRBG)
- Asymmetric key generation (RSA keys with key length 1024, 2048, 3072 and 4096 bits, EC keys with key length 256 bits and 384 bits)
- Symmetric key generation (AES keys with 128, 192 and 256 bits)
- Symmetric and asymmetric key procedures (encryption/decryption, generation and verification of digital signatures)
- Hash algorithms (SHA-1, SHA-256, SHA-384) and MAC (HMAC)
- Secure key and data storage
- Identification and Authorization 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 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 assets, threats, security objectives and the security functional requirements are defined in the Protection Profile PC Client Specific TPM TPM Library Specification Family “2.0” Level 0 Revision 1.59”, [8], and are referenced here.

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 OPTIGA™ Trusted Platform Module SLB9672_2.0 v16.25.19774.00 SLB9673_2.0 v26.25.19812.00. 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. The following is a more detailed description of the TOE than in the “Protection Profile PC Client Specific TPM TPM Library Specification Family “2.0” Level 0 Revision 1.59” [8] as it belongs to the specific TOE.

2.1 TOE Definition

The Target of Evaluation (TOE) is the “OPTIGA™ Trusted Platform Module SLB9672_2.0 v16.25.19774.00 SLB9673_2.0 v26.25.19812.00” of the Infineon Technologies AG called “TPM” 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 assure authenticity, integrity and confidentiality in e-commerce and internet communications within a Trusted Computing Platform as defined in the Trusted Platform Module Library specification. The TOE is a complete solution implementing the TCG Trusted Platform Module Library, Family “2.0” Level 00, [TPM] and the TCG PC Client Platform TPM Profile Specification for TPM 2.0, [9].

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.

The TPM provides three trusted capabilities (Roots of Trust): the measurement capabilities, the reporting capabilities and the 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 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 TPM is basically a secure controller with the following added TOE security services:

Random Number Generation (DRBG)

The random number generator (DRBG) is the source of randomness in the SLB9672_2.0. The DRBG is a protected capability with no access control, intermediate results from the DRBG are not available to any user. When the data is for internal use by the TPM (e.g. key generation, nonces, randomness) the data is held in a shielded location and is not accessible to any user.

Platform Key Hierarchy

The TPM holds a Platform Primary Seed (PPS) and can generate Platform Keys from the PPS. The TPM creates a PPS whenever it is powered on and no PPS is present. The TPM2_ChangePPS() command may change the PPS by replace it with a new PPS. The platform key hierarchy is controlled by the Platform firmware.

Cryptographic Services

The TPM provides the following cryptographic services:

- the RSA algorithm according to PKCS#1 V2.1 for encryption, secret sharing and digital signature with key sizes of up to 4096 bits. The RSA implementation provides protection and detection of failures during the Chinese Remainder Theorem (CRT) process.
- the ECC algorithms according to ECDH for decryption of ECC key and the ECDSA for signature generation and verification, with key sizes of 256 bits and 384 bits, and the ECDAA for signature generation, with key sizes of 256 bits.
- the AES algorithm in CFB mode with key sizes of 128 bits, 192 bits and 256 bits for symmetric encryption and decryption.
- the Secure Hash Algorithm-1 (SHA-1), the Hash Algorithm-256 (SHA-256) and the Hash Algorithm-384 (SHA-384) as defined by United States Federal Information Processing Standard 180-4.
- the Hash Message Authentication Code (HMAC) for symmetric signing and signature verification defined in ISO/IEC 9797-2.
- the Derived Keys which are intended to be derived multiple times from a keyedHash and are not persistently stored. For RSA keys no derivation is possible.

Key Generation

The TPM generates two different key types, the ordinary keys, which are produced using the DRBG seeded with a TRNG value; and the primary keys, which are produced using a DRGB seeded with the Primary Seed value. The TPM generates asymmetric key pairs for RSA and ECC algorithms in accordance with different standards.
The TPM generates symmetric AES keys with key sizes of 128 bits, 192 bits and 256 bits. The generation function is a protected capability and the private key and the AES 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 DRBG based on NIST standard.

Self-Tests

The TPM provides startup self-tests and a mechanism to allow self-tests to be run on demand of the user. The test result can be read out by the user. Self-tests include checks of the following:

- RNG functionality (according [11] class DRG.3).

- Verification of the RSA/EC sign and verify engine by signing and verifying a known value with a stored RSA/EC key.
- Integrity of the protected capabilities of the TPM.

If a failure during any self-test is detected, the part experiencing the failure will return an error code and the TOE enters a secure state.

Identification and Authentication

The TPM identification and authentication capability is used to authorize the use of a protected capability and protected object. The TPM provides therefore two basic mechanisms. The first is the prove of knowledge of a shared secret. This shared secret is assigned to the entity as authValue; the second is the authentication of the user and the verification of an intended state of the TPM assigned to the entity as authPolicy. Note that the TCG TPM Module Library specification refers to the identification and authentication process and access control as authorization.

The protected entities and their authentication data may be held within the TPM itself or outside. The identification and authentication protocols use random nonces. This requires that a nonce from one side be in use only for a message and its reply to prevent replay attacks and man-in-the-middle attacks.

Access control is enforced in the SLB9672_2.0 on all data and operations performed on that data. The SLB9672_2.0 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 called security attributes which are listed in the PP [8], Table 8.

Clock and Time

The SLB9672_2.0 provides timing components (Clock, Time, resetCount, restartCount) for use in time-stamping of attestations and for gating policy.

The SLB9672_2.0 provides also monotonic counters as an ever-increasing incremental value (as long the SLB9672_2.0 is powered) for external use.

Support for the Root of Trust for Measurement

The SLB9672_2.0 supports the integrity measurement of the trusted platform by calculation, storage and reporting of measurement digests of measured values. The measurement values are representation of embedded data or program code scanned and provided to the SLB9672_2.0 by the CPU of the platform (PCPU) controlled by the Core Root of Trust for Measurement (CRTM). The SLB9672_2.0 supports cryptographic hashing of measured values and calculates the measurement digest by extending the value of a Platform Configuration Register (PCR) with a calculated or provided hash value (SHA-1/SHA-256/SHA-384). The PCR are shielded locations of the SLB9672_2.0 which can be reset by SLB9672_2.0 reset or trusted process, written only through measurement digest extensions and read. After each reset the PCPU begins executing the CRTM and then sends values that indicates its identity to the Root of Trust for Storage (RTS).

Root of Trust for Storage

The SLB9672_2.0 provides non-volatile storage as shielded location for data of external entities. The TPM owner controls access to the non-volatile storage. The access control may include the need of authorization of the user, delegations, PCR values and other controls. Additionally the SLB9672_2.0 has the capability of secure storage for an unlimited number of private keys, private keys generated on the TPM or other data, by using external memory of the platform. The data is

transferred in an encrypted file, which contains header information in addition to the data or key, it is called a blob and is outputted by the TPM. The blob can be re-loaded in the TPM when needed, e.g. to use the keys later without ever exposing such keys in the clear outside the TPM.

The TPM holds the Storage Primary Seed (SPS) and generates the Storage Root Keys (SRK) from the SPS. The SRK are roots of Protected Storage Hierarchies associated with the TPM including storage keys in this hierarchy used for symmetric encryption and signing of other keys and data.

Root of Trust for Reporting

The Root of Trust for Reporting reports the contents of the RTS. The values on which the RTR reports, are the evidence of the platform configuration stored in PCR, or audit logs, or key properties. The RTR exposes the measurement digests stored in the PCRs and attest to the authenticity of these measurement digests based on identities. The identity is in the form of asymmetric aliases called Endorsement Keys. Each TPM stores four Endorsement Keys, two RSA Endorsement Keys (2048 bit and 3072 bit) and two ECC Endorsement Keys (NIST P-256 and NIST P-384) and additionally a common Endorsement Primary Seed. Additionally accompanying Endorsement Certificates for each Endorsement Key are stored in the TPM. Each TPM is identified and validated by its Endorsement Key that is used as proof that a TPM is genuine. For assurance that these PCR values accurately reflect that state of the platform (RTM), a binding between the RTR and the RTM is established by the Endorsement Certificate which is generated from the certifying authority. The RSA Endorsement Key, the ECC Endorsement Key, the Endorsement Primary Seed and the accompanying Endorsement Certificates are generated and encrypted by the certifying authority outside the TPM in a secure environment of the manufacturer Infineon Technologies AG and then loaded encrypted into the TPM during the production phase.

Generation and import of the Endorsement Key pair and Endorsement Primary Seed

The TPM includes two ECC Endorsement Keys (EK) and two RSA Endorsement Keys (EK) and the Endorsement Primary Seed (EPS), which can be used to generate additional EKs alternatively. The two ECC Endorsement Keys, the two RSA Endorsement Keys and the Endorsement Primary Seed are generated outside the TPM with the TPM Personalization Certification Authority (TPM-CA) located within the secure production area of the TOE in a secure room. The TPM-CA consists of a Personalization Dataset Generator (PDG) including a hardware security module (HSM-PDA), a Certification Authority (INCA) and a database server. The HSM-PDG generates an Endorsement Primary Seed and derives the ECC Endorsement Keys using a DRBG seeded with the EPS. The RSA Endorsement Key is generated from a proved random number generator by the HSM-PDG and not derived from the Endorsement Seed. The INCA creates the Endorsement Certificates (EK credential) by certifying the public part of the EK. The EK credential is also stored at the database server. During the production process the EPS, the EKs (RSA/ECC) and the EK credentials are stored and transported in encrypted form. The personalization process loads the EPS, the EKs (RSA/ECC) and the EK credentials, which are all encrypted with a TPM individual transport key, together with this TPM individual transport key into the TPM. Within the TPM the EPS and EKs (RSA/ECC) are decrypted with the TPM individual transport key and stored in a shielded location. The generation and import process of the EPS, EKs and Endorsement Certificates (EK credentials) is done completely in the secure production area of the TOE.

Handling of the Endorsement Key pair and Endorsement Primary Seed

The TPM may return the personalized Primary ECC/RSA Endorsement Keys or alternatively the Primary ECC/RSA Endorsement Keys derived from the Endorsement Primary Seed.

Before the first usage of an Primary Endorsement Key, the Primary Endorsement Key has to be generated with the TPM command TPM2_CreatePrimary() or TPM2_CreateLoaded(). This command compares the given command parameter inPublic, a TPM2B_PUBLIC structure (a.k.a. EK Public Area Template) to the EK Public Area Template used for the personalized EKs. If the EK Public Area Templates are the same the TPM will return the personalized RSA or ECC Primary Endorsement Key. Any other EK Public Area Template set lead to the key generation specified by the TCG (Primary Endorsement Keys derived from the personalized Endorsement Primary Seed). This derived Endorsement Keys are not bound to the accompanying Endorsement Certificates and can be alternatively used.

The Endorsement Keys RSA EK and ECC EK, personalized by the TPM vendor, are not visible and changeable for the user, but can be deactivated with the TPM2_EvictControl() and TPM2_FlushContext commands, and can be activated again with the TPM2_CreatePrimary command by the user. As these personalized Endorsement Keys should be used only for the identification of the TPM vendor, the user shall not use these keys for other functions. The Endorsement Keys RSA EK and ECC EK, personalized by the TPM vendor, can be deleted permanently with the vendor specific command TPM2_ZeriozeMfrEk authorized with platformPolicy, after a TPM2_ChangeEPS was processed successfully. The personalized Endorsement Primary Seed (EPS) is not visible and erasable for the user, but it can be changed with the TPM2_ChangeEPS() command to a new random value, if the command is not deactivated by the TPM2_SetCapabilityVendor command. The command TPM2_RestoreMfrEK restores the pre-provisioned Manufacturer Endorsement Key (MfrEK) certificates and enables the generation of the pre-provisioned MfrEK´s with the TPM2_CreatePrimary or TPM2_CreateLoaded commands if the pre-provisioned MfrEK´s have not been erased by executing TPM2_ZeroizeMfrEK.

The vendor specific command TPM2_SetCapabilityVendor used with platform authorization enables the configuration of the availability of the

- NV index storing the TPM unique ID,
- command TPM2_ChangeEPS(),
- command TPM2_EncryptDecrypt2().

During the production phase the so called unique ID is computed, which is unique across all Infineon TPMs and stored as NV index in a reserved Infineon NV index handle area for TPM OEMs. The TPM unique ID can not be changed and is preserved across field upgrades.

To simplify system integration into existing mainboards, the SLB9672_2.0 v16 uses the Serial Peripheral Interface (SPI), the SLB9673_2.0 v26 uses the Inter-Integrated Circuit (I2C) interface.

With these capabilities, the TPM is able to realize the issue of the Trusted Platform Module Library specification 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 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 and 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 SLB9672_2.0 in answering to any challenge, but the user is never able to make the SLB9672_2.0 report false metrics. Moreover, the user is able to create several identities for his interactions.

Offering these features to a system, the SLB9672_2.0 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 SLB9672_2.0 asymmetric encryption functionality. Regarding a network scenario, the client PCs equipped with a SLB9672_2.0 are able to report their platform status to the server so that the network administration is aware of their trustworthiness. In conclusion, the SLB9672_2.0 acting as a service provider to a system helps to make transactions more secure and trustworthy.

The Target of Evaluation, the OPTIGA™ Trusted Platform Module SLB9672_2.0 v16.25.19774.00 SLB9673_2.0 v26.25.19812.00 consists of the following hardware and firmware components.

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

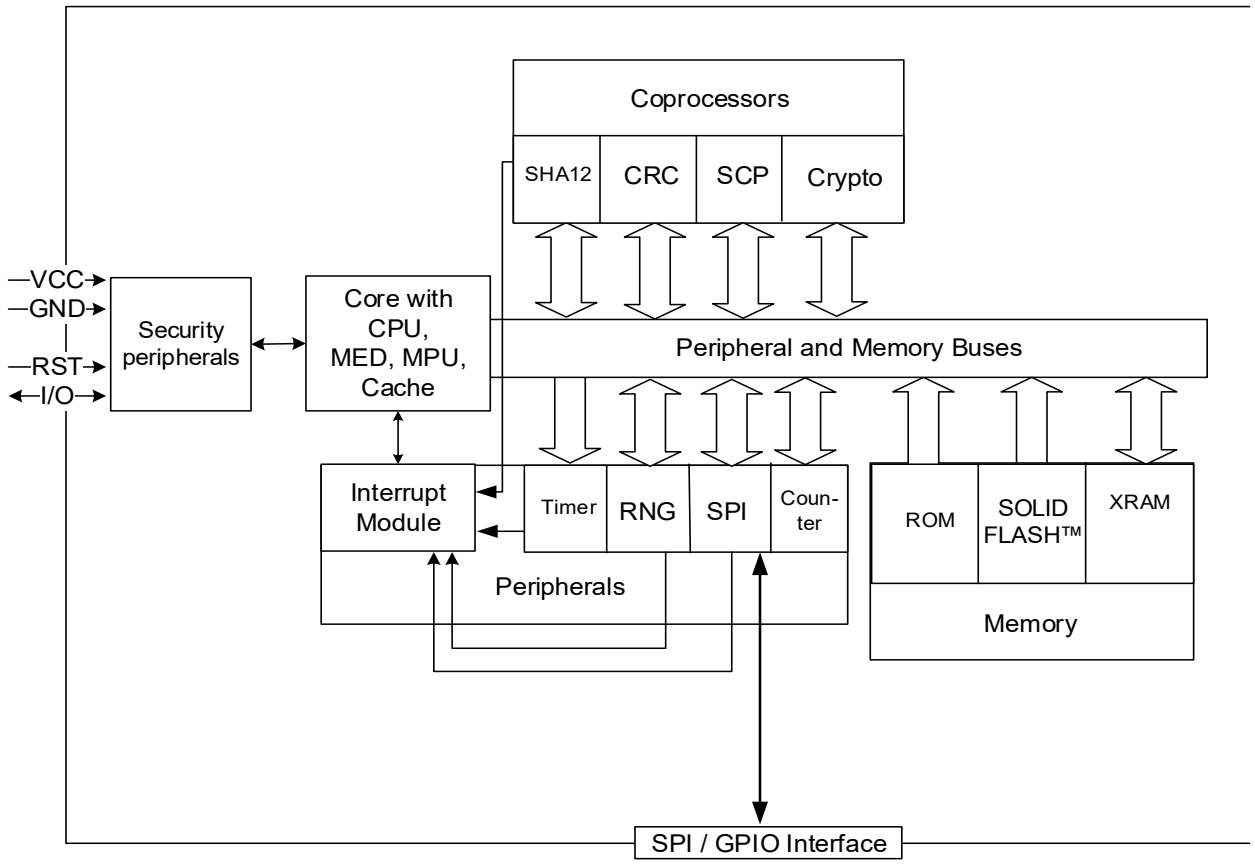
The IC, whose block diagram is shown in Figure 1, consists of a dedicated microprocessor (CPU) with a Memory Protection Unit (MPU), several Coprocessors, several different memories, security logic, shield, timer, an interrupt-controlled I/O interface, a Random Number Generator (RNG), a hardware Hash Accelerator, a Counter, 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™ 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-1, SHA-256 and SHA-384).

[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 TPM

The firmware required for operating the chip includes an operating system that provides the TCG functionality specified in the Trusted Platform Module Library specification. 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 Trusted Platform Module Library specification and a recovery function, 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 SLB9672_2.0.

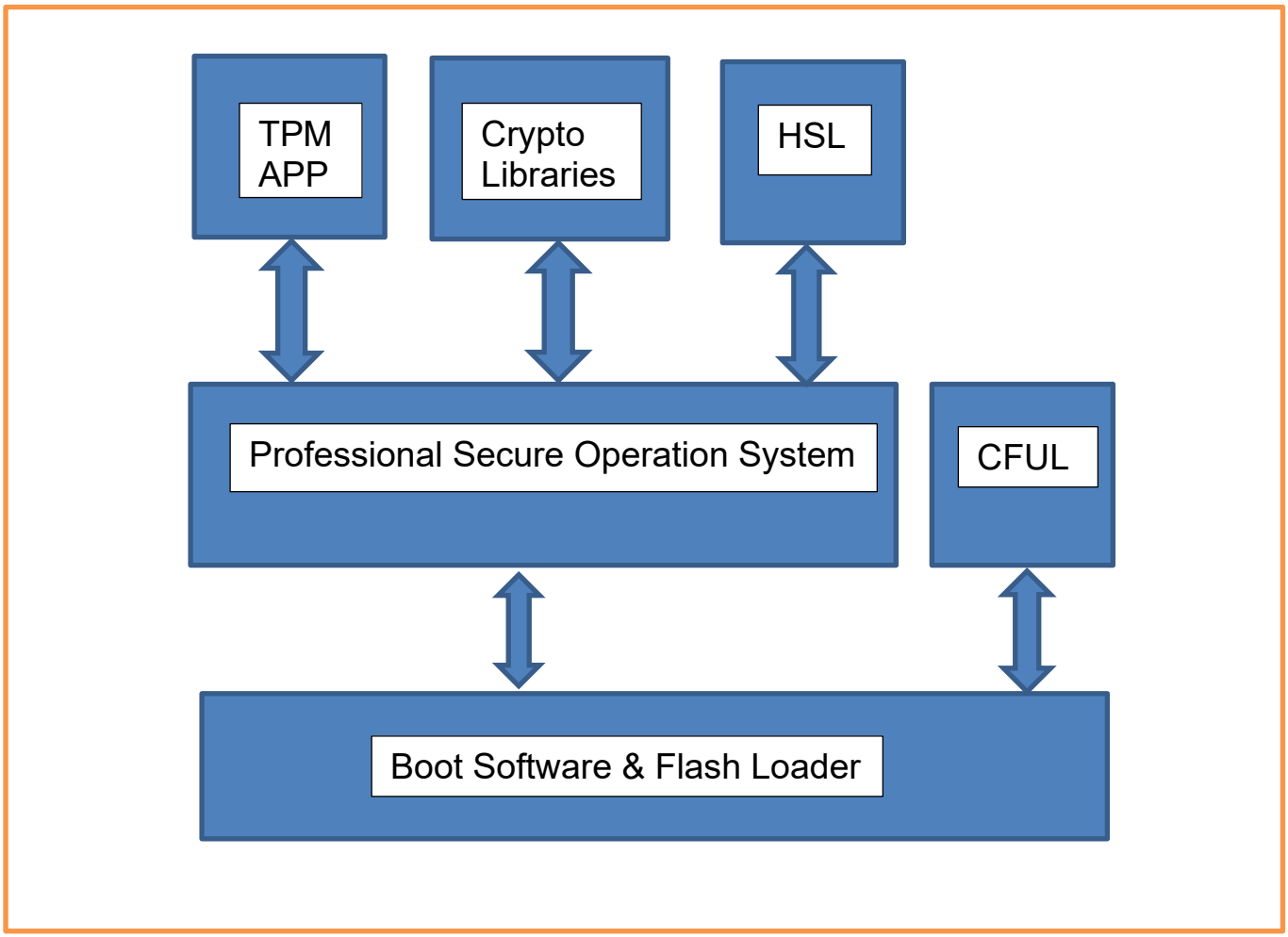


Figure 2: Firmware block diagram of the SLB9672_2.0

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™ NVM memory.

2.2.1 Hardware of the TOE

The *hardware part* of the TOE (cf. Note: The SLB9672_2.0 v16 includes an SPI interface, the SLB9672_2.0 v26 includes an I2C interface) as defined in the PP [8] 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™ NVM
- Coprocessors
  - Crypto2304T for asymmetric algorithms like RSA and ECC
  - Symmetric Crypto Co-processor AES standard (SCP)
  - Hash accelerator (SHA12) for the SHA-1, SHA-256 and SHA-384 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 v16 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 TPM version SLB9672_2.0 v16.24.19084.00 to a newer certified version e.g. SLB9672_2.0 v16.25.19774.00 or to download the actual TPM 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) as defined in the PP [8] 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 different packages (e.g. UQFN) which are listed in the documents OPTIGA™ TPM SLB 9672 TPM 2.0 FW16.xx Errata and Updates and OPTIGA™ TPM SLB 9673 TPM 2.0 FW26.xx Errata and Updates [13].

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 centre 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 PP [8] section 2.2.4 “TPM Life Cycle”. The phase 1 includes the TPM development, the phase 2 includes the TPM manufacturing, the TPM conformance testing, the Platform Primary Seed and the TPM-Mfg EK credential issuance.

3 Conformance Claims (ASE_CCL)

3.1 CC Conformance Claim

This Security Target (ST) and the TOE claim conformance to Common Criteria version CC:2022 part 1 [1], part 2 [2], part 3 [3], part 4 [18], part 5 [19] and Errata and Interpretation for CC:2022 (Release 1) [17] and CEM:2022 (Release 1) [4].

Furthermore, conformance of this ST is claimed for:

Common Criteria version CC:2022 part 2 conformant and part 3 conformant.

3.2 PP Claim

This Security Target is in strict conformance to the
Protection Profile PC Client Specific TPM, TPM Library Specification Family “2.0” Level 0 Revision 1.59, Version 1.3, dated 29 September 2021 [8].

The Protection Profile PC Client Specific TPM, TPM Library Specification Family “2.0” Level 0 Revision 1.59 (PP) is registered and certified by the Agence nationale de la securite des systemes d´information (ANSSI) under the reference
CERTIFICAT ANSSI-CC-PP-2021/02, dated 2021-11-30.

The security assurance requirements of the TOE are according to the “Protection Profile PC Client Specific TPM” [8]. They are all drawn from Part 3 of the Common Criteria version.

3.3 Package Claim

This Security Target claims conformance to the following package from the “Protection Profile PC Client Specific TPM” [8] depending on the TOE configuration:

Package “ECDAA”, conformant, see [8] section 9.

The assurance level for the TOE is EAL4 augmented with ALC_FLR.1 and AVA_VAN.4 defined in CC part 3 [3]. Therefore, this Security target is package-augmented to the packages in PP [8].

3.4 Conformance Claim Rationale

This security target claims strict conformance only to one PP, the PP [8].

The Target of Evaluation (TOE) is a complete solution implementing the TCG Trusted Platform Module Library, Family “2.0”, [5], [6], [7], [10], [15] and the TCG PC Client Platform TPM Profile Specification for TPM 2.0, [9] as defined in the PP [8] section 2.2.1, so the TOE is consistent with the TOE type in the PP [8].

The security problem definition of this security target are consistent with the statement of the security problem definition in the PP [8] in section 5 and 9.3, as the security target claimed strict conformance to the PP [8] and no other threats, organisational security policies and assumptions are added.

The security objectives of this security target are consistent with the statement of the security objectives in the PP [8] in section 6 and 9.6, as the security target claimed strict conformance to the PP [8] and no other security objectives are added.

The security requirements of this security target are consistent with the statement of the security requirements in the PP [8] in section 8 and 9.7, as the security target claimed strict conformance to the PP [8]. All assignments and selections of the security functional requirements are done in the PP [8] and in this security target at section 7.2.

The TOE is designed, produced and/or generated by the TOE Manufacturer.

3.4.1 CC:2022 conformance

With CC:2022 several SFR changes are introduced. Due to this ST claiming conformance to CC:2022 and PP [8], rationales are provided that these changes do not affect the conformance claim to PP [8]:

- FCS_COP.1: for this SFR dependencies are changed in CC:2022. FCS_CKM.4 is removed and instead FCS_CKM.6 added.
- FCS_CKM.1: for this SFR dependencies are changed in CC:2022. Additionally, to FCS_CKM.2 and FCS_COP.1, one further SFR is introduced as alternative: FCS_CKM.5 and additionally FCS_RBG.1 or
  FCS_RNG.1 and FCS_CKM.6 are added. Conformance to PP [8] can still be claimed as FCS_RNG.1 is part of the PP and FCS_CKM.6 replaces FCS_CKM.4 in this security target.
- FCS_CKM.6 replaces FCS_CKM.4 and adds further requirements on the timing of key destruction.
- FCS_RNG.1: this SFR is taken from CC:2022 [2] rather than PP [8]. The SFR is identical in CC2022 [2] so conformance to PP [8] can still be claimed.
- FDP_ETC.2: the FDP_ETC.2.4 is added to the SFR in CC:2022 and also in the security target. Conformance to PP [8] can still be claimed.
- FPT_TST.1: the assign “list of self-tests run by the TSF” is added at FPT_TST.1.1 and included in the security target. Conformance to PP [8] can still be claimed.

Further with CC:2022 some SAR changes were introduced. Rationales are provided that these changes do not affect the conformance claim to PP [8]:

- ASE_CCL.1: for CC:2022 several extensions were introduced (e.g. exact conformance to PP), which add to the already existing assurance requirements. No relaxation was introduced.
- ASE_INT.1: introduction of multi-assurance in combination with PP-configuration: not relevant for PP [8].
- ASE_REQ.2: extended for multi assurance: not relevant for PP [8].
- AVA_VAN.4: extension about third party components introduced. No relaxation was introduced.
- ALC_TAT.1: extension with guidance on the minimum content for an implementation standards description and rules with ADV_COMP.1. No relaxation was introduced.

3.5 Application Notes

The functional requirement FCS_RNG.1 is a refinement of the FCS_RNG.1 defined in the Protection Profile [8] according to “Anwendungshinweise und Interpretationen zum Schema (AIS)” respectively “Functionality classes for random number generators” [11].

4 Security Problem Definition (ASE_SPD)

The content of the PP [8] applies to this chapter completely.

4.1 Assets and Threats

The assets of the TOE are defined in the PP [8], “5.1 Assets” and “9.3.1 Assets”. 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 PP [8], section “5.2 Threats” and “9.3.2 Threats”, no other threats are added.

4.2 Organisational Security Policies

The organisational security policies are defined in the PP [8], section “5.3 Organisational Security Policies” and “9.4 Organisational security policies”, no other organisational security policies are added.

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 PP [8], section “5.4 Assumptions” and “9.5 Assumptions”, no other assumptions are added.

5 Security Objectives (ASE_OBJ)

This section shows the security objectives which are relevant for the TOE. For this section the PP [8] can be applied completely.

5.1 Security Objectives for the TOE

The security objectives of the TOE are defined and described in the PP [8], section “6.1 Security Objectives for the TOE” and “9.6.1 Security Objectives for the TOE”. No other security objectives are added.

5.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are described in the PP [8], section “6.2 Security Objectives for the Operational Environment” and “9.6.2 Security Objectives for the Operational Environment”. No other security objectives for the operational environment are added.

5.3 Security Objectives Rationale

The security objectives rationale is described in the PP [8], section “6.3 Security Objective Rationale” and “9.6.3 Security Objective Rationale”. No other security objectives rationale is added.

6 Extended Components Definition (ASE_ECD)

No extended component definitions are added.

7 IT Security Requirements (ASE_REQ)

For this section the PP [8] section 8 and 9.7 can be applied completely.

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 [20] 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 and described in the PP [8], section 8.1 Security Functional Requirements.

All assignments and selections of the security functional requirements are done in the PP [8] with the exception of the following SFRs. The operations completed in the ST are marked in *italic* font.

FDP_ETC.2/ExIm Export of user data with security attributes (export and import)

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ETC.2.1/ExIm The TSF shall enforce the *Data Export and Import SFP* when exporting user data, controlled under the SFP(s), outside of the TOE.

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

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

FDP_ETC.2.4/ExIm The TSF shall ensure that interpretation of security attributes of the exported user data is as intended by the owner of the user data.

FDP_ETC.2.5/ExIm The TSF shall enforce the following rules when user data is exported from the TOE:

(1) The sensitive area of an object from the TPM hierarchy shall be integrity protected with an HMAC before its export using the command TPM2_Create or TPM2_CreateLoaded. The used key and the IV shall be derived from the secret seed of the parent in the TPM hierarchy.
(2) The sensitive area of an object from the TPM hierarchy shall be symmetrically encrypted before its export using the command TPM2_Create or

TPM2_CreateLoaded. The used key and the IV should be derived from the secret seed of the parent in the TPM hierarchy.

(3) An exported context (using the command TPM2_ContextSave) shall be symmetrically encrypted and integrity protected with a HMAC.

(4) When exporting an object using the command TPM2_Duplicate then the following actions shall be performed:

(a) If the encryptedDuplication attribute is set or the caller provides a symmetric algorithm then the sensitive part of the data shall be symmetrically encrypted and integrity protected (called: inner duplication wrapper).

(b) If the encryptedDuplication attribute is set or the caller provides a new parent in a TPM hierarchy then the inner duplication wrapper shall be symmetrically encrypted and integrity protected (called outer duplication wrapper). The used key shall be derived from a seed that shall be asymmetrically encrypted with the public key of the intended new parent in the TPM object hierarchy.

Note: The FDP_ETC.2 is included as the wording of FDP_ETC.2 of the PP [8] does not match the wording of CC:2022 part 2.

FMT_MSA.2 Secure security attributes

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

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for:
security attributes of keys, PCR, NV storage areas and counter.

Note to FMT_MSA.2:
The TOE supports the mechanism for updating the protected capabilities once the TOE is in the field as defined in the TPM_FieldUpgrade command of the Trusted Platform Module Library specification. Within the scope of the TPM_FieldUpgrade command the security attributes of the TOE are also updated.
End of note.

FCS_CKM.1/PKRSA Cryptographic key generation (RSA primary keys)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1/PKRSA The TSF shall generate cryptographic primary *RSA* keys in accordance with a specified cryptographic key generation algorithm *RSA key generator* and specified cryptographic key sizes *2048 bits, 3072 bits* that meet the following: TPM library specification [5], [6], [7], *and*

RSA key generation:

1. *According to [F1864] section B.3.3 Generation of Random Primes that are Probably Prime and [N890] using CTR_DRBG*

The generated keys are in conformance with:

a) *Sections 3.1 and 3.2 in PKCS#1 v2.1 [RFC3447], for u = 2, i.e., without any (r_i, d_i ,t_i); i > 2:*
   - *3.1 supported for $n < 2^{4096+128}$*
   - *3.2.(1) supported for $n < 2^{4096+128}$*
   - *3.2.(2) supported for $p*q < 2^{4096+128}$*

.

FCS_CKM.1/PKRSA1 Cryptographic key generation (RSA primary keys)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1/PKRSA1 The TSF shall generate cryptographic *primary RSA* keys in accordance with a specified cryptographic key generation algorithm *RSA key generator* and specified cryptographic key sizes *4096 bits* that meet the following: *TPM library specification [5], [6], [7], and*

RSA key generation:

2. *According to [F1864] section B.3.3 Generation of Random Primes that are Probably Prime and [N890] using CTR_DRBG*

The generated keys are in conformance with:

b) *Sections 3.1 and 3.2 in PKCS#1 v2.1 [RFC3447], for u = 2, i.e., without any (r_i, d_i ,t_i); i > 2:*
   - *3.1 supported for $n < 2^{4096+128}$*
   - *3.2.(1) supported for $n < 2^{4096+128}$*
   - *3.2.(2) supported for $p*q < 2^{4096+128}$*

FCS_CKM.1/PKECC Cryptographic key generation (ECC primary keys)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1/PKECC The TSF shall generate cryptographic primary *ECC* keys in accordance with a specified cryptographic key generation algorithm *ECC key*

generator and specified cryptographic key sizes *256 bits, 384 bits* that meet the following: TPM library specification [5], [6], [7], *and*

ECC key generation:

1. *According to [F1864] section B.4.1 Key Pair Generation Using Extra Random Bits and [N890] using CTR_DRBG with curves*
   - *ECC_NIST_P256 [F1864]*
   - *ECC_NIST_P384 [F1864]*
   - *ECC_BN_P256 [159465]*

FCS_CKM.1/PKSYM Cryptographic key generation (SYM primary keys)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1/PKSYM The TSF shall generate cryptographic primary *symmetric* keys in accordance with a specified cryptographic key generation algorithm *AES key generator* and specified cryptographic key sizes *128 bits, 256 bits* that meet the following: TPM library specification [5], [6], [7], *and*

AES key generation:

1. *The AES key is a 128 bit or 256 bit random number according to NIST Special Publication 800-133; Recommendation for Cryptographic Key Generation, section 4 and 6.1 [N8133]*
2. *and*
   NIST Special Publication SP 800-90A, June 2015, Recommendation for Random Number Generation Using Deterministic Random Bit Generators [N890]

FCS_CKM.1/PKSYM1 Cryptographic key generation (SYM primary keys)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1/PKSYM1 The TSF shall generate cryptographic *primary symmetric* keys in accordance with a specified cryptographic key generation algorithm *AES key generator* and specified cryptographic key sizes *192 bits* that meet the following: *TPM library specification [5], [6], [7], and*

AES key generation:

3. *The AES key is a 192 bit random number according to NIST Special Publication 800-133; Recommendation for Cryptographic Key Generation, section 4 and 6.1 [N8133]*
4. *and*
   NIST Special Publication SP 800-90A, June 2015, Recommendation for Random Number Generation Using Deterministic Random Bit Generators [N890]

FCS_CKM.1/RSA Cryptographic key generation (RSA keys)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1/RSA The TSF shall generate cryptographic RSA keys in accordance with a specified cryptographic key generation algorithm *RSA key generator* and specified cryptographic key sizes *1024 bits, 2048 bits, 3072 bits, 4096 bits* that meet the following: TPM library specification [5], [6], [7], *and*

RSA key generation with bit size of 2048 bits, 3072 bits and 4096 bits:

1. *According to [F1864] section B.3.3 Generation of Random Primes that are Probably Prime but with modified Primality Test, and [N890] using CTR_DRBG*

RSA key generation with bit size of 1024 bits:

2. *According to the Infineon key generation method "TPM_RSAGEN2"*

The generated keys with key size of 1024 bits, 2048 bits, 3072 bits and 4096 bits are in conformance with:

a) Sections 3.1 and 3.2 in PKCS#1 v2.1 [RFC3447], for u = 2, i.e., without any (r_i, d_i ,t_i); i > 2:

- *3.1 supported for $n < 2^{4096+128}$*
- *3.2.(1) supported for $n < 2^{4096+128}$*
- *3.2.(2) supported for $p*q < 2^{4096+128}$*

FCS_CKM.1/ECC Cryptographic key generation (ECC keys)

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers]

FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1/ECC The TSF shall generate cryptographic ECC keys in accordance with a specified cryptographic key generation algorithm *ECC key generator* and specified cryptographic key sizes *256 bits, 384 bits* that meet the following: TPM library specification TPM Specification [5], [6], [7], *and*

ECC key generation:

1. *According to [F1864] section B.4.1 Key Pair Generation Using Extra Random Bits and [N890] using CRT_DRGB with curves*
   - *ECC_NIST_P256 [F1864]*
   - *ECC_NIST_P384 [F1864]*
   - *ECC_BN_P256 [159465]*

FCS_CKM.1/SYMM Cryptographic key generation (symmetric keys)

Hierarchical to:	No other components.
Dependencies:	FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1/SYMM The TSF shall generate cryptographic symmetric keys in accordance with a specified cryptographic key generation algorithm *AES key generator* and specified cryptographic key sizes *128 bits, 192 bits, 256 bits* that meet the following: TPM library specification [5], [6], [7], *and*

A*ES key generation:*

1. *The AES key is a 128 bits or 192 bits or 256 bits random number according to NIST Special Publication 800-133; Recommendation for Cryptographic Key Generation, section 4 and 6.1 [N8133].*

FCS_CKM.6 Timing and event of 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 or FCS_CKM.5 Cryptographic key derivation]

FCS_CKM.6.1 The TSF shall destroy *cryptographic keys: primary RSA key, RSA key, primary ECC key, ECC key, primary AES key, AES key* when *on request of the user and automatically in the cryptographic coprocessors if there are no longer used.*

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 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").
The Endorsement Keys RSA EK and ECC EK, personalized by the TPM vendor, can be deleted permanently with the vendor specific command TPM2_ZeriozeMfrEk authorized with platformPolicy, after a TPM2_ChangeEPS was processed successfully.

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, or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of 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 CFB and cryptographic key sizes 128, 256, *192* bits that meet the following:

- ISO/IEC 18033-3: 2005, Information technology - Security techniques – Encryption algorithms -- Part 3: Block ciphers [18033]
- ISO/IEC 10116:2006, Information technology — Security techniques — Modes of operation for an n-bit block cipher [10116].

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, or FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/SHA The TSF shall perform hash value calculation in accordance with a specified cryptographic algorithm SHA-1, SHA-256, SHA-384 and *none* 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/HMAC Cryptographic operation (HMAC calculation)

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, or FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic Key destruction

FCS_COP.1.1/HMAC The TSF shall perform HMAC value generation and verification in

accordance with a specified cryptographic algorithm HMAC with SHA-1, SHA-256, SHA-384 and *none* and cryptographic key sizes *160 bits, 256 bits, 384 bits, 512 bits* that meet the following:

- ISO/IEC 9797-2, Information technology -- Security techniques – Message authentication codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function [9797]
- *ISO/IEC 10118-3: 2004, Information technology -- Security techniques -- Hashfunctions -- Part 3: Dedicated hash-functions [10118]*

FCS_COP.1/RSAED1 Cryptographic operation (asymmetric 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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/RSAED1 The TSF shall perform *asymmetric encryption and decryption* in accordance with a specified cryptographic algorithm *RSA without padding, RSAES-PKCS1-v1_5, RSAES-OAEP,* and cryptographic key sizes *1024 bits* that meet the following: *PKCS#1v2.1 [RFC3447], and*

RSA encryption:

1. *According to section "5.1.1 RSAEP" in PKCS#1 v2.1 [RFC3447]*
   - *Supported for n < $2^{1024+32}$*
   - *5.1.1 (1) not supported*

   and with padding
   - *RSAES-PKCS1-v1_5, [RFC3447] according to section 7.2*
   - *RSAES-OAEP, [RFC3447] according to section 7.1*

RSA decryption:

2. *According to section "5.1.2 RSADP" in PKCS#1 v2.1 [RFC3447] for u = 2, i.e., without any (r_i, d_i ,t_i); i > 2:*
   - *5.1.2(1) not supported*
   - *5.1.2(2.a) supported for n < $2^{1024+32}$*
   - *5.1.2(2.b) supported for p *q < $2^{1024+32}$*
   - *5.1.2(2.b) (ii)&(v) not applicable due to u = 2*

   and with padding
   - *RSAES-PKCS1-v1_5, [RFC3447] according to section 7.2*
   - *RSAES-OAEP, [RFC3447] according to section 7.1*

FCS_COP.1/RSAED Cryptographic operation (asymmetric 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 without security attributes, or
FCS_CKM.1 Cryptographic key generation, or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/RSAED The TSF shall perform asymmetric encryption and decryption in accordance with a specified cryptographic algorithm RSA without padding, RSAES-PKCS1-v1_5, RSAES-OAEP, and cryptographic key sizes 2048 bits, 3072 bits and *4096 bits* that meet the following: PKCS#1v2.1 [RFC3447], *and*

RSA encryption:

1. *According to section "5.1.1 RSAEP" in PKCS#1 v2.1 [RFC3447]*
   - *Supported for n < $2^{4096+128}$*
   - *5.1.1 (1) not supported*

   and with padding
   - *RSAES-PKCS1-v1_5, [RFC3447] according to section 7.2*
   - *RSAES-OAEP, [RFC3447] according to section 7.1*

RSA decryption:

2. *According to section "5.1.2 RSADP" in PKCS#1 v2.1 [RFC3447] for u = 2, i.e., without any (r_i, d_i ,t_i); i > 2:*
   - *5.1.2(1) not supported*
   - *5.1.2(2.a) supported for n < $2^{4096+128}$*
   - *5.1.2(2.b) supported for p*q < $2^{4096+128}$*
   - *5.1.2(2.b) (ii)&(v) not applicable due to u = 2*

   and with padding
   - *RSAES-PKCS1-v1_5, [RFC3447] according to section 7.2*
   - *RSAES-OAEP, [RFC3447] according to section 7.1*

FCS_COP.1/RSASign1 Cryptographic operation (RSA signature generation/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, or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/RSASign1 The TSF shall perform *signature generation and verification* in accordance with a specified cryptographic algorithm *RSASSA-PKCS1-v1_5, RSASSA_PSS* and cryptographic key sizes *1024 bits* that meet the following: *PKCS#1v2.1 [RFC3447], and*

RSA signature generation:

1. *According to section "5.2.1 RSASP1" in PKCS#1 v2.1 [RFC3447] for u = 2, i.e., without any (r_i, d_i ,t_i); i > 2:*
   - *5.2.1(1) not supported*
   - *5.2.1(2.a) supported for n < $2^{1024+32}$*
   - *5.2.1(2b) supported for p*q < $2^{1024+32}$*
   - *5.2.1(2.b) (ii)&(v) not applicable due to u = 2*

and with

- *RSASSA-PKCS1-v1_5, [RFC3447] according to section 8.2*
- *RSASSA_PSS, [RFC3447] according to section 8.1*

RSA signature verification:

2. *According to section "5.2.2 RSAVP1" in PKCS#1 v2.1 [RFC3447]*
   - *Supported for n < 2 $^{1024+32}$*
   - *5.1.1 (1) not supported*

and with

- *RSASSA-PKCS1-v1_5, [RFC3447] according to section 8.2*
- *RSASSA_PSS, [RFC3447] according to section 8.1*

FCS_COP.1/RSASign Cryptographic operation (RSA signature generation/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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/RSASign The TSF shall perform signature generation and verification in accordance with a specified cryptographic algorithm RSASSA-PKCS1-v1_5, RSASSA_PSS and cryptographic key sizes 2048 bits, 3072 bits and *4096 bits* that meet the following: PKCS#1v2.1 [RFC3447], *and*

RSA signature generation:

1. *According to section "5.2.1 RSASP1" in PKCS#1 v2.1 [RFC3447] for u = 2, i.e., without any (r_i, d_i ,t_i); i > 2:*
   - *5.2.1(1) not supported*
   - *5.2.1(2.a) supported for n < 2 $^{4096+128}$*
   - *5.2.1(2b) supported for p*q < 2 $^{4096+128}$*
   - *5.2.1(2.b) (ii)&(v) not applicable due to u = 2*

and with

- *RSASSA-PKCS1-v1_5, [RFC3447] according to section 8.2*
- *RSASSA_PSS, [RFC3447] according to section 8.1*

RSA signature verification:

2. *According to section "5.2.2 RSAVP1" in PKCS#1 v2.1 [RFC3447]*
   - *Supported for n < 2 $^{4096+128}$*
   - *5.1.1 (1) not supported*

and with

- *RSASSA-PKCS1-v1_5, [RFC3447] according to section 8.2*
- *RSASSA_PSS, [RFC3447] according to section 8.1*

FCS_COP.1/ECDSA Cryptographic operation (ECC signature generation/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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/ECDSA The TSF shall perform signature generation and verification in accordance with a specified cryptographic algorithm ECDSA with curve TPM_ECC_NIST_P256, TPM_ECC_NIST_P384 and *none* and cryptographic key sizes 256 bits, 384 bits and *none* that meet the following:

ECDSA signature generation:

1. *According to section "6.4.3 Signature process" in ISO/IEC 14888-3:2006 [14888]:*
   - *6.4.3.3 not supported*
   - *6.4.3.5 not supported: – the hash-code H of the message has to be provided by the caller as input to our function.*
   - *6.4.3.7 not supported*
   - *6.4.3.8 not supported*

   with curve
   - *ECC_NIST_P256 [F1864]*
   - *ECC_NIST_P384 [F1864]*

ECDSA signature verification:

2. *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 has to be provided by the caller as input to our function.*

   with curve
   - *ECC_NIST_P256 [F1864]*
   - *ECC_NIST_P384 [F1864]*

FCS_COP.1/ECDAA Cryptographic operation (ECDAA commit)

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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key estruction

FCS_COP.1.1/ECDAA The TSF shall perform signature generation in accordance with a specified cryptographic algorithm ECDAA with curve TPM_ECC_BN_P256 and *none* and cryptographic key sizes 256 and *none* that meet the following: TPM library specification [5], *section C.4.2 ECDAA with curves*

- *ECC_BN_P256 [159465]*

FCS_COP.1/ECDEC Cryptographic operation (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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1/ECDEC The TSF shall perform decryption of ECC key in accordance with a specified cryptographic algorithm ECDH with curve TPM_ECC_NIST_P256, *TPM_ECC_NIST_P384* and *none* and cryptographic key sizes 256 bits, 384 bits and *none* that that meet the following: TPM library specification [5], NIST Special Publication 800-56A [N856], *section 6.2.2.2*.

FIA_UID.1 Timing of identification

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

FIA_UID.1.1 The TSF shall allow
(1) to execute indication _TPM_Hash_Start, _TPM_Hash_Data and _TPM_Hash_End,
(2) to execute commands that do not require authentication,
(3) to access objects where the entity owner has defined no authentication requirements (authValue, authPolicy),
(4) none

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FPT_TST.1 TSF testing

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

FPT_TST.1.1 The TSF shall run a suite of self tests

(1) at the request of the authorized user “World”
(a) the TPM2_SelfTest command and of selected algorithms using the TPM2_IncrementalSelfTest command,

(2) at the conditions
(a) Initialization state after reset and before the reception of the first command,
(b) prior to execution of a command using a not self-tested function,

(3) *none*

to demonstrate the correct operation of sensitive parts of the TSF: *UMSLC self-tests run by the TSF*.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of *the following TSF data: platformAuth, platformPolicy, ownerAuth, ownerPolicy, lockoutAuth, lockoutPolicy, authValue and authPolicy.*

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of the TSF.

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 by entering the Fail state when the following types of failures occur:
(1) If 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 TPM2_ContextLoad when the decrypted value of sequence is compared to the stored value created by TPM2_ContextSave(),
(3) failure detected by self-test according to FPT_TST.1,
(4) *failure detected by the module SysSec and hardware errors (traps)*

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

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.

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[2]:
(1) Platform firmware with the security attributes platformAuth, platformPolicy and physical presence if supported by the TOE,
(2) all other subjects; their security attributes are irrelevant for this SFP,
Objects as defined in Table 8[3] and Table 9[4]:

[2] located in the Protection Profile [8]

[3] located in the Protection Profile [8]

[4] located in the Protection Profile [8]

(1) Shutdown BLOB with the security attribute validation status,
(2) Firmware update data with security attributes signature of the TPM manufacturer and digest,
(3) 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 *Platform firmware* 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 Platform firmware is authorized to import or activate firmware data only after successful verification of its integrity and authenticity (see FDP_UIT.1/States).
(3) The FUM state shall only be left when *the last data block has success fully been received by the TOE*.
(4) In the Init state the subject “World” is authorized to execute the commands TPM2_Startup and the sequence _TPM_Hash_Start, _TPM_Hash_Data, and _TPM_Hash_End.
(5) In the Init state every subject is authorized to process the Resume operation on the Shutdown BLOB with state transition to Operational.
(6) In the Init state every subject is authorized to process the Restart operation on the Shutdown BLOB with state transition to Operational.
(7) In the Init state, if no Shutdown BLOB was generated or if the Shutdown BLOB is invalid (see attribute “Validation status”) every subject is authorized to process the TPM2_Startup command. In case of the parameter TPM_SU_CLEAR the TPM shall change the state to Operational and initialize its internal operational variables to default initialization values (Reset), otherwise the TPM shall return an error and stay in the same state.
(8) In the Operational state, nobody is authorized to execute the commands TPM2_Startup. For all other subjects, objects and operations, the access control rules of the Access Control SFP shall apply (see FDP_ACF.1/AC).
(9) The Operational state shall change to Self-Test state if the command TPM2_Selftest or TPM2_IncrementalSelfTest is executed or when a test of a dedicated functionality is required (see FPT_TST.1). In the Self-Test state, nobody is authorized to execute any other TPM commands.
(10) The Self-Test state shall be left only after finishing the intended test of the dedicated functionality. In case of a successful test result the state shall change to Operational, otherwise to Fail.
(11) In the Fail state, every subject is authorized to execute the commands TPM2_GetTestResult and TPM2_GetCapability.
(12) In the Fail state the subject World is authorized to send a _TPM_Init indication with state change to Init.
(13) Any subject is authorized to prepare the TPM for a power cycle using the TPM2_Shutdown command and to create a shutdown BLOB by TPM2_Shutdown(TPM_SU_STATE).

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:

(1) Once the TPM receives a TPM2_SelfTest command and before completion of all tests, the TPM shall return TPM_RC_TESTING for any command that uses a command that requires a test.

FDP_UIT.1/States Data exchange integrity (operational states)

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1/States The TSF shall enforce the TPM state control SFP to receive firmware update data in a manner protected from *modification, deletion, insertion, replay* errors.

FDP_UIT.1.2/States The TSF shall be able to determine on receipt of firmware update data, whether *modification, deletion, insertion, replay* has occurred.

FDP_ACF.1/AC Security attribute based access control (access control)

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

FDP_ACF.1.1/AC The TSF shall enforce the Access Control SFP to objects based on the following
Subjects:
(1) Platform firmware with security attribute authorization state gained by authentication with platformAuth, platformPolicy or physical presence if supported by the TOE,
(2) Platform owner with security attribute authorization state gained by authentication with ownerAuth or ownerPolicy,
(3) Privacy administrator with security attribute authorization state gained by authentication with endorsementAuth or endorsementPolicy,
(4) Lockout administrator with security attribute authorization state,
(5) USER with authentication sate gained with userAuth or authPolicy,
(6) DUP with authentication sate gained with authPolicy,
(7) ADMIN with authentication sate gained with userAuth or authPolicy,
(8) World with no security attributes,
Objects:
(1) User key with security attributes TPM_ALG_ID, TPMA_OBJECT,
(2) TPM objects,
(3) Clock with security attributes: resetCount, restartCount, safe-flag,
(4) Data with security attribute “externally provided”.

FDP_ACF.1.2/AC The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
(1) The Platform firmware authorized with platformAuth, platformPolicy or with physical presence if supported by the TOE and the Platform owner are authorized to control the persistence of loadable objects in TPM memory (TPM2_EvictControl). The physical presence is not required if it is not supported by the TOE or disabled for TPM2_EvictControl command.
(2) The Platform firmware platformAuth, platformPolicy or with physical presence if supported by the TOE and the Platform owner are authorized to advance the value and to adjust the rate of advance of the TPMs clock (TPM2_ClockSet, TPM2_ClockRateAdjust). The physical presence is not required if it is not supported by the TOE or disabled for the TPM2_ClockSet respective TPM2_ClockRateAdjust command.

(3) Any subject is authorized to get the current value of time, clock, resetCount and restartCount and safe (TPM2_ReadClock).
(4) A subject with the role USER endorsed by the Privacy administrator and the keyHandle identifier of a loaded key that can perform digital signatures is authorized to get the current value of time and clock (TPM2_GetTime).
(5) No subject is authorized to set the clock to a value less than the current value of clock using the TPM2_ClockSet command.
(6) No subject is authorized to set the clock to a value greater than its maximum value (0xFFFF000000000000) using the TPM2_ClockSet command.
(7) A subject with the role USER is authorized to generate digital signatures using the command TPM2_Sign for externally provided data (hash). The user authorization shall be done based on the required authorization of the key that will perform signing. The key attributes shall allow the signing operation for externally provided data.
(8) Any subject is authorized to verify digital signatures using the command TPM2_VerifySignature.
(9) Any subject is authorized to request data from the random number generator using the command TPM2_GetRandom.
(10) Any subject is authorized to add additional information to the state of the random number generator using the command TPM2_StirRandom.
(11) Any subject is authorized to perform RSA encryption using the command TPM2_RSA_Encrypt for externally provided data. The key attributes shall allow the encrypt operation for externally provided data.
(12) A subject with the role USER is authorized to perform RSA decryption using the command TPM2_RSA_Decrypt for externally provided data. The user authorization shall be done based on the required authorization of the key that will be used for decryption. The key attributes shall allow the decrypt operation for externally provided data.
(13) Any subject is authorized to generate ECC ephemeral key pairs using the command TPM2_ECDH_KeyGen.
(14) A subject with the role USER is authorized to recover a value that is used in ECC based key sharing protocols using the command TPM2_ECDH_ZGen. The user authorization shall be done based on the required authorization of the involved private key.
(15) Any subject is authorized to request the parameters of an identified ECC curve using the command TPM2_ECC_Parameters.
(16) The subject USER is authorized to start a HMAC sequence using the command TPM2_HMAC_Start.
(17) The subject World is authorized to start a hash or event sequence using the command TPM2_HashSequenceStart.
(18) The subject USER is authorized to add data to a hash, event or HMAC sequence using the command TPM2_SequenceUpdate.
(19) The subject USER is authorized to add the last part of data (if any) to a hash or HMAC sequence using the command TPM2_SequenceComplete.
(20) The subject USER is authorized to add the last part of data (if any) to an event sequence using the command TPM2_EventSequenceComplete.
(21) Any subject is authorized to perform hash operations on a data buffer using the command TPM2_Hash.
(22) A subject with the role USER is authorised to perform HMAC operations on a data buffer. The user authorisation shall be done based on the required authorization of the involved symmetric key.
(23) A subject with the role USER is authorised to generate HMACs using the command TPM2_HMAC for externally provided data (hash). The user authorization shall be done based on the required authorization of the key that will perform the HMAC. The key attributes shall allow the signing operation for externally provided data.

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

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

FCS_RNG.1 Random Number Generation

Hierarchical to: No other components
Dependencies: No dependencies

FCS_RNG.1 Random numbers generation Class DRG.3 according to [11]

FCS_RNG.1.1 The TSF shall provide a *deterministic* random number generator that implements: *NIST SP 800-90A CTR_DRBG. [N890]*

FCS_RNG.1.2 The TSF shall provide random numbers that meet: *Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG*.

Application Note 2: To fulfill the requirements defined in “Anwendungshinweise und Interpretationen zum Schema (AIS)” respectively “Functionality classes for random number generators” [11],
a refinement of the functional requirement FCS_RNG.1 is given in the following:

FCS_RNG.1 Random numbers generation Class DRG.3 according to [11]

FCS_RNG.1.1 The TSF shall provide a *deterministic* random number generator that implements:

(DRG.3.1) If initialized with a random seed using a PTRNG of class PTG.2 as random source, the internal state of the RNG shall have at least 100 bit of entropy and implements: NIST SP 800-90A CTR_DRBG. [N890]

(DRG.3.2) The RNG provides forward secrecy.

(DRG.3.3) The RNG provides backward secrecy even if the current internal state is known.

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

(DRG.3.4) The RNG, initialized with a random seed, during every startup and after 2^{31} requests, of minimal 128 bits using a PTRNG of class PTG.2, generates output for which more than 2^{34} strings of bit length 128 are mutually different with probability $w>1-2^{-16}$.

(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A.

End of Application Note 2.

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], [18], [19] and [17] and augmented with *ALC_FLR.1* and *AVA_VAN.4*. They are all drawn from the Common Criteria CC:2022 part 3 [3]. The security assurance components are listed in Table 2.

The security assurance requirements defined in Table 2 are defined in section 7.2 of the PP [8].

The assurance refinements are taken unchanged from PP [8].

Table 2: 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 Rationale

The security requirements rationale of the TOE are defined and described in the PP [8], section 8.3 “Security Requirements rationale” and in “9.8 Security Requirements rationale” and in the following description.

The mapping of the iterations of FCS_COP.1 and FCS_CKM.1 to the security objectives are the following:

TOE Security Functional Requirements	Objective
FCS_COP.1/RSAED1	O.Export O.Import O.Sessions
FCS_COP.1/RSASign1	O.MessageNR O.Reporting
FCS_CKM.1/PKRSA1	O.Crypto_Key_Man
FCS_CKM.1/PKSYM1	O.Crypto_Key_Man

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

The security objective **O.Export** requires that the TOE protects the confidentiality and integrity of data in case of export. Further, the TOE shall unambiguously associate the data security attributes with the data to be exported. This objective is addressed by the following SFRs:

- FCS_COP.1/RSAED1 requires that the TSF provides the ability to perform RSA based asymmetric encryption and decryption of data.

The security objective **O.Import** requires that the TOE ensures that the data security attributes are being imported with the imported data and that the data is from authorised source. Further,the TOE shall verify the security attributes according to the TSF access control rules. The TOE shall support the protection of confidentiality and the verification of the integrity of imported data (except the verification of the integrity of the data within a sealed data blob). This objective is addressed by the following SFR:

- FCS_COP.1/RSAED1 requires that the TSF provides the ability to perform asymmetric encryption and decryption of data.

The security objective **O.MessageNR** requires that the TOE provides user data integrity, source authentication and the basis for source non-repudiation when exchanging data with a remote system. This objective is addressed by the following SFR:

- FCS_COP.1/RSASign1 requires the TSF to be able to perform signature generation and verification. This can be used to support source authentication and source nonrepudiation when exchanging data with a remote system.

The security objective **O.Sessions** requires that the TOE provides the confidentiality of the parameters of commands within an authorised session and the integrity of the audit log of commands. This objective is addressed by the following SFR:

- FCS_COP.1/RSAED1 requires that the TSF provides the ability to perform asymmetric encryption and decryption of data.

The security objective **O.Reporting** requires that the TOE reports measurement digests and attests to the authenticity of measurement digests. This objective is addressed by the following SFR:

- FCS_COP.1/RSASign1 requires the TSF to be able to perform signature generation and verification. This can be used to support authentication of measurement digests.

The security objective **O.Crypto_Key_Man** requires that the TOE manage cryptographic keys, including there generation and derivation using the TOE random number generator as source of randomness, in a manner to protect their confidentiality and integrity. This objective is addressed by the following SFRs:

- FCS_CKM.1/PKRSA requires the TSF to be able to generate cryptographic RSA keys using the internal random number generator of the TOE.

- FCS_CKM.1/PKSYM1 requires the TSF to be able to generate cryptographic AES keys using the internal random number generator of the TOE.

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_I&A:	Identification and Authentication
SF_G&T	General and Test
SF_OBH	Object Hierarchy
SF_TOP	TOE Operation

8.1.1 SF_CRY - Cryptographic Support

There are several functions within the TOE related to cryptographic support: generation of random numbers, generation of asymmetric key pairs, RSA and ECC digital signature (generation and verification), RSA, ECC and AES data encryption and decryption, key destruction, the generation of hash values and the generation and verification of MAC values.

The TOE supports the generation of cryptographic keys in accordance with the specified cryptographic key generation algorithm *RSA key generator* and *ECC key generator* and specified cryptographic key sizes RSA 1024 bits, 2048 bits, 3072 bits and 4096 bits that meet the following: [RFC3447], [F1864] and [N890] and ECC with key sizes of 256 bits and 384 bits that meet [F1864] and [N890]. The source of randomness is the internal random generator.

The covered security functional requirements are FCS_CKM.1/PKRSA, FCS_CKM.1/PKRSA1, FCS_CKM.1/PKECC, FCS_CKM.1/RSA and FCS_CKM.1/ECC.

The TOE supports the generation of symmetric cryptographic keys in accordance with the specified cryptographic key generation algorithm *AES key generator* and specified cryptographic key sizes 128 bits, 192 bits and 256 bits that meet [N8133] and optional [N890].

The covered security functional requirements are FCS_CKM.1/PKSYM, FCS_CKM.1/PKSYM1 and FCS_CKM.1/SYMM.

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.6.

The TOE performs the encryption and decryption in accordance with the specified cryptographic algorithm AES in the CFB mode and cryptographic key size of 128 bits, 192 bits and 256 bits that meet [18033] and [10116].

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-1, SHA-256 and SHA-384 (cryptographic key sizes not available) that meets [F1804].

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

The TOE performs HMAC value calculation and verification in accordance with the specified cryptographic algorithm HMAC with SHA-1, SHA-256 and SHA-384 and cryptographic key sizes 160 bits, 256 bits, 384 bits and 512 bits that meets [9797] and [10118].

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

The TOE performs asymmetric encryption and decryption in accordance with the specified cryptographic algorithm RSA without padding, RSAES-PKCS1-v1_5, RSAES-OAEP and cryptographic key sizes 1024 bits, 2048 bits, 3072 bits and 4096 bits that meet [RFC3447].

The covered security functional requirements are FCS_COP.1/RSAED1 and FCS_COP.1/RSAED.

The TOE performs signature generation and signature verification in accordance with the specified cryptographic algorithm RSASSA-PKCS1v1_5, RSASSA_PSS and cryptographic key sizes 1024 bits, 2048 bits, 3072 bits and 4096 bits that meet [RFC3447].

The covered security functional requirement is FCS_COP.1/RSASign1 and FCS_COP.1/RSASign.

The TOE performs signature generation and signature verification in accordance with the specified cryptographic algorithm ECDSA with curve TPM_ECC_NIST_P256 and TPM_ECC_NIST_P384 and cryptographic key sizes 256 bits and 384 bits that meet TPM library specification [5] section C.4 and [14888].

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

The TOE performs signature generation in accordance with the specified cryptographic algorithm ECDAA with curve TPM_ECC_BN_P256 and cryptographic key sizes 256 bits that meet TPM library specification [5], section C.4.2.

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

The TOE performs decryption of ECC key in accordance with the specified cryptographic algorithm ECDH with curve TPM_ECC_NIST_P256 and TPM_ECC_NIST_P384 and cryptographic key sizes 256 bits and 384 bits that meet TPM library specification [5] and [N856], section 6.2.2.2.

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

The TOE provides a deterministic random number generator (DRBG) including a true random generator, which is used for the seeding of the DRBG, to provide the random numbers. The TOE provides random numbers that fulfils the requirements from the functional class DRG.3 of [11] and [N890].The TOE uses the internal true random generator as the source for any randomness that the processes defined in SF_CRY may require.

The covered security functional requirement is FCS_RNG.1.

The SF_CRY “Cryptographic Support” covers the following security functional requirements: FCS_CKM.1/PKRSA, FCS_CKM.1/PKRSA1, FCS_CKM.1/PKECC, FCS_CKM.1/PKSYM, FCS_CKM.1/PKSYM1, FCS_CKM.1/RSA, FCS_CKM.1/ECC, FCS_CKM.1/SYMM, FCS_CKM.6, FCS_COP.1/AES, FCS_COP.1/SHA, FCS_COP.1/HMAC, FCS_COP.1/RSAED1, FCS_COP.1/RSAED, FCS_COP.1/RSASign1, FCS_COP.1/RSASign, FCS_COP.1/ECDSA, FCS_COP.1/ECDAA, FCS_COP.1/ECDEC and FCS_RNG.1.

8.1.2 SF_I&A - Identification and Authentication

The TPM provides two mechanisms for the identification and authentication capability to authorize the use of an Protected Object and Protected Capability. Note that the TCG TPM Library specification refers to the identification and authentication process and access control as *authorization*. The first authentication mechanisms is the prove of knowledge of a shared secret (password or secret for HMAC) assigned to the entity as *authValue*. The second mechanism is the authentication of the user and verification of an intended state of the TPM and its environment encoded in *authPolicy* and assigned to the entity.

The TOE provides a mechanism to generate secrets that meet uniform distribution of random variable generating the value, and is able to enforce the use of TSF generated secrets for nonce values for authorization sessions unknown authValues.

The covered security functional requirement is FIA_SOS.2.

The TOE use different rules to set the value of security attributes.

The covered security functional requirement is FMT_MSA.4/AUTH.

The TOE provides the management functionality of the TSF data by user authorization.

The covered security functional requirement is FMT_MTD.1/AUTH.

TOE detects when the maximal tries of unsuccessful authentication attempts occur for objects and NV Index where DA is active and blocks the authorizations for a defined time.

The covered security functional requirement is FIA_AFL.1/Recover.

The TOE detect when one unsuccessful authentication attempt occur using lockoutAuth in the command TPM2_DictionaryAttackLockReset and blocks the TPM2_DictionaryAttackLockReset and TPM2_DictionaryAttackParameters commands for a defined time.

The covered security functional requirement is FIA_AFL.1/Lockout.

TOE detects when the pinCount successful/unsuccessful authentication events exceeds pinLimit for an NV Index with the attributes TPM_NT_PIN_PASS/TPM_NT_PIN_FAIL and blocks further authorization if number of successful/unsuccussful events has been met.

The covered security functional requirements are FIA_AFL.1/PINPASS and FIA_AFL.1/PINFAIL.

The TOE allows access to a defined number of commands and objects for the user to be performed before the user is authenticated/identified.

The covered security functional requirements are FIA_UID.1 and FIA_UAU.1.

The TOE provides different authentication mechanisms to support user authentication and authenticate any user's claimed identity according to the different rules. The TOE provides re-authentication of the user for multiple command processing.

The covered security functional requirements are FIA_UAU.5 and FIA_UAU.6.

The TOE associate security attributes with subjects acting on the behalf of that user. The TOE enforces different rules on the initial association of user security attributes with subjects acting on the behalf of users and enforces different rules governing changes to the user security attributes associated with subjects acting on the behalf of users.

The covered security functional requirement is FIA_USB.1.

The SF_I&A “Identification and Authentication” covers the following security functional requirements: FIA_SOS.2, FIA_MSA.4/AUTH, FMT_MTD.1/AUTH, FIA_AFL.1/Recover, FIA_AFL.1/Lockout, FIA_AFL.1/PINPASS, FIA_AFL.1/PINFAIL, FIA_UID.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.6 and FIA_USB.1.

8.1.3 SF_G&T – General and Test

The TOE provides the roles: Platform firmware, Platform owner, Privacy Administrator, Lockout Administrator, User, Admin, DUP and 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 performs different management functions.

The covered security functional requirement is FMT_SMF.1.

The TOE ensures that only secure values are accepted for security attributes.

The covered security functional requirement is FMT_MSA.2.

The TOE provides reliable time stamps as number of milliseconds the TOE has been powered since initialization of the Clock value.

The covered security functional requirement is FPT_STM.1.

The TOE ensures that any previous information content of a resource is made unavailable upon the deallocation of the resource from defined objects.

The covered security functional requirement is FDP_RIP.1.

The TOE supports a suite of self tests during startup and at the request of an authorized user world to demonstrate the correct operation of sensitive parts of the TSF and to verify the integrity of stored TSF executable code and parts of TSF data.

The covered security functional requirement is FPT_TST.1.

The TOE preserves a secure state by entering the Fail state when a failure during TPM Restart or Resume occurs, a failure is detected by TPM2_ContecxtLoad or the self test, of any crypto operations including RSA encryption, RSA decryption, AES encryption, AES decryption, SHA, RNG, RSA signature generation, HMAC generation 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 electro magnetic 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.
- The data in the EEPROM are automatically monitored by the EDC. In case of a 1 bit error the memory content is corrected by the ECC, in case of more bit errors the TOE enters the secure state.
- 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 can not 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 maskerable interrupt (NMI) and an interrupt service routine react on the access violation.

The covered security functional requirement is FPT_PHP.3.

The TOE enforces the TPM state control, TPM Object Hierarchy, Data import and export, Measurement and reporting, Access Control, NVM and Credential SFPs to prevent the disclosure of user data when it is transmitted between physically-separated parts of the TOE.

The covered security functional requirement is FDT_ITT.1.

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, FMT_SMF.1, FMT_MSA.2, FPT_STM.1, FDP_RIP.1, FPT_TST.1, FPT_FLS.1/FS, FPT_FLS.1/SD, FPT_PHP.3, FDT_ITT.1 and FPT_ITT.1.

8.1.4 SF_OBH - Object Hierarchy

The TOE supports different states during his life-cycle as described in [8] section 7.1.4.1 “TPM Operational States” in detail.

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 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 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 restrict the ability to modify the security attributes TPM state and to provide restrictive default values for security attributes that are used to enforce the SFP. The TOE enforce the TPM state control SFP to receive firmware update data in a manner protected from errors and determines on receipt of firmware update data, whether error has occurred.

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

The TOE supports three different hierarchies, the platform hierarchy, the storage hierarchy and the endorsement hierarchy. The root of each TPM hierarchy is defined by a primary seed which is a random value persistently stored in the TOE. A hierarchy may be disabled.

The TOE monitors user data stored in containers controlled by the TSF for data modifications and modification of hierarchy on all objects, based on the different attributes.

The covered security functional requirement is FDP_SDI.1.

The TOE enforces the TPM Object Hierarchy SFP on defined subjects, objects and operations and enforces different rules to determine if an operation among controlled subjects and controlled objects is allowed and deny access of subjects to objects based on different rules.

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

The TOE enforces the TPM Object Hierarchy SFP to not allow the modification of the security attributes fixedTPM and fixedParent.

The covered security functional requirement is FMT_MSA.1/Hier.

The TOE enforces the TPM Object Hierarchy SFP to provide restrictive default values for security attributes that are used to enforce the SFP and allows the creator of an object in a TPM hierarchy to specify alternative initial values to override the default values when an object or information is created.

The covered security functional requirement is FMT_MSA.3/Hier.

The TOE enforces different rules to set the value of security attributes.

The covered security functional requirement is FMT_MSA.4/Hier.

The TOE allows the import and export of data as an object of a hierarchy.

The TOE enforces the Data Export and Import SFP on subjects, objects and operations. The Data Export and Import SFP enforce different rules to determine if an operation between a controlled subject and controlled object is allowed.

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

The TOE enforce the Data Export and Import SFP to restrict the ability to use the security attribute authorization data to every subject, to provide restrictive default values for security attributes that are used to enforce the SFP and to prevent to override the default values when an object or information is created.

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

The TOE enforces the Data Export and Import SFP when exporting user data, controlled under the SFP(s), outside of the TOE and to export the user data with the user data's associated security attributes. The TOE ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data and different rules are enforced when user data is exported from the TOE.

The covered security functional requirement is FDP_ETC.2/ExIm.

The TOE enforces the Data Export and Import SFP when importing user data, controlled under the SFP(s), outside of the TOE. The correct interpretation, association and use of the security attributes associated with the imported user data are ensured and different rules are enforced when user data is imported from outside the TOE.

The covered security functional requirement is FDP_ITC.2/ExIm.

The TOE enforces the Data Export and Import SFP to transmit user data in a manner protected from unauthorised disclosure and to transmit and receive user data in a manner protected from modification errors. The TOE is able to determine on receipt of user data, whether modification has occurred.

The covered security functional requirements are FDP_UCT.1/ExIm and FDP_UIT.1/ExIm.

The TOE enforces the Measurement and Reporting SFP on subjects, objects and operations. The Measurement and Reporting SFP enforce different rules to determine if an operation among controlled subjects and controlled objects is allowed.

The covered security functional requirements are FDP_ACC.1/M&R and FDP_ACF.1/M&R.

The TOE enforces the Measurement and Reporting SFP to restrict the ability to modify the security attributes PCR attributes, PCR extension algorithm and used hash algorithm to the subject Platform firmware, to provide restrictive default values for security attributes that are used to enforce the SFP, and to prevent to override the default values when an object or information is created.

The covered security functional requirements are FMT_MSA.1/M&R and FMT_MSA.3/M&R.

The TOE is able to generate evidence of origin for transmitted attestation structure and object creation tickets at the request of the originator and provide a capability to verify the evidence of origin of information to recipient given as soon as the recipient can verify the signature and has confidence to the key that is used to sign.

The covered security functional requirement is FCO_NRO.1/M&R.

The SF_OBH “Object Hierarchy” covers the following security functional requirements: FDP_ACC.2/States, FDP_ACF.1/States, FMT_MSA.1/States, FMT_MSA.3/States, FDP_UIT.1/States, FDP_SDI.1, FDP_ACC.1/Hier, FDP_ACF.1/Hier, FMT_MSA.1/Hier, FMT_MSA.3/Hier, FMT_MSA.4/Hier, FDP_ACC.1/ExIm, FDP_ACF.1/ExIm, FMT_MSA.1/ExIm, FMT_MSA.3/ExIm, FDP_ETC.2/ExIm, FDP_ITC.2/ExIm, FDP_UCT.1/ExIm, FDP_UIT.1/ExIm, FDP_ACC.1/M&R, FDP_ACF.1/M&R, FMT_MSA.1/M&R, FMT_MSA.3/M&R and FCO_NRO.1/M&R.

8.1.5 SF_TOP – TOE Operation

The TOE enforces the Access Control SFP on different subjects, objects and operations and enforces different rules to determine if an operation among controlled subjects and controlled objects is allowed. The TOE explicitly authorize access of subjects to objects based on different additional rules and explicitly deny access of subjects to objects based on the different additional rules.

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

The TOE enforces the Access Control SFP to restrict the ability to query and modify different security attributes to specific subjects, to provide restrictive default values for security attributes that are used to enforce the SFP and to specify alternative initial values to override the default values when an object or information is created.

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

The TOE enforces the Access Control SFP to transmit user data in a manner protected from unauthorised disclosure. The TOE provides a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. The TOE initiates communication via the trusted channel and permits another trusted IT product to initiate communication via the trusted channel.

The covered security functional requirements are FDP_UCT.1/AC and FTP_ITC.1/AC.

The TSF shall restrict the ability to disable and enable the functions TPM2_Clear to the subjects Platform firmware and Lockout administrator.

The covered security functional requirement is FMT_MOF.1/AC.

The TSF shall enforce the NVM SFP on different subjects, objects and operations and enforces different rules to determine if an operation among controlled subjects and controlled objects is allowed.

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

The TOE enforces the NVM SFP to restrict the ability to query and modify the security attribute NV index attributes to the authorized role of the subject that executes the NVM related command and to provide restrictive default values when an object or information is created. The TOE prohibits to override the default values with alternative initial values when an object or information is created. The TOE enforces different rules to set the value of security attributes and restrict the ability to modify the authorization secret (authValue) for a NV index to the subject ADMIN.

The covered security functional requirements are FMT_MSA.1/NVM, FMT_MSA.3/NVM, FMT_MSA.4/NVM and FMT_MTD.1/NVM.

The TOE enforces the NVM SFP when importing user data, controlled under the SFP, and ignores any security attributes associated with the user data when imported from outside the TOE. Additionally the TOE enforces different rules when importing user data controlled under the SFP from outside the TOE. The TOE enforces the NVM SFP when exporting user data, controlled under the SFP(s), outside of the TOE.

The covered security functional requirements are FDP_ITC.1/NVM and FDP_ETC.1/NVM.

The TOE enforces the Credential SFP on different subjects, objects and operations and enforces different rules to determine if an operation among controlled subjects and controlled objects is allowed.

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

The TOE enforces the Credential SFP to provide restrictive default values for security attributes that are used to enforce the SFP and prevents to override the default values when an object or information is created. The TOE enforces the Credential SFP to restrict the ability to use the security attributes HMAC in the credential BLOB to the subject USER.

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

The TOE generates evidence of origin for transmitted TPM objects at the request of the originator and relates the information whether the object is resident in an authentic TPM of the originator of the information, and the name and the public area of the TPM object of the information to which the evidence applies. The TOE provides a capability to verify the evidence of origin of information to the initiator given based on a credential BLOB that was generated by the credential provider.

The covered security functional requirement is FCO_NRO.1/Cre.

The SF_TOE “TOE Operation” covers the following security functional requirements: FDP_ACC.1/AC, FDP_ACF.1/AC, FMT_MSA.1/AC, FMT_MSA.3/AC, FDP_UCT.1/AC, FTP_ITC.1/AC, FMT_MOF.1/AC, FDP_ACC.1/NVM, FDP_ACF.1/NVM, FMT_MSA.1/NVM, FMT_MSA.3/NVM, FMT_MSA.4/NVM, FMT_MTD.1/NVM, FDP_ITC.1/NVM, FDP_ETC.1/NVM, FDP_ACC.1/Cre, FDP_ACF.1/Cre, FMT_MSA.1/Cre, FMT_MSA.3/Cre and FCO_NRO.1/Cre.

8.1.6 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 – 8.1.5. The results are shown at following table.

Table 3: Assignment security functional requirement to security features

Security Functional Requirement	SF_ CRY	SF_ I&A	SF_ G&T	SF_ OBH	SF_ TOP
FMT_SMR.1			X		
FMT_SMF.1			X		
FMT_MSA.2			X		
FPT_STM.1			X		
FDP_RIP.1			X		
FCS_RNG.1	X				
FCS_CKM.1/PKRSA	X				
FCS_CKM.1/PKRSA1	X				
FCS_CKM.1/PKECC	X				
FCS_CKM.1/PKSYM	X				
FCS_CKM.1/PKSYM1	X				
FCS_CKM.1/RSA	X				
FCS_CKM.1/ECC	X				
FCS_CKM.1/SYMM	X				
FCS_CKM.6	X				
FCS_COP.1/AES	X				
FCS_COP.1/SHA	X				
FCS_COP.1/HMAC	X				
FCS_COP.1/RSAED1	X				
FCS_COP.1/RSAED	X				
FCS_COP.1/RSASign1	X				
FCS_COP.1/RSASign	X				
FCS_COP.1/ECDSA	X				
FCS_COP.1/ECDAA	X				
FCS_COP.1/ECDEC	X				
FIA_SOS.2		X			

FMT_MSA.4/AUTH		X			
FMT_MTD.1/AUTH		X			
FIA_AFL.1/Recover		X			
FIA_AFL.1/Lockout		X			
FIA_AFL.1/PINPASS		X			
FIA_AFL.1/PINFAIL		X			
FIA_UID.1		X			
FIA_UAU.1		X			
FIA_UAU.5		X			
FIA_UAU.6		X			
FIA_USB.1		X			
FPT_TST.1			X		
FPT_FLS.1/FS			X		
FPT_FLS.1/SD			X		
FPT_PHP.3			X		
FDP_ITT.1			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	
FDP_UIT.1/States				X	
FDP_SDI.1				X	
FDP_ACC.1/Hier				X	
FDP_ACF.1/Hier				X	
FMT_MSA.1/Hier				X	
FMT_MSA.3/Hier				X	
FMT_MSA.4/Hier				X	
FDP_ACC.1/ExIm				X	
FDP_ACF.1/ExIm				X	
FMT_MSA.1/ExIm				X	

FMT_MSA.3/ExIm				X	
FDP_ETC.2/ExIm				X	
FDP_ITC.2/ExIm				X	
FDP_UCT.1/ExIm				X	
FDP_UIT.1/ExIm				X	
FDP_ACC.1/M&R				X	
FDP_ACF.1/M&R				X	
FMT_MSA.1/M&R				X	
FMT_MSA.3/M&R				X	
FCO_NRO.1/M&R				X	
FDP_ACC.1/AC					X
FDP_ACF.1/AC					X
FMT_MSA.1/AC					X
FMT_MSA.3/AC					X
FDP_UCT.1/AC					X
FTP_ITC.1/AC					X
FMT_MOF.1/AC					X
FDP_ACC.1/NVM					X
FDP_ACF.1/NVM					X
FMT_MSA.1/NVM					X
FMT_MSA.3/NVM					X
FMT_MSA.4/NVM					X
FMT_MTD.1/NVM					X
FDP_ITC.1/NVM					X
FDP_ETC.1/NVM					X
FDP_ACC.1/Cre					X
FDP_ACF.1/Cre					X
FMT_MSA.1/Cre					X
FMT_MSA.3/Cre					X
FCO_NRO.1/Cre					X

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
- Access Control SFP
- NVM SFP
- TPM Object Hierarchy SFP
- Measurement and Reporting SFP
- Data Export and Import SFP
- Credential 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 PP [8], section 7.1.1 and in Table 7 and Table 8.

The protected objects treated by the TOE are the data generated or stored in the shielded location or to be imported into or be exported from the shielded locations. The operations of the TOE are the protected capabilities of the TPM which are defined by the TPM commands (cf. [7]).

The Table 8 of the PP [8] lists the protected objects, the operation via reference to the commands as described in the TPM Library specification [7] and the security attributes of the objects as described in the TPM Library specification [6].

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, FMT_MSA.3/States and FDP_UIT.1/States.

The policy “Access Control SFP” enforces the TOE to fulfill the requirements given in the following security enforcing functions: FDP_ACC.1/AC, FMT_MSA.1/AC, FMT_MSA.3/AC and FDP_UCT.1/AC.

The policy “NVM SFP” enforces the TOE to fulfill the requirements given in the following security enforcing functions: FDP_ACC.1/NVM, FDP_ACF.1/NVM, FMT_MSA.1/NVM, FMT_MSA.3/NVM, FDP_ITC.1/NVM and FDP_ETC.1/NVM.

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

The policy “Measuremet and Reporting SFP” enforces the TOE to fulfill the requirements given in the following security enforcing functions: FDP_ACC.1/M&R, FDP_ACF.1/M&R, FMT_MSA.1/M&R and FMT_MSA.3/M&R.

The policy “Data Export and Import SFP” enforces the TOE to fulfill the requirements given in the following security enforcing functions: FDP_ACC.1/ExIm, FDP_ACF.1/ExIm, FMT_MSA.1/ExIm, FMT_MSA.3/ ExIm, ETC.2/ExIm, ITC.2/ExIm, UTC.1/ExIm and UIT.1/ExIm.

The policy “Credential SFP” enforces the TOE to fulfill the requirements given in the following security enforcing functions: FDP_ACC.1/Cre, FDP_ACF.1/Cre, FMT_MSA.1/Cre, and FMT_MSA.3/Cre.

9 Reference

9.1 Literature

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; November 2022, CC:2022 Revision 1, CCMB-2022-11-001

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; November 2022, CC:2022 Revision 1, CCMB-2022-11-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; November 2022, CC:2022 Revision 1, CCMB-2022-11-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, November 2022, CC:2022 Revision 1, CCMB-2022-11-006

[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

[11] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS20 Version 3, 15.05.2013
A propsal for: Functionality classes for random number generators, Version 2.0, 2011-09-18
Bundesamt für Sicherheit in der Informationstechnik (BSI9

[12] OPTIGA™ TPM 2.0 Application Note User Guidance
Infineon Technologies AG, Revision 1.04, 2021-10-06

[13] OPTIGA™ TPM SLB 9672 TPM 2.0 FW16.xx Errata and Updates, Infineon Technologies AG, Revision 1.8, 2026-01-13 and
OPTIGA™ TPM SLB 9673 TPM 2.0 FW26.xx Errata and Updates, Infineon Technologies AG, Revision 1.4, 2026-01-21

[14] OPTIGA™ TPM SLB 9672 FW16.25 Extended datasheet, Infineon Technologies AG, Revision 1.8, 2026-01-07 and
OPTIGA™ TPM SLB 9673 FW26.25 Extended datasheet, Infineon Technologies AG, Revision 1.8, 2026-01-07

[15] Errata for TCG Trusted Platform Module Library, Family “2.0” Level 00 Revision 1.59 November 8, 2019, Version 1.1, June 18, 2020

[17] Common Criteria Maintenance Board CC Errata and Interpretation, Errata and Interpretation for CC:2022 (release 1) and CEM:2022 (release 1), Version 1.1, 2024-07-22

[18] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, November 2022,
CC:2022 Revision 1, CCMB-2022-11-004

[19] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements November 2022, CC:2022 Revision 1, CCMB-2022-11-005

[20] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG), Bundesgesetzblatt I p. 2821; BSIG Section 9, Para.4, Clause 2, 2009-08-14

[TPM] Trusted Computing Group TPM Library be made of [5], [6], [7], [10] and [15]

[RFC3447] IETF RFC 3447, Public-Key Cryptography Standards PKCS#1: RSA Cryptography Specifications Version v2.1; June 14, 2002 RSA Cryptography Specifications Version v2.0; October 1, 1998

[IEEE1363] IEEE Std 1363™-2000, Standard Specifications for Public Key Cryptography IEEE Std 1363a™-2004, Standard Specifications for Public Key Cryptography

[N856] NIST SP800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)

[N890] NIST Special Publication SP 800-90A Revision 1; Recommendation for Random Number Generation Using Deterministic Random Bit Generators. June 2015

[N8133] NIST Special Publication SP 800-133 Rev.1; Recommendation for Cryptographic Key Generation; July 2019

[159461] ISO/IEC 15946-1, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General

[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

[10118] ISO/IEC 10118-3: 2004, Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions

[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)

[9797] ISO/IEC 9797-2, Information technology -- Security techniques – Message authentication codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function

[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

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

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
I2C - Inter-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.

HMAC: A mechanism for message authorization according RFC 2104 using the cryptographic hash function SHA-1/SHA-256/SHA-384.

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.

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 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.

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.

SAM: Service Algorithm Minimal

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.

SHA-1: A hashing algorithm producing a 160-bit result from an arbitrary source as specified in FIPS 180-4.

SHA-256: A hashing algorithm producing a 256-bit result from an arbitrary source as specified in FIPS 180-4.

SHA-384: A hashing algorithm producing a 384-bit result from an arbitrary source as specified in FIPS 180-4.

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.

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

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).

TCG-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 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.