OPTIGA™ TPM SLB9673 TPM 2.0 FW26.xx

Datasheet

Trusted Platform Module

Document release reference: Z8F80723108-C

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) — Certificate number BSI-DSZ CC-1278-2026
  - FIPS 140-2 Level 2 — (targeted) — Certificate number 4467
- I2C interface (using clock stretching)
- 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

Device name	Package	Remarks
SLB 9673XU2.0 FW26.xx	PG-UQFN-32-1,-2	Enhanced temperature range -40°C - 85°C
SLB 9673AU2.0 FW26.xx	PG-UQFN-32-1,-2	Extended temperature range -40°C - 105°C

About this document

Scope and purpose

This datasheet describes the SLB 9673 TPM 2.0 FW26.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

Product validation . . . 1
Ordering information . . . 1
About this document . . . 2
Table of contents . . . 3
List of tables . . . 5
List of figures . . . 7
1 Introduction . . . 8
1.1 Product description . . . 8
1.2 Power management . . . 8
1.3 Device address and clock stretching . . . 8
2 Delivery forms and ordering . . . 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
3 Solution details . . . 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 . . . 14
3.1.1.4.1 I2C Interface Characteristics . . . 15
3.1.1.5 Timing . . . 17
3.1.2 Pin description . . . 17
3.1.3 Typical schematic . . . 19
3.2 TPM embedded software . . . 21
3.2.1 Implemented algorithms . . . 21
3.2.2 Available resources . . . 21
3.2.3 Command ordinal list . . . 23
3.2.4 Generation of RSA keys . . . 27
3.2.4.1 Pre-generation of RSA keys . . . 27
3.2.4.2 Generation of RSA 3072- and 4096-bit keys . . . 27
3.2.5 Non-volatile storage . . . 28
3.2.5.1 Predefined NV indices . . . 28
3.2.6 Vendor-specific functionality . . . 29

Table of contents

3.2.6.1 Power saving mode . . . 29
3.2.6.2 TPM and vendor properties . . . 29
3.2.6.3 Selftest operations . . . 31
3.2.6.3.1 TPM2_SelfTest . . . 31
3.2.6.3.2 TPM2_FullFipsSelfTestVendor . . . 31
3.2.6.3.3 TPM2_GetTestResult . . . 31
3.2.6.4 Dictionary attack default values . . . 32
3.2.6.5 RSA signing scheme . . . 33
3.2.6.6 NV index attribute TPMA_NV_WRITTEN . . . 33
3.2.6.7 Allocation of PCR banks . . . 33
3.2.6.8 General purpose I/O (GPIO) . . . 33
3.2.6.8.1 TPM2_NV_DefineSpace . . . 33
3.2.6.8.2 TPM2_NV_Write . . . 34
3.2.6.8.3 TPM2_NV_Read . . . 34
3.2.6.8.4 TPM2_NV_UndefineSpace . . . 34
3.2.6.9 TPM2_SetCapabilityVendor . . . 34
3.2.6.10 Field upgrade . . . 36
3.2.6.10.1 Structures and definitions . . . 36
3.2.6.10.2 TPM2B_MAX_BUFFER_VENDOR . . . 36
3.2.6.10.3 TPML_MAX_BUFFER . . . 36
3.2.6.10.4 Commands in TPM operational mode . . . 37
3.2.6.10.5 Commands in TPM firmware update mode . . . 39
3.2.7 TPM unique identifier . . . 42
3.2.8 NACK handling . . . 42
3.2.9 TPM register polling . . . 42
3.2.10 Configuration of I2C device address . . . 43
3.2.11 Reset timing . . . 44
3.2.12 Firmware version mapping . . . 45

4 Licenses and notices . . . 46

References . . . 47

Revision history . . . 48

Disclaimer . . . 49

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 I2C interface pins (SCL, SDA, TEST#, RST#, I2C_PIRQ#) . . . 14
Table 6 DC characteristics of GPIO pins . . . 14
Table 7 Power supply . . . 15
Table 8 Device reset . . . 15
Table 9 I2C Standard Mode Interface Characteristics . . . 15
Table 10 I2C Fast Mode Interface Characteristics . . . 16
Table 11 I2C Fast Mode plus Interface Characteristics . . . 16
Table 12 Buffer types . . . 17
Table 13 I/O Signals . . . 18
Table 14 Power supply . . . 18
Table 15 Not connected . . . 19
Table 16 Implemented algorithms . . . 21
Table 17 Available resources . . . 21
Table 18 Command code list . . . 23
Table 19 Vendor-specific TPM_CC constants . . . 25
Table 20 Predefined NV indices . . . 28
Table 21 Attributes of predefined NV indices . . . 28
Table 22 Infineon TPM property values . . . 29
Table 23 Infineon vendor-specific property constants . . . 29
Table 24 Infineon vendor-specific property values . . . 30
Table 25 TPM operation modes . . . 30
Table 26 FIFO configuration registers . . . 31
Table 27 TPM_RID register value description . . . 31
Table 28 Incoming operands and sizes . . . 31
Table 29 Outgoing operands and sizes . . . 31
Table 30 TPM2_SelfTest bit mapping of TPM2_SelfTest . . . 32
Table 31 TPM2_SelfTest bit mapping of TPM2_FullFipsSelfTestVendor . . . 32
Table 32 TPM2_SelfTest result . . . 32
Table 33 Mapping of GPIO indices . . . 33
Table 34 Default capability settings . . . 34
Table 35 Incoming operands and sizes . . . 34
Table 36 Outgoing operands and sizes . . . 35
Table 37 Error return codes . . . 35
Table 38 TPM2B_MAX_BUFFER_VENDOR structure definition . . . 36
Table 39 TPML_MAX_BUFFER structure definition . . . 36
Table 40 Incoming operands and sizes . . . 37
Table 41 Outgoing operands and sizes . . . 37
Table 42 Error return codes . . . 37
Table 43 Incoming operands and sizes . . . 38

List of tables

Table 44 Outgoing operands and sizes 38
Table 45 Error return codes 38
Table 46 Incoming operands and sizes 39
Table 47 Outgoing operands and sizes 39
Table 48 Error return codes 39
Table 49 Incoming operands and sizes 40
Table 50 Outgoing operands and sizes 40
Table 51 Error return codes 40
Table 52 Incoming operands and sizes 40
Table 53 Outgoing operands and sizes 40
Table 54 Error return codes 41
Table 55 Incoming operands and sizes 41
Table 56 Outgoing operands and sizes 41
Table 57 TPM2_GetTestResult bit mapping in TPM firmware update 42
Table 58 Definition of the firmware version fields 45
Table 59 Mapping of the firmware versions 45

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 9673 TPM 2.0 (PG-UQFN-32-1,-2 package, top view) 17
Figure 7 Typical schematic 20

1 Introduction

1.1 Product description

The SLB 9673 TPM 2.0 is a Trusted Platform Module. It is available in PG-UQFN-32-1,-2 package. It supports an I2C interface with a transfer rate of up to 1 MHz (typical). The SLB 9673 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 9673 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 I2C 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.

1.3 Device address and clock stretching

The I2C interface uses 7-bit addressing. The default address of the device is 0x2E (also see [4]).

The device uses clock stretching on the I2C interface (this implies that the I2C controller must support this).

2 Delivery forms and ordering

The SLB 9673 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.

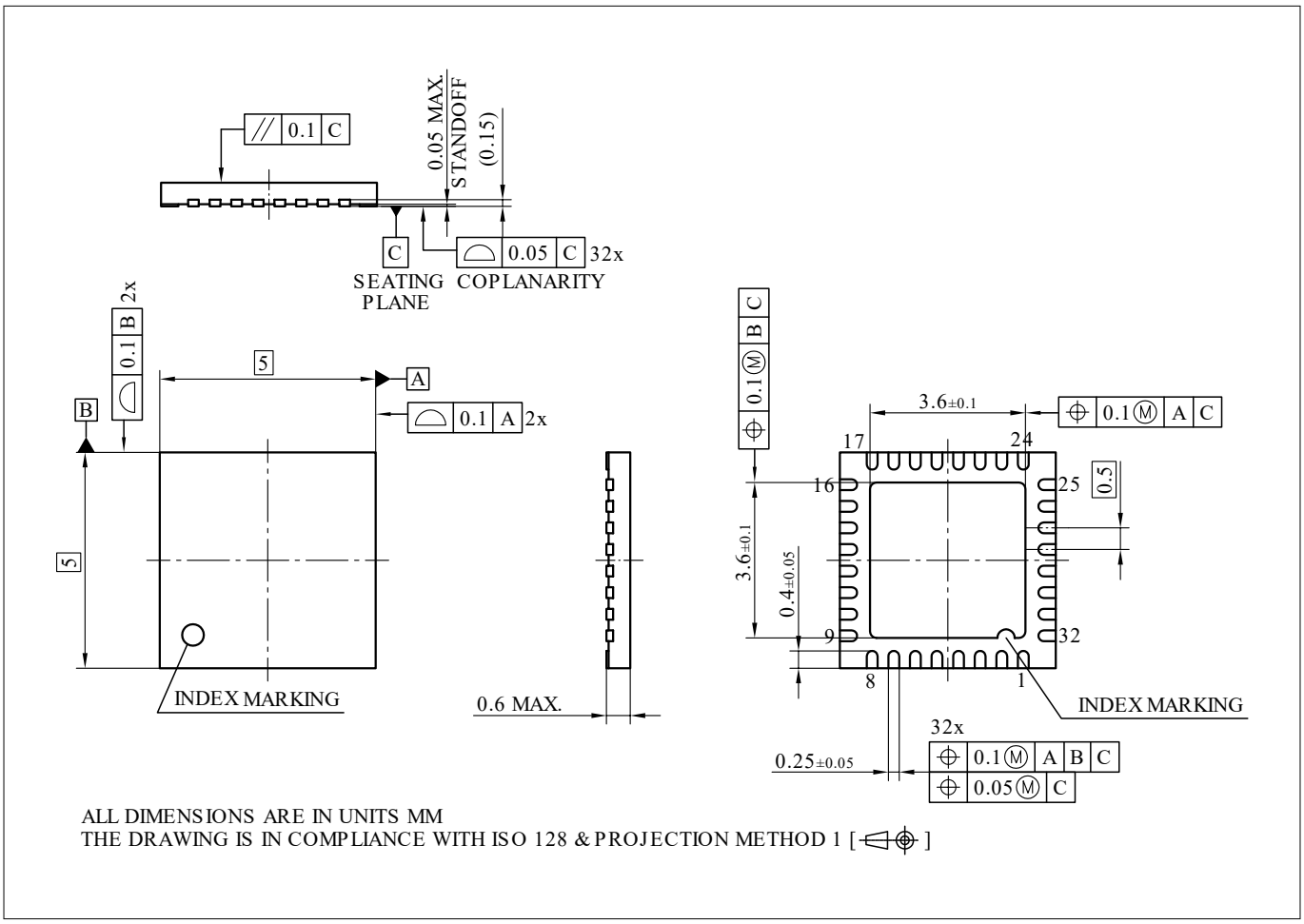


Figure 1 Package dimensions PG-UQFN-32-1,-2

2.1.1 Packing type

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

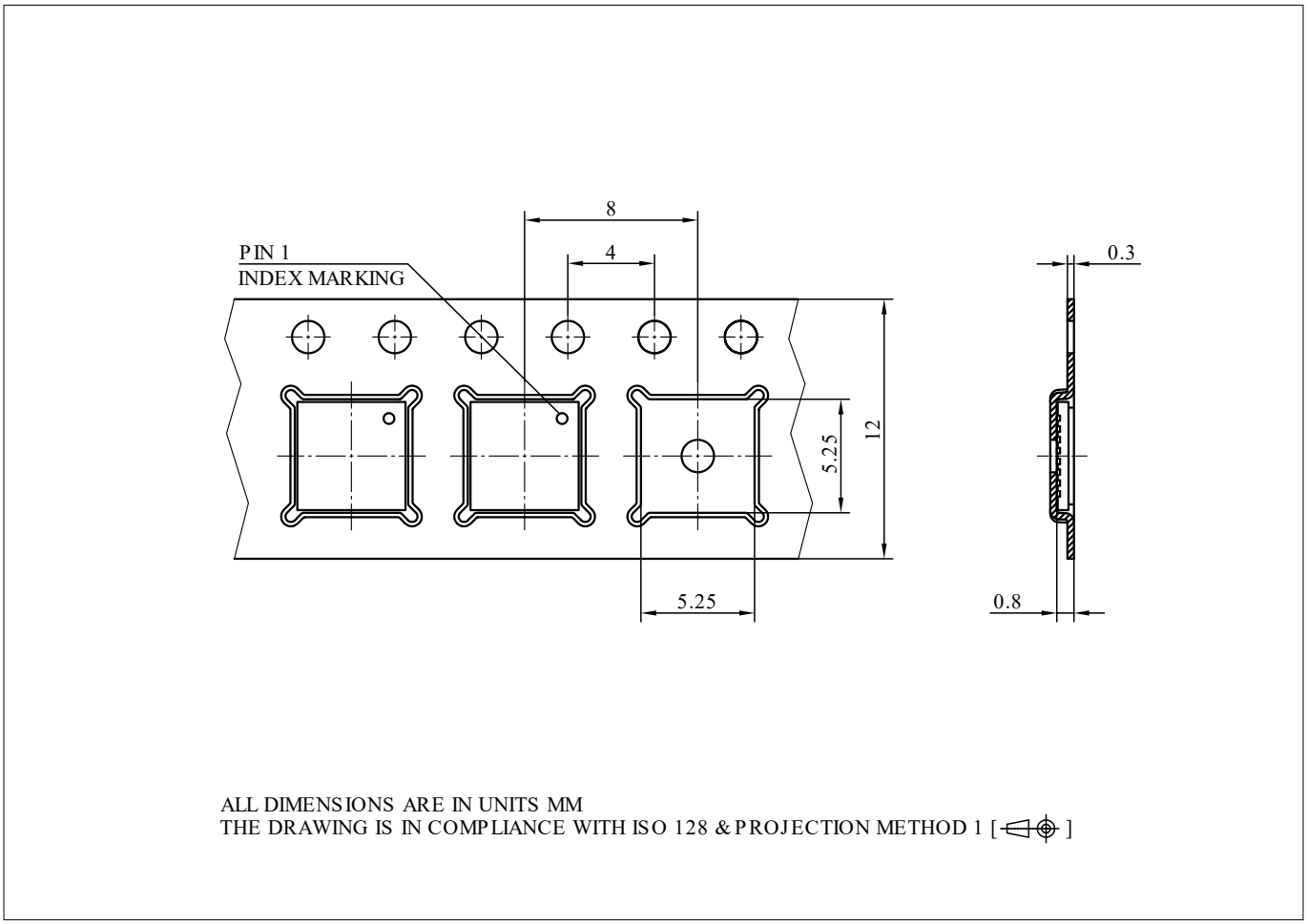


Figure 2 Tape & reel dimensions PG-UQFN-32-1,-2

2.1.2 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.

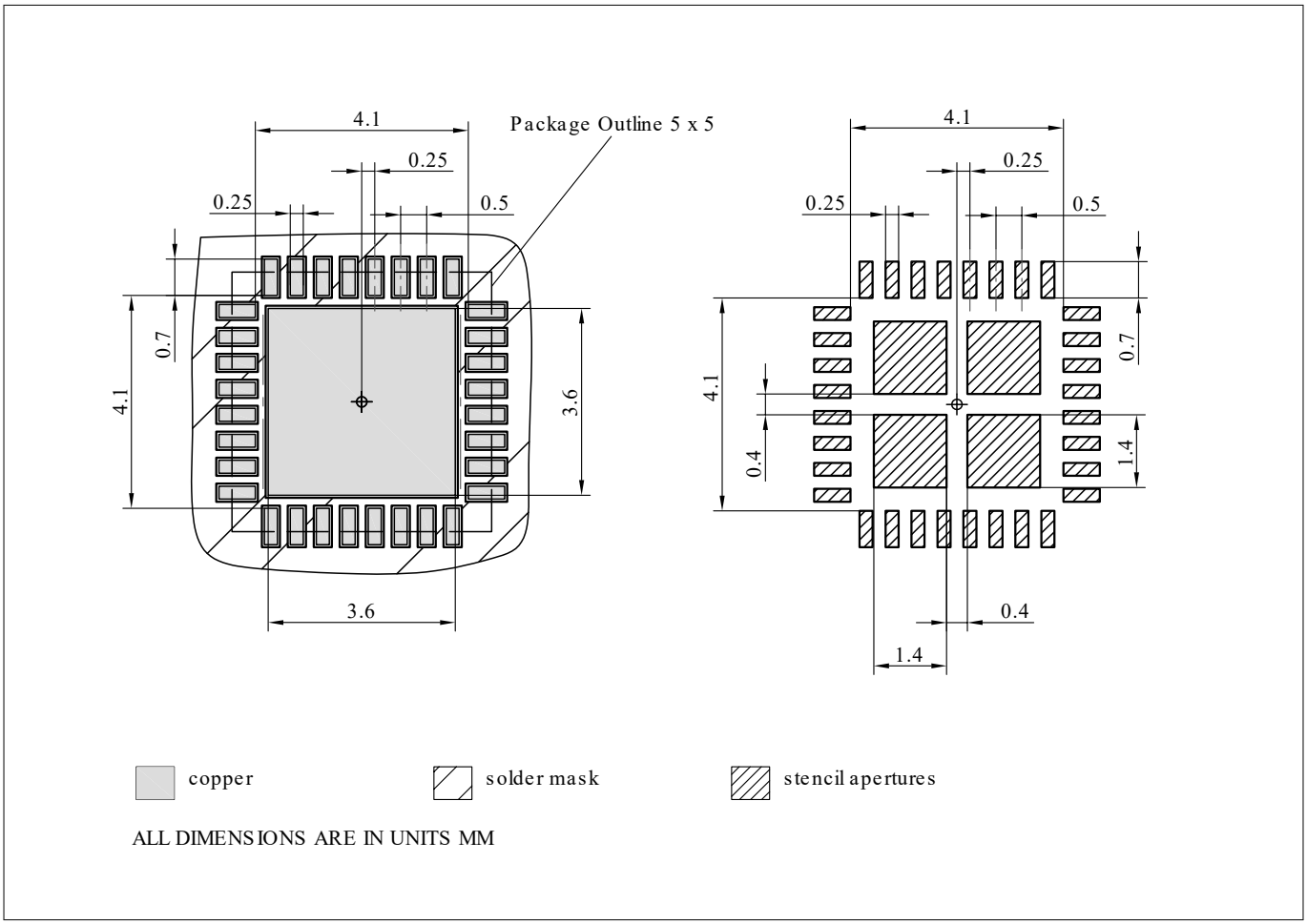


Figure 3 Recommended footprint PG-UQFN-32-1,-2

2.1.3 Chip marking

Line 1: SLB 9673

Line 2: XU20 yy or AU20 yy (see Ordering information and Table 1), the <yy> is an internal FW indication (software code, only valid at manufacturing due to field upgrade option)

Line 3: <Lot number> H <datecode>, the <datecode> is given as year (YY) and calendar week (CW)

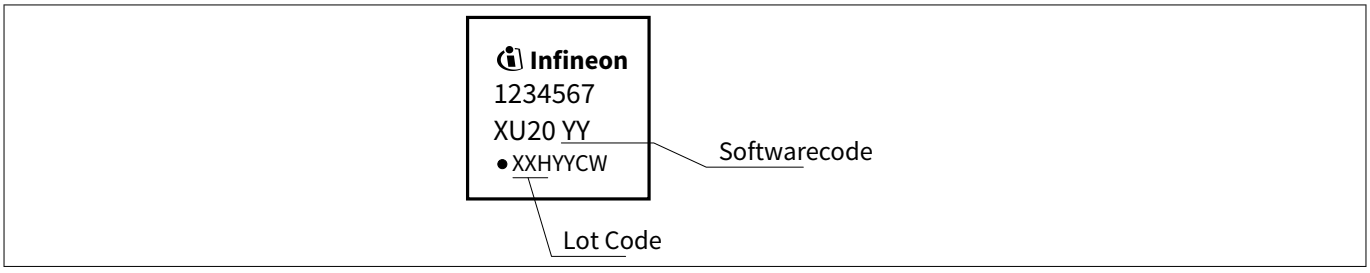


Figure 4 Chip marking

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

2.2 Ordering information

Table 1 Sales order code

Sales code (Sales name/ Product)	Ordering code	Software code	Status
SLB 9673XU2.0 FW26.00	SP005613379	18	Discontinued
SLB 9673AU2.0 FW26.00	SP005613383	18	Discontinued
SLB 9673XU2.0 FW26.10	SP005722390	20	Discontinued
SLB 9673AU2.0 FW26.10	SP005722392	20	Discontinued
SLB 9673XU2.0 FW26.13	SP005919748	29	Active
SLB 9673AU2.0 FW26.13	SP005919750	30	Active
SLB 9673XU2.0 FW26.24	SP006026288	44	Active
SLB 9673AU2.0 FW26.24	SP006026290	44	Active
SLB 9673XU2.0 FW26.25	SP006174656	50	Active
SLB 9673AU2.0 FW26.25	SP006174658	50	Active

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 9673XU2.0 devices
Ambient temperature	T_A	-40	–	105	°C	Extended temperature SLB 9673AU2.0 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 9673XU2.0 devices
Ambient temperature	T_A	-40	–	105	°C	Extended temperature SLB 9673AU2.0 devices
Useful lifetime		–	–	10	y	
Operating lifetime		–	–	10	y	
Average T_A over lifetime		–	55	–	°C	

3.1.1.3 DC characteristics

T_A = 25°C, V_{DD} = 3.3 V ± 0.3 V or V_{DD} = 1.8 V ± 0.15 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		µA	Pins GPIO, RST# and I2C_PIRQ# = V_{DD} , CS# inactive (= V_{DD}), no I2C bus activity
Current Consumption during reset	I_{VDD_Reset}		130		µA	Pin RST# active (= GND), GPIO and I2C_PIRQ# 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 I2C interface pins (SCL, SDA, TEST#, RST#, I2C_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	—
Input voltage low	V_{IL}	-0.5		0.3 V_{DD}	V	—
Input leakage current	I_{LEAK}	-2		2	µA	$0 V < V_{IN} < V_{DD}$
Output high voltage	V_{OH}	0.9 V_{DD}			V	I_{OH} = -100 µA
Output low voltage	V_{OL}			0.1 V_{DD}	V	I_{OL} = 1.5 mA
Pad input capacitance	C_{IN}			10	pF	
Output load capacitance	C_{LOAD}			30	pF	

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	µA	$0 V < V_{IN} < V_{DD}$
Output high voltage	V_{OH}	V_{DD} -0.3			V	I_{OH} = -1 mA, pins GPIO
Output low voltage	V_{OL}			0.3	V	I_{OL} = 1 mA, pins GPIO
Pad input capacitance	C_{IN}			10	pF	Pins GPIO

3.1.1.4 AC characteristics

T_A = 25°C, V_{DD} = 3.3V ± 0.3V or V_{DD} = 1.8V ± 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			µs	
Warm Reset	t_{WRST}	2			µs	

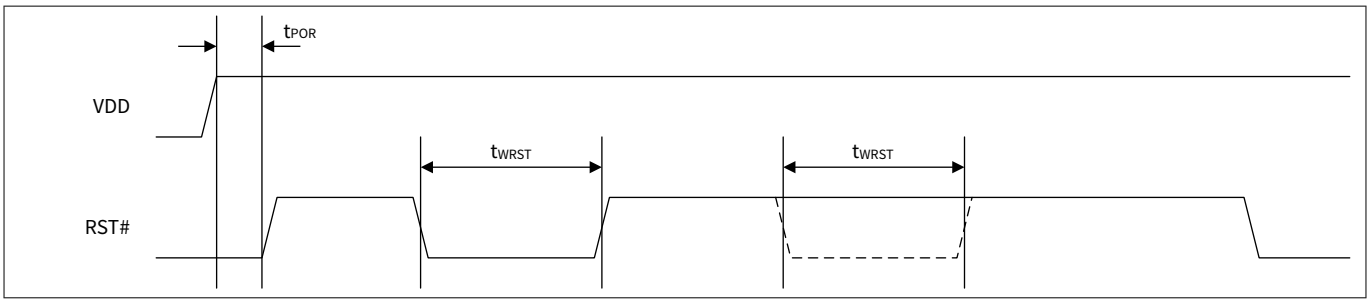


Figure 5 Reset timing

3.1.1.4.1 I2C Interface Characteristics

The electrical characteristics are compliant to the NXP I²C bus specification [1] for “standard-mode” (f_{SCL} ≤ 100 kHz), “fast-mode” (f_{SCL} ≤ 400 kHz) and “fast-mode plus” (f_{SCL} ≤ 1000 kHz), with certain deviations stated in Table 9, Table 10, and Table 11 below

For printed circuit board design the reduced output fall time tOF compared to the NXP I2C bus specification needs to be considered!

TA = 25°C, V_{DD} = 3.3 V ± 0.3 V or V_{DD} = 1.8 V ± 0.15 V unless otherwise noted.

Table 9 I2C Standard Mode Interface Characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
SCL clock frequency	f_{SCL}	0	—	100	kHz	—
Input voltage low	V_{IL}	-0.5	—	0.3 V_{DD}	V	—
Input voltage high	V_{IH}	0.7 V_{DD}	—	V_{DD}+0.5 or $V_{DD,max}$	V	Maximum = min(V_{DD}+0.5, $V_{DD,max}$)
Output low voltage	V_{OL}	—	—	0.4	V	I_{OL} = 2 mA, V_{DD} ≤ 2 V
Output low voltage	V_{OL}	—	—	0.4	V	I_{OL} = 3 mA, V_{DD} > 2 V
Low level output current	I_{OL}	2	—	—	mA	V_{OL} = 0.4 V, V_{DD} < 2.7 V
Low level output current	I_{OL}	3	—	—	mA	V_{OL} = 0.4 V, V_{DD} ≥ 2.7 V
Output fall time from V_{IHmin} to V_{ILmax} (at device)	t_{OF}	—	—	250	ns	C_b ≤ 200 pF, V_{DD} < 2.7 V

(table continues...)

Table 9 (continued) I2C Standard Mode Interface Characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Output fall time from V_{IHmin} to V_{ILmax} (at device)	t_{OF}	—	—	250	ns	$C_b \leq 400$ pF, $V_{DD} \geq 2.7$ V
Capacitive load for each bus line	C_b	—	—	200	pF	$V_{DD} < 2.7$ V
	C_b	—	—			$V_{DD} \geq 2.7$ V

Table 10 I2C Fast Mode Interface Characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
SCL clock frequency	f_{SCL}	0	—	400	kHz	—
Input voltage low	V_{IL}	-0.5	—	0.3 V_{DD}	V	—
Input voltage high	V_{IH}	0.7 V_{DD}	—	V_{DD}+0.5 or $V_{DD,max}$	V	Maximum = min(V_{DD}+0.5, $V_{DD,max}$)
Output low voltage	V_{OL}	—	—	0.4	V	I_{OL} = 2 mA, $V_{DD} \leq 2$ V
Output low voltage	V_{OL}	—	—	0.4	V	I_{OL} = 3 mA, $V_{DD} > 2$ V
Low level output current	I_{OL}	2	—	—	mA	V_{OL} = 0.4 V, $V_{DD} < 2.7$ V
Low level output current	I_{OL}	3	—	—	mA	V_{OL} = 0.4 V, $V_{DD} \geq 2.7$ V
Output fall time from VIHmin to VILmax (at device pin)	t_{OF}	20*V_{DD}/ 5.5 V	—	250	ns	C_b,min< $C_b \leq 200$ pF, $V_{DD} < 2.7$ V
Output fall time from VIHmin to VILmax (at device pin)	t_{OF}	20*V_{DD}/ 5.5 V	—	250	ns	$C_{b,min} < C_b \leq 400$ pF, $V_{DD} \geq 2.7$ V
Capacitive load for each bus line	C_b	15	—	200	pF	$V_{DD} < 2.7$ V
Capacitive load for each bus line	C_b	15	—	400	pF	$V_{DD} \geq 2.7$ V

Table 11 I2C Fast Mode plus Interface Characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
SCL clock frequency	f_{SCL}	0	—	1000	kHz	—
Input voltage low	V_{IL}	-0.5	—	0.3 V_{DD}	V	—
Input voltage high	V_{IH}	0.7 V_{DD}	—	V_{DD}+0.5 or V_{DD},max	V	Maximum = min(V_{DD} + 0.5, $V_{DD,max}$)
Output low voltage	V_{OL}	—	—	0.4	V	I_{OL} = 2 mA, $V_{DD} \leq 2$ V
Output low voltage	V_{OL}	—	—	0.4	V	I_{OL} = 3 mA, $V_{DD} > 2$ V

(table continues...)

Table 11 (continued) I2C Fast Mode plus Interface Characteristics

Parameter	Symbol	Values			Unit	Note or test condition
		Min.	Typ.	Max.		
Low level output current	I_{OL}	2	—	—	mA	V_{OL} = 0.4 V, V_{DD} < 2.7 V
Low level output current	I_{OL}	3	—	—	mA	V_{OL} = 0.4 V, V_{DD} ≥ 2.7 V
Output fall time from VIHmin to VILmax (at device pin)	t_{OF}	20*V_{DD}/ 5.5 V	—	120	ns	$C_{b,min}$ < C_b ≤ 150 pF
Capacitive load for each bus line	C_b	15	—	150	pF	

3.1.1.5 Timing

Some pads are disabled after deassertion of the reset signal for up to 500 µs.
The SLB 9673 TPM 2.0 features security mechanisms which detect and count all resets.

3.1.2 Pin description

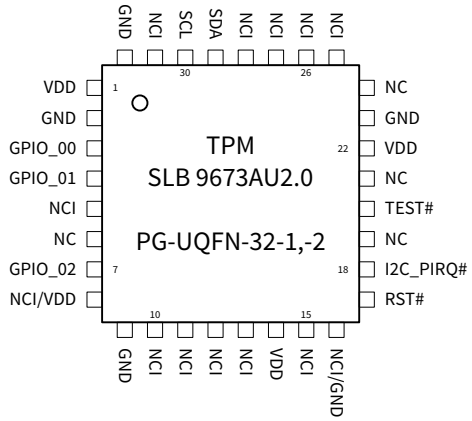


Figure 6 Pinout of the SLB 9673 TPM 2.0 (PG-UQFN-32-1,-2 package, top view)

Table 12 Buffer types

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

Table 13 I/O Signals

Pin number PG-UQFN-32-1,-2	Name	Pin type	Buffer type	Function
30	SCL	I/O	OD	I2C bus clock signal The clock signal of the I2C bus. Note that this pin may also act as output when clock stretching is active.
29	SDA	I/O	OD	I2C bus data signal The data signal of the I2C bus.
18	I2C_PIRQ#	O	OD	Interrupt signal This pin can be connected to the host interrupt controller to allow interrupt driven reads of the response data instead of polling. As soon as a response is available, the signal is asserted (low) and remains active until the complete response is read by the host.
17	RST#	I	IN	Reset External reset signal. Asserting this pin unconditionally resets the device. The signal is active low. This pin has a weak internal pull-up resistor.
20	TEST#	I	IN	Test Test signal, must be externally connected to a static high level.
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 14 Power supply

Pin number PG-UQFN-32-1,-2	Name	Pin type	Buffer type	Function
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 15 Not connected

Pin number PG-UQFN-32-1,-2	Name	Pin type	Buffer type	Function
6, 19, 21, 24	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/GND	—	—	Not connected internally This pin is not connected internally. For future use, it is recommended to connect this pin to GND (preferably via a pull-down resistor).
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.
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 9673 TPM 2.0. The power supply pins should be bypassed to GND with capacitors located close to the device.

3 Solution details

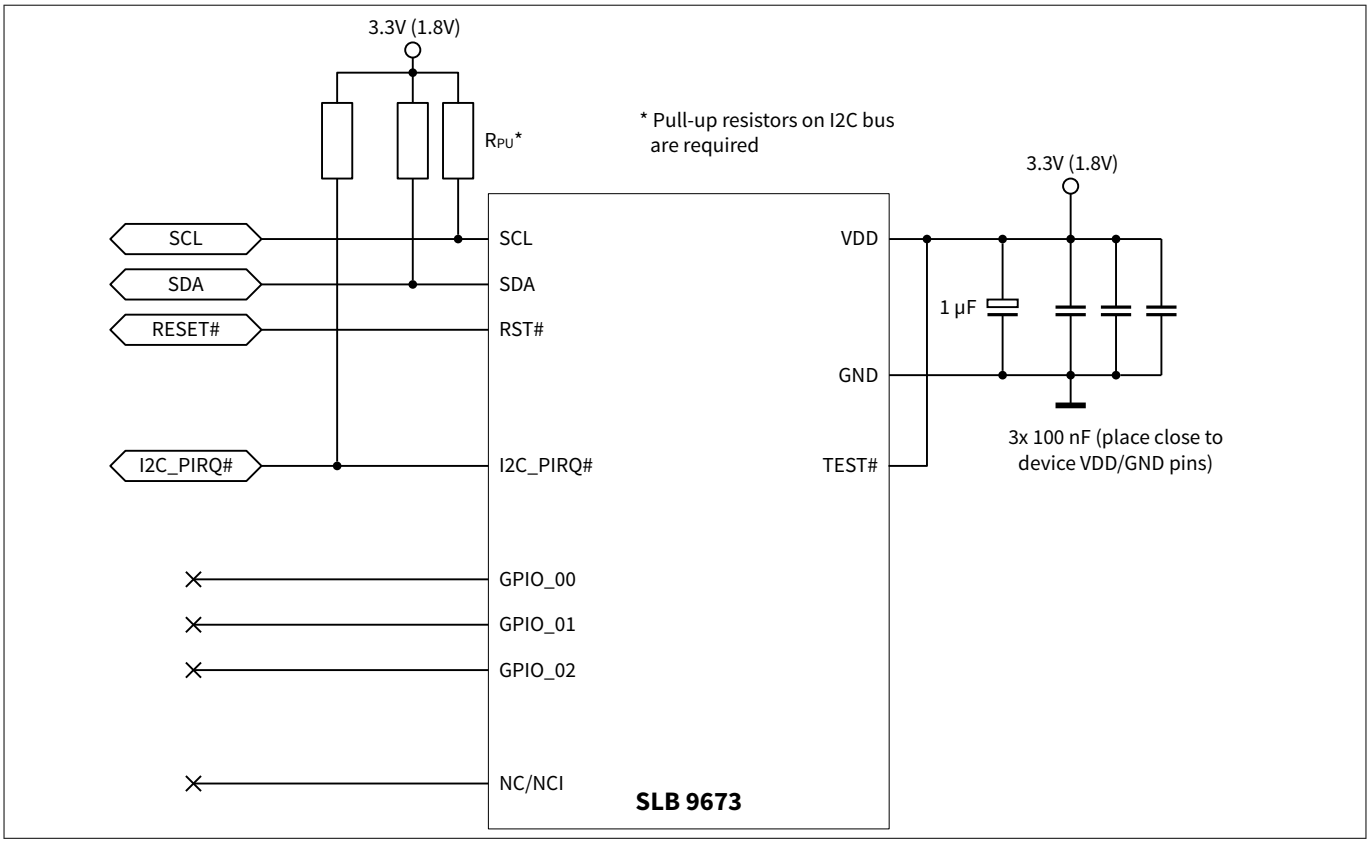


Figure 7 Typical schematic

3.2 TPM embedded software

The embedded software of the Infineon SLB 9673 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 ECDAA.

Table 16 Implemented algorithms

Algorithm name	Key size/curve	Mandatory (M), optional (O) per [2]	Implemented in SLB 9673 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 17 Available resources

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

(table continues...)

Table 17 (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 [1)]
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.

3.2.3 Command ordinal list

The TPM implements the TCG standard commands defined in Table 18 and the vendor-specific commands defined in Table 19. All other ordinals will return TPM_RC_COMMAND_CODE.

Table 18 Command code list

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

(table continues...)

Table 18 (continued) Command code list

TPM_CC_GetTime	
Anonymous Attestation	
TPM_CC_Commit	
Signature Verification	
TPM_CC_VerifySignature	TPM_CC_Sign
Integrity Collection (PCR)	
TPM_CC_PCR_Extend	TPM_CC_PCR_Event
TPM_CC_PCR_Read	TPM_CC_PCR_Allocate
TPM_CC_PCR_Reset	
Enhanced Authorization (EA) Commands	
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	
Hierarchy Commands	
TPM_CC_CreatePrimary	TPM_CC_HierarchyControl
TPM_CC_SetPrimaryPolicy	TPM_CC_ChangePPS
TPM_CC_ChangeEPS [Configurable] [1)]	TPM_CC_Clear
TPM_CC_ClearControl	TPM_CC_HierarchyChangeAuth
Dictionary Attack Functions	
TPM_CC_DictionaryAttackLockReset	TPM_CC_DictionaryAttackParameters
Context Management	
TPM_CC_ContextSave	TPM_CC_ContextLoad
TPM_CC_FlushContext	TPM_CC_EvictControl
Clocks and Timers	
TPM_CC_ReadClock	TPM_CC_ClockSet
TPM_CC_ClockRateAdjust	
Capability Commands	
TPM_CC_GetCapability	TPM_CC_TestParms
Non-Volatile Storage	
TPM_CC_NV_DefineSpace	TPM_CC_NV_UndefineSpace

(table continues...)

Table 18 (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 19 does not comprehensively list all vendor-defined TPM commands.*

Table 19 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 TPM2_SetCapabilityVendor 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 TPM2_FullFipsSelfTestVendor 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 TPM2_FieldUpgradeStartVendor 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 TPM2_FieldUpgradeAbandonVendor for further details.

(table continues...)

Table 19 (continued) Vendor-specific TPM_CC constants

Name	Command code	NV write	Decrypt	Encrypt	Description
TPM_CC_FieldUpgradeManifestVendor	0x20000131	Y	N	N	Vendor specific command for validating the manifest while in TPM firmware update mode. Refer to TPM2_FieldUpgradeManifestVendor 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 TPM2_FieldUpgradeDataVendor 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 TPM2_FieldUpgradeFinalizeVendor for further 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 17. 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.

3.2.5 Non-volatile storage

3.2.5.1 Predefined NV indices

The sizes documented in Table 20 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 20 Predefined NV indices

Value	Index Name	Default Size	Attributes
0x01C00002	RSA 2048 EK Certificate	1427 bytes (RSA Endorsement Key Certificate)	see Table 21
0x01C0000A	ECC NIST P256 EK Certificate	844 bytes (ECC Endorsement Key Certificate)	see Table 21
0x01C00016	ECC NIST P384 EK Certificate	873 bytes (ECC Endorsement Key Certificate)	see Table 21
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 Table 21

Table 21 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

3.2.6 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 9673 TPM 2.0 using the command TPM2_GetCapability (capability = TPM_CAP_TPM_PROPERTIES):

Table 22 Infineon TPM property values

TPM_PT_MANUFACTURER	“IFX”
TPM_PT_VENDOR_STRING_1	“SLB9”
TPM_PT_VENDOR_STRING_2	“673”
TPM_PT_VENDOR_STRING_3	NULL
TPM_PT_VENDOR_STRING_4	NULL
TPM_PT_FIRMWARE_VERSION_1	Major and minor version (for instance, 0x001A0019 indicates FW26.25) [1)]
TPM_PT_FIRMWARE_VERSION_2	Build number and Common Criteria certification state (for instance, 0x004D6400 or 0x004D6402)[1)] Byte 1: reserved for future use (0x00) Byte 2 and 3: Build number (for instance, 0x4D64)[1)] 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_PROPERTY:

Table 23 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.

Table 24 Infineon vendor-specific property values

TPM property	Value	Property value
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 Table 25
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 25 TPM operation modes

Operation Mode	Description
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.

Table 26 FIFO configuration registers

Register	Value	Comments
TPM_VID	0x15D1	Vendor identification of Infineon Technologies AG
TPM_DID	0x001C	Device identification
TPM_RID	0x16	Revision identification register

Table 27 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 0001_B

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 30 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 28 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 29 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 25)

The mapping of the individual bits to the corresponding selftest which is executed by the command TPM2_SelfTest is shown in Table 30 below. The bit mapping of the selftests performed by TPM2_FullFipsSelfTestVendor is listed in Table 31 (bit == 1 means that the test passed, RFU bits are reserved for future use).

Table 30 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 31 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 32 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

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 13 are mapped to ordinary NV indices with the corresponding handle values listed in the table below.

Table 33 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 33
- 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.*

3.2.6.8.2 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. 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 24).

Table 34 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 35 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
TPM_PT	Property	Property to be set

(table continues...)

Table 35 (continued) Incoming operands and sizes

Type	Name	Description
UINT32	value	New property value

Table 36 Outgoing operands and sizes

Type	Name	Description
TPM_ST	tag	
UINT32	responseSize	
TPM_RC	responseCode	

Table 37 Error return codes

Type	Meaning
TPM_RC_VALUE	Property value is not valid

3.2.6.10 Field upgrade

The SLB 9673 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 9673 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_FieldUpgradeFinalzeVendor 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 38 TPM2B_MAX_BUFFER_VENDOR structure definition

Type	Name	Description
UINT16	size	Size of buffer
UINT8[size]	buffer	Buffer

3.2.6.10.3 TPML_MAX_BUFFER

Table 39 TPML_MAX_BUFFER structure definition

Type	Name	Description
UINT32	count	Number of properties
TPM2B_MAX_BUFFER_VENDOR	vendorData	List of property values

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 40 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 41 Outgoing operands and sizes

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

Table 42 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.*

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 43 Incoming operands and sizes

Type	Name	Description
TPMI_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 44 Outgoing operands and sizes

Type	Name	Description
TPM_ST	tag	
UINT32	responseSize	
TPM_RC	responseCode	

Table 45 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

3.2.6.10.5 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 46 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 47 Outgoing operands and sizes

Type	Name	Description
TPM_ST	tag	
UINT32	responseSize	
TPM_RC	responseCode	

Table 48 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

TPM2_FieldUpgradeDataVendor, the field upgrade process must be restarted after a reboot by resending TPM2_FieldUpgradeManifestVendor.

***Note**: A dead time of 3000 ms should be considered before sending the next command.*

Table 49 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 50 Outgoing operands and sizes

Type	Name	Description
TPM_ST	tag	
UINT32	responseSize	
TPM_RC	responseCode	

Table 51 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 52 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 53 Outgoing operands and sizes

Type	Name	Description
TPM_ST	tag	

(table continues...)

Table 53 (continued) Outgoing operands and sizes

Type	Name	Description
UINT32	responseSize	
TPM_RC	responseCode	

Table 54 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 22 (except for TPM_PT_MODES) and vendor-specific properties shown in Table 24. The result of TPM2_GetCapability 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 55 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 56 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 25)

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 57 TPM2_GetTestResult bit mapping in TPM firmware update

Bit	Meaning	Bit	Meaning
31-22	RFU	15	Sensortest
21	ECDSA Verify P521 [1)]	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 .

3.2.8 NACK handling

The I2C TPM may return NACK on TPM register accesses if it is unable to respond to the bus cycle because of internal reasons.

The host driver shall repeat the access with a delay between accesses of at least 250 µs until the TPM returns ACK. It shall attempt these accesses at least 50 times.

***Note**: The device also uses clock stretching on the I2C bus to stall accesses from the host if they cannot be answered immediately.*

3.2.9 TPM register polling

Processing of accesses to registers creates a load on the TPM.

If registers are polled in quick succession, the time until the TPM reaches the target state is increased, which decreases performance and may even lead to violation of maximum timeout values.

To prevent this, a minimum delay between register read accesses must be be respected when polling:

- Minimum delay between TPM register reads for polling of TPM_STS_x during command execution: 1 ms
- Minimum delay between TPM register reads for polling of TPM_STS_x after device reset before commandReady set: 1 ms
- Minimum delay between TPM register reads for all other TPM register polling, including TPM_STS_x.commandReady set between command, TPM_STS_x.valid and TPM_STS_x.burstCount: 100 µs

3.2.10 Configuration of I2C device address

In case the default I2C device address (see Device address and clock stretching) cannot be used, the I2C device address can be changed. The change of the I2C device address must be applied for TPM operational mode and TPM firmware update mode separately. The following sequence shall be used:

1. Ensure that normal TPM operational mode is active. This can be detected by the operation mode (see Table 25) returned by TPM2_GetCapability (capability = TPM_PT_VENDOR_FIX_FU_OPERATION_MODE). Operation mode 0x00 should be returned
2. Write the new I2C device address to register 0x38 (see [4] chapter 8.3.5.15) with **makePersistent bit set**. The new I2C device address becomes effective for TPM operational mode with the next I2C master access
3. Switch from TPM operational mode to TPM firmware update mode by sending TPM2_FieldUpgradeStartVendor (see Section TPM2_FieldUpgradeStartVendor) with random data for the hash digest of the manifest. The newly configured I2C device address must be used
4. Ensure that TPM firmware update mode is active. This can be detected by the operation mode (see Table 25) returned by TPM2_GetCapability (capability = TPM_PT_VENDOR_FIX_FU_OPERATION_MODE). Operation mode 0x01 should be returned. The initially stored I2C device address must be used
5. Write the new I2C device address to register 0x38 (see [4] chapter 8.3.5.15) with **makePersistent bit set**. The new I2C device address becomes effective for TPM firmware update mode with the next I2C master access
6. Switch back to TPM operational mode by sending TPM2_FieldUpgradeAbandonVendor (see Section TPM2_FieldUpgradeAbandonVendor). The newly configured I2C device address must be used

***Note**: In case the I2C device address configuration is only completed for TPM operation mode or TPM firmware update mode, this may result in bus conflicts if additional devices are connected.*

***Note**: In case the new I2C device address was written to register 0x38 with makePersistent bit clear, the new I2C device address is applied but not returned by a read operation to register 0x38. A read operation to register 0x38 always returns the I2C device address which was written with makePersistent bit set.*

3.2.11 Reset timing

The TPM_ACCESS_x.tpmEstablishment bit has the correct value and the TPM_ACCESS_x.tpmRegValidSts bit is set within 30 ms after RST# is deasserted.

***Note**: For accesses of any TPM I2C interface register while RST# is asserted and within 30 ms after deassertion of RST#, the TPM may return an address NACK. If the TPM is in TPM firmware update mode, this time is 140 ms. 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.*

As described in TPM register polling, TPM register accesses increases the duration of TPM state changes. After reset and before TPM_STS_x.commandReady is set, delay between TPM register reads must be at least 1 ms. This can also be achieved by starting to poll for TPM_STS_x.commandReady not before 100 ms after deassertion of RST# in normal TPM operational mode and not before 200 ms in TPM firmware update mode, because TPM_STS_x.commandReady is then already set on the first register read.

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.

3.2.12 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 9673 TPM 2.0 FW26.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 58 Definition of the firmware version fields

	TPM_PT_FIRMWARE_VERSION_1		TPM_PT_FIRMWARE_VERSION_2	
Infineon	Major firmware version	Minor firmware version	0x00 and Build number	Cert. state[1)]
Alternative	Major firmware version	Minor firmware version	first byte of Build number	last byte of Build number and cert. state[1)]

1) Common Criteria certification state (see Table 22)

Table 59 Mapping of the firmware versions

Infineon	Alternative	Firmware Version 1	Firmware Version 2
26.00.16682.02	26.00.65.10754	0x001A0000	0x00412A02
26.10.16688.00	26.10.65.12288	0x001A000A	0x00413000
26.13.17770.00	26.13.69.27136	0x001A000D	0x00456A00
26.24.19041.00	26.24.74.24832	0x001A0018	0x004A6100
26.25.19812.00	26.25.77.25600	0x001A0019	0x004D6400

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) 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 (Revision 01.59)*; 2019-11-08

[2] TCG: *TCG PC Client Platform TPM Profile (PTP) Specification, Family “2.0”, Level 00 (Version 1.05, Revision 14)*; 2020-09-04

[3] TCG: *Errata for TCG Trusted Platform Module Library, Family “2.0”, Level 00, Revision 01.59 (Errata Version 1.8 (tentative))*; 2026-02-01

[4] TCG: *Errata for PC Client Platform TPM Profile for TPM 2.0, Version 1.05 Revision 14 (Errata Version 1.2)*; 2024-02-02

[5] TCG: *Registry of reserved TPM 2.0 handles and localities (Version 1.1, Rev. 1.00)*; 2019-02-06

[6] TCG: *TCG EK Credential Profile (Version 2.3, Rev. 2)*; 2020-07-23

[7] NIST: *NIST Special Publication 800-193, Platform Firmware Resiliency Guidelines*; 2018-05

Revision history

Reference	Description
Revision 1.5, 2026-01-07	
• Chapter • Chapter • Chapter 2.2 • Chapter 3.2.6.2 • Chapter 3.2.12 • [3]	• Updated documentation to FW26.25 - New device name in Table 1 in Cover page - Updated certificate numbers in Key features - New sales order codes in Table 1 in Ordering information - New build number in Table 22 in TPM and vendor properties - New entry in Table 59 in Firmware version mapping - Updated reference [3]
Revision 1.4, 2024-11-13	
	• New document layout with reordered content • Added use of clock-stretching • Added section TPM embedded software • Changed some wording in Key features section (and whole document where applicable) • Changed wording in Product description • Updated name of referenced TCG PTP spec [2] • Removed 0x60 and 0x61 in TPM and vendor properties • Updated reference [3] • Updated reference [4] • Fixed various typos
Revision 1.3, 2023-05-02	
	• Added features to front page • Changed Figure 7 (additional decoupling capacitor) • Added reset power consumption to Table 4
Revision 1.2, 2022-08-24	
	• Fixed package designation in Figure 6
Revision 1.1, 2022-07-08	
	• Added TPM register polling
Revision 1.0, 2022-05-25	
	Initial version

Trademarks

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

Edition 2026-01-07

Published by

Infineon Technologies AG

81726 Munich, Germany

© 2026 Infineon Technologies AG

All Rights Reserved.

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

Email:
CSSCustomerService@infineon.com

Document reference
IFX-ewk1729152785129

Important notice

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

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

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

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

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.