

Trusted Platform Module

TPM

SLB 9660 TCG Rev. 116

SLB 9660VQ1.2

SLB 9660TT1.2

SLB 9660XT1.2

SLB 9660XQ1.2

Data Sheet

Revision 1.0, 2014-12-12

Chip Card and Security ICs



Revision History

Page or Item	Subjects (major changes since previous revision)
Revision 1.0, 2014-12-12	
	Initial version.

Table of Contents

	Table of Contents	3
	List of Figures	4
	List of Tables	5
1	Overview	6
2	LPC Interface	6
2.1	SYNC Field Usage	6
2.2	Localities	6
2.3	Power Management	7
2.4	LPC Access Rights	7
3	Device Types / Ordering Information	8
4	Pin Description	8
4.1	Typical Schematic	12
5	Electrical Characteristics	13
5.1	Absolute Maximum Ratings	13
5.2	Functional Operating Range	13
5.3	DC Characteristics	14
5.4	Timing	15
6	Package Dimensions (TSSOP)	16
6.1	Packing Type	16
6.2	Recommended Footprint	17
6.3	Chip Marking	17
7	Package Dimensions (VQFN)	18
7.1	Packing Type	18
7.2	Recommended Footprint	18
7.3	Chip Marking	19
	References	20
	Terminology	21

List of Figures

List of Figures

Figure 4-1	Pinout of the SLB 9660TT1.2 / SLB 9660XT1.2 (PG-TSSOP-28-2 Package, Top View)	8
Figure 4-2	Pinout of the SLB 9660VQ1.2 / SLB 9660XQ1.2 (PG-VQFN-32-13 Package, Top View)	9
Figure 4-3	Typical Schematic.....	12
Figure 6-1	Package Dimensions PG-TSSOP-28-2.....	16
Figure 6-2	Tape & Reel Dimensions PG-TSSOP-28-2.....	16
Figure 6-3	Recommended Footprint PG-TSSOP-28-2	17
Figure 6-4	Chip Marking PG-TSSOP-28-2.....	17
Figure 7-1	Package Dimensions PG-VQFN-32-13.....	18
Figure 7-2	Tape & Reel Dimensions PG-VQFN-32-13.....	18
Figure 7-3	Recommended Footprint PG-VQFN-32-13	18
Figure 7-4	Chip Marking PG-VQFN-32-13.....	19

List of Tables

List of Tables

Table 2-1	LT Register Access Matrix	7
Table 3-1	Device Configuration	8
Table 4-1	Buffer Types	9
Table 4-2	I/O Signals	9
Table 4-3	Power Supply	11
Table 4-4	Not Connected	11
Table 5-1	Absolute Maximum Ratings	13
Table 5-2	Functional Operating Range	13
Table 5-3	Current Consumption	14
Table 5-4	DC Characteristics for non-LPC Pins	14
Table 5-5	DC Characteristics for LPC Pins	15

1 Overview

The SLB 9660 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 1.2 products and firmware upgrades. It is available in different packages, see [Table 3-1](#). It supports the LPC interface and interrupts are communicated with the serial interrupt (SERIRQ) protocol.

Features

- Compliant to TPM Main Specification, Version 1.2, Rev. 116
- LPC interface
- 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 LPC Interface

The SLB 9660 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 9660 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.

LPC Interface

2.3 Power Management

The SLB 9660 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 the transaction has been finished.

2.4 LPC Access Rights

The registers located in the address space of the SLB 9660 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⁾
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 9660 product family features devices with different packages. [Table 3-1](#) shows the different versions.

Table 3-1 Device Configuration

Device Name	Package	Remarks
SLB 9660TT1.2	PG-TSSOP-28-2	Standard temperature range
SLB 9660VQ1.2	PG-VQFN-32-13	Standard temperature range
SLB 9660XT1.2	PG-TSSOP-28-2	Enhanced temperature range
SLB 9660XQ1.2	PG-VQFN-32-13	Enhanced temperature range

4 Pin Description

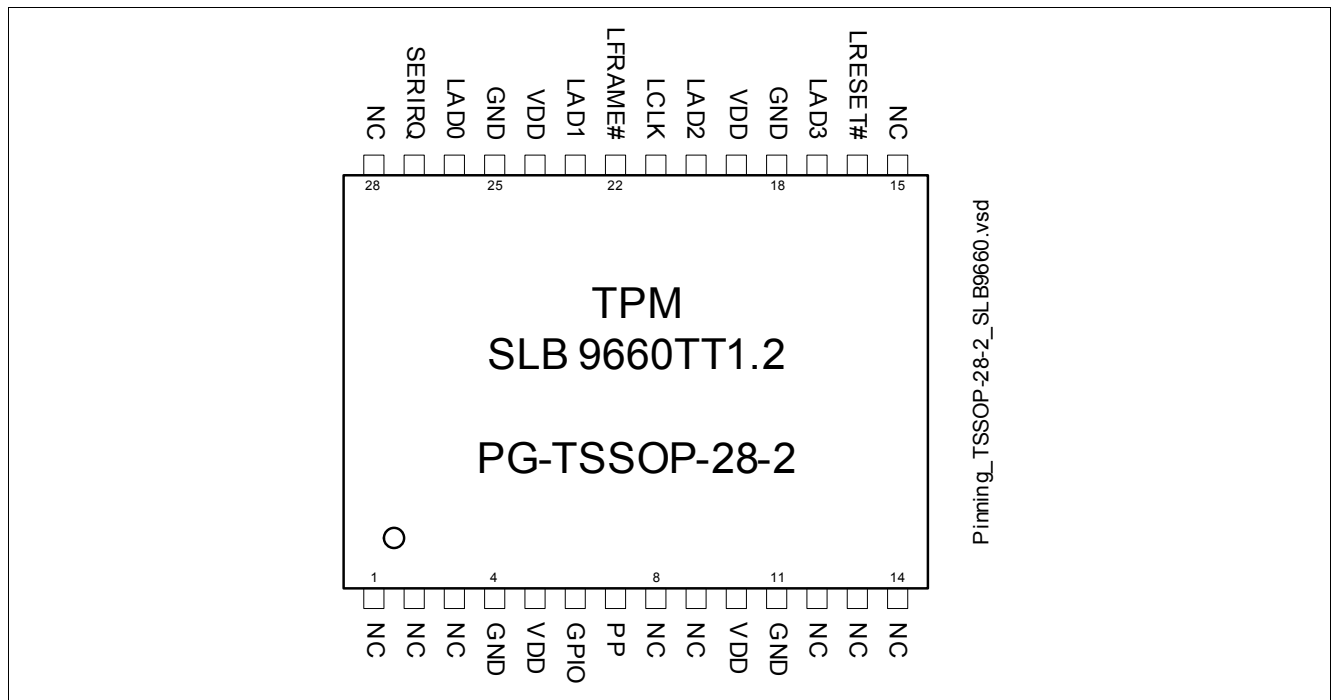


Figure 4-1 Pinout of the SLB 9660TT1.2 / SLB 9660XT1.2 (PG-TSSOP-28-2 Package, Top View)

Pin Description

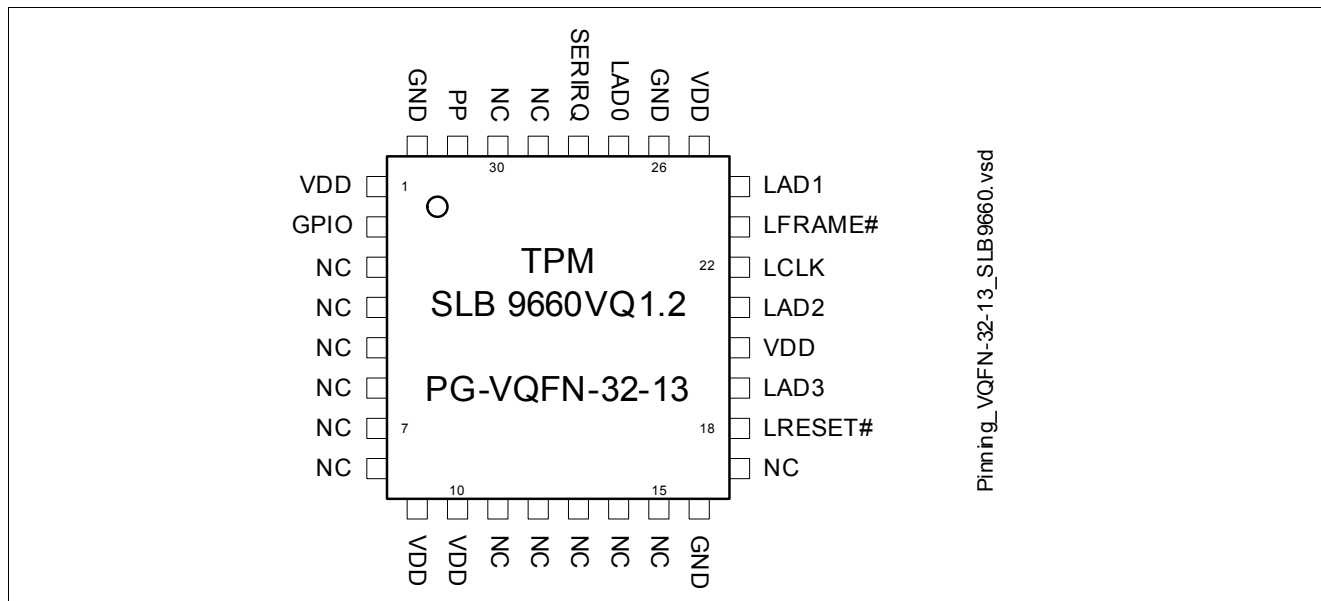


Figure 4-2 Pinout of the SLB 9660VQ1.2 / SLB 9660VQ1.2 (PG-VQFN-32-13 Package, Top View)

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.

Pin Description

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	<p>Clock Input</p> <p>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).</p>
16	18	LRESET#	I	ST	<p>Reset</p> <p>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.</p>
6	2	GPIO	I/O	OD	<p>General Purpose I/O</p> <p>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”.</p> <p>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).</p>
7	31	PP	I	ST	<p>Physical Presence</p> <p>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 [3]).</p> <p>This pin does not have an internal pull-up or pull-down resistor and must not be left floating.</p>
27	28	SERIRQ	I/O	TS	<p>Serial Interrupt Request</p> <p>Interrupt request signal, uses the serial interrupt request protocol (see [2]). Connect to the LPC host.</p>

Pin Description

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.

Pin Description

4.1 Typical Schematic

Figure 4-3 shows the typical schematic for the SLB 9660. 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).

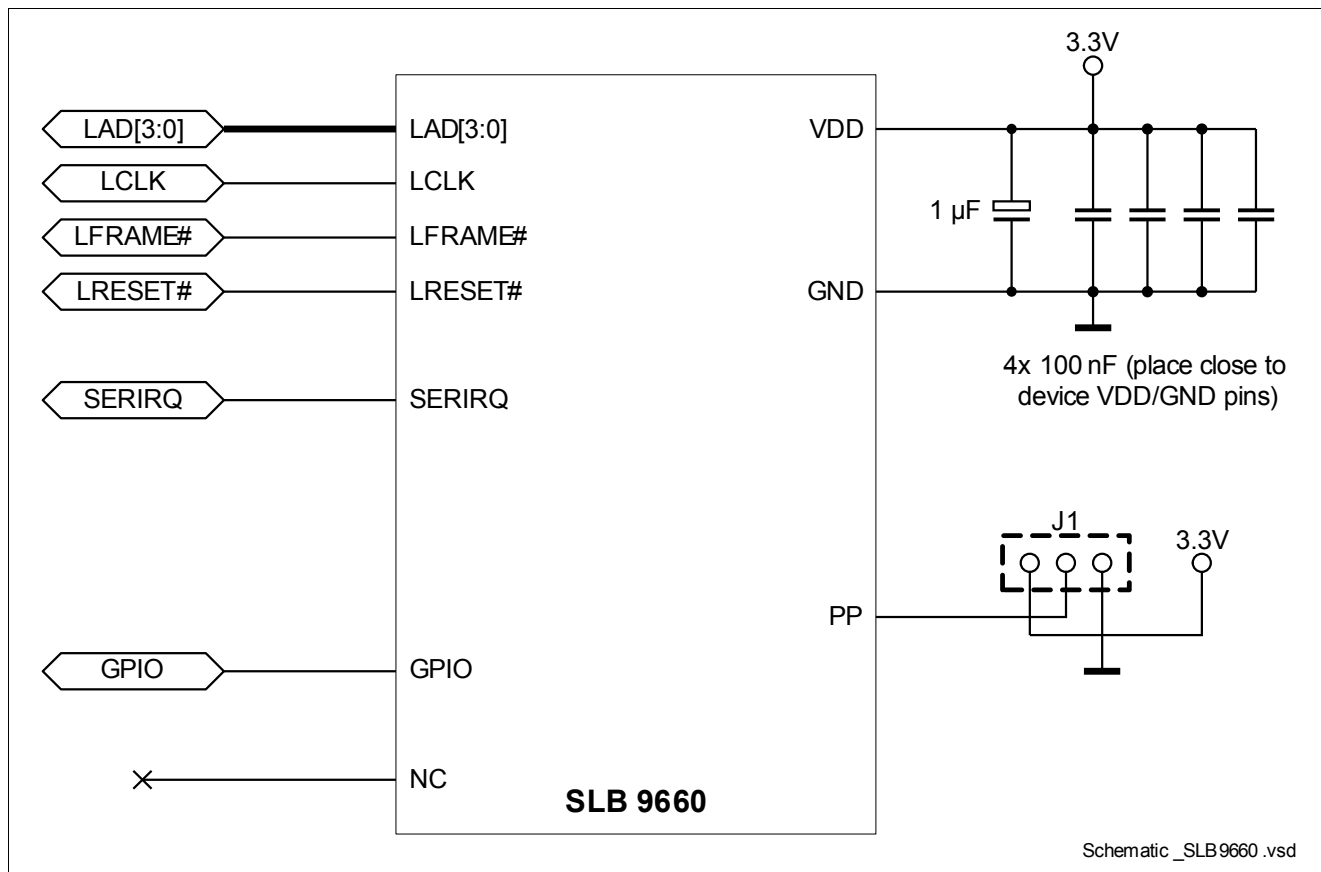


Figure 4-3 Typical Schematic

Electrical Characteristics

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.

Electrical Characteristics

5.3 DC Characteristics

$T_A = 25^\circ\text{C}$, $V_{DD} = 3.3\text{V} \pm 0.3\text{V}$ 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

Electrical Characteristics

Table 5-4 DC Characteristics for non-LPC Pins (continued)

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

Table 5-5 DC Characteristics for LPC Pins

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Input 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	$V_{IN} = 0\text{V}$, all signal pins except GPIO and PP
Output high voltage	V_{OH}	$0.9 V_{DD}$			V	$I_{OH} = -500\mu\text{A}$, pins LAD[3:0] and SERIRQ
Output low voltage	V_{OL}			$0.1 V_{DD}$	V	$I_{OL} = 1.5\text{mA}$, 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.

Package Dimensions (TSSOP)

6 Package Dimensions (TSSOP)

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

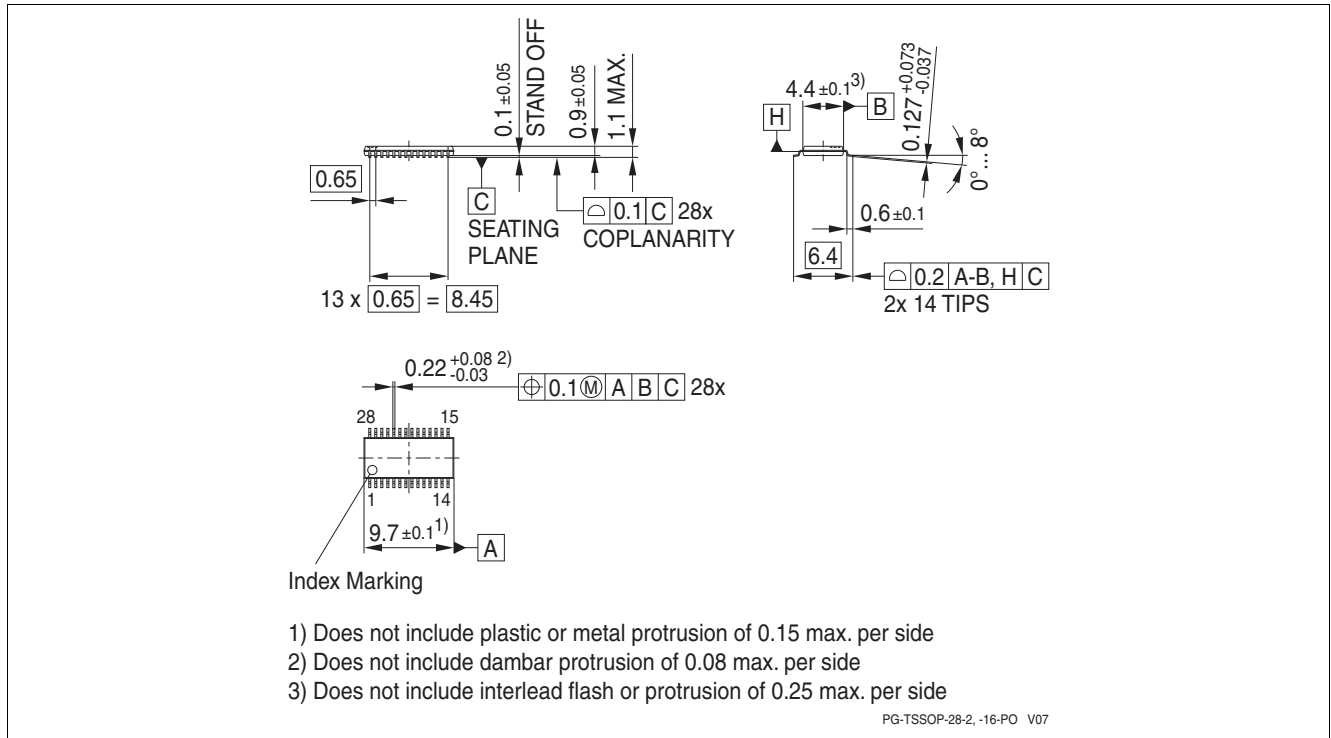


Figure 6-1 Package Dimensions PG-TSSOP-28-2

6.1 Packing Type

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

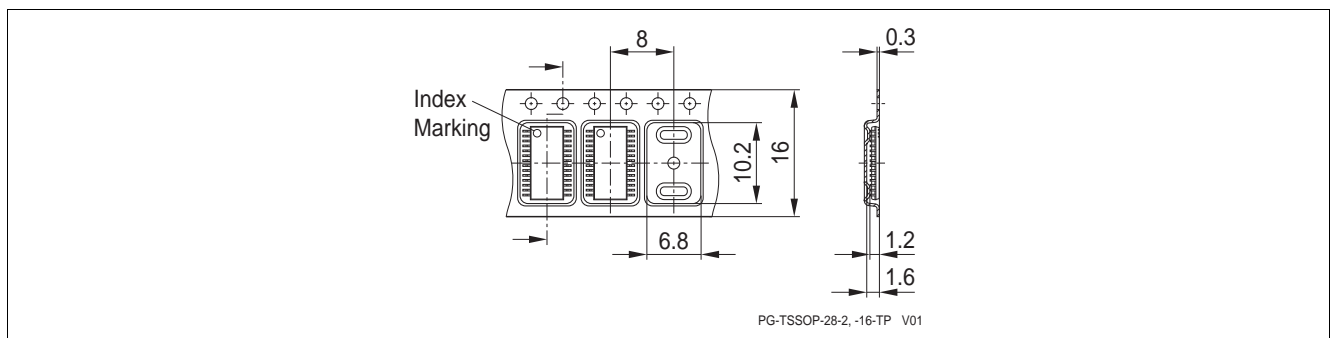


Figure 6-2 Tape & Reel Dimensions PG-TSSOP-28-2

Package Dimensions (TSSOP)

6.2 Recommended Footprint

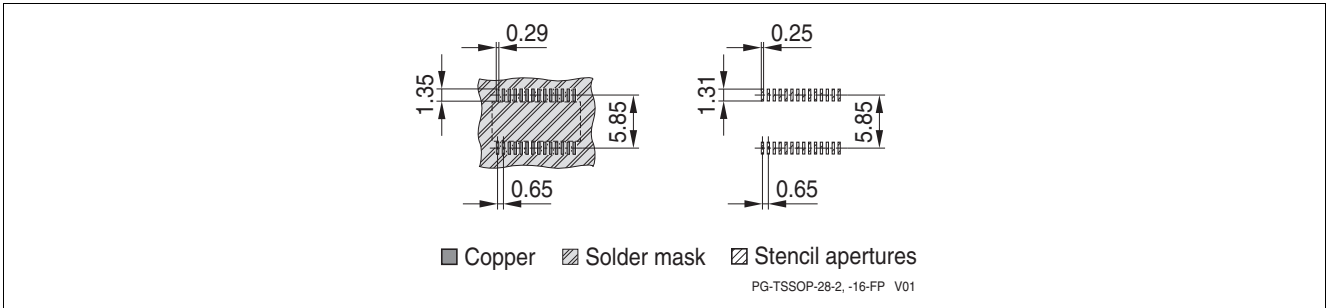


Figure 6-3 Recommended Footprint PG-TSSOP-28-2

6.3 Chip Marking

Line 1: SLB9660TT12 or SLB9660XT12, 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)

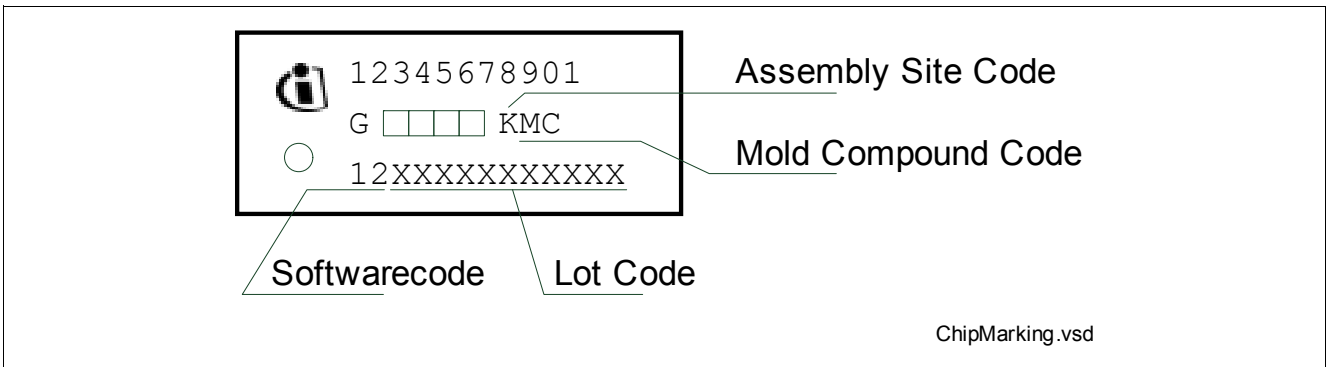


Figure 6-4 Chip Marking PG-TSSOP-28-2

Package Dimensions (VQFN)

7 Package Dimensions (VQFN)

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

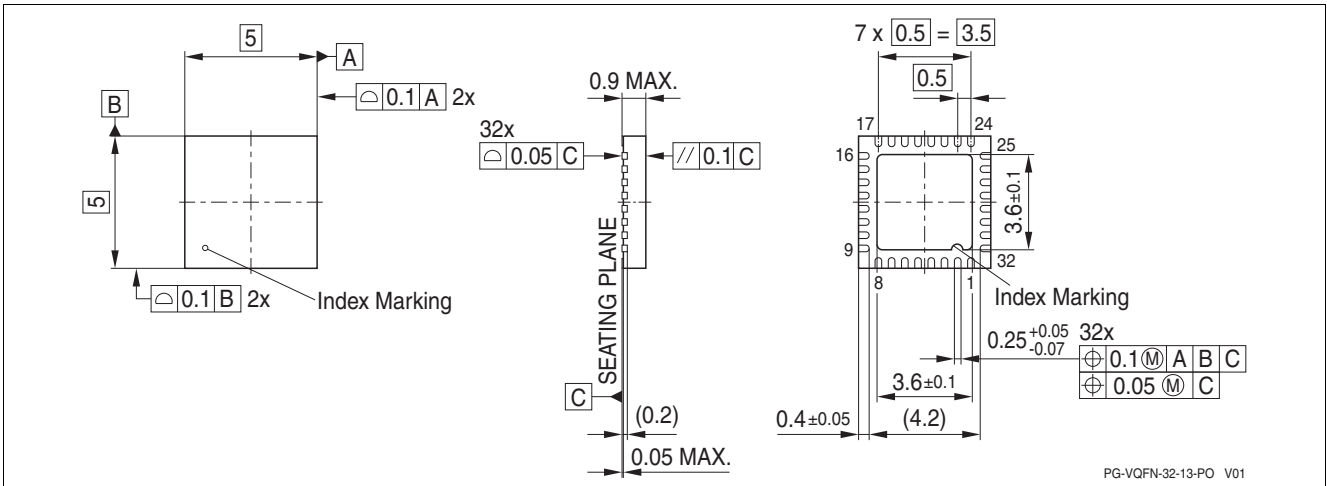


Figure 7-1 Package Dimensions PG-VQFN-32-13

7.1 Packing Type

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

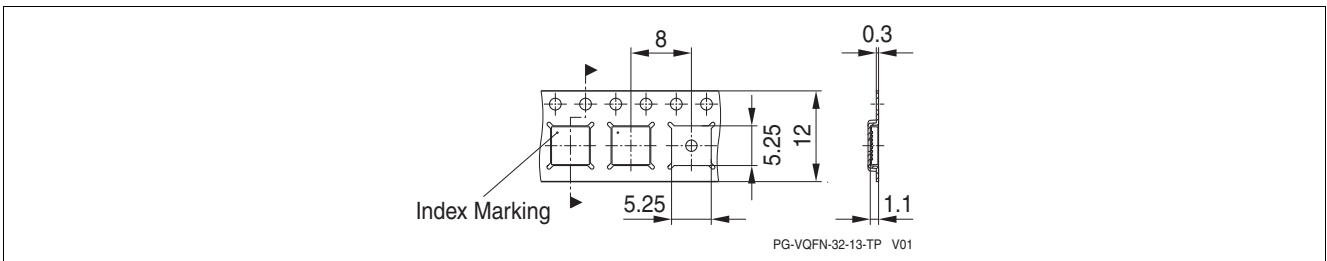


Figure 7-2 Tape & Reel Dimensions PG-VQFN-32-13

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 connect to GND externally as well.

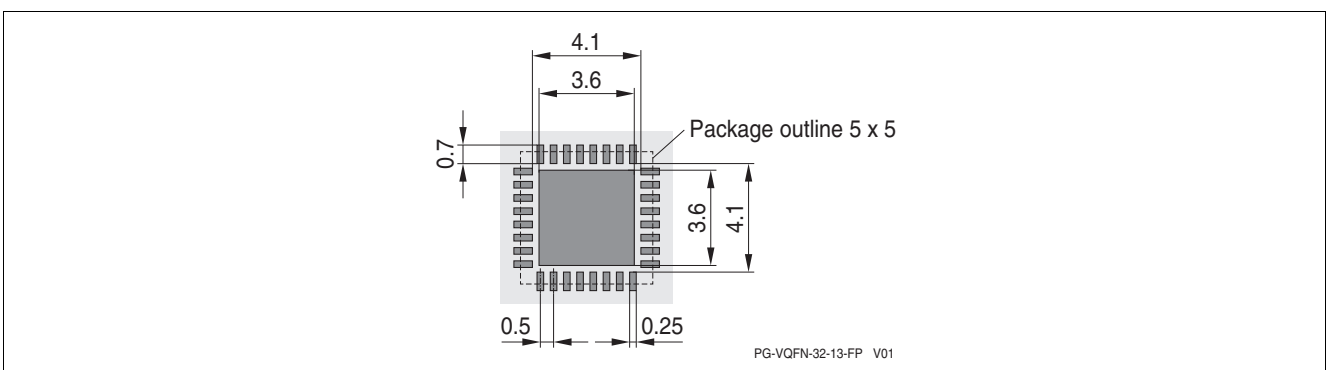


Figure 7-3 Recommended Footprint PG-VQFN-32-13

Package Dimensions (VQFN)

7.3 Chip Marking

Line 1: SLB 9660

Line 2: VQ12 yy or XQ12 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>

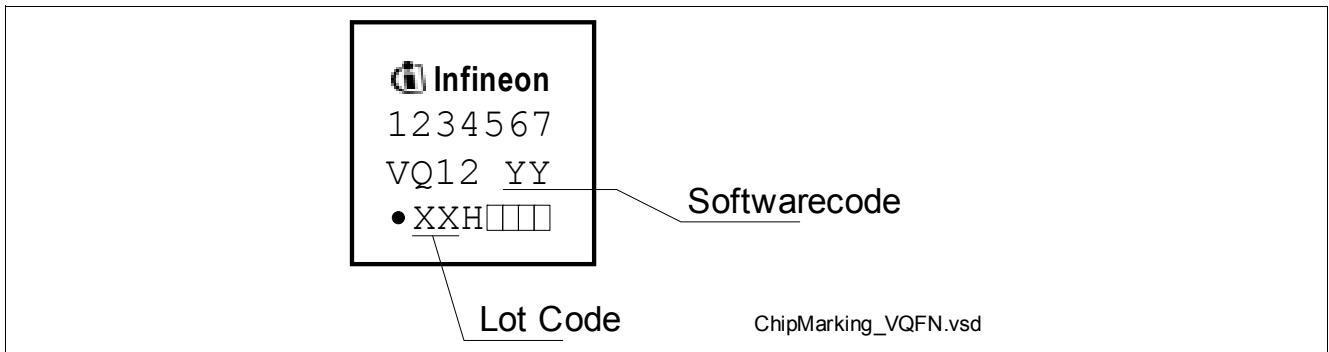


Figure 7-4 Chip Marking PG-VQFN-32-13

References

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] —, “TPM Main Specification”, Version 1.2, Rev. 116, 2011-03-01, TCG (parts 1-3)
- [4] —, “TCG PC Client TPM Interface Specification (TIS)”, Version 1.3, 2013-03-21, TCG

Terminology

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

Trademarks of Infineon Technologies AG

AURIX™, C166™, CanPAK™, CIPOST™, CoolGaN™, CoolMOS™, CoolSET™, CoolSiC™, CORECONTROL™, CROSSAVE™, DAVE™, DI-POL™, DrBLADE™, EasyPIM™, EconoBRIDGE™, EconoDUAL™, EconoPACK™, EconoPIM™, EiceDRIVER™, eupec™, FCOS™, HITFET™, HybridPACK™, ISOFACE™, IsoPACK™, MIPAQ™, ModSTACK™, my-d™, NovalithiC™, OmniTune™, OPTIGA™, OptiMOS™, ORIGA™, POWERCODE™, PRIMARION™, PrimePACK™, PrimeSTACK™, PROFET™, PRO-SIL™, RASIC™, REAL3™, ReverSave™, SatRIC™, SIEGET™, SIPMOS™, SmartLEWIS™, SOLID FLASH™, SPOC™, TEMPFET™, thinQ!™, TRENCHSTOP™, TriCore™.

Other Trademarks

µVision™, AMBA™, ARM™, KEIL™, MULTI-ICE™, THUMB™ of ARM Limited, UK. AUTOSAR™ of AUTOSAR development partnership. CIPURSE™ of OSPT Alliance. EMV™ of EMVCo, LLC (Visa Holdings Inc.). FLEXGO™ of Microsoft Corporation. HYPERTERMINAL™ of Hilgraeve Incorporated. IrDA™ of Infrared Data Association Corporation. MCS™ of Intel Corp. MICROWAVE OFFICE™ (MWO) of Applied Wave Research Inc. TEAKLITE™ of CEVA, Inc. VXWORKS™ of WIND RIVER SYSTEMS, INC. Chrome OS™ of Google, Inc.

Trademarks Update 2014-07-17

www.infineon.com

Edition 2014-12-12

Published by

Infineon Technologies AG
81726 Munich, Germany

© 2014 Infineon Technologies AG.

All Rights Reserved.

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.