

# OPTIGA™ TPM SLB9672 TPM 2.0 FW16.xx

## Datasheet

### Trusted Platform Module

Document release reference: Z8F80723107-B

## Key features

- Optimized TPM device for IoT and ICT applications
- Compliant with TCG TPM Library specification revision 1.59 and PC Client Platform TPM Profile (PTP) version 1.05
- PQC-protected firmware update mechanism
- Certifications:
  - Common Criteria, level EAL4+, AVA\_VAN.4 (moderate) according to TCG PC Client TPM Protection Profile (targeted) – (9 October 2024) – Certificate number CC-1245
  - FIPS 140-2 Level 2 – (7 April 2023) – Certificate Number 4467
- SPI interface
- Meeting Intel TXT and Microsoft Windows certification criteria for successful platform qualification
- Random Number Generator (RNG) implemented according to NIST SP 800-90A using entropy source according to NIST SP 800-90B
- Provisioned with 4 Endorsement Keys (EK) and EK certificates (RSA 2048, RSA 3072, ECC NIST P256, ECC NIST P384)
- Enhanced (-40°C .. +85°C) or extended (-40°C .. +105°C) temperature range
- PG-UQFN-32-1,-2 package
- Optimized for battery operated devices: low standby power consumption (typ. 120 µA)
- 24 PCRs (SHA-1, SHA-256 or SHA384)
- 51 kByte NV memory
- Unlimited amount of NV counters (only depending on NV memory utilization)
- Up to 3 loaded sessions (TPM\_PT\_HR\_LOADED\_MIN)
- Up to 64 active sessions (TPM\_PT\_ACTIVE\_SESSIONS\_MAX)
- Up to 3 loaded transient Objects (TPM\_PT\_HR\_TRANSIENT\_MIN)
- Up to 7 loaded persistent Objects (TPM\_PT\_HR\_PERSISTENT\_MIN)
- Pre-generation of up to 7 RSA key pairs
- RSA (1024, 2048, 3072 and 4096 bit)
- ECC (NIST P256, NIST P384, BN P256)
- SHA-1, SHA-256, SHA-384
- AES-128, AES-192, AES-256

## Product validation

Qualified for applications according to the test conditions in the relevant tests of JEDEC JESD22 and J-STD-020.

---

**Ordering information**

## Ordering information

Device Name	Package	Remarks
SLB 9672XU2.0 FW16.xx	PG-UQFN-32-1,-2	Enhanced temperature range -40°C - 85°C
SLB 9672AU2.0 FW16.xx	PG-UQFN-32-1,-2	Extended temperature range -40°C - 105°C

## About this document

### Scope and purpose

This datasheet describes the SLB 9672 TPM 2.0 FW16.xx Trusted Platform Module together with its features, functionality and programming interface.

### Intended audience

This datasheet is primarily intended for system developers.

## **Table of contents**

	<b>Product validation</b> .....	1
	<b>Ordering information</b> .....	2
	<b>About this document</b> .....	2
	<b>Table of contents</b> .....	3
	<b>List of tables</b> .....	5
	<b>List of figures</b> .....	7
<b>1</b>	<b>Introduction</b> .....	8
1.1	Product description .....	8
1.2	Power management .....	8
<b>2</b>	<b>Delivery forms and ordering</b> .....	9
2.1	Package dimensions (UQFN) .....	9
2.1.1	Packing type .....	10
2.1.2	Recommended footprint .....	11
2.1.3	Chip marking .....	11
2.2	Ordering information .....	12
<b>3</b>	<b>Solution details</b> .....	13
3.1	Hardware .....	13
3.1.1	Electrical characteristics .....	13
3.1.1.1	Absolute maximum ratings .....	13
3.1.1.2	Functional operating range .....	13
3.1.1.3	DC characteristics .....	14
3.1.1.4	AC characteristics .....	15
3.1.1.5	Timing .....	16
3.1.2	Pin description .....	17
3.1.3	Typical schematic .....	19
3.2	TPM embedded software .....	20
3.2.1	Implemented algorithms .....	20
3.2.2	Available resources .....	20
3.2.3	Command ordinal list .....	22
3.2.4	Generation of RSA keys .....	26
3.2.4.1	Pre-generation of RSA keys .....	26
3.2.4.2	Generation of RSA 3072- and 4096-bit keys .....	26
3.2.5	Non-volatile storage .....	27
3.2.5.1	Predefined NV indices .....	27
3.2.6	Vendor-specific functionality .....	28
3.2.6.1	Power saving mode .....	28
3.2.6.2	TPM and vendor properties .....	28

**Table of contents**

3.2.6.3	Selftest operations . . . . .	30
3.2.6.3.1	TPM2_SelfTest . . . . .	30
3.2.6.3.2	TPM2_FullFipsSelfTestVendor . . . . .	30
3.2.6.3.3	TPM2_GetTestResult . . . . .	30
3.2.6.4	Dictionary attack default values . . . . .	31
3.2.6.5	RSA signing scheme . . . . .	32
3.2.6.6	NV index attribute TPMA_NV_WRITTEN . . . . .	32
3.2.6.7	Allocation of PCR banks . . . . .	32
3.2.6.8	General purpose I/O (GPIO) . . . . .	32
3.2.6.8.1	TPM2_NV_DefineSpace . . . . .	32
3.2.6.8.2	TPM2_NV_Write . . . . .	33
3.2.6.8.3	TPM2_NV_Read . . . . .	33
3.2.6.8.4	TPM2_NV_UndefineSpace . . . . .	33
3.2.6.9	TPM2_SetCapabilityVendor . . . . .	33
3.2.6.10	Field upgrade . . . . .	35
3.2.6.10.1	Structures and definitions . . . . .	35
3.2.6.10.2	TPM2B_MAX_BUFFER_VENDOR . . . . .	35
3.2.6.10.3	TPML_MAX_BUFFER . . . . .	35
3.2.6.10.4	Commands in TPM operational mode . . . . .	36
3.2.6.10.5	Commands in TPM firmware update mode . . . . .	38
3.2.7	TPM unique identifier . . . . .	41
3.2.8	Reset timing . . . . .	42
3.2.9	Firmware version mapping . . . . .	43
<b>4</b>	<b>Licenses and notices . . . . .</b>	<b>44</b>
	<b>References . . . . .</b>	<b>45</b>
	<b>Revision history . . . . .</b>	<b>46</b>
	<b>Disclaimer . . . . .</b>	<b>47</b>

**List of tables**

**List of tables**

Table 1	Sales order code .....	12
Table 2	Absolute maximum ratings .....	13
Table 3	Functional operating range .....	13
Table 4	Current consumption .....	14
Table 5	DC characteristics of SPI interface pins (SCLK, CS#, MISO, MOSI, RST#, PIRQ#) .....	14
Table 6	DC characteristics of GPIO pins .....	15
Table 7	Power supply .....	15
Table 8	Device reset .....	15
Table 9	AC characteristics of SPI interface .....	15
Table 10	Buffer types .....	17
Table 11	I/O Signals .....	17
Table 12	Power supply .....	18
Table 13	Not connected .....	18
Table 14	Implemented algorithms .....	20
Table 15	Available resources .....	20
Table 16	Command code list .....	22
Table 17	Vendor-specific TPM_CC constants .....	24
Table 18	Predefined NV indices .....	27
Table 19	Attributes of predefined NV indices .....	27
Table 20	Infineon TPM property values .....	28
Table 21	Infineon vendor-specific property constants .....	28
Table 22	Infineon vendor-specific property values .....	29
Table 23	TPM operation modes .....	29
Table 24	FIFO configuration registers .....	30
Table 25	TPM_RID register value description .....	30
Table 26	Incoming operands and sizes .....	30
Table 27	Outgoing operands and sizes .....	30
Table 28	TPM2_SelfTest bit mapping of TPM2_SelfTest .....	31
Table 29	TPM2_SelfTest bit mapping of TPM2_FullFipsSelfTestVendor .....	31
Table 30	TPM2_SelfTest result .....	31
Table 31	Mapping of GPIO indices .....	32
Table 32	Default capability settings .....	33
Table 33	Incoming operands and sizes .....	33
Table 34	Outgoing operands and sizes .....	34
Table 35	Error return codes .....	34
Table 36	TPM2B_MAX_BUFFER_VENDOR structure definition .....	35
Table 37	TPML_MAX_BUFFER structure definition .....	35
Table 38	Incoming operands and sizes .....	36
Table 39	Outgoing operands and sizes .....	36
Table 40	Error return codes .....	36
Table 41	Incoming operands and sizes .....	37
Table 42	Outgoing operands and sizes .....	37
Table 43	Error return codes .....	37

**List of tables**

Table 44	Incoming operands and sizes . . . . .	38
Table 45	Outgoing operands and sizes . . . . .	38
Table 46	Error return codes . . . . .	38
Table 47	Incoming operands and sizes . . . . .	39
Table 48	Outgoing operands and sizes . . . . .	39
Table 49	Error return codes . . . . .	39
Table 50	Incoming operands and sizes . . . . .	39
Table 51	Outgoing operands and sizes . . . . .	39
Table 52	Error return codes . . . . .	40
Table 53	Incoming operands and sizes . . . . .	40
Table 54	Outgoing operands and sizes . . . . .	40
Table 55	TPM2_GetTestResult bit mapping in TPM firmware update . . . . .	41
Table 56	Definition of the firmware version fields . . . . .	43
Table 57	Mapping of the firmware versions . . . . .	43

---

**List of figures**

**List of figures**

Figure 1	Package dimensions PG-UQFN-32-1,-2 .....	9
Figure 2	Tape & reel dimensions PG-UQFN-32-1,-2 .....	10
Figure 3	Recommended footprint PG-UQFN-32-1,-2 .....	11
Figure 4	Chip marking .....	11
Figure 5	Reset timing .....	15
Figure 6	Pinout of the SLB 9672 TPM 2.0 (PG-UQFN-32-1,-2 package, top view) .....	17
Figure 7	Typical schematic .....	19

## **1 Introduction**

# **1 Introduction**

## **1.1 Product description**

The SLB 9672 TPM 2.0 is a Trusted Platform Module. It is available in PG-UQFN-32-1,-2 package. It supports an SPI interface with a transfer rate of up to 33 MHz (typical). The SLB 9672 TPM 2.0 is compliant with TCG TPM Library specification revision 1.59 [1] and PC Client Platform TPM Profile (PTP) version 1.05 [2], including Errata (see [3] and [4]).

This TPM product is targeted to be certified, using the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Rev.5, in the level EAL4+, AVA\_VAN.4 (moderate), ALC\_FLR.1 according to the Protection Profile PC Client Specific TPM, TPM Library Specification Family "2.0" Level 0 Revision 1.59 (CERTIFICATE ANSSI-CC-PP-2020/01).

## **1.2 Power management**

In the SLB 9672 TPM 2.0, power management is handled internally; no explicit power-down or standby mode is available. The device automatically enters a low-power state after each successful command/response transaction. If a transaction is started on the SPI bus from the host platform, the device will wake up immediately and will return to the low-power mode after the transaction has been finished.



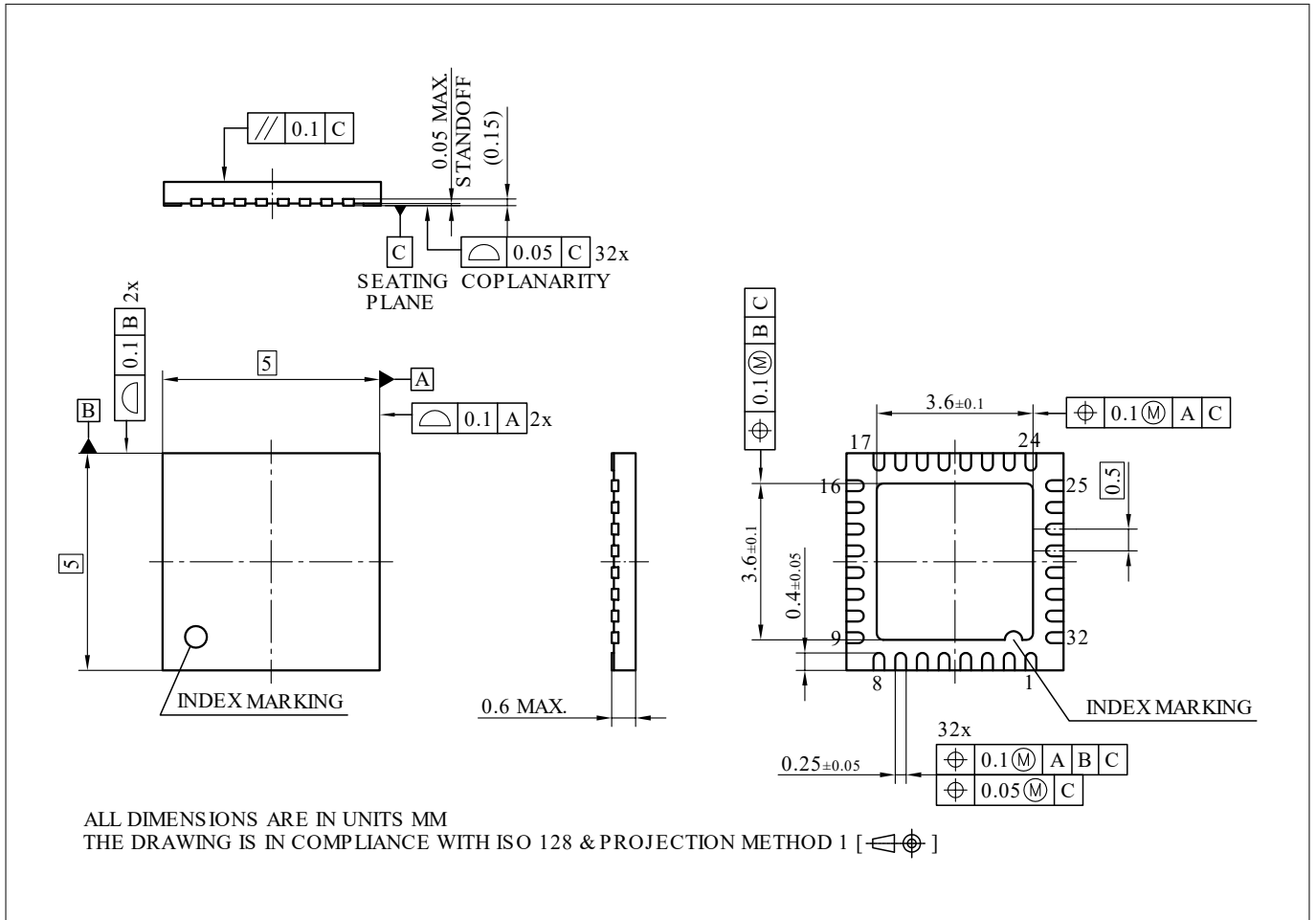
**2 Delivery forms and ordering**

**2 Delivery forms and ordering**

The SLB 9672 TPM 2.0 product family features devices using an UQFN package.

**2.1 Package dimensions (UQFN)**

All dimensions are given in millimeters (mm) unless otherwise noted. The packages are "green" and RoHS compliant.



**Figure 1 Package dimensions PG-UQFN-32-1,-2**

## 2 Delivery forms and ordering

### 2.1.1 Packing type

PG-UQFN-32-1,-2: Tape & Reel (reel diameter 330mm), 5000 pcs. per reel

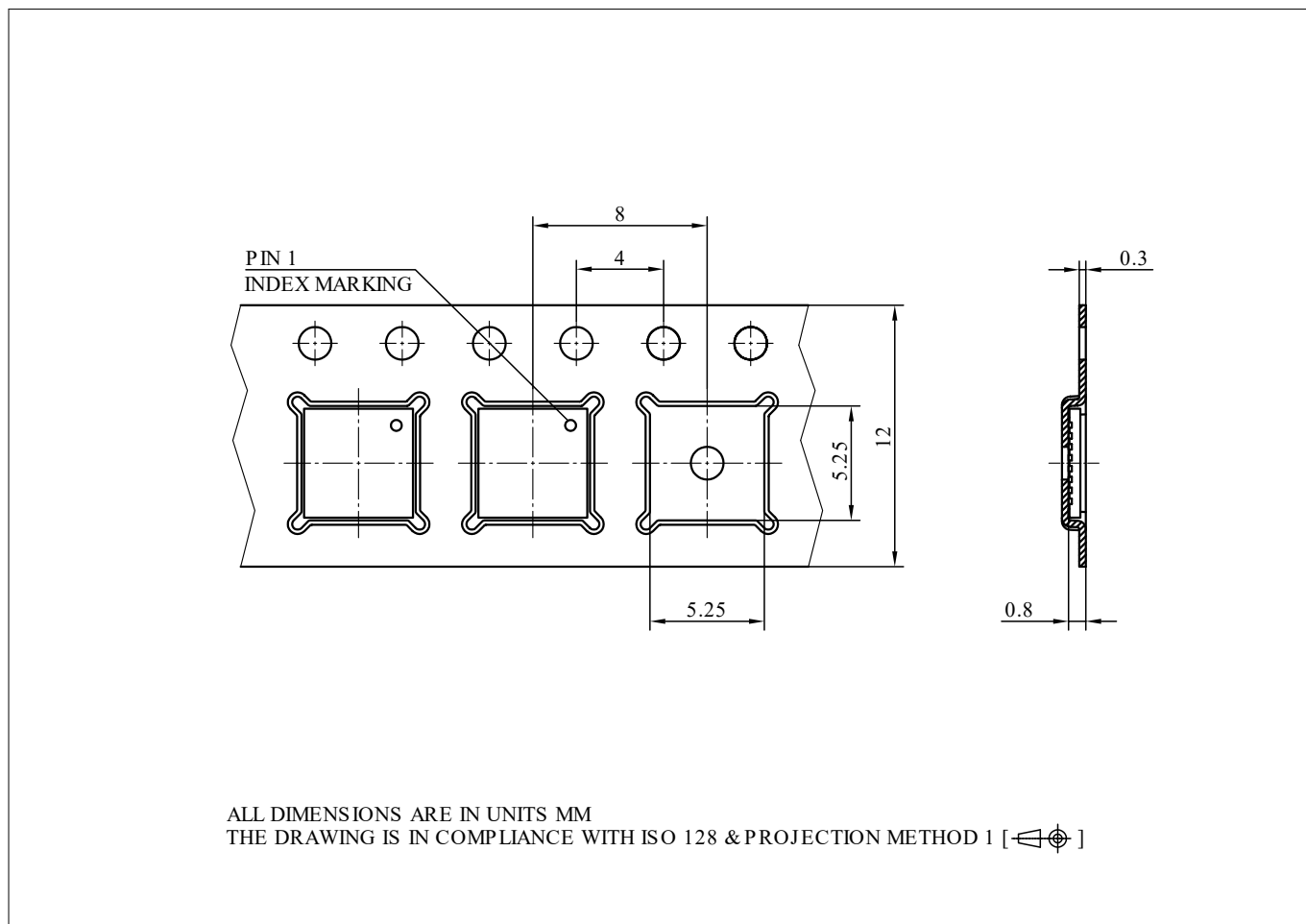
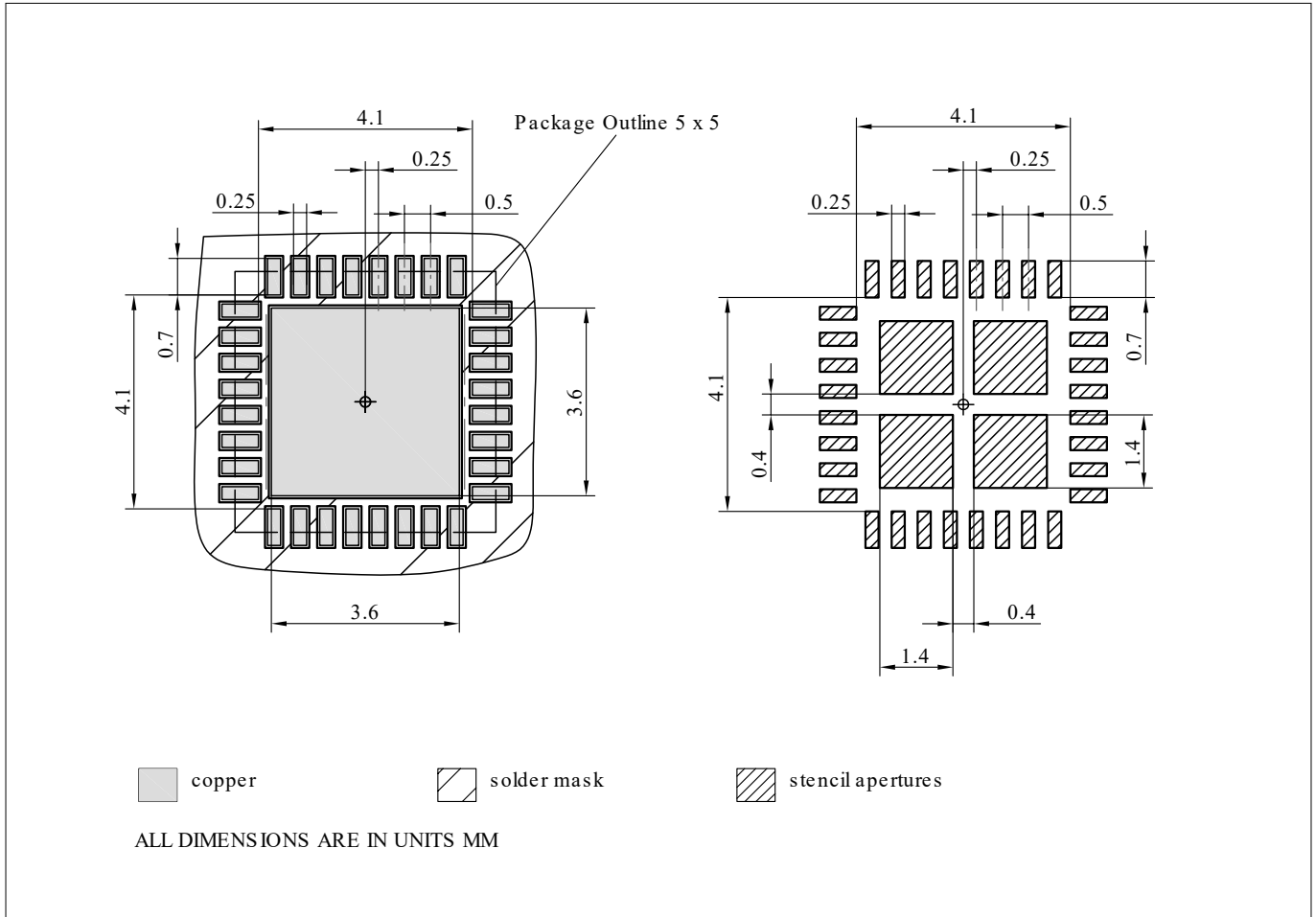


Figure 2 Tape & reel dimensions PG-UQFN-32-1,-2

**2 Delivery forms and ordering**

**2.1.2 Recommended footprint**

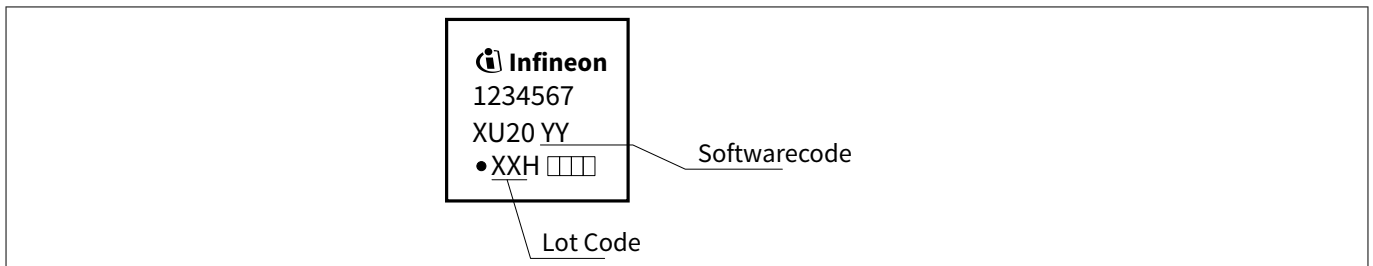
The figure below shows the recommended footprint for the PG-UQFN-32-1,-2 package. The exposed pad of the package is internally connected to GND. It shall be connected to GND externally as well.



**Figure 3 Recommended footprint PG-UQFN-32-1,-2**

**2.1.3 Chip marking**

Line 1: SLB 9672  
 Line 2: XU20 yy or AU20 yy (see [Ordering information](#) ), the <yy> is an internal FW indication (only at manufacturing due to field upgrade option)  
 Line 3: <Lot number> H <datecode>



**Figure 4 Chip marking**

For details and recommendations regarding assembly of packages on PCBs, please refer to <https://www.infineon.com/cms/en/product/packages/>

---

## 2 Delivery forms and ordering

### 2.2 Ordering information

**Table 1** Sales order code

<b>Sales code (Sales name/ Product)</b>	<b>Ordering code</b>	<b>Software code</b>	<b>Status</b>
SLB 9672XU2.0 FW16.00	SP005588472	09	Discontinued
SLB 9672AU2.0 FW16.00	SP005588478	11	Discontinued
SLB 9672XU2.0 FW16.10	SP005612365	15	Discontinued
SLB 9672AU2.0 FW16.10	SP005612363	13	Discontinued
SLB 9672XU2.0 FW16.12	SP005750341	23	Discontinued
SLB 9672AU2.0 FW16.12	SP005750322	23	Discontinued
SLB 9672XU2.0 FW16.13	SP005919744	27	Active
SLB 9672AU2.0 FW16.13	SP005919746	28	Active
SLB 9672XU2.0 FW16.24	SP006026284	43	Active
SLB 9672AU2.0 FW16.24	SP006026286	43	Active

3 Solution details

3 Solution details

3.1 Hardware

3.1.1 Electrical characteristics

This chapter lists the maximum and operating ranges for various electrical and timing parameters.

3.1.1.1 Absolute maximum ratings

Table 2 Absolute maximum ratings

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Supply Voltage	$V_{DD}$	-0.3	–	4.1	V	–
Voltage on any pin	$V_{max}$	-0.5	–	4.1	V	–
Ambient temperature	$T_A$	-40	–	85	°C	Enhanced temperature SLB 9672XU2.0 devices
Ambient temperature	$T_A$	-40	–	105	°C	Extended temperature SLB 9672AU2.0 devices
Storage temperature	$T_S$	-40	–	125	°C	–
ESD robustness HBM: 1.5 kΩ, 100 pF	$V_{ESD,HBM}$	–	–	2000	V	According to EIA/JESD22-A114-B
ESD robustness	$V_{ESD,CDM}$	–	–	500	V	According to ESD Association Standard STM5.3.1 - 1999
Latchup immunity	$I_{latch}$			100	mA	According to EIA/JESD78

**Attention:** Stresses above the maximum values listed here may cause permanent damage to the device. Exposure to absolute maximum rating conditions for extended periods may affect device reliability. Maximum ratings are absolute ratings; exceeding only one of these values may cause irreversible damage to the integrated circuit.

3.1.1.2 Functional operating range

Table 3 Functional operating range

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Supply Voltage	$V_{DD}$	3.0	3.3	3.6	V	–
		1.65	1.8	1.95	V	–
Ambient temperature	$T_A$	-40	–	85	°C	Enhanced temperature SLB 9672XU2.0 devices
Ambient temperature	$T_A$	-40	–	105	°C	Extended temperature SLB 9672AU2.0 devices
Useful lifetime		–	–	10	y	
Operating lifetime		–	–	10	y	
Average $T_A$ over lifetime		–	55	–	°C	

**3 Solution details**

**3.1.1.3 DC characteristics**

$T_A = 25^\circ\text{C}$ ,  $V_{DD} = 3.3\text{ V} \pm 0.3\text{ V}$  or  $V_{DD} = 1.8\text{ V} \pm 0.15\text{ V}$  unless otherwise noted.

**Table 4 Current consumption**

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Current Consumption in Active Mode	$I_{VDD\_Active}$			35	mA	
Current Consumption in Sleep Mode	$I_{VDD\_Sleep}$		120		$\mu\text{A}$	Pins GPIO, RST# and PIRQ# = $V_{DD}$ , CS# inactive (= $V_{DD}$ ), MOSI, MISO and SCLK don't care
Current Consumption during reset	$I_{VDD\_Reset}$		130		$\mu\text{A}$	Pin RST# active (= GND), GPIO, PIRQ#, CS#, MOSI, MISO and SCLK don't care

**Note:** Current consumption does not include any currents flowing through resistive loads on output pins!

**Note:** Device sleep mode will be entered after 50 milliseconds of inactivity after the last TPM command was executed.

**Table 5 DC characteristics of SPI interface pins (SCLK, CS#, MISO, MOSI, RST#, PIRQ#)**

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Input voltage high	$V_{IH}$	$0.7 V_{DD}$		$V_{DD}+0.5$	V	$V_{DD,typ} = 3.3\text{ V}$ , only pins SCLK, MISO, MOSI and CS#
		$0.7 V_{DD}$		$V_{DD}+0.3$	V	$V_{DD,typ} = 3.3\text{ V}$ , pin RST#
		$0.7 V_{DD}$		$V_{DD}+0.3$	V	$V_{DD,typ} = 1.8\text{ V}$
Input voltage low	$V_{IL}$	-0.5		$0.3 V_{DD}$	V	$V_{DD,typ} = 3.3\text{ V}$
		-0.3		$0.3 V_{DD}$	V	$V_{DD,typ} = 1.8\text{ V}$
Input leakage current	$I_{LEAK}$	-4		4	$\mu\text{A}$	$0\text{ V} < V_{IN} < V_{DD}$
		-4.5			mA	Pins SCLK, CS#, MISO, MOSI $-0.5\text{ V} < V_{IN} < V_{DD} + 0.5\text{ V}$ $V_{DD,typ} = 3.3\text{ V}$
		-4.5			mA	Pins SCLK, CS#, MISO, MOSI $-0.3\text{ V} < V_{IN} < V_{DD} + 0.3\text{ V}$ $V_{DD,typ} = 1.8\text{ V}$
		-2		2	$\mu\text{A}$	Pin RST# $0\text{ V} < V_{IN} < V_{DD}$
Output high voltage	$V_{OH}$	$0.9 V_{DD}$			V	$I_{OH} = -100\ \mu\text{A}$
Output low voltage	$V_{OL}$			$0.1 V_{DD}$	V	$I_{OL} = 1.5\text{ mA}$
Pad input capacitance	$C_{IN}$			10	pF	
Output load capacitance	$C_{LOAD}$			30	pF	

3 Solution details

Table 6 DC characteristics of GPIO pins

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Input voltage high	$V_{IH}$	$0.7 V_{DD}$		$V_{DD}+0.3$	V	Pins GPIO
Input voltage low	$V_{IL}$	-0.5		$0.3 V_{DD}$	V	Pins GPIO
Input leakage current	$I_{LEAK}$	-2		2	$\mu A$	$0 V < V_{IN} < V_{DD}$
Output high voltage	$V_{OH}$	$V_{DD}-0.3$			V	$I_{OH} = -1 \text{ mA}$ , pins GPIO
Output low voltage	$V_{OL}$			0.3	V	$I_{OL} = 1 \text{ mA}$ , pins GPIO
Pad input capacitance	$C_{IN}$			10	pF	Pins GPIO

3.1.1.4 AC characteristics

$T_A = 25^\circ C$ ,  $V_{DD} = 3.3V \pm 0.3V$  or  $V_{DD} = 1.8V \pm 0.15V$  unless otherwise noted.

Table 7 Power supply

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Supply voltage rise time	$t_{VDDR}$			1.0	V/ns	

Table 8 Device reset

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Cold (Power-On) Reset	$t_{POR}$	80			$\mu s$	
Warm Reset	$t_{WRST}$	2			$\mu s$	

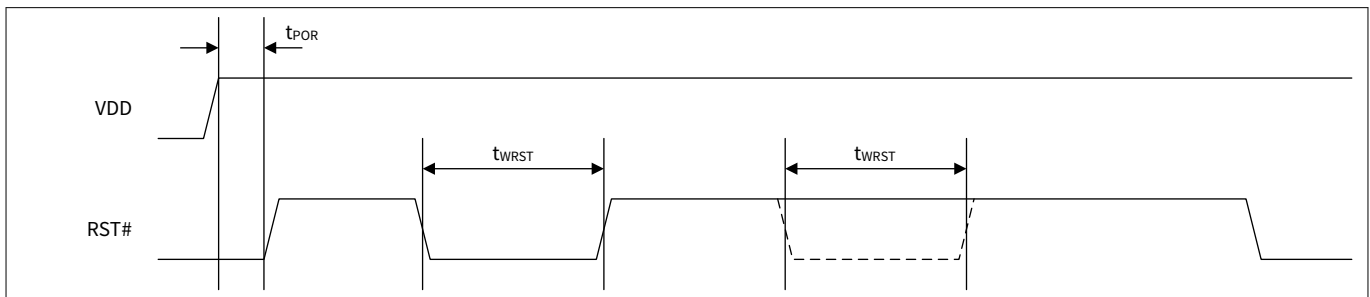


Figure 5 Reset timing

Table 9 AC characteristics of SPI interface

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
SCLK frequency	$f_{CLK}$		33	34.65	MHz	
SCLK period	$t_{CLK}$	$1/f_{CLK} - 5\%$	$1/f_{CLK}$	$1/f_{CLK} + 5\%$	$\mu s$	Rising edge to rising edge, measured at $V_{IN} = 0.5 V_{DD}$
SCLK low time	$t_{CLKL}$	$0.45 t_{CLK}$			$\mu s$	Falling edge to rising edge, measured at $V_{IN} = 0.5 V_{DD}$

(table continues...)

**3 Solution details**

**Table 9 (continued) AC characteristics of SPI interface**

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
SCLK high time	$t_{CLKH}$	$0.45 t_{CLK}$			$\mu s$	Rising edge to falling edge, measured at $V_{IN} = 0.5 V_{DD}$
SCLK slew rate (rising/falling)	$t_{SLEW}$	0.1		4	V/ns	$f_{CLK} \leq 20$ MHz, between $0.2 V_{DD}$ and $0.6 V_{DD}$
		0.27		4	V/ns	$f_{CLK} > 20$ MHz, between $0.2 V_{DD}$ and $0.6 V_{DD}$
CS# high time	$t_{CS}$	50			ns	Rising edge to falling edge
		60			ns	$V_{DD,typ} = 1.8$ V and $t_{SLEW} < 1$ V/ns, rising edge to falling edge, TPM protocol abort only
CS# setup time	$t_{CSS}$	5			ns	CS# falling edge to SCLK rising edge
		7			ns	$V_{DD,typ} = 1.8$ V and $t_{SLEW} < 1$ V/ns, CS# falling edge to SCLK rising edge
CS# hold time	$t_{CSH}$	5			ns	SCLK falling edge to CS# rising edge
MOSI setup time	$t_{SU}$	2			ns	Data setup time to SCLK rising edge
MOSI hold time	$t_H$	3			ns	Data hold time from SCLK rising edge
MISO hold time	$t_{HO}$	0			ns	Output hold time from SCLK falling edge
MISO valid delay time	$t_V$	0		$0.7 t_{CLKL}$	ns	Output valid delay from SCLK falling edge
MISO active time	$t_{DRV}$	0			ns	Delay from chip select assertion to driving of MISO

**3.1.1.5 Timing**

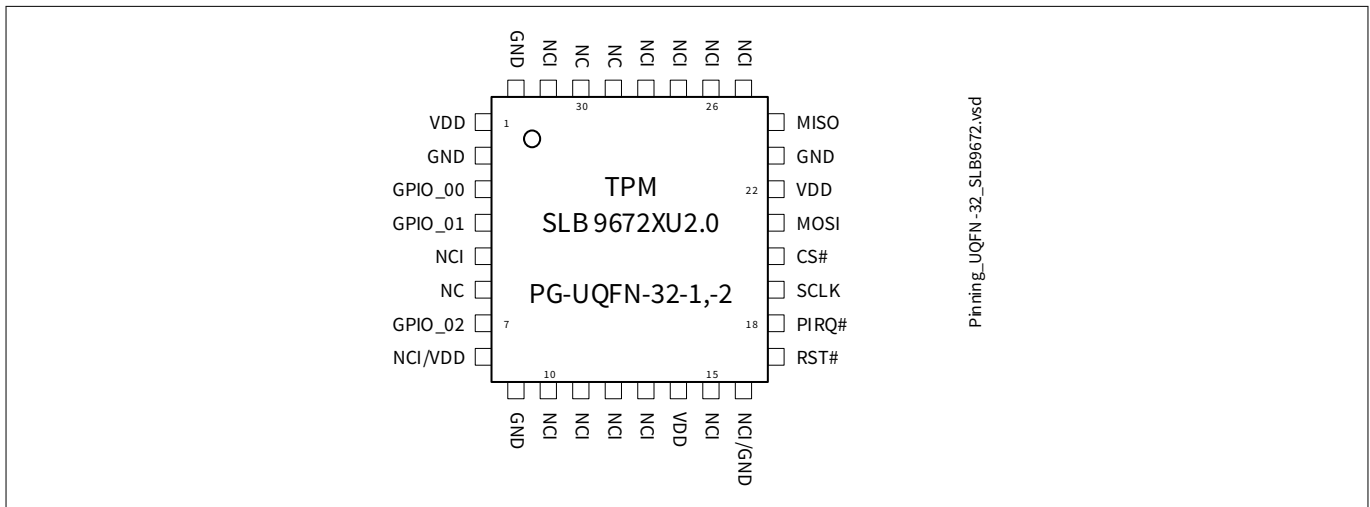
Some pads are disabled after deassertion of the reset signal for up to 500  $\mu s$ .

The SLB 9672 TPM 2.0 features security mechanisms which detect and count all resets.



**3 Solution details**

**3.1.2 Pin description**



**Figure 6 Pinout of the SLB 9672 TPM 2.0 (PG-UQFN-32-1,-2 package, top view)**

**Table 10 Buffer types**

Buffer type	Description
TS	Tri-state pin
IN	Input pin
OD	Open-drain pin

**Table 11 I/O Signals**

Pin number	Name	Pin type	Buffer type	Function
PG-UQFN-32-1,-2				
20	CS#	I	IN	Chip select The SPI chip select signal (active low).
19	SCLK	I	IN	SPI clock The SPI clock signal. Only SPI mode 0 is supported by the device.
21	MOSI	I	IN	Master out slave in (SPI data) SPI data which is received from the master.
24	MISO	O	TS	Master in slave out (SPI data) SPI data which is sent to the SPI bus master.
18	PIRQ#	O	OD	Interrupt request Interrupt request signal to the host. The pin has no internal pull-up resistor. The interrupt is active low.
17	RST#	I	IN	Reset External reset signal. Asserting this pin unconditionally resets the device. The signal is active low and is typically connected to the PCIRST# signal of the host. This pin has a weak internal pull-up resistor.

**(table continues...)**

**3 Solution details**

**Table 11 (continued) I/O Signals**

Pin number	Name	Pin type	Buffer type	Function
<b>PG-UQFN-32-1,-2</b>				
3	GPIO_00	I/O	TS	General purpose IO This pin may be left unconnected; it has an internal pull-up resistor. It can be controlled via TPM NV GPIO functionality.
4	GPIO_01	I/O	TS	General purpose IO This pin may be left unconnected; it has an internal pull-up resistor. It can be controlled via TPM NV GPIO functionality.
7	GPIO_02	I/O	TS	General purpose IO This pin may be left unconnected; it has an internal pull-up resistor. It can be controlled via TPM NV GPIO functionality.

**Table 12 Power supply**

Pin number	Name	Pin type	Buffer type	Function
<b>PG-UQFN-32-1,-2</b>				
1, 14, 22	VDD	PWR	—	Power supply All VDD pins must be connected externally and should be bypassed to GND via 100 nF capacitors.
2, 9, 23, 32	GND	GND	—	Ground All GND pins must be connected externally.

**Table 13 Not connected**

Pin number	Name	Pin type	Buffer type	Function
<b>PG-UQFN-32-1,-2</b>				
6, 29, 30	NC	NU	—	No connect All pins must not be connected externally (must be left floating).
5, 11 - 13, 15, 25 - 28, 31	NCI	—	—	Not connected internally All pins are not connected internally (can be connected externally).
10	NCI/VDD	—	—	Not connected internally This pin is not connected internally. For future use, it is recommended to either connect this pin to VDD via a pull-up resistor (preferred) or to leave this pin unconnected.
8	NCI/VDD	—	—	Not connected internally/VDD This pin is not connected internally (can be connected externally). Note that pin 8 is defined as VDD in the TCG specification [2]. To be compliant, VDD can be connected to this pin. For future use, it is recommended to connect this pin to VDD.

**(table continues...)**

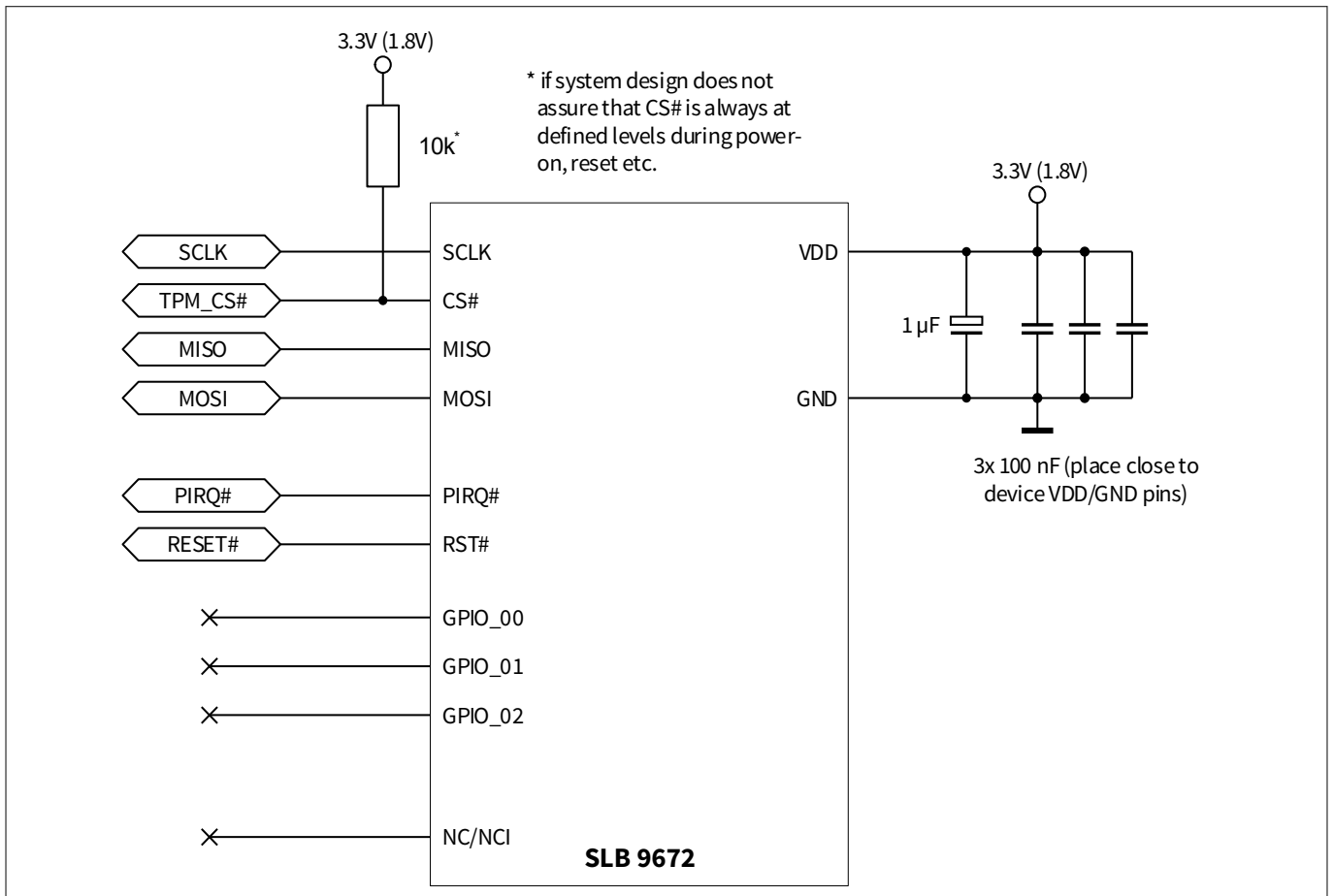
**3 Solution details**

**Table 13 (continued) Not connected**

Pin number	Name	Pin type	Buffer type	Function
PG-UQFN-32-1,-2				
16	NCI/GND	—	—	Not connected internally/GND This pin is not connected internally (can be connected externally). Note that pin 16 is defined as GND in the TCG specification [2]. To be compliant, GND can be connected to this pin. For future use, it is recommended to connect this pin to GND.

**3.1.3 Typical schematic**

The figure below shows the typical schematic for the SLB 9672 TPM 2.0. The power supply pins should be bypassed to GND with capacitors located close to the device.



**Figure 7 Typical schematic**

**3 Solution details**

**3.2 TPM embedded software**

The embedded software of the Infineon SLB 9672 TPM 2.0 is fully compliant with the TPM Library specification [1] and the PC Client Platform TPM Profile (PTP) [2], including Errata (see [3] and [4]).

This section documents vendor-specific functionality and also the actual parameters of the implementation since the specified values in [1] and [2] are only minimum requirements.

**3.2.1 Implemented algorithms**

A list of algorithms implemented in the TPM can be read using the TPM2\_GetCapability command (capability = TPM\_CAP\_ALGS).

TPM\_ALG\_AES supports CFB mode and may be used for all specified use cases (see [1]) and also for bulk encryption via the command TPM2\_EncryptDecrypt2, which is supported by this TPM.

The elliptic curve TPM\_ECC\_BN\_P256 can only be used for ECDA.

**Table 14 Implemented algorithms**

Algorithm name	Key size/curve	Mandatory (M), optional (O) per [2]	Implemented in SLB 9672 TPM 2.0
TPM_ALG_RSA	1024	SHOULD NOT BE USED	X (D)
	2048	M	X
	3072	M	X
	4096	O	X
TPM_ALG_AES	128	M	X
	192	O	X
	256	M	X
TPM_ALG_SHA1	n.a.	M/D	X (D)
TPM_ALG_SHA256	n.a.	M	X
TPM_ALG_SHA384	n.a.	M	X
TPM_ALG_ECC	TPM_ECC_NIST_P256	M	X
	TPM_ECC_NIST_P384	M	X
	TPM_ECC_BN_P256	O	X

**Note:** *TPM\_ALG\_RSA with 1024-bit and TPM\_ALG\_SHA1 support is implemented but deprecated (D). Consequently, support for these algorithms may be removed in a future version and it is not recommended to use them anymore.*

**3.2.2 Available resources**

The table below provides an overview of the available resources.

**Table 15 Available resources**

Number of PCRs (SHA-1, SHA-256 or SHA-384) (TPM_PT_PCR_COUNT) See <a href="#">Allocation of PCR banks</a> for further details.	24
Amount of free NV memory including space of predefined NV indices (4 EK certificates)	51072 Bytes

**(table continues...)**

**3 Solution details**

**Table 15 (continued) Available resources**

Amount of free NV memory without space of predefined NV indices (4 EK certificates)	45720 Bytes
Maximum number of loaded sessions (TPM_PT_HR_LOADED_MIN)	3
Maximum number of active sessions (TPM_PT_ACTIVE_SESSIONS_MAX)	64
Maximum number of loaded transient Objects (TPM_PT_HR_TRANSIENT_MIN)	3
Maximum number of loaded persistent Objects (TPM_PT_HR_PERSISTENT_MIN)	7
Maximum number of NV counters (NV Index with TPMA_NV_COUNTER set, TPM_PT_NV_COUNTERS_MAX)	0 <sup>1)</sup>
Minimum number of NV indices with TPM_NT_PIN_FAIL or TPM_NT_PIN_PASS set	2
Maximum parameter size (TPM_PT_INPUT_BUFFER)	1024 Bytes
Maximum data size for NV read or NV write (TPM_PT_NV_BUFFER_MAX)	768 Bytes
I/O-Buffer size in TPM operational mode (max. command/response size) TPM_PT_MAX_COMMAND_SIZE TPM_PT_MAX_RESPONSE_SIZE	2000 Bytes
I/O-Buffer size in TPM firmware update mode (max. command/response size) TPM_PT_MAX_COMMAND_SIZE TPM_PT_MAX_RESPONSE_SIZE	1100 Bytes

1) The value 0 indicates that there is no fixed maximum. The number of counter indices is determined by the available NV memory pool.

**3 Solution details**

**3.2.3 Command ordinal list**

The TPM implements the TCG standard commands defined in [Table 16](#) and the vendor-specific commands defined in [Table 17](#). All other ordinals will return TPM\_RC\_COMMAND\_CODE.

**Table 16 Command code list**

<b>Signals</b>	
_TPM_INIT	_TPM_HashData
_TPM_HashStart	_TPM_HashEnd
<b>Startup</b>	
TPM_CC_Startup	TPM_CC_Shutdown
<b>Testing</b>	
TPM_CC_IncrementalSelfTest	TPM_CC_SelfTest
TPM_CC_GetTestResult	
<b>Session Commands</b>	
TPM_CC_StartAuthSession	TPM_CC_PolicyRestart
<b>Object Commands</b>	
TPM_CC_Create	TPM_CC_Load
TPM_CC_LoadExternal	TPM_CC_ReadPublic
TPM_CC_ActivateCredential	TPM_CC_MakeCredential
TPM_CC_Unseal	TPM_CC_ObjectChangeAuth
TPM_CC_CreateLoaded	
<b>Duplication Commands</b>	
TPM_CC_Duplicate	TPM_CC_Import
<b>Asymmetric Primitives</b>	
TPM_CC_RSA_Encrypt	TPM_CC_RSA_Decrypt
TPM_CC_ECDH_KeyGen	TPM_CC_ECDH_ZGen
TPM_CC_ECC_Parameters	
<b>Symmetric Primitives</b>	
TPM_CC_Hash	TPM_CC_HMAC
TPM_CC_EncryptDecrypt2 [Configurable] <sup>1)</sup>	
<b>Random Number Generator</b>	
TPM_CC_GetRandom	TPM_CC_StirRandom
<b>Hash/HMAC/Event Sequences</b>	
TPM_CC_HMAC_Start	TPM_CC_HashSequenceStart
TPM_CC_SequenceUpdate	TPM_CC_SequenceComplete
TPM_CC_EventSequenceComplete	
<b>Attestation Commands</b>	
TPM_CC_Certify	TPM_CC_CertifyCreation
TPM_CC_Quote	TPM_CC_GetSessionAuditDigest

**(table continues...)**

**3 Solution details**

**Table 16 (continued) Command code list**

TPM_CC_GetTime	
<b>Anonymous Attestation</b>	
TPM_CC_Commit	
<b>Signature Verification</b>	
TPM_CC_VerifySignature	TPM_CC_Sign
<b>Integrity Collection (PCR)</b>	
TPM_CC_PCR_Extend	TPM_CC_PCR_Event
TPM_CC_PCR_Read	TPM_CC_PCR_Allocate
TPM_CC_PCR_Reset	
<b>Enhanced Authorization (EA) Commands</b>	
TPM_CC_PolicySigned	TPM_CC_PolicySecret
TPM_CC_PolicyTicket	TPM_CC_PolicyOR
TPM_CC_PolicyPCR	TPM_CC_PolicyLocality
TPM_CC_PolicyNV	TPM_CC_PolicyCounterTimer
TPM_CC_PolicyCommandCode	TPM_CC_PolicyCpHash
TPM_CC_PolicyNameHash	TPM_CC_PolicyDuplicationSelect
TPM_CC_PolicyAuthorize	TPM_CC_PolicyAuthValue
TPM_CC_PolicyPassword	TPM_CC_PolicyGetDigest
TPM_CC_PolicyNvWritten	TPM_CC_PolicyTemplate
TPM_CC_PolicyAuthorizeNV	
<b>Hierarchy Commands</b>	
TPM_CC_CreatePrimary	TPM_CC_HierarchyControl
TPM_CC_SetPrimaryPolicy	TPM_CC_ChangePPS
TPM_CC_ChangeEPS [Configurable] <sup>1)</sup>	TPM_CC_Clear
TPM_CC_ClearControl	TPM_CC_HierarchyChangeAuth
<b>Dictionary Attack Functions</b>	
TPM_CC_DictionaryAttackLockReset	TPM_CC_DictionaryAttackParameters
<b>Context Management</b>	
TPM_CC_ContextSave	TPM_CC_ContextLoad
TPM_CC_FlushContext	TPM_CC_EvictControl
<b>Clocks and Timers</b>	
TPM_CC_ReadClock	TPM_CC_ClockSet
TPM_CC_ClockRateAdjust	
<b>Capability Commands</b>	
TPM_CC_GetCapability	TPM_CC_TestParms
<b>Non-Volatile Storage</b>	
TPM_CC_NV_DefineSpace	TPM_CC_NV_UndefineSpace

**(table continues...)**

**3 Solution details**

**Table 16 (continued) Command code list**

TPM_CC_NV_UndefineSpaceSpecial	TPM_CC_NV_ReadPublic
TPM_CC_NV_Write	TPM_CC_NV_Increment
TPM_CC_NV_Extend	TPM_CC_NV_SetBits
TPM_CC_NV_WriteLock	TPM_CC_NV_Read
TPM_CC_NV_ReadLock	TPM_CC_NV_ChangeAuth
TPM_CC_NV_Certify	

1) See [TPM2\\_SetCapabilityVendor](#) for configuration

**Note:** [Table 17](#) does not comprehensively list all vendor-defined TPM commands.

**Table 17 Vendor-specific TPM\_CC constants**

Name	Command code	NV write	Decrypt	Encrypt	Description
TPM_CC_SetCapabilityVendor	0x20000400	Y	N	N	Vendor-specific command to enable/disable and lock of configurable commands. Refer to <a href="#">TPM2_SetCapabilityVendor</a> for further details.
TPM_CC_FullFipsSelfTestVendor	0x20000401	N	N	N	Vendor specific command for executing all selftests which are performed at first power-up. Refer to <a href="#">TPM2_FullFipsSelfTestVendor</a> for further details.
TPM_CC_FieldUpgradeStartVendor	0x2000012F	Y	N	N	Vendor specific command for starting TPM firmware update mode while in TPM operational mode. Refer to <a href="#">TPM2_FieldUpgradeStartVendor</a> for further details.
TPM_CC_FieldUpgradeAbandonVendor	0x20000130	N	N	N	Vendor specific command for aborting the field upgrade while in TPM firmware update mode. Refer to <a href="#">TPM2_FieldUpgradeAbandonVendor</a> for further details.

**(table continues...)**



**3 Solution details**

**Table 17 (continued) Vendor-specific TPM\_CC constants**

<b>Name</b>	<b>Command code</b>	<b>NV write</b>	<b>Decrypt</b>	<b>Encrypt</b>	<b>Description</b>
TPM_CC_FieldUpgradeManifestVendor	0x20000131	Y	N	N	Vendor specific command for validating the manifest while in TPM firmware update mode. Refer to <a href="#">TPM2_FieldUpgradeManifestVendor</a> for further details.
TPM_CC_FieldUpgradeDataVendor	0x20000132	Y	N	N	Vendor specific command for updating the firmware while in TPM firmware update mode. Refer to <a href="#">TPM2_FieldUpgradeDataVendor</a> for further details.
TPM_CC_FieldUpgradeFinalizeVendor	0x20000133	Y	N	N	Vendor-specific command for finalizing the field upgrade process in TPM operational mode. Refer to <a href="#">TPM2_FieldUpgradeFinalizeVendor</a> for further details.

### 3 Solution details

#### 3.2.4 Generation of RSA keys

##### 3.2.4.1 Pre-generation of RSA keys

The TPM provides pre-generation of 2048-bit RSA keys in the background during idle times. A maximum of seven 2048-bit RSA keys can be generated and stored in non-volatile memory without any impact on the available amount of free non-volatile memory as stated in [Table 15](#). When the user instructs the TPM to generate a new 2048-bit ordinary RSA key using TPM2\_Create or TPM2\_CreateLoaded, one of the pre-generated keys (if available) will be picked and returned. If the user demands more keys than the number of currently available pre-generated keys, the TPM will need to generate new keys in place, which will increase the total response time. All pre-generated keys will be discarded if command TPM2\_StirRandom is sent to the TPM and reseeding of TPM Random Number Generator (RNG) is triggered.

Pre-generation is only supported for (RSA 2k) Ordinary keys. Pre-generation of Primary and Derived keys are not supported because their generation depends on caller-provided data. Pre-generation of any key types other than RSA is not supported because there is no performance advantage.

**Note:** *The key pre-generation is activated after TPM2\_SelfTest has been executed after a reset (\_TPM\_INIT). Pre-generation of RSA 3072- and 4096-bit keys is not supported.*

##### 3.2.4.2 Generation of RSA 3072- and 4096-bit keys

The creation of a 3072- or 4096-bit RSA primary key may take several minutes. For this reason, the duration of TPM2\_CreatePrimary may violate the configured driver timeout value when waiting for the response of TPM2\_CreatePrimary. For example, the Linux Kernel v4.17 or higher uses a timeout value of 300 seconds for TPM2\_CreatePrimary. This value may also be violated in some cases.

For Windows 10 or 11, when using a 3072-bit RSA key, update the following key if it exists in the registry editor:  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TPM]  
"TimeoutCommandCreate" = dword:02000000

**3 Solution details**

**3.2.5 Non-volatile storage**

**3.2.5.1 Predefined NV indices**

The sizes documented in [Table 18](#) are typical values and may vary by some bytes. The actual size can be read from the TPM using the command TPM2\_NV\_ReadPublic where parameter nvIndex defines the certificate whose size is to be determined.

**Note:** *The validity period of the EK certificate spans 15 years starting with production. This covers the validity for an expected lifetime of 10 years plus a buffer of 5 years between production and TPM assembly.*

**Table 18 Predefined NV indices**

Value	Index Name	Default Size	Attributes
0x01C00002	RSA 2048 EK Certificate	1427 bytes (RSA Endorsement Key Certificate)	see <a href="#">Table 19</a>
0x01C0000A	ECC NIST P256 EK Certificate	844 bytes (ECC Endorsement Key Certificate)	see <a href="#">Table 19</a>
0x01C00016	ECC NIST P384 EK Certificate	873 bytes (ECC Endorsement Key Certificate)	see <a href="#">Table 19</a>
0x01C0001C	RSA 3072 EK Certificate	The size of the RSA Endorsement Key Certificate is typically 1560 bytes but may vary by some bytes. The actual size can be read from the TPM using the command TPM2_NV_ReadPublic(nvIndex = RSA 3072 EK Certificate).	see <a href="#">Table 19</a>

**Table 19 Attributes of predefined NV indices**

Attributes
TPMA_NV_PPWRITE
TPMA_NV_WRITEDEFINE
TPMA_NV_PPREAD
TPMA_NV_OWNERREAD
TPMA_NV_AUTHREAD
TPMA_NV_NO_DA
TPMA_NV_WRITTEN
TPMA_NV_PLATFORMCREATE

**3 Solution details**

**3.2.6 Vendor-specific functionality**

This section describes vendor-specific functionality, such as vendor-specific properties, commands and default values/settings, which extends the functionality described in the TPM Library specification [1].

**3.2.6.1 Power saving mode**

The TPM supports a reduced power consumption mode which is entered after inactivity for at least 50 ms has been detected. The resulting power consumption in this mode is shown in Table 4 (current consumption in sleep mode).

**3.2.6.2 TPM and vendor properties**

Properties defined within the TPM can be read with the command TPM2\_GetCapability. The values are vendor dependent or determined by a platform-specific specification. The following properties are returned by the Infineon SLB 9672 TPM 2.0 using the command TPM2\_GetCapability (capability = TPM\_CAP\_TPM\_PROPERTIES):

**Table 20 Infineon TPM property values**

TPM_PT_MANUFACTURER	“IFX”
TPM_PT_VENDOR_STRING_1	“SLB9”
TPM_PT_VENDOR_STRING_2	“672”
TPM_PT_VENDOR_STRING_3	NULL
TPM_PT_VENDOR_STRING_4	NULL
TPM_PT_FIRMWARE_VERSION_1	Major and minor version (for instance, 0x00100018 indicates V16.24) <sup>1)</sup>
TPM_PT_FIRMWARE_VERSION_2	Build number and Common Criteria certification state (for instance, 0x004A8C00 or 0x004A8C02) <sup>1)</sup> Byte 1: reserved for future use (0x00) Byte 2 and 3: Build number (for instance, 0x4A8C) <sup>1)</sup> Byte 4: Common Criteria certification state/mode: 0x00 = TPM operational mode/TPM is CC certified 0x02 = TPM operational mode/TPM is not certified 0x62 = TPM firmware update mode
TPM_PT_MODES	Bit 0 (FIPS_140_2) = 1 Bits 1..31 = 0

1) The build- and version numbers given here are examples and do not necessarily match the numbers of the device this datasheet has been provided for.

The vendor-specific properties shown in the table below can be read by using the vendor-specific capability selector TPM\_CAP\_VENDOR\_PROPERTIES:

**Table 21 Infineon vendor-specific property constants**

TPM property	Value	Property value
PT_VENDOR_FIX	0x80000000	The group of fixed vendor specific properties.
PT_VENDOR_VAR	0xC0000000	The group of variable vendor specific properties.

**3 Solution details**

**Table 22 Infineon vendor-specific property values**

<b>TPM property</b>	<b>Value</b>	<b>Property value</b>
TPM_PT_VENDOR_FIX_FU_COUNTER	PT_VENDOR_FIX + 3	UINT16 field upgrade counter for upgrades to different firmware version
TPM_PT_VENDOR_FIX_FU_COUNTER_SAME	PT_VENDOR_FIX + 4	UINT16 field upgrade counter for upgrades to same firmware version
TPM_PT_VENDOR_FIX_FU_START_HASH_DIGEST	PT_VENDOR_FIX + 5	TPMT_HA structure containing manifest hash digest for field upgrade: Bytes 1-2: Hash digest algorithm (TPM_ALG_SHA384, TPM_ALG_SHA512) Bytes 3-66: SHA512 manifest digest or Bytes 3-50: SHA384 manifest digest or
TPM_PT_VENDOR_FIX_FU_OPERATION_MODE	PT_VENDOR_FIX + 7	UINT8 operation mode of firmware as described in <a href="#">Table 23</a>
TPM_PT_VENDOR_FIX_FU_KEYGROUP_ID	PT_VENDOR_FIX + 8	UINT32 ID of field upgrade keys
TPM_PT_VENDOR_VAR_ENCRYPTDECRYPT2	PT_VENDOR_VAR + 5	Bytes 1-2: 0x0001 means feature is enabled Bytes 3-4: 0x0001 means feature is permanently locked
TPM_PT_VENDOR_VAR_CHANGEEPS	PT_VENDOR_VAR + 6	Bytes 1-2: 0x0001 means feature is enabled Bytes 3-4: 0x0001 means feature is permanently locked
TPM_PT_VENDOR_VAR_TPMID_NV	PT_VENDOR_VAR + 7	Bytes 1-2: 0x0001 means feature is enabled Bytes 3-4: 0x0001 means feature is permanently locked

An overview of all possible values returned for the operation mode is given in the following table:

**Table 23 TPM operation modes**

<b>Operation Mode</b>	<b>Description</b>
0x00	Normal TPM operational mode
0x01	TPM firmware update mode when abandoning the field upgrade process is possible
0x02	TPM firmware update mode when abandoning the field upgrade process is not possible anymore
0x03	After successful field upgrade, but before TPM2_FieldUpgradeFinalizeVendor
0x04	After TPM2_FieldUpgradeFinalizeVendor or TPM2_FieldUpgradeAbandonVendor until the next reboot

The next table lists FIFO Configuration registers initialized by the vendor.

**3 Solution details**

**Table 24 FIFO configuration registers**

Register	Value	Comments
TPM_VID	0x15d1	Vendor identification of Infineon Technologies AG
TPM_DID	0x001d	Device identification
TPM_RID	0x36	Revision identification register

**Table 25 TPM\_RID register value description**

Bit	Description
0	TPM 1.2 if set
1	TPM 2.0 if set
2	FIPS if set
3	Reserved for future use, value 0
4-7	Interface revision, currently 0011 <sub>B</sub>

**3.2.6.3 Selftest operations**

**3.2.6.3.1 TPM2\_SelfTest**

This command executes all selftests except for the tests which are only performed at first power-up (see [Table 28](#) for further details). The selftest can be done in two ways. TPM2\_Selftest(fullTest = YES) always performs all tests while TPM2\_Selftest(fullTest = NO) only executes tests which have not been run yet.

**3.2.6.3.2 TPM2\_FullFipsSelfTestVendor**

This command executes on demand all selftests which are performed at first power-up as required by FIPS 140-2. The selftest result can be read using the command TPM2\_GetTestResult.

**Table 26 Incoming operands and sizes**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_FullFipsSelfTestVendor

**Table 27 Outgoing operands and sizes**

Type	Name	Description
TPM_ST	tag	
UINT32	responseSize	
TPM_RC	responseCode	

**3.2.6.3.3 TPM2\_GetTestResult**

The TPM will return to the caller with outData = 11 bytes consisting of

- 4 bytes: a bit field describing the result of the passed selftests
- 4 bytes: a bit-field describing the not yet executed selftests
- 2 bytes: internal information
- 1 byte: operation mode (see [Table 23](#))

**3 Solution details**

The mapping of the individual bits to the corresponding selftest which is executed by the command TPM2\_SelfTest is shown in Table 28 below. The bit mapping of the selftests performed by TPM2\_FullFipsSelfTestVendor is listed in Table 29 (bit == 1 means that the test passed, RFU bits are reserved for future use).

**Table 28 TPM2\_SelfTest bit mapping of TPM2\_SelfTest**

Bit	Meaning	Bit	Meaning
31-21	RFU	10	RFU
20	AES-CFB-128	9	RSA PKCS1 2048
19-16	RFU	8-6	RFU
15	Sensortest	5	SHA384
14	RFU	4	RFU
13	TPM Firmware Integrity App Partial	3	SHA1
12	RFU	2-1	RFU
11	TRNG	0	ECC Sign

**Table 29 TPM2\_SelfTest bit mapping of TPM2\_FullFipsSelfTestVendor**

Bit	Meaning	Bit	Meaning
31-21	RFU	9	RSA PKCS1 2048
20	AES-CFB-128	8	KDFe
19	RSA PKCS1 3072	7	KDFa SHA256
18-16	RFU	6	RFU
15	Sensortest	5	SHA384
14	TPM Firmware Integrity App Full	4	RFU
13	TPM Firmware Integrity App Partial	3	SHA1
12	TPM Firmware Integrity OS Full	2	ECC ECDH
11	TRNG	1	RFU
10	DRNG	0	ECC Sign

The next table below shows the expected result returned after a successful selftest command:

**Table 30 TPM2\_SelfTest result**

Selftest command	Passed selftests (first 4 bytes of outData) returned by TPM2_GetTestResult
TPM2_FullFipsSelfTestVendor	0x00, 0x18, 0xFF, 0xAD
TPM2_SelfTest	0x00, 0x10, 0xAA, 0x29

**3.2.6.4 Dictionary attack default values**

Besides other security mechanisms, the TPM 2.0 supports protection against guessing or exhaustive searches of authorization values stored in the device (see [1] for further details). To provide suitable protection, the parameters for this dictionary attack protection need to be chosen carefully. The command

### 3 Solution details

TPM2\_DictionaryAttackParameters is used to program these values into the TPM. The following parameters are set as factory default:

- maxTries: 32
- recoveryTime: 7200 seconds
- lockoutRecovery: 86400 seconds

#### 3.2.6.5 RSA signing scheme

RSASSA-PSS signing operation uses the digest size for the salt. RSASSA-PSS signature verification may only succeed if the size of the used salt is from 0 to digest size, or equals (key size) - (digest size) - 2.

#### 3.2.6.6 NV index attribute TPMA\_NV\_WRITTEN

The TPMA\_NV\_WRITTEN bit is set if an NV index write operation completed successfully; otherwise, it is not set. Additionally, the TPMA\_NV\_WRITTEN bit is also cleared before writing data to an NV index and only set again if data has been completely written to an NV index.

As a consequence, the TPMA\_NV\_WRITTEN bit will not be set if a write to a NV index was discontinued (for instance, due to a reset or a power loss of the device during that write operation).

This allows checking the consistency of data of an NV index. If an NV index contains inconsistent data due to a discontinued write operation, the TPMA\_NV\_WRITTEN bit is 0.

#### 3.2.6.7 Allocation of PCR banks

This TPM supports only one bank of PCRs, default allocation is Hash Algorithm ID 0x000B (SHA256). The TPM2\_PCR\_Allocate command can be used to change the allocation of the PCR bank as described in [1] Part 1, chapter 17.8 and [1] Part 3, chapter 22.5.

#### 3.2.6.8 General purpose I/O (GPIO)

All GPIO pins described in Table 11 are mapped to ordinary NV indices with the corresponding handle values listed in the table below.

**Table 31 Mapping of GPIO indices**

GPIO name	TPM_NV_INDEX
GPIO_00	0x01C40000
GPIO_01	0x01C40001
GPIO_02	0x01C40002

The NV GPIO functionality complies with [2], section 4.5.4.1 General Purpose I/O (GPIO). The TPM NV commands are used to access the NV GPIO pins.

##### 3.2.6.8.1 TPM2\_NV\_DefineSpace

Before a NV GPIO pin can be used, an NV Index must be defined with TPM2\_NV\_DefineSpace:

- nvIndex handle must be set to a handle value in Table 31
- dataSize must be 1
- index type must be TPM\_NT\_ORDINARY
- attribute TPMA\_NV\_WRITEALL must be CLEAR

If TPMA\_NV\_CLEAR\_STCLEAR is CLEAR, the written GPIO state is preserved across TPM Reset and TPM Restart.

**Note:** All other NV index attributes have the same meaning as for a conventional NV Index.



**3 Solution details**

**3.2.6.8.2 TPM2\_NV\_Write**

TPM2\_NV\_Write will configure the GPIO pin as output pin and set the pin value:

- write 1 byte at offset 0
- data = 1 will set the GPIO output to high level (1)
- data = 0 will set the GPIO output to low level (0)

**Note:** *data > 1 will also set the GPIO output to high level (1).*

**3.2.6.8.3 TPM2\_NV\_Read**

TPM2\_NV\_Read will configure the GPIO pin as input pin and read the pin value:

- read 1 byte at offset 0
- data = 1 means the GPIO input is at high level (1)
- data = 0 means the GPIO input is at low level (0)

**Note:** *Reading the GPIO NV index will succeed even if TPMA\_NV\_WRITTEN is CLEAR.*

**3.2.6.8.4 TPM2\_NV\_UndefineSpace**

TPM2\_NV\_UndefineSpace will undefine the NV index used to access the GPIO pin. After TPM2\_UndefineSpace, the GPIO pin is in the same state as after power on. The GPIO state is set to ‘off’ with a weak pullup.

**3.2.6.9 TPM2\_SetCapabilityVendor**

The TPM2\_SetCapabilityVendor command allows configuration of some TPM features. It is possible to enable or disable the TPM2\_EncryptDecrypt2 and TPM2\_ChangeEPS commands. The availability of the TPM Unique ID (see [TPM unique identifier](#)) can also be changed. Platform authorization is required to configure these features. The configuration of every feature can be lifetime locked separately. The default configuration is shown in the following table and can be read via TPM2\_GetCapability (see [Table 22](#)).

**Table 32 Default capability settings**

Feature	Enabled/disabled	Locked/unlocked
TPM2_EncryptDecrypt2	Enabled	Unlocked
TPM2_ChangeEPS	Enabled	Unlocked
TPM unique ID NV index	Enabled	Unlocked

**Note:** *For operation in FIPS 140-2 approved mode, it is not allowed to disable command TPM2\_ChangeEPS and lifetime lock this configuration state.*

**Table 33 Incoming operands and sizes**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_SetCapabilityVendor
TPMI_RH_PLATFORM	@authorization	TPM_RH_PLATFORM Auth Index: 1 Auth Role: ADMIN

**(table continues...)**

**3 Solution details**

**Table 33** (continued) **Incoming operands and sizes**

<b>Type</b>	<b>Name</b>	<b>Description</b>
TPM_PT	Property	Property to be set
UINT32	value	New property value

**Table 34** **Outgoing operands and sizes**

<b>Type</b>	<b>Name</b>	<b>Description</b>
TPM_ST	tag	
UINT32	responseSize	
TPM_RC	responseCode	

**Table 35** **Error return codes**

<b>Type</b>	<b>Meaning</b>
TPM_RC_VALUE	Property value is not valid

**3 Solution details**

**3.2.6.10 Field upgrade**

The SLB 9672 TPM 2.0 has two different modes of operation. One mode is the normal TPM operational mode with the capability to execute all TPM 2.0 commands, the other mode is the TPM firmware update mode in which the capabilities of the TPM 2.0 are limited to those commands necessary to perform a successful field upgrade.

After successfully executing the TPM2\_FieldUpgradeStartVendor command, the SLB 9672 TPM 2.0 transitions from normal TPM operational mode to TPM firmware update mode. Once in the mode for updating TPM firmware, the manifest has to be transmitted using TPM2\_FieldUpgradeManifestVendor. The size of a typical manifest necessitates multiple calls to TPM2\_FieldUpgradeManifestVendor. After sending the complete manifest, the TPM2\_FieldUpgradeDataVendor command must be invoked as many times as required to send the entire field upgrade image in multiple blocks. After the firmware has been completely updated, the command TPM2\_FieldUpgradeFinalizeVendor completes the field upgrade process and returns the TPM to its operational mode. During TPM firmware update mode, the TPM 2.0 standard command format is used.

The TPM field upgrade protected capability is divided into several commands. The next sections list these different commands.

If the field upgrade process is not completed successfully (hence leaving an invalid TPM firmware), the TPM enters failure mode. After a reboot, the command sequence to execute the field upgrade process again will be allowed starting with the command TPM2\_FieldUpgradeManifestVendor.

The TPM is provided with two counters (field upgrade counters), which limit the number of field upgrade attempts. A total maximum of 1256 field upgrades is possible. For field upgrades to the same firmware version an additional constraint of 256 attempts applies. The number of counted attempts for field upgrades to the same version is reset when field upgrade to a newer version was applied. Interrupted or failed upgrades will increment the field upgrade counters as well. When one of the counters reaches its maximum, no further field upgrade to any firmware version or to the same firmware version is possible and the command TPM2\_FieldUpgradeManifestVendor will return 'TPM\_RC\_FAILURE'. Care should be taken during the last available attempt: if interrupted, the TPM will remain in TPM firmware update mode and will not be usable anymore.

**3.2.6.10.1 Structures and definitions**

**3.2.6.10.2 TPM2B\_MAX\_BUFFER\_VENDOR**

**Table 36 TPM2B\_MAX\_BUFFER\_VENDOR structure definition**

Type	Name	Description
uint16_t	size	Size of buffer
uint8_t[size]	buffer	Buffer

**3.2.6.10.3 TPML\_MAX\_BUFFER**

**Table 37 TPML\_MAX\_BUFFER structure definition**

Type	Name	Description
uint32_t	count	Number of properties
TPM2B_MAX_BUFFER_VENDOR	vendorData	List of property values

**3 Solution details**

**3.2.6.10.4 Commands in TPM operational mode**

**TPM2\_FieldUpgradeStartVendor**

This command can be used to start the field upgrade process.

This command requires authorization with platformPolicy.

**Note:** *The command is not available when the TPM is in TPM firmware update mode. After successful execution of the command, the TPM operates in TPM firmware update mode.*

**Note:** *A dead time of 300 ms must be considered before sending the first command within TPM firmware update mode.*

**Table 38 Incoming operands and sizes**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_FieldUpgradeStartVendor
TPM_RH_PLATFORM	@authorization	TPM_RH_PLATFORM Auth Index: 1 Auth Role: ADMIN
UINT8	type	type that defines the content of data
TPM2B_MAX_BUFFER	data	For type = 0x01: buffer contains a TPMT_HA structure with a hash algorithm and digest value of the manifest

**Table 39 Outgoing operands and sizes**

Type	Name	Description
TPM_ST	tag	
UINT32	responseSize	
TPM_RC	responseCode	
UINT16	reserved	set to 0x0000

**Table 40 Error return codes**

Return Code	Meaning
TPM_RC_POLICY_FAIL	A policy check failed
PM_RC_SIZE	The size of the digest is invalid
TPM_RC_VALUE	Type or hash algorithm value is not valid
TPM_RC_HANDLE	The handle is not correct for this usage
TPM_RC_FAILURE	The command failed

**Note:** *Other return codes may occur; they are compliant with [1] Part 2, chapter 6.6.*

**3 Solution details**

**TPM2\_FieldUpgradeFinalizeVendor**

This is the last command of the field upgrade process. After execution of this command, a power cycle or a reset cycle is required.

**Table 41 Incoming operands and sizes**

Type	Name	Description
TPM_ST_COMMAND_TAG	tag	TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_FieldUpgradeFinalizeVendor
TPM2B_MAX_BUFFER	data	Reserved for future use, must be zero

**Table 42 Outgoing operands and sizes**

Type	Name	Description
TPM_ST	tag	
UINT32	responseSize	
TPM_RC	responseCode	

**Table 43 Error return codes**

Return Code	Meaning
TPM_RC_BAD_TAG	Incorrect tag
TPM_RC_FAILURE	The command failed
TPM_RC_REBOOT	Indicates that a reboot is required

**3 Solution details**

**3.2.6.10.5 Commands in TPM firmware update mode**

**TPM2\_FieldUpgradeManifestVendor**

This command validates and processes the manifest and increments the field upgrade counters. It requires that TPM2\_FieldUpgradeStartVendor has been executed before. Since the manifest exceeds a limit of 1024 bytes, it must be splitted into chunks of 1024 bytes or smaller. The parameter processingInfo must be used accordingly to signal chained transmission of the manifest.

After successful execution of TPM2\_FieldUpgradeManifestVendor aborting the field upgrade process is still possible by executing the command TPM2\_FieldUpgradeAbandonVendor. If power loss occurs before sending the first TPM2\_FieldUpgradeDataVendor, the field upgrade process can be restarted after a reboot by resending TPM2\_FieldUpgradeManifestVendor. Alternatively, it can be aborted after the reboot by TPM2\_FieldUpgradeAbandonVendor.

**Table 44 Incoming operands and sizes**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_FieldUpgradeManifestVendor
UINT8	processingInfo	0 = last block 1 = first block 2 = consecutive block
TPM2B_MAX_BUFFER	data	Block of the signed manifest

**Table 45 Outgoing operands and sizes**

Type	Name	Description
TPM_ST	tag	
UINT32	responseSize	
TPM_RC	responseCode	

**Table 46 Error return codes**

Return Code	Meaning
TPM_RC_COMMAND_SIZE	Incorrect command size
TPM_RC_BAD_TAG	Incorrect tag
TPM_RC_LOCALITY	The locality is not correct
TPM_RC_AUTH_FAIL	Manifest validation failed
TPM_RC_DISABLED	The command has already been executed successfully before
TPM_RC_TOO_MANY_CONTEXTS	TPM2_FieldUpgradeDataVendor has been executed before
TPM_RC_FAILURE	The command failed

**TPM2\_FieldUpgradeDataVendor**

This command shall be called as often as necessary until the complete firmware is upgraded. It requires that either TPM2\_FieldUpgradeManifestVendor or TPM2\_FieldUpgradeDataVendor has been executed before.

After sending the first TPM2\_FieldUpgradeDataVendor the field upgrade process cannot be aborted anymore by the command TPM2\_FieldUpgradeAbandonVendor. If power loss occurs after sending the first

**3 Solution details**

TPM2\_FieldUpgradeDataVendor, the field upgrade process must be restarted after a reboot by resending TPM2\_FieldUpgradeManifestVendor.

**Note:** A dead time of 300 ms should be considered before sending the next command.

**Table 47 Incoming operands and sizes**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_FieldUpgradeDataVendor
TPM2B_MAX_BUFFER	fuData	Encrypted field upgrade image data block

**Table 48 Outgoing operands and sizes**

Type	Name	Description
TPM_ST	tag	
UINT32	responseSize	
TPM_RC	responseCode	

**Table 49 Error return codes**

Return Code	Meaning
TPM_RC_COMMAND_SIZE	Incorrect command size
TPM_RC_BAD_TAG	Incorrect tag
TPM_RC_LOCALITY	The locality is not correct
TPM_RC_AUTH_MISSING	Manifest validation using TPM2_FieldUpgradeManifestVendor is required
TPM_RC_FAILURE	The command failed

**TPM2\_FieldUpgradeAbandonVendor**

This command allows aborting the field upgrade process and switching back to the TPM operational mode after a system reset is performed. Aborting the field upgrade process is no longer possible if TPM2\_FieldUpgradeDataVendor was successfully executed before (at least once).

**Note:** A dead time of 300 ms should be considered before sending the next command.

**Table 50 Incoming operands and sizes**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_FieldUpgradeAbandonVendor
TPM2B_MAX_BUFFER	data	Optional data

**Table 51 Outgoing operands and sizes**

Type	Name	Description
TPM_ST	tag	

(table continues...)

**3 Solution details**

**Table 51 (continued) Outgoing operands and sizes**

Type	Name	Description
UINT32	responseSize	
TPM_RC	responseCode	

**Table 52 Error return codes**

Return Code	Meaning
TPM_RC_COMMAND_SIZE	Incorrect command size
TPM_RC_BAD_TAG	Incorrect tag
TPM_RC_LOCALITY	The locality is not correct
RPM_RC_DISABLED	Abandon is not possible anymore
TPM_RC_FAILURE	The command failed

**TPM2\_GetCapability**

While in TPM firmware update mode, this command can be used to read the TPM properties listed in [Table 20](#) (except for TPM\_PT\_MODES) and vendor-specific properties shown in [Table 22](#). The result is returned as TPML\_MAX\_BUFFER (see [TPML\\_MAX\\_BUFFER](#) for definition).

**Note:** *In TPM firmware update mode, the TPM returns always only one single value at a time when TPM2\_GetCapability is used. This deviates from the behavior when TPM2\_GetCapability is used in normal TPM operational mode.*

**TPM2\_Selftest**

In TPM firmware update mode this command can be used to execute on demand all selftests relevant for the field upgrade process, which are performed at first power-up. The selftest result can be read using the command TPM2\_GetTestResult as described below.

**Table 53 Incoming operands and sizes**

Type	Name	Description
TPMI_ST_COMMAND_TAG	tag	TPM_ST_NO_SESSIONS
UINT32	commandSize	
TPM_CC	commandCode	TPM_CC_SelfTest

**Table 54 Outgoing operands and sizes**

Type	Name	Description
TPM_ST	tag	
UINT32	responseSize	
TPM_RC	responseCode	

**TPM2\_GetTestResult**

In TPM firmware update mode, the TPM will return to the caller with outData = 11 bytes consisting of

- 4 bytes: a bit field describing the result of the passed selftests
- 4 bytes: a bit-field describing the not yet executed selftests
- 2 bytes: internal information
- 1 byte: operation mode (see [Table 23](#))



**3 Solution details**

The mapping of the individual bits to the corresponding selftest is shown in the table below (bit == 1 means that the test passed, RFU bits are reserved for future use).

**Table 55 TPM2\_GetTestResult bit mapping in TPM firmware update**

Bit	Meaning	Bit	Meaning
31-22	RFU	15	Sensortest
21	ECDSA Verify P521 <sup>1)</sup>	14-7	RFU
20-19	RFU	6	SHA512
18	KDF AES256 CMAC	5	SHA384
17	AES256 ECB	4	SHA256
16	RFU	3-0	RFU

1) This selftest is only performed at first power up or if TPM2\_SelfTest command is executed.

**TPM2\_Startup and TPM2\_Shutdown**

TPM2\_Startup and TPM2\_Shutdown are implemented, but only to satisfy requests of a host platform when TPM is in TPM firmware update mode. Both commands are not part of the authenticated field upgrade sequence and do not have any impact when called in the TPM firmware update mode.

**3.2.7 TPM unique identifier**

When the TPM is integrated into a non-user device (such as an embedded device, network equipment, etc.), unique identification of such a device is of critical importance while device privacy is not a critical concern. For this use case, the TPM supports reading out the TPM Unique ID at NV Index 0x01C20000 using TPM2\_NV\_Read with platform authorization. TPM Unique ID has a permanent value which does not change over the TPM lifetime and is guaranteed to be unique across Infineon TPMs. The availability of the TPM Unique ID can be configured as described in [TPM2\\_SetCapabilityVendor](#).

---

### 3 Solution details

#### 3.2.8 Reset timing

The TPM\_ACCESS\_x.tpmEstablishment bit has the correct value and the TPM\_ACCESS\_x.tpmRegValidSts bit is set within 500  $\mu$ s after RST# is deasserted.

**Note:** *Access of any TPM SPI interface register is not allowed while RST# is asserted and within 500  $\mu$ s after deassertion of RST#. If the TPM is in TPM firmware update mode, this time is 700  $\mu$ s.*

The TPM typically is ready to receive a command after less than 50 ms in TPM operational mode.

**Note:** *If the TPM is in TPM firmware update mode, the time until the TPM is ready to receive a command is 140 ms.*

If a TPM command is running, RST# should not be asserted; otherwise, this might also trigger some security functions. When the TPM shall be reset, the command TPM2\_Shutdown should be issued before the assertion of the RST# signal.

**3 Solution details**

**3.2.9 Firmware version mapping**

The TCG (see [1] and [2]) has defined two property tags for the reporting of the FW version (TPM\_PT\_FIRMWARE\_VERSION\_1 and TPM\_PT\_FIRMWARE\_VERSION\_2). TPM\_PT\_FIRMWARE\_VERSION\_1 is clearly defined to report the major firmware version in the upper 16 bits and the minor firmware version in the lower 16 bits. For TPM\_PT\_FIRMWARE\_VERSION\_2 there is no definition except that this field may be used as an extension to TPM\_PT\_FIRMWARE\_VERSION\_1. Therefore, interpretation of TPM\_PT\_FIRMWARE\_VERSION\_2 may lead to different results based on different definitions of this field. The following table provides a mapping between the definition of TPM\_PT\_FIRMWARE\_VERSION\_2 for SLB 9672 TPM 2.0 FW16.xx and the interpretation of TPM\_PT\_FIRMWARE\_VERSION\_2 as if this field was defined as two 16 bit values (like TPM\_PT\_FIRMWARE\_VERSION\_1).

**Table 56 Definition of the firmware version fields**

	TPM_PT_FIRMWARE_VERSION_1		TPM_PT_FIRMWARE_VERSION_2		
Infineon	MM	mm	0x00	bb	Cert. state
Alternative	MM	mm	BB	bb	

**Note:** *MM = Major firmware version*  
*mm = Minor firmware version*  
*BB = Major build number*  
*bb = Minor build number (or just build number for Infineon)*  
*Cert. State = Common Criteria certification state (see Table 20)*

**Table 57 Mapping of the firmware versions**

Infineon	Alternative	Firmware Version 1	Firmware Version 2
16.00.16280.02	16.00.3F.9802	0x00100000	0x003F9802
16.10.16488.00	16.10.40.6800	0x0010000A	0x00406800
16.12.16858.00	16.12.41.DA00	0x0010000C	0x0041DA00
16.13.17733.00	16.13.45.4500	0x0010000D	0x00454500
16.24.19084.00	16.24.4A.8C00	0x00100018	0x004A8C00

## **4 Licenses and notices**

### **Licenses and Notices**

The following license and notice statements are reproduced from [\[1\]](#).

#### 1. Copyright Licenses:

Trusted Computing Group (TCG) grants to the user of the source code in this specification (the "Source Code") a worldwide, irrevocable, nonexclusive, royalty free, copyright license to reproduce, create derivative works, distribute, display and perform the Source Code and derivative works thereof, and to grant others the rights granted herein. The TCG grants to the user of the other parts of the specification (other than the Source Code) the rights to reproduce, distribute, display, and perform the specification solely for the purpose of developing products based on such documents.

#### 2. Source Code Distribution Conditions:

Redistributions of Source Code must retain the above copyright licenses, this list of conditions and the following disclaimers.

Redistributions in binary form must reproduce the above copyright licenses, this list of conditions and the following disclaimers in the documentation and/or other materials provided with the distribution.

#### 3. Disclaimers:

THE COPYRIGHT LICENSES SET FORTH ABOVE DO NOT REPRESENT ANY FORM OF LICENSE OR WAIVER, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, WITH RESPECT TO PATENT RIGHTS HELD BY TCG MEMBERS (OR OTHER THIRD PARTIES) THAT MAY BE NECESSARY TO IMPLEMENT THIS SPECIFICATION OR OTHERWISE. Contact TCG Administration ([admin@trustedcomputinggroup.org](mailto:admin@trustedcomputinggroup.org)) for information on specification licensing rights available through TCG membership agreements.

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO EXPRESS OR IMPLIED WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, COMPLETENESS, OR NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

Without limitation, TCG and its members and licensors disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

Any marks and brands contained herein are the property of their respective owners.

## References

- [1] TCG: "*Trusted Platform Module Library (Part 1-4)*", Family 2.0, Level 00, Rev. 01.59; November 8, 2019
- [2] TCG: "*TCG PC Client Platform TPM Profile Specification for TPM 2.0*", Version 1.05, Revision 14; September 4, 2020
- [3] TCG: "*Errata for TCG Trusted Platform Module Library, Family 2.0, Level 00, Rev. 01.59, November 8, 2019*", Errata Version 1.5; January 25, 2024
- [4] TCG: "*Errata for PC Client Platform TPM Profile for TPM 2.0 Version 1.05 Revision 14*", Errata Version 1.2; February 2, 2024
- [5] TCG: "*Registry of reserved TPM 2.0 handles and localities*", Version 1.1, Rev. 1.00; February 6, 2019
- [6] TCG: "*TCG EK Credential Profile*", Version 2.3, Rev. 2; July 23, 2020
- [7] NIST: "*NIST Special Publication 800-193, Platform Firmware Resiliency Guidelines*"; May 2018

**Revision history**

## Revision history

Document version	Date of release	Description of changes
Revision 1.3	2024-11-18	Set sales codes for FW16.00, FW16.10 and FW 16.12 to Discontinued in <a href="#">Table 1</a>
Revision 1.2	2024-11-13	<ul style="list-style-type: none"><li>• New document layout with reordered content</li><li>• Added section <a href="#">TPM embedded software</a></li><li>• Changed some wording in <a href="#">Key features</a> section (and whole document where applicable)</li><li>• Changed wording in <a href="#">Product description</a></li><li>• Updated name of referenced TCG PTP spec <a href="#">[2]</a></li><li>• Removed 0x60 and 0x61 in <a href="#">TPM and vendor properties</a></li><li>• Updated reference <a href="#">[3]</a></li><li>• Updated reference <a href="#">[4]</a></li><li>• Fixed various typos</li></ul>
Revision 1.1	2023-04-27	Added features to front page Fixed wrong revision number in Introduction Changed <a href="#">Figure 7</a> (additional decoupling capacitor) Updated version and build numbers in <a href="#">TPM and vendor properties</a> Minor editorial changes
Revision 1.0	2022-01-20	Initial document version

## Trademarks

All referenced product or service names and trademarks are the property of their respective owners.

**Edition 2024-11-18**

**Published by**

**Infineon Technologies AG**

**81726 Munich, Germany**

**© 2024 Infineon Technologies AG**

**All Rights Reserved.**

**Do you have a question about any aspect of this document?**

**Email:**

**[CSSCustomerService@infineon.com](mailto:CSSCustomerService@infineon.com)**

**Document reference**

**IFX-lak1728461960559**

## Important notice

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

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

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

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

## Warnings

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

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