



Welcome to [E-XFL.COM](#)

### [Embedded - Microcontrollers - Application Specific](#): Tailored Solutions for Precision and Performance

[Embedded - Microcontrollers - Application Specific](#) represents a category of microcontrollers designed with unique features and capabilities tailored to specific application needs. Unlike general-purpose microcontrollers, application-specific microcontrollers are optimized for particular tasks, offering enhanced performance, efficiency, and functionality to meet the demands of specialized applications.

### What Are [Embedded - Microcontrollers - Application Specific](#)?

Application specific microcontrollers are engineered to

#### Details

|                         |                                                                                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product Status          | Active                                                                                                                                                                          |
| Applications            | Trusted Platform Module (TPM)                                                                                                                                                   |
| Core Processor          | 16-Bit                                                                                                                                                                          |
| Program Memory Type     | NVM (6.8kB)                                                                                                                                                                     |
| Controller Series       | -                                                                                                                                                                               |
| RAM Size                | -                                                                                                                                                                               |
| Interface               | SPI                                                                                                                                                                             |
| Number of I/O           | 1                                                                                                                                                                               |
| Voltage - Supply        | 1.65V ~ 3.6V                                                                                                                                                                    |
| Operating Temperature   | -20°C ~ 85°C (TA)                                                                                                                                                               |
| Mounting Type           | Surface Mount                                                                                                                                                                   |
| Package / Case          | 32-VFQFN Exposed Pad                                                                                                                                                            |
| Supplier Device Package | PG-VQFN-32-13                                                                                                                                                                   |
| Purchase URL            | <a href="https://www.e-xfl.com/product-detail/infineon-technologies/slb9670vq12fw641xuma1">https://www.e-xfl.com/product-detail/infineon-technologies/slb9670vq12fw641xuma1</a> |

# Trusted Platform Module

TPM

SLB 9670 TCG Rev. 1.16

SLB 9670VQ1.2

SLB 9670XQ1.2

## Data Sheet

Revision 1.0, 2015-11-05

Chip Card and Security

---

**Revision History**

| <b>Page or Item</b>             | <b>Subjects (major changes since previous revision)</b> |
|---------------------------------|---------------------------------------------------------|
| <b>Revision 1.0, 2015-11-05</b> |                                                         |
|                                 | Initial version.                                        |

## Table of Contents

|          |                                            |           |
|----------|--------------------------------------------|-----------|
| <b>1</b> | <b>Overview</b>                            | <b>6</b>  |
| 1.1      | Power Management                           | 6         |
| <b>2</b> | <b>Device Types / Ordering Information</b> | <b>6</b>  |
| <b>3</b> | <b>Pin Description</b>                     | <b>7</b>  |
| 3.1      | Typical Schematic                          | 9         |
| <b>4</b> | <b>Electrical Characteristics</b>          | <b>10</b> |
| 4.1      | Absolute Maximum Ratings                   | 10        |
| 4.2      | Functional Operating Range                 | 10        |
| 4.3      | DC Characteristics                         | 11        |
| 4.4      | AC Characteristics                         | 12        |
| 4.5      | Timing                                     | 13        |
| <b>5</b> | <b>Package Dimensions (VQFN)</b>           | <b>14</b> |
| 5.1      | Packing Type                               | 14        |
| 5.2      | Recommended Footprint                      | 14        |
| 5.3      | Chip Marking                               | 15        |



List of Figures

List of Figures

Figure 3-1 Pinout of the SLB 9670VQ1.2 and SLB 9670XQ1.2 (PG-VQFN-32-13 Package, Top View) ..... 7

Figure 3-2 Typical Schematic..... 9

Figure 5-1 Package Dimensions PG-VQFN-32-13..... 14

Figure 5-2 Tape & Reel Dimensions PG-VQFN-32-13..... 14

Figure 5-3 Recommended Footprint PG-VQFN-32-13 ..... 14

Figure 5-4 Chip Marking PG-VQFN-32-13..... 15



List of Tables

List of Tables

|           |                                                                                     |    |
|-----------|-------------------------------------------------------------------------------------|----|
| Table 2-1 | Device Configuration .....                                                          | 6  |
| Table 3-1 | Buffer Types .....                                                                  | 7  |
| Table 3-2 | I/O Signals .....                                                                   | 7  |
| Table 3-3 | Power Supply .....                                                                  | 8  |
| Table 3-4 | Not Connected .....                                                                 | 8  |
| Table 4-1 | Absolute Maximum Ratings .....                                                      | 10 |
| Table 4-2 | Functional Operating Range .....                                                    | 10 |
| Table 4-3 | Current Consumption .....                                                           | 11 |
| Table 4-4 | DC Characteristics of SPI Interface Pins (SCLK, CS#, MISO, MOSI, RST#, PIRQ#) ..... | 11 |
| Table 4-5 | DC Characteristics of GPIO and PP Pins .....                                        | 12 |
| Table 4-6 | Device Reset .....                                                                  | 12 |
| Table 4-7 | AC Characteristics of SPI Interface .....                                           | 12 |

## **1 Overview**

The SLB 9670 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 PG-VQFN-32-13 package. It supports an SPI interface with a transfer rate of up to 43 MHz. The SLB 9670 is a TPM based on TCG family 1.2 specifications (see [\[1\]](#) and [\[2\]](#)).

- Compliant to TPM Main Specification, Version 1.2, Rev. 116
- SPI interface
- Approved for Google Chromebook / Chromebox
- Standard (-20..+80°C) and Enhanced temperature range (-40..+85°C)
- PG-VQFN-32-13 package
- Optimized for battery operated devices: low standby power consumption (typ. 110µA)
- 24 PCRs
- 6 kByte free NV memory
- Up to 10 concurrent sessions
- Up to eight 2048-bit keys can be loaded into volatile storage
- 16 slots for keys of up to 2048-bit
- 8 monotonic counters
- 1280 Byte I/O buffer
- Built-in support by Linux Kernel

### **1.1 Power Management**

In the SLB 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 will wake immediately and will return to the low-power mode after the transaction has been finished.

## **2 Device Types / Ordering Information**

The SLB 9670 product family features devices using a VQFN package. [Table 2-1](#) shows the different versions.

**Table 2-1 Device Configuration**

| <b>Device Name</b> | <b>Package</b> | <b>Remarks</b>             |
|--------------------|----------------|----------------------------|
| SLB 9670VQ1.2      | PG-VQFN-32-13  | Standard temperature range |
| SLB 9670XQ1.2      | PG-VQFN-32-13  | Enhanced temperature range |

## Pin Description

### 3 Pin Description

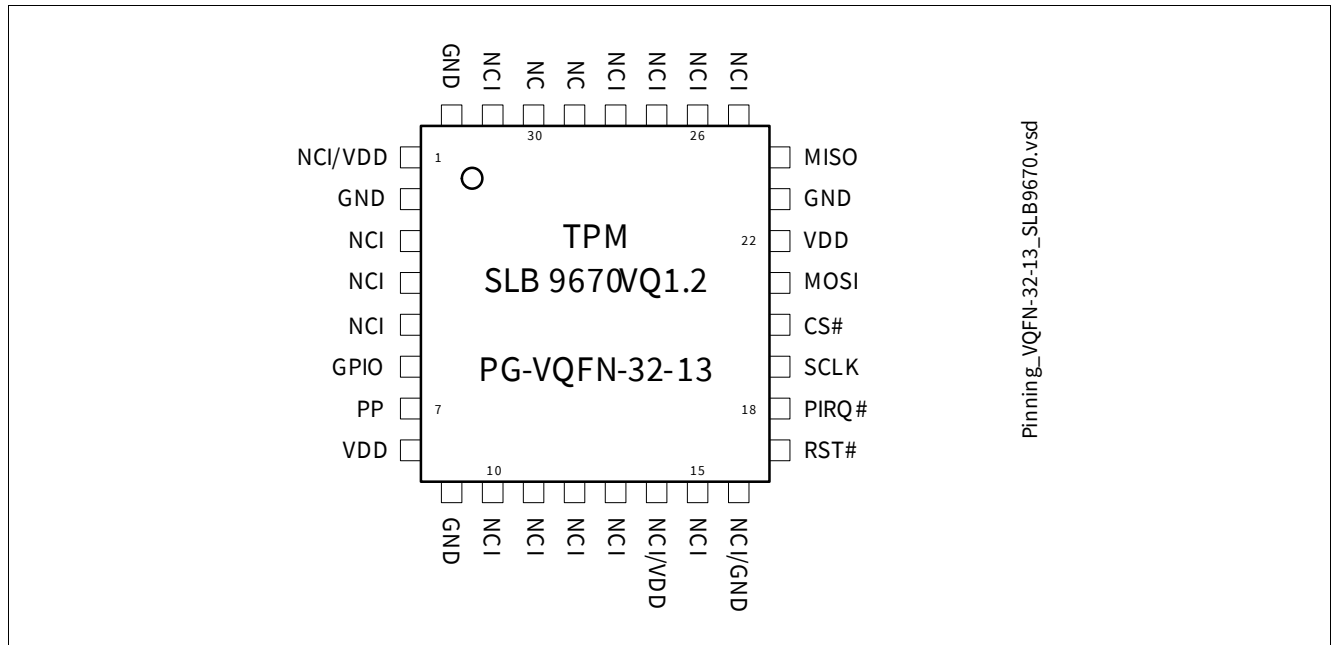


Figure 3-1 Pinout of the SLB 9670VQ1.2 and SLB 9670XQ1.2 (PG-VQFN-32-13 Package, Top View)

Table 3-1 Buffer Types

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

Table 3-2 I/O Signals

| Pin Number           | Name  | Pin Type | Buffer Type | Function                                                                                                                                 |
|----------------------|-------|----------|-------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PG-VQFN-32-13</b> |       |          |             |                                                                                                                                          |
| 20                   | CS#   | I        | ST          | <b>Chip Select</b><br>The SPI chip select signal (active low).                                                                           |
| 19                   | SCLK  | I        | ST          | <b>SPI Clock</b><br>The SPI clock signal. Only SPI mode 0 is supported by the device.                                                    |
| 21                   | MOSI  | I        | ST          | <b>Master Out Slave In (SPI Data)</b><br>SPI data which is received from the master.                                                     |
| 24                   | MISO  | O        | TS          | <b>Master In Slave Out (SPI Data)</b><br>SPI data which is sent to the SPI bus master.                                                   |
| 18                   | PIRQ# | O        | OD          | <b>Interrupt Request</b><br>Interrupt request signal to the host. The pin has no internal pull-up resistor. The interrupt is active low. |

Pin Description

Table 3-2 I/O Signals (continued)

| Pin Number<br>PG-VQFN-32-13 | Name | Pin Type | Buffer Type | Function                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|------|----------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 17                          | RST# | I        | ST          | <b>Reset</b><br>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          | <b>GPIO-Express-00 Signal</b><br>This pin is a general purpose I/O pin. It is defined as GPIO-Express-00, please refer to [2] and the PCISIG ECN “Trusted Configuration Space for PCI Express”. This pin may be left unconnected; it has an internal pull-up resistor.                                                                             |
| 7                           | PP   | I        | ST          | <b>Physical Presence</b><br>This pin should be connected to a jumper. The standard position of the jumper should connect the pin to GND. If the pin is connected to VDD, some special commands are enabled (for instance, the command TPM_ForceClear, also refer to [1]). This pin may be left unconnected; it has an internal pull-down resistor. |

Table 3-3 Power Supply

| Pin Number<br>PG-VQFN-32-13 | Name | Pin Type | Buffer Type | Function                                                                                                              |
|-----------------------------|------|----------|-------------|-----------------------------------------------------------------------------------------------------------------------|
| 8, 22                       | VDD  | PWR      | —           | <b>Power Supply</b><br>All VDD pins must be connected externally and should be bypassed to GND via 100 nF capacitors. |
| 2, 9, 23, 32                | GND  | GND      | —           | <b>Ground</b><br>All GND pins must be connected externally.                                                           |

Table 3-4 Not Connected

| Pin Number<br>PG-VQFN-32-13     | Name | Pin Type | Buffer Type | Function                                                                                                |
|---------------------------------|------|----------|-------------|---------------------------------------------------------------------------------------------------------|
| 29, 30                          | NC   | NU       | —           | <b>No Connect</b><br>All pins must not be connected externally (must be left floating).                 |
| 3 - 5, 10 - 13, 15, 25 - 28, 31 | NCI  | —        | —           | <b>Not Connected Internally</b><br>All pins are not connected internally (can be connected externally). |

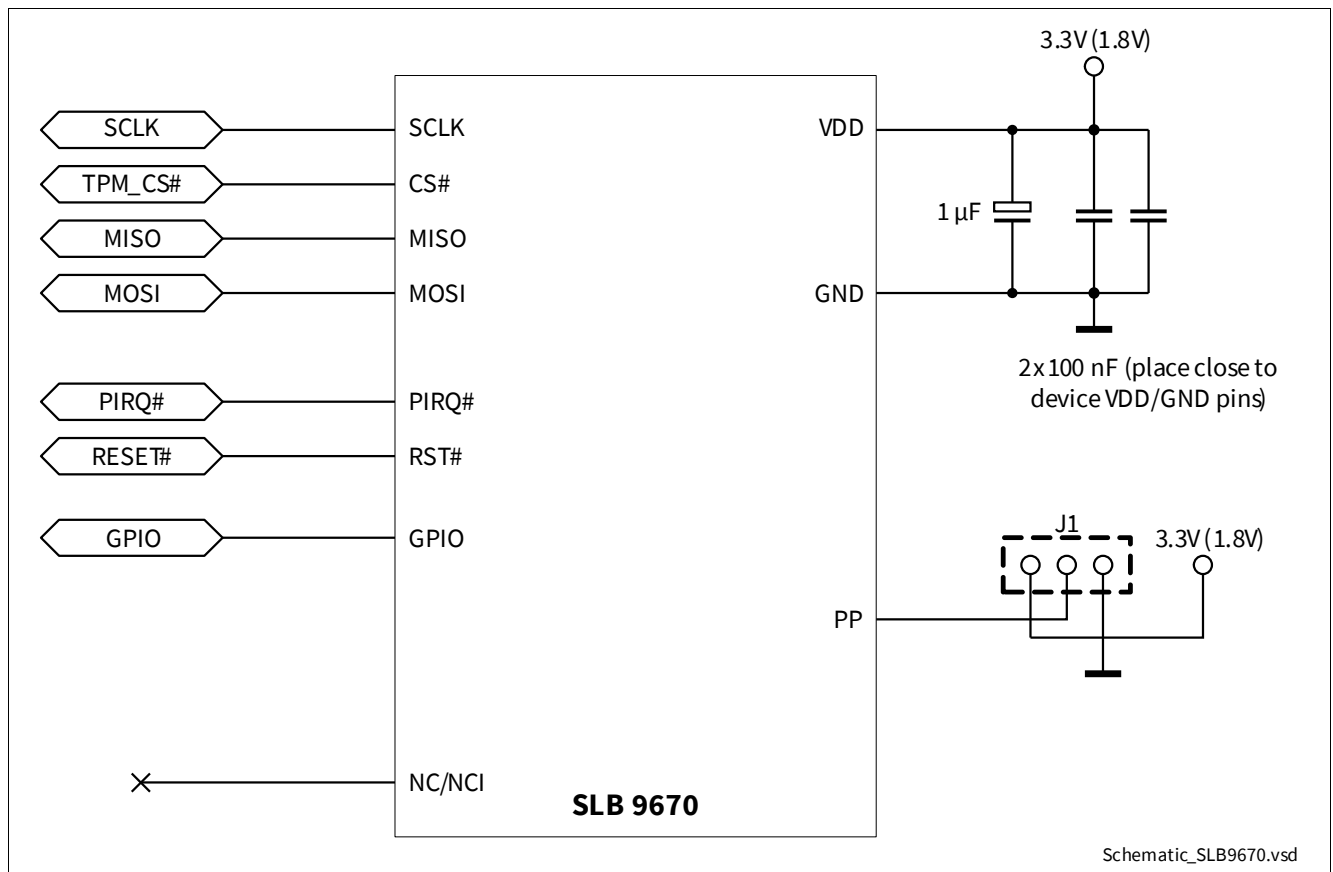
## Pin Description

**Table 3-4 Not Connected** (continued)

| Pin Number           | Name    | Pin Type | Buffer Type | Function                                                                                                                                                                                                                                     |
|----------------------|---------|----------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PG-VQFN-32-13</b> |         |          |             |                                                                                                                                                                                                                                              |
| 1, 14                | NCI/VDD | —        | —           | <b>Not Connected Internally/VDD</b><br>All pins are not connected internally (can be connected externally).<br>Note that pins 1 and 14 are defined as VDD in the TCG specification [5]. To be compliant, VDD can be connected to these pins. |
| 16                   | NCI/GND | —        | —           | <b>Not Connected Internally/GND</b><br>This pin is not connected internally (can be connected externally).<br>Note that pin 16 is defined as GND in the TCG specification [5]. To be compliant, GND can be connected to this pins.           |

### 3.1 Typical Schematic

**Figure 3-2** shows the typical schematic for the SLB 9670. 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 3-2 Typical Schematic**

## Electrical Characteristics

### 4 Electrical Characteristics

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

#### 4.1 Absolute Maximum Ratings

**Table 4-1 Absolute Maximum Ratings**

| Parameter                                      | Symbol        | Values |      |              | Unit | Note or Test Condition                                   |
|------------------------------------------------|---------------|--------|------|--------------|------|----------------------------------------------------------|
|                                                |               | Min.   | Typ. | Max.         |      |                                                          |
| Supply Voltage                                 | $V_{DD}$      | -0.3   | –    | 7.0          | V    | –                                                        |
| Voltage on any pin                             | $V_{max}$     | -0.3   | –    | $V_{DD}+0.3$ | V    | –                                                        |
|                                                |               | -0.5   | –    | $V_{DD}+0.5$ | V    | $V_{DD} = 3.3V \pm 10\%$ ; pins MISO, MOSI, SCLK and CS# |
| 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:<br>1.5 k $\Omega$ , 100 pF | $V_{ESD,HBM}$ | –      | –    | 2000         | V    | According to EIA/JESD22-A114-B                           |
| ESD robustness                                 | $V_{ESD,CDM}$ | –      | –    | 500          | V    | According to ESD Association<br>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 4-2 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    | –                            |
|                                  |          | 1.65   | 1.8  | 1.95 | V    | –                            |
| Ambient temperature              | $T_A$    | -20    | –    | 85   | °C   | Standard temperature devices |
| Ambient temperature              | $T_A$    | -40    | –    | 85   | °C   | Enhanced temperature devices |
| Useful lifetime <sup>1)</sup>    |          | –      | –    | 5    | y    |                              |
| Operating lifetime <sup>1)</sup> |          | –      | –    | 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%. A 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

### 4.3 DC Characteristics

$T_A = 25^\circ\text{C}$ ,  $V_{DD} = 3.3\text{V} \pm 0.3\text{V}$  or  $V_{DD} = 1.8\text{V} \pm 0.15\text{V}$  unless otherwise noted.

**Table 4-3 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  |      | $\mu\text{A}$ | Pin PP = GND, pins GPIO, RST# and PIRQ# = $V_{DD}$ , CS# inactive ( $=V_{DD}$ ), MOSI, MISO and SCLK don't care |

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

**Table 4-4 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             | $V_{DD,typ} = 3.3\text{V}$ , only pins SCLK, MISO, MOSI and CS#                                          |
|                         |            | $0.7 V_{DD}$ |      | $V_{DD}+0.3$ | V             | $V_{DD,typ} = 3.3\text{V}$ , pin RST#                                                                    |
|                         |            | $0.7 V_{DD}$ |      | $V_{DD}+0.3$ | V             | $V_{DD,typ} = 1.8\text{V}$                                                                               |
| Input voltage low       | $V_{IL}$   | -0.5         |      | $0.3 V_{DD}$ | V             | $V_{DD,typ} = 3.3\text{V}$ , only pins SCLK, MISO, MOSI and CS#                                          |
|                         |            | -0.3         |      | $0.3 V_{DD}$ | V             | $V_{DD,typ} = 3.3\text{V}$ , pin RST#                                                                    |
|                         |            | -0.3         |      | $0.3 V_{DD}$ | V             | $V_{DD,typ} = 1.8\text{V}$                                                                               |
| Input leakage current   | $I_{LEAK}$ | -20          |      | 20           | $\mu\text{A}$ | $0\text{V} < V_{IN} < V_{DD}$                                                                            |
|                         |            | -150         |      | 150          | $\mu\text{A}$ | Pins SCLK, CS#, MISO, MOSI<br>$-0.5\text{V} < V_{IN} < V_{DD}+0.5\text{V}$<br>$V_{DD,typ} = 3.3\text{V}$ |
|                         |            | -150         |      | 150          | $\mu\text{A}$ | Pin RST#<br>$-0.5\text{V} < V_{IN} < V_{DD}+0.3\text{V}$<br>$V_{DD,typ} = 3.3\text{V}$                   |
|                         |            | -150         |      | 150          | $\mu\text{A}$ | $-0.3\text{V} < V_{IN} < V_{DD}+0.3\text{V}$<br>$V_{DD,typ} = 1.8\text{V}$                               |
| Output high voltage     | $V_{OH}$   | $0.9 V_{DD}$ |      |              | V             | $I_{OH} = -100\mu\text{A}$                                                                               |
| Output low voltage      | $V_{OL}$   |              |      | $0.1 V_{DD}$ | V             | $I_{OL} = 1.5\text{mA}$                                                                                  |
| Pad input capacitance   | $C_{IN}$   |              |      | 10           | pF            |                                                                                                          |
| Output load capacitance | $C_{LOAD}$ |              |      | 40           | pF            |                                                                                                          |

## Electrical Characteristics

**Table 4-5 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           | $\mu A$ | $0V < V_{IN} < V_{DD}$           |
|                       |            | -150         |      | 150          | $\mu A$ | $-0.3V < V_{IN} < V_{DD} + 0.3V$ |
| 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                 |

## 4.4 AC Characteristics

$T_A = 25^\circ C$ ,  $V_{DD} = 3.3V \pm 0.3V$  or  $V_{DD} = 1.8V \pm 0.15V$  unless otherwise noted.

**Table 4-6 Device Reset**

| Parameter         | Symbol    | Values |      |      | Unit    | Note or Test Condition |
|-------------------|-----------|--------|------|------|---------|------------------------|
|                   |           | Min.   | Typ. | Max. |         |                        |
| Reset Pulse Width | $t_{RST}$ | 80     |      |      | $\mu s$ | Cold (power-on) reset  |
| Reset Pulse Width | $t_{RST}$ | 2      |      |      | $\mu s$ | Warm reset             |

**Table 4-7 AC Characteristics of SPI Interface**

| Parameter                       | Symbol     | Values            |             |                   | Unit    | Note or Test Condition                                         |
|---------------------------------|------------|-------------------|-------------|-------------------|---------|----------------------------------------------------------------|
|                                 |            | Min.              | Typ.        | Max.              |         |                                                                |
| SCLK frequency                  | $f_{CLK}$  |                   |             | 43                | MHz     | $V_{DD,typ} = 3.3V$                                            |
|                                 |            |                   |             | 22.5              | MHz     | $V_{DD,typ} = 1.8V$                                            |
| SCLK period                     | $t_{CLK}$  | $1/f_{CLK} - 5\%$ | $1/f_{CLK}$ | $1/f_{CLK} + 5\%$ | $\mu s$ | Rising edge to rising edge, measured at $V_{IN} = 0.5 V_{DD}$  |
| SCLK low time                   | $t_{CLKL}$ | $0.45 t_{CLK}$    |             |                   | $\mu s$ | Falling edge to rising edge, measured at $V_{IN} = 0.5 V_{DD}$ |
| SCLK high time                  | $t_{CLKL}$ | $0.45 t_{CLK}$    |             |                   | $\mu s$ | Rising edge to falling edge, measured at $V_{IN} = 0.5 V_{DD}$ |
| SCLK slew rate (rising/falling) | $t_{SLEW}$ | 1                 |             | 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                                    |
| CS# setup time                  | $t_{CSS}$  | 5                 |             |                   | ns      | CS# falling edge to SCLK rising edge                           |
| CS# hold time                   | $t_{CSH}$  | 5                 |             |                   | ns      | SCLK falling edge to CS# rising edge                           |

## Electrical Characteristics

**Table 4-7 AC Characteristics of SPI Interface** (continued)

| Parameter             | Symbol   | Values |      |                | Unit | Note or Test Condition                    |
|-----------------------|----------|--------|------|----------------|------|-------------------------------------------|
|                       |          | Min.   | Typ. | Max.           |      |                                           |
| 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   |
| MISO valid delay time | $t_V$    | 0      |      | $0.7 t_{CLKL}$ | ns   | Output valid delay from SCLK falling edge |

### 4.5 Timing

Some pads are disabled after deassertion of the reset signal for up to 500  $\mu$ s.

## Package Dimensions (VQFN)

### 5 Package Dimensions (VQFN)

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

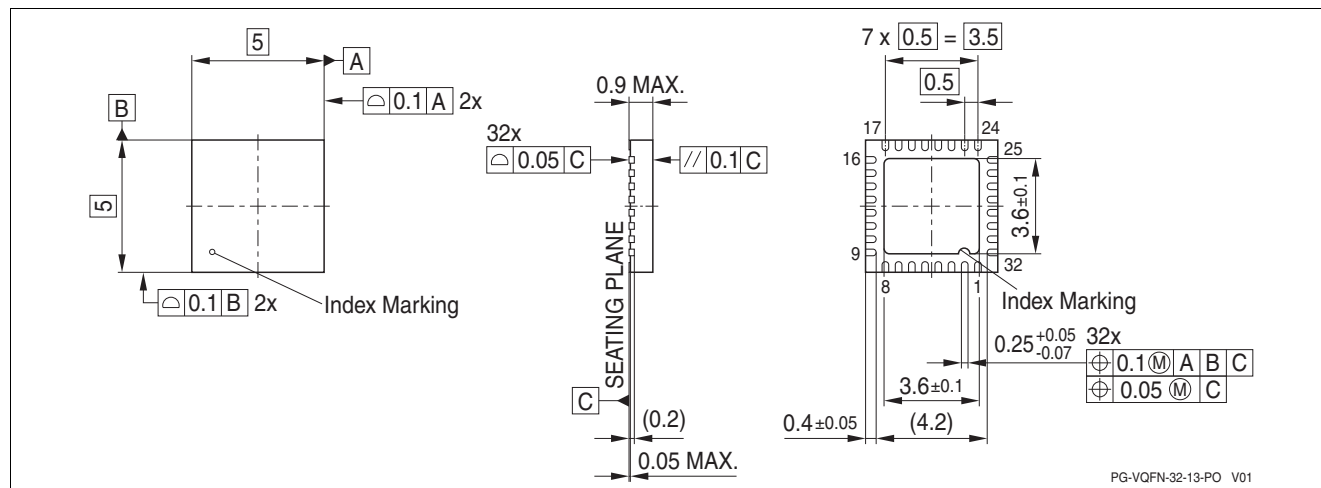


Figure 5-1 Package Dimensions PG-VQFN-32-13

#### 5.1 Packing Type

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

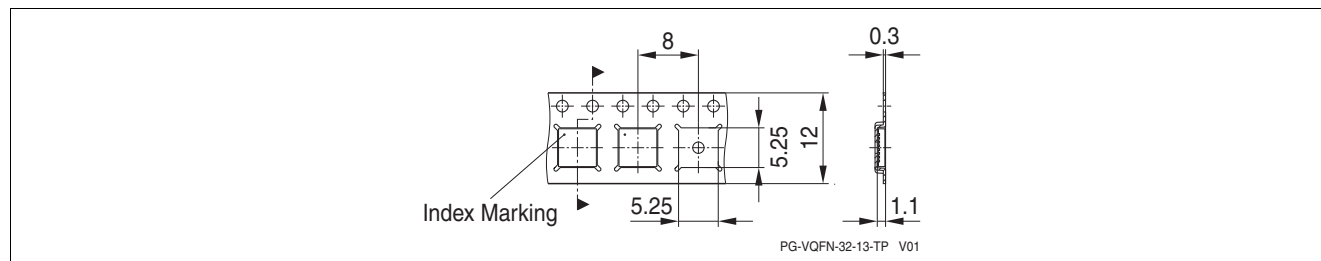


Figure 5-2 Tape & Reel Dimensions PG-VQFN-32-13

#### 5.2 Recommended Footprint

**Figure 5-3** 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.

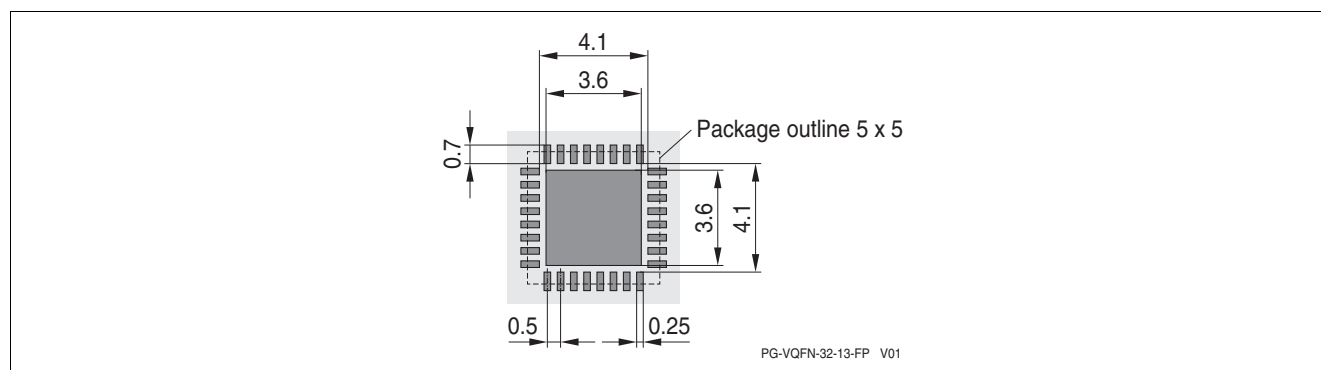


Figure 5-3 Recommended Footprint PG-VQFN-32-13

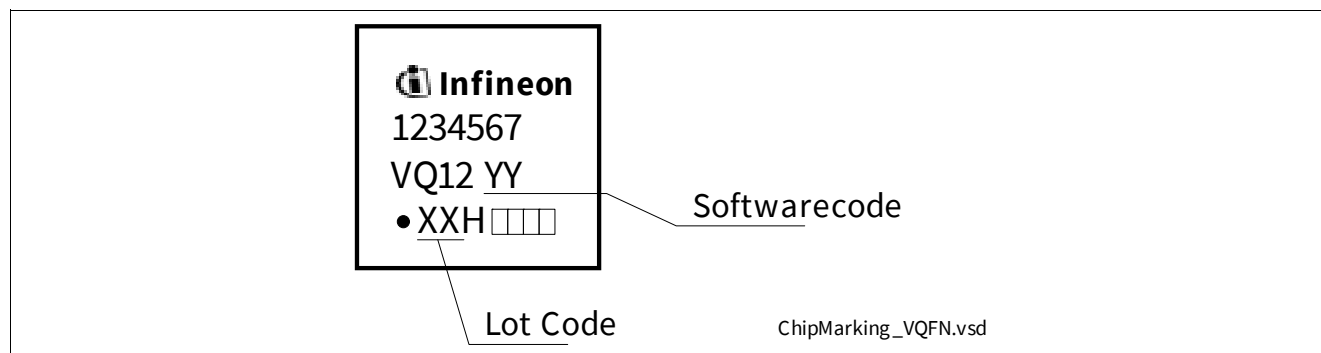
Package Dimensions (VQFN)

### 5.3 Chip Marking

Line 1: SLB9670

Line 2: VQ12 yy or XQ12 yy (see [Table 2-1](#)), the <yy> is an internal FW indication (only at manufacturing due to field upgrade option)

Line 3: <Lot number> H <datecode>



**Figure 5-4 Chip Marking PG-VQFN-32-13**

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

---

**References**

**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 1.3, 2013-03-21, 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] —, “TCG PC Client Platform TPM Profile (PTP) Specification”, Rev. 00.43, 2014-08-04, TCG

---

**Terminology**

**Terminology**

|       |                                    |
|-------|------------------------------------|
| ESW   | Embedded Software                  |
| HMAC  | Hashed Message Authentication Code |
| LPC   | Low Pin Count (bus)                |
| 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                 |

---

#### 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](http://www.infineon.com)

**Edition 2015-11-05**

**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](mailto: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](http://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.