OPTIGA™ TPM

SLB 9672 TPM2.0

Data Sheet

Devices

- SLB 9672XU2.0 FW16.xx
- SLB 9672AU2.0 FW16.xx

Key features

- Optimized TPM device for IoT and ICT applications
- PQC-protected firmware update mechanism
- Compliant to TPM Main Specification, Family "2.0", Level 00, Revision 01.59
- Certifications:
  - CC, Version 3.1 Rev.5, level EAL4+, AVA_VAN.4 (moderate) according to TCG PC Client TPM Protection Profile
  - FIPS 140-2 level 2 (physical security level 3) (targeted)
- SPI interface
- Meeting Intel TXT and Microsoft Windows certification criteria for successful platform qualification
- Random Number Generator (RNG) implemented according to NIST SP800-90A using entropy source according to NIST SP800-90B
- Full personalization with 4 Endorsement Keys (EK) and 4 EK certificates (RSA 2048, RSA 3072, ECC NIST P256, ECC NIST P384)
- Enhanced temperature range (-40°C .. +85°C or -40°C .. +105°C)
- 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, BN P256, NIST P384)
- SHA-1, SHA-256, SHA-384
- AES-128, AES-192, AES-256

About this document

Scope and purpose

This data sheet describes the OPTIGA™ TPM SLB 9672 FW16.xx Trusted Platform Module together with its features, functionality and programming interface.

Intended audience

This data sheet is primarily intended for system developers.

Table of contents

List of figures

List of tables

1 Overview

The OPTIGA™ TPM SLB 9672 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 OPTIGA™ TPM SLB 9672 is a TPM based on TCG family 2.0 specifications (see **[1]** and **[2]**).

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).

1.1 Power management

In the OPTIGA™ TPM SLB 9672, 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 immediately and will return to the low-power mode after the transaction has been finished.

2 Device types and ordering information

The OPTIGA™ TPM SLB 9672 product family features devices using an UQFN package. **Table 1** shows the different versions.

Table 1 Device configuration

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	Enhanced temperature range -40°C - 105°C

3 Pin description

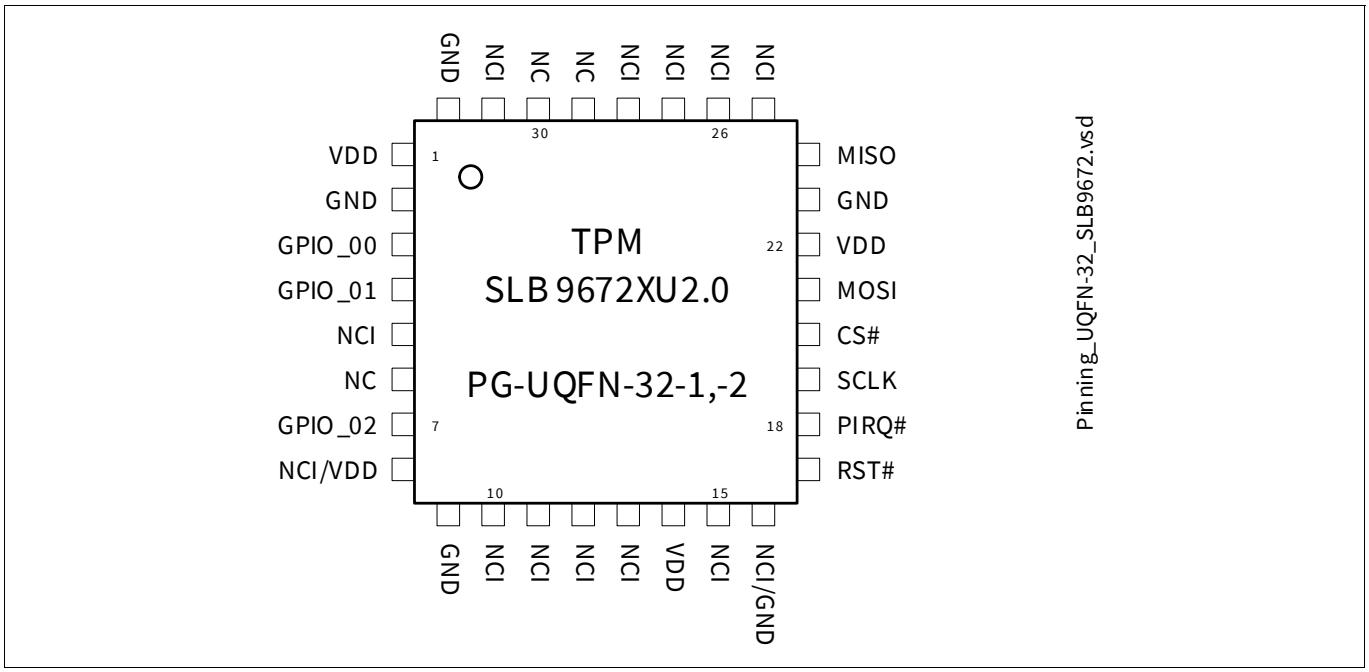

Figure 1 Pinout of the OPTIGA™ TPM SLB 9672 (PG-UQFN-32-1,-2 package, top view)

Table 2 Buffer types

Buffer type	Description
TS	Tri-state pin
ST	Schmitt-trigger pin
OD	Open-drain pin

Table 3 I/O Signals

Pin number PG-UQFN-32-1,-2	Name	Pin type	Buffer type	Function
20	CS#	I	ST	**Chip select** The SPI chip select signal (active low).
19	SCLK	I	ST	**SPI clock** The SPI clock signal. Only SPI mode 0 is supported by the device.
21	MOSI	I	ST	**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	ST	**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.
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 4 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 5 Not connected

Pin number PG-UQFN-32-1,-2	Name	Pin type	Buffer type	Function
6, 29, 30	NC	NU	—	**No connect** All pins must not be connected externally (must be left floating).
5, 10 - 13, 15, 25 - 28, 31	NCI	—	—	**Not connected internally** All pins are not connected internally (can be connected externally).
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.
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 pins.

3.1 Typical schematic

Figure 2 shows the typical schematic for the OPTIGA™ TPM SLB 9672. The power supply pins should be bypassed to GND with capacitors located close to the device.

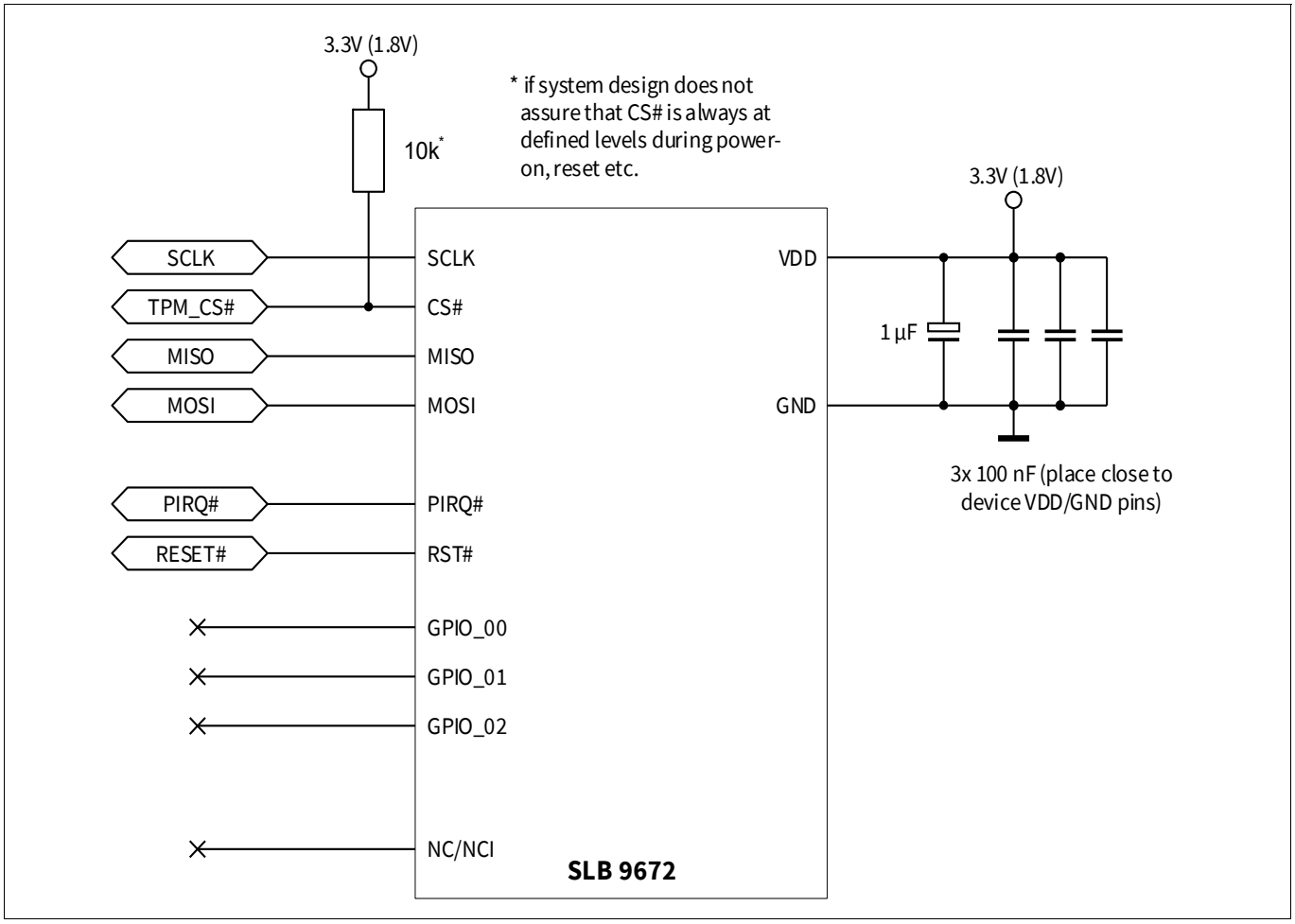

Figure 2 Typical schematic

4 TPM 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 OPTIGA™ TPM SLB 9672 using the command TPM2_GetCapability (capability = TPM_CAP_TPM_PROPERTIES):

Table 6 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, 0x0010000D indicates V16.13)[1)]
TPM_PT_FIRMWARE_VERSION_2	Build number and Common Criteria certification state (for instance, 0x00454500 or 0x00454502)[1)] Byte 1: reserved for future use (0x00) Byte 2 and 3: Build number (for instance, 0x4545)[1)] Byte 4: Common Criteria certification state/mode: 0x00 = TPM operational mode/TPM is CC certified 0x02 = TPM operational mode/TPM is not certified 0x60 = Manually entered TPM firmware recovery mode (triggered externally for testing purposes) 0x61 = TPM firmware recovery mode (triggered by code integrity failure detection) 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.

5 Electrical characteristics

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

5.1 Absolute maximum ratings

Table 7 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	Enhanced 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 max. 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.

5.2 Functional operating range

Table 8 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	Enhanced temperature SLB 9672AU2.0 devices
Useful lifetime		–	–	10	y	
Operating lifetime		–	–	10	y	
Average T_A over lifetime		–	55	–	°C	

5.3 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 9 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 PIRQ# = V_{DD}, CS# inactive (= V_{DD}), MOSI, MISO and SCLK don't care
Current Consumption during reset	I_{VDD_Reset}		130		µA	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 10 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 V, only pins SCLK, MISO, MOSI and CS#
		0.7 V_{DD}		V_{DD}+0.3	V	$V_{DD,typ}$ = 3.3 V, pin RST#
		0.7 V_{DD}		V_{DD}+0.3	V	$V_{DD,typ}$ = 1.8 V
Input voltage low	V_{IL}	-0.5		0.3 V_{DD}	V	$V_{DD,typ}$ = 3.3 V
		-0.3		0.3 V_{DD}	V	$V_{DD,typ}$ = 1.8 V
Input leakage current	I_{LEAK}	-4		4	µA	0 V < V_{IN} < V_{DD}
		-4.5			mA	Pins SCLK, CS#, MISO, MOSI -0.5 V < V_{IN} < V_{DD}+0.5 V $V_{DD,typ}$ = 3.3 V
		-4.5			mA	Pins SCLK, CS#, MISO, MOSI -0.3 V < V_{IN} < V_{DD}+0.3 V $V_{DD,typ}$ = 1.8 V
		-2		2	µA	Pin RST# 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 11 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

5.4 AC characteristics

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

Table 12 Power supply

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

Table 13 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	

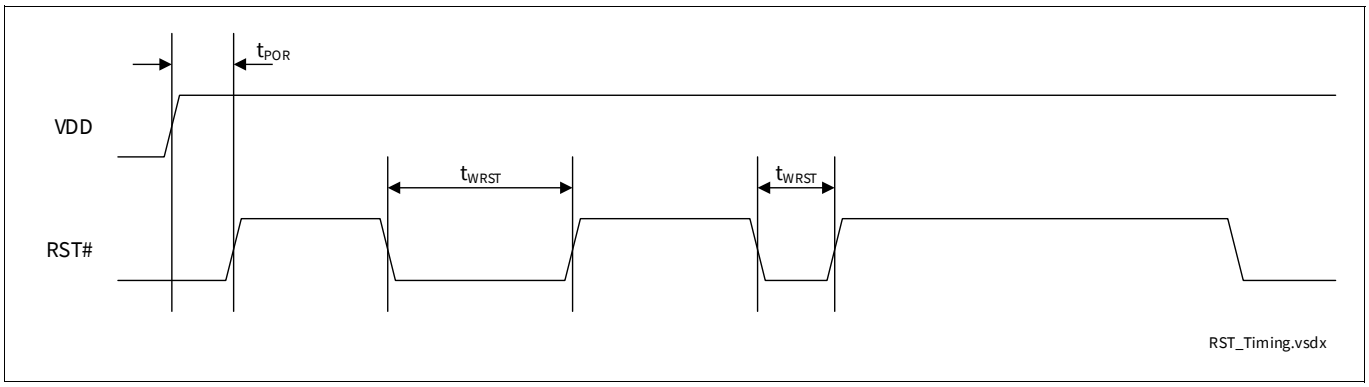

Figure 3 Reset timing

Table 14 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%	µs	Rising edge to rising edge, measured at V_{IN} = 0.5 V_{DD}

Table 14 AC characteristics of SPI interface (continued)

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
SCLK low time	t_{CLKL}	0.45 t_{CLK}			µs	Falling edge to rising edge, measured at V_{IN} = 0.5 V_{DD}
SCLK high time	t_{CLKH}	0.45 t_{CLK}			µs	Rising edge to falling edge, measured at V_{IN} = 0.5 V_{DD}
SCLK slew rate (rising/falling)	t_{SLEW}	0.216		4	V/ns	f_{CLK} < 20 MHz, between 0.2 V_{DD} and 0.6 V_{DD}
		0.4		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

5.5 Timing

Some pads are disabled after deassertion of the reset signal for up to 500 µs.

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

6 Package dimensions (UQFN)

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

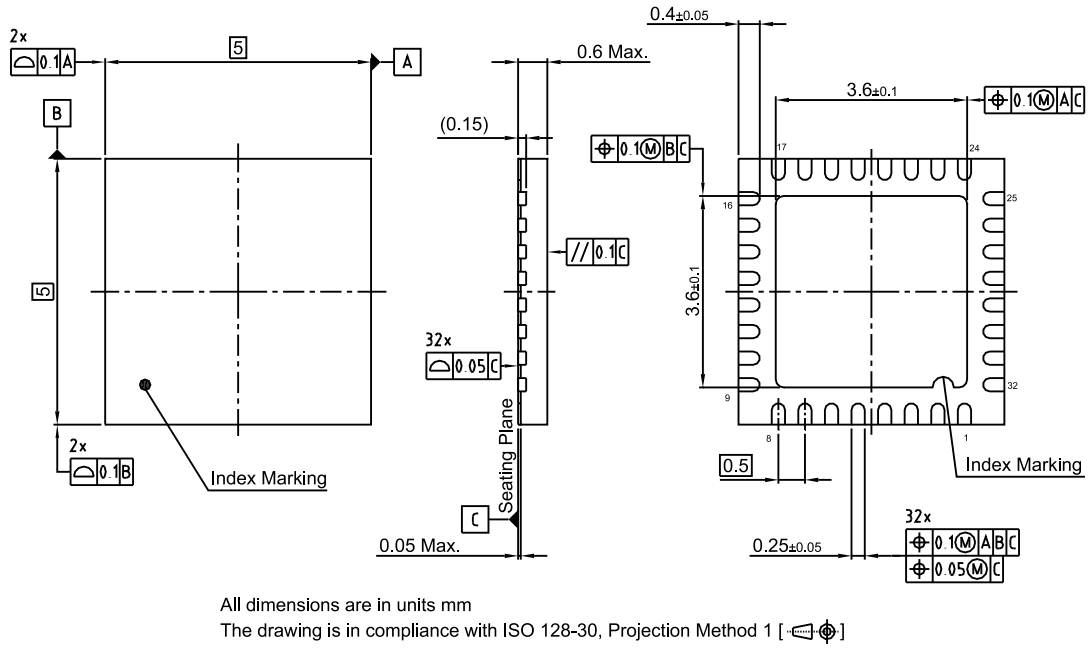

Figure 4 Package dimensions PG-UQFN-32-1,-2

6.1 Packing type

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

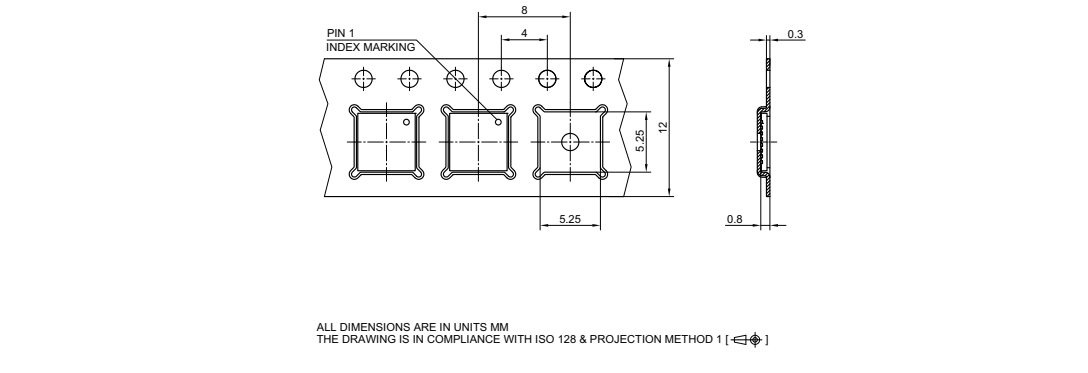

Figure 5 Tape & reel dimensions PG-UQFN-32-1,-2

6.2 Recommended footprint

Figure 6 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.

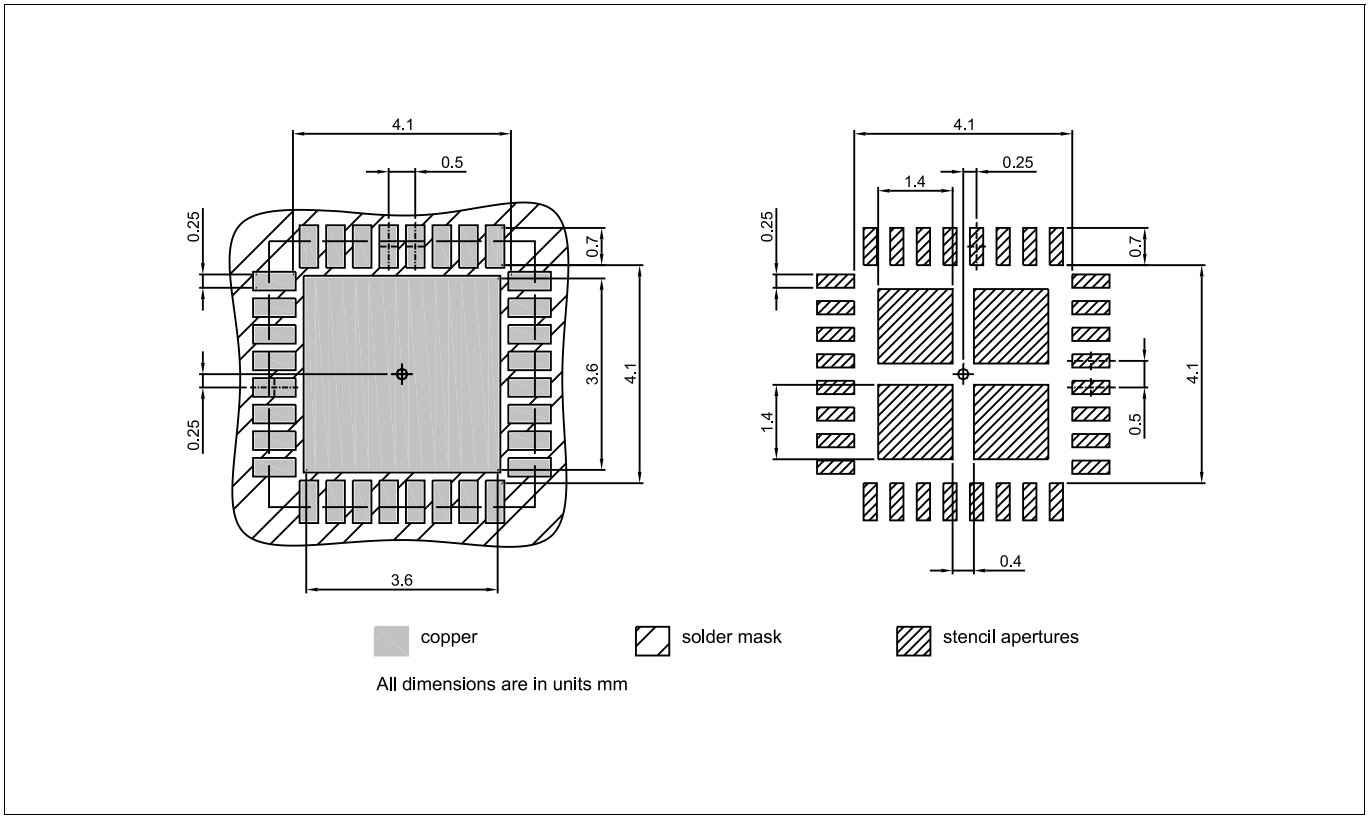

Figure 6 Recommended footprint PG-UQFN-32-1,-2

6.3 Chip marking

Line 1: SLB9672

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

Line 3: <Lot number> H <datecode>

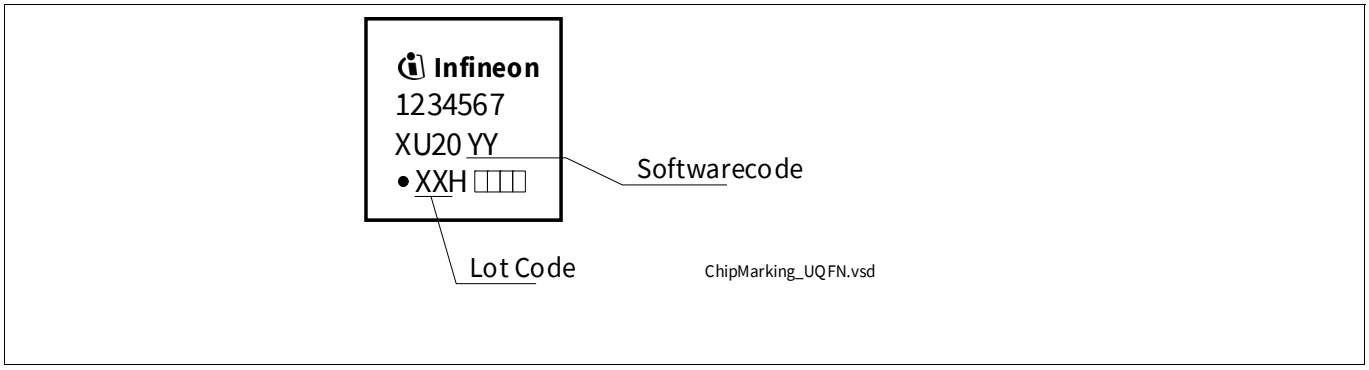

Figure 7 Chip marking

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

References

[1] —, “Trusted Platform Module Library (Part 1-4)”, Family 2.0, Level 00, Rev. 01.59, November 8, 2019, TCG

[2] —, “TCG PC Client Platform TPM Profile (PTP) Specification”, Family 2.0, Level 00, Rev. 01.05 v14, September 4, 2020, TCG

[3] —, “Errata For TCG Trusted Platform Libary, Family 2.0, Level 00, Rev. 01.59, November 8, 2019”, Errata Version 1.1, June 18, 2020, TCG

[4] —, “Errata for PC Client Platform TPM Profile for TPM 2.0 Version 1.05 Revision 14”, Errata Version 1.0, September 04, 2020, TCG

[5] —, “Registry of reserved TPM 2.0 handles and localities”, Version 1.1, Rev. 1.00, February 6, 2019, TCG

[6] —, “TCG EK Credential Profile”, Version 2.3, Rev. 2, July 23, 2020, TCG

[7] —, "NIST Special Publication 800-193, Platform Firmware Resiliency Guidelines", May, 2018, NIST

Terminology

ESW	Embedded Software
HMAC	Hashed Message Authentication Code
PCR	Platform Configuration Register
PUBEK	Public Endorsement Key
SPI	Serial Peripheral Interface (bus)
TCG	Trusted Computing Group
TPM	Trusted Platform Module
TSS	TCG Software Stack

Licenses and notices

The following license and notice statements are reproduced from [1].

Licenses and Notices

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.

Revision history	
Page or item	**Subjects (major changes since previous revision)**
Revision 1.1, 2023-04-27	
	Added features to front page Fixed wrong revision number in **Section 1** Changed **Figure 2** (additional decoupling capacitor) Updated version and build numbers in **Section 4** 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 2023-04-27
Published by
Infineon Technologies AG
81726 Munich, Germany

Do you have a question about any aspect of this document?
Email:
csscustomerservice@infineon.com

IMPORTANT NOTICE

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

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

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

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

For further information on technology, delivery terms and conditions and prices, please contact the nearest Infineon Technologies Office (**www.infineon.com**).

WARNINGS

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

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