Trusted Platform Module 2.0 SLB 9672 FW 17.10, 17.12, 17.13 and SLB 9673 FW 27.10, 27.13

FIPS 140 2 Level 2 Non-Proprietary Security Policy

Version: Release 1.3

Date: 2023-06-28

Table of Contents

List of Figures

List of Tables

1 Acronyms and Definitions

Table 1 Acronyms and Definitions

Acronym	Definition
CSS ESS	The Infineon group: Connected Secure Systems, Embedded Security Solutions
CPU	Central Processing Unit
CRNGT	FIPS 140-2 AS09.42 Continuous Random Number Generator Test
CSP	Critical Security Parameters
EEPROM	Electrically Erasable Programmable Read-Only Memory
GPIO	General Purpose Input Output
IC	Integrated Circuit
I2C	Inter-Integrated Circuit
KAT	Known Answer Test
KAS	Key Agreement Scheme
KBKDF	Key Based Key Derivation Function
MPU	Memory Protection Unit
NVM	Non-Volatile Memory (e.g., EEPROM, Flash)
PCT	Pairwise Consistency Test
PSP	Public Security Parameters
RAM	Random-Access Memory
ROM	Read-Only Memory
SPI	Serial Peripheral Interface; Motorola / de-facto standard for a synchronous serial communication interface. An alternative to the LPC for the TPM.
SSP	CSP or PSP
TCG	Trusted Computing Group (http://www.trustedcomputinggroup.org)
TPM	Trusted Platform Module
TRNG	True Random Number Generator (a form of hardware random number generator)

2 Overview

This document defines the Security Policy for the Infineon Trusted Platform Module 2.0 SLB 9672 and SLB 9673 cryptographic module, hereafter denoted *TPM*. The SLB 9672 uses the SPI interface, the SLB 9673 uses the I2C interface.

The TPM is a single chip module 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 TCG specifications for the TPM 2.0 family, [1][2][3][4][5][6]. See http://www.trustedcomputinggroup.org for further information on TCG and TPM.

The TPM is designated as a limited operational environment under the FIPS 140-2 definitions. The FIPS 140-2 security levels for the TPM are as follows:

Table 2 Security Level of Security Requirements

Security Requirement	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	2

2.1 Version, Configurations and Modes of Operation

Table 3 Configuration Part and Version Numbers

HW Part	Variant	Package	Firmware Version
SLB 9672	AU20	PG-UQFN-32-3	17.10.16488
SLB 9672	AU20	PG-UQFN-32-3	17.12.16858
SLB 9672	AU20	PG-UQFN-32-3	17.13.17733
SLB 9673	AU20	PG-UQFN-32-3	27.10.16688
SLB 9673	AU20	PG-UQFN-32-3	27.13.17770

The TPM is intended for use in general purpose computing environments, as a device peripheral to the CPU, with application controlling the usage of the module. The TPM is operated in the FIPS 140-2 Approved mode when the application complies with the conditions listed in Section 9.1.

The module provides two modes of operations: TPM Full Operational Mode and Field Upgrade Mode.

Overview

In TPM Full Operational Mode, all services and authentication mechanisms are available. The TPM Full Operational Mode is entered as soon as One Time Initialization (first power-up) of the TPM is done.

In Field Upgrade Mode, the module mainly provides Field Upgrade services to load a new Firmware. The Field Upgrade Mode is entered after successful Administrator Authentication to authorize an update to a newer version of the installed Firmware. In addition recovery of the already authorized and installed Firmware is also provided.

If the requirements for secure operation from section 9.1 are met, the TPM Full Operational Mode and Field Upgrade Mode are Approved Modes of operation in the meaning of FIPS 140-2. For the detailed differences for the Modes of Operation in terms of Algorithms, Services and Self-Tests please refer to section 3, section 4.2 and section 4.2.2.

The security functions available in the non-approved mode are listed in Table 9.

The *Show Status* service (specifically TPM2_GetCapability with the capability=TPM_CAP_PROPERTIES and property=TPM_PT_FIRMWARE_VERSION_1 qualifier) may be used to verify the FIPS-compliant version of the TPM firmware is installed on the TPM.

2.2 Physical Characteristics and Cryptographic Boundary

The TPM cryptographic boundary is represented by the surfaces, edges and connection points of the IC package. The chip comes with the support of one temperature range:

- The AU20 is the enhanced temperature type from -40°C to 105°C (Figure 1 and Figure 2)

The package is shown on a one (1) millimeter by one (1) millimeter grid to indicate size on the following figure. The physical ports and logical interfaces are detailed in Table 5.

Figure 1 Pictures of SLB9672AU20

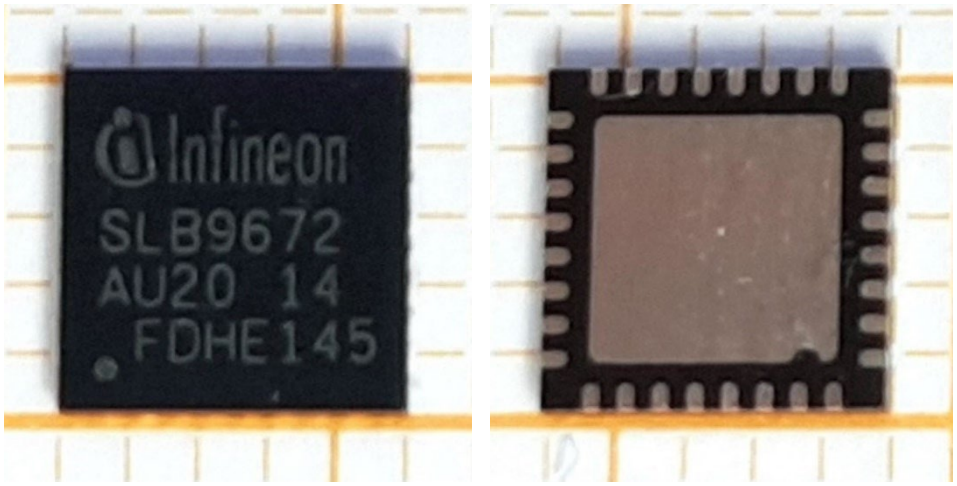

Figure 2 Pictures of SLB9673AU20

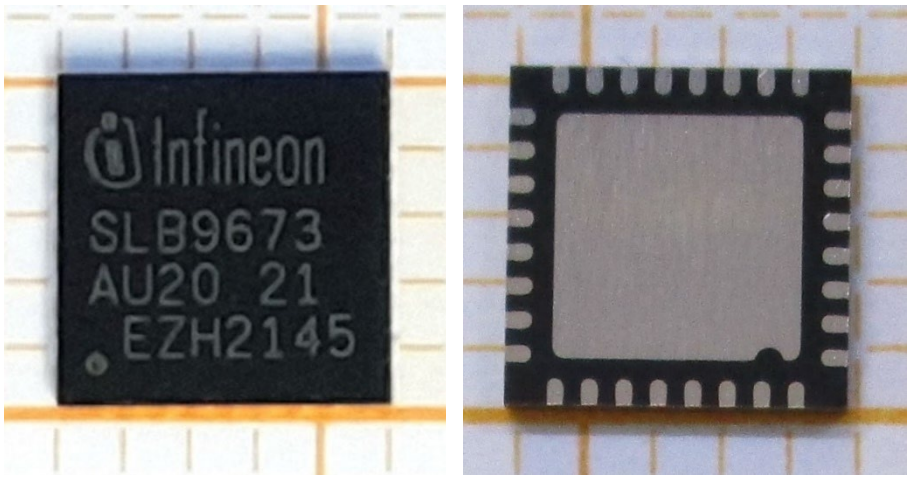

Table 4 Types printed on packages

Package	HW Part	Type printed on package
PG-UQFN-32-3	SLB 9672	SLB9672AU20 (Figure 1)
PG-UQFN-32-3	SLB 9673	SLB9673AU20 (Figure 2)

Table 5 Ports and Interfaces

Port	Ports common to all configurations	Logical Interface Type
GND	Ground	Power
GPIO	General Purpose I/O	Control Input, Status Output
NC	No connects	Unused
VDD	1.8V or 3.3V	Power
RST#	Reset	Control Input
SPI Interface Specific (SLB 9672) Ports and mapping to Logical Interfaces		
MISO	Master Input, Slave Output	Control Input, Data Output, Status Output
MOSI	Master Output, Slave Input	Control Input, Data Input, Status Output
SCLK	Serial Clock	Control Input
CS#	Chip Select	Control Input
I2C Interface Specific (SLB 9673) Ports and mapping to Logical Interfaces		
SDA	Serial Data	Control Input, Data Input, Status Output
SCL	Serial Clock	Control Input

2.3 Operational Environment

The module has a limited operational environment under the FIPS 140-2 definitions. The module includes a firmware load function to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of scope of this validation and requires a separate FIPS 140-2 validation.

2.4 TPM Composition

Figure 3 and Figure 4 depict the TPM hardware block diagram, shown from logical perspective. The red outline indicates the cryptographic boundary. Figure 3 depicts SLB 9672 (SPI) and Figure 4 depicts SLB 9673 (I2C).

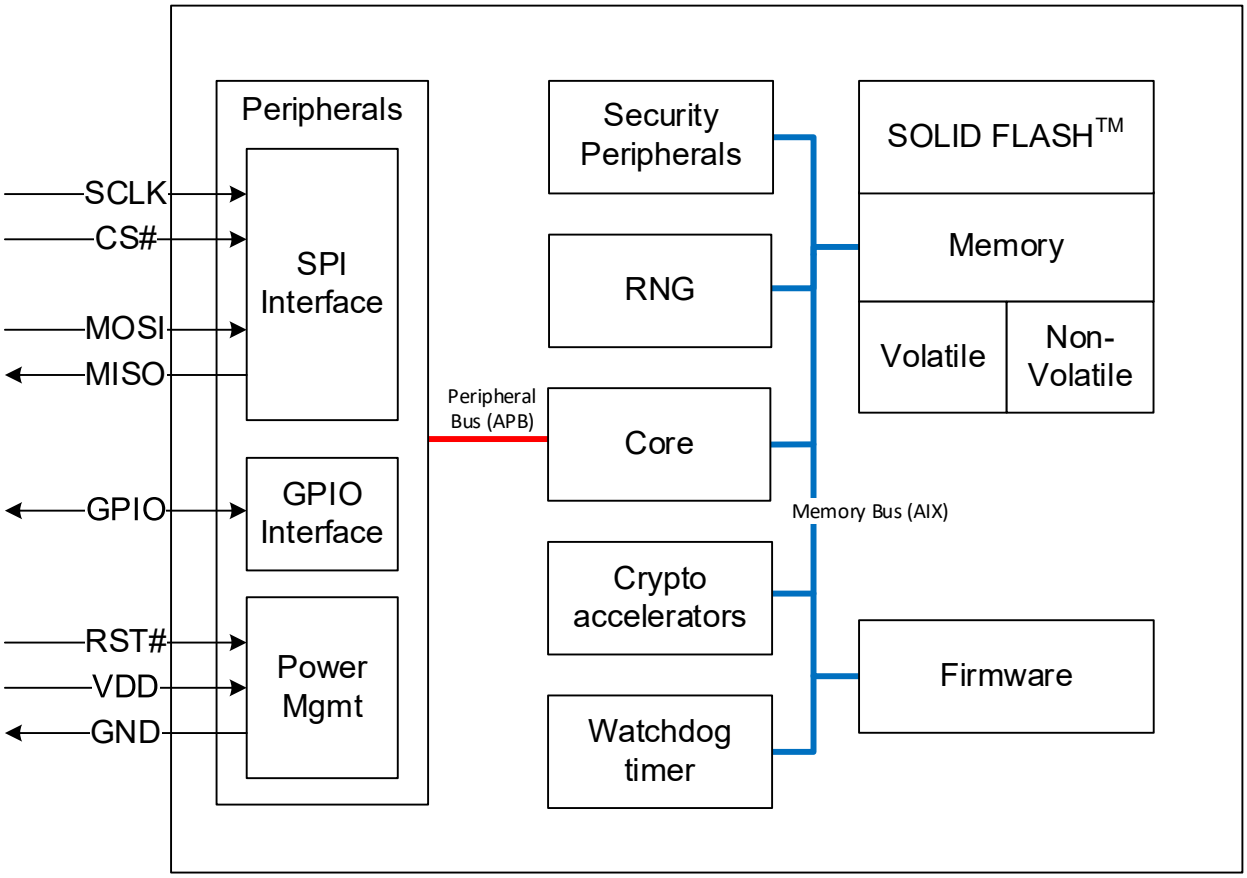

Figure 3 TPM Composition SLB 9672

Overview

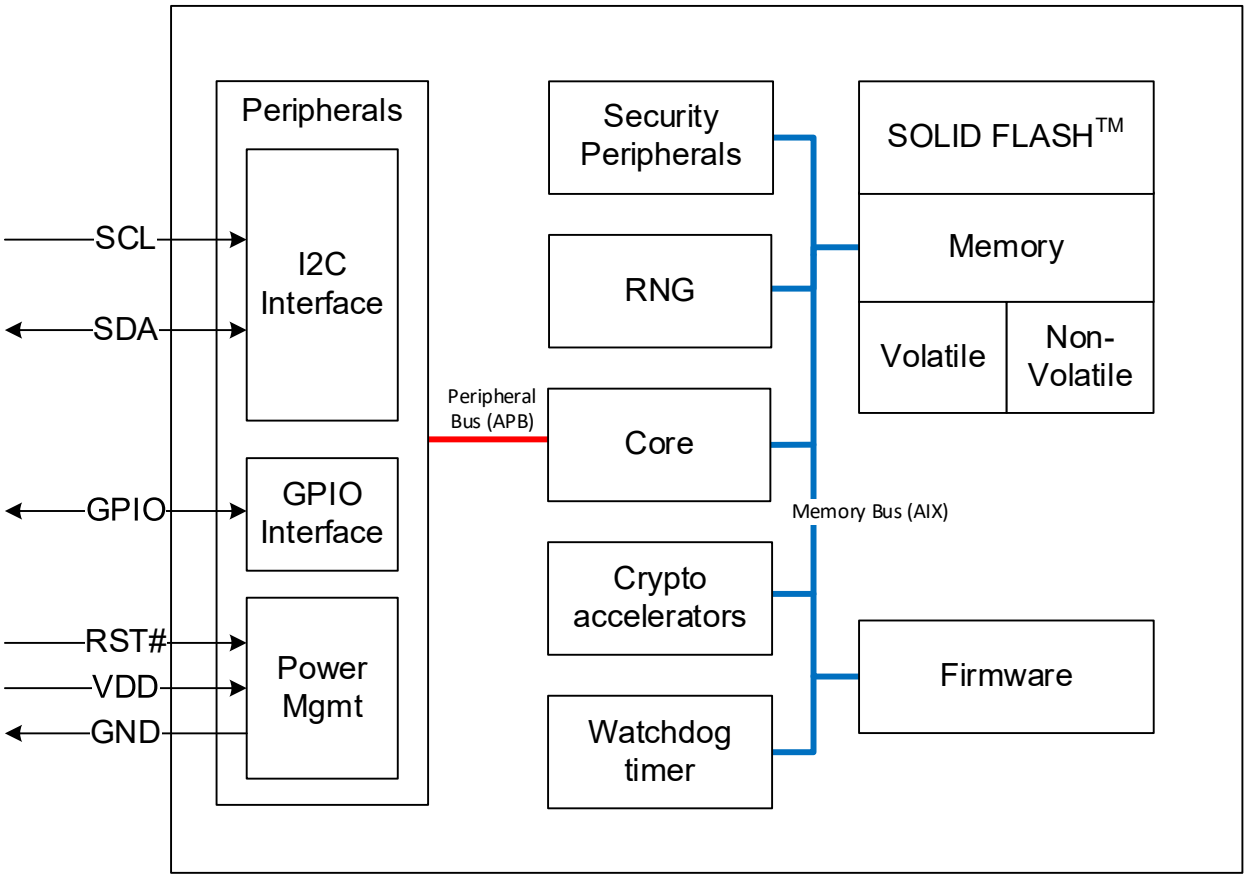

Figure 4 TPM Composition SLB 9673

The major blocks of the TPM are:

- Peripherals:
  - Power Mgmt: power management module to support low power modes
  - GPIO: Bidirectional signal which can be set or read by the caller; not otherwise used by the TPM
  - SPI / I2C: communication interface to receive TPM commands
- Security peripherals
- The RNG includes a physical, SP800-90B entropy source
- The core includes a 32-bit CPU with MPU and Cache
- The hardware crypto accelerators provide symmetric and asymmetric cryptographic functionalities
- The firmware provides the TCG functionality specified in [1][2][3][4][5] and the services described in Section 4.2. The firmware is stored in non-volatile memory.

3 Cryptographic Functionality

3.1 Cryptographic Functions

The TPM implements the approved and allowed cryptographic functions listed in Table 6, Table 7, Table 8 and Table 9 in the approved modes of operation.

Table 6 Approved Cryptographic Functions – Field Upgrade Mode

ACVP Cert	Algorithm	Standard(s)	Mode/Method	Key Lengths/ Curves/Moduli	Use
A1718 A2072 A2588 A3736 A3738	ECDSA	FIPS 186-4 [9]	SHA-512	P-521	Signature Verification
A1718 A2072 A2588 A3736 A3738	SHA	FIPS 180-4 [7]	SHA-512 SHA-384	n.a.	Message Digest

Table 7 Approved Cryptographic Functions – TPM Full Operational Mode

ACVP Cert	Algorithm	Standard(s)	Mode/Method	Key Lengths/ Curves/Moduli	Use
A1718 A2072 A2588 A3736 A3738	AES	FIPS 197 [10] SP800-38A [12]	CFB128	128 bits 192 bits 256 bits	Data Encryption/Decryption
A1718 A2072 A2588 A3736 A3738	AES	FIPS 197 [10] SP800-38A [12]	ECB used by CTR_DRBG: AES-256	256 bits	Deterministic Random Bit Generation
Vendor affirmed	CKG	SP800-133 [21][17]	“Direct Generation” of Symmetric Keys (section 6.1) and Key Pairs for Digital Signature Schemes (section 5.1) are using the output of the Approved DRBG (section 4)		Key Generation
A1718 A2072 A2588 A3736 A3738	CVL RSADP	SP800-56Br2 [15]	--	2048 bits	Key Transport Primitive

Cryptographic Functionality

ACVP Cert	Algorithm	Standard(s)	Mode/Method	Key Lengths/ Curves/Moduli	Use
A1718 A2072 A2588 A3736 A3738	CVL RSASP	FIPS 186-4 [9]	--	2048 bits	Tested, but not used
A1718 A2072 A2588 A3736 A3738	DRBG	SP800-90A [17]	CTR_DRBG: AES-256 (with derivation function)	256 bits	Deterministic Random Bit Generation
A1718 A2072 A2588 A3736 A3738	ECDSA	FIPS 186-4 [9]	--	P-256 P-384	Key Generation, Public Key Validation
			SHA-384 SHA-256	P-384	Signature Generation, Signature Verification
			SHA-256 SHA-384	P-256	Signature Generation, Signature Verification
			SHA-1	P-256, P-384	Signature Verification
N/A	ENT (P)	SP 800-90B [19]	Internal entropy source	Minimum entropy of 7.51729 bits per 8-bit bloc. Provide a minimum entropy of 256 bits to the DRBG.	Seeding/Reseeding of the DRBG
A1718 A2072 A2588 A3736 A3738	HMAC	FIPS 198-1 [11]	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	160 bits, 256 bits, 384 bits	Message Authentication, output data are not truncated
A1718 A2072 A2588 A3736 A3738	KAS	SP800-56Ar3 [14] SP800-56Cr1 [16]	One-Pass DH, Initiator/Responder, No Key Confirmation, oneStepKdf using SHA-1, SHA-256, SHA-384	P-256 P-384	Key Generation, Partial Public Key Validation, Key Agreement Key Derivation (key establishment methodology provides 128 or 192 bits of encryption strength)
A1718 A2072 A2588	KAS-SSC	SP800-56Ar3 [14]	One-Pass DH, Initiator/Responder	P-256 P-384	Key Agreement Primitive

Cryptographic Functionality

ACVP Cert	Algorithm	Standard(s)	Mode/Method	Key Lengths/ Curves/Moduli	Use
A3736 A3738					
A1718 A2072 A2588 A3736 A3738	KBKDF	SP800-108 [19]	CTR mode HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	160 bits, 256 bits, 384 bits	Key Derivation
A1718 A2072 A2588 A3736 A3738	KTS	FIPS 197 [10] FIPS 198-1 [11] SP800-38F [13]	AES-128, AES-192, AES-256 CFB & HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	128 bits (AES), 192 bits (AES) 256 bits (AES) & 160 bits (SHA-1), 256 bits (SHA-256), 384 bits (SHA-384)	Key Wrapping/Unwrapping (key establishment methodology provides between 128 and 256 bits of encryption strength)
A1718 A2072 A2588 A3736 A3738	KTS-RSA	SP800-56Br2 [15]	KTS-OAEP-basic encapsulate & decapsulate	2048 bits 3072 bits 4096 bits	Key Transport (key establishment methodology provides between 112 and 150 bits of encryption strength)
A1718 A2072 A2588 A3736 A3738	RSA	FIPS 186-4 [9]	--	2048 bits 3072 bits 4096 bits	Key Generation
			SHA-256 & PKCS1-V1_5, PSS SHA-384 & PKCS1-V1_5, PSS	2048 bits 3072 bits 4096 bits	Signature Generation, Signature Verification
			SHA-1 & PKCS1-V1_5, PSS	2048 bits 3072 bits 4096 bits	Signature Verification
A1718 A2072 A2588 A3736 A3738	SHA	FIPS 180-4 [8]	SHA-1, SHA-256, SHA-384	160 bits, 256 bits, 384 bits	Message Digest

Table 8 Allowed Cryptographic Functions – Field Upgrade Mode

Algorithm	Use
XMSS (Extended Merkle Signature Scheme)	Signature Verification

Note: This Post Quantum signature algorithm is used in parallel to the approved ECDSA signature. No security is claimed for the XMSS signature algorithm.

Cryptographic Functionality

The following table shows the cryptographic functions of the TPM, which are neither approved nor allowed.

Table 9 Non-allowed Cryptographic Functions – TPM Full Operational Mode

Algorithm	Use
ECDAA	For Elliptic Curve Direct Anonymous Attestation used to generate anonymous signatures with the Barreto-Naehrig (BN) elliptic curve BN-256
RSA 1024-bit (non-compliant)	Key Generation, Signature Generation, Key Wrapping (non-compliant because less than 112 bits of encryption strength)
SHA-1 (non-compliant)	Signature Generation using SHA-1

3.2 Critical Security Parameters and Public Keys

All CSPs and PSPs used by the Module are listed in the following sections.

3.2.1 CSPs and Public Keys in TPM Full Operational Mode

Table 10 Cryptographic Keys and CSPs used in TPM Full Operational Mode

Name	Description and usage
DRBG-EI	TPM DRBG Entropy Input – produced by the NDRNG, used during DRBG instantiation and reseed.
DRBG-STATE	TPM DRBG State – Current values of AES 256 CTR_DRBG state (128 bit V and 256 bit K).
TPM-EPS	TPM Endorsement Primary Seed – Minimum of 512 bits random value; used as master seed value to derive primary keys and secrets in the Endorsement Hierarchy;
TPM-PS	TPM Platform, Storage Primary Seed – Minimum of 512 bits random value; used as master seed value to derive primary keys and secrets in the Platform respective Storage Hierarchy.
TPM-Proof	TPM Proof Value – 512 bits random value used as KW-KDK Key in an HMAC-SHA-384 KBKDF (to derive confidentiality keys KW-CK) and used as KW-IK for HMAC-SHA-384 Integrity Protection of CSP wrapping in the TPM Context Management Service. Also used as HMAC-SHA-384 Integrity Key to prove that data structures have only been generated by a specific TPM module.
AS-AD-K	Authorization Session Authentication Data Key – 160-bit or 256-bit or 384-bit secret authentication data known by the Object Owner or Hierarchy Owner. E.g. used to derive TPM AS-SK for Bound Authorization Sessions.
AS-SALT	Authorization Session Salt – 160-bit or 256-bit or 384-bit Salt value used to derive a TPM AS-SK for Salted Authorization Sessions. The AS-SALT serves as the Key Derivation Key within the SP800-108 KBKDF.
AS-SK	Authorization Session – Session Key – HMAC-SHA-1 160-bit or HMAC-SHA-256 256-bit or HMAC-SHA-384 384-bit session key used for message authentication in a bound and/or salted TPM Authorization Session.
ES-KDK	Encryption Session Key Derivation Key – 160-bit or 256-bit or 384-bit Key used to derive ES-EK.
ES-EK	Encryption Session Ephemeral Key – AES-128, AES-192 or AES-256 ephemeral key used in CFB mode for message parameter encrypt/decrypt within a secure messaging session.

Cryptographic Functionality

Name	Description and usage
KW-KDK	Key Wrap – Key Derivation Key – 160-bit or 256-bit or 384-bit secret used to derive KW-IK and KW-CK.
KW-IK	Key Wrap – Integrity Key – HMAC-SHA-1 160-bit or HMAC-SHA-256 or HMAC-SHA-384 Key used for integrity protection of encrypted data used in the TPM for Key Wrapping Mechanism.
KW-CK	Key Wrap – Confidentiality Key – AES-128 or AES-256 key used to protect CSP confidentiality via Key Wrapping used in the TPM.
SIGK	Signing Key – RSA 2048-bit or RSA 3072-bit or RSA 4096-bit or ECC P-256 or ECC P-384 private key used for TPM Protocols and User Signature Generation Services.
IFX-PE-KEK	Infineon Primary Endorsement Key Establishment Key – RSA 2048-bit or RSA 3072-bit or RSA 4096-bit (key transport) or ECC P-256 or ECC P-384 (key agreement) private key used in TPM Protocols and uniquely associated with each TPM device via an Infineon X509 Certificate; installed at the factory.
TPM-KEK	TPM Key Establishment Key – RSA 2048-bit or RSA 3072-bit or RSA 4096-bit (key transport) or ECC P-256 or ECC P-384 (key agreement) private key used in TPM Protocols.
U-KEK	User Key Establishment Key – RSA 2048-bit or RSA 3072-bit or RSA 4096-bit (key transport) or ECC P-256 or ECC P-384 (key agreement) private key used in a User Key Agreement Primitive Services.
U-MACK	User HMAC Key – 160-bit or 256-bit or 384-bit HMAC key used in User HMAC Services.
U-E-KAK	User Ephemeral Key Agreement Key – ECC P-256 or ECC P-384 private key used in a User Key Agreement Primitive Services.
U-KDK	User Key Derivation Key – 160-bit or 256-bit or 384-bit secret used to derive U-MACK.
U-EDK	User Encryption/Decryption Key - AES-128, AES-192 or AES-256 key used in CFB mode or CTR mode in AES Encrypt/Decrypt Service.

Table 11 Public Keys used in TPM Full Operational Mode

Name	Description and usage
SIGK-PUB	Public Signing Key – RSA 2048-bit or RSA 3072-bit or RSA 4096-bit or ECC P-256 or ECC P-384 public signature verification key used for TPM Enhanced Authorization Protocols and User Signature Verification Service.
TPM-KEK-PUB	TPM Public Key Establishment Key – RSA 2048-bit or RSA 3072-bit or RSA 4096-bit (key transport) or ECC P-256 or ECC P-384 (key agreement) used in TPM Protocols.
U-KEK-PUB	User Public Key Establishment Key – RSA 2048-bit or RSA 3072-bit or RSA 4096-bit (key transport) or ECC P-256 or ECC P-384 (key agreement) key used in User Key Agreement Primitive Services.
U-E-KAK-PUB	User Public Ephemeral Key Agreement Key – ECC P-256 or ECC P-384 ephemeral public key used in User Key Agreement Primitive Services.
IFX-PE-KEK-PUB	Infineon Public Primary Endorsement Key Establishment Key – RSA 2048-bit or RSA 3072-bit or RSA 4096-bit (key transport) or ECC P-256 or ECC P-384 (key agreement) public key used in TPM Protocols and uniquely associated with each TPM device via Infineon X509 Certificate; installed at the factory.

3.2.2 CSPs and Public Keys in Field Upgrade Mode

No cryptographic Keys nor CSPs are used in Field Upgrade Mode

Table 12 Public Keys and Information used in Field Upgrade Mode

Name	Description and usage
PUB-SIGK-SIA	Public Signature Verification Key for Source and Integrity Authentication – ECDSA NIST P-521 public key for field upgrade signature verification to verify source and integrity authentication of a Firmware Manifest; installed at factory

4 Roles, Authentication and Services

The TPM supports three roles, a CO role, a User role and a DUP role, as described in Table 13.

The TPM:

- Does not support a maintenance role or concurrent operators.
- Requires re-authentication following a power-cycle.

Table 13 Roles Supported by the Module

Role ID	Role Description
CO	Cryptographic Officer, also known as the TPM Administrator or Admin Role. Controls certification of objects and changes Authentication Data of objects.
User	User, also known as the object owner. Uses the TPM to create cryptographic objects and to obtain cryptographic services for cryptographic objects.
DUP	Duplication Officer. Uses the TPM to duplicate TPM objects.

4.1 TPM Identification and Authentication Methods

The TPM supports the following Authentication Methods:

4.1.1 Password Verification

Operators in the CO or User roles are authenticated by a demonstration of knowledge of a Password as authentication data. Typically, this will be used (but is not restricted) in a limited pre-boot environment.

4.1.2 HMAC Challenge-Response Authentication

This Challenge-Response Authentication is described as HMAC Authorization Session within TCG Specifications. Operators in the CO or User roles are authenticated by a challenge and response demonstration of knowledge of a shared secret. The shared secrets are HMAC-SHA-1, HMAC-SHA-256 or HMAC-SHA-384 cryptographic keys. The TPM HMAC authorization session mechanism includes nonce values to prevent replay attacks.

4.1.3 Enhanced Authorization for Authentication

Enhanced Authorization is also referred to as Policy Authorization Session within TCG Specifications. Enhanced Authorization allows object creators to define specific actions and test which have to be performed before the service using CSP key can be executed. The specific policy is encapsulated in a policy digest being SHA-1/SHA-256/SHA-384 Digest Value and associated with the CSP key.

Operators in the CO or User roles can be authenticated via policy digest, which requires as action the use of an authentication mechanism. Password Verification or HMAC Challenge-Response Authentication as described above, or Challenge-Response Authentication based on a Public Key Digital Signature Algorithm (2048-bit or 3072-bit or 4096-bit or 256-bit ECDSA or 384-bit ECDSA) can be used as authentication mechanism. The TPM policy authorization session mechanism includes nonce values to prevent replay attacks. For guidance on the use of Enhanced Authorization for authentication please refer to Section 9.1.

4.1.4 Role Based Authentication Method Summary

The following table shows the allowed authentication mechanisms and data options for each Role. Enhanced Authorization is always allowed for each Role. For CO and User roles the TPM object attributes control if Password and Challenge-response Mechanism is allowed in addition.

Table 14 Roles and Required Identification and Authentication

Role ID	Role Description	Authentication Data
Admin (CO)	Password verification	Password
	Challenge-response authentication using HMAC-SHA-1, HMAC-SHA-256 or HMAC-SHA-384	Cryptographic Key (HMAC 160-bit key, HMAC 256-bit key or HMAC 384-bit key)
	Enhanced Authorization requiring an authentication mechanism	Password or Cryptographic Key included as reference in the policy digest
User	Password verification	Password
	Challenge-response authentication using HMAC-SHA-1, HMAC-SHA-256 or HMAC-SHA-384	Cryptographic Key (HMAC 160-bit key, HMAC 256-bit key or HMAC 384-bit key)
	Enhanced Authorization requiring an authentication mechanism	Password or Cryptographic Key included as reference in the policy digest
DUP	Enhanced Authorization requiring an authentication mechanism	Password or Cryptographic Key included as reference in the policy digest

4.1.5 Strength of Mechanism

Table 15 Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
Password verification	When using the password verification mechanism, a password consisting of at least 12 alphanumeric characters shall be used, see Section 9.1 for details. Assuming as a worst case that the operator uses 12 decimal digits only, but still randomly chosen, the probability that a single random authentication attempt (by guessing the password value) will succeed is: $10^{-12} < 10^{-6}$ A very conservative estimate of the maximum authentication rate is 10^6/minute (60µs per attempt). Under this assumption the probability that random authentication attempts will succeed within one-minute interval is: $10^6 \times 10^{-12} = 10^{-6} < 10^{-5}$
Challenge-response authentication using HMAC	As a worst case it is assumed that for challenge-response authentication HMAC-SHA-1 is used, which has smaller key length and smaller tag length (160-bit each) than HMAC-SHA-256 and HMAC-SHA-384. Under this assumption the probability that a random authentication attempt (by guessing key value or tag value) will succeed is: $2^{-160} = 6.8 \times 10^{-49} < 10^{-6}$ With the same assumed maximum authentication rate of 10^6/minute as above, the probability that random authentication attempts will succeed within a one-minute interval is: $10^6 \times 6.8 \times 10^{-49} = 6.8 \times 10^{-43} < 10^{-5}$
Enhanced Authorization	For the strength of this mechanism when using password verification or HMAC challenge-response authentication as required authentication mechanism see the two rows above.

Roles, Authentication and Services

Authentication Mechanism	Strength of Mechanism
requiring an authentication mechanism	For challenge-response authentication using a Public Key Digital Signature Algorithm as required authentication mechanism it is assumed as worst case that RSA 2048-bit is used, which provides 112 bits of security strength (ECDSA 256-bit provides 128-bit security strength, ECDSA 384-bit provides 192 bits of security strength). Therefore, the probability that a random authentication attempt will succeed using this authentication mechanism is: $2^{-112} = 1.9x10^{-34} < 10^{-6}$ With the same assumed maximum authentication rate of 10^6/minute as above, the probability that random authentication attempts will succeed within a one-minute interval is: $10^6 \times 1.9x10^{-34} = 1.9x10^{-28} < 10^{-5}$

4.2 Services

All services implemented by the module are listed in the tables below, with corresponding access to SSPs indicated according to the legend below.

All services are grouped according to the Mode, in which they are available. For a detailed description of available Modes please see section 2.1.

Table 16 Modes of access

Code	Description
E	Execute: The TPM executes using the SSP
G	Generate: The TPM generates the CSP
O	Output: A SSP is output from the TPM
I	Input: A SSP is input to the TPM
Z	Zeroize: The TPM zeroizes the CSP
--	Not accessed by the service

4.2.1 Services in TPM Full Operational Mode

See [1] [2][3][4] for a public description of all commands.

Roles, Authentication and Services

Table 17 Unauthenticated Services SSP Access

Un-authenticated Services	DRBG-EI	DRBG-STATE	TPM-EPS	TPM-PS	TPM-Proof	AS-AD-K	AS-SALT	AS-SK	ES-KDK	ES-EK	KW-KDK	KW-IK	KW-CK	SIGK	IFX-PE-KEK	TPM-KEK	U-KEK	U-MACK	U-E-KAK	U-KDK	SIGK-PUB	TPM-KEK-PUB	U-KEK-PUB	U-E-KAK-PUB	IFX-PE-KEK-PUB	U-EDK
TPM Full Operational Mode																										
TPM DRBG Services [1]																										
DRBG Generated Random Number	GZ	GEZ	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
DRG Reseed	GZ	GEZ	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
TPM Credential Protection																										
External Entity Authentication [2]	--	EI	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	E	--
User Cryptographic Support Function																										
RSA Key Transport Scheme [2]	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--
ECC CDH Primitive [2]	--	EI	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--
Verify Digital Signature [RSA, ECC]	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--
Create HASH	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
TPM Protected Storage [Public Keys Only]																										
Write & Read Public Keys [4]	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	OI	OI	OI	--	O	--
TPM Enhanced Authorization																										
Create + Verify HMAC Signature [3]	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Verify Digital Signature	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--
TPM Startup																										
DRGB Instantiate	GZ	GEZ	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Zeroize CSP	--	--	--	--	--	Z	--	--	--	--	--	--	--	Z	Z	Z	Z	Z	--	Z	Z	Z	Z	--	--	Z
TPM SelfTest & Show Status Service																										
SelfTest	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Show Status	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Note: Unauthenticated Services Notes:

1. Generation of Random Numbers based on SP800-90A, allowed per IG 3.1

Roles, Authentication and Services

2. *This service uses the Static Public Key of the relevant Key Establishment Method in the Module and does not disclose, modify, or create any CSP, allowed per IG 3.1.*
3. *This service is used for local TPM Data Structure Verification and Generation Services for the purpose of re-signing of data and does not disclose, modify or create any CSP, allowed per IG 3.1.*
4. *This service is only used for Public Key Entry and does not modify or substitute any CSP.*

Utility Support services are unauthenticated services, which are always associated with larger set of operations or services. These larger sets of operations or services comply with FIPS CSP Authentication Requirements.

Table 18 Utility Support Services SSP Access

Utility Support Services	DRBG-EI	DRBG-STATE	TPM-EPS	TPM-PS	TPM-Proof	AS-AD-K	AS-SALT	AS-SK	ES-KDK	ES-EK	KW-KDK	KW-IK	KW-CK	SIGK	IFX-PE-KEK	TPM-KEK	U-KEK	U-MACK	U-E-KAK	U-KDK	SIGK-PUB	TPM-KEK-PUB	U-KEK-PUB	U-E-KAK-PUB	IFX-PE-KEK-PUB	U-EDK
	TPM Full Operational Mode																									
TPM Context Management [1)]																										
Derive Keys based on KBKDF	--	--	--	--	--	--	--	--	--	--	E	--	G	--	--	--	--	--	--	--	--	--	--	--	--	--
Wrap CSPs [AES and HMAC Protection]	--	--	--	--	--	--	--	--	--	--	--	E	EZ	--	--	--	--	--	--	--	--	--	--	--	--	--
Backup CSP	--	--	--	--	--	O	--	O	--	O	--	--	--	O	O	O	O	O	--	O	--	--	--	--	--	O
Restore CSP	--	--	--	--	--	I	--	I	--	I	--	--	--	I	I	I	I	I	--	I	--	--	--	--	--	I
Zeroize CSP	--	--	--	--	--	Z	--	Z	--	Z	--	--	--	Z	Z	Z	Z	Z	--	Z	--	--	--	--	--	Z
TPM Session Service Initialization [2)]																										
RSA Key Transport Scheme	--	--	--	--	--	--	I	--	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	--	--	--
ECC Key Agreement Scheme	--	--	--	--	--	--	G	--	--	--	--	--	--	--	E	E	E	--	--	--	--	--	--	IEZ	--	--
Derive Keys based on KBKDF	--	--	--	--	--	E	EZ	GI	GEZ	GI	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Note: Utility Support Service Notes:

1. *CSP can only be backed up if their associated set of operations (e.g., creation or loading of the CSP) complies with FIPS CSP Authentication Requirements. Restored CSPs can only be used by the associated operations (e.g., Signature Creation), which comply with FIPS CSP Authentication Requirements. Backup and Restore Services are protected via FIPS Approved Key Wrapping KTS AES & HMAC.*
2. *CSPs are only generated if the CSPs involved in the generation have been loaded via Authentication Service.*

Roles, Authentication and Services

Table 19 User Authenticated Services SSP Access

User Authenticated Services	DRBG-EI	DRBG-STATE	TPM-EPS	TPM-PS	TPM-Proof	AS-AD-K	AS-SALT	AS-SK	ES-KDK	ES-EK	KW-KDK	KW-IK	KW-CK	SIGK	IFX-PE-KEK	TPM-KEK	U-KEK	U-MACK	U-E-KAK	U-KDK	SIGK-PUB	TPM-KEK-PUB	U-KEK-PUB	U-E-KAK-PUB	IFX-PE-KEK-PUB	U-EDK
	TPM Full Operational Mode																									
TPM Protected Storage																										
Derive Primary Asym Key Pair (RSA, ECC)	--	--	E	E	--	--	--	--	--	--	--	--	--	G	--	G	G	--	--	--	--	--	--	--	--	--
Derive Primary Sym Keys (HMAC, KDK, AES)	--	--	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--	G	--	G	--	--	--	--	--	G
Write Primary Sym Key (HMAC, KDK, AES)	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	I	--	I	--	--	--	--	--	I
Derive Primary KDK for Asym Storage & Sym Key	--	--	E	E	E	--	--	--	--	--	G	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Generate Asym Key (RSA, ECC)	--	EI	--	--	--	--	--	--	--	--	--	--	--	G	--	G	G	--	--	--	--	--	--	--	--	--
Generate Sym Key (HMAC, KDK, AES)	--	EI	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	G	--	G	--	--	--	--	--	G
Write Sym Key (HMAC, KDK, AES)	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	I	--	I	--	--	--	--	--	I
Derive Sym Key (HMAC, KDK, AES)	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	G	--	EG	--	--	--	--	--	G
Generate Sym KDK for Asym Storage & Sym Key	--	EI	--	--	--	--	--	--	--	--	G	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Derive Keys based on KBKDF	--	--	--	--	--	--	--	--	--	--	E	G	G	--	--	--	--	--	--	--	--	--	--	--	--	--
Wrap CSPs [AES and HMAC Protection]	--	--	--	--	--	--	--	--	--	--	--	EZ	EZ	--	--	--	--	--	--	--	--	--	--	--	--	--
Create HMAC Signature	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Write CSP	--	--	--	--	--	I	--	--	--	--	I	--	--	I	--	I	I	I	--	I	I	I	I	--	--	I
Read CSP	--	--	--	--	--	O	--	--	--	--	O	--	--	O	--	O	O	O	--	O	O	O	O	--	O	O
TPM Hierarchy Management																										
Generate CSP	--	EI	GI	GI	GI	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Zeroize CSP[1)]	--	--	Z	Z	Z	Z	--	--	--	--	--	--	--	Z	Z	Z	Z	Z	--	Z	--	--	--	--	--	Z
Write CSP [Authentication Data]	--	--	--	--	--	I	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
TPM Import Services																										
RSA Key Transport Scheme	--	--	--	--	--	--	--	--	--	--	I	--	--	--	E	E	--	--	--	--	--	--	--	--	--	--
ECC Key Agreement Scheme	--	--	--	--	--	--	--	--	--	--	G	--	--	--	E	E	--	--	--	--	--	--	--	IEZ	--	--
Derive Keys based on KBKDF	--	--	--	--	--	--	--	--	--	--	EZ	G	G	--	--	--	--	--	--	--	--	--	--	--	--	--
Re-Wrap CSPs [AES and HMAC Protection]	--	--	--	--	--	--	--	--	--	--	--	EZ	EZ	--	--	--	--	--	--	--	--	--	--	--	--	--
Read CSP	--	--	--	--	--	O	--	--	--	--	O	--	--	O	--	O	O	O	--	O	O	O	O	--	O	O
TPM Attestation																										
Create Digital Signature [RSA, ECC]	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--
Verify HMAC Signature	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
User Cryptographic Support Function																										
RSA Key Transport Scheme	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--
ECC CDH Primitive	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--

Roles, Authentication and Services

User Authenticated Services	DRBG-EI	DRBG-STATE	TPM-EPS	TPM-PS	TPM-Proof	AS-AD-K	AS-SALT	AS-SK	ES-KDK	ES-EK	KW-KDK	KW-IK	KW-CK	SIGK	IFX-PE-KEK	TPM-KEK	U-KEK	U-MACK	U-E-KAK	U-KDK	SIGK-PUB	TPM-KEK-PUB	U-KEK-PUB	U-E-KAK-PUB	IFX-PE-KEK-PUB	U-EDK
Create Digital Signature [RSA, ECC]	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--
Create HMAC	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--
Create HASH	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
AES Encrypt/Decrypt[2)]	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E
TPM Enhanced Authorization & Validation																										
Create & Verify HMAC Signature	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
TPM Context Management																										
Write CSP	--	--	--	--	--	I	--	--	--	--	I	--	--	I	I	I	I	I	--	I	I	I	I	--	I	I
Zeroize CSP	--	--	--	--	--	Z	--	--	--	--	Z	--	--	Z	Z	Z	Z	Z	--	Z	Z	Z	Z	--	Z	Z

Note: User Authenticated Services Notes

1. *This service can be activated, deactivated or permanently activated or deactivated for TPM-EPS and IFX-PE-KEK by configuration service (see Table 20). For permanent deactivation see [9.1].*
2. *This service can be activated, deactivated or permanently activated or deactivated by configuration service (see Table 20).*

Table 20 ADMIN (CO) Authenticated Services SSP Access

ADMIN (CO) Authenticated Services	DRBG-EI	DRBG-STATE	TPM-EPS	TPM-PS	TPM-Proof	AS-AD-K	AS-SALT	AS-SK	ES-KDK	ES-EK	KW-KDK	KW-IK	KW-CK	SIGK	IFX-PE-KEK	TPM-KEK	U-KEK	U-MACK	U-E-KAK	U-KDK	SIGK-PUB	TPM-KEK-PUB	U-KEK-PUB	U-E-KAK-PUB	IFX-PE-KEK-PUB
	TPM Full Operational Mode																								
TPM Credential Protection																									
External Entity Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E	--	--	--	--	--	--	--	--	--
TPM Key Attestation																									
Create Digital Signature [RSA, ECC]	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	--
TPM Protected Storage Management																									
Write CSP [Authentication Data]	--	--	--	--	--	I	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
TPM Field Upgrade Service																									
Activate Field Upgrade Mode & Install Manifest	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
TPM Hierarchy Management																									
Zeroize CSP	--	--	--	--	--	--	--	--	--	--	--	--	--	--	Z	--	--	--	--	--	--	--	--	--	--
TPM Misc Management																									
Configuration[1)]	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Roles, Authentication and Services

Note: ADMIN (CO) Authenticated Services Notes

1. *This service can activate, deactivate or permanently activate or deactivate AES Encrypt/Decrypt or Zeroization service for TPM-EPS and IFX-PE-KEK (see Table 19). For permanent deactivation see [9.1].*

Table 21 DUP Authenticated Services SSP Access

DUP Authenticated Services	DRBG-EI	DRBG-STATE	TPM-EPS	TPM-PS	TPM-Proof	AS-AD-K	AS-SALT	AS-SK	ES-KDK	ES-EK	KW-KDK	KW-IK	KW-CK	SIGK	IFX-PE-KEK	TPM-KEK	U-KEK	U-MACK	U-E-KAK	U-KDK	SIGK-PUB	TPM-KEK-PUB	U-KEK-PUB	U-E-KAK-PUB	IFX-PE-KEK-PUB	U-EDK
	TPM Full Operational Mode																									
TPM Duplication																										
RSA Key Transport Scheme	--	EI	--	--	--	--	--	--	--	--	G	--	--	--	--	--	--	--	--	--	--	E	--	--	E	--
ECC Key Agreement Scheme	--	EI	--	--	--	--	--	--	--	--	G	--	--	--	--	--	--	--	--	GEZ	--	E	--	GOZ	E	--
Derive Keys based on KBKDF	--	--	--	--	--	--	--	--	--	--	EZ	G	G	--	--	--	--	--	--	--	--	--	--	--	--	--
Wrap CSPs [AES and HMAC Protection]	--	--	--	--	--	--	--	--	--	--	--	EZ	EZ	--	--	--	--	--	--	--	--	--	--	--	--	--
Read CSPs	--	--	--	--	--	O	--	--	--	--	O	--	--	O	--	O	O	O	--	O	O	O	O	--	--	O

The following unauthenticated services are part of the authentication process and do not create, modify, disclose or substitute cryptographic keys or CSPs in accordance with IG 3.1.

Table 22 TPM Challenge + Response Authentication and Encryption Services

TPM Challenge + Response Authentication and Encryption	DRBG-EI	DRBG-STATE	TPM-EPS	TPM-PS	TPM-Proof	AS-AD-K	AS-SALT	AS-SK	ES-KDK	ES-EK	KW-KDK	KW-IK	KW-CK	SIGK	IFX-PE-KEK	TPM-KEK	U-KEK	U-MACK	U-E-KAK	U-KDK	SIGK-PUB	TPM-KEK-PUB	U-KEK-PUB	U-E-KAK-PUB	IFX-PE-KEK-PUB	U-EDK
	TPM Full Operational Mode																									
Message Authentication	--	--	--	--	--	E	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Message Encryption using AES Encrypt Decrypt	--	--	--	--	--	--	--	--	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Zeroize CSP	--	--	--	--	--	--	--	Z	--	Z	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

4.2.2 Services in Field Upgrade Mode

Table 23 Field Upgrade Mode Unauthenticated Services CSP Access

Unauthenticated Field Upgrade Services	PUB-SIGK-SIA
Field Upgrade Process Manifest Service [1)]	
Verify Digital Signature [ECDSA-P-521]	E
Field Upgrade Process Payload Finalize Service	
Create Hash, Post-Installation Digest [SHA-512]	--
Verify Hash, Post-Installation Digest [SHA-512]	--
SelfTest & Show Status Service	
SelfTest	--
Show Status	--

Note: Unauthenticated Services Notes

1. *This service is indirectly authenticated since the Manifest has been installed via ADMIN Authenticated TPM Field Upgrade Service from Table 23.*

5 Self-tests

On power-on or reset, the TPM must ensure that all self-tests as described in Table 24 and Table 25 below have been performed. All KATs/PCT must be completed successfully prior to any other use of cryptography by the TPM. If one of the KATs/PCTs fails, the system is halted (in the Failure Mode state). In this mode only TPM2_GetTestResult and TPM2_GetCapabiliy is accepted by the TPM; no CSP access is possible.

In Field Upgrade Mode, self-tests may be invoked at any time using TPM2_SelfTest with self-test results returned in TPM2_GetTestResult.

In Full Operational Mode, self-tests may be invoked at any time using TPM2_FullFipsSelfTestVendor with self-test results returned.

According to [22], IG 9.11, self-tests for Full Operational Mode are not done during each power on or reset but only once after the following events:

- First startup after installation of the TPM
- First startup after a Field Upgrade of the TPM firmware

Table 24 Operational mode Self-Tests

Self-Test	Description
Critical Function Self-Tests	
Hardware Integrity Test	The TPM perform a hardware integrity test at power-up and at fixed periods. In either case, if the hardware integrity test fails, TPM hardware immediately enters security reset state (the TPM is mute).
Self-Tests performed on each power up	
Firmware Integrity Test	The startup code uses an EDC with at least 16 bits. The startup code measures the TPM application with a SHA-256. Error Detection Code with at least 16 bits performed over Code located in NVM.
SHA-1, SHA-384 KAT (Certs. #A1718, #A2072, #A2588, #A3736 and #A3738)	Performs a fixed input KAT for SHA-1 and SHA-384 Note: There is no explicit test for SHA-256. It is implicitly tested by the Firmware integrity test which uses SHA-256 as a checksum.
AES-128 KAT (Certs. #A1718, #A2072, #A2588, #A3736 and #A3738)	Performs encrypt KAT using AES-128 key in CFB mode.
Self-Tests performed only once according to IG 9.11	
DRBG KAT (Certs. #A1718, #A2072, #A2588, #A3736 and #A3738)	Performs a fixed input KAT, inclusive of the SP800-90A [17] health monitoring tests.
RSA KATs (Certs. #A1718, #A2072, #A2588, #A3736 and #A3738)	Performs RSA Digital Signature (RSASSA-PKCS1-V1_5 using SHA-256) Generation and Verification KATs using RSA 2048-bit key and RSA 3072-bit key.
ECDSA PCT (Certs. #A1718, #A2072, #A2588, #A3736 and #A3738)	Performs an ECDSA pairwise consistency test (PCT) using NIST recommended curve P-256 with SHA-256
ECC KAS KAT (Certs. #A1718, #A2072, #A2588, #A3736 and #A3738)	Performs ECC CDH primitive Z computation using NIST- recommended curve P-256.

Self-tests

KBKDF KAT (Certs. #A1718, #A2072, #A2588, #A3736 and #A3738)	Performs fixed input KAT of the KDF [19] using HMAC-SHA-256 Note: There is no explicit test for HMAC SHA-256. It is implicitly tested by the KBKDF KAT which uses HMAC SHA-256 as allowed per IG 9.4.
Concatenation KDF KAT (Certs. #A1718, #A2072, #A2588, #A3736 and #A3738)	Performs fixed input KAT of Concatenation KDF (KDFe) using SHA-256 (SP 800-56Cr1 one-pass KDF)
Conditional Self-Tests	
NDRNG CRNGT	The TPM performs testing according to DTR AS09.42 to assure the NDRNG output is different than the previous value. Failure of this NDRNG CRNGT is treated as an attack; the TPM enters an error state. This conditional self-test is also performed in operational mode when DRBG is reseeded (and therefore new entropy from the NDRNG is collected).
RSA Key Gen PCT	On generation of RSA key pair, the TPM performs a pairwise consistency test. For key transport keys, the PCT sequence is encrypt/decrypt; for signature keys, the PCT sequence sign/verify is applied.
ECC Key Gen PCT	On generation of an ECDSA key pair, the TPM performs an ECDSA pairwise consistency test. Before usage of the key, a full public key validation will be done.
Key load test	When RSA or ECC key pairs or public keys are loaded into TPM, TPM performs – depending on the key type – pair-wise consistency or key regeneration tests and or assurance tests as required by SP 800-56Ar3 and SP 800-56Br2. Key material is loaded only if corresponding key load tests succeeds.

Table 25 Field Upgrade mode Self-Tests

Self-Test	Description
Critical Function Self-Tests	
Hardware Integrity Test	The TPM perform a hardware integrity test at power-up and at fixed periods. In either case, if the hardware integrity test fails, TPM hardware immediately enters security reset state (the TPM is mute).
Self-Tests performed on each power up	
Firmware Integrity Test	Error Detection Code with at least 16 bits performed over Code located in NVM.
SHA-384, SHA-512 KAT (Certs. #A1718, #A2072, #A2588, #A3736 and #A3738)	Performs a fixed input KAT for SHA-384 and SHA-512.
Self-Tests performed only once according to IG 9.11	
ECDSA KAT (Certs. #A1718, #A2072, #A2588, #A3736 and #A3738)	Performs an ECDSA Verify Test (KAT) using NIST recommended curve P-521.
Conditional Self-Tests	
Firmware Load Test 1	The TPM performs ECDSA NIST P-521 asymmetric signature verification with SHA-512 over firmware manifest to be loaded. New Firmware is only processed if verification succeeds.
Firmware Load Test 2	SHA-512 message digest performed as Approved Integrity Technique over the Loaded Firmware. The new Firmware is only executed after restart if Approved Integrity Verification succeeds.

6 Physical Security Policy

The TPM is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The TPM employs standard passivation techniques. The TPM is intended for deployment on standard PCBs or similar assemblies. TPM packaging provides opacity and tamper evidence protections and will cause serious damage to the module, sufficient to meet FIPS 140-2 Physical Security Level 3.

TPM comes with a hard and opaque coating (see images in Section 2.2). Any attempt of physical tampering by mechanical means will leave evidence in form of scratches, broken edges of the coating or similar.

The TPM shall be visually inspected for evidence of tampering at least once before integration into a host device. After integration, it is possible to check for tamper evidence by opening the host device and inspecting the TPM.

7 Electromagnetic Interference and Compatibility (EMI/EMC)

The Module conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

8 Mitigation of Other Attacks Policy

The TPM implements the mechanism listed in Table 26 to mitigate attacks beyond the requirements of FIPS 140-2 Security Level 2. There are no specific limitations for any of these attack mitigations.

Table 26 Mitigation of Other Attacks

Other Attack	Mitigation Mechanism
Fault induction	External clock conditions, temperature and electromagnetic radiation (e.g., light) are monitored using sensors. Operation outside specific parameters causes the chip to enter the *Security reset* state until condition is cleared.
Software fault induction	The address mapping together with the memory protection unit (MPU) gives the possibility to define different access rights for memory areas. In case of an access violation (e.g., embedded software trying to read memory of IC-dedicated software) hardware enters the *Security reset* state.
Design analysis and surveillance attacks (in operational or power off condition)	The TPM integrated circuit level layout uses masking, critical circuit shielding and synthesized logic to deter attacker knowledge of the part design. Outer layer lines are protected with a proprietary masking technique, with active shielding in internal layers to protect the masking mechanism. The use of synthesized logic deters attackers from pattern recognition of logic clusters. As well, a dedicated CPU with non-public bus protocol is used which makes analysis complicated.
Physical probing of memory and data buses	Proprietary memory and bus masking to deter probing memories or busses.

9 Security Rules and Guidance

The TPM implementation also enforces the following security rules:

- The module provides three distinct operator roles: Duplication Officer, User and Cryptographic Officer.
- The module provides role-based authentication.
- The module clears previous authentications on power cycle.
- Power-up self-tests do not require any operator action.
- No additional interface or service is implemented by the module which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, Zeroization, and error states.
- There are no restrictions on which keys or CSPs are zeroized by the Zeroization service.
- The module does not support manual key entry.
- The module does not output plaintext CSPs or intermediate key values.
- Status information does not contain CSPs or sensitive data that is misused could lead to compromise of the module.

9.1 Requirements for Secure Operation

The application must assure the following conditions are met for operation of the TPM in the FIPS 140-2 Approved mode:

Requirements for Approved and Allowed Function Usage:

- Only Approved and allowed cryptographic functions as listed in Table 6, Table 7 and Table 8 may be used.
- Non-approved cryptographic functions listed in Table 9 shall not be used.
- TPM2_ChangeEPS must not be permanently disabled.

Requirements for Key Management:

- When using U-KDK to derive other Keys only symmetric Keys (e.g. HMAC) shall be derived and asymmetric Keys (e.g. ECC Keys) shall not be derived
- When using U-KDK to derive symmetric Keys, Key Separation Requirements [19], Section 7.5 shall be met

Requirements for Key Entry and Output to and from the Module:

- When entering CSP keys into the module the operator shall ensure usage of FIPS Approved Key Wrapping via usage of Message Encryption using AES Encrypt Decrypt in combination with Message Authentication using HMAC Service listed in Table 22.
- When generating CSP keys for ‘TPM Duplication’ Service listed in Table 21 (export) the operator shall set the CSP key attribute encryptedDuplication, which enforces
  - FIPS Approved key transport when using RSA Keys or
  - FIPS Approved key agreement when using ECC Keys
  - In combination with FIPS Approved Key Wrapping using AES and HMAC during export.
- When using ‘TPM Import Service’ listed in Table 19, for importing CSP keys into the module the operator shall only import CSP keys, which attribute encryptedDuplication set, enforcing
  - FIPS Approved key transport when using RSA Keys or
  - FIPS Approved key agreement when using ECC Keys
  - In combination with FIPS Approved Key Wrapping using AES and HMAC Keys by the module.

- As a consequence imported CSPs (and hence CSP protected under these imported CSPs) shall not be used in any service of the CSP attribute encryptedDuplication is not set.
- Unauthorized loading of Secret Keys into the module via TPM2_LoadExternal shall not be used.
- When using approved KTS with 3072-bit and 4096-bit RSA, the module shall obtain an assurance from a Trusted Third-Party that a partial public-key validation was performed on the public key received by the module.

Requirements for Authentication:

- When using the password verification mechanism for operator authentication, a password consisting of at least 12 randomly chosen characters, containing at least one character of the following 4 groups: uppercase letters, lowercase letters, numerals and symbols but still randomly chosen shall be used.
- When using Enhanced Authorization the operator shall ensure that the policy will require at least one of the following authentication mechanisms:
  - Password verification
  - Challenge-response mechanism based on a Message Authentication Code
  - Challenge-response mechanism based on a Public Key Digital Signature Algorithm

Requirements for Initialization:

- In case the TPM is in an un-owned state (e.g. default state after shipment) the operator shall initialize the authentication data to control the Owner and the Endorsement Hierarchy via usage of the *Write CSP Service [Authentication Data]* listed in the TPM Hierarchy Group in Table 19. For detailed information how to perform this please refer to section 10.
- After each Reset the operator shall initialize the authentication data to control the Platform Hierarchy via usage of the Write CSP Service [Authentication Data] listed in the TPM Hierarchy Group in Table 19.

10 Annex A – Module Initialization

When the TPM 2.0 is in an un-owned state (e.g., when the TPM is in the default state after shipment) the TPM shall be initialized, since all authentication values have a default value set to an EmptyAuth. Module Initialization (also referred to as Taking Ownership of the TPM 2.0) basically means to initialize several authorization and policy values and optionally to create a primary storage key. Initializing the authorization values (endorsementAuth, ownerAuth, lockoutAuth) will be performed with TPM2_HierarchyChangeAuth and initializing the policies (endorsementPolicy, ownerPolicy, lockoutPolicy) will be done with TPM2_SetPrimaryPolicy. The following flow shows a secure way to initialize the module:

- Check capabilities to see if ownership is enabled
  - TPM2_GetCapability with TPM_PT_PERMANENT and TPM_PT_STARTUP_CLEAR checking for ownerAuthSet == 0 and shEnable == 1
- TPM2_CreatePrimary to get the IFX-PE-KEK, for which a certificate exists
- Check the Endorsement Key certificate to verify that ownership is taken of an authentic Infineon TPM
- Start an encrypted authorization session using the IFX-PE-KEK-PUB to protect the secret
- TPM2_HierarchyChangeAuth using parameter encryption to protect the new auth values (endorsementAuth, ownerAuth, lockoutAuth)
- TPM2_SetPrimaryPolicy using the previously set auth values to set the corresponding policies (endorsementPolicy, ownerPolicy, lockoutPolicy)
- Optional: TPM2_CreatePrimary to create a storage primary key
- Optional: TPM2_EvictControl to make the storage primary key persistent

11 Annex B – Module Startup

When the TPM 2.0 is reset (e.g., when power is supplied to the TPM) the TPM shall be correctly started up since some authentication values have a default value set to an EmptyAuth. The TPM 2.0 sets the platformAuth to an EmptyAuth after a TPM reset (_TPM_Init) by default, which can be easily satisfied using the NULL password. To avoid control of the TPM 2.0 Platform Hierarchy using platformAuth from other entities than the platform BIOS, it is required to change the platformAuth to a secure random value immediately after a TPM reset. The changed platformAuth may be stored at a secure storage location, if needed by the BIOS or other processes during platform boot. Before transitioning to the OS the platformAuth value must be securely discarded at the stored secure location (e.g., overwritten with zeroes). The following flow shows a secure way to start up the module:

- Check the Endorsement Key certificate to verify that ownership is taken of an authentic Infineon TPM
- Start an encrypted authorization session using the IFX-PE-KEK-PUB to protect the secret
- TPM2_HierarchyChangeAuth using parameter encryption to protect the new auth values (platformAuth)
- TPM2_SetPrimaryPolicy using the previously set auth values to set the corresponding policies (platformPolicy)

References

[1] Trusted Platform Module Library Part 1: Architecture, Family “2.0”, Level 00 Revision 1.59, November 8 2019

[2] Trusted Platform Module Library Part 2: Structures, Family “2.0”, Level 00 Revision 1.59, November 8 2019

[3] Trusted Platform Module Library Part 3: Commands, Family “2.0”, Level 00 Revision 1.59, November 8 2019

[4] Trusted Platform Module Library Part 4: Supporting Routines, Family “2.0”, Level 00 Revision 1.59, November 8 2019

[5] Errata for TCG Trusted Platform Module Library, Version 1.1, June 18, 2020

[6] TCG PC Client Platform TPM Profile Specification for TPM 2.0, Version 1.05 Revision 14, May 13, 2020

[7] Security Requirements for Cryptographic Modules, FIPS Publication 140-2, May 25, 2001

[8] NIST, Secure Hash Standard, FIPS Publication 180-4, August 2015

[9] Digital Signature Standard (DSS), FIPS Publication 186-4, July 2013

[10] Advanced Encryption Standard (AES), FIPS Publication 197, November 26, 2001

[11] The Keyed-Hash Message Authentication Code (HMAC), FIPS Publication 198-1, July 2008

[12] NIST Special Publication SP 800-38A, Recommendation for Block Cipher Modes of Operation, 2001

[13] NIST Special Publication SP 800-38F, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, December 2012

[14] NIST Special Publication SP 800-56A, Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018

[15] NIST Special Publication SP800-56B, Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, March 2019

[16] NIST Special Publication SP800-56C, Revision 1, Recommendation for Key Derivation Methods in Key-Establishment Schemes, April 2018

[17] NIST Special Publication 800-90A, Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015

[18] NIST Special Publication 800-90B, Recommendation for Entropy Sources Used for Random bit Generation, January 2018

[19] NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009

[20] NIST Special Publication 800-131A, Revision 2, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019

[21] NIST Special Publication 800-133, Revision 2, Recommendation for Cryptographic Key Generation, June 2020

[22] NIST, January 5, 2021, Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program

[23] PKCS #1 v2.1, RSA Cryptography Standard, RSA Laboratories, June 14, 200

Trademarks
Areferenced product or service names and trademarks are the property of their respective owners

Edition 2023-06-28

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email:
dsscustomerservice@infineon.com

IMPORTANT NOTICE
The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenheitsgarantie").

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, 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.

In addition, any information given in this document is subject to customer's compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer's products and any use of the product of Infineon Technologies in customer's applications.

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.