



## STMICROELECTRONICS

### Trusted Platform Module ST33TPHF20SPI & ST33TPHF20I2C

ST33HTPH2E28AAF0 / ST33HTPH2E32AAF0 /  
ST33HTPH2E28AAF1 / ST33HTPH2E32AAF1 /  
ST33HTPH2028AAF3 / ST33HTPH2032AAF3 /  
ST33HTPH2E28AHB3 / ST33HTPH2E32AHB3 /  
ST33HTPH2E28AHB4 / ST33HTPH2E32AHB4 /  
ST33HTPH2E28AHB7 / ST33HTPH2E32AHB7 /  
ST33HTPH2E28AHB8 / ST33HTPH2E32AHB8 /  
ST33HTPH2028AHB9 / ST33HTPH2032AHB9

### FIPS 140-2 Security Policy Level 2

**Firmware revision:** 49.00 / 4A.00 / 49.04 / 4A.04 /  
49.05 / 4A.05  
**HW version:** ST33HTPH revision A

Date: 2017/10/12  
Document Version: 02-02

NON-PROPRIETARY DOCUMENT

# Table of Contents

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>MODULE DESCRIPTION</b>                       | <b>3</b>  |
| 1.1      | DEFINITION                                      | 3         |
| 1.2      | MODULE IDENTIFICATION                           | 3         |
| 1.2.1    | AHB3 / AHB4                                     | 3         |
| 1.2.2    | AHB7 / AHB8                                     | 4         |
| 1.2.3    | AHB9  | 5         |
| 1.2.4    | AAF0 / AAF1                                     | 6         |
| 1.2.5    | AAF3  | 7         |
| 1.3      | PINOUT DESCRIPTION                              | 8         |
| 1.3.1    | SPI configuration                               | 8         |
| 1.3.2    | PC configuration                                | 10        |
| 1.4      | BLOCK DIAGRAMS                                  | 11        |
| 1.4.1    | HW block diagram                                | 11        |
| 1.4.2    | FW block diagrams                               | 12        |
| 1.5      | SECURITY LEVELS                                 | 14        |
| 1.6      | CRYPTOGRAPHIC FUNCTIONS                         | 15        |
| 1.7      | MODES OF OPERATION                              | 16        |
| 1.7.1    | Security module configuration                   | 17        |
| 1.7.2    | Approved modes of operation                     | 17        |
| 1.7.3    | FIPS mode recommendations                       | 18        |
| 1.7.4    | Limited and error modes                         | 19        |
| 1.8      | PORTS AND INTERFACES                            | 19        |
| <b>2</b> | <b>IDENTIFICATION AND AUTHENTICATION POLICY</b> | <b>21</b> |
| 2.1      | ROLES   | 21        |
| 2.2      | AUTHENTICATION                                  | 21        |
| 2.2.1    | Description                                     | 21        |
| 2.2.2    | Authorization strength                          | 22        |
| 2.2.3    | Authorization protection                        | 22        |
| <b>3</b> | <b>ACCESS CONTROL POLICY</b>                    | <b>23</b> |
| 3.1      | LIST OF KEYS AND CSPS                           | 23        |
| 3.2      | SERVICES  | 28        |
| 3.2.1    | Services list                                   | 28        |
| 3.2.2    | Authorization                                   | 34        |
| 3.3      | KEY MANAGEMENT                                  | 36        |
| 3.3.1    | Key entry and output                            | 36        |
| 3.3.2    | Key transport                                   | 37        |
| <b>4</b> | <b>SELF-TESTS</b>                               | <b>38</b> |
| 4.1      | POWER-UP TESTS LIST                             | 38        |
| 4.2      | ASYMMETRIC CRYPTOGRAPHY SELF-TESTS LIST         | 39        |
| 4.3      | CONDITIONAL TESTS LIST                          | 39        |
| 4.4      | VERIFICATION                                    | 40        |
| <b>5</b> | <b>PHYSICAL SECURITY POLICY</b>                 | <b>41</b> |
| <b>6</b> | <b>OPERATIONAL ENVIRONMENT</b>                  | <b>42</b> |
| <b>7</b> | <b>MITIGATIONS OF OTHER ATTACKS</b>             | <b>43</b> |
| 7.1      | INTERNAL TAMPER DETECTION                       | 43        |
| 7.2      | ENVIRONMENTAL PROTECTION                        | 43        |
| <b>8</b> | <b>REFERENCES</b>                               | <b>44</b> |
| <b>9</b> | <b>ACRONYMS</b>                                 | <b>46</b> |
|          | <b>IMPORTANT NOTICE – PLEASE READ CAREFULLY</b> | <b>47</b> |

# 1 MODULE DESCRIPTION

## 1.1 Definition

The ST33TPHF20SPI / ST33TPHF20I2C Trusted Platform Module are fully integrated security modules 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 and I<sup>2</sup>C interfaces 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 (SPI) / 4A.00 (SPI) / 49.04 (SPI) / 4A.04 (SPI) / 49.05 (I<sup>2</sup>C) / 4A.05 (I<sup>2</sup>C)

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 AHB3 / AHB4

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.

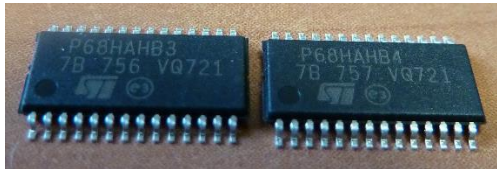
The current FIPS 140-2 level2 security policy applies to these security module configurations when the module is irreversibly locked in TPM2.0 mode (cf. §1.7.3 for mode lock recommendations). As a consequence the TPM FW version 1.2 is excluded from the security requirements of FIPS 140-2.

**Table 1: Security module configurations**

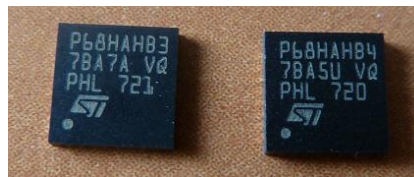
|                           | Module configuration                  |                      |                      |                      |
|---------------------------|---------------------------------------|----------------------|----------------------|----------------------|
| Product name / HW version | ST33TPHF2ESPI/<br>ST33HTPH revision A |                      |                      |                      |
| Package                   | TSSOP28                               | VQFN32               | TSSOP28              | VQFN32               |
| Part number               | ST33HTPH2E28<br>AHB3                  | ST33HTPH2E32<br>AHB3 | ST33HTPH2E28<br>AHB4 | ST33HTPH2E32<br>AHB4 |
| Default mode              | TPM1.2                                |                      | TPM2.0               |                      |
| Marking                   | P68HAHB3                              |                      | P68HAHB4             |                      |
| FW version                | 49.04                                 |                      |                      |                      |

P68HAHB3 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. P68HAHB4 corresponds to the module configured by default in TPM2.0 execution mode.

**Figure 1: Picture of the Cryptographic Module (TSSOP28) – Marking P68HAHB3 & P68HAHB4**



**Figure 2: Picture of the Cryptographic Module (VQFN32) – Marking P68HAHB3 & P68HAHB4**



1.2.2 AHB7 / AHB8

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.

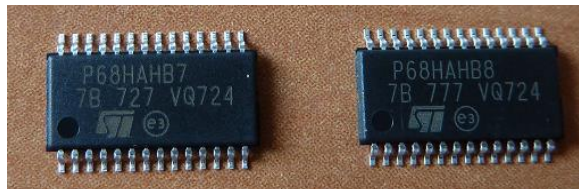
**Table 2: Security module configurations**

|                           | Module configuration                  |                      |                      |                      |
|---------------------------|---------------------------------------|----------------------|----------------------|----------------------|
| Product name / HW version | ST33TPHF2EI2C/<br>ST33HTPH revision A |                      |                      |                      |
| Package                   | TSSOP28                               | VQFN32               | TSSOP28              | VQFN32               |
| Part number               | ST33HTPH2E28<br>AHB7                  | ST33HTPH2E32<br>AHB7 | ST33HTPH2E28<br>AHB8 | ST33HTPH2E32<br>AHB8 |
| Default mode              | TPM1.2                                |                      | TPM2.0               |                      |

|                   |          |          |
|-------------------|----------|----------|
| <b>Marking</b>    | P68HAHB7 | P68HAHB8 |
| <b>FW version</b> | 49.05    |          |

P68HAHB7 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. P68HAHB8 corresponds to the module configured by default in TPM2.0 execution mode.

**Figure 3: Picture of the Cryptographic Module (TSSOP28) – Marking P68HAHB7 & P68HAHB8**



**Figure 4: Picture of the Cryptographic Module (VQFN32) – Marking P68HAHB7 & P68HAHB8**



### 1.2.3 AHB9

This configuration 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 this security module configuration.

**Table 3: Security module configuration**

|                                  | Module configuration                  |                  |
|----------------------------------|---------------------------------------|------------------|
| <b>Product name / HW version</b> | ST33TPHF20I2C/<br>ST33HTPH revision A |                  |
| <b>Package</b>                   | TSSOP28                               | VQFN32           |
| <b>Part number</b>               | ST33HTPH2028AHB9                      | ST33HTPH2032AHB9 |
| <b>Marking</b>                   | P68HAHB9                              |                  |
| <b>FW version</b>                | 4A.05                                 |                  |

**Figure 5: Picture of the Cryptographic Module (TSSOP28) – Marking P68HAHB9**



**Figure 6: Picture of the Cryptographic Module (VQFN32) – Marking P68HAHB9**



1.2.4 AAF0 / AAF1

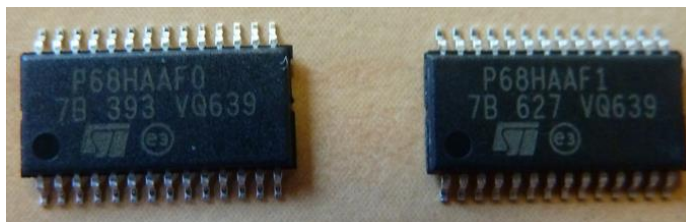
These configurations of the security module implement both version 1.2 and version 2.0 of the Trusted Computing Group (TCG) specification for Trusted Platform Modules (TPM). Versions are exclusive and security module manufactured will operate in a default mode (TPM1.2 or TPM2.0) depending on the configuration.

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 4: Security module configurations**

|                                  |                                       | Module configuration |                      |                      |  |
|----------------------------------|---------------------------------------|----------------------|----------------------|----------------------|--|
| <b>Product name / HW version</b> | ST33TPHF2ESPI/<br>ST33HTPH revision A |                      |                      |                      |  |
| <b>Package</b>                   | TSSOP28                               | VQFN32               | TSSOP28              | VQFN32               |  |
| <b>Part number</b>               | ST33HTPH2E28<br>AAF0                  | ST33HTPH2E32<br>AAF0 | ST33HTPH2E28<br>AAF1 | ST33HTPH2E32<br>AAF1 |  |
| <b>Default mode</b>              | TPM1.2                                |                      | TPM2.0               |                      |  |
| <b>Marking</b>                   | P68HAAF0                              |                      | P68HAAF1             |                      |  |
| <b>FW version</b>                | 49.00 / 49.04 <sup>1</sup>            |                      |                      |                      |  |

**Figure 7: Picture of the Cryptographic Module (TSSOP28) – Marking**



**Figure 8: 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.

<sup>1</sup> The default FW version of this configuration is 49.00. To operate with FW version 49.04, module FW must be first field upgraded from 49.00 to 49.04.

1.2.5 AAF3

This configuration 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 this security module configuration.

**Table 5: Security module configuration**

|                                  | Module configuration                  |                  |
|----------------------------------|---------------------------------------|------------------|
| <b>Product name / HW version</b> | ST33TPHF20SPI/<br>ST33HTPH revision A |                  |
| <b>Package</b>                   | TSSOP28                               | VQFN32           |
| <b>Part number</b>               | ST33HTPH2028AAF3                      | ST33HTPH2032AAF3 |
| <b>Marking</b>                   | P68HAAF3                              |                  |
| <b>FW version</b>                | 4A.00 / 4A.04 <sup>1</sup>            |                  |

**Figure 9: Picture of the Cryptographic Module (TSSOP28) – Marking**



**Figure 10: Picture of the Cryptographic Module (VQFN32) – Marking**



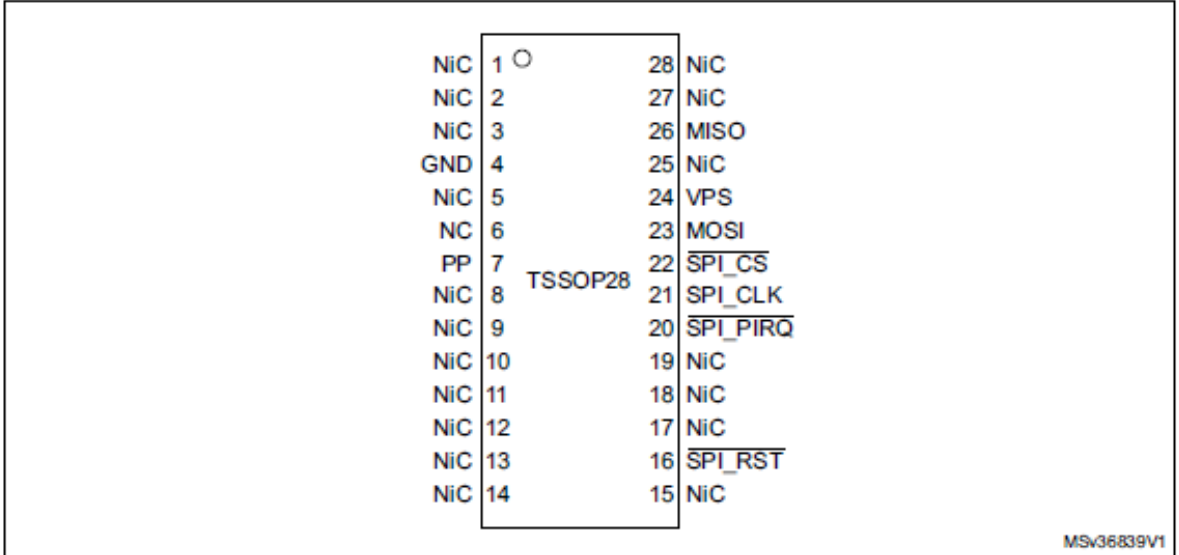
<sup>1</sup> The default FW version of this configuration is 4A.00. To operate with FW version 4A.04, module FW must be first field upgraded from 4A.00 to 4A.04

**1.3 Pinout description**

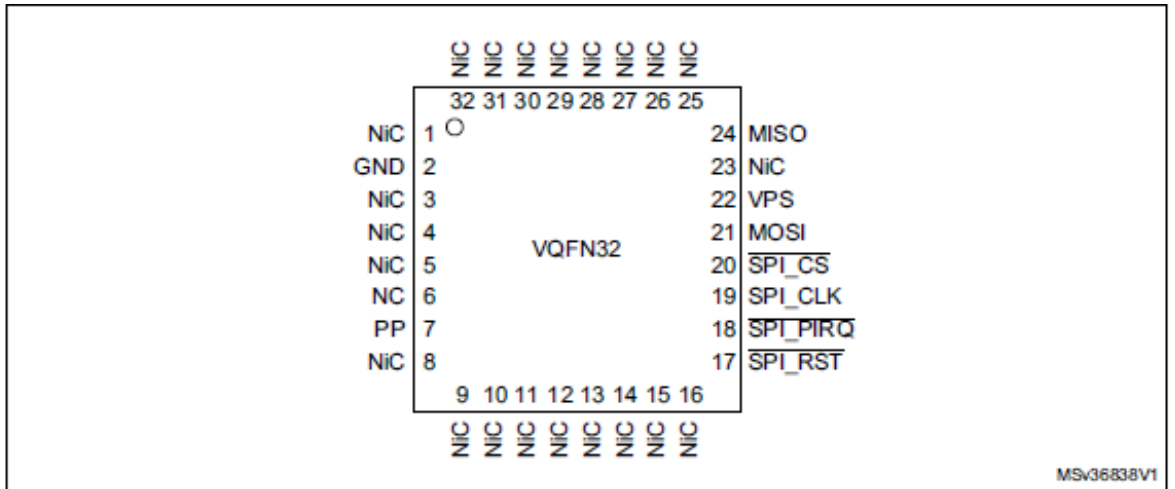
The pin layouts for the ST33TPHF20SPI are shown in Figure 11 and in Figure 12: VQFN32 Pinout Diagram. The pin layouts for the ST33TPHF20I2C are shown in Figure 13: TSSOP28 Pinout Diagram and Figure 14: VQFN32 Pinout Diagram.

**1.3.1 SPI configuration**

**Figure 11: TSSOP28 Pinout Diagram**



**Figure 12: VQFN32 Pinout Diagram**



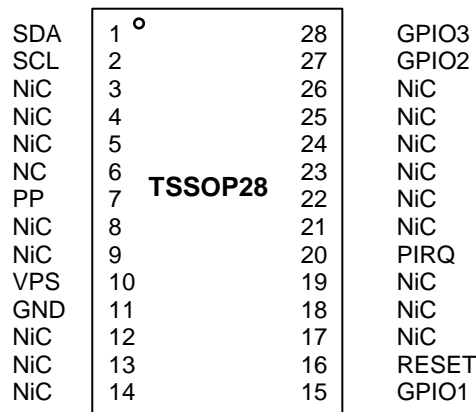


Next table gives a description of the products pins.

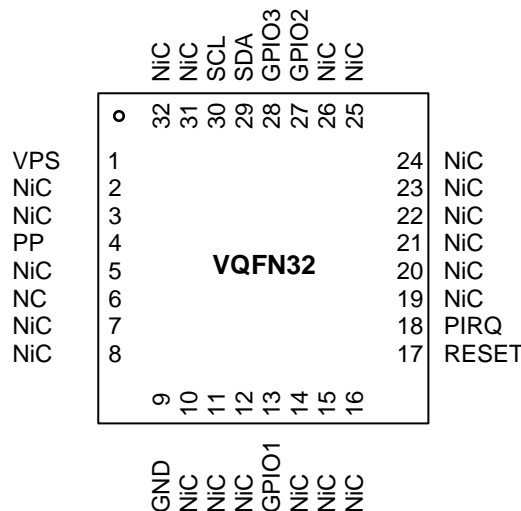
**Table 6: ST33TPHF20 Pin definition (SPI configuration)**

| Signal                        | Type   | Description   |
|-------------------------------|--------|---|
| VPS                           | Input  | <b>Power supply.</b> 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  | <b>SPI Reset</b> used to re-initialize the device   |
| MISO                          | Output | <b>SPI Master Input, Slave Output</b> (output from slave)   |
| MOSI                          | Input  | <b>SPI Master Output, Slave Input</b> (output from master)  |
| SPI_CLK                       | Input  | <b>SPI</b> serial clock (output from master)  |
| $\overline{\text{SPI\_CS}}$   | Input  | <b>SPI</b> slave select (active low; output from master)  |
| $\overline{\text{SPI\_PIRQ}}$ | Output | <b>SPI IRQ</b> used by TPM to generate an interrupt   |
| PP                            | Input  | <b>Physical presence</b> , active high, internal pull-down. Used to indicate Physical Presence to the TPM.            |
| NiC                           | -      | <b>Not internally connected:</b> not connected to the die. May be left unconnected but no impact on TPM if connected. |
| NC                            | -      | <b>Not Connected:</b> connected to the die but not usable. May be left unconnected. Internal pull-down.               |

**Figure 13: TSSOP28 Pinout Diagram**



**Figure 14: VQFN32 Pinout Diagram**



Next table gives a description of the products pins.

**Table 7: ST33TPHF20 Pin definition (I<sup>2</sup>C configuration)**

| Signal | Type         | Description   |
|--------|--------------|---|
| VPS    | Input        | <b>Power supply.</b> 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.   |
| RESET  | Input        | Reset used to re-initialize the device  |
| SCL    | Input        | I <sup>2</sup> C serial clock (Open drain with no weak pull-up resistor)  |
| SDA    | Input/Output | I <sup>2</sup> C serial data (Open drain with no weak pull-up resistor)   |
| PIRQ   | Output       | IRQ used by TPM to generate an interrupt  |
| GPIO1  | Input/Output | GPIO default to low (not used, reserved for future use)   |
| GPIO2  | Input/Output | GPIO default to low (not used, reserved for future use)   |
| GPIO3  | Input/Output | GPIO default to low (not used, reserved for future use)   |
| PP     | Input        | <b>Physical presence</b> , active high, internal pull-down. Used to indicate Physical Presence to the TPM.            |
| NiC    | -            | <b>Not internally connected:</b> not connected to the die. May be left unconnected but no impact on TPM if connected. |
| NC     | -            | <b>Not Connected:</b> connected to the die but not usable. May be left unconnected. Internal pull-down.               |

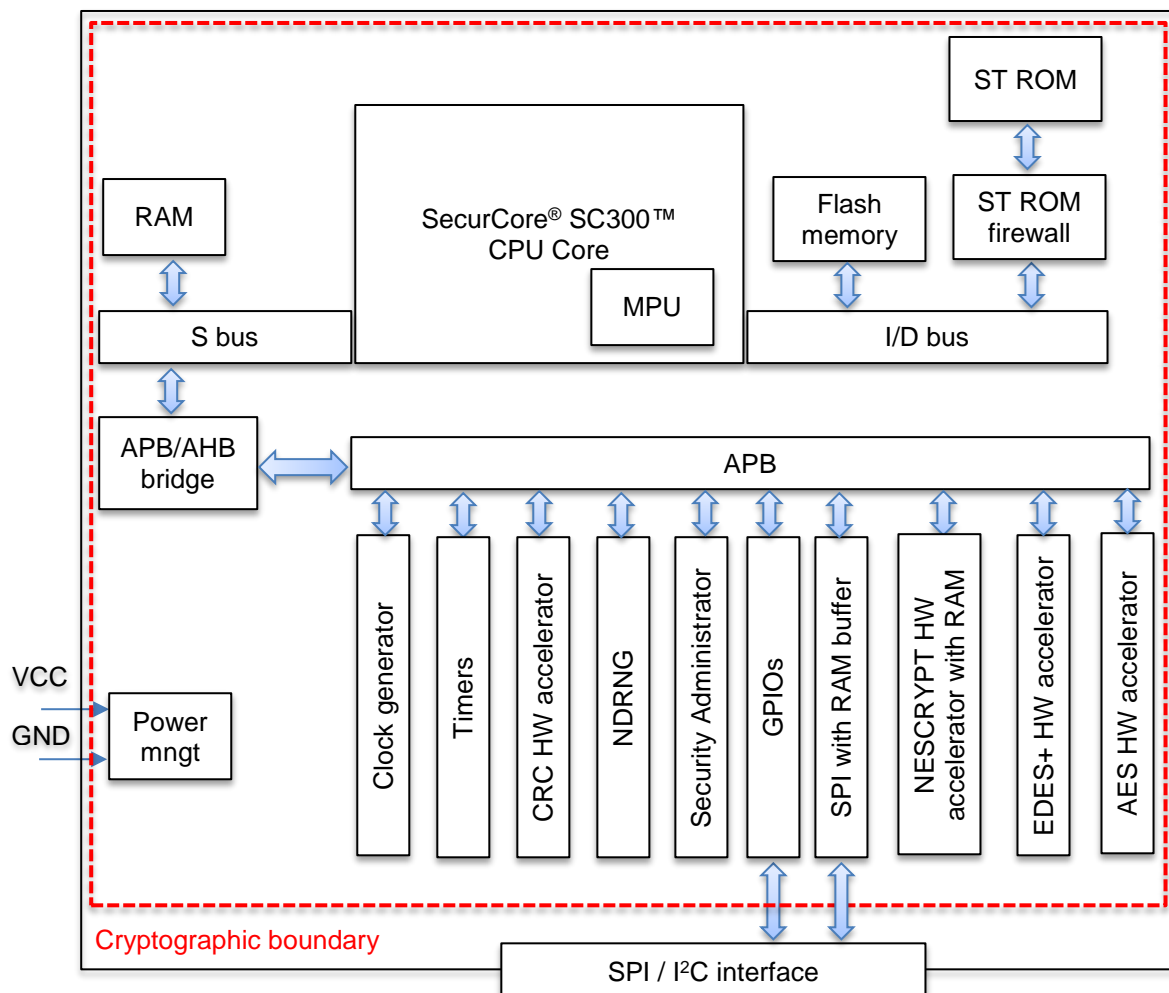
## 1.4 Block diagrams

### 1.4.1 HW block diagram

A block diagram of the hardware ST33HTPH (with its associated cryptographic boundary) is provided in Figure 15. 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 15: ST33HTPH block diagram**

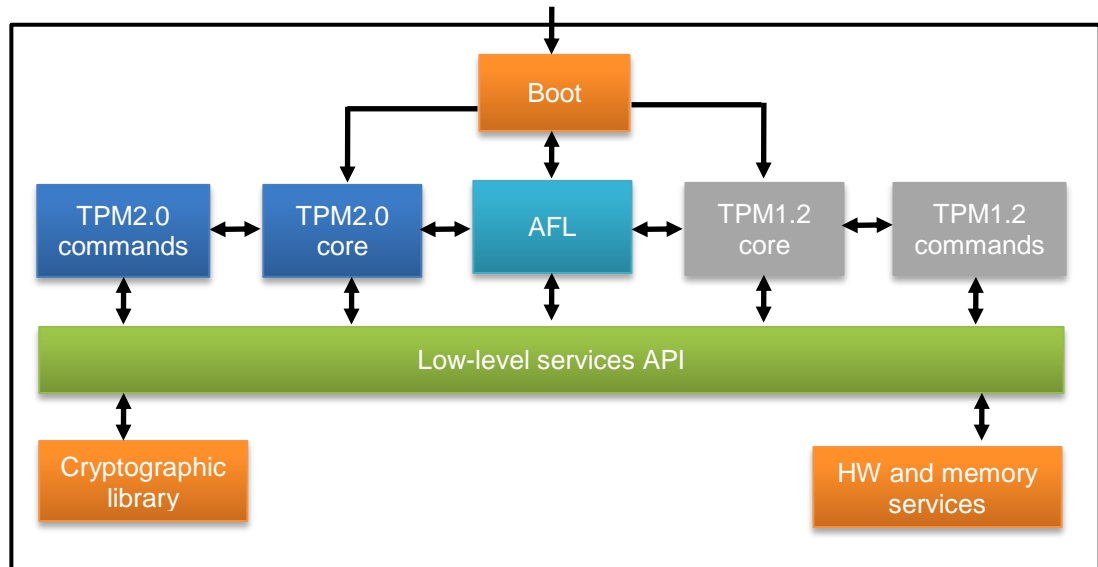


## 1.4.2 *FW block diagrams*

Block diagrams of the TPM FW are provided at Figure 16: TPM FW block diagram (TPM2E) and Figure 17: TPM FW block diagram.

### 1.4.2.1 *AAF0 / AAF1 / AHB3 / AHB4 / AHB7 / AHB8*

Figure 16: TPM FW block diagram (TPM2E)

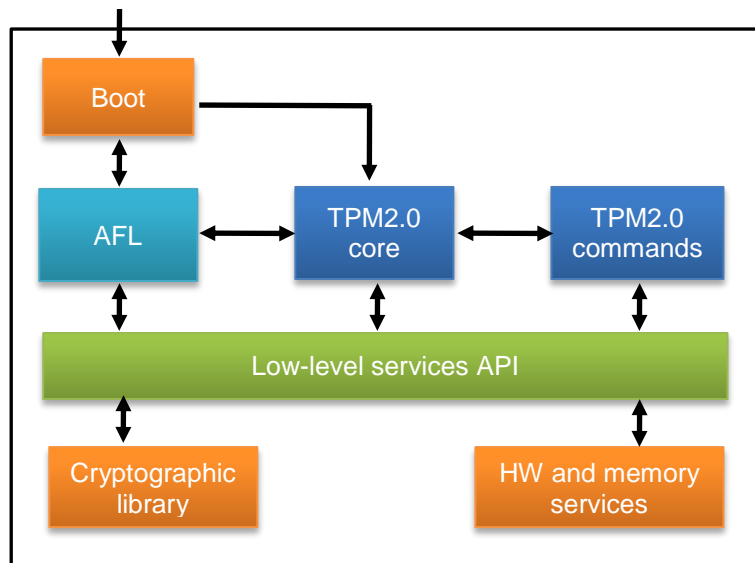


TPM FW is composed of:

- 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 / AHB9

Figure 17: 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 8: Module Security Level Specification**

| <b>Security Requirements Section</b>      | <b>Level</b> |
|---|--------------|
| 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            |
| <b>Overall</b>                            | <b>2</b>     |

## 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 9: 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 & 3118 & 3120 & 3122 & 3124 | HMAC (single call)   | FIPS 198-1            | SHA-1, SHA-256                               | 160, 256                      | Message authentication              |
| 2878 & 2876 & 3119 & 3121 & 3123 & 3125 | HMAC (sequence)  | FIPS 198-1            | SHA-1, SHA-256                               | 160, 256                      | Message authentication              |
| 123 & 121 & 146 & 147 & 148 & 149       | 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)<br><br>KTS (AES cert #4338 + HMAC cert #3118)<br><br>KTS (AES cert #4338 + HMAC cert #3120) | SP 800-38F            | CFB  | 128, 256                      | Key transport                       |

|                           |  |                         |                               |  |                             |
|---------------------------|--|-------------------------|-------------------------------|--|-----------------------------|
|                           | KTS (AES cert #4336 + HMAC cert #2875)<br><br>KTS (AES cert #4336 + HMAC cert #3122)<br><br>KTS (AES cert #4336 + HMAC cert #3124) |                         |                               |  |                             |
| <b>3539</b>               | SHS  | FIPS 180-4              | SHA-1, SHA-256                |  | Message digest              |
| <b>Vendor affirmation</b> | CKG  | SP800-133 (per IG D.12) | Direct generation, Generation |  | Key generation <sup>1</sup> |

**Table 10: Allowed algorithms**

| Algorithm        | Caveat                 | Use   |
|------------------|------------------------|---|
| RSA              | Key length = 1024 bits | Digital signature verification  |
| RSA key wrapping | Key length = 2048 bits | Key establishment   |
| SHA-1            | NA                     | Digital signature verification  |
| NDRNG            | NA                     | Seed or reseed DRBG 800-90A (with approximately 366 bits of entropy). Generate random numbers not dedicated to be used as cryptographic material. |

**Table 11: 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 |
| ECDA                         | 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

<sup>1</sup> 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 17: Keys and CSPs list.



## 1.7.1 Security module configuration

### 1.7.1.1 **AAF0 / AHB3 / AHB7**

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 / AHB4 / AHB8**

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 / AHB9**

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 12: 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 18: 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 18: 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 13: 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.
- Limit number of encryptions with a same TDES key to a maximum of 2<sup>28</sup> encryptions.
- 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 17: 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 17: 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 TPM2\_GetCapability / TPM2\_GetTestResult. TPM answers to all other commands with a specific error code: 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: TPM2\_FieldUpgradeStart / TPM2\_FieldUpgradeData / TPM2\_GetCapability / TPM2\_GetTestResult / TPM2\_SelfTest. 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 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 or I<sup>2</sup>C Bus. The logical interfaces and their mapping to physical ports of the module are described below:

**Table 14 : Ports and interfaces**

| Logical interface       | Description   | Physical port  |
|-------------------------|---|--|
| Control Input Interface | Control Input commands issued to the security module              | <b>SPI</b> : $\overline{\text{SPI\_CS}}$ / SPI_CLK / MOSI / SPI_RST / PP<br><b>I<sup>2</sup>C</b> : SCL / SDA / RESET / PP |
| Status Output Interface | Status data output by the chip                                    | <b>SPI</b> : $\overline{\text{SPI\_CS}}$ / SPI_CLK / MISO / SPI_PIRQ<br><b>I<sup>2</sup>C</b> : SCL / SDA / PIRQ           |
| Data Input Interface    | Data provided to the chip as part of the data processing commands | <b>SPI</b> : $\overline{\text{SPI\_CS}}$ / SPI_CLK / MOSI<br><b>I<sup>2</sup>C</b> : SCL / SDA                             |
| Data Output Interface   | Data output by the chip as part of the data processing command    | <b>SPI</b> : $\overline{\text{SPI\_CS}}$ / SPI_CLK / MISO<br><b>I<sup>2</sup>C</b> : SCL / SDA                             |
| 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]<sup>1</sup>.
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\_EncryptDecryptTo 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 keyHowever 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.

---

<sup>1</sup> 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 15: 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 18: 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 18 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 16: DAM lockout durations**

|                                      |      |
|--------------------------------------|------|
| <b>Failed authentication counter</b> | >31  |
| <b>Lockout period (in seconds)</b>   | 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\_DictionaryAttackParameters 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 18, 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 17: Keys and CSPs list**

| Keys/CSPs          |                 | Description  | Zeroized                     |
|--------------------|-----------------|--|------------------------------|
| Index              | Name            |  |                              |
| <b>Hierarchies</b> |                 |  |                              |
| 1                  | nullSeed        | 32 bytes primary seed values resp. for NULL, platform, endorsement and storage hierarchies.<br>NullSeed is a random value generated by HDRBG at each TPM power-up.   | TPM reset                    |
| 2                  | ppSeed          | PpSeed / epSeed / spSeed are random values generated by HDRBG at first TPM power-up.   | TPM2_Change PPS              |
| 3                  | epSeed          | They are used as keys for:   | TPM2_Change EPS              |
| 4                  | spSeed          | <ul style="list-style-type: none"> <li>KDFa to derive seedValue and sensitive during object creation (cf. [TPM2.0 Part1 r1.16] §27.6.4)</li> <li>KDFa to generate a symmetric encryption key used in TPM2B_PRIVATE structure en/decryption.</li> <li>KDFa to generate HMAC key used in TPM2B_PRIVATE integrity protection generation or verification</li> </ul> They are used as seeds for: <ul style="list-style-type: none"> <li>DRBG to generate random as input to prime numbers (RSA) and private key generation (ECC)</li> </ul>                 | TPM2_Clear                   |
| 5                  | nullProof       | 32 bytes secret values resp. for NULL, platform, endorsement and storage hierarchies.<br>NullProof is a random value generated by HDRBG at each TPM power-up.  | TPM reset                    |
| 6                  | phProof         | PhProof / ehProof / shProof are random values generated by HDRBG at first TPM power-up.  | TPM2_Change PPS              |
| 7                  | ehProof         | They are used as keys for:   | TPM2_Clear                   |
| 8                  | shProof         | <ul style="list-style-type: none"> <li>KDFa to generate context encryption key and IV (cf. [TPM2.0 Part1 r1.16] §30.3.1)</li> <li>HMAC to compute context blob integrity (cf. [TPM2.0 Part1 r1.16] §30.3.2)</li> <li>HMAC to compute/verify tickets</li> </ul> shProof is used also as key for: <ul style="list-style-type: none"> <li>KDFa to generate obfuscation value used in attestation commands (cf. [TPM2.0 Part1 r1.16] §36.7)</li> </ul>   | TPM2_Clear                   |
| 9                  | platformAuth    | 32 bytes authorization data (authValue) used in authorization session based resp. on platform, endorsement, and storage or lockout hierarchy authorization.<br>PlatformAuth is set to 0 at each TPM2_Startup (CLEAR).  | TPM2_Startup                 |
| 10                 | endorsementAuth | EndorsementAuth / ownerAuth / lockoutAuth are set to 0 at first TPM power-up.<br>Primary auth values can be changed with command TPM2_HierarchyChangeAuth.   | TPM2_Clear / TPM2_Change EPS |
| 11                 | ownerAuth       | They are used as keys for:   | TPM2_Clear                   |
| 12                 | lockoutAuth     | <ul style="list-style-type: none"> <li>HMAC authorization in case of unsalted and unbound session</li> <li>KDFa to generate session key used in HMAC authorization in case of bound session</li> </ul> They are used as part of keys for: <ul style="list-style-type: none"> <li>HMAC authorization in case of salted or bound session (key is concatenation of sessionKey and authValue)</li> <li>KDFa to generate session key used in HMAC authorization in case of salted and bound session (key is concatenation of authValue and salt)</li> </ul> | 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.<br>platformPolicy is set to 0 at each TPM2_Startup (CLEAR).  | TPM2_Change PPS   |
| 14             | endorsementPolicy | endorsementPolicy / ownerPolicy / lockoutPolicy are set to 0 at first TPM power-up.  | TPM2_Clear / TPM2_Change EPS  |
| 15             | ownerPolicy       | Primary policies can be changed with command TPM2_SetPrimaryPolicy.<br>They are used as reference values for a comparison in case of policy session.   | TPM2_Clear  |
| 16             | lockoutPolicy     |  | TPM2_Clear  |
| <b>Objects</b> |                   |  |   |
| 17             | authValue         | 0 to 32 bytes authorization data defined during object creation (TPM2_Create/TPM2_CreatePrimary) used to authorize commands based on this object.<br>Value can be changed with command TPM2_ObjectChangeAuth.<br>It is used as: <ul style="list-style-type: none"> <li>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)</li> <li>Secret value extended into policyDigest on TPM2_PolicySecret command</li> </ul>  | TPM2_Clear (owner & endorsement)<br>TPM2_Change PPS (platform)<br>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.<br>It is used as reference value for a comparison in case of policy session  | TPM2_Clear (owner & endorsement)<br>TPM2_Change PPS (platform)<br>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).<br>It is used as key for: <ul style="list-style-type: none"> <li>KDFa to generate seedValue and sensitive during object creation (cf. [TPM2.0 Part1 r1.16] §27.6.4)</li> </ul>  | 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.<br>It is used (when not set to 0) as: <ul style="list-style-type: none"> <li>Data in SHA computation to generate object's unique value (HMAC and symmetric key creation)</li> <li>Key in KDFa to generate a symmetric encryption key used in TPM2B_PRIVATE structure en/decryption.</li> <li>Key in KDFa to generate HMAC key used in TPM2B_PRIVATE integrity protection generation or verification</li> </ul> | TPM2_Clear (owner & endorsement)<br>TPM2_Change PPS (platform)<br>TPM2_Change EPS (endorsement) |
| 21             | symKey            | 16 bytes generated from derivation of seedValue through KDFa usage.<br>It is used as key for: <ul style="list-style-type: none"> <li>Symmetric en/decryption of TPM2B_PRIVATE structure</li> </ul>   | Transient value only available during command processing  |
| 22             | hmacKey           | 32 bytes generated from derivation of seedValue through KDFa usage.<br>It is used as key for:  | Transient value only available during command processing  |



|                   |   |  |  |
|-------------------|---|--|--|
|                   |   | <ul style="list-style-type: none"> <li>HMAC used in TPM2B_PRIVATE integrity protection generation or verification</li> </ul>   |  |
| 23                | sensitive   | <p>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.</p> <p>Depending on object's nature, sensitive is used as key for:</p> <ul style="list-style-type: none"> <li>en/decryption (RSA, AES, TDES)</li> <li>signature generation (RSA, ECDSA, HMAC)</li> <li>secret value exchange (ECDH)</li> </ul> <p>Available key lengths correspond to the ones listed in <b>Table 9: Approved algorithms</b> (Key nature and length are selected by user thanks to the interface of the keys creation commands).</p> | <p>TPM2_Clear (owner &amp; endorsement)</p> <p>TPM2_Change PPS (platform)</p> <p>TPM2_Change EPS (endorsement)</p> |
| <b>NV Indexes</b> |   |  |  |
| 24                | authValue   | <p>0 to 32 bytes authorization data defined during NV index creation (TPM2_DefineSpace) used to authorize commands based on this object.</p> <p>Value can be changed with command TPM2_NV_ChangeAuth.</p> <p>It is used as:</p> <ul style="list-style-type: none"> <li>HMAC and/or KDFa keys or part of keys in authorization session based on HMAC or password.</li> <li>Secret value extended into policyDigest on TPM2_PolicySecret command</li> </ul>  | <p>TPM2_NV_UndefineSpace</p> <p>/</p> <p>TPM2_NV_UndefineSpaceSpecial</p>  |
| 25                | authPolicy  | <p>0 to 32 bytes authorization data defined during object creation (TPM2_DefineSpace) used to authorize commands based on this object.</p> <p>It is used as reference value for a comparison in case of policy session</p>   | <p>TPM2_NV_UndefineSpace</p> <p>/</p> <p>TPM2_NV_UndefineSpaceSpecial</p>  |
| <b>Sessions</b>   |   |  |  |
| 26                | salt  | <p>Value passed encrypted (with a loaded decrypt key) to TPM2_StartAuthSession.</p> <p>It is used as:</p> <ul style="list-style-type: none"> <li>Part of KDFa key to generate the sessionKey (cf. [TPM2.0 Part1 r1.16] §19.6)</li> </ul>   | <p>Transient value only available during TPM2_StartAuthSession processing</p>                                      |
| 27                | sessionKey  | <p>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).</p> <p>It is used as:</p> <ul style="list-style-type: none"> <li>HMAC key used to generate and verify command authorization</li> <li>Part of KDFa key used to generate encryption key and IV of encryption-based session</li> </ul>   | <p>TPM2_FlushContext</p>   |
| 28                | encryption key and IV of encryption-based session | <p>Symmetric key and IV generated by KDFa (cf. [TPM2.0 Part1 r1.16] §21.3) from sessionKey and object's authValue.</p> <p>It is used as key and IV for:</p> <ul style="list-style-type: none"> <li>Symmetric en/decryption of first parameter of command/response if parameter structure is of type TPM2B_</li> </ul>  | <p>TPM2_FlushContext</p>   |
| <b>Context</b>    |   |  |  |
| 29                | contextKey  | <p>16 bytes randomly generated by HDRBG at each TPM reset.</p> <p>It is used as:</p> <ul style="list-style-type: none"> <li>1<sup>st</sup> part of key used in KDFa to generate a symmetric encryption key and IV used in context blob en/decryption.</li> </ul>   | <p>TPM reset</p>   |

|                    |  |  |  |
|--------------------|--|--|--|
| 30                 | symKey, IV                               | 2*16 bytes derived from the concatenation of contextKey and one of the proof (CSP 5, 6, 7, 8). It is used as key and IV for: <ul style="list-style-type: none"> <li>Symmetric en/decryption of context blob</li> </ul>   | Transient value only available during TPM2_ContextSave / TPM2_ContextLoad processing |
| <b>Duplication</b> |  |  |  |
| 31                 | inner symKey                             | Symmetric key passed as input to duplication commands or generated by HDRBG (size depends on symmetric algorithm used).<br>It is used as: <ul style="list-style-type: none"> <li>Symmetric en/decryption key to protect TPM2B_PRIVATE output structure</li> </ul>  | 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.<br>It is used as key for : <ul style="list-style-type: none"> <li>KDFa to generate a symmetric en/decryption key for outer protection</li> <li>KDFa to generate a HMAC key for outer integrity protection</li> </ul>                      |  |
| 33                 | outer symKey                             | Symmetric key generated via KDFa from seed. It is used as key for: <ul style="list-style-type: none"> <li>Symmetric en/decryption key for outer protection of TPM2B_PRIVATE output structure</li> </ul>  |  |
| 34                 | outer hmacKey                            | HMAC key generated via KDFa from seed. It is used as key for: <ul style="list-style-type: none"> <li>HMAC integrity key for outer protection of TPM2B_PRIVATE output structure</li> </ul>  |  |
| <b>Credential</b>  |  |  |  |
| 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.<br>It is used as key for : <ul style="list-style-type: none"> <li>KDFa to generate a symmetric en/decryption key for outer protection</li> <li>KDFa to generate a HMAC key for outer integrity protection</li> </ul>                      | Transient value only available during command processing                             |
| 36                 | symKey                                   | Symmetric key generated via KDFa from seed. It is used as key for: <ul style="list-style-type: none"> <li>Symmetric en/decryption key for outer protection of credentialBlob</li> </ul>  |  |
| 37                 | hmacKey                                  | HMAC key generated via KDFa from seed. It is used as key for: <ul style="list-style-type: none"> <li>HMAC integrity key for outer protection of credentialBlob</li> </ul>  |  |
| <b>DRBG</b>        |  |  |  |
| 38                 | DRBG state                               | Internal state (V and C secret values) of the HDRBG (based on SHA256) stored in RAM.   | TPM2_Clear   |
| <b>ECC</b>         |  |  |  |
| 39                 | commitNonce                              | 32 bytes value randomly generated by HDRBG at each TPM2_Startup (CLEAR).<br>It is used as key for : <ul style="list-style-type: none"> <li>KDFa to generate an ECC ephemeral private key used in TPM2_EC_Ephemeral command / TPM2_ZGen_2Phase</li> </ul>   | 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: <ul style="list-style-type: none"> <li>TPM2_Ephemeral command (scalar multiplication) to generate the associated ephemeral public key</li> <li>TPM2_Zgen_2Phase (ECDH scheme) to generate outZ2 (output point)</li> </ul> |  |
| 41                 | ephemeral key                            | ECC private key (size depends on curve selected) generated with HDRBG. It is used as ephemeral private key in: <ul style="list-style-type: none"> <li>TPM2_ECDH_KeyGen command (ECDH scheme) to generate zPoint (output point)</li> </ul>  |  |

| 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.<br>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.<br>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 18: Command support table**

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

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

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

| Services                               |                                | Role | Keys and CSP access<br>W = write, O = output, Z = zeroize<br>C = used as key in cryptographic operation<br>R = read (and not used as C) | Authorized in limited approved mode |
|--|--------------------------------|------|---|-------------------------------------|
| 46                                     | TPM2_SetCommandCodeAuditStatus | CO   | R : 13, 18<br>C : 9, 11, 15, 27   |                                     |
| <b>Integrity collection (PCR)</b>      |                                |      |   |                                     |
| 47                                     | TPM2_PCR_Extend                | U    | R : 18<br>C : 27  |                                     |
| 48                                     | TPM2_PCR_Event                 | U    | R : 18<br>W : 28, 38, 48<br>C : 27, 28, 38  |                                     |
| 49                                     | TPM2_PCR_Read                  | NA   | -   | X                                   |
| 50                                     | TPM2_PCR_Allocate              | CO   | R : 13, 18<br>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                                   |
| <b>Enhanced authorization commands</b> |                                |      |   |                                     |
| 57                                     | TPM2_PolicySigned              | NA   | C : 28  |                                     |
| 58                                     | TPM2_PolicySecret              | U    | R : 18<br>W : 28, 38, 48<br>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<br>W : 28<br>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   | -   |                                     |
| <b>Hierarchy commands</b>              |                                |      |   |                                     |

| Services                    |                                 | Role | Keys and CSP access<br>W = write, O = output, Z = zeroize<br>C = used as key in cryptographic operation<br>R = read (and not used as C)      | Authorized in limited approved mode |
|-----------------------------|---------------------------------|------|--|-------------------------------------|
| 75                          | TPM2_CreatePrimary              | CO   | R : 13, 14, 15, 16, 18, 42, 43<br>W : 20, 21, 22, 23, 28, 38, 47, 48<br>C : 1, 2, 3, 4, 17, 19, 20, 21, 22, 27, 28, 38, 42, 43, 48<br>Z : 47 |                                     |
| 76                          | TPM2_HierarchyControl           | CO   | C : 9, 10, 11, 27  |                                     |
| 77                          | TPM2_SetPrimaryPolicy           | CO   | W : 13, 14, 15, 16, 28<br>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<br>W : 38, 48<br>Z : 4, 7, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 20, 23, 24, 25, 38, 48<br>C : 38                                 |                                     |
| 81                          | TPM2_ClearControl               | CO   | R : 13, 16<br>W : 38, 48<br>C : 9, 12, 38, 48  |                                     |
| 82                          | TPM2_HierarchyChangeAuth        | CO   | R : 13, 16<br>W : 9, 10, 11, 12, 28, 38, 48<br>C : 9, 10, 11, 12, 28, 38, 48   |                                     |
| <b>Non-Volatile Storage</b> |                                 |      |  |                                     |
| 83                          | TPM2_DictionaryAttackLockReset  | CO   | R : 16<br>W : 38, 48<br>C : 12, 38, 48   |                                     |
| 84                          | TPM2_DictionaryAttackParameters | CO   | R : 16<br>W : 38, 48<br>C : 12, 38, 48   |                                     |
| <b>Field Upgrade</b>        |                                 |      |  |                                     |
| 86                          | TPM2_FieldUpgradeStart          | CO   | W : 28<br>C : 9, 13, 28, 44  |                                     |
| 87                          | TPM2_FieldUpgradeData           | NA   | -  |                                     |
| <b>Context Management</b>   |                                 |      |  |                                     |
| 88                          | TPM2_ContextSave                | NA   | W : 30<br>C : 5, 6, 7, 8, 29, 30   |                                     |
| 89                          | TPM2_ContextLoad                | NA   | W : 30<br>C : 5, 6, 7, 8, 29, 30   |                                     |
| 90                          | TPM2_FlushContext               | NA   | Z : 17, 18, 20, 23, 27, 28   | X                                   |
| 91                          | TPM2_EvictControl               | CO   | R : 13, 15<br>C : 9, 11  |                                     |
| <b>Clock and Timers</b>     |                                 |      |  |                                     |
| 92                          | TPM2_ReadClock                  | NA   | -  | X                                   |



| Services                    |                              | Role  | Keys and CSP access<br>W = write, O = output, Z = zeroize<br>C = used as key in cryptographic operation<br>R = read (and not used as C) | Authorized in limited approved mode |
|-----------------------------|------------------------------|-------|---|-------------------------------------|
| 93                          | TPM2_ClockSet                | CO    | R : 13, 15<br>C : 9, 11   |                                     |
| 94                          | TPM2_ClockRateAdjust         | CO    | R : 13, 15<br>C : 9, 11   |                                     |
| <b>Capability Commands</b>  |                              |       |   |                                     |
| 95                          | TPM2_GetCapability           | NA    | -   | X                                   |
| 96                          | TPM2_TestParms               | NA    | -   | X                                   |
| <b>Non-volatile storage</b> |                              |       |   |                                     |
| 97                          | TPM2_NV_DefineSpace          | CO    | R : 13, 15, 18<br>W : 24, 25, 28, 38, 48<br>C : 9, 11, 27, 28, 38, 48   |                                     |
| 98                          | TPM2_NV_UndefineSpace        | CO    | W : 38, 48<br>C : 27, 38, 48<br>Z : 24, 25  |                                     |
| 99                          | TPM2_NV_UndefineSpaceSpecial | CO, A | W : 38, 48<br>C : 27, 38, 48<br>Z : 24, 25  |                                     |
| 100                         | TPM2_NV_ReadPublic           | NA    | C : 28  | X                                   |
| 101                         | TPM2_NV_Write                | U     | W : 28, 38, 48<br>R : 25<br>C : 27, 28, 38, 48  |                                     |
| 102                         | TPM2_NV_Increment            | U     | W : 38, 48<br>R : 25<br>C : 27, 38, 48  |                                     |
| 103                         | TPM2_NV_Extend               | U     | W : 28, 38, 48<br>R : 25<br>C : 27, 28, 38, 48  |                                     |
| 104                         | TPM2_NV_SetBits              | U     | W : 38, 48<br>R : 25<br>C : 27, 38, 48  |                                     |
| 105                         | TPM2_NV_WriteLock            | U     | W : 38, 48<br>R : 25<br>C : 27, 38, 48  |                                     |
| 106                         | TPM2_NV_GlobalWriteLock      | CO    | W : 38, 48<br>C : 27, 38, 48  |                                     |
| 107                         | TPM2_NV_Read                 | U     | W : 28, 38, 48<br>R : 25<br>C : 27, 28, 38, 48  |                                     |
| 108                         | TPM2_NV_ReadLock             | U     | W : 38, 48<br>R : 25<br>C : 27, 38, 48  |                                     |
| 109                         | TPM2_NV_ChangeAuth           | A     | W : 24, 28, 38, 48<br>C : 27, 28, 38, 48  |                                     |

| Services                    |   | Role      | Keys and CSP access<br>W = write, O = output, Z = zeroize<br>C = used as key in cryptographic operation<br>R = read (and not used as C) | Authorized in limited approved mode |
|-----------------------------|---|-----------|---|-------------------------------------|
| 110                         | TPM2_NV_Certify                           | <b>U</b>  | W : 28, 38, 48<br>R : 25<br>C : 27, 28, 38, 48  |                                     |
| <b>Proprietary commands</b> |   |           |   |                                     |
| 111                         | TPM2_SetMode                              | <b>CO</b> | W : 28, 38, 48<br>C : 27, 28, 38, 48  |                                     |
| 112                         | TPM2_SetCommandSet                        | <b>CO</b> | W : 28, 38, 48<br>C : 27, 28, 38, 48  |                                     |
| 113                         | TPM2_RestoreEK                            | <b>CO</b> | Z : 3, 7, 10, 14, 17, 18, 20<br>R : 42, 43<br>W : 23, 28, 38, 48<br>C : 27, 28, 38, 48  |                                     |
| 114                         | TPM2_SetCommandSetLock                    | <b>CO</b> | W : 28, 38, 48<br>C : 27, 28, 38, 48  |                                     |
| <b>Misc commands</b>        |   |           |   |                                     |
| 115                         | TPM2_PP_Commands                          | <b>CO</b> | -   |                                     |
| <b>Non FIPS services</b>    |   |           |   |                                     |
| 116                         | Field upgrade de-obfuscation <sup>1</sup> | <b>NA</b> | -   |                                     |

### 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

<sup>1</sup> 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\_EC\_Ephemeral: ephemeral ECC key generation

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 19 : 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 20: 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) <sup>1</sup> | 128                                   |
| AES CFB (256 bits) <sup>2</sup> | 256                                   |

<sup>1</sup> AES is used in conjunction with HMAC approved authentication method ([SP800-38F] compliant)

<sup>2</sup> 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 22 : 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 21 : 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<br>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.       |

|                     |  |
|---------------------|--|
| <b>FW integrity</b> | 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. |
| <b>HW integrity</b> | 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 22 : Asymmetric cryptography self-tests list**

| Algorithm tested | Test description   |
|------------------|--|
| <b>RSA</b>       | 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. |
| <b>ECDH</b>      | 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.  |
| <b>ECDSA</b>     | 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 23 : TPM conditional tests**

| Algorithm tested          | Test description  |
|---------------------------|---|
| <b>FW integrity</b>       | FW integrity is verified by computing an EDC (CRC-16 ISO 13239) and comparing it to reference values.   |
| <b>Hash-DRBG</b>          | 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.  |
| <b>NDRNG</b>              | 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.  |
| <b>FW load</b>            | During field upgrade procedure, several checks are performed before authorizing the FW to be upgraded: <ul style="list-style-type: none"> <li>- Verification of signature (RSASSA-PSS) on the first data blob to ensure authentication of the FW</li> <li>- Verification of digest (SHA256) on each subsequent blob to guarantee integrity of the full FW.</li> </ul> |
| <b>RSA key generation</b> | 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).  |
| <b>ECC key generation</b> | On each ECC key generation, an ECDSA signature is generated and verified on curve NIST P-256.   |

|                            |   |
|----------------------------|---|
| <b>TDES key generation</b> | <p>TDES key generation process consists in generating a pseudo-random value from KDFa and checking that this value passes the following conditional tests to be considered and next used as a functional TDES key. Conditional tests are:</p> <ol style="list-style-type: none"> <li>1. Check that the 3 TDES cryptographic keys are different: <math>Key_1 \neq Key_2</math>, <math>Key_2 \neq Key_3</math>, <math>Key_1 \neq Key_3</math> (Keying option 1 from §3.2 of [SP800-67])</li> <li>2. Key is not one of the weak key listed in §3.4.2 of [SP800-67]</li> </ol> <p>In case of failure, new pseudo-random values are generated until a valid TDES key is found.</p> |
|----------------------------|---|

#### 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] / [ST33TPHF20SPI DS] / [ST33TPHF2EI2C DS] / [ST33TPHF20I2C 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.

| Reference            | Document  |
|----------------------|---|
| [ST33TPHF20SPI DS]   | ST33TPHF20SPI Datasheet, STMicroelectronics, May 2017   |
| [ST33TPHF20I2C DS]   | ST33TPHF20I2C Datasheet, STMicroelectronics, May 2017   |
| [ST33TPHF2ESPI DS]   | ST33TPHF2ESPI Datasheet, STMicroelectronics, April 2017   |
| [ST33TPHF2EI2C DS]   | ST33TPHF2EI2C Datasheet, STMicroelectronics, May 2017   |
| [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, <i>Derived Test Requirements(DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules</i> |
| [FIPS IG]            | National Institute of Standards and Technology and Communications Security, <i>Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program</i>         |
| [FIPS 180-4]         | National Institute of Standards and Technology, <i>Secure Hash Standard</i> , Federal Information Processing Standards Publication 180-4, March 2012                                  |
| [FIPS 186-4]         | National Institute of Standards and Technology, <i>Digital Signature Standard (DSS)</i> , Federal Information Processing Standards Publication 186-4, July 2013                       |
| [FIPS 197]           | National Institute of Standards and Technology, <i>Advanced Encryption Standard (AES)</i> , Federal Information Processing Standards Publication 197, November 2001                   |
| [SP800-135]          | National Institute of Standards and Technology, <i>Existing Application-Specific Key Derivation Function Validation System</i> , September 2015.                                      |
| [SP800-108]          | National Institute of Standards and Technology, <i>Recommendation for Key Derivation Using Pseudorandom Functions</i> , October 2009.   |
| [SP800-131A]         | National Institute of Standards and Technology, <i>Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths</i> , 11/06/15.                  |

| Reference        | Document  |
|------------------|---|
| [FIPS 198-1]     | National Institute of Standards and Technology, <i>The Keyed-Hash Message Authentication Code</i> , NIST Computer Security Division Page 3 07/26/2011, (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008 |
| [SP800-90A]      | National Institute of Standards and Technology, <i>Recommendation for Random Number Generation Using Deterministic Random Bit Generators</i> , January 2012.  |
| [SP800-38F]      | National Institute of Standards and Technology, <i>Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping</i> , December 2012.  |
| [SP800-56A]      | National Institute of Standards and Technology, <i>Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography</i> , March 2007.   |
| [SP800-67]       | National Institute of Standards and Technology, <i>Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher</i> , January 2012.  |
| [FIPS 140-2 TPM] | TCG FIPS 140-2 Guidance for TPM2.0, v1.0, TCG   |

| 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                             |

## **IMPORTANT NOTICE – PLEASE READ CAREFULLY**

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2017 STMicroelectronics - All rights reserved  
[www.st.com](http://www.st.com)