OPTIGA™ TPM SLM 9670 TPM2.0

Trusted Platform Module

Data Sheet

Devices

- SLM 9670AQ2.0

TPM Key Features

- Random Number Generator (RNG) according to NIST SP800-90A
- TPM FW update functionality installed
- 6962 Bytes of free NV memory
- Full personalization with Endorsement Key (EK) and EK certificate
- Up to 3 keys in the volatile memory
- Up to 7 keys in the NV memory
- Up to 8 NV counters
- Support of various cryptographic algorithms
  - RSA-1024 and RSA-2048
  - SHA-1 and SHA-256
  - ECC NIST P256
  - ECC BN256

Hardware Features

- Qualified for industrial applications (JEDEC JESD-47)
- Highly reliable flash technology with hardening extension for industrial applications
- Enhanced industrial temperature range (-40..+105°C)
- SPI interface up to 43 MHz
- Low standby power consumption (typ. 110µA)
- Supply voltage 1.8V or 3.3V
- PG-VQFN-32-13 package
- Pin compatible to OPTIGA™ TPM SLB9670 TPM1.2

Compliance and Security Features

- Compliant to TPM Main Specification, Family “2.0”, Level 00, Revision 1.38
- Certification according Common Criteria EAL4+
- TPM2.0 compliant according to TCG test suites
- Sophisticated cryptographic hardware modules (crypto processor and cryptographic engines)
- Internal memory and bus encryption
- Tamper-resistant secure MCU
- Shielding and sensors against physical and logical attacks

About this document

Scope and purpose

This data sheet describes the OPTIGA™ TPM SLM 9670 TPM2.0 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 General Description

This chapter gives a high-level overview of the OPTIGA™ TPM SLM 9670 Trusted Platform Module and its features.

1.1 Overview

The OPTIGA™ TPM SLM 9670 (Trusted Platform Module) is a standardized security controller that protects the integrity and authenticity of devices in industrial systems. Built on proven technologies and supporting the latest TPM 2.0 standard, the OPTIGA™ TPM SLM 9670 features include secured storage for keys, certificates and passwords as well as dedicated key management. For details about the TCG specification, please refer to www.trustedcomputinggroup.org.

To simplify system integration into hardware, the OPTIGA™ TPM SLM 9670 uses an SPI interface according to the TCG specification (see **[2]**). Infineon provides driver software for a simple adaptation to any standard microcontroller SPI interface.

The TPM is a secure controller with added cryptographic functionality:

- High-end security controller with advanced cryptographic algorithms implemented in hardware (for instance, RSA-2048, ECC-256, SHA-256)
- Common criteria (EAL4+) security certification
- Flexible integration with SPI interface support
- Extended temperature range (-40 to +105°C) for a variety of applications
- Easy to integrate with wide range open source support
- Unique key that identifies each TPM

The OPTIGA™ TPM SLM 9670 is a quality-hardened Trusted Platform Module (TPM) for special use in industrial applications and based on a tamper-resistant secure microcontroller (MCU) using advanced hardware security technology.

As a turn-key solution, it is flashed with a securely coded firmware according to the latest TCG family 2.0 specifications (see **[1]** and **[2]**) offering a rich feature set of security functions.

The device is qualified according to the industrial JEDEC JESD-47 standard. It is targeting industrial applications requiring a higher level of security like components of industrial automation and control systems.

The OPTIGA™ TPM SLM 9670 is security certified according to Common Criteria EAL4+. It is available in a PG-VQFN-32-13 package.

1.2 Security Features

The security logic consists of sophisticated features, including error detection units, a set of sensors, regulators and filters along with an enhanced signal shield to detect faults as well as electrical and physical conditions, and initiate alarms to indicate security breaches.

1.3 Main Features and Customer Benefits

Main features and customer benefits of the industrial OPTIGA™ TPM SLM 9670:

- Reduced risk based on proven technology
- Fast time to market through concept reuse
- Flexibility thanks to wide range of security functions as well as dedicated key management
- Easy integration into all platform architectures and operating systems
- Tamper resistant hardware architecture with performant core and peripheral set (crypto coprocessors, RNG etc.) based on market leading security expertise

- Standardized and market approved turn-key security solution, preprogrammed with rich security functions (TCG standard TPM 2.0)
- Highly reliable NVM technology
- Industrial qualification according to JEDEC JESD-47
- Security certification according Common Criteria EAL4+
- Secured key store: secured personalization (key injection in secured environment), additional keys generated on chip
- Plug-and-play security solution: easy and cost efficient system integration through available open source complex drivers

The listed features support demanding customers to cope with increasing security requirements of today's and future complex industrial systems. The OPTIGA™ TPM SLM 9670 as plug-and play security solution helps tremendously to increase systems security level with very limited additional effort in software development and system integration and thus helps to reduce the total cost of ownership of the complete system.

1.4 Applications and Use Cases

The OPTIGA™ TPM SLM 9670, a member of the OPTIGA™ family, is a turn-key high security solution offering tamper resistance and strong functional security protection to industrial applications, which due to their functionality have an enhanced demand for security.

The industrial OPTIGA™ TPM SLM 9670 provides an outstanding level of security, from hardware as well as from software point of view. The standardized TPM 2.0 OPTIGA™ TPM SLM 9670 provides more than 90 commands according the TCG Specification **[1]** like

- key generation
- life cycle key management (key duplication back-up and refurbishment)
- authentication
- signature functions (signing / verifying)
- encryption / decryption
- secured logging
- secured time

The OPTIGA™ TPM SLM 9670 offers ready-to-use security to complex industrial systems and supports industrial security use cases like

- secured key store and management
- remote attestation
- device identity
- protection of software and configuration data
- privacy protection
- protection of secrets and intellectual property
- diagnostic and remote access

The OPTIGA™ TPM SLM 9670 can be used in various host platforms and host operating systems.

1.5 Power Management

In the OPTIGA™ TPM SLM 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 wakes up immediately and returns to the low-power mode after the transaction has been finished.

2 Block Diagram

Figure 1 show a high-level block diagram of the OPTIGA™ TPM SLM 9670.

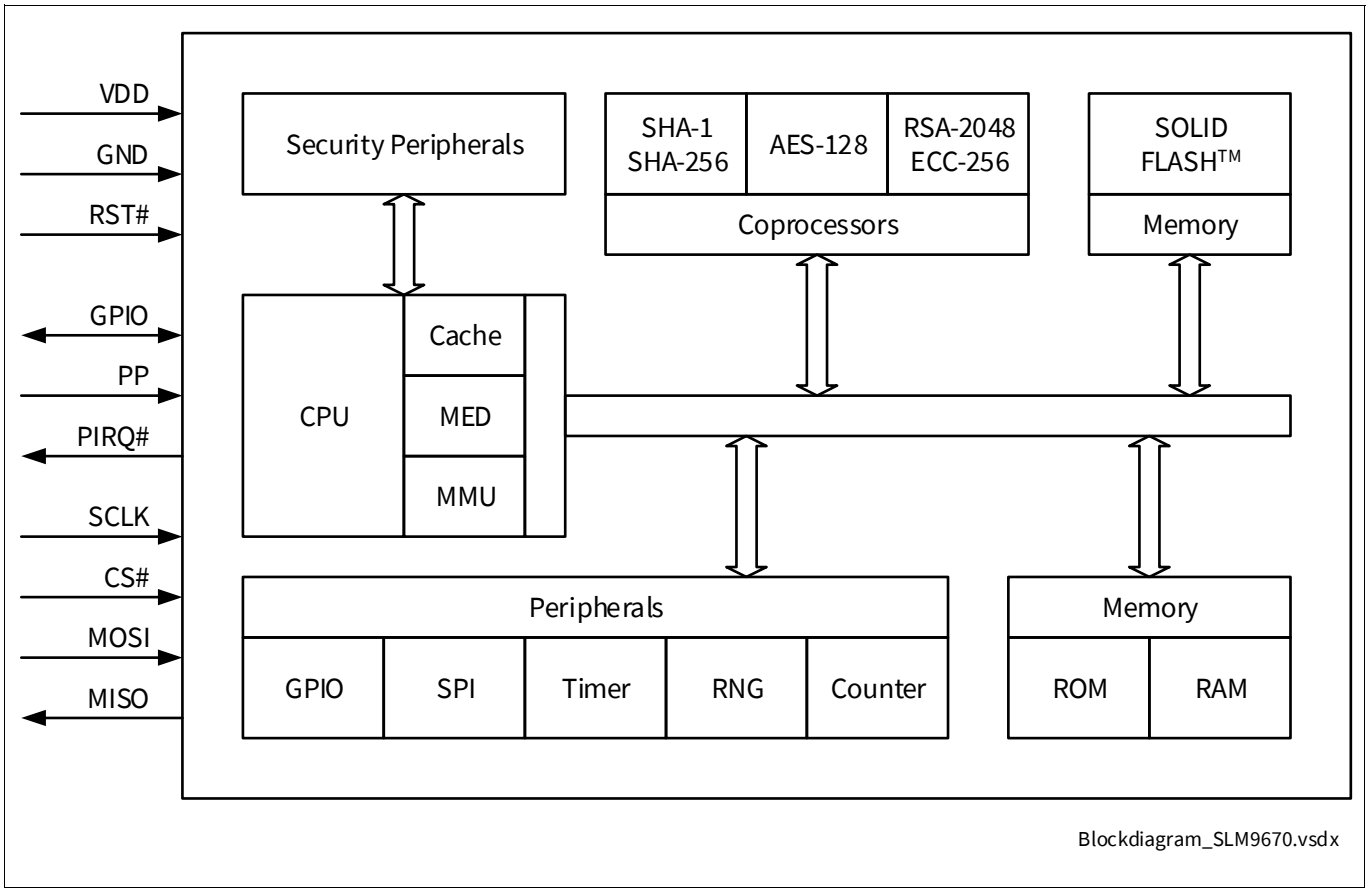

Figure 1 Block Diagram of OPTIGA™ TPM SLM 9670

3 Pin Description

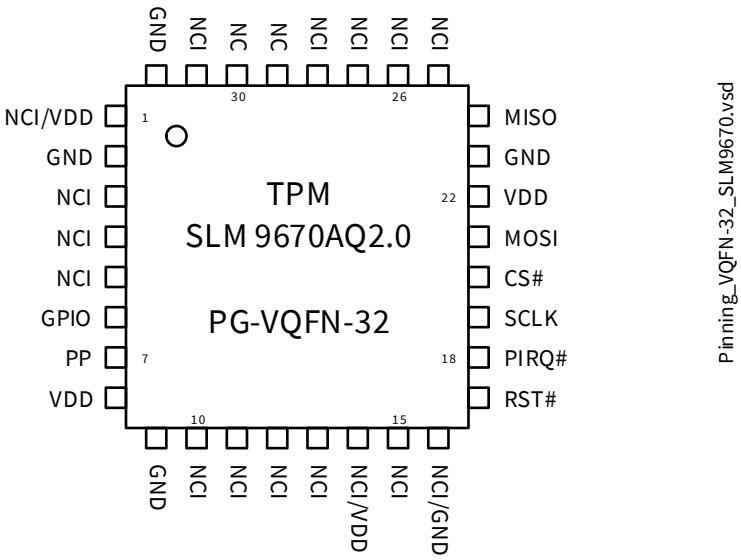

Figure 2 Pinout of the OPTIGA™ TPM SLM 9670 (PG-VQFN-32-13 Package, Top View)

Table 1 Buffer Types

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

Table 2 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.

Pin Description

Table 2 I/O Signals (continued)

Pin Number PG-VQFN-32-13	Name	Pin Type	Buffer Type	Function
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** The TPM 2.0 device does not use this functionality. This pin may be left unconnected; it has an internal pull-up resistor.
7	PP	I	ST	**Physical Presence** The TPM2.0 device does not use this functionality. This pin may be left unconnected; it has an internal pulldown resistor.

Table 3 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 4 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 [2]. To be compliant, VDD can be connected to this pin.

Table 4 Not Connected (continued)

Pin Number PG-VQFN-32-13	Name	Pin Type	Buffer Type	Function
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 [2]. 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 [2]. To be compliant, GND can be connected to this pins.

3.1 Typical Schematic

Figure 3 shows the typical schematic for the OPTIGA™ TPM SLM 9670. The power supply pins should be bypassed to GND with capacitors located close to the device.

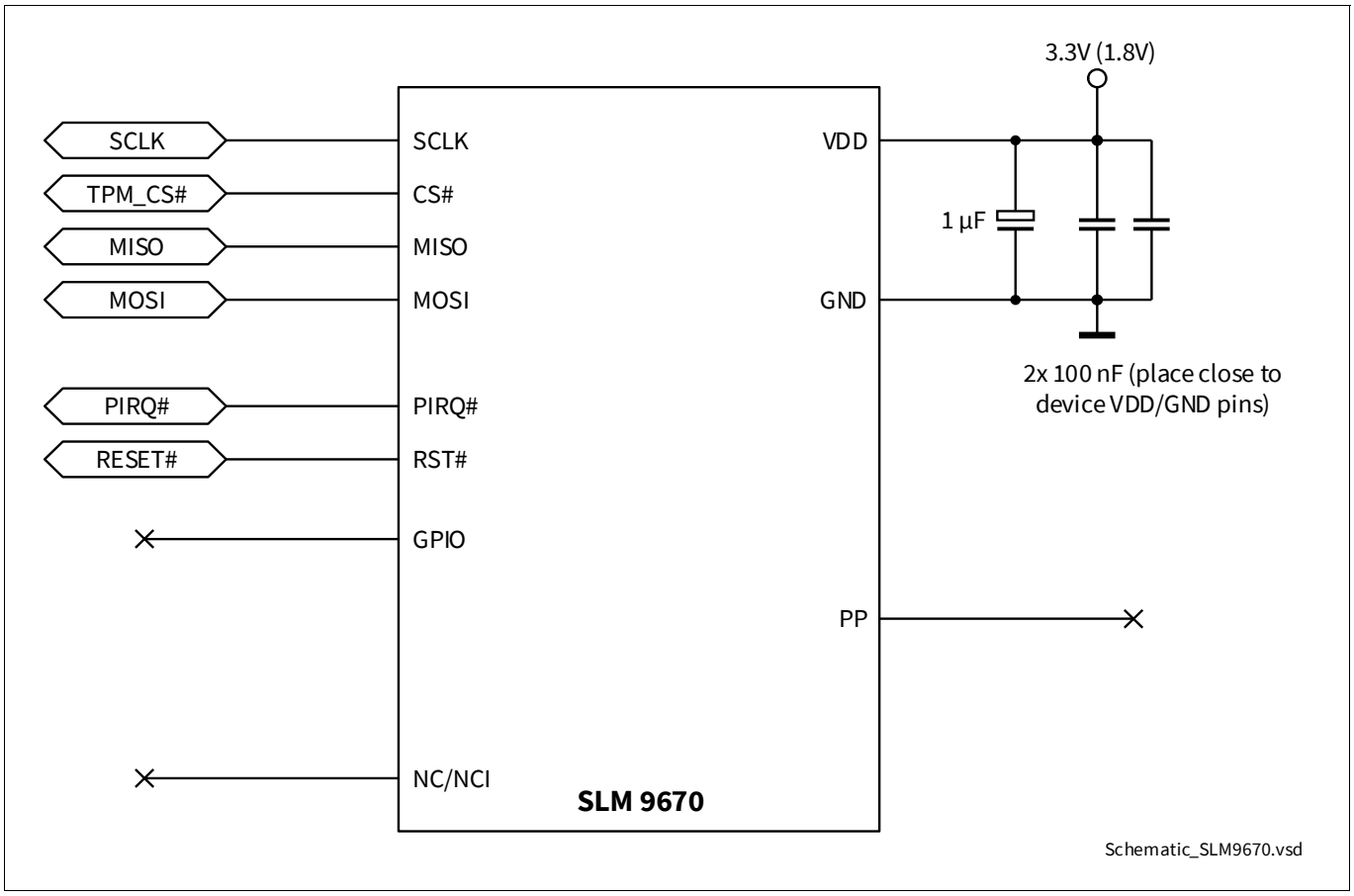

Figure 3 Typical Schematic

4 TPM Properties

All properties defined within the TPM can be read with the command TPM2_GetCapability (capability = TPM_CAP_TPM_PROPERTIES). The values are vendor dependent or determined by a platform-specific specification. The following properties are returned by the Infineon OPTIGA™ TPM SLM 9670:

Table 5 Infineon Specific Property Values

TPM_PT_MANUFACTURER	“IFX”
TPM_PT_VENDOR_STRING_1	“SLM9”
TPM_PT_VENDOR_STRING_2	“670”
TPM_PT_VENDOR_STRING_3	NULL
TPM_PT_VENDOR_STRING_4	NULL
TPM_PT_FIRMWARE_VERSION_1	Major and minor version (for instance, 0x00070055 indicates V7.85)
TPM_PT_FIRMWARE_VERSION_2	Build number and Common Criteria certification state (for instance, 0x0011CB00 or 0x0011CB02) Byte 1: reserved for future use (0x00) Byte 2 and 3: Build number (for instance, 0x11CB) Byte 4: Common Criteria certification state, 0x00 means TPM is CC certified, 0x02 means TPM is not certified
TPM_PT_MODES	Bit 0 (FIPS_140_2) = 1 Bits 1..31 = 0

Reading these properties returns the current version and state of the firmware. This implies that the values read back might differ from the ones shown in **Table 5** above.

5 Electrical Characteristics

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

5.1 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	-40	–	105	°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.

5.2 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	-40	–	105	°C	–
Junction temperature	T_j	–	–	110	°C	see **Section 5.3** below
Useful lifetime		–	–	20	y	–

5.3 Thermal Resistance

Table 8 Thermal Resistance

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Junction to case	$R_{th(JC)}$		35		K/W	to exposed pad (bottom)[1]
Junction to ambient	$R_{th(JA)}$		179		K/W	1) 2)

1) not subject to production test, specified by design

2) according to JEDEC JESD 51-5, JESD 51-7 at free convection and radiation on FR4 2s2p board. Board size 76.2mm x 114.3mm x 1.5mm, 2 inner copper layers (35µm), thermal via array under the exposed pad connected to the first inner copper layer. Also refer to **http://www.infineon.com/cms/en/product/technology/packages/PG-VQFN**

As shown in **Table 7**, a maximum junction temperature of **110**°C must not be exceeded. Thermal simulations (done using the FEM software ANSYS®) show that this temperature limit is not reached at an ambient temperature of 105°C when the device is mounted on a PCB according to JEDEC 2s2p (JESD 51-7, JESD 51-5).

If the device is mounted on a PCB compliant to JEDEC 1s0p (JESD 51-3), the simulation shows that due to self-heating of the device, the maximum junction temperature is exceeded at an ambient temperature of 105°C.

5.4 DC Characteristics

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

Table 9 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, MISOand SCLK don't care

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

Note: Device sleep mode will be entered after 50 milliseconds of inactivity after the last TPM command was executed.

Table 10 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

Table 10 DC Characteristics of SPI Interface Pins (SCLK, CS#, MISO, MOSI, RST#, PIRQ#) (continued)

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
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 11 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

5.5 AC Characteristics

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

Table 12 Device Reset

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Cold (Power-On) Reset	t_{POR}	80			µs	see **Section 5.6**
Warm Reset	t_{WRST}	2			µs	see **Section 5.6**
Reset Inactive Time	t_{RSTIN}	60			ms	see **Section 5.6**

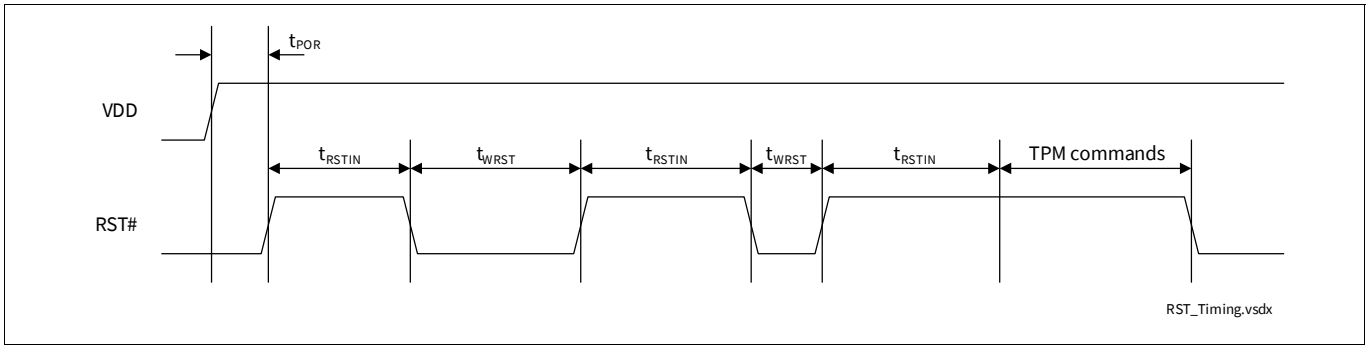

Figure 4 RST# Timing

Table 13 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, $t_{SLEW} \geq$ 1V/ns
				22.5	MHz	$V_{DD,typ}$ = 1.8V, $t_{SLEW} \geq$ 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}
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

Table 13 AC Characteristics of SPI Interface (continued)

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
MISO valid delay time	t_V	0		0.7 t_{CLKL}	ns	Output valid delay from SCLK falling edge
MISO active time	t_{DRV}	0			ns	Delay from chip select assertion to driving of MISO

5.6 Timing

Some pads are disabled after deassertion of the reset signal for up to 500 µs.

The OPTIGA™ TPM SLM 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 SLM 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 SLM 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 4** and **Table 12**).

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 TPM2_Shutdown should be issued before the assertion of the RST# signal.

6 Package Dimensions (VQFN)

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

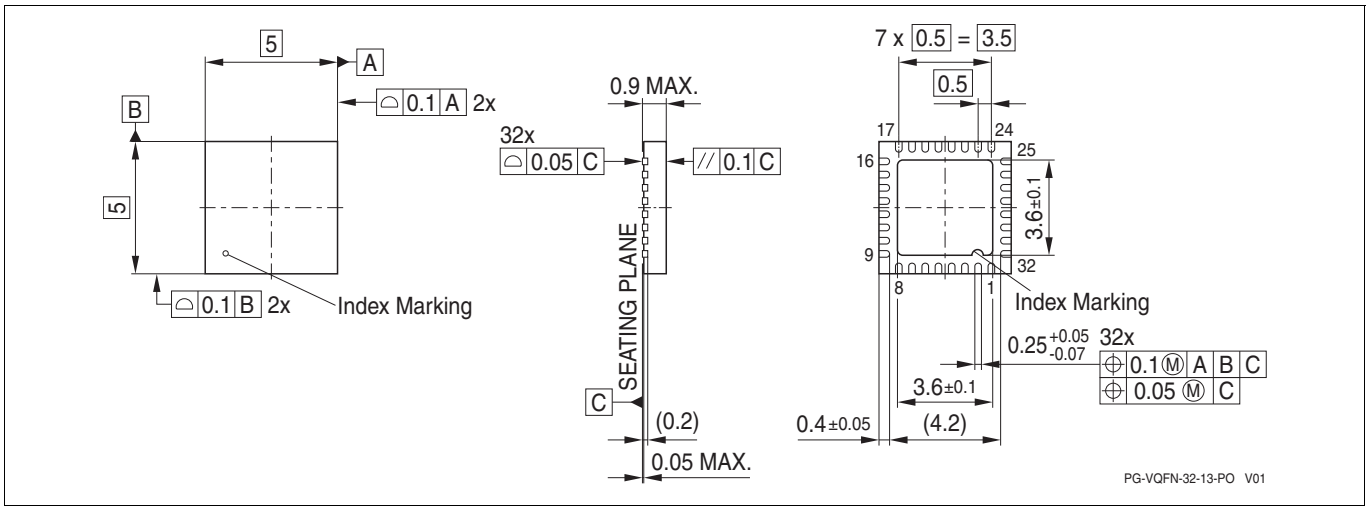

Figure 5 Package Dimensions PG-VQFN-32-13

6.1 Packing Type

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

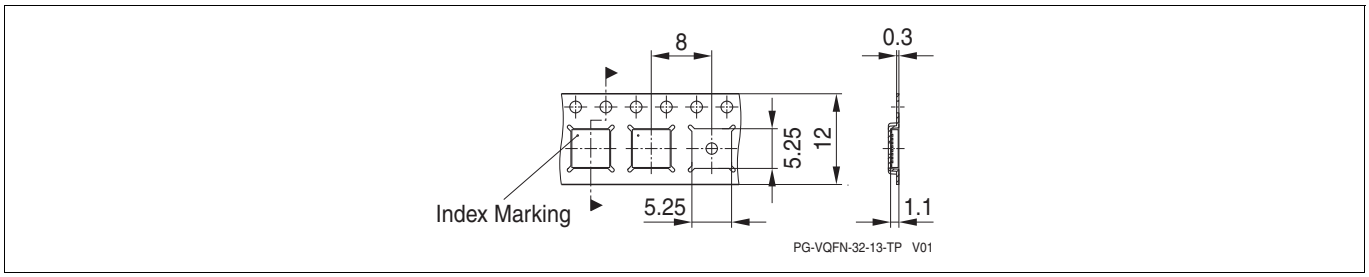

Figure 6 Tape & Reel Dimensions PG-VQFN-32-13

6.2 Recommended Footprint

Figure 7 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.

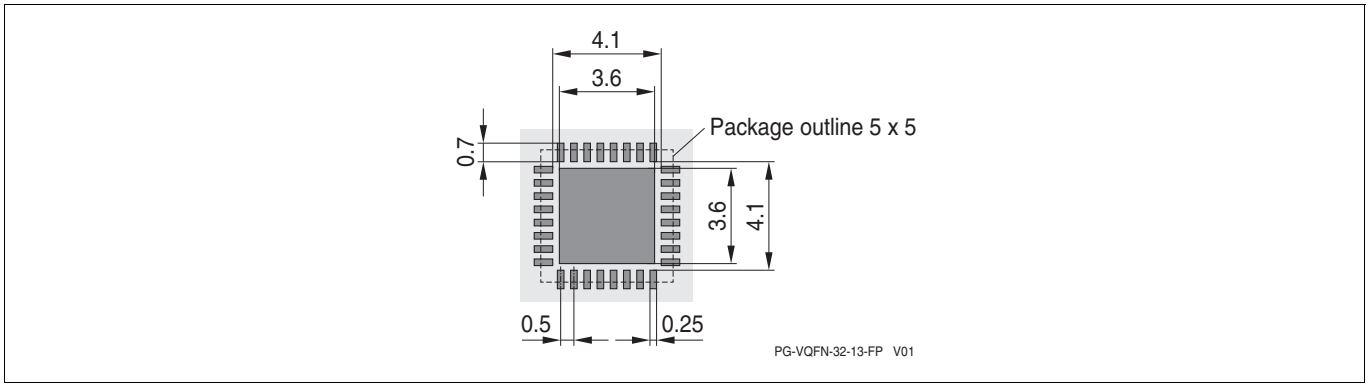

Figure 7 Recommended Footprint PG-VQFN-32-13

6.3 Chip Marking

Line 1: SLM9670

Line 2: AQ20 yy, the <yy> is an internal FW indication (only at manufacturing due to field upgrade option)

Line 3: <Lot number> H <datecode>

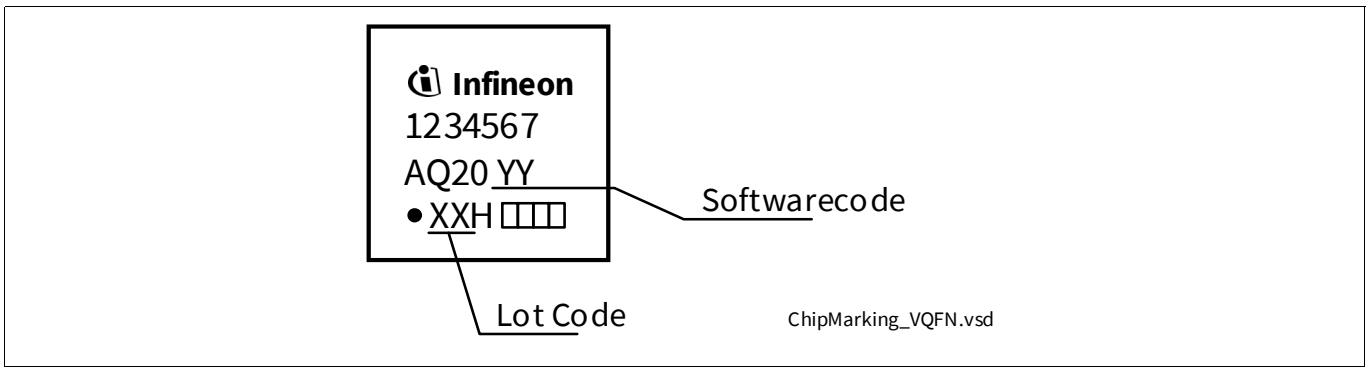

Figure 8 Chip Marking PG-VQFN-32-13

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

References

[1] —, “Trusted Platform Module Library (Part 1-4)”, Family 2.0, Level 00, Rev. 01.38, 2016-09-29, TCG

[2] —, “TCG PC Client Platform TPM Profile (PTP) Specification”, Family 2.0, Level 00, Rev. 01.03 v22, May 22, 2017, TCG

Terminology

ESW	Embedded Software
HMAC	Hashed Message Authentication Code
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

Licenses and Notices

The following License and Notice Statements are reproduced from [1].

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.

Revision History

Reference	Description
Revision 1.0, 2019-04-08	
	Initial revision.

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

Edition 2019-04-08
Published by
Infineon Technologies AG
81726 Munich, Germany

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

单击下面可查看定价，库存，交付和生命周期等信息

>>Infineon(英飞凌)