Xenon - SPI TPM

Evaluation Board for OPTIGA™ Trusted Platform Module

Devices

- TPM 70 1.2 XENONBOARD
- TPM 70 2.0 XENONBOARD

Board Rev. V4.0.2

About this document

Scope and purpose

This document describes the evaluation board for the Infineon OPTIGA™ TPM SLB 9670VQ1.2 and OPTIGA™ TPM SLB 9670VQ2.0.

The Xenon –SPI TPM board can be used to evaluate the functionality of OPTIGA™ SLB 9670 Trusted Platform Module (TPM) in a target system environment.

The purpose of this document is also to help customers to use and integrate the OPTIGA™ TPM into their system solutions.

Intended audience

This document has been written for system design and verification engineers, who use the OPTIGA™ SLB 9670VQ1.2 or OPTIGA™ SLB 9670VQ2.0 TPM evaluation board as a verification platform or reference design.

Please read the Important Notice and Warnings at the end of this document

Table of contents

List of figures

List of tables

1 Overview

1.1 Hardware

The Trusted Platform Module (TPM) OPTIGA™ TPM SLB 9670VQ1.2 or OPTIGA™ TPM SLB 9670VQ2.0 in PG-VQFN-32-13 package is the main part of the Xenon - SPI TPM evaluation board with revision V4.0.2.

The pinning of the OPTIGA™ TPM SLB 9670VQ1.2 or OPTIGA™ TPM SLB 9670VQ2.0 TPM is compliant to the TCG [5], [6], [7], [8], [9].

1.2 Features

- Infineon's OPTIGA™ TPM SLB 9670VQ1.2 or OPTIGA™ TPM SLB 9670VQ2.0 Trusted Platform Module (TPM)
- PG-VQFN-32-13 package
- 1.8V or 3.3V power supply
- Serial Peripheral Interface (SPI) accessible via 2x10 pin header connector
- GPIO and PP signal routed to pin for optional use
- Small form factor PCB, 4 layer technology

2 Xenon - SPI TPM Hardware Components

The main component on the Xenon – SPI TPM evaluation board is the OPTIGA™ SLB 9670VQ1.2 or OPTIGA™ SLB 9670VQ2.0.

2.1 TPM Interfaces

2.1.1 Serial Peripheral Interface - SPI

This OPTIGA™ TPM supports communication over an SPI interface.

For further details refer also to OPTIGA™ TPM Data Sheet [1], [2], [3].

2.2 Electrical Characteristics

For electrical characteristics of the OPTIGA™ TPM, please refer to the OPTIGA™ TPM Data Sheet [1], [2], [3].

2.3 Pin Configuration of OPTIGA™ TPM

Figure 1 shows the pin configuration of OPTIGA™ TPM SLB 9670VQ1.2 in PG-VQFN-32-13 package, which is the same also for OPTIGA™ TPM SLB 9670VQ2.0. Please note, that the OPTIGA™ TPM SLB 9670VQ2.0 does not use PP functionality.

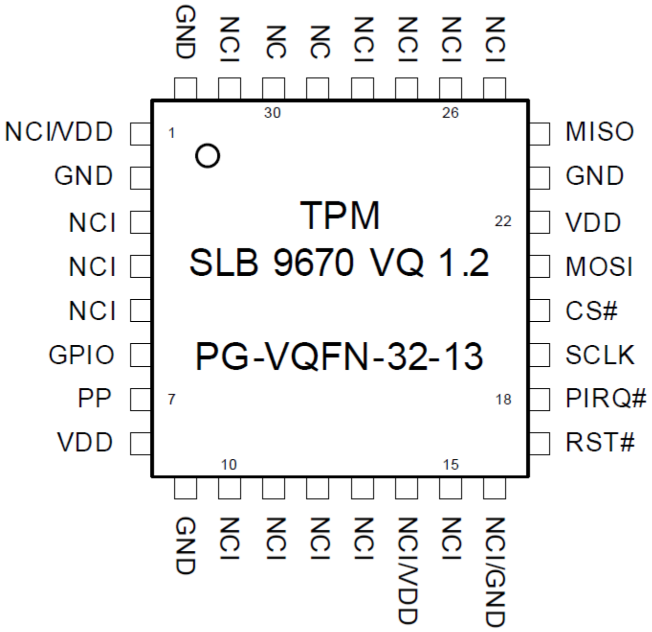


Figure 1 Pin Configuration of OPTIGA™ TPM SLB 9670VQ1.2 in PG-VQFN-32-13 Package (Top View).

2.4 Package

Package: PG-VQFN-32-13

For details on the package outline and the footprint, please refer to the OPTIGA™ TPM Data Sheet [1], [2], [3].

3 Xenon - SPI TPM Board Signals

3.1 Power - VDD

VDD are external power supplies provided on the main board SPI connector. VDD = 3.3 or 1.8V

3.2 CS# - SPI chip select

Signal to select device on the multi slave SPI bus.

For further details see also OPTIGA™ TPM Data Sheet [1], [2], [3] and TCG specification [5], [6], [7], [8], [9].

3.3 RST# - TPM reset

This is an external reset signal. Asserting this pin unconditionally resets the OPTIGA™ TPM. The signal is active-low and is usually connected to the system reset of the host.

3.4 MOSI

SPI TPM input signal for data transfers from the SPI master to the SPI slave.

3.5 MISO

SPI TPM output signal for data transfer from SPI slave to SPI master.

3.6 SCLK

Input of SPI clock provided by SPI master. PCB designed to support up to 43MHz SPI clk.

3.7 PIRQ#

Output signal for signaling TPM interrupt to the host.

3.8 GPIO

The general purpose IO (GPIO) signal of the evaluation board is connected to the GPIO pin of the OPTIGA™ TPM.

Note: *This pin may be left unconnected; it has an internal pull-up resistor. See board pin J2.*

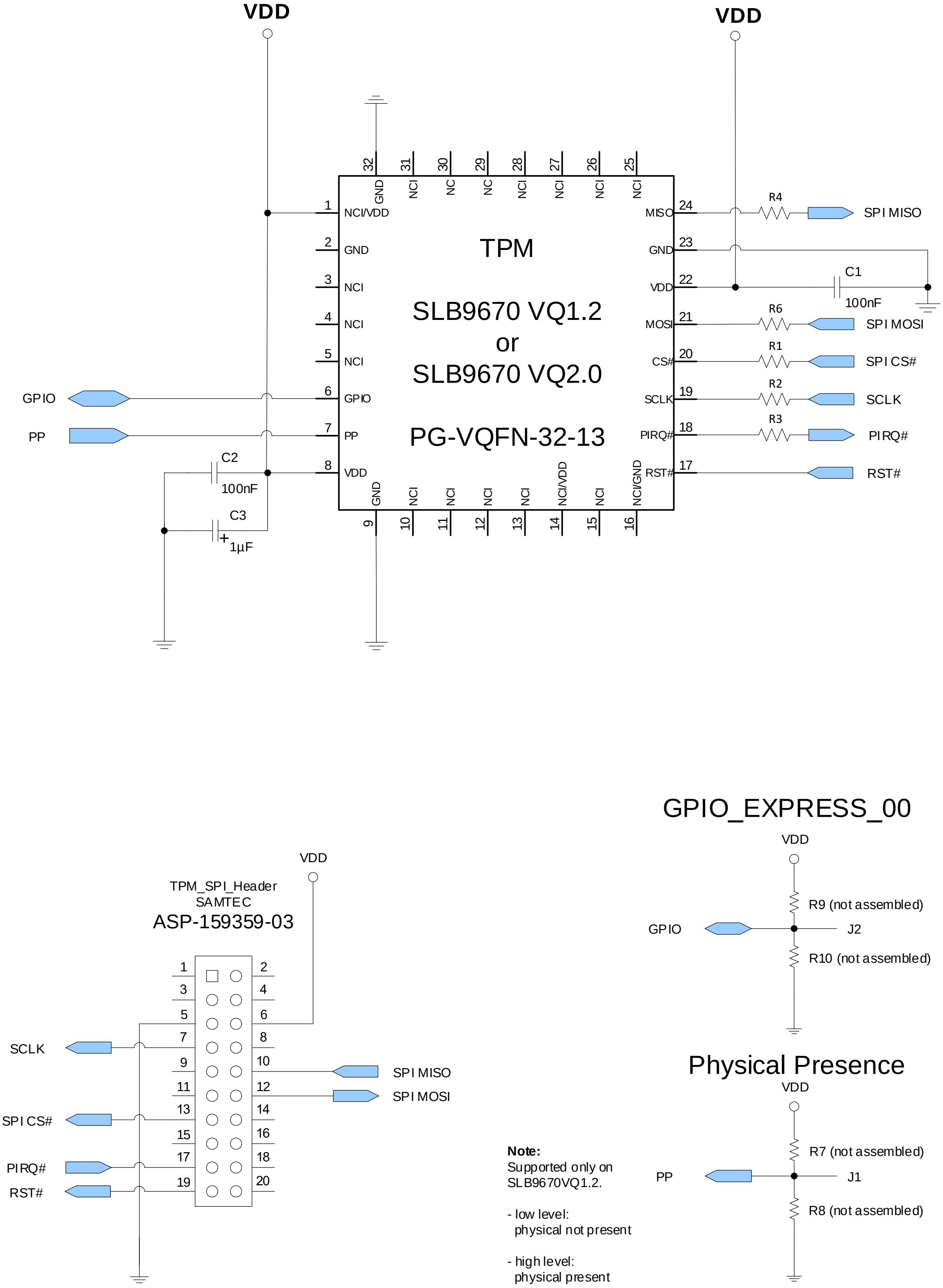
3.9 PP (TPM1.2 only)

The firmware implements commands defined by the Trusted Computing Group (TCG) which require physical presence at the platform. Physical presence can be proven either by the use of software commands or by the use of a defined level on physical presence signal pin. 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 [5], [6], [7], [8], [9]).

Note: *This pin may be left unconnected; it has an internal pulldown resistor. See board pin J1.*

4 Schematics

4.1 Xenon – SPI TPM Connection Diagram



Note:
Supported only on SLB9670VQ1.2.

- low level:
  physical not present

- high level:
  physical present

Figure 2 **Xenon – SPI TPM board Connection Diagram.**

4.2 Xenon – SPI TPM Board Layout

- 4 Layers PCB design
- SMD and THT technologies

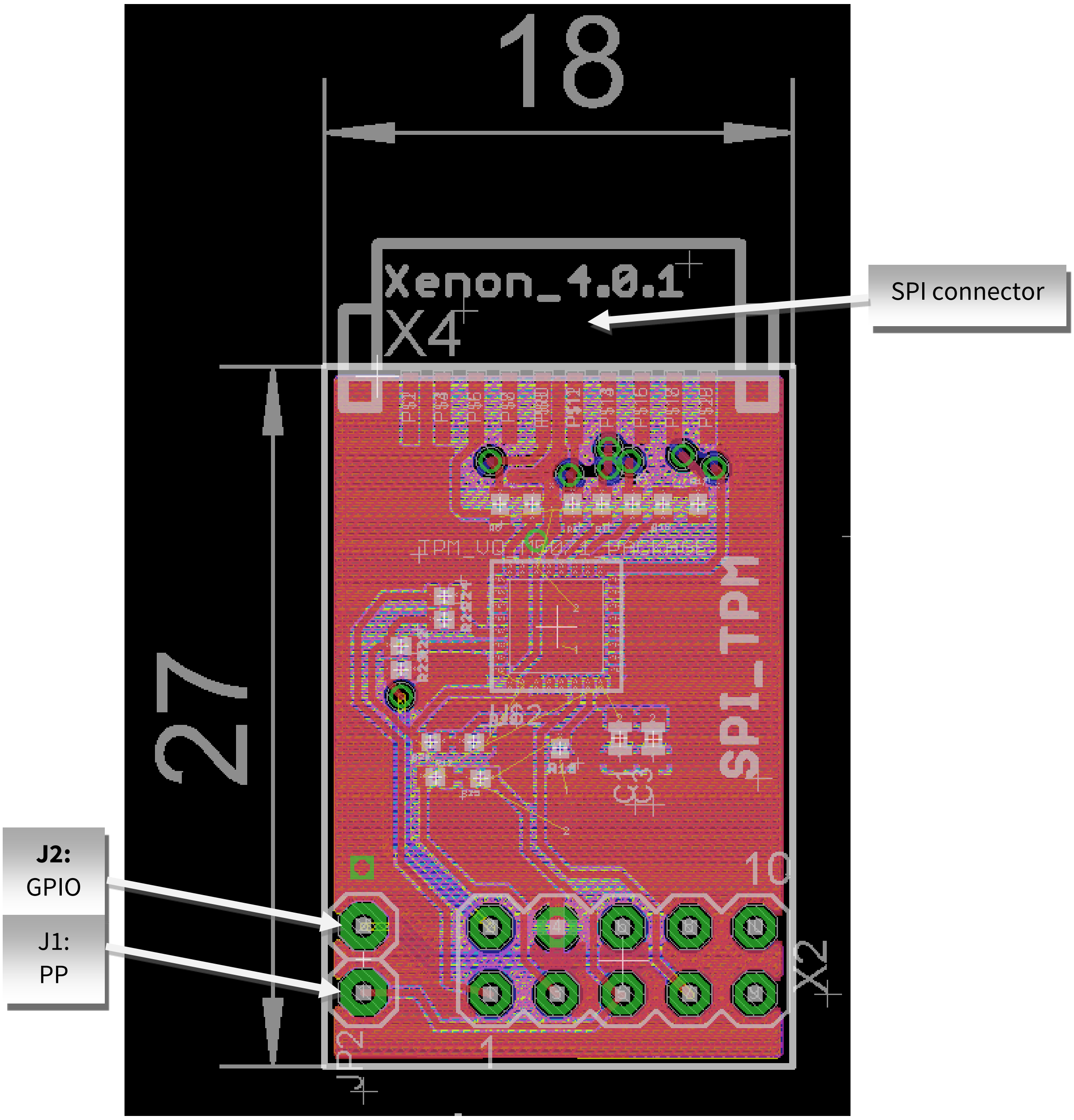


Figure 3 Top view of Xenon - SPI TPM board PCB for SPI TPM

5 Xenon – SPI TPM Board Details

5.1 Xenon – SPI TPM Board Dimensions

- ~ 27 x 18 mm (including SPI connector)
- Thickness: ~ 3 mm
- SPI accessible via 2x10 pin header (50mil / 1.27mm pin spacing)

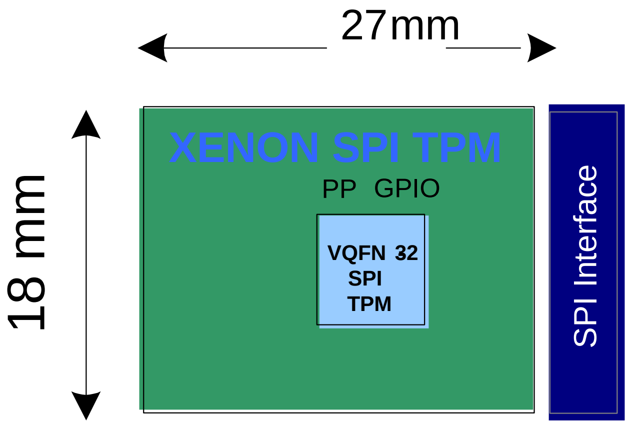
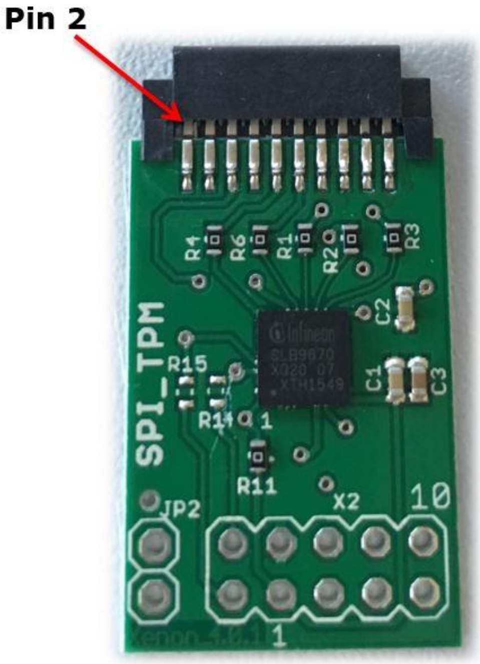


Figure 4 Xenon – SPI TPM board (V4.0.2)

5.2 Xenon – SPI TPM – Pin Configuration



Signal	Pin	Pin	Signal
Key	1	2	-
-	3	4	-
GND	5	6	VDD
SCLK	7	8	-
-	9	10	MISO
-	11	12	MOSI
TPM_CS	13	14	GND[1]
-	15	16	-
PIRQ	17	18	-
PLT_RST	19	20	-

[1] Note: Pin 14 - GND of the connector is not connected to GND on the Xenon SPI TPM Board

Figure 5 Xenon – SPI TPM board - Pin Configuration

6 Xenon – SPI TPM Board Connectors

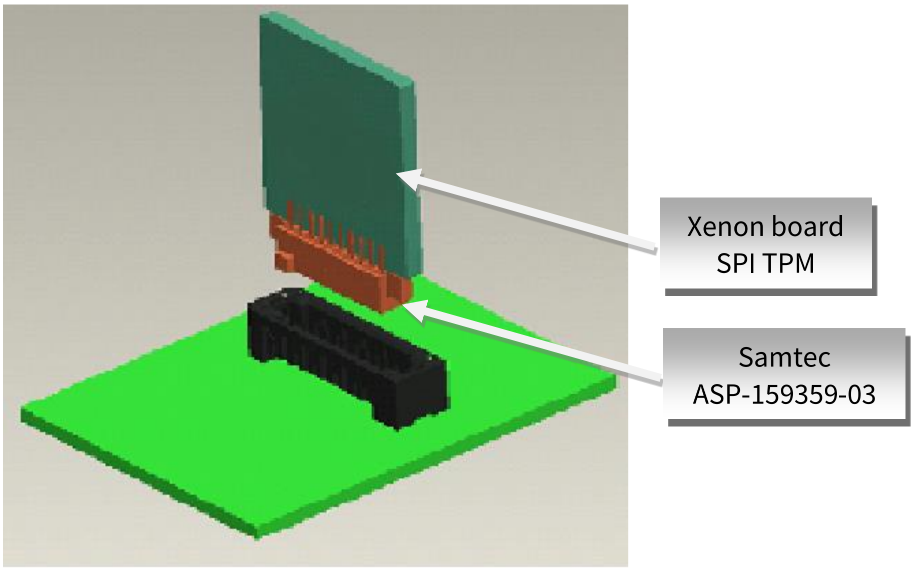


Figure 6 Board connection Xenon –SPI TPM board with motherboard

The Xenon – SPI TPM board with the Samtec ASP-159359-03 connector can be plugged to a Samtec ASP-159358-01 (Through Hole Technology) or to a Samtec ASP-159358-03 (Surface Mount Technology)

Samtec ASP-159359-03
(edge/straddle mount)

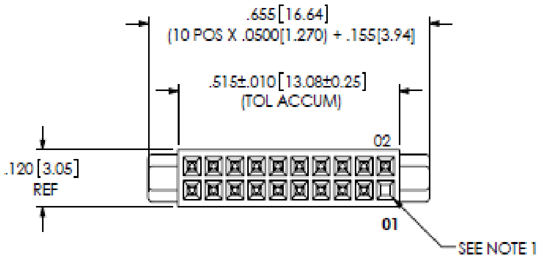


Figure 7 SPI TPM connector on Xenon – SPI TPM board – Samtec ASP-159359-03

PIN	Name	PIN	Name
1	Key	2	NC
3	NC	4	NC
5	**GND**	6	**VCC 3.3 V (or 1.8V) –** TPM power supply
7	**SCLK –** TPM SPI clock	8	NC
9	NC	10	**MISO**
11	NC	12	**MOSI**
13	**TPM CS2# -** TPM SPI chip select signal	14	**GND** - on Xenon SPI TPM board not connected to GND
15	NC	16	NC
17	**PIRQ# -** TPM interrupt signal, active low	18	NC
19	**PLT_RST# -** TPM reset signal, active low	20	NC

Table 1 Xenon - SPI TPM connector – Pin layout

7 Xenon – SPI TPM Board Optional Features

7.1 Physical Presence pin – optional and TPM1.2 only

The purpose of this pin is to stimulate the physical presence indication signal PP. Please refer also to the TCG specification [6], [8].

J1 pin conditions:

• J1 floating:	PP not asserted, (internal Pulldown resistor)
• J1 connected to VDD:	PP asserted
• J1 connected to GND:	PP not asserted

Additional: The board has foot prints to solder pull up (R7) or pull down (R8) resistors – see also Figure 2.

Default: Resistors R7 and R8 are not assembled.

7.2 GPIO pin – optional

The purpose of this pin is to emulate the GPIO-Express-00 Signal - see TCG specification [6], [8].

The pin is a Tri-State I/O GPIO.

J2 pin conditions:

• J2 floating:	GPIO input high level,
• J2 signal level:	GPIO input / output level.

Additional: The board has foot prints to solder pull up (R9) or pull down (R10) resistors – see also Figure 2.

Default: Resistors R9 and R10 are not assembled.

8 Board Ordering

Sales Code / Ordering Code:

Sales Code	Ordering Code
TPM 70 1.2 XENONBOARD	SP001299760
TPM 70 2.0 XENONBOARD	SP001299764

Table 2 Xenon – SPI TPM board ordering information

8.1 BOM – Bill of Material

List of materials used for assembling the Xenon – SPI TPM board V4.0.2

Part ID	Value	Footprint	Description	Supplier
PCB	-	-	Xenon - SPI TPM V4.0.2 PCB	IFX
IC1	OPTIGA™ TPM SLB 9670VQ1.2 or OPTIGA™ TPM SLB 9670VQ2.0	VQFN-32	TPM controller	IFX
C1, C2	100nF	C_0603	Ceramic capacitor	-
C3	1µF	C_0603	Ceramic capacitor	-
R1-4, R6	0 Ohm	SMD 0402	SPI termination resistor	-
R7, R8, R9, R10	-	SMD 0402	Optional, see 7.1, 7.2	-
R11	0 Ohm	SMD 0402	For internal test purposes only – not necessary for standard operation	-
X4	-	-	Samtec ASP-159359-03 pin header (female)	Samtec

Table 3 Bill of Material for Xenon – SPI TPM board

References

[1] http://www.infineon.com/tpm

[2] Data Sheet of Trusted Platform Module SLB 9670 TPM1.2 TCG, Rev 1.3, 2018-09-21

[3] Data Sheet of Trusted Platform Module SLB 9670VQ2.0 TCG, Rev 1.4, 2018-12-07

[4] https://www.trustedcomputinggroup.org

[5] "TCG PC Client TPM Interface Specification (TIS)", Version 1.3, 2013-03-21, TCG

[6] "TPM Main Specification", Version 1.2, Rev. 116, 2011-03-01, TCG (parts 1-3), TCG

[7] "TCG PC Client Platform TPM Profile (PTP) Specification", Rev. 00.43, 2014-08-04, TCG

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

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

Revision history

Reference	Description
Revision 1.1, 2020-04-06	
all	First released version
Revision 1.0	
all	Initial version – not released – Xenon - SPI TPM board

Trademarks

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

Edition 2020-05-06

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email: **dsscustomerservice@infineon.com**

IMPORTANT NOTICE

The information contained in this application note is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this application note must verify any function and other technical information given herein in the real application. 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) with respect to any and all information given in this application note.

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 the product, technology delivery terms and conditions and prices please contact your 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.