OPTIGA™ TPM

SLB 9645 TPM1.2

Data Sheet

Devices

- SLB 9645VQ1.2
- SLB 9645XQ1.2
- SLB 9645TT1.2
- SLB 9645XT1.2

Key Features

- Compliant to TPM Main Specification, Version 1.2, Rev. 116 (see [1])
- I2C 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 or PG-TSSOP-28-2 package
- Optimized for battery operated devices: low standby power consumption (typ. 150µA)
- 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 9645 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

List of figures

List of tables

1 Overview

The OPTIGA™ TPM SLB 9645 is a Trusted Platform Module. It is available in different packages, see Table 1 below. It only supports the I2C interface and features a dedicated interrupt pin which increases performance (since no polling on the I2C bus is necessary). The I2C interface is compliant to both standard mode operation (up to 100 kHz) and fast mode operation (up to 400 kHz); for details regarding the characteristics in these modes, please refer to Section 4.6.

2 Device Types / Ordering Information

The OPTIGA™ TPM SLB 9645 product family features devices with different packages and different temperature ranges. Table 1 shows the available versions.

Table 1 Device Types

Device Name	Package	Remarks
SLB 9645VQ1.2	PG-VQFN-32-13	Standard temperature range
SLB 9645XQ1.2	PG-VQFN-32-13	Enhanced temperature range
SLB 9645TT1.2	PG-TSSOP-28-2	Standard temperature range
SLB 9645XT1.2	PG-TSSOP-28-2	Enhanced temperature range

3 Pin Description

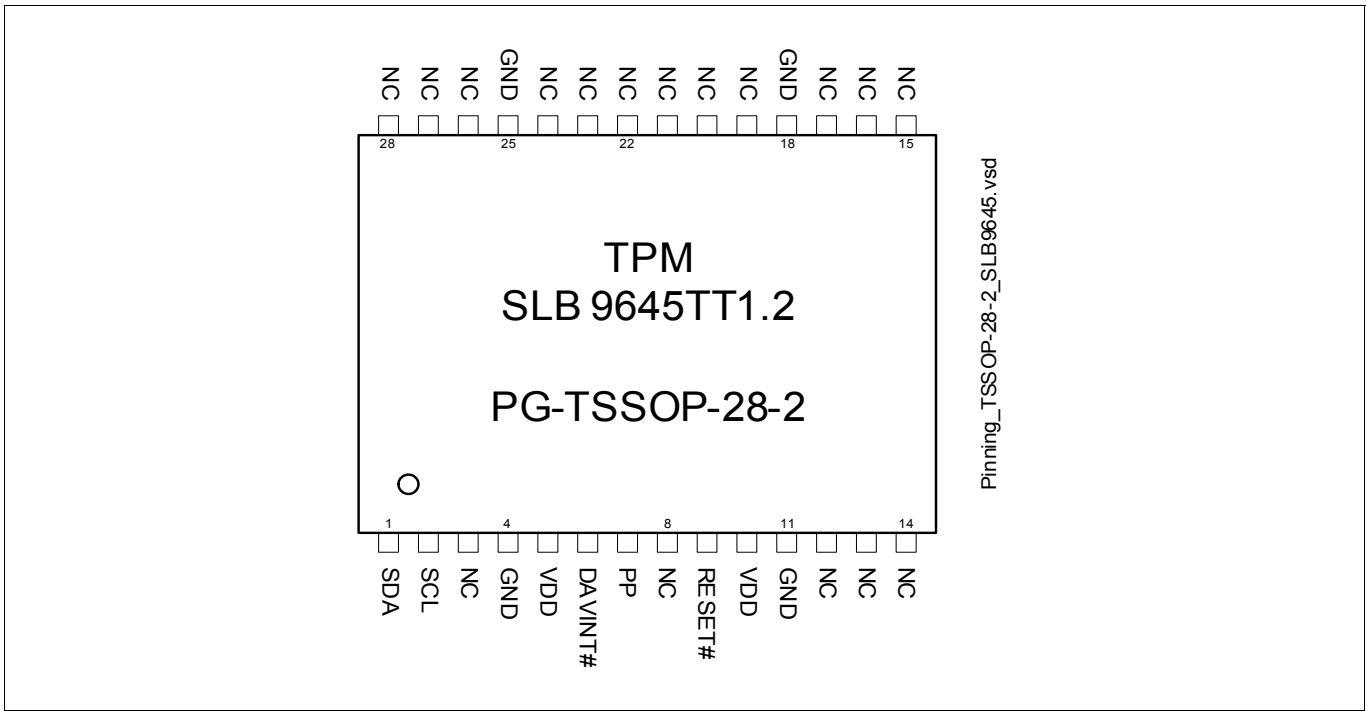

Figure 1 Pinout of the SLB 9645TT1.2 / SLB 9645XT1.2 (PG-TSSOP-28-2 Package, Top View)

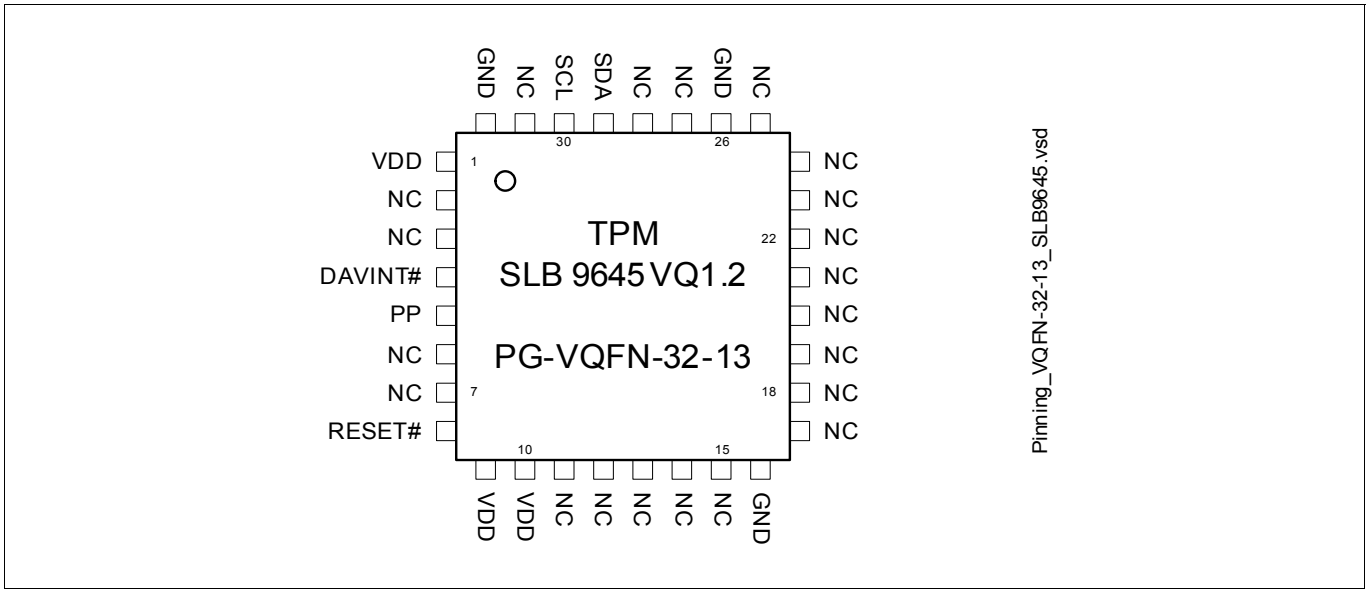

Figure 2 Pinout of the SLB 9645VQ1.2 / SLB 9645XQ1.2 (PG-VQFN-32-13 Package, Top View)

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		Name	Pin Type	Buffer Type	Function
PG-TSSOP-28-2	PG-VQFN-32-13				
1	29	SDA	I/O	OD	**I2C Bus Data Signal** The data line of the I2C bus.
2	30	SCL	I/O	OD	**I2C Bus Clock Signal** The clock signal of the I2C bus.
9	8	RESET#	I	ST	**Reset** External reset signal. Asserting this pin unconditionally resets the device. The signal is active low.

Table 3 I/O Signals (continued)

Pin Number		Name	Pin Type	Buffer Type	Function
PG-TSSOP-28-2	PG-VQFN-32-13				
6	4	DAVINT#	I/O	ST	**Data Available Interrupt** This pin can be connected to the host interrupt controller to allow interrupt driven reads of the response data instead of polling of the TPM_STS_x.dataAvail bit. The signal remains inactive (high) as long as TPM_STS_x.dataAvail is 0. As soon as a response is available, the signal is asserted (low) and remains active until the complete response is read by the host.
7	5	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 does not have an internal pull-up or pulldown resistor and must not be left floating if it is used for physical presence detection via hardware pin. If physical presence detection via hardware pin is not used, this pin may be left unconnected; however, to minimize power consumption, it shall be connected to a fixed level (either GND or VDD).

Table 4 Power Supply

Pin Number		Name	Pin Type	Buffer Type	Function
PG-TSSOP-28-2	PG-VQFN-32-13				
5, 10	1, 9, 10	VDD	PWR	—	**Power Supply** All VDD pins must be connected externally and should be bypassed to GND via 100 nF capacitors.
4, 11, 18, 25	16, 26, 32	GND	GND	—	**Ground** All GND pins must be connected externally.

Table 5 Not Connected

Pin Number		Name	Pin Type	Buffer Type	Function
PG-TSSOP-28-2	PG-VQFN-32-13				
3, 8, 12 - 17, 19 - 24, 26 - 28	2, 3, 6, 7, 11 - 15, 17 - 25, 27, 28, 31	NC	NU	—	**Not Connected** All NC pins must not be connected externally (must be left floating).

3.1 Typical Schematic

Figure 3 shows the typical schematic for the OPTIGA™ TPM SLB 9645. 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).

Note that pull-up resistors are needed on the I2C clock and data signals, these are not shown in the schematic.

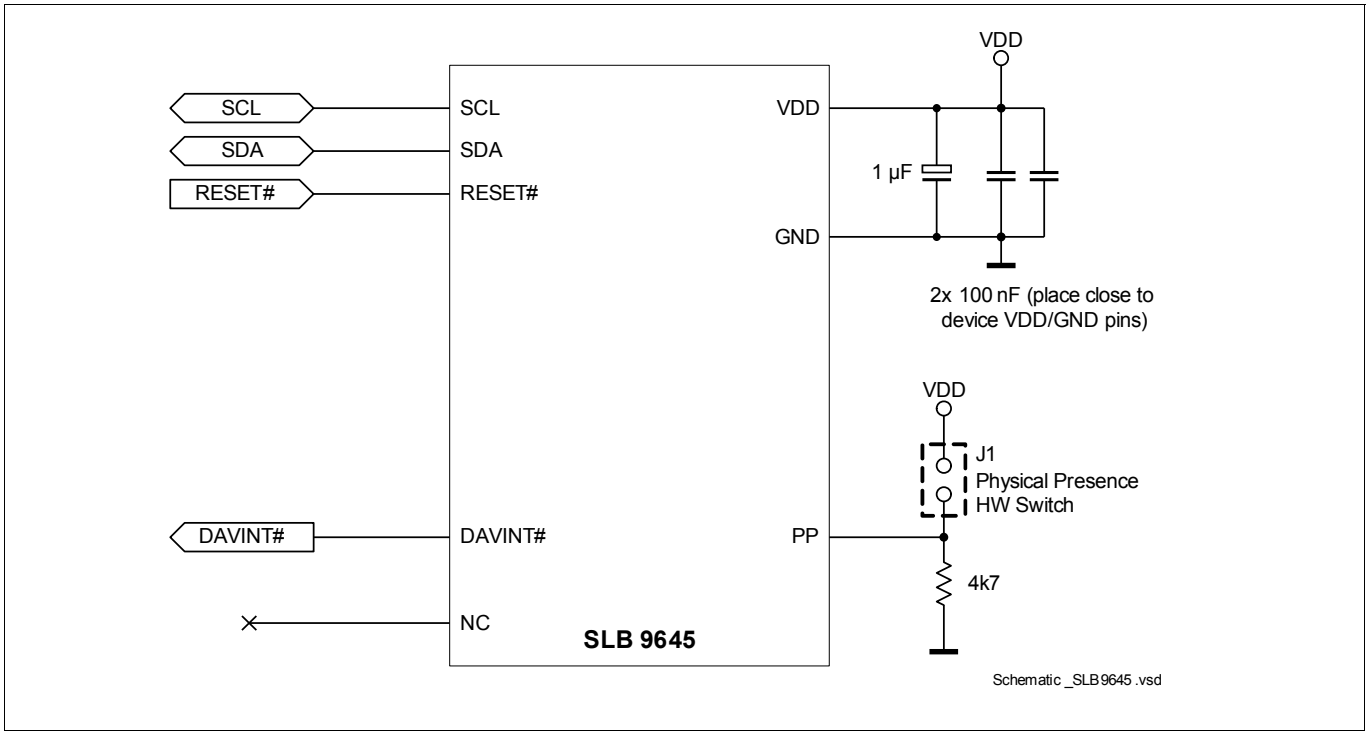

Figure 3 Typical Schematic

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	–	7	V	–
Voltage on any pin	V_{max}	-0.3	–	V_{DD}+0.3	V	–
Ambient temperature	T_A	-40	–	85	°C	–
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	3.3 V system environment
Supply Voltage	V_{DD}	1.62	1.8	1.98	V	1.8 V system environment
Ambient temperature	T_A	-20	–	85	°C	Standard temperature range devices
Ambient temperature	T_A	-40	–	85	°C	Enhanced temperature range 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 1.8V ± 0.18V 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}		3.0	25	mA	V_{DD} = 3.3V ± 0.3V Device is active and is operating internally. Note that since the device is mostly in an internal sleep state in a “typical” application, the typical average current consumption is far less than the maximum value. It is assumed that in a normal environment, the device is in an internal sleep state for approximately 90% of the operating time of the platform.
Current Consumption in Sleep Mode	I_{VDD_Sleep}		0.9		mA	V_{DD} = 3.3V ± 0.3V Device is active, SCL is toggling but no ongoing internal TPM operation. The device is in an internal sleep state.
Current Consumption in Sleep Mode with Stopped Clock	$I_{VDD\_Sleep\_CS}$		150		µA	V_{DD} = 3.3V ± 0.3V Device is active, SCL is not toggling and no ongoing internal TPM operation. The device is in an internal sleep state.

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

Table 9 DC Characteristics

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	All pins except RESET#
Input voltage low	V_{IL}	-0.3		0.3 V_{DD}	V	All pins except RESET#
Input voltage high	V_{IH}	0.8 V_{DD}		V_{DD}	V	Pin RESET#
Input voltage low	V_{IL}	0		0.2 V_{DD}	V	Pin RESET#
Input high leakage current	I_{IH}	-15		15	µA	V_{IN} = V_{DD}
Input low leakage current	I_{IL}	-15		15	µA	V_{IN} = 0V
Output high voltage	V_{OH}	V_{DD}-0.3			V	I_{OH} = 1mA
Output low voltage	V_{OL}			0.3	V	I_{OL} = 1mA

4.4 AC Characteristics

T_A = 25°C, V_{DD} = 3.3V ± 0.3V or 1.8V ± 0.18V unless otherwise noted

Table 10 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}	10			µs	
Reset Inactive Time	t_{RSTIN}	30			ms	

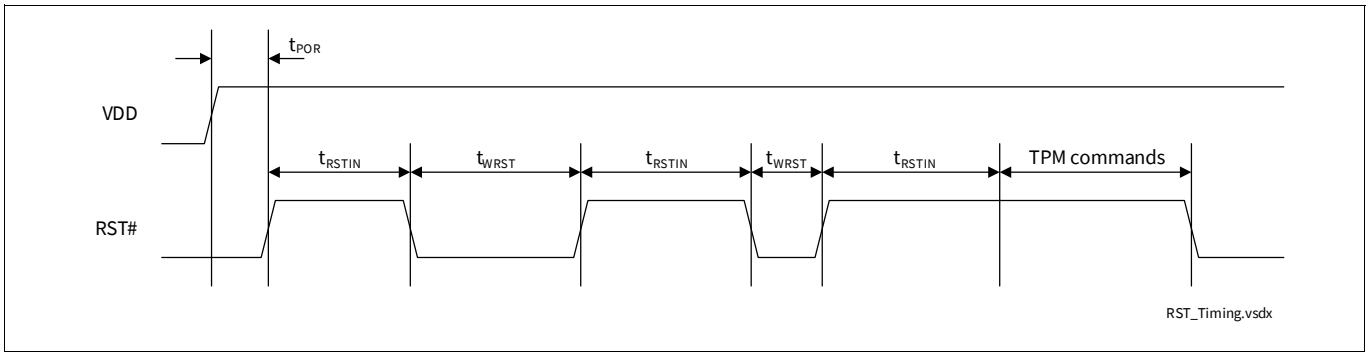

Figure 4 RST# Timing

4.5 Timing

The TPM_ACCESS_x.tpmEstablishment bit has the correct value and the TPM_ACCESS_x.tpmRegValidSts bit is typically set within 8ms after RESET# is deasserted.

The TPM is ready to receive a command after less than 30 ms.

The OPTIGA™ TPM SLB 9645 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 circumvent that mechanism by resetting the device after the authorization attempt but before the updated failure counter has been written into the NVM.

As a countermeasure, another feature called early reset detection (ERD) has been added to the OPTIGA™ TPM SLB 9645. This mechanism detects external resets and counts them. 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 9645 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 4 and Table 10).

TPM commands should only be started after t_{RSTIN} has expired (see Figure 4 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 TPM_SaveState should be issued before the assertion of the RST# signal.

4.6 I2C Standard/Fast Mode Interface Characteristics

The electrical characteristics are compliant to the NXP I²C bus specification [5] and [6] for “standard-mode” (f_{SCL} ≤ 100 kHz) and “fast-mode” (f_{SCL} ≤ 400 kHz), with certain deviations stated in Table 11 and Table 12 below.

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

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

Table 11 I2C Standard Mode Interface Characteristics

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
SCL clock frequency	f_{SCL}	0	—	100	kHz	—
Output fall time from V_{IHmin} to V_{ILmax} (at device pin)	t_{OF}	—	—	75	ns	10 pF ≤ C_b ≤ 400 pF
SCL fall time (bus line, output)	t_{fSCL}	—	—	25	ns	—

Table 12 I2C Fast Mode Interface Characteristics

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
SCL clock frequency	f_{SCL}	0	—	400	kHz	—
Hysteresis of input stage	V_{HYS}	0.05	—	—	V	—
Output fall time from V_{IHmin} to V_{ILmax} (at device pin)	t_{OF}	0.4	—	75	ns	10 pF ≤ C_b ≤ 400 pF
Spikes suppressed by input filter	t_{SP}	—	20	—	ns	Input filter implemented for SCL, not for SDA
SCL fall time (bus line, output)	t_{fSCL}	—	—	25	ns	—
Input current (SCL, SDA)	I_I	-10	—	10	µA	V_{IN} between 10% and 90% of the supply voltage V_{DD}; the condition “If VDD is switched off, I/O pins of fast-mode devices must not obstruct the SDA and SCL lines” is not fulfilled.

5 Package Dimensions (TSSOP)

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

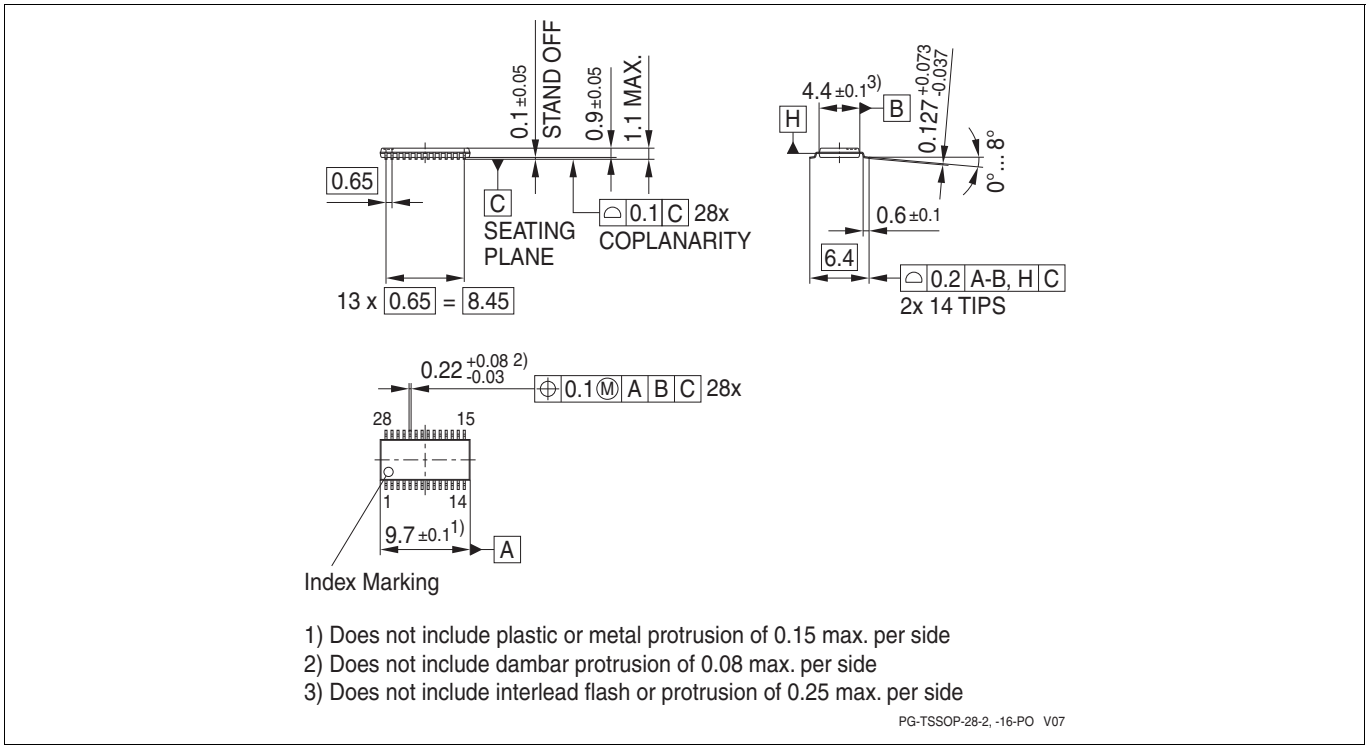

Figure 5 Package Dimensions PG-TSSOP-28-2

5.1 Packing Type

PG-TSSOP-28-2: Tape & Reel (reel diameter 330mm), 3000 pcs. per reel

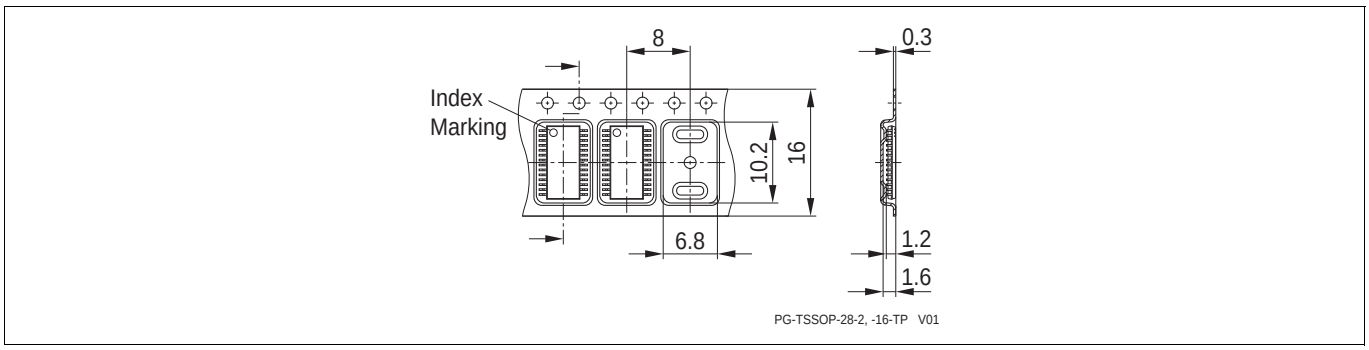

Figure 6 Tape & Reel Dimensions PG-TSSOP-28-2

5.2 Recommended Footprint

Controlling dimension is millimeters (mm).

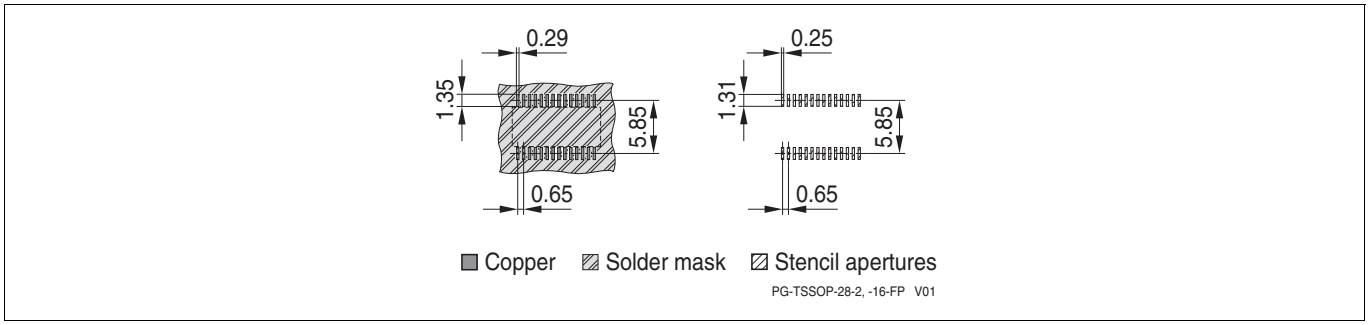

Figure 7 Recommended Footprint PG-TSSOP-28-2

5.3 Chip Marking

Line 1: SLB9645TT12 or SLB9645XT12 (see Table 1)

Line 2: G <datecode> KMC, <K> indicates assembly site code, <MC> indicates mold compound code

Line 3: 00 <Lot number>, the 00 is an internal FW indication (only at manufacturing due to field upgrade option)

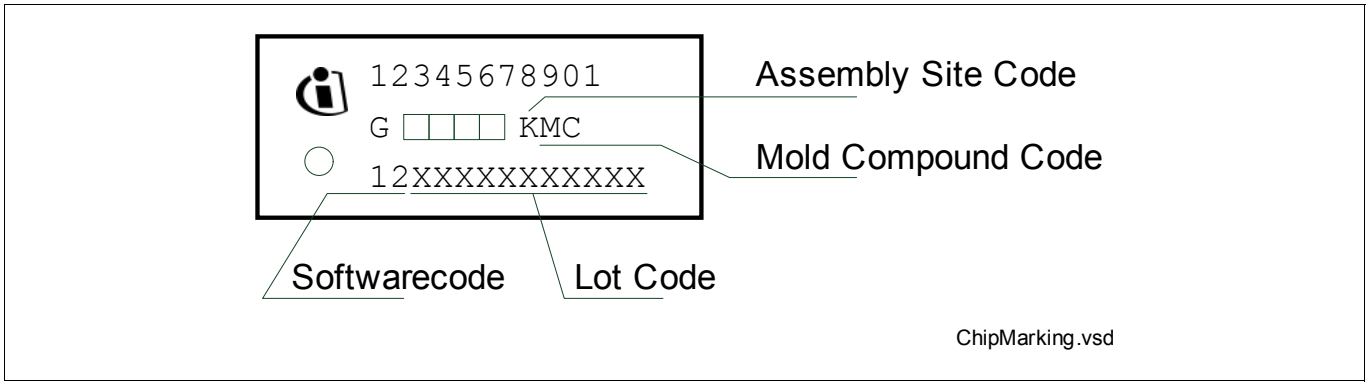

Figure 8 Chip Marking PG-TSSOP-28-2

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

6 Package Dimensions (VQFN)

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

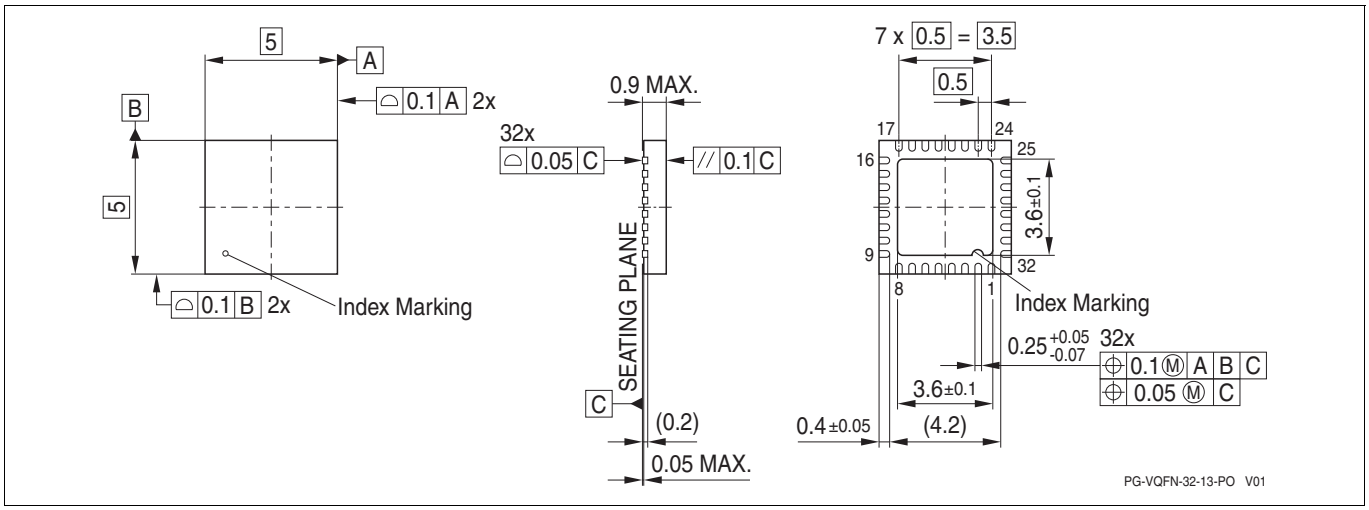

Figure 9 Package Dimensions PG-VQFN-32-13

6.1 Packing Type

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

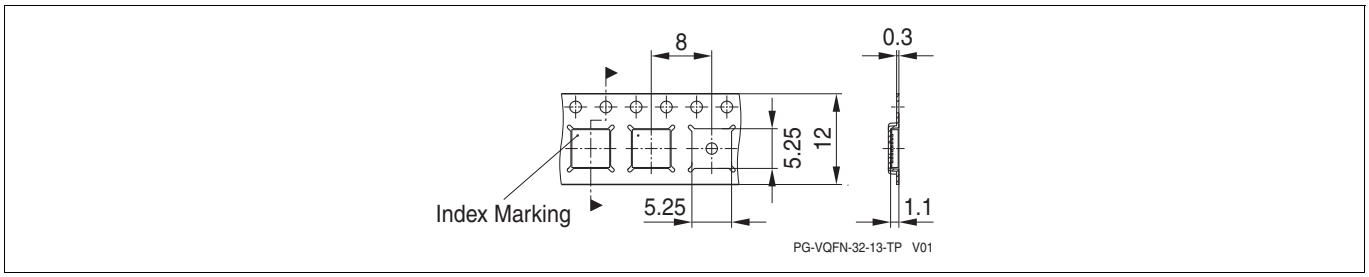

Figure 10 Tape & Reel Dimensions PG-VQFN-32-13

6.2 Recommended Footprint

Figure 11 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.

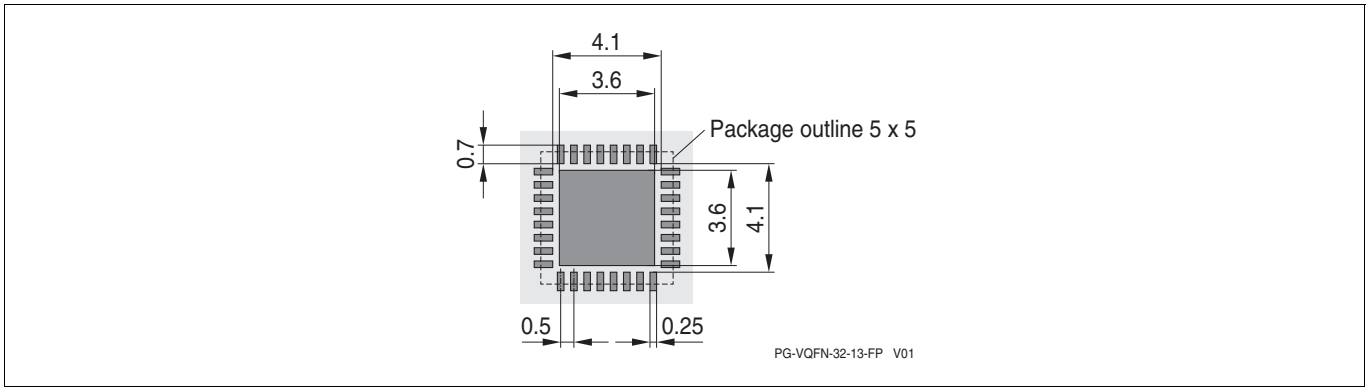

Figure 11 Recommended Footprint PG-VQFN-32-13

6.3 Chip Marking

Line 1: SLB9645

Line 2: VQ12 yy or XQ12_yy (see Table 1), the <yy> is an internal FW indication

Line 3: <Lot number> H <datecode>

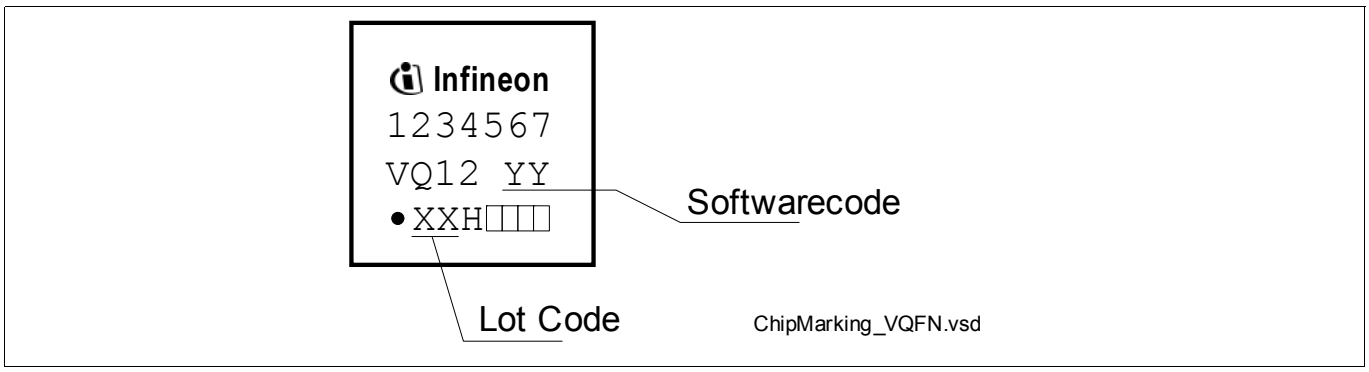

Figure 12 Chip Marking PG-VQFN-32-13

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 1.21, 2011-04-28, 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] —, “NXP I^2C bus specification, Rev. 03”, 19 June 2007

[6] —, “NXP I^2C bus specification, Rev. 4”, 13 February 2012

Terminology

ERD	Early Reset Detection
ESW	Embedded Software
HMAC	Hashed Message Authentication Code
I2C	Inter-Integrated Circuit
PCR	Platform Configuration Register
PUBEK	Public Endorsement Key
TCG	Trusted Computing Group
TPM	Trusted Platform Module
TSS	TCG Software Stack

Revision History	
Page or Item	**Subjects (major changes since previous revision)**
Revision 1.2, 2018-09-21	
	New document template. Inserted Section 4.5.
Revision 1.1, 2014-02-12	
	Fixed typos, document references, added note to Table 8.
Revision 1.0, 2013-01-31	
	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.