OPTIGA™ TPM SLB 9670 TPM1.2

Trusted Platform Module

Data Sheet

Devices

- SLB 9670VQ1.2
- SLB 9670XQ1.2

Key Features

- Compliant to TPM Main Specification, Version 1.2, Rev. 116 (see [1])
- SPI interface
- Approved for Google Chromebook / Chromebox
- Standard (-20°C to +85°C) and enhanced temperature range (-40°C to +85°C)
- PG-VQFN-32-13 package
- Optimized for battery operated devices: low standby power consumption (typ. 110µA)
- 24 PCRs
- 6 kByte free NV memory
- Up to 10 concurrent sessions
- Up to eight 2048-bit keys can be loaded into volatile storage
- 16 slots for keys of up to 2048-bit
- 8 monotonic counters
- 1280 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 TPM1.2 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

Table of contents . . . 2
List of figures . . . 3
List of tables . . . 4
1 Overview . . . 5
1.1 Power Management . . . 5
2 Device Types / Ordering Information . . . 5
3 Pin Description . . . 5
3.1 Typical Schematic . . . 8
4 Electrical Characteristics . . . 9
4.1 Absolute Maximum Ratings . . . 9
4.2 Functional Operating Range . . . 9
4.3 DC Characteristics . . . 10
4.4 AC Characteristics . . . 11
4.5 Timing . . . 12
5 Package Dimensions (VQFN) . . . 13
5.1 Packing Type . . . 13
5.2 Recommended Footprint . . . 13
5.3 Chip Marking . . . 14
References . . . 15
Terminology . . . 16

List of figures

Figure 1 Pinout of the SLB 9670VQ1.2 and SLB 9670XQ1.2 (PG-VQFN-32-13 Package, Top View) 5
Figure 2 Typical Schematic 8
Figure 3 RST# Timing 11
Figure 4 Package Dimensions PG-VQFN-32-13 13
Figure 5 Tape & Reel Dimensions PG-VQFN-32-13 13
Figure 6 Recommended Footprint PG-VQFN-32-13 13
Figure 7 Chip Marking PG-VQFN-32-13 14

List of tables

Table 1 Device Configuration 5
Table 2 Buffer Types 6
Table 3 I/O Signals 6
Table 4 Power Supply 7
Table 5 Not Connected 7
Table 6 Absolute Maximum Ratings 9
Table 7 Functional Operating Range 9
Table 8 Current Consumption 10
Table 9 DC Characteristics of SPI Interface Pins (SCLK, CS#, MISO, MOSI, RST#, PIRQ#) 10
Table 10 DC Characteristics of GPIO and PP Pins 11
Table 11 Device Reset 11
Table 12 AC Characteristics of SPI Interface 11

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 specification version 1.2 (see [1] and [2]).

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 9670VQ1.2	PG-VQFN-32-13	Standard temperature range
SLB 9670XQ1.2	PG-VQFN-32-13	Enhanced temperature range

3 Pin Description

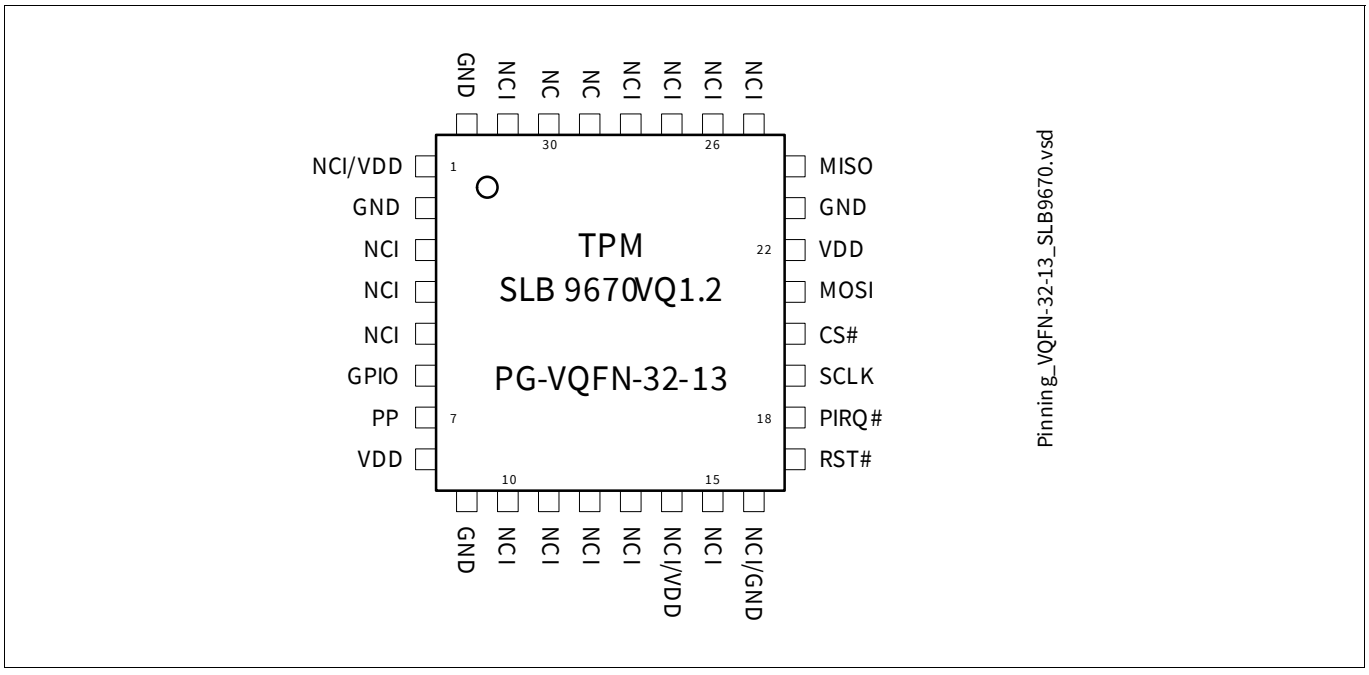

Figure 1 Pinout of the SLB 9670VQ1.2 and SLB 9670XQ1.2 (PG-VQFN-32-13 Package, Top View)

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** This pin is a general purpose I/O pin. It is defined as GPIO-Express-00, please refer to [2] and the PCISIG ECN “Trusted Configuration Space for PCI Express”. This pin may be left unconnected; it has an internal pull-up resistor.
7	PP	I	ST	**Physical Presence** This pin should be connected to a jumper. The standard position of the jumper should connect the pin to GND. If the pin is connected to VDD, some special commands are enabled (for instance, the command TPM_ForceClear, also refer to [1]). This pin may be left unconnected; it has an internal pull-down resistor.

Pin Description

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 [5]. 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 [5]. 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 [5]. 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. The physical presence input may be connected to a jumper as shown in the schematic; or it may be driven by other devices (this is application- or platform-dependent).

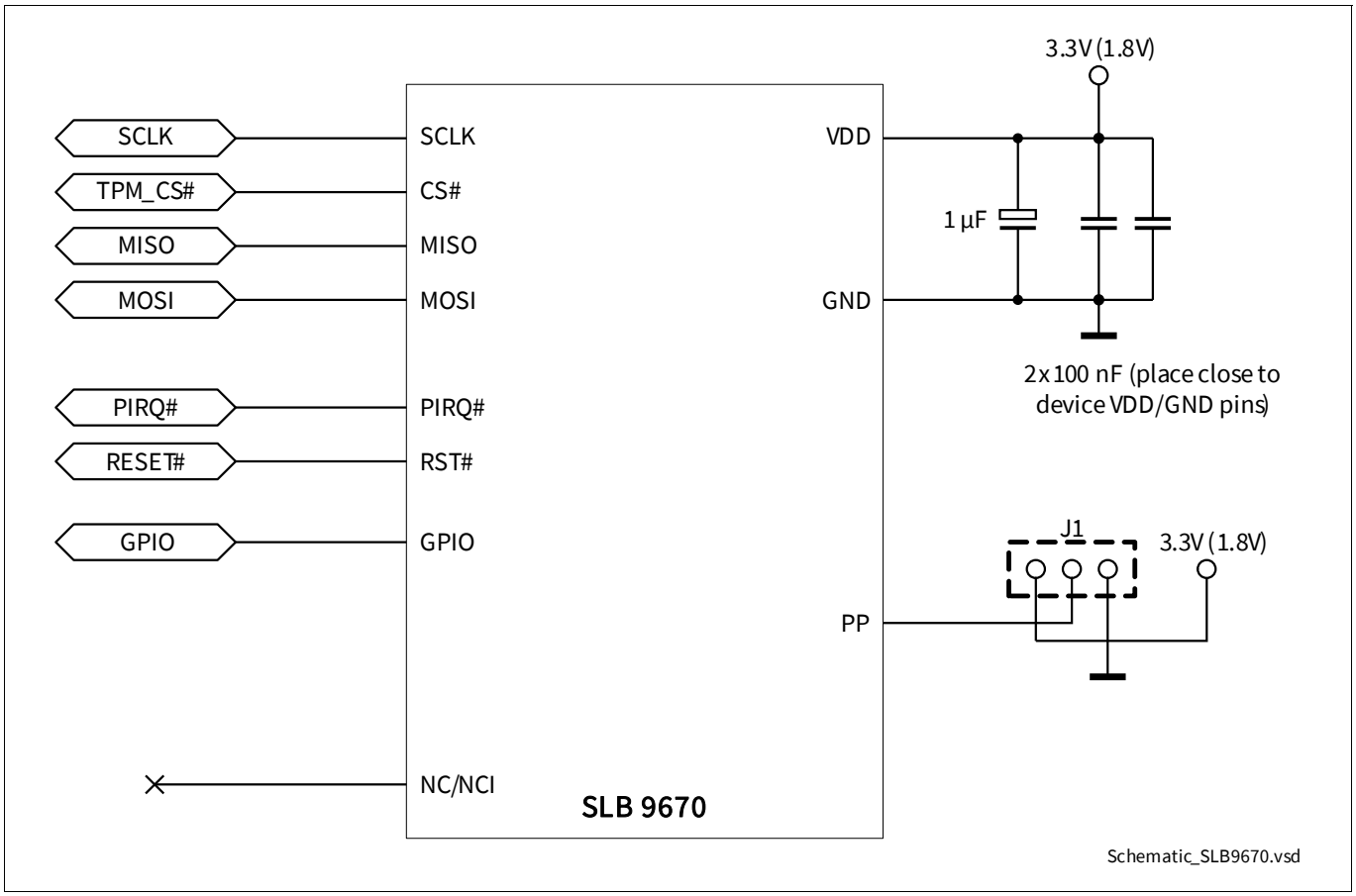

Figure 2 Typical Schematic

4 Electrical Characteristics

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

4.1 Absolute Maximum Ratings

Table 6 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.

4.2 Functional Operating Range

Table 7 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	

4.3 DC Characteristics

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

Table 8 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, MISO and SCLK don't care

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

Table 9 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	

Table 10 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

4.4 AC Characteristics

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

Table 11 Device Reset

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Cold (Power-On) Reset	t_{POR}	80			µs	see Section 4.5
Warm Reset	t_{WRST}	2			µs	see Section 4.5
Reset Inactive Time	t_{RSTIN}	30			ms	see Section 4.5

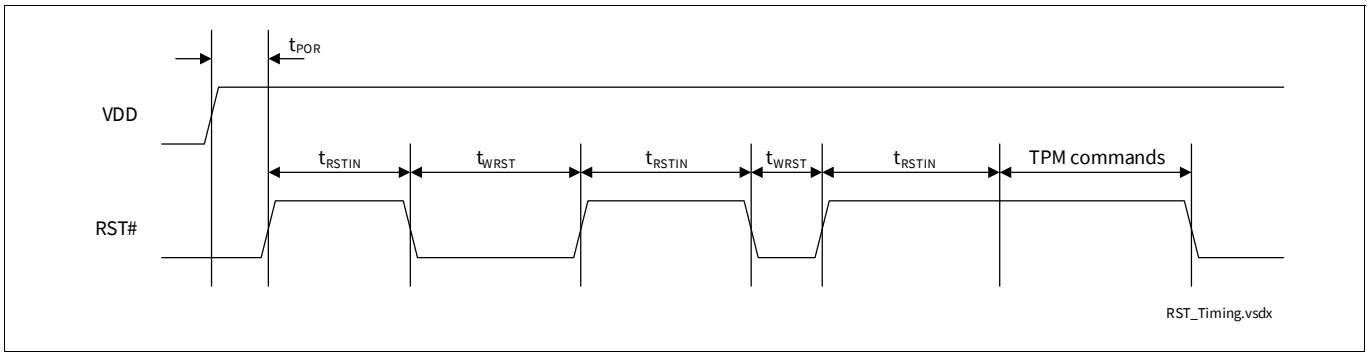

Figure 3 RST# Timing

Table 12 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 12 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

4.5 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 11).

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.

5 Package Dimensions (VQFN)

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

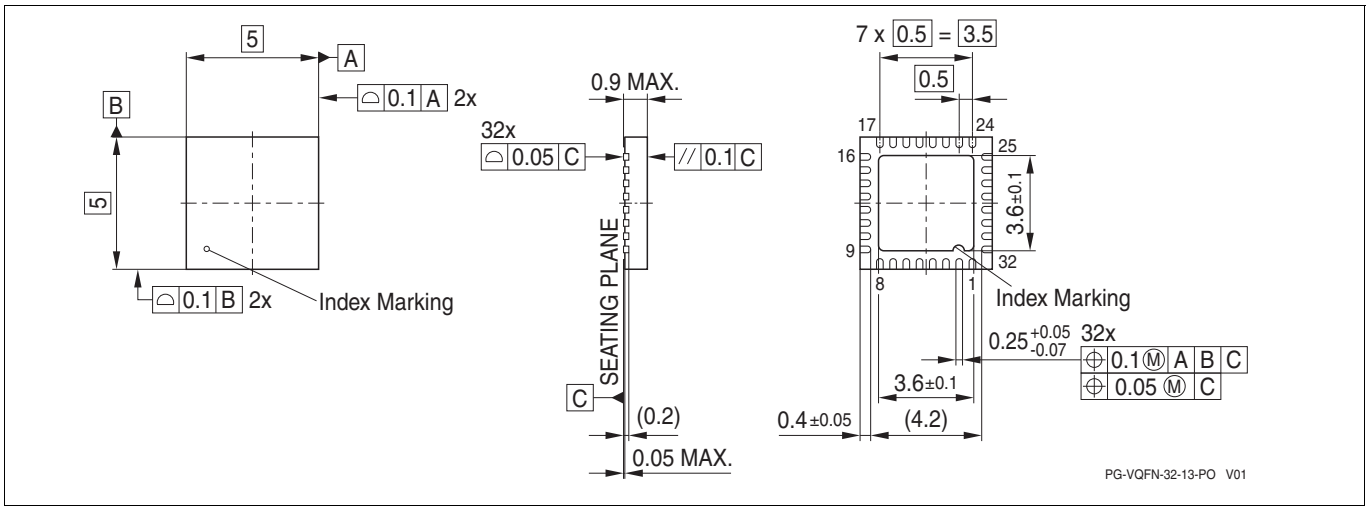

Figure 4 Package Dimensions PG-VQFN-32-13

5.1 Packing Type

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

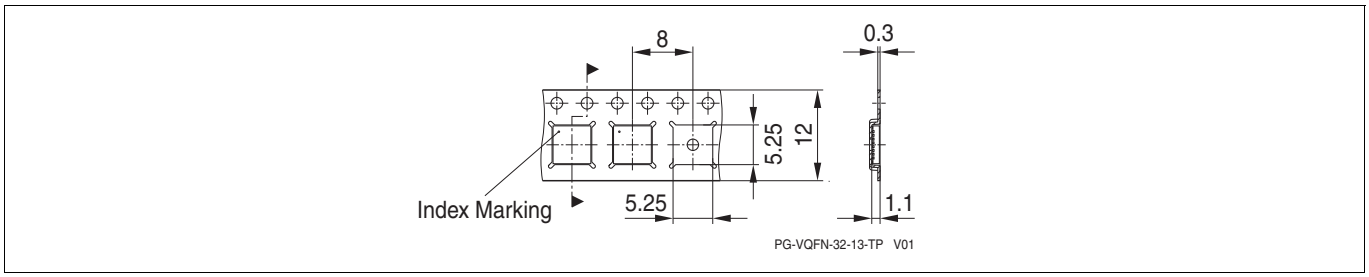

Figure 5 Tape & Reel Dimensions PG-VQFN-32-13

5.2 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.

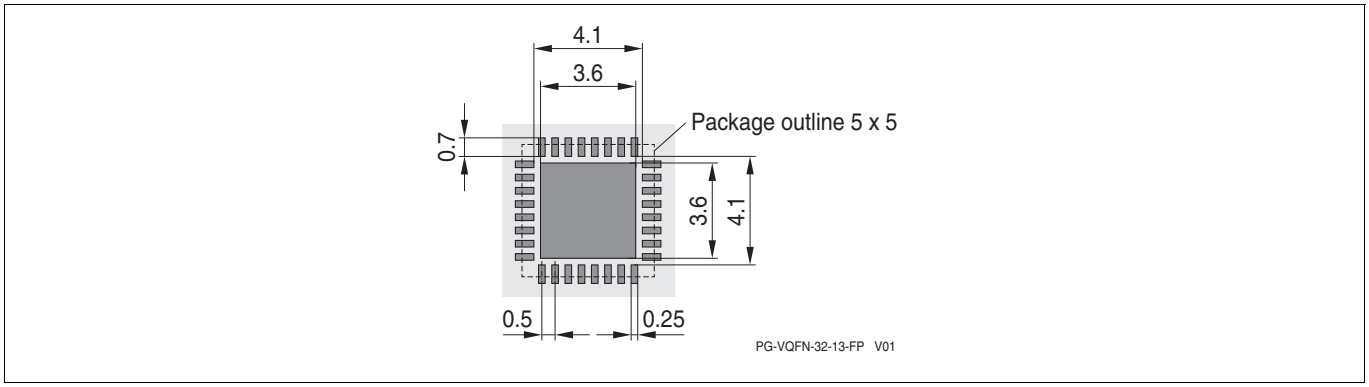

Figure 6 Recommended Footprint PG-VQFN-32-13

5.3 Chip Marking

Line 1: SLB9670

Line 2: VQ12 yy or XQ12 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>

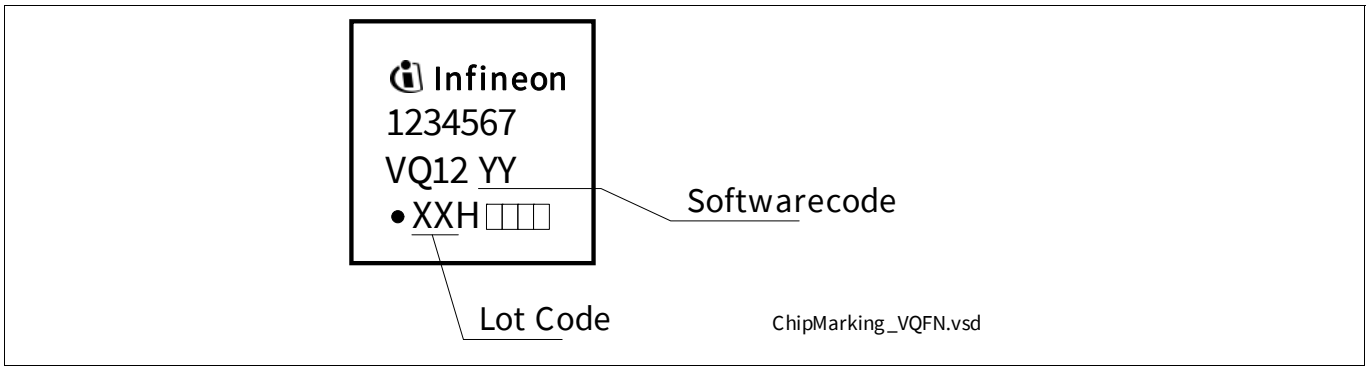

Figure 7 Chip Marking PG-VQFN-32-13

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

References

[1] —, “TPM Main Specification”, Version 1.2, Rev. 116, 2011-03-01, TCG (parts 1-3)

[2] —, “TCG PC Client TPM Interface Specification (TIS)”, Version 1.3, 2013-03-21, TCG

[3] —, “PC Client Implementation Specification”, Version 1.2, 2005-07-13, TCG

[4] —, “TCG Software Stack Specification (TSS)”, Version 1.2, 2005-11-02, TCG

[5] —, “TCG PC Client Platform TPM Profile (PTP) Specification”, Rev. 00.43, 2014-08-04, TCG

Terminology

ERD	Early Reset Detection
ESW	Embedded Software
HMAC	Hashed Message Authentication Code
LPC	Low Pin Count (bus)
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

Revision History	
Page or Item	**Subjects (major changes since previous revision)**
Revision 1.3, 2018-09-21	
	Updated document template. Added details to Section 4.5.
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 12.
Revision 1.1, 2016-02-12	
	Updated lifetime parameters in Table 7.
Revision 1.0, 2015-11-05	
	Initial version.

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

Edition 2018-09-21
Published by
Infineon Technologies AG
81726 Munich, Germany

Do you have a question about any aspect of this document?
Email:
security.chipcard.ics@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.