

# OPTIGA™ TPM

## SLB 9673 TPM2.0

### Data Sheet

#### Devices

- SLB 9673XU2.0 FW26.xx
- SLB 9673AU2.0 FW26.xx

#### Key features

- Optimized TPM device for IoT and ICT applications
- Compliant to TPM Main Specification, Family "2.0", Level 00, Revision 01.59
- Certifications:
  - CC, Version 3.1 Rev.5, level EAL4+, AVA\_VAN.4 (moderate) according to TCG PC Client TPM Protection Profile (targeted)
  - FIPS 140-2 level 2 (physical security level 3) (targeted)
- I2C interface
- Random Number Generator (RNG) implemented according to NIST SP800-90A using entropy source according to NIST SP800-90B
- Full personalization with 4 Endorsement Keys (EK) and 4 EK certificates (RSA 2048, RSA3072, ECC NIST P256, ECC NIST P384)
- Standard temperature range (-40°C .. +85°C) or enhanced temperature range (-40°C .. +105°C)
- PG-UQFN-32-1,-2 package
- Optimized for battery operated devices: low standby power consumption (typ. 120 µA)
- 24 PCRs (SHA-1, SHA-256 or SHA384)
- 51 kByte NV memory
- Unlimited amount of NV counters (only depending on NV memory utilization)
- 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)
- Pre-generation of up to 7 RSA key pairs
- RSA key generation (1024, 2048, 3072 and 4096 bit)
- ECC (NIST P256, BN P256, NIST P384)
- SHA1, SHA256, SHA384

## **About this document**

### **Scope and purpose**

This data sheet describes the OPTIGA™ TPM SLB 9673 FW26.xx 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**

<b>1</b>	<b>Overview</b>	<b>6</b>
1.1	Power management	6
1.2	Device address	6
<b>2</b>	<b>Device types and 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>TPM properties</b>	<b>10</b>
4.1	TPM register polling	10
<b>5</b>	<b>Electrical characteristics</b>	<b>11</b>
5.1	Absolute maximum ratings	11
5.2	Functional operating range	11
5.3	DC characteristics	12
5.4	AC characteristics	13
5.4.1	I2C Interface Characteristics	13
5.5	Timing	15
<b>6</b>	<b>Package dimensions (UQFN)</b>	<b>16</b>
6.1	Packing type	16
6.2	Recommended footprint	17
6.3	Chip marking	17

---

**List of figures**

**List of figures**

Figure 1	Pinout of the OPTIGA™ TPM SLB 9673 (PG-UQFN-32-1,-2 package, top view) .....	7
Figure 2	Typical schematic.....	9
Figure 3	Reset timing.....	13
Figure 4	Package dimensions PG-UQFN-32-1,-2 .....	16
Figure 5	Tape & reel dimensions PG-UQFN-32-1,-2 .....	16
Figure 6	Recommended footprint PG-UQFN-32-1,-2 .....	17
Figure 7	Chip marking .....	17

**List of tables**

**List of tables**

Table 1	Device configuration .....	6
Table 2	Buffer types .....	7
Table 3	I/O Signals .....	7
Table 4	Power supply .....	8
Table 5	Not connected .....	8
Table 6	Infineon TPM property values .....	10
Table 7	Absolute maximum ratings .....	11
Table 8	Functional operating range .....	11
Table 9	Current consumption .....	12
Table 10	DC characteristics of interface pins (SCL, SDA, TEST#, RST#, I2C_PIRQ#) .....	12
Table 11	DC characteristics of GPIO pins .....	12
Table 12	Power supply .....	13
Table 13	Device reset .....	13
Table 14	I2C Standard Mode Interface Characteristics .....	13
Table 15	I2C Fast Mode Interface Characteristics .....	14
Table 16	I2C Fast Mode plus Interface Characteristics .....	15

## Overview

# 1 Overview

The OPTIGA™ TPM SLB 9673 is a Trusted Platform Module. It is available in PG-UQFN-32-1,-2 package. It supports an I2C interface with a transfer rate of up to 1 MHz. The OPTIGA™ TPM SLB 9673 is a TPM based on TCG family 2.0 specifications (see [\[1\]](#) and [\[2\]](#)).

This TPM product is targeted to be certified, using the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Rev.5, in the level EAL4+, AVA\_VAN.4 (moderate), ALC\_FLR.1 according to the Protection Profile PC Client Specific TPM, TPM Library Specification Family "2.0" Level 0 Revision 1.59 (CERTIFICATE <td><sup>1)</sup>

## 1.1 Power management

In the OPTIGA™ TPM SLB 9673, 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 I2C bus from the host platform, the device will wake immediately and will return to the low-power mode after the transaction has been finished.

## 1.2 Device address

The I2C interface uses 7-bit addressing. The default address of the device is 0x2E (also see [\[2\]](#)).

# 2 Device types and ordering information

The OPTIGA™ TPM SLB 9673 product family features devices using an UQFN package. [Table 1](#) shows the available versions.

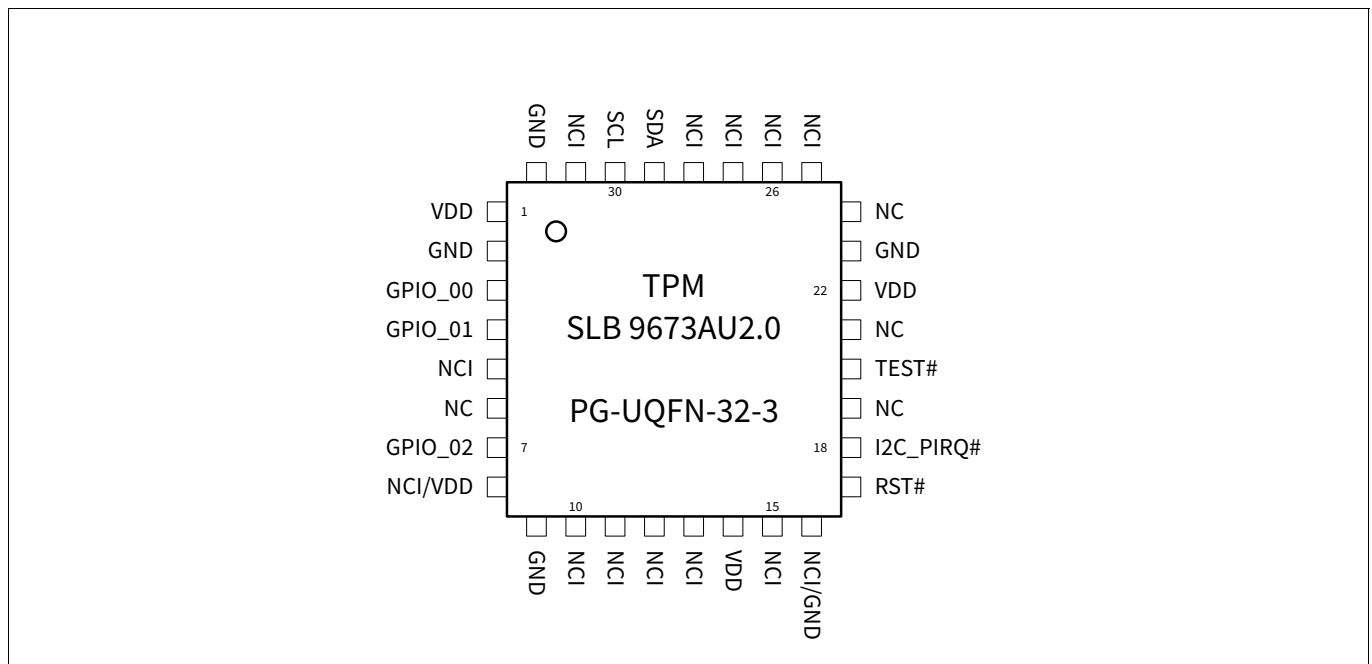
**Table 1 Device configuration**

Device Name	Package	Remarks
SLB 9673XU2.0 FW26.xx	PG-UQFN-32-1,-2	Standard temperature range -40°C - 85°C
SLB 9673AU2.0 FW26.xx	PG-UQFN-32-1,-2	Enhanced temperature range -40°C - 105°C

1) Exact reference not yet available at document generation time

## Pin description

### 3 Pin description



**Figure 1** Pinout of the OPTIGA™ TPM SLB 9673 (PG-UQFN-32-1,-2 package, top view)

**Table 2** Buffer types

Buffer type	Description
TS	Tri-state pin
ST	Schmitt-trigger pin
OD	Open-drain pin

**Table 3** I/O Signals

Pin number	Name	Pin type	Buffer type	Function
<b>PG-UQFN-32-1,-2</b>				
30	SCL	I	ST	<b>I2C bus clock signal</b> The clock signal of the I2C bus.
29	SDA	I/O	TS	<b>I2C bus data signal</b> The data signal of the I2C bus.
18	I2C_PIRQ#	O	OD	<b>Interrupt signal</b> This pin can be connected to the host interrupt controller to allow interrupt driven reads of the response data instead of polling. As soon as a response is available, the signal is asserted (low) and remains active until the complete response is read by the host.
17	RST#	I	ST	<b>Reset</b> External reset signal. Asserting this pin unconditionally resets the device. The signal is active low. This pin has a weak internal pull-up resistor.

## Pin description

**Table 3 I/O Signals** (continued)

Pin number	Name	Pin type	Buffer type	Function
PG-UQFN-32-1,-2				
20	TEST#	I	ST	<b>Test</b> Test signal, must be externally connected to a static high level.
3	GPIO_00	I/O	TS	<b>General purpose IO</b> This pin may be left unconnected; it has an internal pull-up resistor. It can be controlled via TPM NV GPIO functionality.
4	GPIO_01	I/O	TS	<b>General purpose IO</b> This pin may be left unconnected; it has an internal pull-up resistor. It can be controlled via TPM NV GPIO functionality.
7	GPIO_02	I/O	TS	<b>General purpose IO</b> This pin may be left unconnected; it has an internal pull-up resistor. It can be controlled via TPM NV GPIO functionality.

**Table 4 Power supply**

Pin number	Name	Pin type	Buffer type	Function
PG-UQFN-32-1,-2				
1, 14, 22	VDD	PWR	—	<b>Power supply</b> 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> All GND pins must be connected externally.

**Table 5 Not connected**

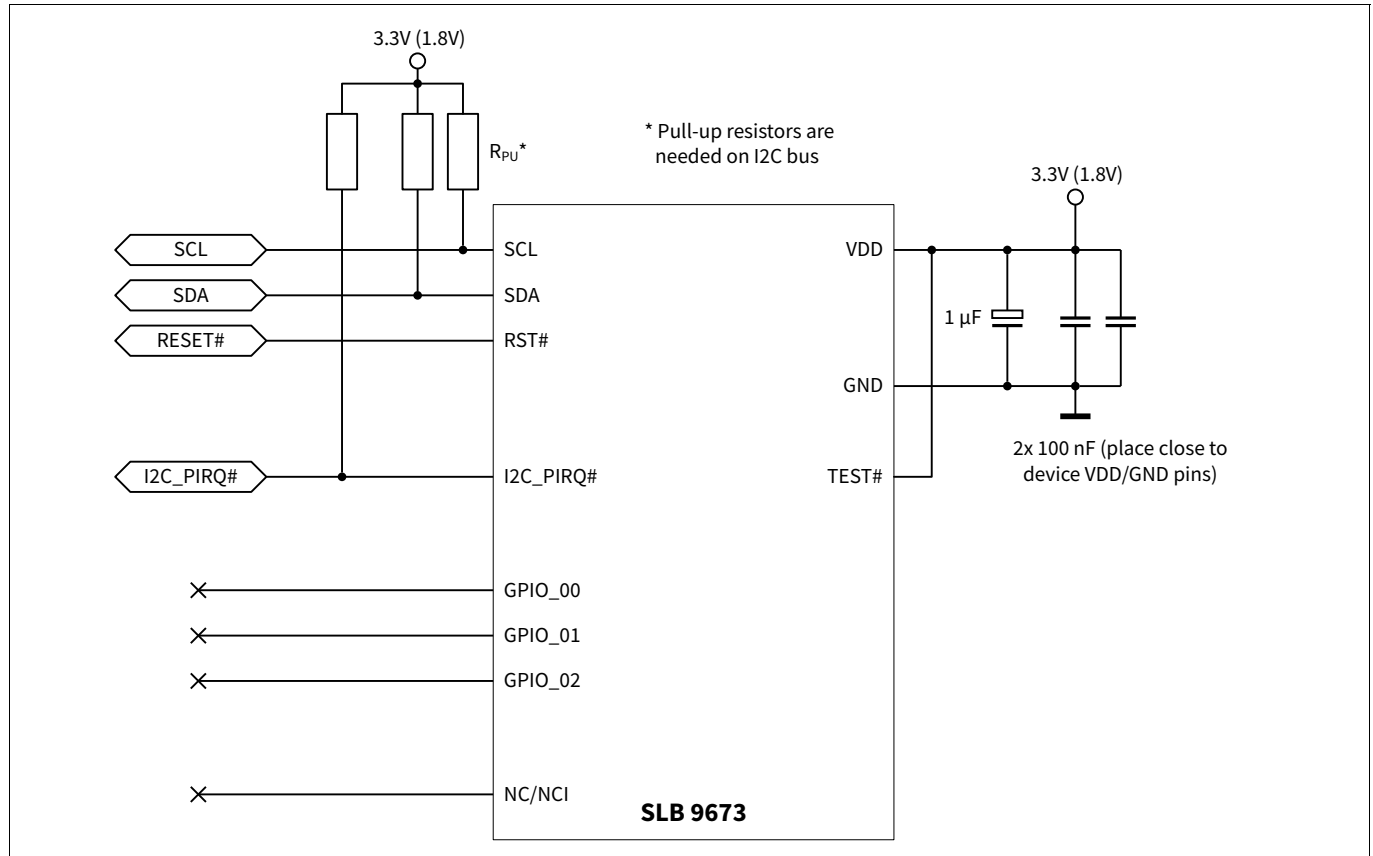
Pin number	Name	Pin type	Buffer type	Function
PG-UQFN-32-1,-2				
6, 19, 21, 24	NC	NU	—	<b>No connect</b> All pins must not be connected externally (must be left floating).
5, 10 - 13, 15, 25 - 28, 31	NCI	—	—	<b>Not connected internally</b> All pins are not connected internally (can be connected externally).
8	NCI/VDD	—	—	<b>Not connected internally/VDD</b> This pin is not connected internally (can be connected externally). Note that pin 8 is defined as VDD in the TCG specification <a href="#">[2]</a> . To be compliant, VDD can be connected to this pin.
16	NCI/GND	—	—	<b>Not connected internally/GND</b> This pin is not connected internally (can be connected externally). Note that pin 16 is defined as GND in the TCG specification <a href="#">[2]</a> . To be compliant, GND can be connected to this pins.



## Pin description

### 3.1 Typical schematic

**Figure 2** shows the typical schematic for the OPTIGA™ TPM SLB 9673. The power supply pins should be bypassed to GND with capacitors located close to the device.



**Figure 2** Typical schematic

## TPM properties

### 4 TPM properties

Properties defined within the TPM can be read with the command TPM2\_GetCapability. The values are vendor dependent or determined by a platform-specific specification. The following properties are returned by the Infineon OPTIGA™ TPM SLB 9673 using the command TPM2\_GetCapability (capability = TPM\_CAP\_TPM\_PROPERTIES):

**Table 6 Infineon TPM property values**

TPM_PT_MANUFACTURER	"IFX"
TPM_PT_VENDOR_STRING_1	"SLB9"
TPM_PT_VENDOR_STRING_2	"673"
TPM_PT_VENDOR_STRING_3	NULL
TPM_PT_VENDOR_STRING_4	NULL
TPM_PT_FIRMWARE_VERSION_1	Major and minor version (for instance, 0x001A000A indicates V26.10) <sup>1)</sup>
TPM_PT_FIRMWARE_VERSION_2	Build number and Common Criteria certification state (for instance, 0x00413000 or 0x00413002) <sup>1)</sup> Byte 1: reserved for future use (0x00) Byte 2 and 3: Build number (for instance, 0x4130) <sup>1)</sup> Byte 4: Common Criteria certification state/mode: 0x00 = TPM operational mode/TPM is CC certified 0x02 = TPM operational mode/TPM is not certified 0x60 = Manually entered TPM firmware recovery mode (triggered externally for testing purposes) 0x61 = TPM firmware recovery mode (triggered by code integrity failure detection) 0x62 = TPM firmware update mode
TPM_PT_MODES	Bit 0 (FIPS_140_2) = 1 Bits 1..31 = 0

1) The build- and version numbers given here are examples and do not necessarily match the numbers of the device this data sheet has been provided for.

#### 4.1 TPM register polling

Processing of accesses to registers creates a load on the TPM.

If registers are polled in quick succession, the time until the TPM reaches the target state is increased, which decreases performance and may even lead to violation of maximum timeout values.

To prevent this, a minimum delay between register read accesses must be respected when polling:

- Minimum delay between TPM register reads for polling of TPM\_STS\_x during command execution: 1 ms
- Minimum delay between TPM register reads for polling of TPM\_STS\_x after device reset before commandReady set: 1 ms
- Minimum delay between TPM register reads for all other TPM register polling, including TPM\_STS\_x.commandReady set between command, TPM\_STS\_x.valid and TPM\_STS\_x.burstCount: 100 µs

## 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 7 Absolute maximum ratings**

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Supply Voltage	$V_{DD}$	-0.3	–	4.1	V	–
Voltage on any pin	$V_{max}$	-0.5	–	4.1	V	–
Ambient temperature	$T_A$	-40	–	85	°C	Standard temperature SLB 9673XU2.0 devices
Ambient temperature	$T_A$	-40	–	105	°C	Enhanced temperature SLB 9673AU2.0 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 8 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	–	85	°C	Standard temperature SLB 9673XU2.0 devices
Ambient temperature	$T_A$	-40	–	105	°C	Enhanced temperature SLB 9673AU2.0 devices
Useful lifetime		–	–	10	y	
Operating lifetime		–	–	10	y	
Average $T_A$ over lifetime		–	55	–	°C	

## Electrical characteristics

### 5.3 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 9 Current consumption**

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Current Consumption in Active Mode	$I_{VDD\_Active}$			35	mA	
Current Consumption in Sleep Mode	$I_{VDD\_Sleep}$		120		$\mu\text{A}$	Pins GPIO, RST# and I2C_PIRQ# = $V_{DD}$ , no I2C bus activity

*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 interface pins (SCL, SDA, TEST#, RST#, I2C\_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	—
Input voltage low	$V_{IL}$	-0.5		$0.3 V_{DD}$	V	—
Input leakage current	$I_{LEAK}$	-2		2	$\mu\text{A}$	$0\text{ V} < V_{IN} < V_{DD}$
Output high voltage	$V_{OH}$	$0.9 V_{DD}$			V	$I_{OH} = -100\text{ }\mu\text{A}$
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	$C_{LOAD}$			30	pF	

**Table 11 DC characteristics of GPIO 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
Input voltage low	$V_{IL}$	-0.5		$0.3 V_{DD}$	V	Pins GPIO
Input leakage current	$I_{LEAK}$	-2		2	$\mu\text{A}$	$0\text{ V} < V_{IN} < V_{DD}$
Output high voltage	$V_{OH}$	$V_{DD}-0.3$			V	$I_{OH} = -1\text{ mA}$ , pins GPIO
Output low voltage	$V_{OL}$			0.3	V	$I_{OL} = 1\text{ mA}$ , pins GPIO
Pad input capacitance	$C_{IN}$			10	pF	Pins GPIO

## Electrical characteristics

### 5.4 AC characteristics

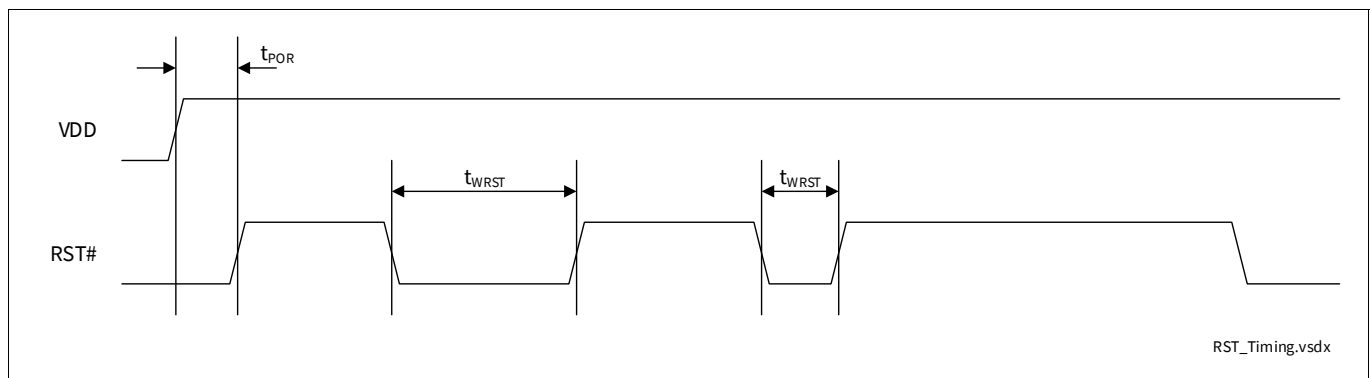
$T_A = 25^\circ\text{C}$ ,  $V_{DD} = 3.3\text{V} \pm 0.3\text{V}$  or  $V_{DD} = 1.8\text{V} \pm 0.15\text{V}$  unless otherwise noted.

**Table 12 Power supply**

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Supply voltage rise time	$t_{VDDR}$			1.0	V/ns	

**Table 13 Device reset**

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Cold (Power-On) Reset	$t_{POR}$	80			$\mu\text{s}$	
Warm Reset	$t_{WRST}$	2			$\mu\text{s}$	



**Figure 3 Reset timing**

#### 5.4.1 I2C Interface Characteristics

The electrical characteristics are compliant to the NXP I<sup>2</sup>C bus specification [1] for “standard-mode” ( $f_{SCL} \leq 100\text{ kHz}$ ), “fast-mode” ( $f_{SCL} \leq 400\text{ kHz}$ ) and “fast-mode plus” ( $f_{SCL} \leq 1000\text{ kHz}$ ), with certain deviations stated in [Table 14](#), [Table 15](#), and [Table 16](#) below.

For printed circuit board design the reduced output fall time  $t_{OF}$  compared to the NXP I<sup>2</sup>C bus specification needs to be considered!

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

**Table 14 I2C Standard Mode Interface Characteristics**

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
SCL clock frequency	$f_{SCL}$	0	—	100	kHz	—
Input voltage low	$V_{IL}$	-0.5	—	$0.3 V_{DD}$	V	—
Input voltage high	$V_{IH}$	$0.7 V_{DD}$	—	$V_{DD} + 0.5$ or $V_{DD,max}$	V	Maximum = $\min(V_{DD} + 0.5, V_{DD,max})$
Output low voltage	$V_{OL}$	—	—	0.4	V	$I_{OL} = 2\text{ mA}$ , $V_{DD} \leq 2\text{ V}$

**Electrical characteristics**

**Table 14 I2C Standard Mode Interface Characteristics** (continued)

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
Output low voltage	$V_{OL}$	—	—	0.4	V	$I_{OL} = 3 \text{ mA}$ , $V_{DD} > 2 \text{ V}$
Low level output current	$I_{OL}$	2	—	—	mA	$V_{OL} = 0.4 \text{ V}$ , $V_{DD} < 2.7 \text{ V}$
Low level output current	$I_{OL}$	3	—	—	mA	$V_{OL} = 0.4 \text{ V}$ , $V_{DD} \geq 2.7 \text{ V}$
Output fall time from $V_{IHmin}$ to $V_{ILmax}$ (at device pin)	$t_{OF}$	—	—	250	ns	$C_b \leq 200 \text{ pF}$ , $V_{DD} < 2.7 \text{ V}$
Output fall time from $V_{IHmin}$ to $V_{ILmax}$ (at device pin)	$t_{OF}$	—	—	250	ns	$C_b \leq 400 \text{ pF}$ , $V_{DD} \geq 2.7 \text{ V}$
Capacitive load for each bus line	$C_b$	—	—	200	pF	$V_{DD} < 2.7 \text{ V}$
Capacitive load for each bus line	$C_b$	—	—	400	pF	$V_{DD} \geq 2.7 \text{ V}$

**Table 15 I2C Fast Mode Interface Characteristics**

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
SCL clock frequency	$f_{SCL}$	0	—	400	kHz	—
Input voltage low	$V_{IL}$	-0.5	—	$0.3 V_{DD}$	V	—
Input voltage high	$V_{IH}$	$0.7 V_{DD}$	—	$V_{DD} + 0.5$ or $V_{DD,max}$	V	Maximum = $\min(V_{DD} + 0.5, V_{DD,max})$
Output low voltage	$V_{OL}$	—	—	0.4	V	$I_{OL} = 2 \text{ mA}$ , $V_{DD} \leq 2 \text{ V}$
Output low voltage	$V_{OL}$	—	—	0.4	V	$I_{OL} = 3 \text{ mA}$ , $V_{DD} > 2 \text{ V}$
Low level output current	$I_{OL}$	2	—	—	mA	$V_{OL} = 0.4 \text{ V}$ , $V_{DD} < 2.7 \text{ V}$
Low level output current	$I_{OL}$	3	—	—	mA	$V_{OL} = 0.4 \text{ V}$ , $V_{DD} \geq 2.7 \text{ V}$
Output fall time from $V_{IHmin}$ to $V_{ILmax}$ (at device pin)	$t_{OF}$	$20 \cdot V_{DD} / 5.5 \text{ V}$	—	250	ns	$C_{b,min} < C_b \leq 200 \text{ pF}$ , $V_{DD} < 2.7 \text{ V}$
Output fall time from $V_{IHmin}$ to $V_{ILmax}$ (at device pin)	$t_{OF}$	$20 \cdot V_{DD} / 5.5 \text{ V}$	—	250	ns	$C_{b,min} < C_b \leq 400 \text{ pF}$ , $V_{DD} \geq 2.7 \text{ V}$
Capacitive load for each bus line	$C_b$	15	—	200	pF	$V_{DD} < 2.7 \text{ V}$
Capacitive load for each bus line	$C_b$	15	—	400	pF	$V_{DD} \geq 2.7 \text{ V}$

**Electrical characteristics**

**Table 16 I2C Fast Mode plus Interface Characteristics**

Parameter	Symbol	Values			Unit	Note or Test Condition
		Min.	Typ.	Max.		
SCL clock frequency	$f_{SCL}$	0	—	1000	kHz	—
Input voltage low	$V_{IL}$	-0.5	—	$0.3 V_{DD}$	V	—
Input voltage high	$V_{IH}$	$0.7 V_{DD}$	—	$V_{DD}+0.5$ or $V_{DD,max}$	V	Maximum = $\min(V_{DD}+0.5, V_{DD,max})$
Output low voltage	$V_{OL}$	—	—	0.4	V	$I_{OL} = 2 \text{ mA}, V_{DD} \leq 2 \text{ V}$
Output low voltage	$V_{OL}$	—	—	0.4	V	$I_{OL} = 3 \text{ mA}, V_{DD} > 2 \text{ V}$
Low level output current	$I_{OL}$	2	—	—	mA	$V_{OL} = 0.4 \text{ V}, V_{DD} < 2.7 \text{ V}$
Low level output current	$I_{OL}$	3	—	—	mA	$V_{OL} = 0.4 \text{ V}, V_{DD} \geq 2.7 \text{ V}$
Output fall time from $V_{IHmin}$ to $V_{ILmax}$ (at device pin)	$t_{OF}$	$20 \cdot V_{DD} / 5.5 \text{ V}$	—	120	ns	$C_{b,min} < C_b \leq 150 \text{ pF}$
Capacitive load for each bus line	$C_b$	15	—	150	pF	

## 5.5 Timing

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

The OPTIGA™ TPM SLB 9673 features security mechanisms which detect and count all resets.

## Package dimensions (UQFN)

### 6 Package dimensions (UQFN)

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

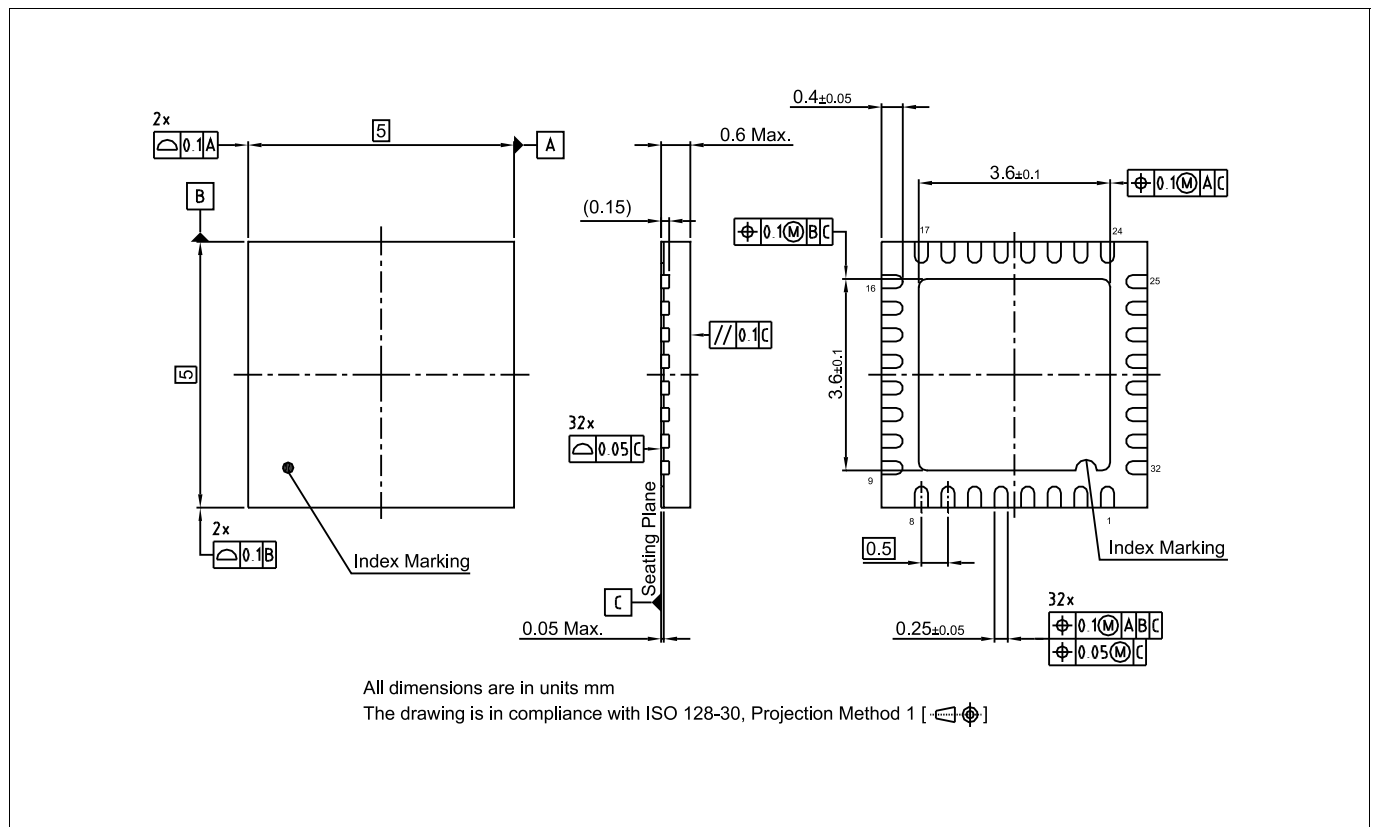


Figure 4 Package dimensions PG-UQFN-32-1,-2

#### 6.1 Packing type

PG-UQFN-32-1,-2: Tape & Reel (reel diameter 330mm), 5000 pcs. per reel

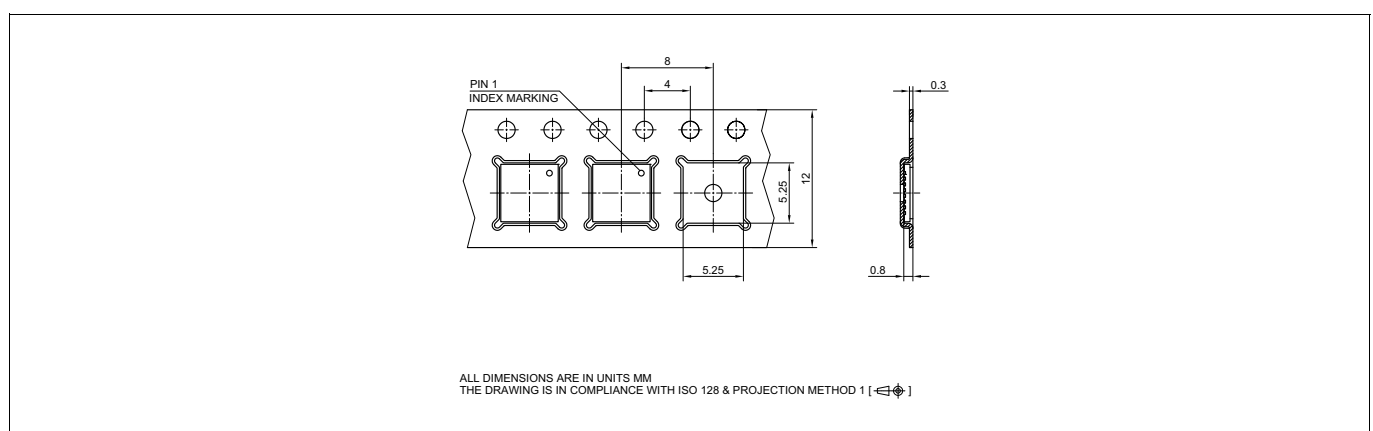


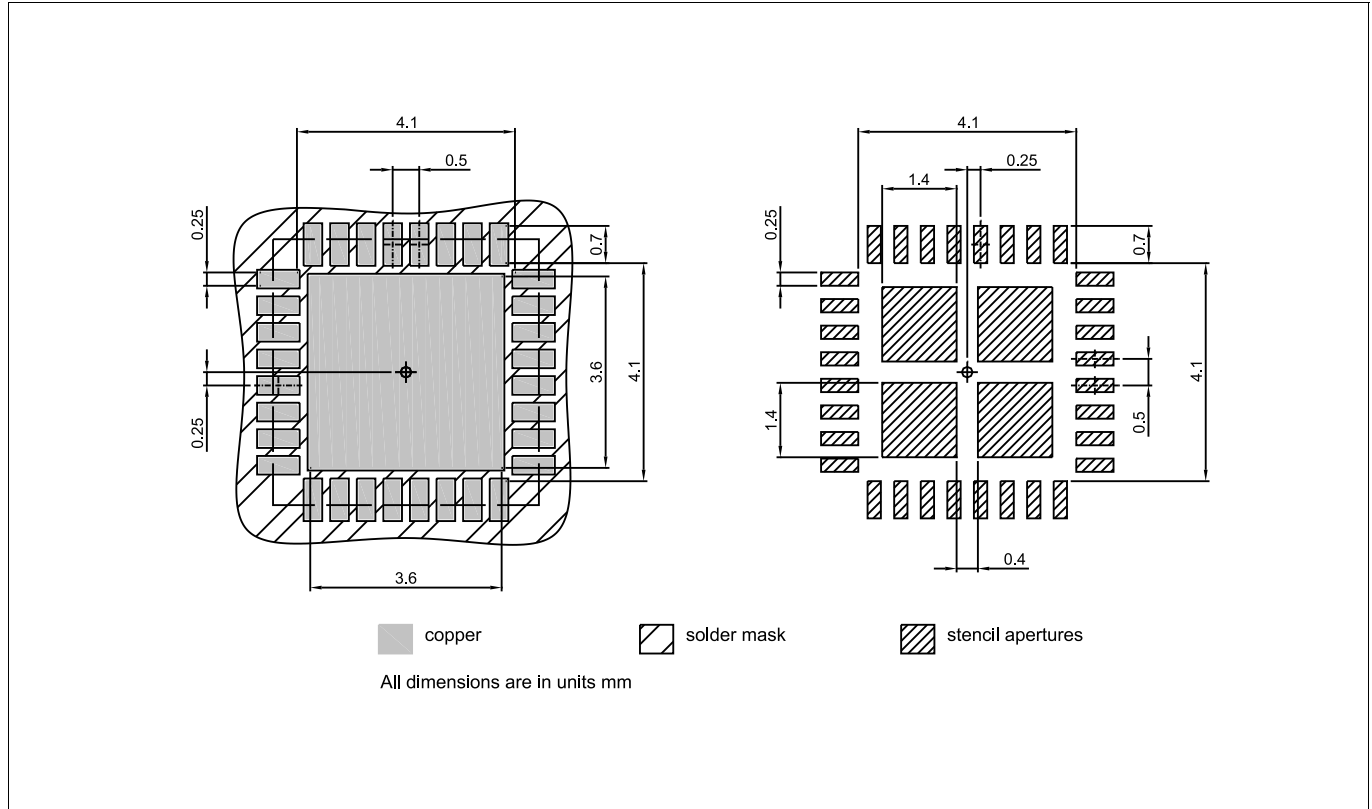
Figure 5 Tape & reel dimensions PG-UQFN-32-1,-2



## Package dimensions (UQFN)

### 6.2 Recommended footprint

**Figure 6** shows the recommended footprint for the package. The exposed pad of the package is internally connected to GND. It shall be connected to GND externally as well.



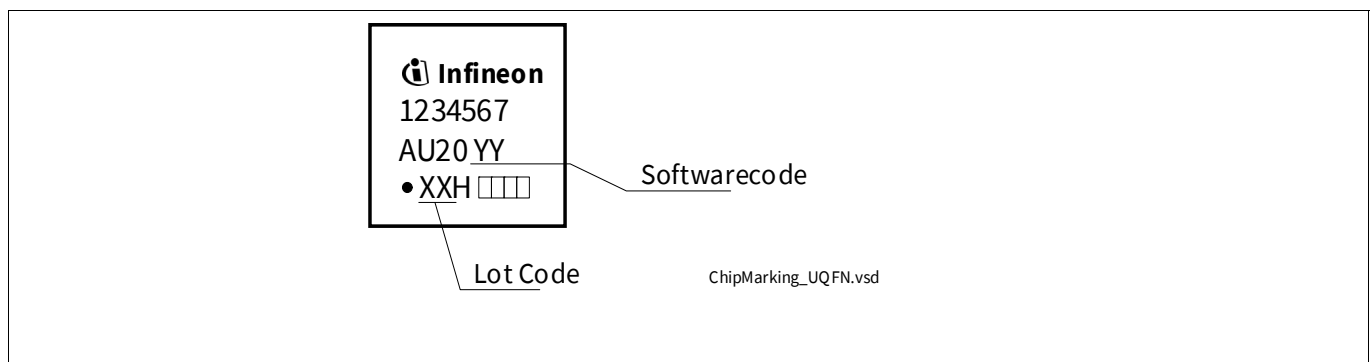
**Figure 6** Recommended footprint PG-UQFN-32-1,-2

### 6.3 Chip marking

Line 1: SLB9673

Line 2: XU20 yy or AU20 yy (see **Table 1**), the <yy> is an internal FW indication (only at manufacturing due to field upgrade option)

Line 3: <Lot number> H <datecode>



**Figure 7** Chip marking

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] —, “Trusted Platform Module Library (Part 1-4)”, Family 2.0, Level 00, Rev. 01.59, November 8, 2019, TCG
- [2] —, “TCG PC Client Platform TPM Profile (PTP) Specification”, Family 2.0, Level 00, Rev. 01.05 v14, September 4, 2020, TCG
- [3] —, “Errata For TCG Trusted Platform Library, Family 2.0, Level 00, Rev. 01.59, November 8, 2019”, Errata Version 1.1, June 18, 2020, TCG
- [4] —, “Errata for PC Client Platform TPM Profile for TPM 2.0 Version 1.05 Revision 14”, Errata Version 1.0, September 04, 2020, TCG
- [5] —, “Registry of reserved TPM 2.0 handles and localities”, Version 1.1, Rev. 1.00, February 6, 2019, TCG
- [6] —, “TCG EK Credential Profile”, Version 2.3, Rev. 2, July 23, 2020, TCG
- [7] —, "NIST Special Publication 800-193, Platform Firmware Resiliency Guidelines", May, 2018, NIST

## Terminology

## Terminology

ESW	Embedded Software
HMAC	Hashed Message Authentication Code
I2C	Inter Integrated Circuit (bus)
ICT	Information and Communications Technology
IoT	Internet of Things
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](mailto: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**

Page or item	Subjects (major changes since previous revision)
<b>Revision 1.1, 2022-07-08</b>	
	Added <a href="#">Section 4.1</a>
<b>Revision 1.0, 2022-05-25</b>	
	Initial version

#### Trademarks

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

**Edition 2022-07-08**

**Published by**

**Infineon Technologies AG**

**81726 Munich, Germany**

**© 2022 Infineon Technologies AG.**

**All Rights Reserved.**

**Do you have a question about any aspect of this document?**

**Email:**

**[csscustomerservice@infineon.com](mailto:csscustomerservice@infineon.com)**

#### IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenhheitsgarantie").

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](http://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.