OPTIGA™ TPM SLB 9670 TPM2.0

Trusted Platform Module

Data Sheet

Devices

- SLB 9670VQ2.0
- SLB 9670XQ2.0

Key Features

- Compliant to TPM Main Specification, Family "2.0"
- Hardware and firmware are validated according to FIPS 140-2 Level 2
- SPI interface
- Meeting Intel TXT, Microsoft Windows and Google Chromebook certification criteria for successful platform qualification
- Random Number Generator (RNG) according to NIST SP800-90A
- Full personalization with Endorsement Key (EK) and EK certificate
- Standard (-20..+85°C) and enhanced temperature range (-40..+85°C)
- PG-VQFN-32-13 package
- Pin compatible to OPTIGA™ TPM SLB 9670 TPM1.2 version
- Optimized for battery operated devices: low standby power consumption (typ. 110µA)
- 24 PCRs (SHA-1 or SHA-256)
- Minimum of 6962 bytes free NV memory
- 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)
- Up to 8 NV counters
- Up to 1 kByte for command parameters and response parameters
- Up to 768 Byte for NV read or NV write
- 1420 Byte I/O buffer
- Built-in support by Linux Kernel

About this document

Scope and purpose

This data sheet describes the OPTIGA™ TPM SLB 9670 TPM2.0 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 9670 is a Trusted Platform Module and is based on advanced hardware security technology. This TPM implementation has achieved CC EAL4+ certification and serves as a basis for other TPM products and firmware upgrades. It is available in PG-VQFN-32-13 package. It supports an SPI interface with a transfer rate of up to 43 MHz. The OPTIGA™ TPM SLB 9670 is a TPM based on TCG family 2.0 specifications (see [1], [2] and [3]).

1.1 Power Management

In the OPTIGA™ TPM SLB 9670, 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 / Ordering Information

The OPTIGA™ TPM SLB 9670 product family features devices using a VQFN package. Table 1 shows the different versions.

Table 1   Device Configuration

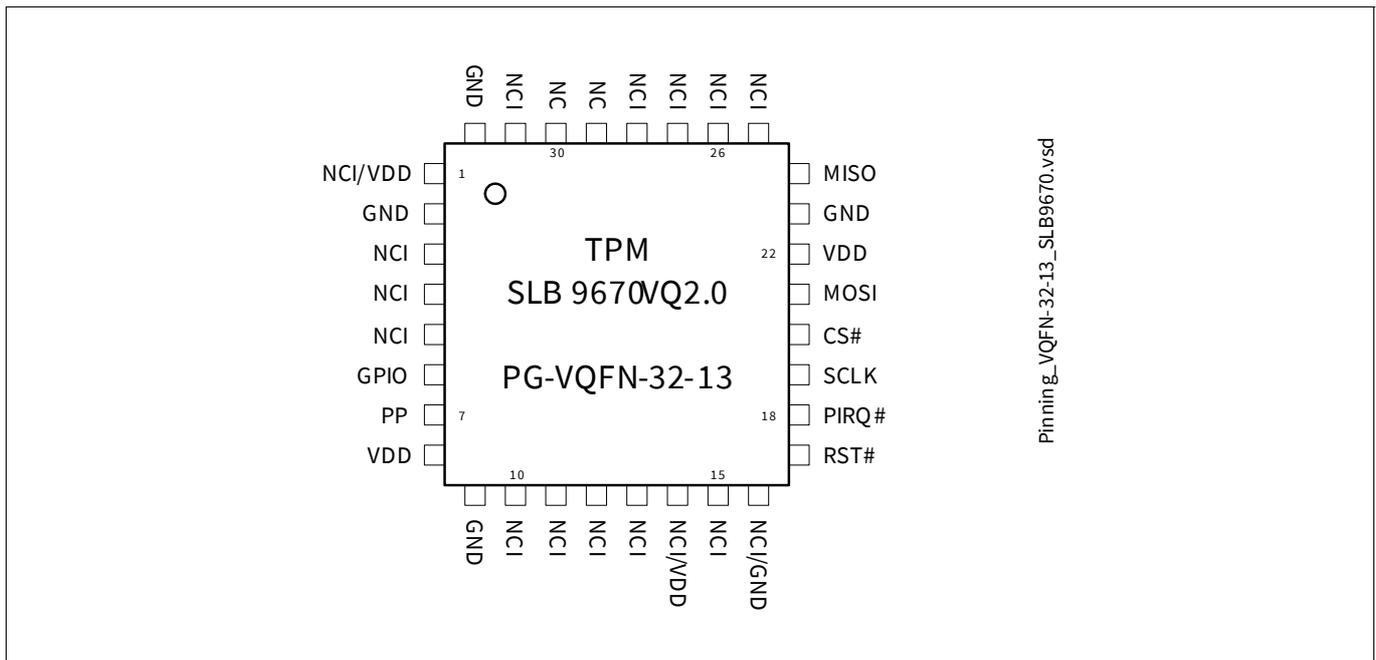| Device Name	Package	Remarks
SLB 9670VQ2.0	PG-VQFN-32-13	Standard temperature range
SLB 9670XQ2.0	PG-VQFN-32-13	Enhanced temperature range

3 Pin Description

Figure 1   Pinout of the OPTIGA™ TPM SLB 9670 (PG-VQFN-32-13 Package, Top View)

Pin Description

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-VQFN-32-13	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.
6	GPIO	I/O	TS	**GPIO-Express-00 Signal** The TPM2.0 device does not use this functionality. This pin may be left unconnected; it has an internal pull-up resistor.
7	PP	I	ST	**Physical Presence** The TPM2.0 device does not use this functionality. This pin may be left unconnected; it has an internal pulldown resistor.

Table 4   Power Supply

Pin Number PG-VQFN-32-13	Name	Pin Type	Buffer Type	Function
8, 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-VQFN-32-13	Name	Pin Type	Buffer Type	Function
29, 30	NC	NU	—	**No Connect** All pins must not be connected externally (must be left floating).
3 - 5, 10 - 13, 15, 25 - 28, 31	NCI	—	—	**Not Connected Internally** All pins are not connected internally (can be connected externally).
1	NCI/VDD	—	—	**Not Connected Internally/VDD** This pin is not connected internally (can be connected externally). Note that pin 1 is defined as VDD in the TCG specification [3]. To be compliant, VDD can be connected to this pin.
14	NCI/VDD	—	—	**Not Connected Internally/VDD** This pin is not connected internally (can be connected externally). Note that pin 14 is defined as VDD in the TCG specification [3]. To be compliant and to ensure upwards compatibility to future TPMs, VDD must 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 [3]. To be compliant, GND can be connected to this pin.

3.1 Typical Schematic

Figure 2 shows the typical schematic for the OPTIGA™ TPM SLB 9670. The power supply pins should be bypassed to GND with capacitors located close to the device.
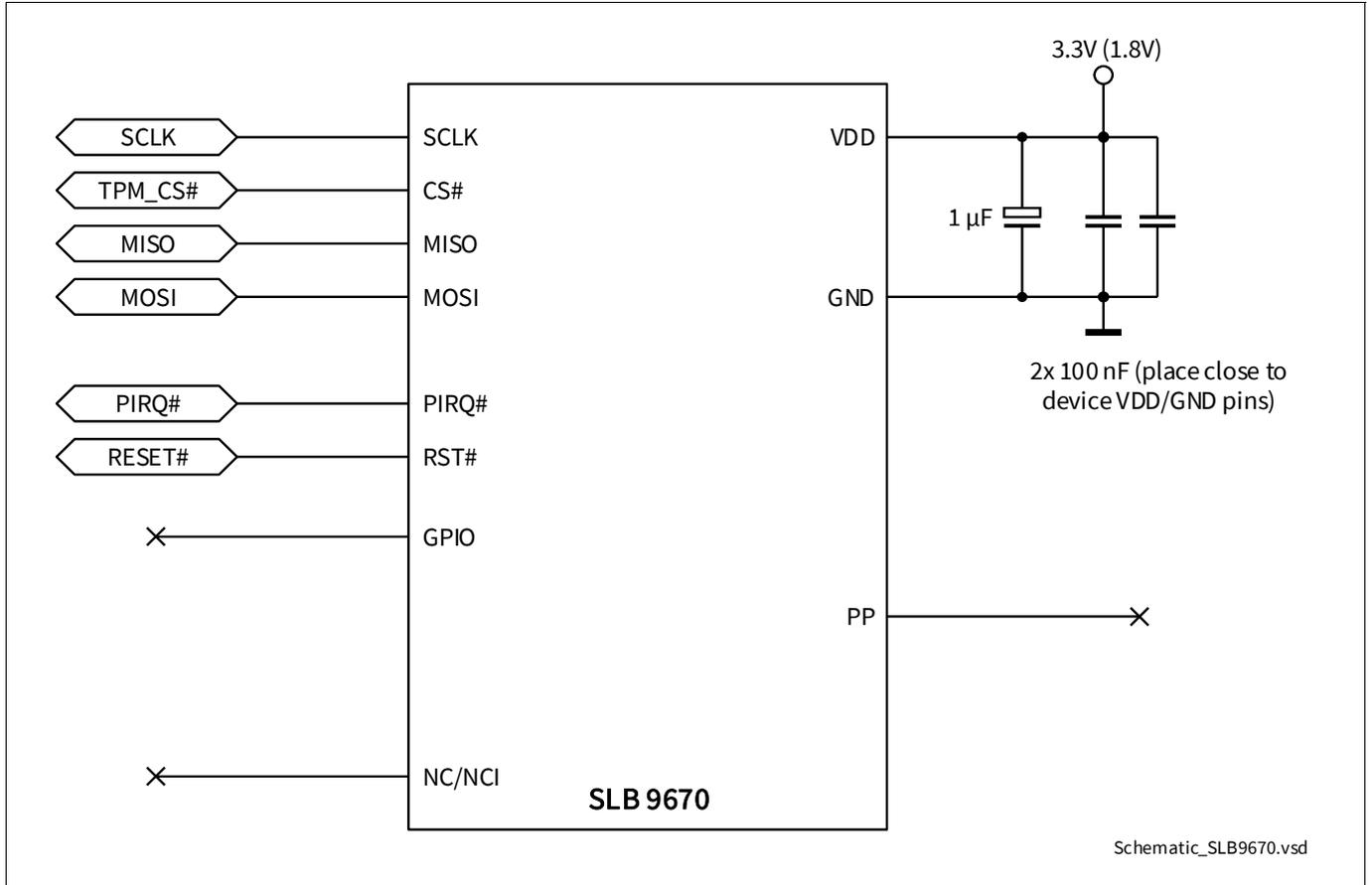

Figure 2   Typical Schematic

4 TPM Properties

All properties defined within the TPM can be read with the command TPM2_GetCapability (capability = TPM_CAP_TPM_PROPERTIES). The values are vendor dependent or determined by a platform-specific specification. The following properties are returned by the Infineon OPTIGA™ TPM SLB 9670:

Table 6   Infineon Specific Property Values

TPM_PT_MANUFACTURER	"IFX"
TPM_PT_VENDOR_STRING_1	"SLB9"
TPM_PT_VENDOR_STRING_2	"670"
TPM_PT_VENDOR_STRING_3	NULL
TPM_PT_VENDOR_STRING_4	NULL
TPM_PT_FIRMWARE_VERSION_1	Major and minor version (for instance, 0x00070055 indicates V7.85)
TPM_PT_FIRMWARE_VERSION_2	Build number and Common Criteria certification state (for instance, 0x0011CB00 or 0x0011CB02) Byte 1: reserved for future use (0x00) Byte 2 and 3: Build number (for instance, 0x11CB) Byte 4: Common Criteria certification state, 0x00 means TPM is CC certified, 0x02 means TPM is not certified
TPM_PT_MODES	Bit 0 (FIPS_140_2) = 1 Bits 1..31 = 0

Reading these properties returns the current version and state of the firmware. This implies that the values read back might differ from the ones shown in Table 6 above.

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	–	5.0	V	–
Voltage on any pin	V_{max}	-0.3	–	V_{DD}+0.3	V	–
		-0.5	–	V_{DD}+0.5	V	V_{DD} = 3.3V ± 10%; pins MISO, MOSI, SCLK and CS#
Ambient temperature	T_A	-20	–	85	°C	Standard temperature devices
Ambient temperature	T_A	-40	–	85	°C	Enhanced temperature 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	-20	–	85	°C	Standard temperature devices
Ambient temperature	T_A	-40	–	85	°C	Enhanced temperature 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} = 3.3V ± 0.3V or V_{DD} = 1.8V ± 0.15V 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}			25	mA	
Current Consumption in Sleep Mode	I_{VDD_Sleep}		110		µA	Pin PP = GND, pins GPIO, RST# and PIRQ# = V_{DD}, CS# inactive (= V_{DD}), MOSI, MISOand SCLK don't care

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

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	$V_{DD,typ}$ = 3.3V, only pins SCLK, MISO, MOSI and CS#
		0.7 V_{DD}		V_{DD}+0.3	V	$V_{DD,typ}$ = 3.3V, pin RST#
		0.7 V_{DD}		V_{DD}+0.3	V	$V_{DD,typ}$ = 1.8V
Input voltage low	V_{IL}	-0.5		0.3 V_{DD}	V	$V_{DD,typ}$ = 3.3V, only pins SCLK, MISO, MOSI and CS#
		-0.3		0.3 V_{DD}	V	$V_{DD,typ}$ = 3.3V, pin RST#
		-0.3		0.3 V_{DD}	V	$V_{DD,typ}$ = 1.8V
Input leakage current	I_{LEAK}	-20		20	µA	0V < V_{IN} < V_{DD}
		-150		150	µA	Pins SCLK, CS#, MISO, MOSI -0.5V < V_{IN} < V_{DD}+0.5V $V_{DD,typ}$ = 3.3V
		-150		150	µA	Pin RST# -0.5V < V_{IN} < V_{DD}+0.3V $V_{DD,typ}$ = 3.3V
		-150		150	µA	-0.3V < V_{IN} < V_{DD}+0.3V $V_{DD,typ}$ = 1.8V
Output high voltage	V_{OH}	0.9 V_{DD}			V	I_{OH} = -100µA
Output low voltage	V_{OL}			0.1 V_{DD}	V	I_{OL} = 1.5mA
Pad input capacitance	C_{IN}			10	pF	
Output load capacitance	C_{LOAD}			40	pF	

Electrical Characteristics

Table 11   DC Characteristics of GPIO and PP 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 and PP
Input voltage low	V_{IL}	-0.3		0.2 V_{DD}	V	Pins GPIO and PP
Input leakage current	I_{LEAK}	-20		20	µA	0V < V_{IN} < V_{DD}
		-150		150	µA	-0.3V < V_{IN} < V_{DD} + 0.3V
Output high voltage	V_{OH}	0.7 V_{DD}			V	I_{OH} = -1mA, pin GPIO
Output low voltage	V_{OL}			0.3	V	I_{OL} < 1mA, pin GPIO
Pad input capacitance	C_{IN}			10	pF	Pins GPIO and PP

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   Device Reset

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Cold (Power-On) Reset	t_{POR}	80			µs	see Section 5.5
Warm Reset	t_{WRST}	2			µs	see Section 5.5
Reset Inactive Time	t_{RSTIN}	60			ms	see Section 5.5
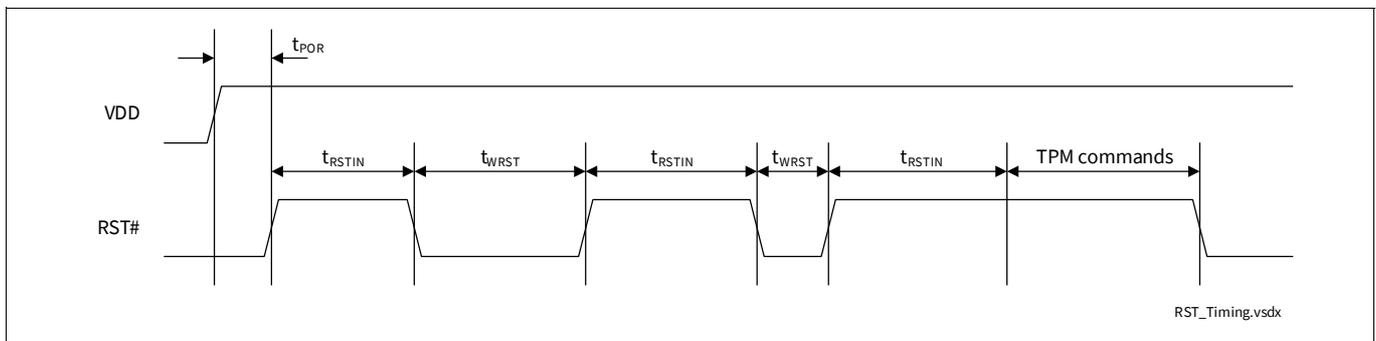
Figure 3   RST# Timing

Table 13   AC Characteristics of SPI Interface

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
SCLK frequency	f_{CLK}			43	MHz	$V_{DD,typ}$ = 3.3V, t_{SLEW} ≥ 1V/ns
				22.5	MHz	$V_{DD,typ}$ = 1.8V, t_{SLEW} ≥ 1V/ns
				38	MHz	$V_{DD,typ}$ = 3.3V, t_{SLEW} < 1V/ns
				18.5	MHz	$V_{DD,typ}$ = 1.8V, t_{SLEW} < 1V/ns
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 13   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	between 0.2 V_{DD} and 0.6 V_{DD}
CS# high time	t_{CS}	50			ns	Rising edge to falling edge
		60			ns	$V_{DD,typ}$ = 1.8V and t_{SLEW} < 1V/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	$V_{DD,typ}$ = 1.8V and t_{SLEW} < 1V/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

5.5   Timing

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

The OPTIGA™ TPM SLB 9670 features a sophisticated protection mechanism against dictionary attacks on TPM-based authorization data. Basically, the device counts the number of failed authorization attempts in a counter which is located in the non-volatile memory. An attacker who has physical access to the device could try to cirumvent that mechanism by resetting the device after the authorization attempt but before the updated failure counter has been written into the NVM.

Certain countermeasures have been added to the OPTIGA™ TPM SLB 9670. In certain time windows during power-on or warm boot of the device, such reset events might influence the dictionary attack counters and trigger other security mechanisms as well. In worst case, this might trigger special security defense modes from which a recovery is very complex or even not possible.

To avoid that the OPTIGA™ TPM SLB 9670 reaches such a security defense state, the RST# signal must not be asserted in certain time windows. After the deassertion of the RST# signal, the system should wait for a minimum time of t_{RSTIN} before asserting RST# again (see Figure 3 and Table 12).

TPM commands should only be started after t_{RSTIN} has expired (see Figure 3 again). 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.

6 Package Dimensions (VQFN)

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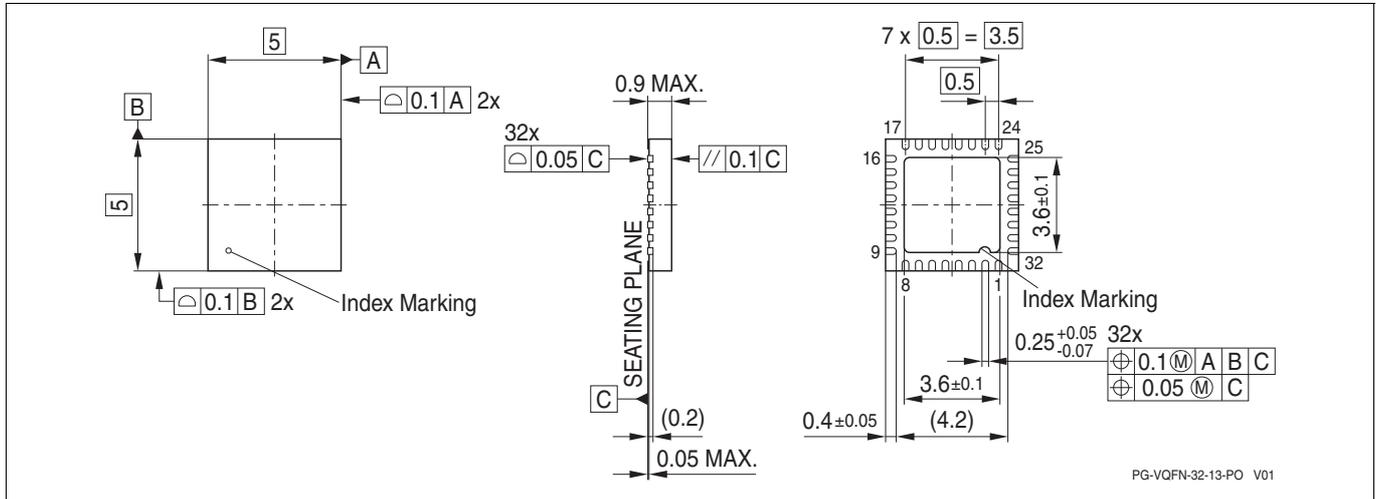

Figure 4   Package Dimensions PG-VQFN-32-13

6.1 Packing Type

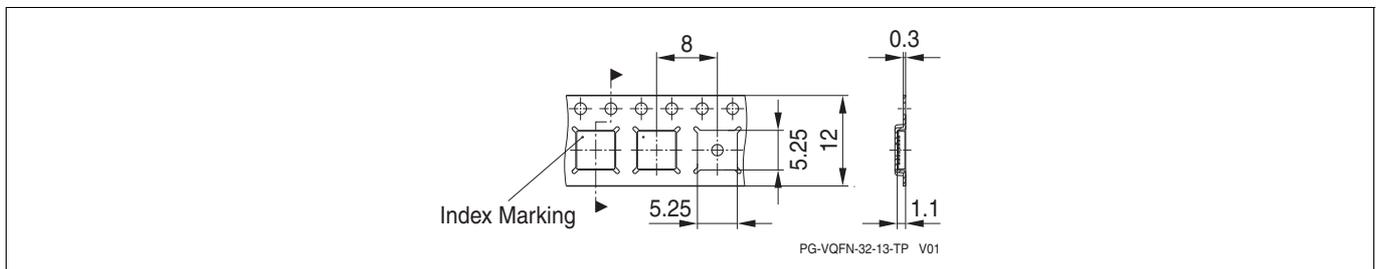PG-VQFN-32-13: Tape & Reel (reel diameter 330mm), 5000 pcs. per reel

Figure 5   Tape & Reel Dimensions PG-VQFN-32-13

6.2 Recommended Footprint

Figure 6 shows the recommended footprint for the PG-VQFN-32-13 package. The exposed pad of the package is internally connected to GND. It shall be connected to GND externally as well.
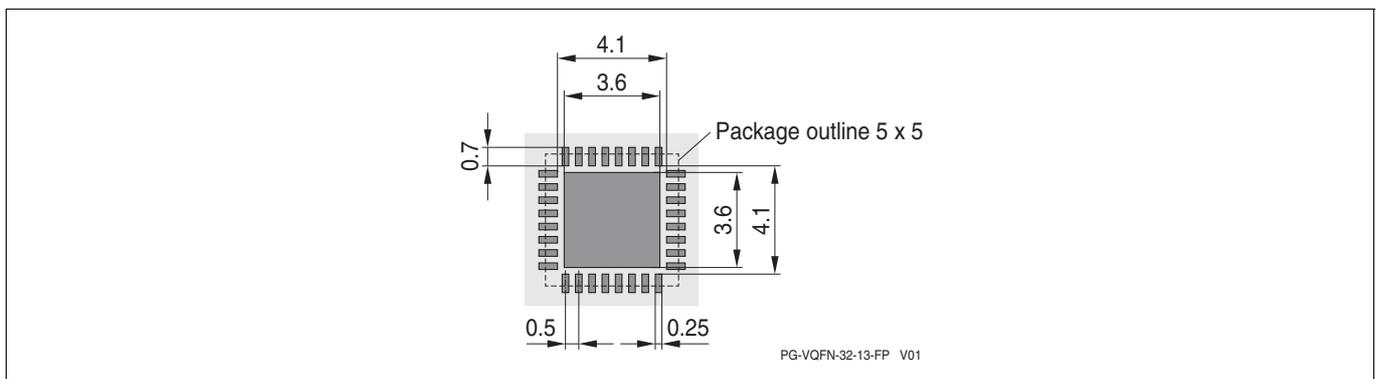

Figure 6   Recommended Footprint PG-VQFN-32-13

Package Dimensions (VQFN)

6.3   Chip Marking

Line 1: SLB 9670

Line 2: VQ20 yy or XQ20 yy (see Table 1), the <yy> is an internal FW indication (only at manufacturing due to field upgrade option)
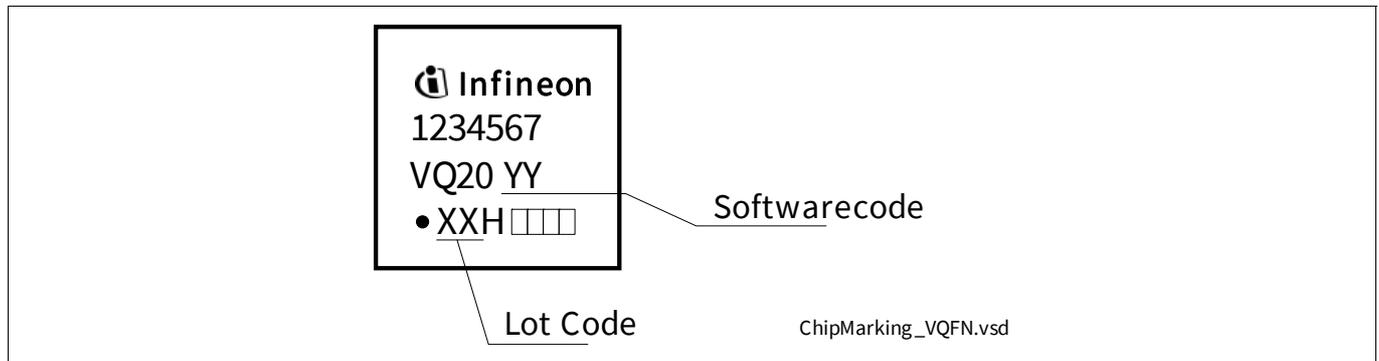
Line 3: <Lot number> H <datecode>

Figure 7   Chip Marking PG-VQFN-32-13

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. 01.16, 2014-10-30, TCG

[2] —, "Trusted Platform Module Library (Part 1-4)", Family 2.0, Level 00, Rev. 01.38, 2016-09-29, TCG

[3] —, "TCG PC Client Platform TPM Profile (PTP) Specification", Family 2.0, Level 00, Rev. 01.03 v22, May 22, 2017, TCG

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 [2].

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 1.4, 2018-12-07	
	Inserted new **Chapter 4** describing TPM properties.
Revision 1.3, 2018-11-26	
	Deleted UQFN package.
Revision 1.2, 2018-09-21	
	Updated document template. Added details to **Section 5.5**.
Revision 1.1, 2016-08-30	
	New document template. Changed SPI AC parameters (maximum clock frequeny, permissible SCLK slew rate, chip select high time and chip select setup time) in **Table 13**.
Revision 1.0, 2015-11-05	
	Initial version.

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

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.