STMICROELECTRONICS

Trusted Platform Module ST33TPHF20SPI

ST33HTPH2E28AAF0 / ST33HTPH2E32AAF0 /
ST33HTPH2E28AAF1 / ST33HTPH2E32AAF1
ST33HTPH2028AAF3 / ST33HTPH2032AAF3

FIPS 140-2 Security Policy
Level 2

Firmware revision:	49.00 / 4A.00
HW version:	ST33HTPH revision A

Date: 2017/07/19
Document Version: 01-11

NON-PROPRIETARY DOCUMENT

Table of Contents

1 MODULE DESCRIPTION 3

1.1 DEFINITION 3
1.2 MODULE IDENTIFICATION 3
1.2.1 AAF0 / AAF1 3
1.2.2 AAF3 4
1.3 PINOUT DESCRIPTION 6
1.4 BLOCK DIAGRAMS 8
1.4.1 HW block diagram 8
1.4.2 FW block diagrams 9
1.5 SECURITY LEVELS 11
1.6 CRYPTOGRAPHIC FUNCTIONS 12
1.7 MODES OF OPERATION 13
1.7.1 Security module configuration 13
1.7.2 Approved modes of operation 14
1.7.3 FIPS mode recommendations 14
1.7.4 Limited and error modes 15
1.8 PORTS AND INTERFACES 16

2 IDENTIFICATION AND AUTHENTICATION POLICY 17

2.1 ROLES 17
2.2 AUTHENTICATION 17
2.2.1 Description 17
2.2.2 Authorization strength 18
2.2.3 Authorization protection 18

3 ACCESS CONTROL POLICY 19

3.1 LIST OF KEYS AND CSPS 19
3.2 SERVICES 24
3.2.1 Services list 24
3.2.2 Authorization 30
3.3 KEY MANAGEMENT 32
3.3.1 Key entry and output 32
3.3.2 Key transport 33

4 SELF-TESTS 34

4.1 POWER-UP TESTS LIST 34
4.2 ASYMMETRIC CRYPTOGRAPHY SELF-TESTS LIST 35
4.3 CONDITIONAL TESTS LIST 35
4.4 VERIFICATION 36

5 PHYSICAL SECURITY POLICY 37

6 OPERATIONAL ENVIRONMENT 38

7 MITIGATIONS OF OTHER ATTACKS 39

7.1 INTERNAL TAMPER DETECTION 39
7.2 ENVIRONMENTAL PROTECTION 39

8 REFERENCES 40

9 ACRONYMS 42

IMPORTANT NOTICE – PLEASE READ CAREFULLY 43

1 MODULE DESCRIPTION

1.1 Definition

The ST33TPHF20SPI Trusted Platform Module is a fully integrated security module designed to be integrated into personal computers and other embedded systems. The security module is used primarily for cryptographic key generation, key storage and key management as well as generation and secure storage for digital certificates.

The TPM is a single chip cryptographic HW module as defined in **[FIPS 140-2]**. The single silicon chip is encapsulated in a hard, opaque, production grade integrated circuit (IC) package.

The cryptographic boundary is defined as the perimeter of the IC package. The security module supports SPI interface compliant with the Trusted Computing Group (TCG) specification for PC Client [PTP 0.43]. The HW and FW cryptographic boundaries are indicated in §1.4 of the current document.

The security module implements version 2.0 of the Trusted Computing Group (TCG) specification for Trusted Platform Modules (TPM).

1.2 Module identification

The hardware and firmware versions covered by the FIPS evaluation are identified as follow:

- Hardware version: ST33HTPH revision A
- Firmware version: 49.00 / 4A.00

FW version can be retrieved via response to the command TPM2_GetCapability with property set to TPM_PT_FIRMWARE_VERSION_1.

The cryptographic services are provided by the cryptographic library "NesLib 5.1 for ST33".

The product is manufactured in two packages:

- TSSOP28
  - TSSOP 28-pin
  - 4.4 x 9.7 mm
- VQFN32
  - Very thin pitch Quad pack no-lead 32-pin
  - 5 x 5 mm

The security module is available in the following configurations:

1.2.1 AAF0 / AAF1

These configurations of the security module implement both version 1.2 and version 2.0 of the Trusted Computing Group (TCG) specification for Trusted Platform Modules (TPM). Versions are exclusive and security module manufactured will operate in a default mode (TPM1.2 or TPM2.0) depending on the configuration.

The current FIPS 140-2 level2 security policy applies to these security module configurations when the module is irreversibly locked in TPM2.0 mode (cf. §1.7.3 for mode lock recommendations). As a consequence the TPM FW version 1.2 is excluded from the security requirements of FIPS 140-2.

Table 1: Security module configurations

	Module configuration			
Product name / HW version	ST33TPHF2ESPI/ ST33HTPH revision A			
Package	TSSOP28	VQFN32	TSSOP28	VQFN32
Part number	ST33HTPH2E28 AAF0	ST33HTPH2E32 AAF0	ST33HTPH2E28 AAF1	ST33HTPH2E32 AAF1
Default mode	TPM1.2		TPM2.0	
Marking	P68HAAF0		P68HAAF1	
FW version	49.00			

Figure 1: Picture of the Cryptographic Module (TSSOP28) – Marking

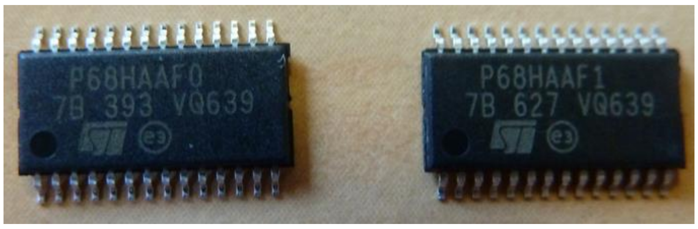
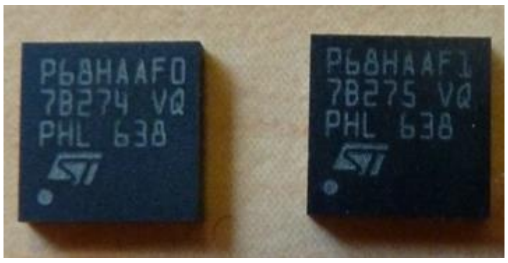


Figure 2: Picture of the Cryptographic Module (VQFN32) – Marking



P68HAAF0 corresponds to the module configured by default in TPM1.2 execution mode. This module is listed as it can be configured in TPM2.0 execution mode as described in §1.7. P68HAAF1 corresponds to the module configured by default in TPM2.0 execution mode.

1.2.2 AAF3

These configurations of the security module implement only the version 2.0 of the Trusted Computing Group (TCG) specification for Trusted Platform Modules (TPM). The current FIPS 140-2 level2 security policy always applies (no mode lock requested) to these security module configurations.

Table 2: Security module configurations

	Module configuration	
Product name / HW version	ST33TPHF20SPI/ ST33HTPH revision A	
Package	TSSOP28	VQFN32
Part number	ST33HTPH2028AAF3	ST33HTPH2032AAF3
Marking	P68HAAF3	
FW version	4A.00	

Figure 3: Picture of the Cryptographic Module (TSSOP28) – Marking

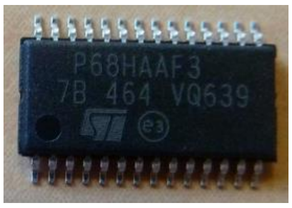
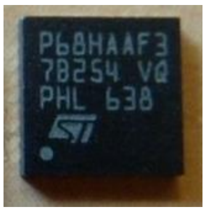


Figure 4: Picture of the Cryptographic Module (VQFN32) – Marking



1.3 Pinout description

The pin layouts for the ST33TPHF20SPI are shown in Figure 5 and in Figure 6: VQFN32 Pinout Diagram.

Figure 5: TSSOP28 Pinout Diagram

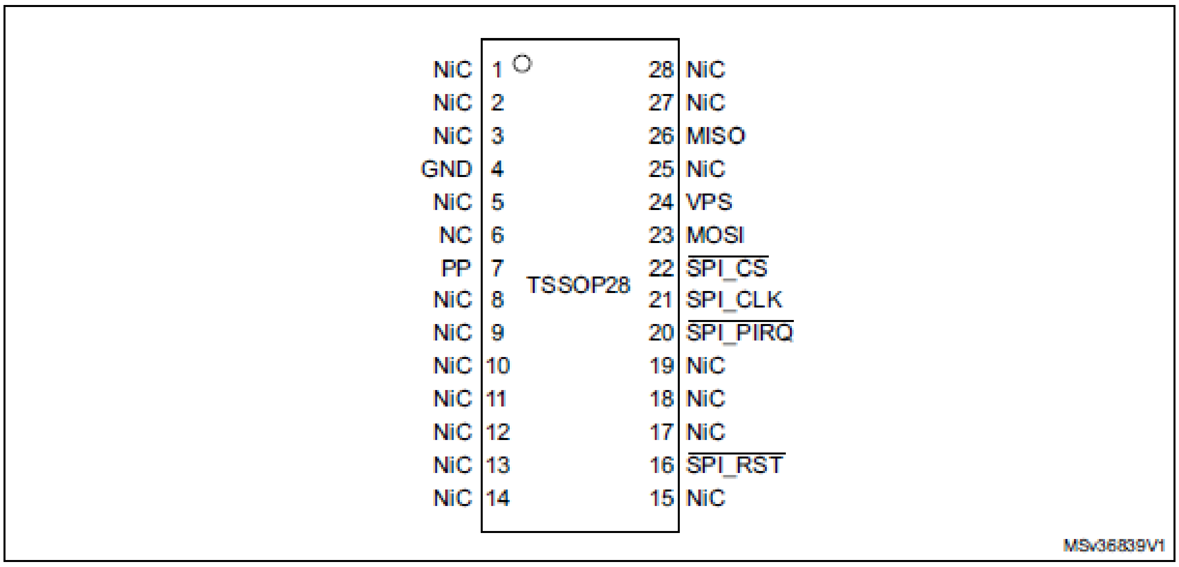
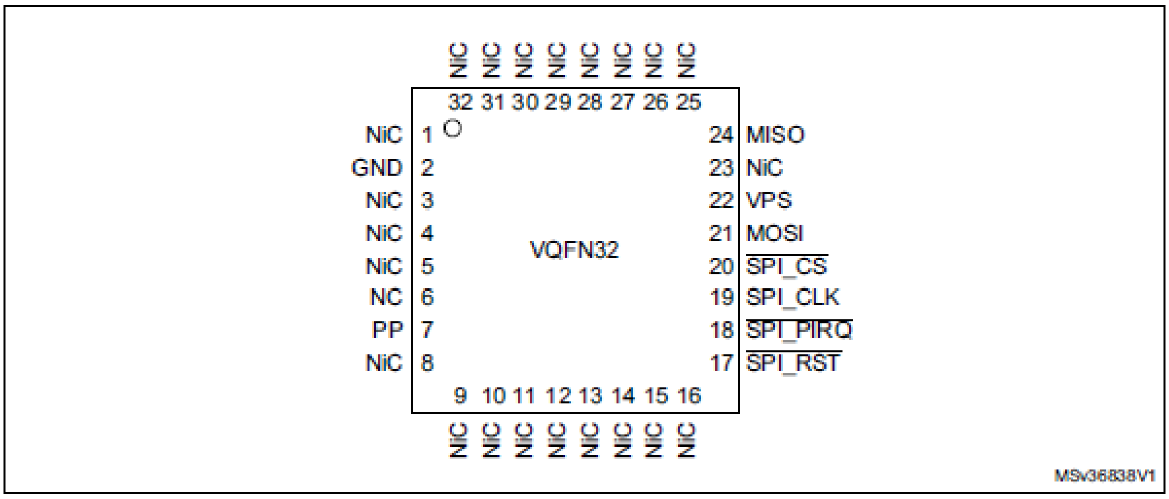


Figure 6: VQFN32 Pinout Diagram



NiC NiC NiC NiC NiC NiC NiC NiC
32 31 30 29 28 27 26 25
NiC 1
GND 2
NiC 3
NiC 4
NiC 5
NC 6
PP 7
NiC 8
VQFN32
24 MISO
23 NiC
22 VPS
21 MOSI
20 $\overline{\text{SPI\_CS}}$
19 SPI_CLK
18 $\overline{\text{SPI\_PIRQ}}$
17 $\overline{\text{SPI\_RST}}$
9 10 11 12 13 14 15 16
NiC NiC NiC NiC NiC NiC NiC NiC
MSv36838V1

Next table gives a description of the products pins.

Table 3: ST33TPHF20 Pin definition (SPI configuration)

Signal	Type	Description
VPS	Input	**Power supply**. This pin must be connected to 1.8V or 3.3V DC power rail supplied by the motherboard.
GND	Input	GND has to be connected to the main motherboard ground.
$\overline{\text{SPI\_RST}}$	Input	**SPI Reset** used to re-initialize the device
MISO	Output	**SPI** Master Input, Slave Output (output from slave)
MOSI	Input	**SPI** Master Output, Slave Input (output from master)
SPI_CLK	Input	**SPI** serial clock (output from master)
$\overline{\text{SPI\_CS}}$	Input	**SPI** slave select (active low; output from master)
$\overline{\text{SPI\_PIRQ}}$	Output	**SPI IRQ** used by TPM to generate an interrupt
PP	Input	**Physical presence**, active high, internal pull-down. Used to indicate Physical Presence to the TPM.
NiC	-	**Not internally connected:** not connected to the die. May be left unconnected but no impact on TPM if connected.
NC	-	**Not Connected:** connected to the die but not usable. May be left unconnected. Internal pull-down.

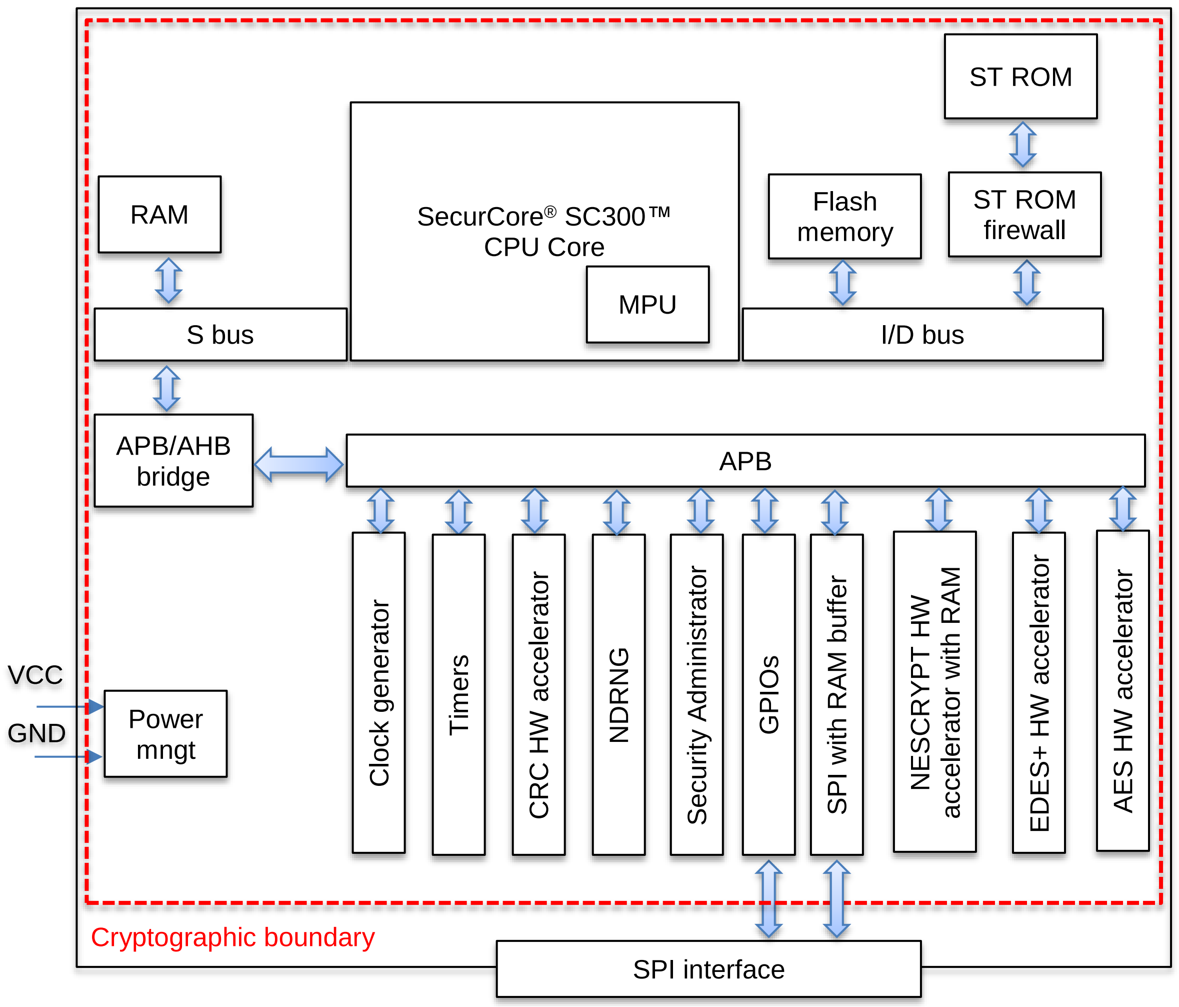
1.4 Block diagrams

1.4.1 HW block diagram

A block diagram of the hardware ST33HTPH (with its associated cryptographic boundary) is provided in Figure 7. TPM is composed of:

- A SecurCore® SC300™ CPU core including a MPU (Memory Protection Unit)
- Memories (RAMs, Flash and ROM)
- HW accelerators for CRC (16 and 32-bits) and cryptographic operations (symmetric with EDES+ and AES and asymmetric with NESCRYPT)
- A clock generator and three 16-bit timers
- NDRNG (non-deterministic random bit generator)
- SPI master/slave block
- A security administration block dedicated to chip security configuration and alarms detection
- FW and data stored in the memory areas

Figure 7: ST33HTPH block diagram

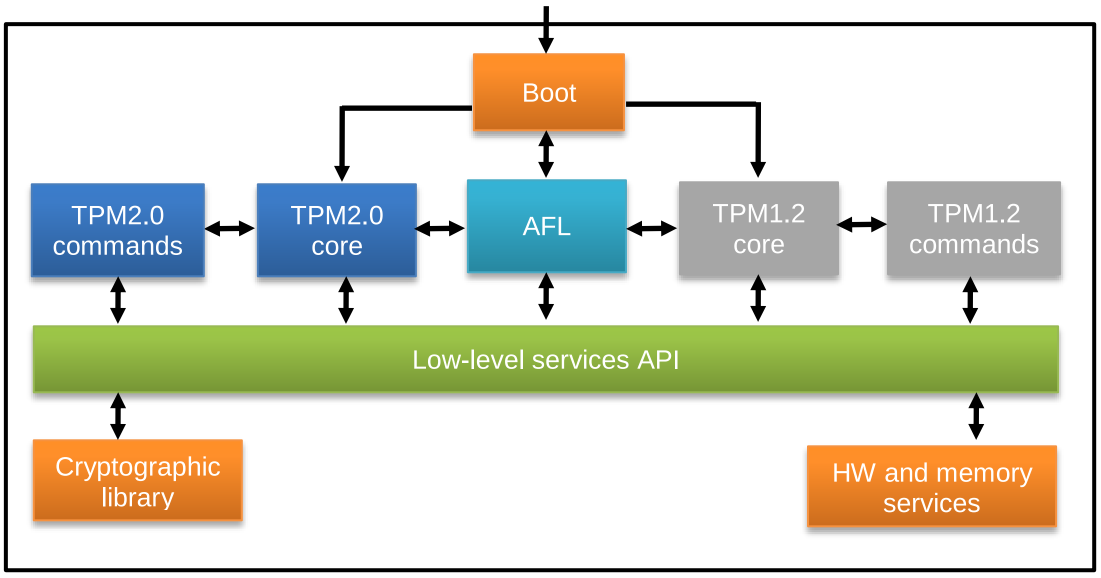


1.4.2 FW block diagrams

Block diagrams of the TPM FW are provided at Figure 8: TPM FW block diagram (TPM2E) and Figure 9: TPM FW block diagram.

1.4.2.1 AAF0 / AAF1

Figure 8: TPM FW block diagram (TPM2E)



TPM FW is composed of:

- Non-upgradable code blocks located in ROM & flash memories (depicted in orange)
  - Boot code
  - Cryptographic library
  - HW and memory low-level services
- Upgradable code blocks via secure field upgrade mechanism (blue and green boxes)
  - Application flash loader (AFL) in charge of TPM field upgrade
  - TPM1.2 core (irreversibly deactivated as indicated in §1.7.1)
  - TPM1.2 commands code (irreversibly deactivated as indicated in §1.7.1)
  - TPM2.0 core
  - TPM2.0 commands code
  - Low-level services API (incl. cryptographic services, memory management, …)

1.4.2.2 AAF3

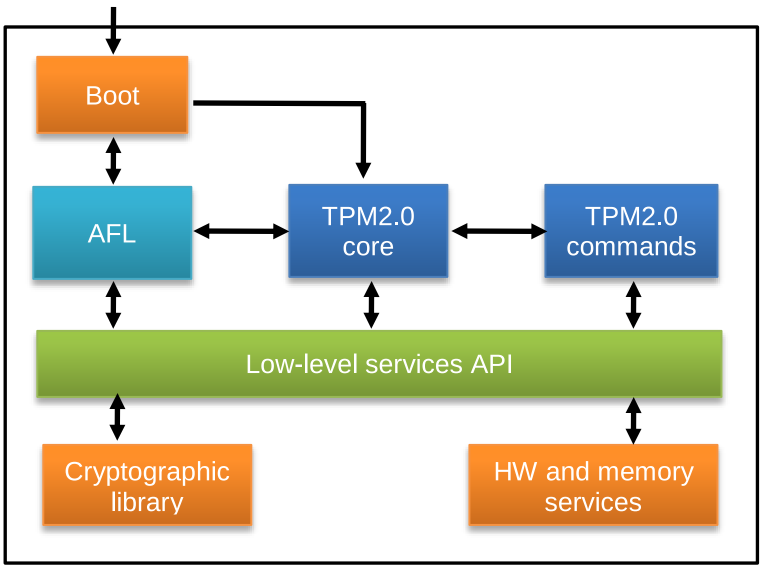


Figure 9: TPM FW block diagram (TPM20)

TPM FW is composed of:

- Non-upgradable code blocks located in ROM & flash memories (depicted in orange)
    - Boot code
    - Cryptographic library
    - HW and memory low-level services
- Upgradable code blocks via secure field upgrade mechanism (blue and green boxes)
    - Application flash loader (AFL) in charge of TPM field upgrade
    - TPM2.0 core
    - TPM2.0 commands code
    - Low-level services API

1.5 Security levels

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 4: Module Security Level Specification

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

1.6 Cryptographic functions

The security module supports the following cryptographic algorithms (both approved and non-approved). Algorithm certificate numbers for each approved algorithm are listed below. All algorithms, keys size or curve lengths listed below are part of services offered by the module.

Table 5: Approved algorithms

CAVP Cert	Algorithm	Standard	Mode / Method	Key lengths, curves or moduli	Use
2342 & 2340	RSA	FIPS 186-4	SHA-256, RSASSA-PKCS-v1.5	2048	Digital signature generation
		FIPS 186-4	SHA-1, SHA-256, RSASSA-PKCS-v1.5, RSASSA-PSS	2048	Digital signature verification
		FIPS 186-4	Appendix C3.1	2048	Key generation
1045 & 1041	CVL RSADP	FIPS 186-4	RSA decryption primitive	2048	Key transport
1025	ECDSA	FIPS 186-4	SHA-256	P-224, P-256	Digital signature generation
		FIPS 186-4	SHA-1, SHA-256	P-224, P-256	Digital signature verification
		FIPS 186-4	Appendix B.4.2	P-224, P-256	Key generation
110 & 108	KAS EC-DH	SP 800-56A	ECC	P-224, P-256	Key agreement
2870 & 2875	HMAC (single call)	FIPS 198-1	SHA-1, SHA-256	160, 256	Message authentication
2878 & 2876	HMAC (sequence)	FIPS 198-1	SHA-1, SHA-256	160, 256	Message authentication
123 & 121	KBKDF	SP 800-108	CTR		Key derivation
1361	DRBG	SP 800-90A	HASH_based		Deterministic random bit generation
4338 & 4336	AES	FIPS 197, SP 800-38A	ECB, CFB128, OFB, CBC, CTR	128, 192, 256	Data encryption/decryption
2345 & 2343	Triple-DES	SP 800-67, SP 800-38A	TECB, TCBC, TCFB64, TOFB, CTR	192	Data encryption/decryption
NA	KTS (AES cert #4338 + HMAC cert #2870) KTS (AES cert #4336 + HMAC cert #2875)	SP 800-38F	CFB	128, 256	Key transport
3539	SHS	FIPS 180-4	SHA-1, SHA-256		Message digest
Vendor affirmation	CKG	SP800-133 (per IG D.12)	Direct generation, Generation		Key generation[1]

Table 6: Allowed algorithms

Algorithm	Caveat	Use
RSA	Key length = 1024 bits	Digital signature verification

[1] Symmetric keys and seeds used for generating the asymmetric keys are either generated by using KBKDF or DRBG methods. Methods are detailed per CSPs in Table 13: Keys and CSPs list.

RSA key wrapping	Key length = 2048 bits	Key establishment
SHA-1	NA	Digital signature verification
NDRNG	NA	Seed or reseed DRBG 800-90A (with approximatively 366 bits of entropy). Generate random numbers not dedicated to be used as cryptographic material.

Table 7: Non-approved algorithms

Algorithm	**Use**
RSA (key length = 1024 bits)	Key and digital signature generation
SHA-1	Digital signature generation
ECSchnorr	Digital signature generation and verification
ECDAA	Digital signature generation

1.7 Modes of Operation

This security policy only applies to the security module when TPM operator follows the recommendations from:

- §1.7.1 to set and irreversibility lock the security module in the TPM2.0 mode and exclude the non-compliant mode TPM1.2 that is outside the scope of the evaluation.
- §1.7.2 to execute all self-tests required in a FIPS 140-2 approved mode of operation
- §1.7.3 to use the security module in a FIPS 140-2 approved mode of operation

1.7.1 Security module configuration

1.7.1.1 AAF0

These security module configurations implement both TPM1.2 and TPM2.0 specifications and are set to operate by default in TPM1.2 mode. To set and irreversibility lock the security module in the TPM2.0 mode, TPM operator shall:

- Execute the TPM_SetMode proprietary command with the following parameters:
  - mode = 0x01 (TPMLib SET to switch to TPM2.0)
  - modeLock = 0x01 (TPMLibLock SET to lock the selected mode)
- Reset the TPM

1.7.1.2 AAF1

These security module configurations implement both TPM1.2 and TPM2.0 specifications and are set to operate by default in TPM2.0 mode. To irreversibility lock the security module in the TPM2.0 mode, TPM operator shall:

- Execute the TPM2_SetMode proprietary command with the following parameters:
  - mode = 0x01 (TPMLib SET to maintain the module in TPM2.0 mode)
  - modeLock = 0x01 (TPMLibLock SET to lock the selected mode)
- Reset the TPM

1.7.1.3 AAF3

No action requested for these security modules configurations.

1.7.2 *Approved modes of operation*

TPM supports 2 sequential approved modes of operation.

1.7.2.1 *Approved mode 1*

This mode is the default mode when TPM starts. This mode is limited to a subset of TPM services.

Table 8: Approved mode 1

Properties	Description
Definition	Transient mode of operation when TPM is power-up and before TPM2_SelfTest(full=YES) execution
Configuration	No configuration required
Services available	List of available services is indicated in last column of Table 14: Command support table.
Algorithms used	SHA / HMAC / AES / DRBG / KDF / TDES
CSPs used	List of CSPs that might be accessed in this mode is indicated in Table 14: Command support table.
Self-tests	SHS / HMAC / AES / DRBG / KDF / TDES / HW integrity / FW integrity / NDRNG

1.7.2.2 *Approved mode 2*

This mode is the full FIPS approved mode of operation.

Table 9: Approved mode 2

Properties	Description
Definition	Full approved mode of operation
Configuration	TPM2_SelfTest(full=YES) execution
Services available	All services
Algorithms used	All supported algorithms (cf. §1.6)
CSPs used	All CSPs
Self-tests	SHS / HMAC / AES / DRBG / KDF / TDES / RSA / ECDH / ECDSA / HW integrity / FW integrity / NDRNG

1.7.3 *FIPS mode recommendations*

To use the TPM in a FIPS approved mode of operation (valid for mode1 and mode2), the TPM operator **shall**:

- Use an encryption session for the commands that inputs/outputs CSPs (List is indicated at §3.3.1). For commands without authorization, encryptedSalt used in TPM_StartAuthSession on encryption session creation must be different from the empty buffer.
- Use an approved symmetric algorithm (AES) for encryption sessions
- Use authorization session based on HMAC or policy (no password allowed, cf. §2.2.1).
- Duplicate only objects with *encryptedDuplication* attribute set.
- Not use FIPS 140-2 non-approved algorithms:
    - SHA-1 for RSA digital signature generation
    - EC Schnorr for ECC digital signature generation

- ECDAA for ECC digital signature generation

  For the following services:

  - TPM2_Sign, TPM2_Certify, TPM2_CertifyCreation, TPM2_Quote, TPM2_GetSessionAuditDigest, TPM2_GetCommandAuditDigest, TPM2_GetTime, TPM2_NV_Certify, TPM2_Commit

- Not use TPM2_LoadExternal service to load TDES keys into the TPM
- Use a policy including TPM2_PolicyAuthValue as a minimum in the policy sequence in case authorization is ensured by policy (authorization by policy must be at least as secure as authorization by HMAC).
- Use TPM2_HierarchyChangeAuth after first TPM init or after each TPM2_Clear to set the authorization value for the endorsement, platform, owner and lockout hierarchies.
- Use TPM2_CreatePrimary command only for RSA and ECC key with default template.

If operator does not strictly follow the FIPS approved mode recommendations (ex: use of XOR instead of AES in encryption session), TPM is considered as being in a FIPS non-approved mode of operation.

To use the TPM in a FIPS approved mode if it was previously used in a FIPS non-approved mode, the operator shall:

- Zeroize all data listed in Table 13: Keys and CSPs list that could potentially be reused as CSPs in FIPS approved mode

To use the TPM in a FIPS non-approved mode if it was previously used in a FIPS approved mode, the operator shall:

- Zeroize all CSPs listed in Table 13: Keys and CSPs list that could potentially be used by FIPS non-approved algorithms in FIPS approved mode

1.7.4 Limited and error modes

TPM may reach specific states depending on sequence of operation that occurred.

1.7.4.1 Shutdown mode

The shutdown mode is an infinite HW reset loop that may be exit only by a power-off/power-on sequence. This state is entered when TPM detects that a FW integrity check failed during the TPM boot sequence.

1.7.4.2 Failure mode

Failure mode is a state of TPM that restricts the commands that can be executed to TPM_Startup / TPM_GetCapability / TPM_GetTestResult for TPM1.2 and TPM2_GetCapability / TPM2_GetTestResult for TPM2.0. TPM answers to all other commands with a specific error code: TPM_FAILEDSELFTEST (0x1C) for TPM1.2 and TPM_RC_FAILURE (0x101). This state is entered when one (except FW integrity test) of the self-tests fails.

1.7.4.3 Reduced mode

The reduced mode is a specific state of the field upgrade mode (refer to §6) that can be reached if the on-going field upgrade procedure failed due to an error detected in the field upgrade commands received. In reduced mode, only a subset of commands might be executed: TPM_FieldUpgradeStart / TPM_FieldUpgradeData / TPM_GetCapability / TPM_GetTestResult / TPM_ContinueSelfTest for TPM1.2 and TPM2_FieldUpgradeStart / TPM2_FieldUpgradeData / TPM2_GetCapability / TPM2_GetTestResult / TPM2_SelfTest for TPM2.0. TPM answers to all other commands with the error TPM_RC_COMMAND_CODE (0x143). Reduced mode can be exited in case of the reception of a successful TPM_FieldUpgradeStart/TPM2_FieldUpgradeStart command that reloads the previous installed firmware.

1.8 Ports and interfaces

The physical port of the security module is the SPI bus. The logical interfaces and their mapping to physical ports of the module are described below:

Table 10 : Ports and interfaces

Logical interface	Description	Physical port
Control Input Interface	Control Input commands issued to the security module	**SPI :** $\overline{\text{SPI\_CS}}$ / SPI_CLK / MOSI / SPI_RST / PP
Status Output Interface	Status data output by the chip	**SPI :** $\overline{\text{SPI\_CS}}$ / SPI_CLK / MISO / SPI_PIRQ
Data Input Interface	Data provided to the chip as part of the data processing commands	**SPI :** $\overline{\text{SPI\_CS}}$ / SPI_CLK / MOSI
Data Output Interface	Data output by the chip as part of the data processing command	**SPI :** $\overline{\text{SPI\_CS}}$ / SPI_CLK / MISO
Power interface	Power interface of the chip	VPS / GND

Here are some details concerning the ports and interfaces of TPM:

1. The module does not include a maintenance interface.
2. Control and data inputs are multiplexed over the same physical interface. Control and data are distinguished by properly parsing input TPM command parameters according to input structures description, indicated for each command in **[TPM2.0 Part3 r1.16]**[1].
3. Status and data output are multiplexed over the same physical interface. Status and data are distinguished by properly setting output TPM response parameters according to output structures description, indicated for each command in **[TPM2.0 Part3 r1.16]**.
4. The logical state machine and the command structure parsing of the module prevent from using input data externally from the "data input path" and prevent from outputting data externally from the "data output path".
5. While performing key generation or key zeroization (no manual key entry on TPM), the output data path is logically disconnected while the output status path remains connected to report any possible failure during command processing. Generally, the output data path is only connected when TPM outputs response containing data.
6. Plaintext data can be output through usage of:
   - TPM2_Unseal, TPM2_RSA_Decrypt, TPM2_EncryptDecrypt

   To prevent inadvertent release of the plaintext data, command performs:
   - Check of command input structure
   - Check of command authorization
   - Decryption of the input blob with private part of specified key

   However an encryption session might be used with these commands to avoid releasing plaintext data.
7. The logical state machine and command structure of the module guarantees the inhibition of all data output via the data output interface whenever an error state exists and while doing self-tests.

[1] Some commands only deal with control input and status output parameters

2 IDENTIFICATION AND AUTHENTICATION POLICY

This chapter gives details about the roles managed by TPM.

2.1 Roles

Services proposed by TPM are accessible under different roles. Next table defines the different roles supported by the TPM.

Table 11: Roles

Role	Description	Type of authentication	Authentication data
Crypto officer (CO)	Role that requires knowledge of the authValue or authPolicy associated to one of the hierarchy (incl. lockout).	Role based	256-bit secret data (authValue and/or authPolicy)
User (U)	Role that requires knowledge of the authValue or authPolicy associated to one object or NV index.	Role based	160-bit or 256-bit secret data (authValue and/or authPolicy). Authorization depends on userWithAuth object attribute.
Admin (A)	The object Administrator controls the certification of an object (TPM2_Certify and TPM2_ActivateCredential) and controls changing of the authValue of an object (TPM2_ObjectChangeAuth).	Role based	160-bit or 256-bit secret data (authValue and/or authPolicy). Authorization depends on adminWithPolicy object attribute.
DUP (D)	This authorization role is only used for TPM2_Duplicate(). If duplication is allowed, authorization must always be provided by a policy session and the authPolicy equation of the object must contain a command that sets the policy command code to TPM_CC_Duplicate.	Role based	160-bit or 256-bit secret data (authPolicy).

Some commands can also be executed without any authorization role. Those commands are marked as NA in the service list table (Table 14: Command support table).

The security module does NOT provide a Maintenance Role or Maintenance Interface and does NOT support concurrent operators.

Roles are implicitly selected by TPM operator on command execution (cf. Table 14 for correspondence between service and supported role) by proving knowledge of the authorization value or knowledge of the policy sequence (nature of authorization session indicates the type of authorization) that are associated with the object the command is operating on.

An operator might switch from one role to another by executing commands requiring different roles and proving knowledge of the authorization value or policy sequence of objects the role is associated to.

2.2 Authentication

2.2.1 Description

In FIPS approved mode of operation, TPM uses a mechanism for authorization that consists in:

1. Opening an authorization session that may be of the following types:
    a. HMAC
    b. Policy

2. Executing the expected policy commands sequence in case of policy authorization session (defined policy must follow recommendations listed in §1.7.3).
3. Do the comparison between reference value and computed value. If both match, command execution is authorized.

More details on HMAC and policy sessions can be found in §19 of [TPM2.0 Part1 r1.16].

2.2.2 *Authorization strength*

As minimum value of authorization or policy values might be 160-bit random values (based on unbiased distribution of '0' and '1'), the probability for an attacker to guess the authorization data is:

$$\frac{1}{2^{160}} = 6.84 * 10^{-49}$$

This value is then higher than the minimum of $1*10^{-6}$ required by **[FIPS140-2]**.

The number of attempts per minute that an attacker can make is limited by the DAM (Dictionary Attack Mechanism). DAM consists in counting the number of failed authentication. When this counter reaches a pre-defined threshold, a lockout period is started. During this period, no authorized command execution is allowed and a specific error is returned in TPM response until period expires. Next table indicates the threshold values and the lockout durations:

Table 12: DAM lockout durations

Failed authentication counter	>31
Lockout period (in seconds)	7200

This table indicates that an attacker can do a maximum (during the first minute) of 32 trials per minute before DAM being active. As a result the probability per minute that a random attempt will lead to a successful authorization matches FIPS requirements. Value is equal to:

$$32 * \frac{1}{2^{160}} = 2.19 * 10^{-47}$$

This value is then higher than the minimum of $1*10^{-5}$ required by **[FIPS140-2]**.

NB: commands handling (reception, processing and response sending) is negligible compared to the lockout periods and not taken into account in the above computation.

NB2: DAM parameters might be changed by using TPM2_DictionnaryAttackParameters command. However to operate in a FIPS approved mode, they shall not be changed in order not to decrease the authorization strength computed above.

2.2.3 *Authorization protection*

By following recommendations to operate in FIPS mode of operation, authorization data associated to objects, NV indexes or hierarchies are never output from TPM in plaintext form and thus are protected from unauthorized disclosure.

Authorization can be changed via the following services:

- TPM2_ObjectChangeAuth
- TPM2_HierarchyChangeAuth
- TPM2_NV_ChangeAuth

As indicated in Table 14, roles that imply authentication are associated with these services meaning that authentication are protected against unauthorized modification and substitution.

TPM authorization mechanism (HMAC or policy digest comparison) does not provide any information about authentication data or policy sequence. Authentication indicates pass (command executed) or fail (command not executed) and does not provide feedback that could weaken the strength of authentication.

3 ACCESS CONTROL POLICY

This chapter gives details about the services, keys and CSPs that the TPM manages.

3.1 List of Keys and CSPs

Table 13: Keys and CSPs list

Keys/CSPs		Description	Zeroized
Index	Name		
Hierarchies			
1	nullSeed	32 bytes primary seed values resp. for NULL, platform, endorsement and storage hierarchies. NullSeed is a random value generated by HDRBG at each TPM power-up. PpSeed / epSeed / spSeed are random values generated by HDRBG at first TPM power-up. They are used as keys for: • KDFa to derive seedValue and sensitive during object creation (cf. [TPM2.0 Part1 r1.16] §27.6.4) • KDFa to generate a symmetric encryption key used in TPM2B_PRIVATE structure en/decryption. • KDFa to generate HMAC key used in TPM2B_PRIVATE integrity protection generation or verification They are used as seeds for: • DRBG to generate random as input to prime numbers (RSA) and private key generation (ECC)	TPM reset
2	ppSeed		TPM2_Change PPS
3	epSeed		TPM2_Change EPS
4	spSeed		TPM2_Clear
5	nullProof	32 bytes secret values resp. for NULL, platform, endorsement and storage hierarchies. NullProof is a random value generated by HDRBG at each TPM power-up. PhProof / ehProof / shProof are random values generated by HDRBG at first TPM power-up. They are used as keys for: • KDFa to generate context encryption key and IV (cf. [TPM2.0 Part1 r1.16] §30.3.1) • HMAC to compute context blob integrity (cf. [TPM2.0 Part1 r1.16] §30.3.2) • HMAC to compute/verify tickets shProof is used also as key for: • KDFa to generate obfuscation value used in attestation commands (cf. [TPM2.0 Part1 r1.16] §36.7)	TPM reset
6	phProof		TPM2_Change PPS
7	ehProof		TPM2_Clear
8	shProof		TPM2_Clear
9	platformAuth	32 bytes authorization data (authValue) used in authorization session based resp. on platform, endorsement, and storage or lockout hierarchy authorization. PlatformAuth is set to 0 at each TPM2_Startup (CLEAR). EndorsementAuth / ownerAuth / lockoutAuth are set to 0 at first TPM power-up. Primary auth values can be changed with command TPM2_HierarchyChangeAuth. They are used as keys for: • HMAC authorization in case of unsalted and unbound session • KDFa to generate session key used in HMAC authorization in case of bound session They are used as part of keys for: • HMAC authorization in case of salted or bound session (key is concatenation of sessionKey and authValue) • KDFa to generate session key used in HMAC authorization in case of salted and bound session (key is concatenation of authValue and salt)	TPM2_Startup
10	endorsementAuth		TPM2_Clear / TPM2_Change EPS
11	ownerAuth		TPM2_Clear
12	lockoutAuth		TPM2_Clear

		They are used as reference values for comparison in case of password authorization session.	
13	platformPolicy	32 bytes authorization data (authPolicy) used in authorization session based resp. on platform, endorsement, storage or lockout hierarchy policy. platformPolicy is set to 0 at each TPM2_Startup (CLEAR). endorsementPolicy / ownerPolicy / lockoutPolicy are set to 0 at first TPM power-up. Primary policies can be changed with command TPM2_SetPrimaryPolicy. They are used as reference values for a comparison in case of policy session.	TPM2_Change PPS
14	endorsementPolicy		TPM2_Clear / TPM2_Change EPS
15	ownerPolicy		TPM2_Clear
16	lockoutPolicy		TPM2_Clear
		Objects	
17	authValue	0 to 32 bytes authorization data defined during object creation (TPM2_Create/TPM2_CreatePrimary) used to authorize commands based on this object. Value can be changed with command TPM2_ObjectChangeAuth. It is used as: • HMAC and/or KDFa keys or part of keys in authorization session based on HMAC or password (usage is the same than for CSPs 9/10/11/12) • Secret value extended into policyDigest on TPM2_PolicySecret command	TPM2_Clear (owner & endorsement) TPM2_Change PPS (platform) TPM2_Change EPS (endorsement)
18	authPolicy	0 to 32 bytes authorization data defined during object creation (TPM2_Create/TPM2_CreatePrimary) used to authorize commands based on this object. It is used as reference value for a comparison in case of policy session	TPM2_Clear (owner & endorsement) TPM2_Change PPS (platform) TPM2_Change EPS (endorsement)
19	seed	32 random bytes generated by HDRBG if object parent is not a hierarchy (if hierarchy, primary seed is used, cf. CSPs 1/2/3/4). It is used as key for: • KDFa to generate seedValue and sensitive during object creation (cf. [TPM2.0 Part1 r1.16] §27.6.4)	Transient value only available during object creation
20	seedValue	32 bytes generated from seed (CSP 19) or one of the primary seeds (CSP 1/2/3/4) through use of KDFa. Set to 0 for asymmetric keys that are not used as storage key. It is used (when not set to 0) as: • Data in SHA computation to generate object's unique value (HMAC and symmetric key creation) • Key in KDFa to generate a symmetric encryption key used in TPM2B_PRIVATE structure en/decryption. • Key in KDFa to generate HMAC key used in TPM2B_PRIVATE integrity protection generation or verification	TPM2_Clear (owner & endorsement) TPM2_Change PPS (platform) TPM2_Change EPS (endorsement)
21	symKey	16 bytes generated from derivation of seedValue through KDFa usage. It is used as key for: • Symmetric en/decryption of TPM2B_PRIVATE structure	Transient value only available during command processing
22	hmacKey	32 bytes generated from derivation of seedValue through KDFa usage. It is used as key for:	Transient value only available during command processing

		• HMAC used in TPM2B_PRIVATE integrity protection generation or verification	
23	sensitive	Object sensitive part that might be passed as encrypted parameter to TPM2_Create command or generated with KDFa from seed or primary seed (if sensitiveDataOrigin attribute is set) in case object is a symmetric key or a HMAC key. For RSA or ECC key, sensitive corresponds to the private key. Depending on object's nature, sensitive is used as key for: • en/decryption (RSA, AES, TDES) • signature generation (RSA, ECDSA, HMAC) • secret value exchange (ECDH) Available key lengths correspond to the ones listed in **Table 5: Approved algorithms** (Key nature and length are selected by user thanks to the interface of the keys creation commands).	TPM2_Clear (owner & endorsement) TPM2_Change PPS (platform) TPM2_Change EPS (endorsement)
NV Indexes			
24	authValue	0 to 32 bytes authorization data defined during NV index creation (TPM2_DefineSpace) used to authorize commands based on this object. Value can be changed with command TPM2_NV_ChangeAuth. It is used as: • HMAC and/or KDFa keys or part of keys in authorization session based on HMAC or password. • Secret value extended into policyDigest on TPM2_PolicySecret command	TPM2_NV_Und efineSpace / TPM2_NV_Und efineSpaceSpec ial
25	authPolicy	0 to 32 bytes authorization data defined during object creation (TPM2_DefineSpace) used to authorize commands based on this object. It is used as reference value for a comparison in case of policy session	TPM2_NV_Und efineSpace / TPM2_NV_Und efineSpaceSpec ial
Sessions			
26	salt	Value passed encrypted (with a loaded decrypt key) to TPM2_StartAuthSession. It is used as: • Part of KDFa key to generate the sessionKey (cf. [TPM2.0 Part1 r1.16] §19.6)	Transient value only available during TPM2_StartAut hSession processing
27	sessionKey	Key generated by KDFa (cf. [TPM2.0 Part1 r1.16] §19.6) and whose value depends on salt and bind parameters of TPM2_StartAuthSession command (size depends on symmetric algorithm used). It is used as: • HMAC key used to generate and verify command authorization • Part of KDFa key used to generate encryption key and IV of encryption-based session	TPM2_FlushCo ntext
28	encryption key and IV of encryption-based session	Symmetric key and IV generated by KDFa (cf. [TPM2.0 Part1 r1.16] §21.3) from sessionKey and object's authValue. It is used as key and IV for: • Symmetric en/decryption of first parameter of command/response if parameter structure is of type TPM2B_	TPM2_FlushCo ntext
Context			
29	contextKey	16 bytes randomly generated by HDRBG at each TPM reset. It is used as: • Key in KDFa to generate a symmetric encryption key and IV used in context blob en/decryption	TPM reset

30	symKey, IV	2*16 bytes derived by using KDFa from contextKey. It is used as key and IV for: • Symmetric en/decryption of context blob	Transient value only available during TPM2_ContextSave / TPM2_ContextLoad processing
Duplication			
31	inner symKey	Symmetric key passed as input to duplication commands or generated by HDRBG (size depends on symmetric algorithm used). It is used as: • Symmetric en/decryption key to protect TPM2B_PRIVATE output structure	Transient value only available during command processing
32	seed	32 bytes value randomly generated by HDRBG if new parent is a RSA key or via KDFe if new parent is an ECC key. It is used as key for : • KDFa to generate a symmetric en/decryption key for outer protection • KDFa to generate a HMAC key for outer integrity protection	
33	outer symKey	Symmetric key generated via KDFa from seed. It is used as key for: • Symmetric en/decryption key for outer protection of TPM2B_PRIVATE output structure	
34	outer hmacKey	HMAC key generated via KDFa from seed. It is used as key for: • HMAC integrity key for outer protection of TPM2B_PRIVATE output structure	
Credential			
35	seed	32 bytes value randomly generated by HDRBG if new parent is a RSA key or via KDFe if new parent is an ECC key. It is used as key for : • KDFa to generate a symmetric en/decryption key for outer protection • KDFa to generate a HMAC key for outer integrity protection	Transient value only available during command processing
36	symKey	Symmetric key generated via KDFa from seed. It is used as key for: • Symmetric en/decryption key for outer protection of credentialBlob	
37	hmacKey	HMAC key generated via KDFa from seed. It is used as key for: • HMAC integrity key for outer protection of credentialBlob	
DRBG			
38	DRBG state	Internal state (V and C secret values) of the HDRBG (based on SHA256) stored in RAM.	TPM2_Clear
ECC			
39	commitNonce	32 bytes value randomly generated by HDRBG at each TPM2_Startup (CLEAR). It is used as key for : • KDFa to generate an ECC ephemeral private key used in TPM2_EC_Ephemeral command / TPM2_ZGen_2Phase	Transient value only available during command processing
40	ephemeral key – derived from commitNonce	ECC private key (size depends on curve selected) generated with KDFa from commitNonce. It is used as ephemeral private key in: • TPM2_Ephemeral command (scalar multiplication) to generate the associated ephemeral public key • TPM2_Zgen_2Phase (ECDH scheme) to generate outZ2 (output point)	
41	ephemeral key	ECC private key (size depends on curve selected) generated with HDRBG. It is used as ephemeral private key in: • TPM2_ECDH_KeyGen command (ECDH scheme) to generate zPoint (output point)	

Primary keys			
42	Endorsement key - RSA primes	2 primes of 1024 bits used to construct EK if parameters in TPM2_CreatePrimary command match the default EK RSA template. Generated by FIPS140-2 compliant HSM.	TPM2_Change EPS
43	Endorsement key - ECC private key	ECC 256 bits private key used to construct EK if parameters in TPM2_CreatePrimary command match the default EK ECC template. Generated by FIPS140-2 compliant HSM.	TPM2_Change EPS
Field upgrade keys			
44	Field upgrade verification key	2048 bits permanent RSA key unique per TPM product line. Only public part of the key is stored in the TPM (modulus, exponent).	No (public key)
Transient DRBG			
47	Transient DRBG state	Internal state (V and C secret values) of a HDRBG instance (based on SHA256) stored in RAM. HDRBG is instantiated from primary seeds and used only in TPM2_CreatePrimary to generate prime numbers for primary RSA keys.	Transient DRBG state cleared at the end of random numbers generation
DRBG input seed			
48	DRBG input seed	48-bytes value output from a NDRNG.	Transient value

3.2 Services

Next table lists all services supported by the TPM and indicates for each service, the role that can use this service and the keys/CSPs that can be accessed.

3.2.1 Services list

Table 14: Command support table

Services		**Role**	**Keys and CSP access** W = write, O = output, Z = zeroize C = used as key in cryptographic operation R = read (and not used as C)	**Authorized in limited approved mode**
Start-up				
1	_TPM_Init	**NA**	W (first boot only) : 2, 3, 4, 6, 7, 8, 10, 11, 12, 14, 15, 16 W : 29, 38, 48	X
2	TPM2_Startup	**NA**	W : 1, 5, 9, 13, 39	X
3	TPM2_Shutdown	**NA**	**-**	X
Testing				
4	TPM2_SelfTest	**NA**	**-**	X
5	TPM2_IncrementalSelfTest	**NA**	**-**	X
6	TPM2_GetTestResult	**NA**	**-**	X
Session commands				
7	TPM2_StartAuthSession	**NA**	W : 26, 27, 38, 48 C : 9, 10, 11, 12, 17, 24, 26, 28, 38, 48	
8	TPM2_PolicyRestart	**NA**	-	
Objects commands				
9	TPM2_Create	**U**	R : 18 W : 19, 20, 21, 22, 23, 28, 38, 48 C : 17, 19, 20, 21, 22, 27, 28, 38, 48 O : 20, 23	
10	TPM2_Load	**U**	R : 18 W : 17, 18, 20, 21, 22, 23, 28, 38, 48 C : 17, 19, 20, 21, 22, 27, 28, 38, 48	
11	TPM2_LoadExternal	**NA**	W : 17, 18, 20, 21, 22, 23, 28, 38, 48 C : 17, 19, 20, 21, 22, 27, 28, 38, 48	X
12	TPM2_ReadPublic	**NA**	R : 23 W : 28 C : 28	X
13	TPM2_ActivateCredential	**A, U**	R : 18, 23, 35 W : 28, 36, 37, 38, 48 C : 27, 28, 35, 36, 37, 38, 48	
14	TPM2_MakeCredential	**NA**	R : 23 W : 28, 35, 36, 37 C : 28, 36, 37 O : 35	
15	TPM2_Unseal	**U**	R : 18, 23 W : 28, 38, 48 C : 27, 28, 38, 48 O : 23	

Services		Role	Keys and CSP access W = write, O = output, Z = zeroize C = used as key in cryptographic operation R = read (and not used as C)	Authorized in limited approved mode
16	TPM2_ObjectChangeAuth	**A**	R : 18 W : 17, 28, 38, 48 C : 27, 28, 38, 48	
Duplication commands				
17	TPM2_Duplicate	**D**	R : 18 W : 28, 31, 32, 33, 34, 38, 48 C : 27, 28, 31, 32, 33, 34, 38, 48 O : 23, 31, 32	
18	TPM2_Rewrap	**U**	R : 18, 32 W : 28, 31, 32, 33, 34, 38, 48 C : 27, 28, 31, 32, 33, 34, 38, 48 O : 23, 31, 32	
19	TPM2_Import	**U**	R : 18, 32 W : 28, 31, 33, 34, 38, 48 C : 27, 28, 31, 32, 33, 34, 38, 48 O : 23	
Asymmetric primitives				
20	TPM2_RSA_Encrypt	**NA**	C: 28	
21	TPM2_RSA_Decrypt	**U**	R : 18 W : 28, 38, 48 C : 23, 27, 28, 38, 48	
22	TPM2_ECDH_KeyGen	**NA**	W : 28, 41 C : 28, 41	
23	TPM2_ECDH_ZGen	**U**	R : 18 W : 28, 38, 48 C : 23, 27, 28, 38, 48	
24	TPM2_ECC_Parameters	**NA**	-	X
25	TPM2_ZGen_2Phase	**U**	R : 18 W : 28, 38, 48 C : 23, 27, 28, 38, 40, 48	
Symmetric primitives				
26	TPM2_EncryptDecrypt	**U**	R : 18 W : 28, 38, 48 C : 23, 27, 28, 38, 48	
27	TPM2_Hash	**NA**	W: 28 C: 28	
28	TPM2_HMAC	**U**	R : 18 W : 28, 38, 48 C : 23, 27, 28, 38, 48	
Random number generator				
29	TPM2_GetRandom	**NA**	C : 28, 38, 48	X
30	TPM2_StirRandom	**NA**	W : 28, 38, 48 C: 28	X
Hash/HMAC/Event sequences				

Services		Role	Keys and CSP access W = write, O = output, Z = zeroize C = used as key in cryptographic operation R = read (and not used as C)	Authorized in limited approved mode
31	TPM2_HMAC_Start	**U**	R : 18 W : 17, 28, 38, 48 C : 23, 27, 28, 38, 48	
32	TPM2_HashSequenceStart	**NA**	W: 17, 28 C: 28	X
33	TPM2_SequenceUpdate	**U**	R : 18 W : 28, 38, 48 C : 23, 27, 28, 38, 48	
34	TPM2_SequenceComplete	**U**	R : 18 W : 28, 38, 48 C : 23, 27, 28, 38, 48	
35	TPM2_EventSequenceComplete	**U**	R : 18 W : 28, 38, 48 C : 23, 27, 28, 38, 48	
Attestation commands				
36	TPM2_Certify	**A, U**	R : 18 W : 28, 38, 48 C : 8, 23, 27, 28, 38, 48	
37	TPM2_CertifyCreation	**U**	R : 18 W : 28, 38, 48 C : 8, 23, 27, 28, 38, 48	
38	TPM2_Quote	**U**	R : 18 W : 28, 38, 48 C : 8, 23, 27, 28, 38, 48	
39	TPM2_GetSessionAuditDigest	**CO**	R : 18 W : 28, 38, 48 C : 8, 23, 27, 28, 38, 48	
40	TPM2_GetCommandAuditDigest	**CO**	R : 18 W : 28, 38, 48 C : 8, 23, 27, 28, 38, 48	
41	TPM2_GetTime	**CO**	R : 18 W : 28, 38, 48 C : 8, 23, 27, 28, 38, 48	
Ephemeral EC keys				
43	TPM2_EC_Ephemeral	**NA**	W : 28, 40 C : 28, 39	
Signing and signature verification				
44	TPM2_VerifySignature	**NA**	R : 23 W : 28 C : 5, 6, 7, 8, 28	
45	TPM2_Sign	**U**	R : 18 W : 28, 38, 48 C : 5, 6, 7, 8, 23, 27, 28, 38, 48	
Command audit				

Services		Role	Keys and CSP access W = write, O = output, Z = zeroize C = used as key in cryptographic operation R = read (and not used as C)	Authorized in limited approved mode
46	TPM2_SetCommandCodeAuditStatus	**CO**	R : 13, 18 C : 9, 11, 15, 27	
Integrity collection (PCR)				
47	TPM2_PCR_Extend	**U**	R : 18 C : 27	
48	TPM2_PCR_Event	**U**	R : 18 W : 28, 38, 48 C : 27, 28, 38	
49	TPM2_PCR_Read	**NA**	**-**	X
50	TPM2_PCR_Allocate	**CO**	R : 13, 18 C : 9, 27	
53	TPM2_PCR_Reset	**NA**	**-**	
54	_TPM_Hash_Start	**NA**	**-**	X
55	_TPM_Hash_Data	**NA**	**-**	X
56	_TPM_Hash_End	**NA**	**-**	X
Enhanced authorization commands				
57	TPM2_PolicySigned	**NA**	C: 28	
58	TPM2_PolicySecret	**U**	R : 18 W : 28, 38, 48 C : 9, 10, 11, 12, 17, 24, 27, 28, 38, 48	
59	TPM2_PolicyTicket	**NA**	W : 28 C: 28	
60	TPM2_PolicyOR	**NA**	-	
61	TPM2_PolicyPCR	**NA**	W : 28 C: 28	
62	TPM2_PolicyLocality	**NA**	-	
63	TPM2_PolicyNV	**U**	R : 18 W : 28 C : 27, 28	
64	TPM2_PolicyCounterTimer	**NA**	W : 28 C: 28	
65	TPM2_PolicyCommandCode	**NA**	-	
66	TPM2_PolicyPhysicalPresence	**NA**	-	
67	TPM2_PolicyCpHash	**NA**	W : 28 C: 28	
68	TPM2_PolicyNameHash	**NA**	W : 28 C: 28	
69	TPM2_PolicyDuplicationSelect	**NA**	W : 28 C: 28	
70	TPM2_PolicyAuthorize	**NA**	W : 28 C: 28	
71	TPM2_PolicyAuthValue	**NA**	-	
72	TPM2_PolicyPassword	**NA**	-	
73	TPM2_PolicyGetDigest	**NA**	W : 28 C: 28	
74	TPM2_PolicyNvWritten	**NA**	-	
Hierarchy commands				

Services		Role	Keys and CSP access W = write, O = output, Z = zeroize C = used as key in cryptographic operation R = read (and not used as C)	Authorized in limited approved mode
75	TPM2_CreatePrimary	**CO**	R : 13, 14, 15, 16, 18, 42, 43 W : 20, 21, 22, 23, 28, 38, 47, 48 C : 1, 2, 3, 4, 17, 19, 20, 21, 22, 27, 28, 38, 42, 43, 48 Z : 47	
76	TPM2_HierarchyControl	**CO**	C : 9, 10, 11, 27	
77	TPM2_SetPrimaryPolicy	**CO**	W : 13, 14, 15, 16, 28 C : 9, 10, 11, 12, 27, 28	
78	TPM2_ChangePPS	**CO**	Z : 2, 6, 13,14, 17, 18, 20, 23, 43	
79	TPM2_ChangeEPS	**CO**	Z : 3, 7, 10, 14, 17, 18, 20, 23, 42	
80	TPM2_Clear	**CO**	R : 13, 16 W : 38, 48 Z : 4, 7, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 20, 23, 24, 25, 38, 48 C : 38	
81	TPM2_ClearControl	**CO**	R : 13, 16 W : 38, 48 C : 9, 12, 38, 48	
82	TPM2_HierarchyChangeAuth	**CO**	R : 13, 16 W : 9, 10, 11, 12, 28, 38, 48 C : 9, 10, 11, 12, 28, 38, 48	
Non-Volatile Storage				
83	TPM2_DictionaryAttackLockReset	**CO**	R : 16 W : 38, 48 C : 12, 38, 48	
84	TPM2_DictionaryAttackParameters	**CO**	R : 16 W : 38, 48 C : 12, 38, 48	
Field Upgrade				
86	TPM2_FieldUpgradeStart	**CO**	W : 28 C : 9, 13, 28, 44	
87	TPM2_FieldUpgradeData	**NA**	**-**	
Context Management				
88	TPM2_ContextSave	**NA**	W : 30 C : 29, 30	
89	TPM2_ContextLoad	**NA**	W : 30 C : 29, 30	
90	TPM2_FlushContext	**NA**	Z : 17, 18, 20, 23, 27, 28	X
91	TPM2_EvictControl	**CO**	R : 13, 15 C : 9, 11	
Clock and Timers				
92	TPM2_ReadClock	**NA**	**-**	X
93	TPM2_ClockSet	**CO**	R : 13, 15 C : 9, 11	

Services		Role	**Keys and CSP access** W = write, O = output, Z = zeroize C = used as key in cryptographic operation R = read (and not used as C)	**Authorized in limited approved mode**
94	TPM2_ClockRateAdjust	**CO**	R : 13, 15 C : 9, 11	
Capability Commands				
95	TPM2_GetCapability	**NA**	**-**	X
96	TPM2_TestParms	**NA**	**-**	X
Non-volatile storage				
97	TPM2_NV_DefineSpace	**CO**	R : 13, 15, 18 W : 24, 25, 28, 38, 48 C : 9, 11, 27, 28, 38, 48	
98	TPM2_NV_UndefineSpace	**CO**	W : 38, 48 C : 27, 38, 48 Z : 24, 25	
99	TPM2_NV_UndefineSpaceSpecial	**CO, A**	W : 38, 48 C : 27, 38, 48 Z : 24, 25	
100	TPM2_NV_ReadPublic	**NA**	C: 28	X
101	TPM2_NV_Write	**U**	W : 28, 38, 48 R : 25 C : 27, 28, 38, 48	
102	TPM2_NV_Increment	**U**	W : 38, 48 R : 25 C : 27, 38, 48	
103	TPM2_NV_Extend	**U**	W : 28, 38, 48 R : 25 C : 27, 28, 38, 48	
104	TPM2_NV_SetBits	**U**	W : 38, 48 R : 25 C : 27, 38, 48	
105	TPM2_NV_WriteLock	**U**	W : 38, 48 R : 25 C : 27, 38, 48	
106	TPM2_NV_GlobalWriteLock	**CO**	W : 38, 48 C : 27, 38, 48	
107	TPM2_NV_Read	**U**	W : 28, 38, 48 R : 25 C : 27, 28, 38, 48	
108	TPM2_NV_ReadLock	**U**	W : 38, 48 R : 25 C : 27, 38, 48	
109	TPM2_NV_ChangeAuth	**A**	W : 24, 28, 38, 48 C : 27, 28, 38, 48	
110	TPM2_NV_Certify	**U**	W : 28, 38, 48 R : 25 C : 27, 28, 38, 48	

Services		Role	**Keys and CSP access** W = write, O = output, Z = zeroize C = used as key in cryptographic operation R = read (and not used as C)	Authorized in limited approved mode
Proprietary commands				
111	TPM2_SetMode	**CO**	W : 28, 38, 48 C : 27, 28, 38, 48	
112	TPM2_SetCommandSet	**CO**	W : 28, 38, 48 C : 27, 28, 38, 48	
113	TPM2_RestoreEK	**CO**	Z : 3, 7, 10, 14, 17, 18, 20 R : 42, 43 W : 23, 28, 38, 48 C : 27, 28, 38, 48	
114	TPM2_SetCommandSetLock	**CO**	W : 28, 38, 48 C : 27, 28, 38, 48	
Misc commands				
115	TPM2_PP_Commands	**CO**	**-**	
Non FIPS services				
116	Field upgrade de-obfuscation[1]	**NA**	**-**	

3.2.2 *Authorization*

Some of the services listed above manipulate CSPs without requiring the operator to assume an authorized role:

- Services restricted to use of SHS:

  TPM2_Hash, TPM2_HashSequenceStart

- Services using DRNG (read, state update without manipulation):

  TPM2_GetRandom, TPM2_StirRandom

- Services used for authentication mechanism:

  TPM2_StartAuthSession, TPM2_PolicySigned, TPM2_PolicyTicket, TPM2_PolicyPCR, TPM2_PolicyCounterTimer TPM2_PolicyLocality, TPM2_PolicyCpHash, TPM2_PolicyNameHash, TPM2_PolicyAuthorize, TPM2_PolicyAuthorize, TPM2_PolicyDuplicationSelect, TPM2_PolicyGetDigest

- Services using (read, cryptographic operation) only public part of objects:

  TPM2_ReadPublic, TPM2_RSA_Encrypt, TPM2_NV_ReadPublic

- Specific services that do not affect security of the module:

  TPM2_LoadExternal: loaded object not considered as protected object (specific attribute).

  TPM2_MakeCredential: convenience function that do not use TPM secrets.

  TPM2_ECDH_KeyGen: ephemeral ECC key generation

  TPM2_EC_Ephemeral: ephemeral ECC key generation

[1] This service is not callable from TPM interface but is only used internally by TPM2_FieldUpgradeData command. It consists of de-obfuscating data received by the TPM2_FieldUpgradeData command with a non-FIPS approved algorithm.

	TPM2_FieldUpgradeData: transport command for field upgrade. Can be used only if TPM2_FieldUpgradeStart command has been successfully executed (authorized command) TPM2_ContextSave: save objects under an encrypted and integrity protected format TPM2_ContextLoad: load encrypted and integrity protected objects into TPM TPM2_FlushContext: flush loaded object/session from TPM volatile memory

3.3 Key management

3.3.1 Key entry and output

Next table indicates the approved method used to encrypt all secret, private keys and data (indicated by S for secret value, P for private key and D for user defined data in type column), entered into or output from the cryptographic module.

Table 15 : Encrypted methods for secret and private keys input

Service	Parameter name	Type	Input or output	Encryption algorithm
TPM2_ActivateCredential	credentialBlob	S	Input	AES CFB
	secret	S	Input	RSA OAEP or ECDH
TPM2_ContextSave	context	D	Output	AES CFB
TPM2_ContextLoad	context	D	Input	AES CFB
TPM2_Create	inSensitive	P / S	Input	AES CFB (*)
	outPrivate	P / S	Output	AES CFB
TPM2_CreatePrimary	inSensitive	P / S	Input	AES CFB (*)
TPM2_Duplicate	encryptionKeyIn (if present)	S	Input	AES CFB (*)
	encryptionKeyOut	S	Output	AES CFB (*)
	duplicate	S	Output	AES CFB
	outSymSeed	S	Output	RSA OAEP or ECDH
TPM2_EventSequenceComplete	buffer	D	Input	AES CFB (*)
TPM2_GetRandom	randomBytes	D	Output	AES CFB (**)
TPM2_Hash	data	D	Input	AES CFB (*)
TPM2_HashSequenceStart	auth	S	Input	AES CFB (*)
TPM2_HierarchyChangeAuth	newAuth	S	Input	AES CFB (*)
TPM2_HMAC	buffer	D	Input	AES CFB (*)
TPM2_HMACStart	auth	S	Input	AES CFB (*)
TPM2_Import	encryptionKeyIn (if present)	S	Input	AES CFB (*)
	duplicate	S	Input	AES CFB
	inSymSeed	S	Input	RSA OAEP or ECDH
	outPrivate	S	Output	AES CFB
TPM2_Load	inPrivate	P / S	Input	AES CFB
TPM2_LoadExternal	inPrivate	P / S	Input	AES CFB (*)
TPM2_MakeCredential	credentialBlob	S	Output	AES CFB
	secret	S	Output	RSA OAEP or ECDH
TPM2_NV_ChangeAuth	newAuth	S	Input	AES CFB (*)
TPM2_NV_DefineSpace	auth	S	Input	AES CFB (*)
TPM2_NV_Extend	data	D	Input	AES CFB (*)
TPM2_NV_Read	data	D	Output	AES CFB (**)

TPM2_NV_Write	data	D	Input	AES CFB (*)
TPM2_ObjectChangeAuth	newAuth	S	Input	AES CFB (*)
	outPrivate	S	Output	AES CFB
TPM2_PCR_Event	eventData	D	Input	AES CFB (*)
TPM2_Rewrap	inDuplicate	S	Input	AES CFB
	inSymSeed	S	Input	RSA OAEP or ECDH
	outDuplicate	S	Output	AES CFB
	outSymSeed	S	Output	RSA OAEP or ECDH
TPM2_RSA_Decrypt	message	D	Output	AES CFB (**)
TPM2_RSA_Encrypt	message	D	Input	AES CFB (*)
TPM2_SequenceComplete	buffer	D	Input	AES CFB (*)
TPM2_SequenceUpdate	buffer	D	Input	AES CFB (*)
TPM2_SetPrimaryPolicy	authPolicy	S	Input	AES CFB (*)
TPM2_StirRandom	inData	D	Input	AES CFB (*)
TPM2_Unseal	outData	D	Output	AES CFB (**)
TPM2_EncryptDecrypt	outData	D	Output	AES CFB (**)

(*): Parameter decryption is ensured by use of a decryption session (attribute DECRYPT set)

(**): Parameter encryption is ensured by use of an encryption session (attribute ENCRYPT set). This is mandatory if output data is a CSP.

3.3.2 Key transport

Relative security strength has been calculated for each cryptographic algorithm supported by the module and used for key transport. TPM FW prevents use of key in a transport scheme with lower strength than the transported key.

Table 16: Cryptographic Functions

Algorithm	**Comparable number of bits of security**
RSA OAEP (2048 bits)	112
ECDH (P-224 curve)	112
ECDH (P-256 curve)	128
AES CFB (128 bits)[1]	128
AES CFB (256 bits)[2]	256

[1] AES is used in conjunction with HMAC approved authentication method (**[SP800-38F]** compliant)
[2] AES is used in conjunction with HMAC approved authentication method (**[SP800-38F]** compliant)

4 SELF-TESTS

Self-tests run by the cryptographic module are split in three categories:

- Power-up self-tests
- Full self-tests
- Conditional self-tests

The power-on self-tests do not require operator intervention in order to run. Power-on self-tests execution completes all tests except KATs on asymmetric algorithms (RSA, ECDSA, ECDH). Completion of power-on self-tests allows the TPM to be in a limited approved mode allowing to process only a subset of TPM commands (see §1.7.2.1).

To switch from limited approved mode to full approved mode, operator shall execute TPM_SelfTestFull command. This command requests the module to switch mode by executing all self-tests listed in Table 18 : Asymmetric cryptography self-tests list (power-up self-tests plus the remaining self-tests, that mainly concern asymmetric cryptography).

The security module outputs an "error" Return Code via the status interface when the error state is entered due to a failed self-test. While in error state, security module does not perform any cryptographic functions and all data output via the data output interface are inhibited.

If power-on self-tests have passed successfully, no status is indicated but commands that require self-tests to be completed can be successfully executed.

4.1 Power-up tests list

Table 17 : Power-up self-tests list

Algorithm tested	Test description
SHA1	SHA1 computation on known data (16 bytes) and comparison of output to the expected digest (20 bytes)
SHA256	SHA256 computation on known data (16 bytes) and comparison of output to the expected digest (32 bytes)
HMAC SHA256	HMAC-SHA256 computation on known data (16 bytes) / known key (16 bytes, same value as data) and comparison of output to the expected MAC (32 bytes). Self-test allows validating the secure SHA algorithm also used in standalone (out of HMAC context).
KDF SP800-108	KDF (based on SHA1) computation on known data (16 bytes) / known label ("TEST") and comparison of output to the expected value (32 bytes).
Hash-DRBG	Instantiate, Generate and Reseed API are tested in a single test sequence in accordance with §11.3 of **[SP800-90A]**. Output of HDRBG (55 bytes) is compared to a reference value.
AES	AES CFB encryption is done on known data (32 bytes) / known key (16 bytes) and known IV (16 bytes, same value as key). The 32 bytes output data are compared to the expected reference data. If comparison succeeds, AES CFB decryption is done on encrypted data with same key & same IV as encryption. 32 bytes output are compared to the initial plaintext data.
Triple-DES	Triple-DES CFB encryption is done on known data (32 bytes) / known key (24 bytes) and known IV (8 bytes). The 32 bytes output data are compared to the expected reference data. If comparison succeeds, Triple-DES CFB decryption is done on encrypted data with same key & same IV as encryption. 32 bytes output are compared to the initial plaintext data.

FW integrity	FW integrity is verified by computing an EDC (CRC-16 ISO 13239) and comparing it to reference values. FW integrity is verified during boot sequence before execution of one of the code block (CML, AFL and TPM) and during full self-tests execution. If failure is detected during boot sequence, TPM enters an infinite reset loop that can be exit only by power-off/power-on sequence. In failure is detected during self-tests, status is set to FAIL and error is returned.
HW integrity	HW integrity is guaranteed via check of HW sensors. If failure is detected during boot sequence, status is set to FAIL and error is returned.

4.2 Asymmetric cryptography self-tests list

Table 18 : Asymmetric cryptography self-tests list

Algorithm tested	Test description
RSA	A known key is loaded (2048 bits length). Signature RSASSA-PKCS1-v1_5 is generated on known data (20 bytes). Output of signature is compared to a reference signature. Signature verification is performed on the generated signature.
ECDH	A known private key d (32 bytes length) is used with a known point P of NIST P-256 curve to compute P = dQ. Q is compare to known reference point.
ECDSA	A known private key (256 bits) is used to generate ECDSA signature based on NIST P-256 curve. Output of signature is compared to a reference signature. Signature verification is performed on the generated signature.

4.3 Conditional tests list

Table 19 : TPM conditional tests

Algorithm tested	Test description
FW integrity	FW integrity is verified by computing an EDC (CRC-16 ISO 13239) and comparing it to reference values.
Hash-DRBG	Each 32 bytes of generated data are compared to the previous generated data. If data are equal, status is set to FAIL and error is returned.
NDRNG	TPM performs AIS31 statistical test verification on NDRNG output and continuous HW self-tests (AS09.42) on NDRNG 48-bits output sequence. If test fails, TRNG_ERR bit is raised in SEC_STAT register. Status is set to FAIL and error is returned.
FW load	During field upgrade procedure, several checks are performed before authorizing the FW to be upgraded: - Verification of signature (RSASSA-PSS) on the first data blob to ensure authentication of the FW - Verification of digest (SHA256) on each subsequent blob to guarantee integrity of the full FW.
RSA **key generation**	A new RSA key is generated or retrieved from pre-computed keys (done in BKG). Depending on the key purpose (signing or encrypting) indicated in sign attribute of the key, en/decryption or signing/verification is done on known data (16 bytes).
ECC key generation	On each ECC key generation, an ECDSA signature is generated and verified on curve NIST P-256.

4.4 Verification

Successful completion of self-tests can be verified through use of TPM2_GetTestResult command. The first 4 bytes of response indicate self-tests status. If they are equal to 0, self-tests completed successfully. If not, the subsequent 4 bytes indicate the list of algorithms not fully self-tested.

5 PHYSICAL SECURITY POLICY

The security module meets Physical Security protection requirements for FIPS level 2. CSPs are physically protected from unexpected disclosure and modification. Security module is tamper evident, encapsulated in an opaque package. Regular visual inspection must be conducted by user to check that HW integrity of the chip has not been damaged. Some physical security protection mechanisms beyond the requirements for level 2 have been implemented and are described in “Mitigations of other attacks”.

Normal operating ranges are defined in the respective TOE datasheet **[ST33TPHF2ESPI DS]**:

- **Temperature:**

  The normal operating temperature range of the security module is -40°C to +105°C.

- **Voltage:**

  The normal operating voltage range of the security module is 1.8V or 3.3V (±10%).

- **Frequency:**

  The internal system clock is created by an internal oscillator.

Operation outside these ranges is not guaranteed, but physical security mechanisms are implemented to assure that CSPs remain protected from unauthorized disclosure, usage, modification or deletion.

6 OPERATIONAL ENVIRONMENT

Module operational environment is “limited modifiable” because TPM FW can only be modified through field upgrade service (use of TPM2_FieldUpgradeStart and TPM2_FieldUpgradeData commands). The Non-upgradable code blocks are non-modifiable.

FIPS 140-2 level 1 & 2 operational environment requirements of **[FIPS 140-2]** section 4.6.1 are then not applicable to the security module.

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 the scope of this validation and require a separate FIPS 140-2 validation.

7 MITIGATIONS OF OTHER ATTACKS

The security module meets Physical Security protection requirements for FIPS level 2.

7.1 Internal Tamper Detection

The security module contains an active metal shield that covers the internal TPM circuitry and memory components. Cutting, removing or modifying the shield layer will cause the TPM to Reset and enter a SHUTDOWN mode.

7.2 Environmental protection

The security module contains circuitry which will detect environmental conditions outside the range described in the product datasheet. Power supply voltage is continuously monitored. If conditions exist outside the range determined by the TPM tamper detection circuitry, the chip will reset and will enter a FAILURE mode. The chip will remain Reset and in FAIL mode as long as the environmental condition causing the tamper event persists.

8 REFERENCES

Reference	Document
[ST33TPHF2ESPI DS]	ST33TPHF2ESPI Datasheet, STMicroelectronics, December 2015
[TPM2.0 Part1 r1.16]	TPM2.0 Main, Part 1, Architecture, rev 1.16, TCG
[TPM2.0 Part2 r1.16]	TPM2.0 Main, Part 2, Structures, rev 1.16, TCG
[TPM2.0 Part3 r1.16]	TPM2.0 Main, Part 3, Commands, rev 1.16, TCG
[TPM2.0 Part4 r1.16]	TPM2.0 Main, Part 4, Supporting routines, rev 1.16, TCG
[PTP 0.43]	TCG PC Client Platform TPM Profile (PTP) Specification, rev. 00.43 with errata
[FIPS 140-2]	FIPS PUB 140-2, Security Requirements for Cryptographic Modules / National Institute of Standards and Technology (NIST), CHANGE NOTICES (12-03-2002)
[FIPS DTR]	National Institute of Standards and Technology and Communications Security, *Derived Test Requirements(DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*
[FIPS IG]	National Institute of Standards and Technology and Communications Security, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[FIPS 180-4]	National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-4, March 2012
[FIPS 186-4]	National Institute of Standards and Technology, *Digital Signature Standard (DSS),* Federal Information Processing Standards Publication 186-4, July 2013
[FIPS 197]	National Institute of Standards and Technology, *Advanced Encryption Standard (AES),* Federal Information Processing Standards Publication 197, November 2001
[SP800-135]	National Institute of Standards and Technology, *Existing Application-Specific Key Derivation Function Validation System*, September 2015.
[SP800-108]	National Institute of Standards and Technology, *Recommendation for Key Derivation Using Pseudorandom Functions*, October 2009.
[SP800-131A]	National Institute of Standards and Technology, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, 11/06/15.
[FIPS 198-1]	National Institute of Standards and Technology, *The Keyed-Hash Message Authentication Code,* NIST Computer Security Division Page 3 07/26/2011, *(HMAC)*, Federal Information Processing Standards Publication 198-1, July, 2008

Reference	Document
[SP800-90A]	National Institute of Standards and Technology, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, January 2012.
[SP800-38F]	National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* December 2012.
[SP800-56A]	National Institute of Standards and Technology, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography,* March 2007.
[FIPS 140-2 TPM]	TCG FIPS 140-2 Guidance for TPM2.0, v1.0, TCG

9 ACRONYMS

Term	Definition
AES	Advanced Encryption Standard
CO	Crypto Officer
DES	Data Encryption Standard
DSAP	Delegate Specific Authorization Protocol
EK	Endorsement Key
FIPS	Federal Information Processing Standard
FUM	Field Upgrade Mode
GPIO	General Purpose I/O
HMAC	Keyed-Hashing for Message Authentication
NIST	National Institute of Standards and Technology
NV	Non-volatile (memory)
OIAP	Object-Independent Authorization Protocol
OSAP	Object Specific Authorization Protocol
PCR	Platform Configuration Register
RSA	Rivest Shamir Adelman
RTM	Root of Trust for Measurement
RTR	Root of Trust for Reporting
SHA	Secure Hash Algorithm
SPI	Serial Peripheral Interface
SRK	Storage Root Key
TCG	Trusted Computed Group
TPM	Trusted Platform Module
TSS	TPM Software Stack