TPM

Trusted Platform Module
SLB 9645 TCG Rev. 116

SLB 9645 VQ 1.2
SLB 9645 TT 1.2
SLB 9645 XT 1.2
SLB 9645 XQ 1.2

Data Sheet

Hardware Description
Rev. 1.1, 2014-02-12

Chip Card & Security ICs

Edition 2014-02-12

Published by
Infineon Technologies AG
81726 Munich, Germany

Legal Disclaimer

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics. With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, 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.

Information

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, components may contain dangerous substances. For information on the types in question, please contact the nearest Infineon Technologies Office.

Infineon Technologies components may be used in life-support devices or systems only with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

Revision History	
Page or Item	**Subjects (major changes since previous revision)**
Rev. 1.1, 2014-02-12	
	Fixed typos, document references, added note to **Table 8**
Rev 1.0, 2013-09-17	
	Initial version

Trademarks of Infineon Technologies AG

AURIX™, BlueMoon™, C166™, CanPAK™, CIPOS™, CIPURSE™, COMNEON™, EconoPACK™, CoolMOS™, CoolSET™, CORECONTROL™, CROSSAVE™, DAVE™, EasyPIM™, EconoBRIDGE™, EconoDUAL™, EconoPIM™, EiceDRIVER™, eupec™, FCOS™, HITFET™, HybridPACK™, I²RF™, ISOFACE™, IsoPACK™, MIPAQ™, ModSTACK™, my-d™, NovalithIC™, OmniTune™, OptiMOS™, ORIGA™, PRIMARION™, PrimePACK™, PrimeSTACK™, PRO-SIL™, PROFET™, RASIC™, ReverSave™, SatRIC™, SIEGET™, SINDRION™, SIPMOS™, SMARTi™, SmartLEWIS™, SOLID FLASH™, TEMPFET™, thinQ!™, TRENCHSTOP™, TriCore™, X-GOLD™, X-PMU™, XMM™, XPOSYS™.

Other Trademarks

Advance Design System™ (ADS) of Agilent Technologies, AMBA™, ARM™, MULTI-ICE™, KEIL™, PRIMECELL™, REALVIEW™, THUMB™, µVision™ of ARM Limited, UK. AUTOSAR™ is licensed by AUTOSAR development partnership. Bluetooth™ of Bluetooth SIG Inc. CAT-iq™ of DECT Forum. COLOSSUS™, FirstGPS™ of Trimble Navigation Ltd. EMV™ of EMVCo, LLC (Visa Holdings Inc.). EPCOS™ of Epcos AG. FLEXGO™ of Microsoft Corporation. FlexRay™ is licensed by FlexRay Consortium. HYPERTERMINAL™ of Hilgraeve Incorporated. IEC™ of Commission Electrotechnique Internationale. IrDA™ of Infrared Data Association Corporation. ISO™ of INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. MATLAB™ of MathWorks, Inc. MAXIM™ of Maxim Integrated Products, Inc. MICROTEC™, NUCLEUS™ of Mentor Graphics Corporation. Mifare™ of NXP. MIPI™ of MIPI Alliance, Inc. MIPS™ of MIPS Technologies, Inc., USA. muRata™ of MURATA MANUFACTURING CO., MICROWAVE OFFICE™ (MWO) of Applied Wave Research Inc., OmniVision™ of OmniVision Technologies, Inc. Openwave™ Openwave Systems Inc. RED HAT™ Red Hat, Inc. RFMD™ RF Micro Devices, Inc. SIRIUS™ of Sirius Satellite Radio Inc. SOLARIS™ of Sun Microsystems, Inc. SPANSION™ of Spansion LLC Ltd. Symbian™ of Symbian Software Limited. TAIYO YUDEN™ of Taiyo Yuden Co. TEAKLITE™ of CEVA, Inc. TEKTRONIX™ of Tektronix Inc. TOKO™ of TOKO KABUSHIKI KAISHA TA. UNIX™ of X/Open Company Limited. VERILOG™, PALLADIUM™ of Cadence Design Systems, Inc. VLYNQ™ of Texas Instruments Incorporated. VXWORKS™, WIND RIVER™ of WIND RIVER SYSTEMS, INC. ZETEX™ of Diodes Zetex Limited.

Last Trademarks Update 2010-10-26

Table of Contents

List of Figures

List of Tables

1 Overview

The 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 4.5**.

Features

- Compliant to TPM Main Specification, Version 1.2, Rev. 116
- I2C compatible interface up to 400 kbps
- Approved for Google Chromebook/Chromebox
- Standard (-20..+85°C) and wide temperature range (-40..+85°C)
- TSSOP-28 and VQFN-32 package
- Optimized for battery operated devices: low standby power consumption (typ.150 µA)
- 24 PCRs
- 6 kBytes 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 Bytes IO buffer
- Built-in support by Linux™ kernel version 3.10 and higher

2 Device Types / Ordering Information

The 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 9645 TT 1.2	PG-TSSOP-28-2	Standard temperature range
SLB 9645 XT 1.2	PG-TSSOP-28-2	Enhanced temperature range
SLB 9645 VQ 1.2	PG-VQFN-32-13	Standard temperature range
SLB 9645 XQ 1.2	PG-VQFN-32-13	Enhanced temperature range

3 Pin Description

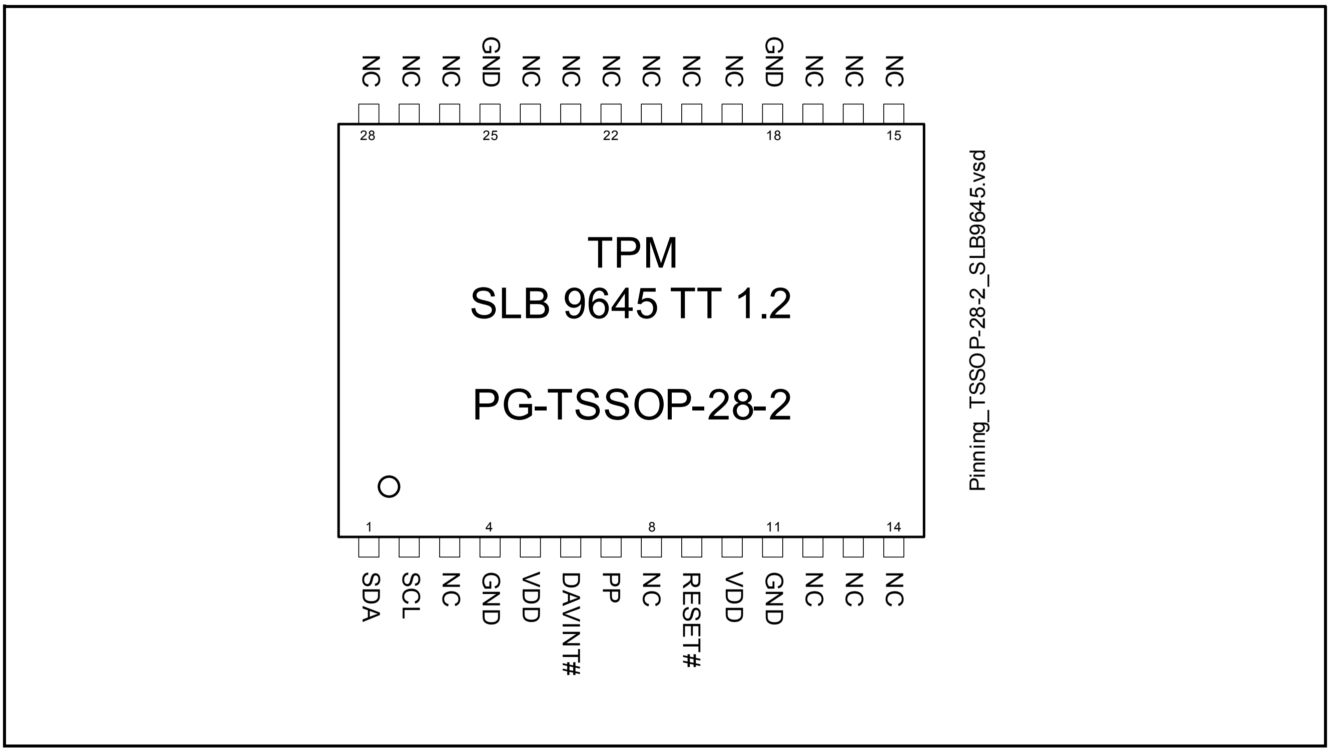


Figure 1 Pinout of the SLB 9645 TT 1.2 (PG-TSSOP-28-2 Package, Top View)

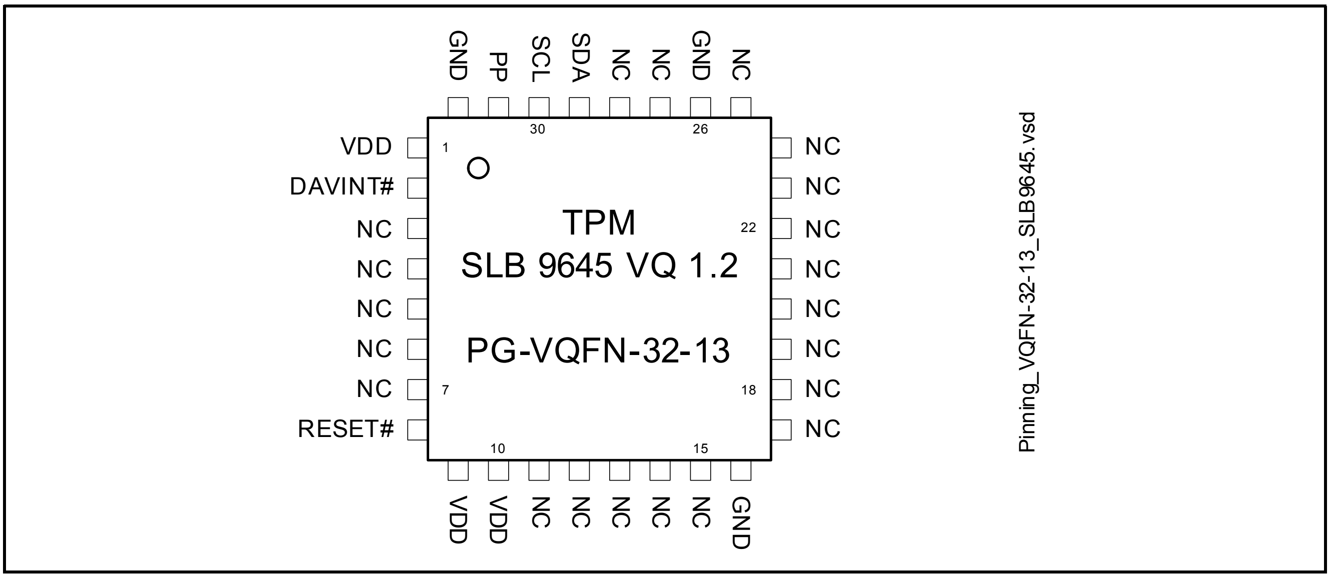


Figure 2 Pinout of the SLB 9645 VQ 1.2 (PG-VQFN-32-13 Package, Top View)

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.
6	2	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	31	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]).

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	3 - 7, 11 - 15, 17 - 25, 27, 28	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 SLB9645. 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.

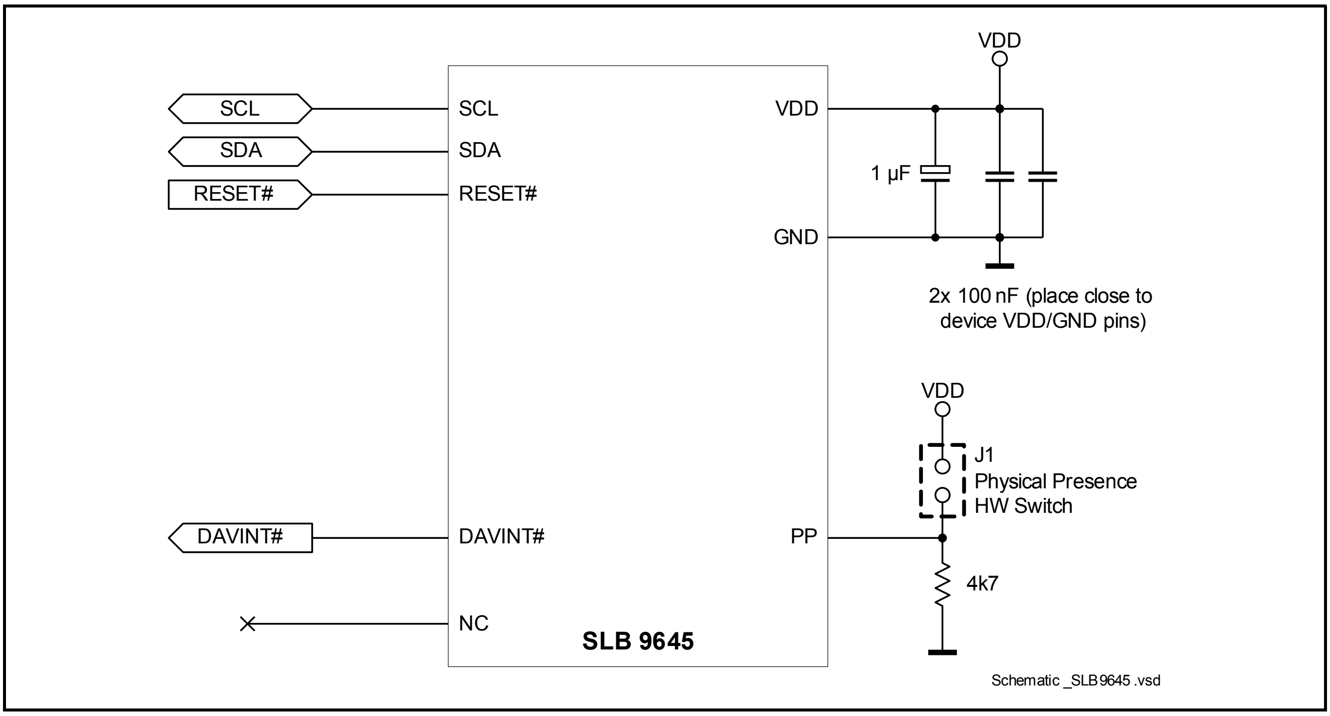


Figure 3 Typical Schematic

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 / 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 / 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[1]		–	–	5	y	
Operating lifetime[1]		–	–	5	y	
Average T_A over lifetime		–	55	–	°C	

[1] The useful lifetime of the device is 5 (five) years with a duty cycle (that means, a power-on time) of 100%. An useful lifetime of 7 (seven) years can be guaranteed for a duty cycle of 70%. For both scenarios, it is assumed that the device will be used for calculations for approximately 5% of the maximum useful lifetime.

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 / 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, pins SDA and RESET# = V_{DD} 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, pins SDA, SCL and RESET# = V_{DD} 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!

Note: Device sleep mode will be entered after 30 seconds of inactivity after the last TPM command was executed.

Table 9 DC Characteristics

Parameter	Symbol	Values			Unit	Note / 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 / Test Condition
		Min.	Typ.	Max.		
Reset Pulse Width	t_{RST}	80	—	—	µs	Cold (power-on) reset
Reset Pulse Width	t_{RST}	10	—	—	µs	Warm reset

4.5 I2C Standard/Fast Mode Interface Characteristics

The electrical characteristics are compliant to the NXP I²C bus specification [5] and [6] for “standard-mode” ($f_{SCL} \leq$ 100 kHz) and “fast-mode” ($f_{SCL} \leq$ 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

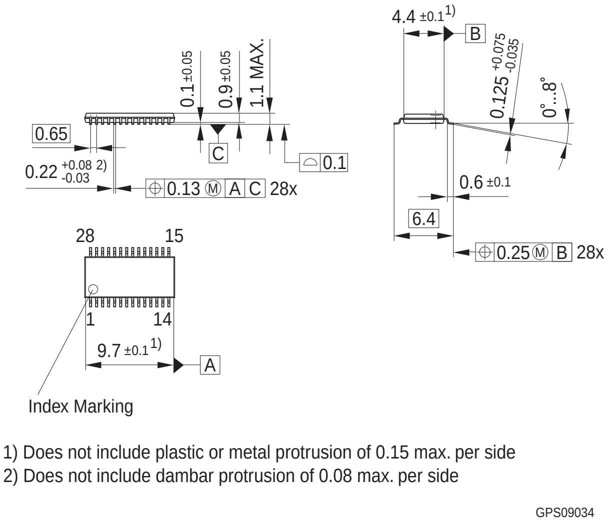
Parameter	Symbol	Values			Unit	Note / Test Condition
		Min.	Typ.	Max.		
SCL clock frequency	f_{SCL}	0	—	100	kHz	—
Output fall time from V_{IHmin} to V_{ILmax} (at device pin)	t_{OF}	—	—	75	ns	10 pF ≤ C_b ≤ 400 pF
SCL fall time (bus line, output)	t_{fSCL}	—	—	25	ns	—

Table 12 I2C Fast Mode Interface Characteristics

Parameter	Symbol	Values			Unit	Note / 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.



1) Does not include plastic or metal protrusion of 0.15 max. per side
2) Does not include dambar protrusion of 0.08 max. per side

Figure 4 Package Dimensions PG-TSSOP-28-2

5.1 Packing Type

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

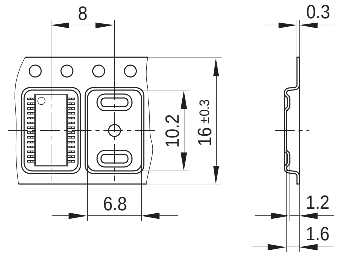


Figure 5 Tape & Reel Dimensions PG-TSSOP-28-2

5.2 Recommended Footprint

Controlling dimension is millimeters (mm).

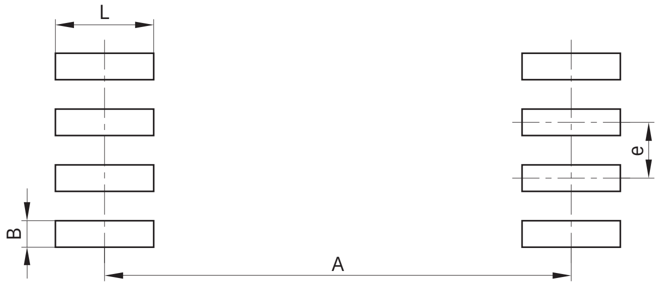


Figure 6 Recommended Footprint PG-TSSOP-28-2

Table 13 Recommended Footprint Dimensions (PG-TSSOP-28-2)

e	0.65 mm	25.6 mil
A	6.10 mm	240 mil
L	1.30 mm	51 mil
B	0.40 mm	16 mil

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)

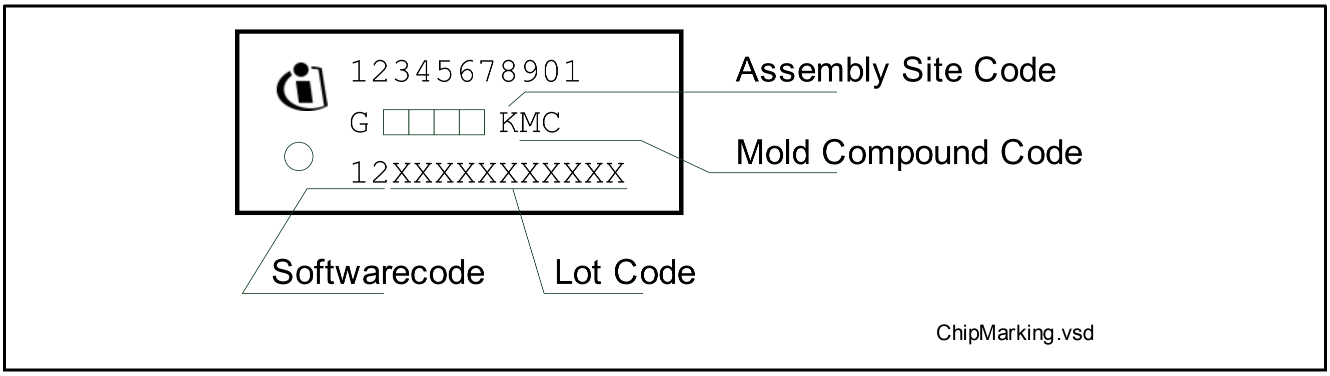


Figure 7 Chip Marking PG-TSSOP-28-2

6 Package Dimensions (VQFN)

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

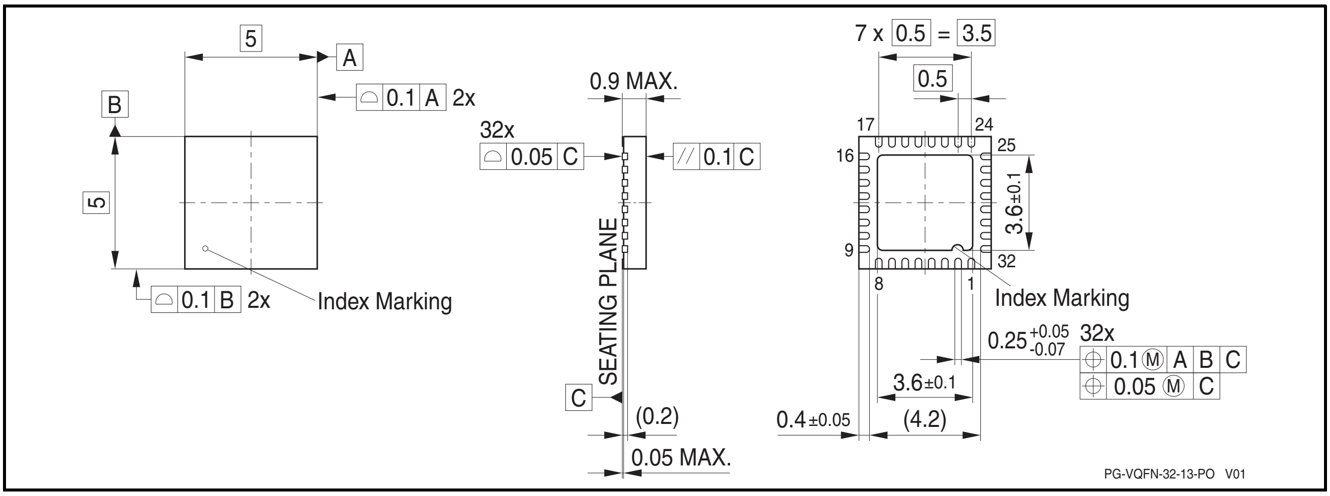


Figure 8 Package Dimensions PG-VQFN-32-13

6.1 Packing Type

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

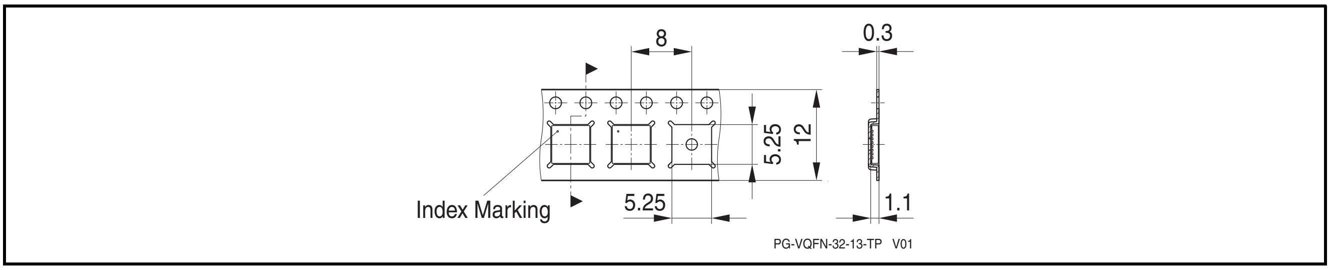


Figure 9 Tape & Reel Dimensions PG-VQFN-32-13

6.2 Recommended Footprint

Figure 10 shows the recommended footprint for the PG-VQFN-32-13 package.

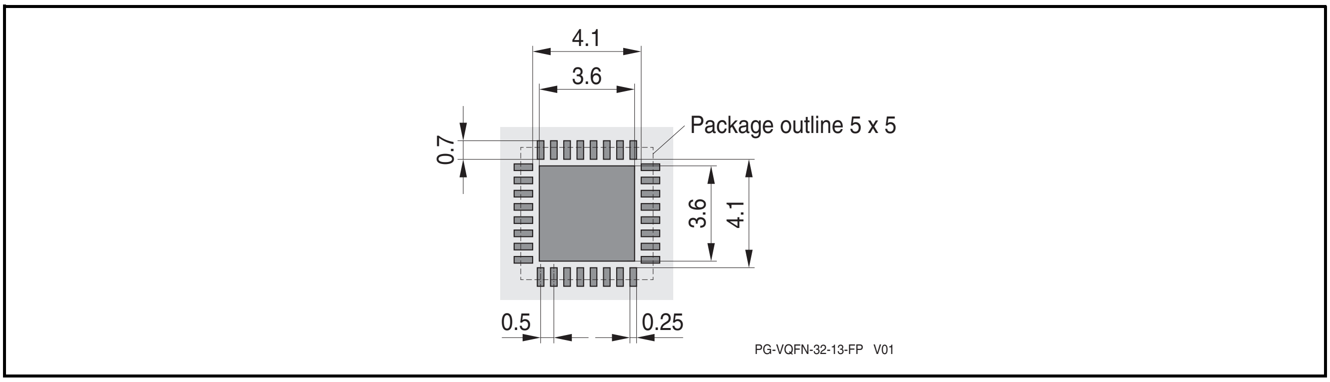


Figure 10 Recommended Footprint PG-VQFN-32-13

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>

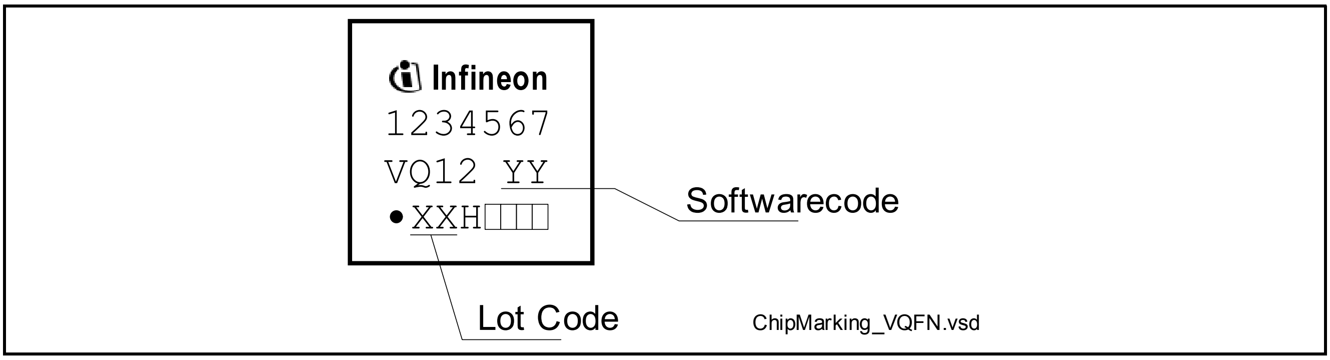


Figure 11 Chip Marking PG-VQFN-32-13

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 I²C bus specification, Rev. 03”, 19 June 2007

[6] —, “NXP I²C bus specification, Rev. 4”, 13 February 2012

Terminology

I2C	Inter-Integrated Circuit
PCR	Platform Configuration Register
TCG	Trusted Computing Group
TPM	Trusted Platform Module
TSS	TCG Software Stack

www.infineon.com

Published by Infineon Technologies AG