Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!

Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832
Email & Skype: info@chipsmall.com Web: www.chipsmall.com
Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China

Trusted Platform Module

TPM

SLB 9665 TCG Family 2 Level 00 Rev. 01.16

SLB 9665VQ2.0
SLB 9665XQ2.0
SLB 9665TT2.0
SLB 9665XT2.0

Data Sheet

Revision 1.0, 2015-10-27

Chip Card and Security

Revision History	
Page or Item	**Subjects (major changes since previous revision)**
Revision 1.0, 2015-10-27	
	Initial version.

Table of Contents

List of Figures

List of Tables

1 Overview

The SLB 9665 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 different packages, see **Table 3-1** below. It supports the LPC interface and interrupts are communicated with the serial interrupt (SERIRQ) protocol.

Features

- Compliant to TPM Main Specification, Family "2.0", Level 00, Revision 01.16 (see **[3]**)
- LPC interface
- Meeting Intel TXT, Microsoft Windows and Google Chromebook certification criteria for successful platform qualification
- True Random Number Generator (TRNG)
- Full personalization with Endorsement Key (EK) and EK certificate
- Standard (-20..+85°C) and Enhanced temperature range (-40..+85°C)
- TSSOP-28 and VQFN-32 package
- Pin-compatible to SLB 9660
- Optimized for battery operated devices: low standby power consumption (typ.150µA)
- 24 PCRs (SHA-1 or SHA-256)
- 7206 Byte 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
- 1280 Byte I/O buffer
- Built-in support by Linux Kernel Version 3.10 and higher

2 LPC Interface

The SLB 9665 features the Low Pin Count (LPC) interface (for a specification, please refer to **[1]**). From the cycle types defined in the mentioned specification, only the TPM-type cycles (read and write) are supported. All accesses with different cycle types are ignored by the device.

2.1 SYNC Field Usage

Since the legacy interface is not supported anymore, the SLB 9665 will never generate SYNC ERRORs on the LPC. It will either acknowledge a cycle with SYNC OK or use a “Long Wait” SYNC field to enlarge a cycle (that means, inserting wait states on the bus).

2.2 Localities

The interface explicitly does not support standard IO cycles (read and write). This implies that IO-mapped addressing of the device is not possible; only accesses via the locality-based TPM-type cycles are possible which also means that “locality none” as defined in **[4]** is not supported as well.

For a detailed description of the locality addressing scheme and the registers located in each locality, please refer to **[4]** as well.

2.3 Power Management

The SLB 9665 does not support the LPC power down signal (signal $\overline{\text{LPCPD}}$) or the clock run protocol (signal $\overline{\text{CLKRUN}}$). 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 LPC bus from the host platform, the device will wake immediately and will return to the low-power mode after 30 seconds of inactivity after the last TPM command has been executed.

2.4 LPC Access Rights

The registers located in the address space of the SLB 9665 are described in the respective TCG document (please refer to **[4]**). The registers READFIFO and WRITEFIFO mentioned in **Table 2-1** below refer to the DATAFIFO register, the names are used to state whether this register is read or written.

Each register has its own access rights which describe if the register is updated on a write or can be read if the associated ACTIVE.LOCALITY is set respectively not set. If the access cycle is not accepted by the TPM, it will be master aborted (no LPC SYNC cycle will be generated and no action is done on the internal registers). **Table 2-1** shows which operation is done by the TPM on each register depending on the ACTIVE.LOCALITY bit.

Note: In Table 2-1, “abort” means that no valid SYNC is generated when a cycle is seen by the interface which shall be aborted. The data present in an aborted write access cycle does not change the addressed register.

Table 2-1 LT Register Access Matrix

	ACTIVE.LOCALITY set for this locality		**ACTIVE.LOCALITY set for different LOCALITY**		**ACTIVE.LOCALITY not set**	
	READ	**WRITE**	**READ**	**WRITE**	**READ**	**WRITE**
STS	read	write	abort	abort	abort	abort
INT.ENABLE	read	write	read	abort	read	abort
INT.VECTOR	read	write	read	abort	read	abort
INT.STATUS	read	reset interrupt	read	abort	read	abort
INT.CAPABILITY	read	- (abort)	read	- (abort)	read	- (abort)
ACCESS	read	write	read	write	read	write
READFIFO	read[1)]	abort	abort	abort	abort	abort
WRITEFIFO	abort	write	abort	abort	abort	abort
Configuration Registers	read	write	read	abort	read	abort
HASH.START	abort	write	abort	abort	abort	write[2)]

Table 2-1 LT Register Access Matrix (continued)

	ACTIVE.LOCALITY set for this locality		ACTIVE.LOCALITY set for different LOCALITY		ACTIVE.LOCALITY not set	
	READ	**WRITE**	**READ**	**WRITE**	**READ**	**WRITE**
HASH.DATA	abort	write	abort	abort	abort	abort
HASH.END	abort	write[3)]	abort	abort	abort	abort

1) If STS.DATA.AVAIL is not set, this access is ‘abort’.

2) The write to HASH.START sets ACCESS.ACTIVE.LOCALITY of locality 4.

3) The write to HASH.END is an implicit release of the TPM (like a ‘1’-write to the ACCESS.ACTIVE.LOCALITY bit of locality 4).

3 Device Types / Ordering Information

The SLB 9665 product family features devices with different packages. **Table 3-1** shows the different versions. Please check the latest “Errata and Updates” document of the SLB 9665 for availability of these versions.

Table 3-1 Device Configuration

Device Name	Package	Remarks
SLB 9665VQ2.0	PG-VQFN-32-13	Standard temperature range
SLB 9665XQ2.0	PG-VQFN-32-13	Enhanced temperature range
SLB 9665TT2.0	PG-TSSOP-28-2	Standard temperature range
SLB 9665XT2.0	PG-TSSOP-28-2	Enhanced temperature range

4 Pin Description

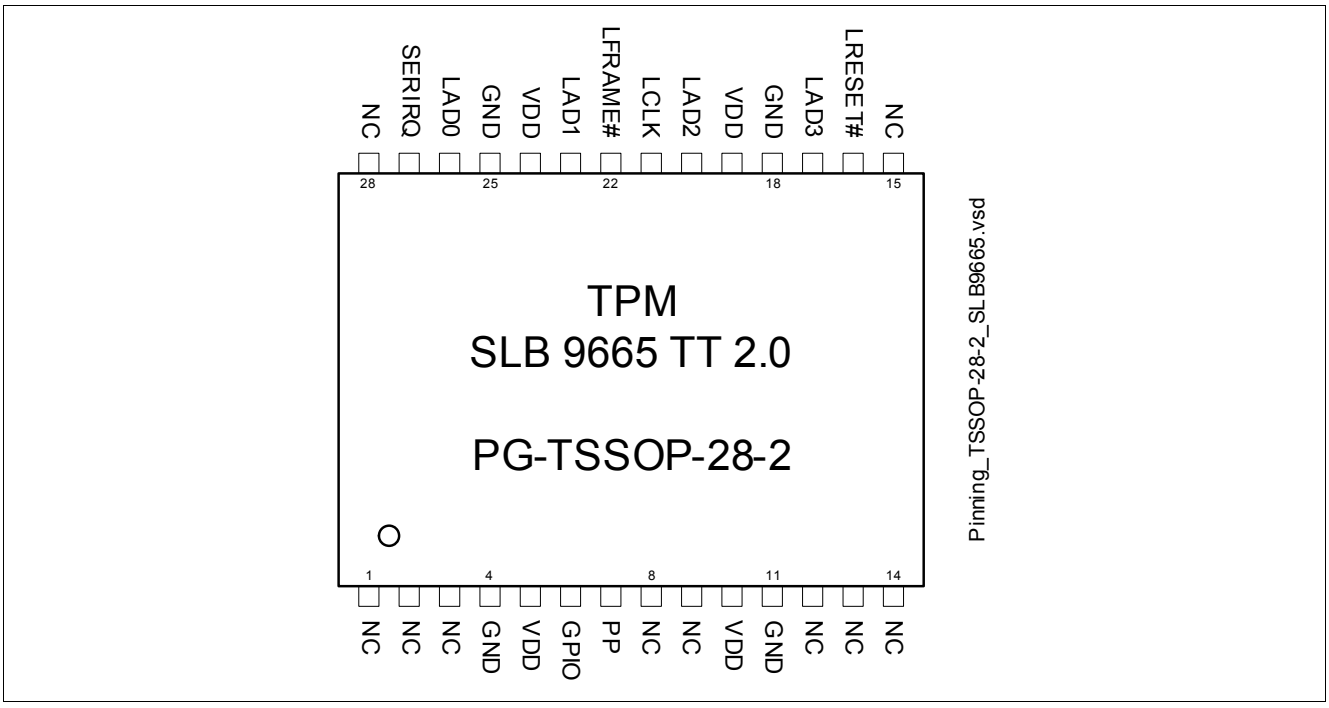

Figure 4-1 Pinout of the SLB 9665TT2.0 / SLB 9665XT2.0 (PG-TSSOP-28-2 Package, Top View)

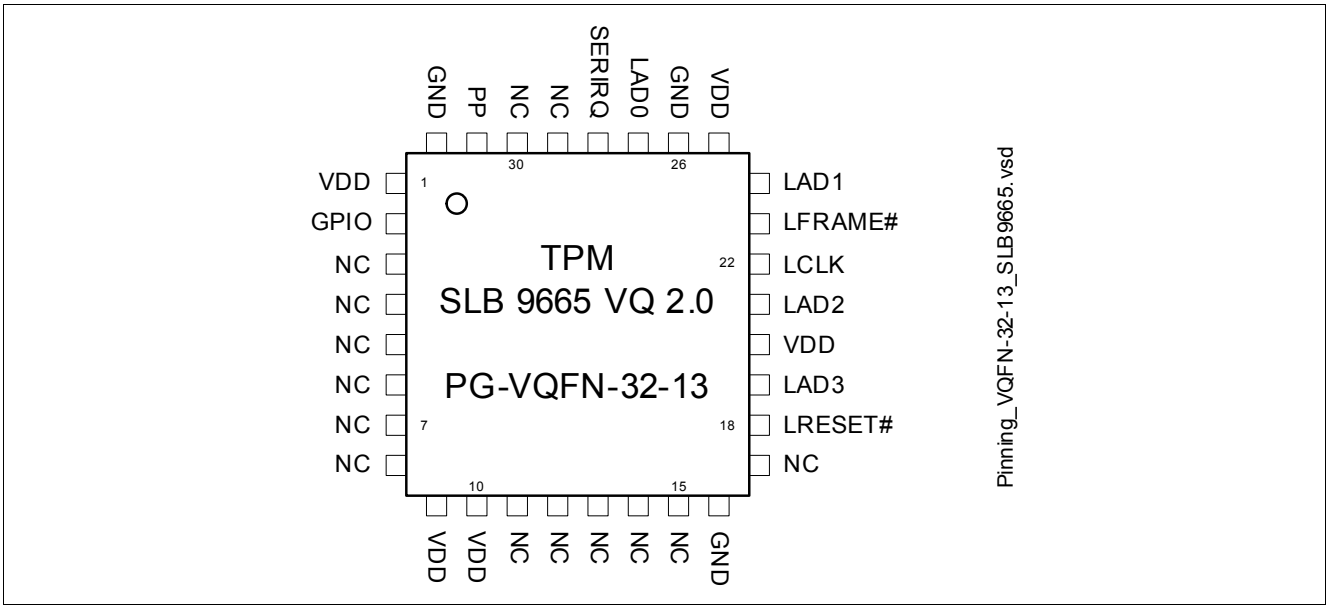

Figure 4-2 Pinout of the SLB 9665VQ2.0 / SLB 9665XQ2.0 (PG-VQFN-32-13 Package, Top View)

Table 4-1 Buffer Types

Buffer Type	Description
TS	Tri-State pin
ST	Schmitt-Trigger pin
OD	Open-Drain pin

Table 4-2 I/O Signals

Pin Number		Name	Pin Type	Buffer Type	Function
PG-TSSOP-28-2	PG-VQFN-32-13				
26	27	LAD0	I/O	TS	**LPC Address/Data Bit 0** Multiplexed LPC command, address and data bus. Connect these pins to the LAD[3:0] pins of the LPC host.
23	24	LAD1	I/O	TS	**LPC Address/Data Bit 1** see description of LAD0 above.
20	21	LAD2	I/O	TS	**LPC Address/Data Bit 2** see description of LAD0 above.
17	19	LAD3	I/O	TS	**LPC Address/Data Bit 3** see description of LAD0 above.
22	23	LFRAME#	I	ST	**LPC Framing Signal** LPC framing signal. This pin is connected to the LPC LFRAME# signal and indicates the start of a new cycle on the LPC bus or the termination of a broken cycle. The signal is active low.

Table 4-2 I/O Signals (continued)

Pin Number		Name	Pin Type	Buffer Type	Function
PG-TSSOP-28-2	PG-VQFN-32-13				
21	22	LCLK	I	ST	**Clock Input** This pin provides the external clock for the chip and is typically connected to the PCI clock of the host. The clock frequency range is 1 MHz - 33 MHz (nominal).
16	18	LRESET#	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.
6	2	GPIO	I/O	OD	**General Purpose I/O** This pin is a general purpose I/O pin. It is defined as GPIO-Express-00, please refer to [4] and the PCI-SIG ECN “Trusted Configuration Space for PCI Express”. This pin may be left unconnected; however, to minimize power consumption, it shall be connected to a fixed level (either GND or VDD) via an external resistor (4.7 kΩ..10 kΩ).
7	31	PP	I	ST	**Physical Presence** This pin indicates physical presence; for usage of this signal, please refer to the TCG specification v1.2. The TPM 2.0 device does not use this functionality. For compatibility reasons (downgrade capability to a TPM 1.2), the 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 a TPM 1.2. This pin does not have an internal pull-up or pull-down resistor and must not be left floating.
27	28	SERIRQ	I/O	TS	**Serial Interrupt Request** Interrupt request signal, uses the serial interrupt request protocol (see [2]). Connect to the LPC host.

Table 4-3 Power Supply

Pin Number		Name	Pin Type	Buffer Type	Function
PG-TSSOP-28-2	PG-VQFN-32-13				
5, 10, 19, 24	1, 9, 10, 20, 25	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 4-4 Not Connected

Pin Number		Name	Pin Type	Buffer Type	Function
PG-TSSOP-28-2	PG-VQFN-32-13				
1, 2, 3, 8, 12, 13, 14, 15, 28	3, 4, 5, 6, 7, 11, 12, 13, 14, 15, 17, 29, 30	NC	NU	—	**Not Connected** All pins must not be connected externally (must be left floating).
9	8	NC	NU	—	**Not Connected** This pin may be connected to the **Reset** signal (for backward compatibility) or may be left floating.

4.1 Typical Schematic

Figure 4-3 shows the typical schematic for the SLB 9665. 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).

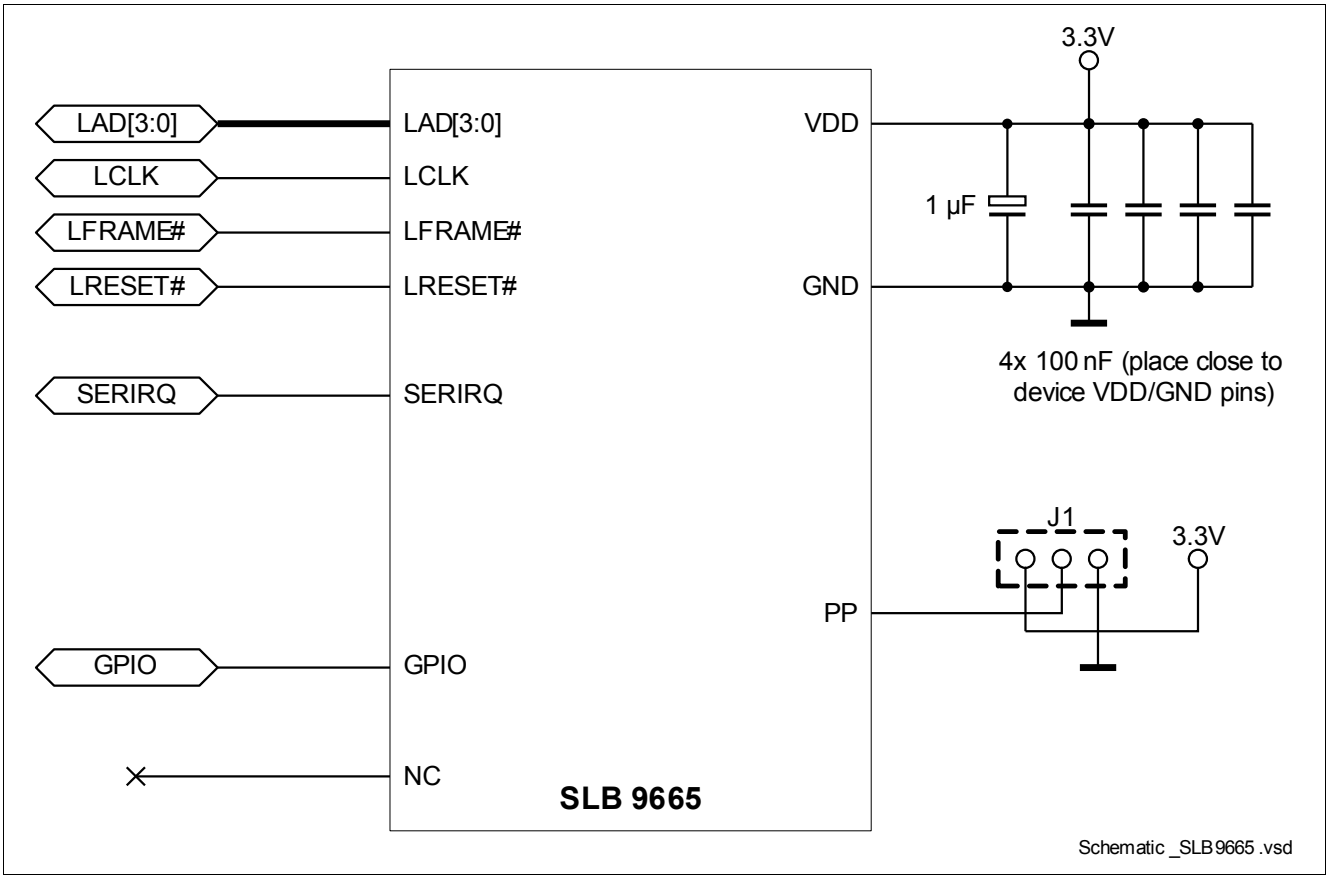

Figure 4-3 Typical Schematic

5 Electrical Characteristics

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

5.1 Absolute Maximum Ratings

Table 5-1 Absolute Maximum Ratings

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Supply Voltage	V_{DD}	-0.3	–	3.6	V	–
Voltage on any pin	V_{max}	-0.3	–	V_{DD}+0.3	V	–
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 5-2 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	–
Ambient temperature	T_A	-20	–	85	°C	Standard temperature devices
Ambient temperature	T_A	-40	–	85	°C	Enhanced temperature 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.

5.3 DC Characteristics

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

Table 5-3 Current Consumption

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Current Consumption in Active Mode	I_{VDD_Active}		2.5	25	mA	Assuming operating state **S0**, that means active. 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	Pins LRESET#, LFRAME#, LADn,SERIRQ = V_{DD}. Assuming operating state **S0** with active clock. 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	Pins LRESET#, LFRAME#, LADn,SERIRQ = V_{DD} and LCLK = GND. Assuming operating state **S3** with clock stopped. Obviously, this value is zero if the TPM is not powered in S3 state (this is platform dependent).

Note: Current consumption does not include any currents flowing through resistive loads on output pins! For the definition of power/operating states, please refer to the ACPI standard.

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

Table 5-4 DC Characteristics for non-LPC Pins

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Input voltage high	V_{IH}	0.7 V_{DD}		V_{DD}	V	GPIO and PP pins
Input voltage low	V_{IL}	0		0.3 V_{DD}	V	GPIO and PP pins
Input high leakage current	I_{IH}	-15		15	µA	V_{IN} = V_{DD}, GPIO and PP pins
Input low leakage current	I_{IL}	-15		15	µA	V_{IN} = 0V, GPIO and PP pins
Output high voltage	V_{OH}	V_{DD}-0.3			V	I_{OH} = 1mA, Pin GPIO
Output low voltage	V_{OL}			0.3	V	I_{OL} = 1mA, Pin GPIO

Table 5-5 DC Characteristics for LPC Pins

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Ínput voltage high	V_{IH}	0.5 V_{DD}		V_{DD}+0.3	V	All signal pins except GPIO and PP
Input voltage low	V_{IL}	-0.3		0.28 V_{DD}	V	All signal pins except GPIO and PP
Input high leakage current	I_{IH}	-10		10	µA	V_{IN} = V_{DD}, all signal pins except GPIO and PP
Input low leakage current	I_{IL}	-10		10	µA	V_{IN} = 0V, all signal pins except GPIO and PP
Output high voltage	V_{OH}	0.9 V_{DD}			V	I_{OH} = -500µA, pins LAD[3:0] and SERIRQ
Output low voltage	V_{OL}			0.1 V_{DD}	V	I_{OL} = 1.5mA, pins LAD[3:0] and SERIRQ

5.4 Timing

Some pads are disabled after deassertion of the reset signal for up to 500 µs. This is especially important for the SERIRQ signal; after deassertion of the reset signal, this signal is only valid after that time has expired.

6 Package Dimensions (TSSOP)

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

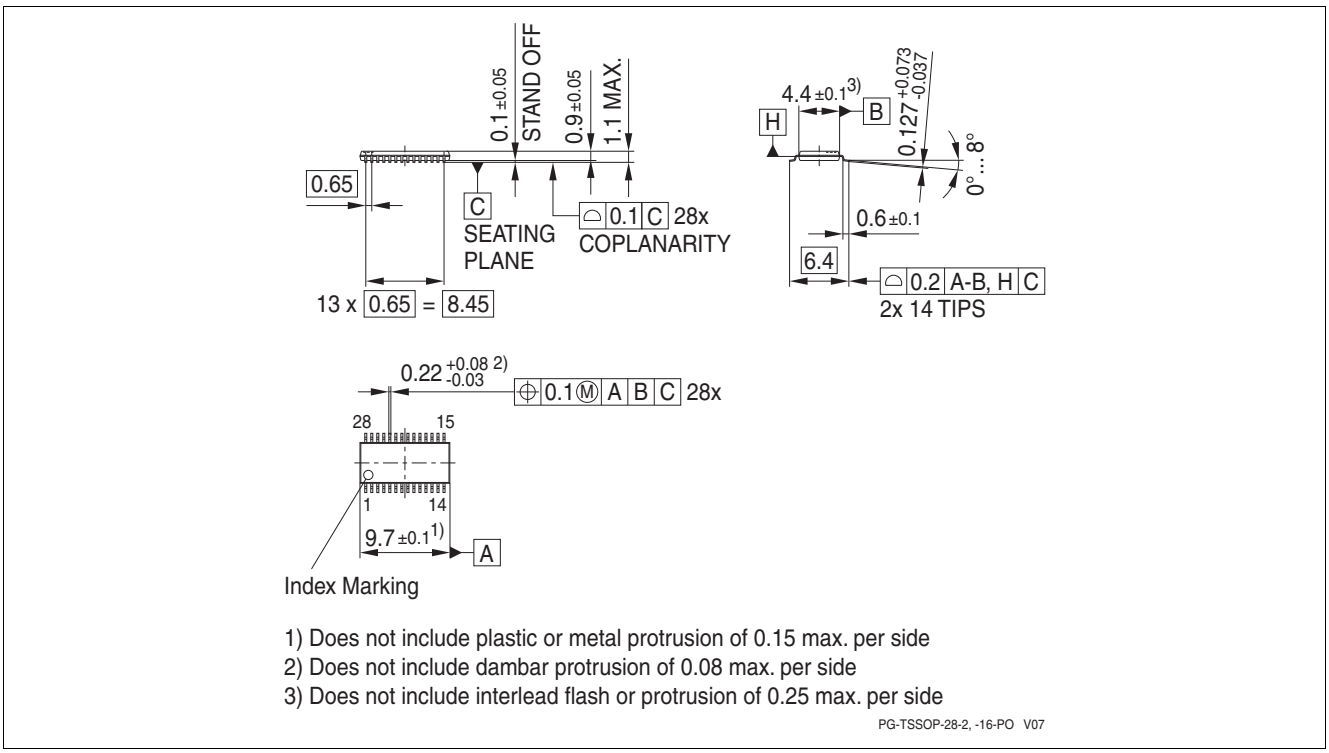

Figure 6-1 Package Dimensions PG-TSSOP-28-2

6.1 Packing Type

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

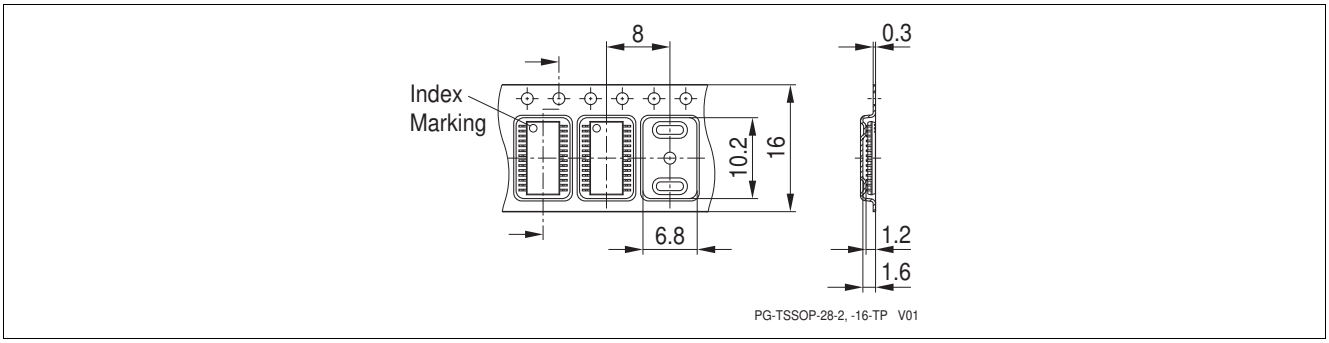

Figure 6-2 Tape & Reel Dimensions PG-TSSOP-28-2

6.2 Recommended Footprint

Controlling dimension is millimeters (mm).

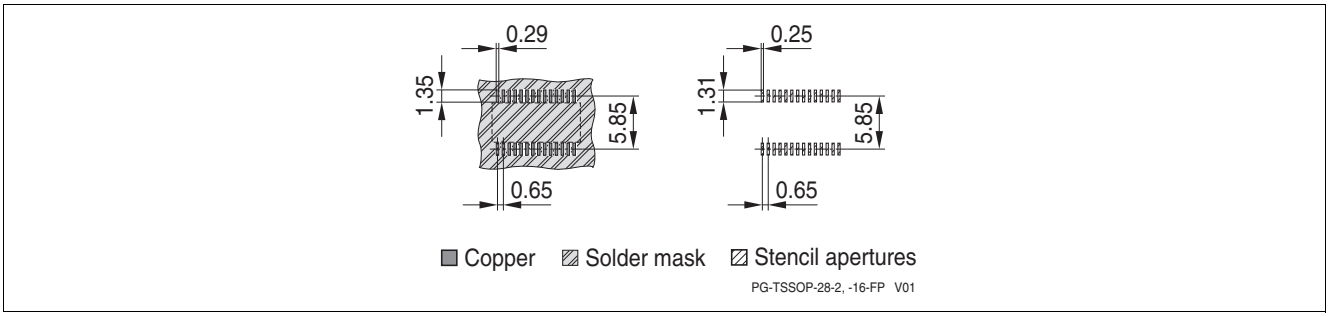

Figure 6-3 Recommended Footprint PG-TSSOP-28-2

6.3 Chip Marking

Line 1: SLB9665TT20 or SLB9665XT20, see **Table 3-1**

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)

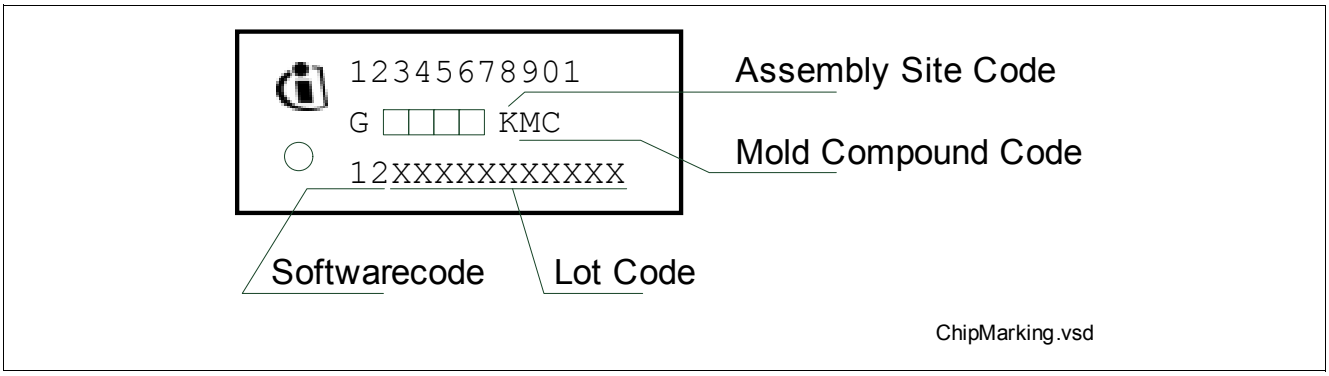

Figure 6-4 Chip Marking PG-TSSOP-28-2

7 Package Dimensions (VQFN)

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

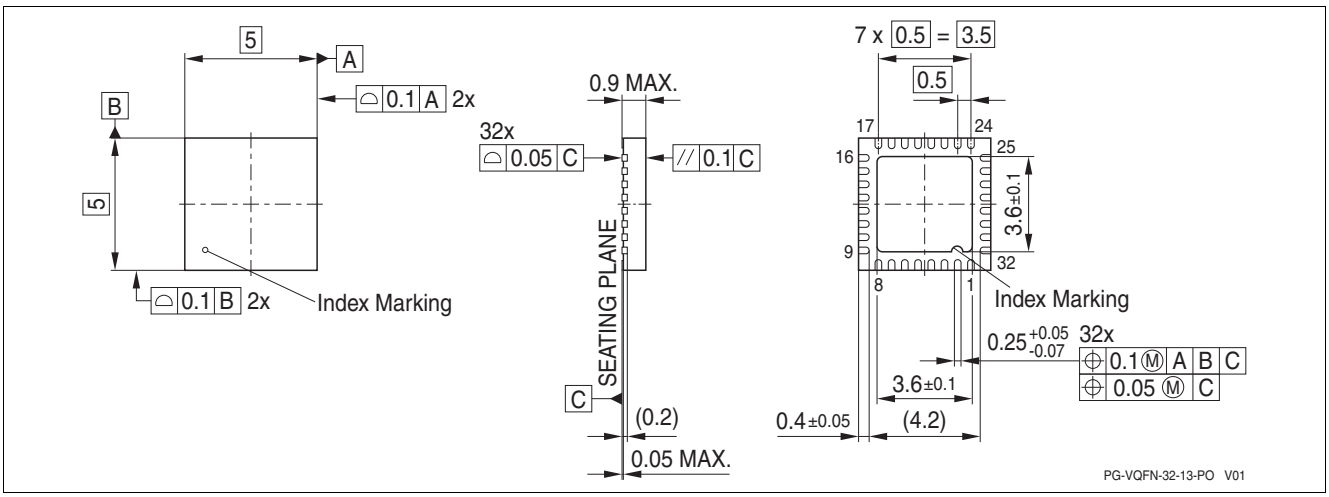

Figure 7-1 Package Dimensions PG-VQFN-32-13

7.1 Packing Type

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

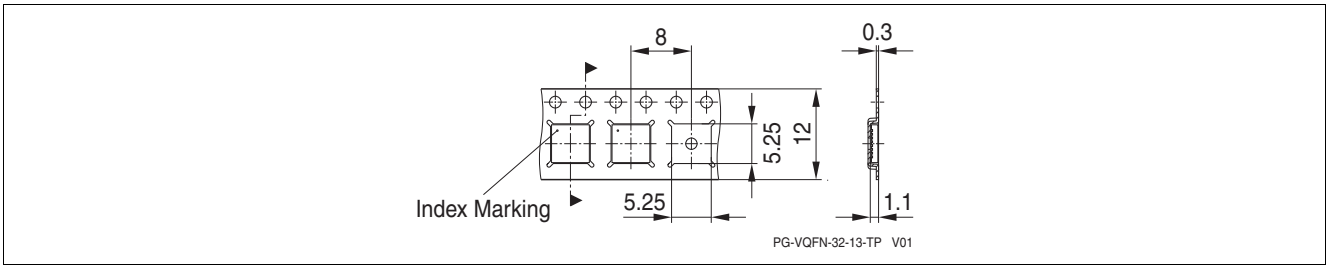

Figure 7-2 Tape & Reel Dimensions PG-VQFN-32-13

7.2 Recommended Footprint

Figure 7-3 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.

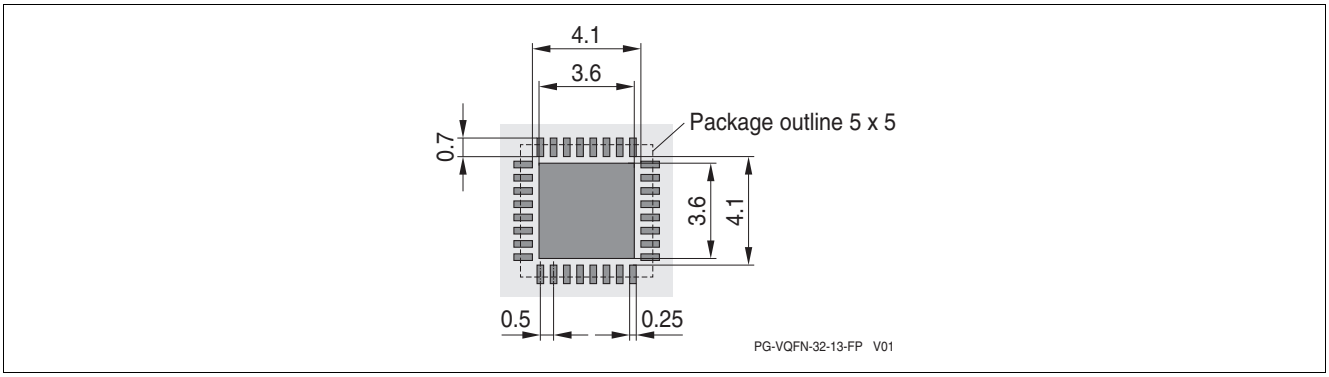

Figure 7-3 Recommended Footprint PG-VQFN-32-13

7.3 Chip Marking

Line 1: SLB9665

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

Line 3: <Lot number> H <datecode>

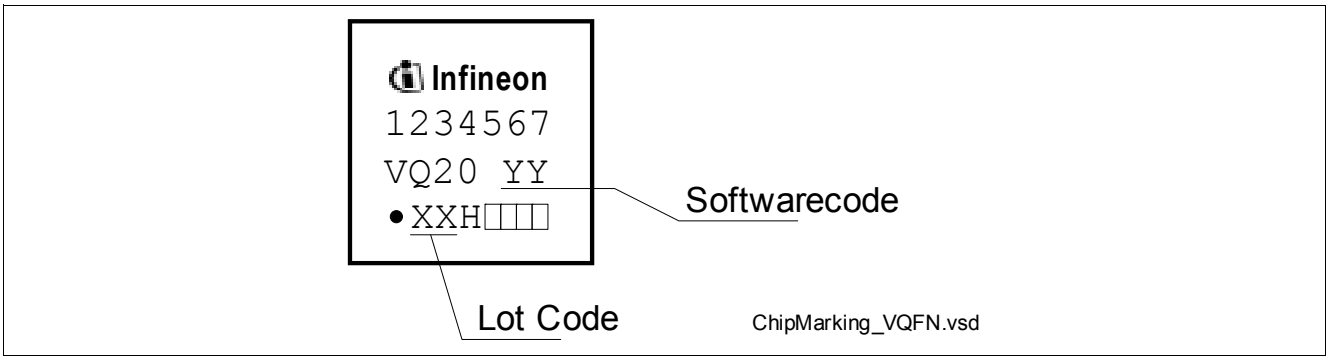

Figure 7-4 Chip Marking PG-VQFN-32-13

References

[1] —, “Low Pin Count (LPC) Interface Specification”, Version 1.1, Intel

[2] —, “Serialized IRQ Support for PCI Systems”, Version 6.0, September 1, 1995, Cirrus Logic et al.

[3] —, “Trusted Platform Module Library (Part 1-4)”, Family 2.0, Level 00, Rev. 01.16, October 30, 2014, TCG

[4] —, “TCG PC Client Specific Platform TPM Profile (PTP) Specification”, Family 2.0, Level 00, Rev. 43, January 26, 2015, TCG

Terminology

ESW	Embedded Software
HMAC	Hashed Message Authentication Code
LPC	Low Pin Count (bus)
PCR	Platform Configuration Register
PUBEK	Public Endorsement Key
SCP	Symmetric Crypto Processor
TCG	Trusted Computing Group
TPM	Trusted Platform Module
TSS	TCG Software Stack

Licenses and Notices

The following License and Notice Statements are reproduced from [3].

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.

www.infineon.com

Edition 2015-10-27
Published by
Infineon Technologies AG
81726 Munich, Germany

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

Document reference

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.