Xenon - SPI TPM

Evaluation Board for OPTIGA™ Trusted Platform Module

Devices

- TPM 72 FW15.21 XENON

Board Rev. V4.1.0

About this document

Scope and purpose

This document describes the evaluation board for the Infineon OPTIGA^{TM} TPM SLB 9672VU2.0 FW15.xx.

The Xenon –SPI TPM board can be used to evaluate the functionality of OPTIGA^{TM} SLB 9672 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^{TM} TPM into their system solutions.

Intended audience

This document has been written for system design and verification engineers, who use the

OPTIGA™ SLB 9672VU2.0 FW15.xx TPM evaluation board as a verification platform or reference design.

Table of contents

List of figures

List of tables

1 Overview

1.1 Hardware

The Trusted Platform Module (TPM) OPTIGA^{TM} TPM SLB 9672VU2.0 FW15.xx in PG-UQFN-32-1,-2 package is the main part of the Xenon - SPI TPM evaluation board with revision V4.1.0

The pinning of the OPTIGA^{TM} TPM SLB 9672VU2.0 FW15.xx is compliant to the TCG [5].

1.2 Features

- Infineon's OPTIGA^{TM} TPM SLB 9672VU2.0 FW15.xx Trusted Platform Module (TPM),
- PG-UQFN-32-1,-2 package,
- 1.8V or 3.3V power supply,
- Serial Peripheral Interface (SPI) accessible via 2x10 pin header connector,
- 3 GPIO signals routed to pin header 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 9672VU2.0 FW15.xx.

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 [2].

2.2 Electrical Characteristics

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

2.3 Pin Configuration of OPTIGA™ TPM

Figure 1 shows the pin configuration of OPTIGA™ TPM SLB 9672VU2.0 FW15.xx in PG-UQFN-32-1,-2 package.

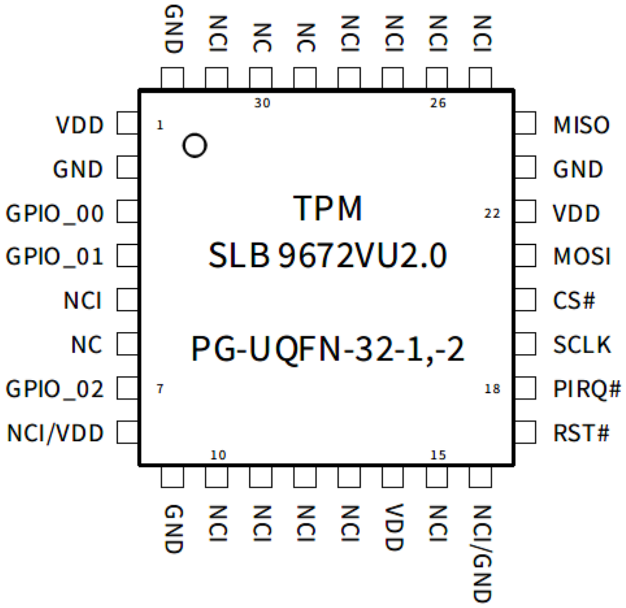


Figure 1 Pin Configuration of OPTIGA™ TPM SLB 9672VU2.0 FW15.xx in PG-UQFN-32-1,-2 Package (Top View).

2.4 Package

Package: PG-UQFN-32-1,-2

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

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 [2] and TCG specification [5].

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 34.65 MHz SPI clk.

3.7 PIRQ#

Output signal for signaling TPM interrupt to the host.

3.8 GPIO

The general purpose IO signals (3 GPIO pins) of the evaluation board are connected to the GPIO pins of the OPTIGA™ TPM SLB 9672

Note: These pins may be left unconnected; they have internal pull-up resistors. See board X1 pin header.

4 Schematics

4.1 Xenon – SPI TPM Connection Diagram

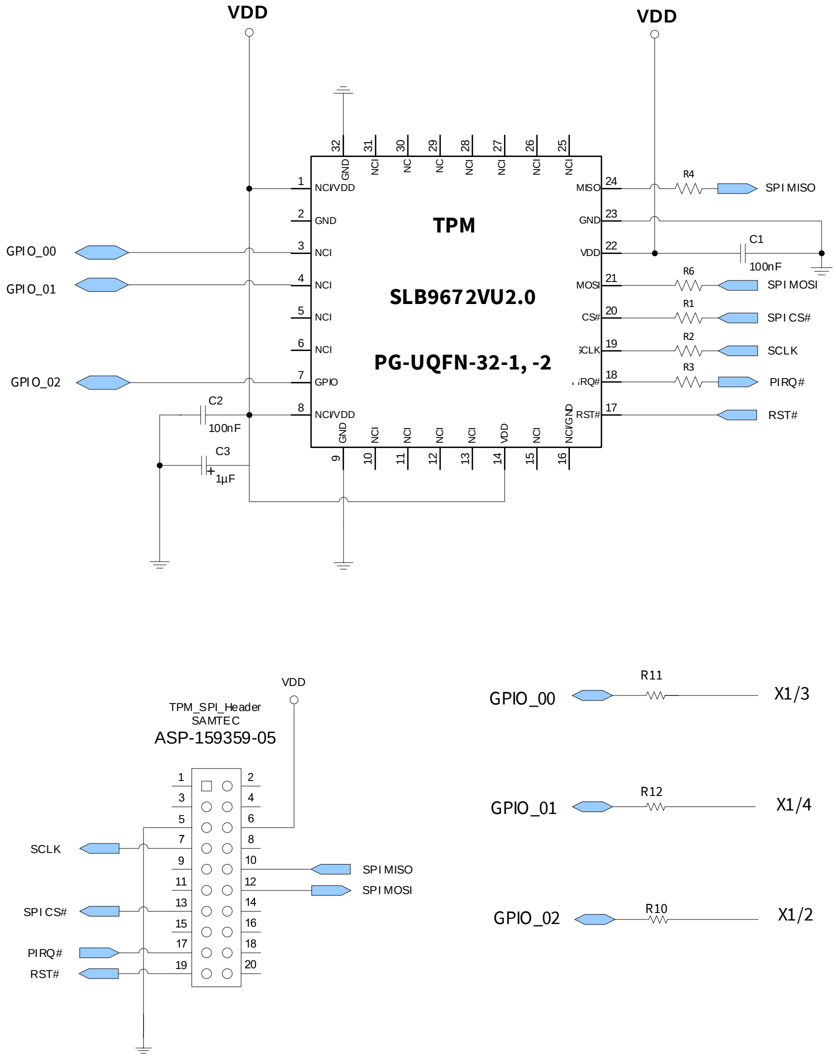


Figure 2 Xenon – SPI TPM board connection diagram.

4.2 Xenon – SPI TPM Board Layout

- 4 Layers PCB design
- SMD and THT technologies

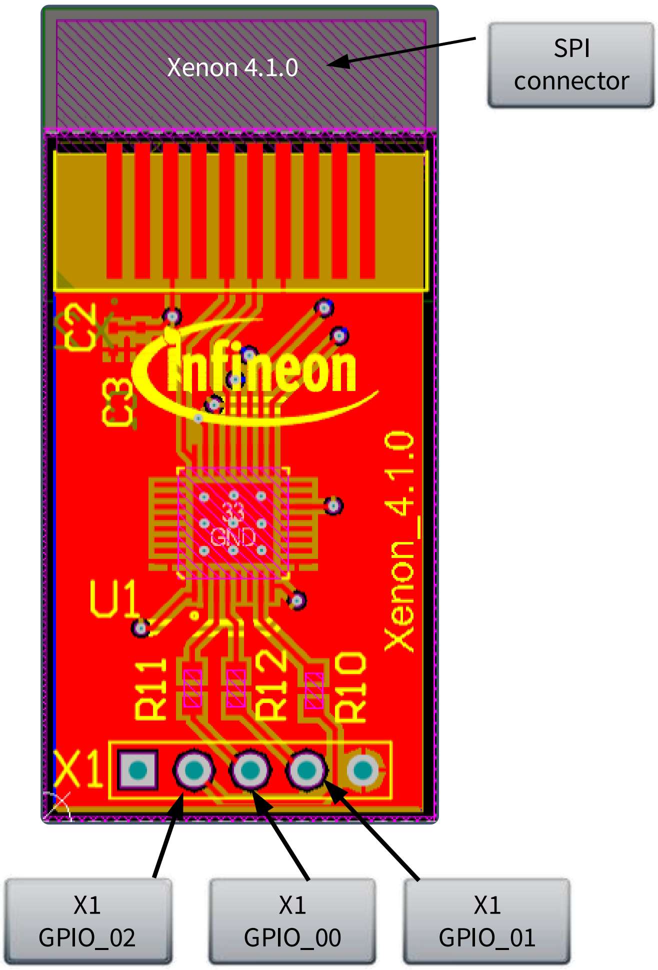


Figure 3 Top view of Xenon - SPI TPM board PCB for SPI TPM

5 Xenon – SPI TPM Board Details

5.1 Xenon – SPI TPM Board Dimensions

- ~ 33 x 18 mm (including SPI connector)
- Thickness: ~ 3 mm
- SPI accessible via 2x10 pin header (50mil / 1.27mm pin spacing)

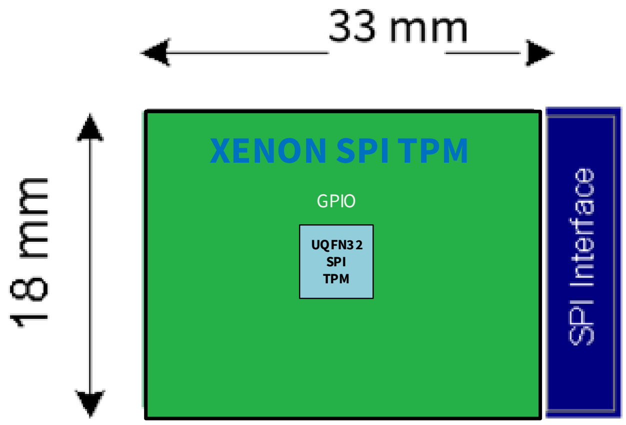
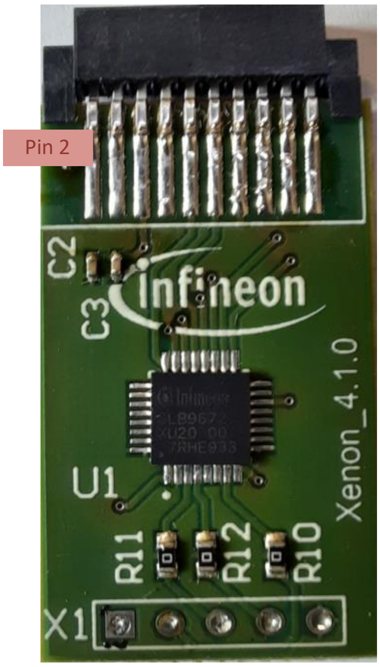
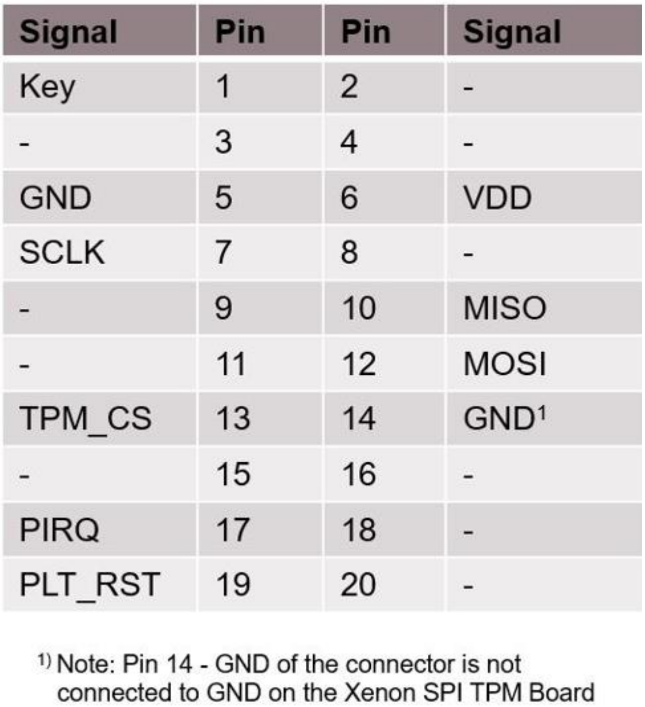


Figure 4 Xenon – SPI TPM board (V4.1.0)

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

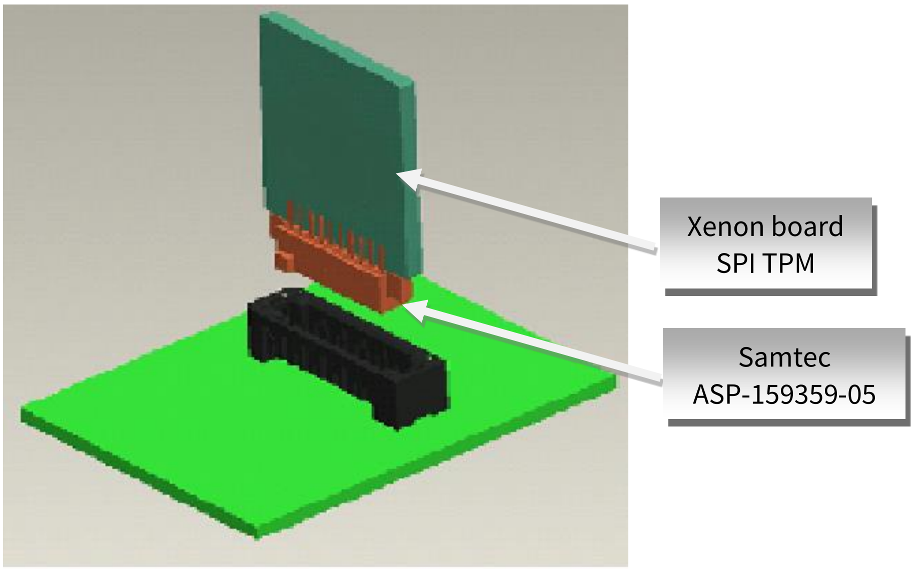


Figure 6 Board connection Xenon –SPI TPM board with motherboard

The Xenon – SPI TPM board with the Samtec ASP-159359-05 connector can be plugged to a Samtec ASP-159358-01 (Through Hole Technology) or to a Samtec ASP-159358-03 (Surface Mount Technology)

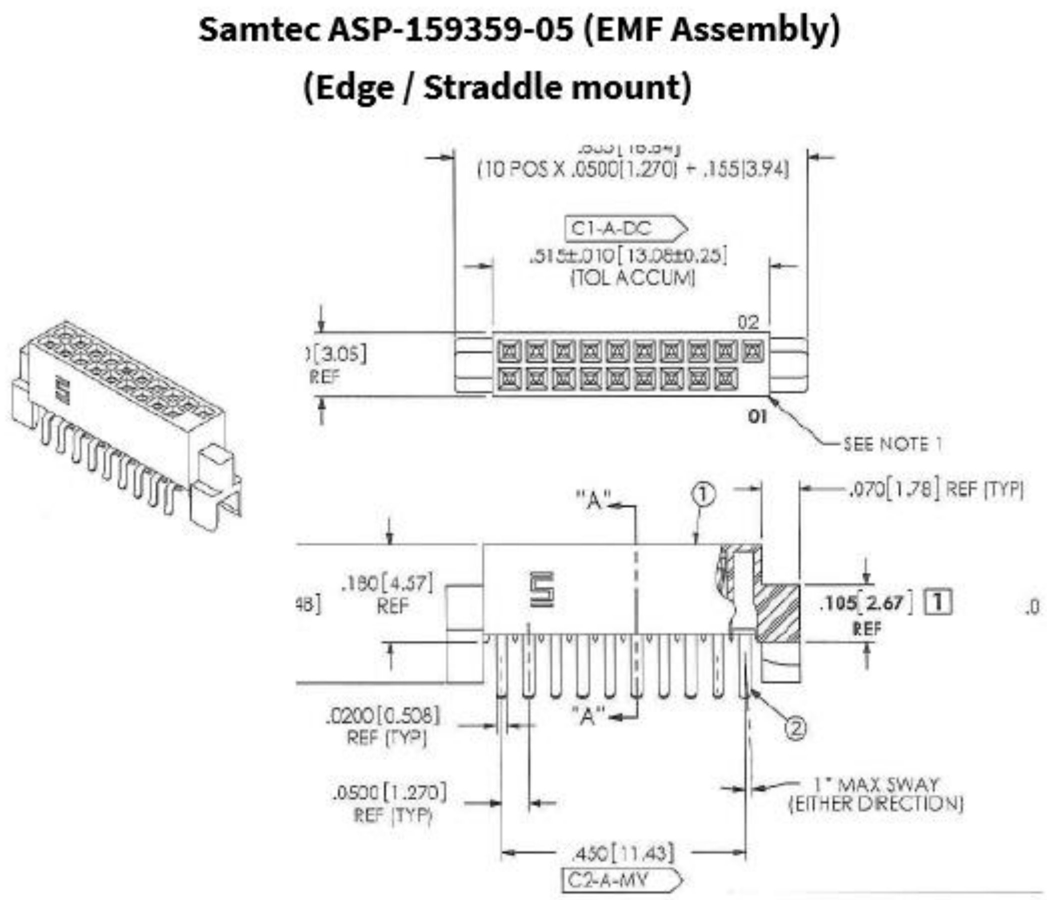


Figure 7 SPI TPM connector on Xenon – SPI TPM board – Samtec ASP-159359-05

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 GPIO pins – optional

The purpose of these pins is to emulate GPIO signals - see TCG specification [5].

These pins may be left unconnected, they have internal pull-up resistors.

X1 pin 2, 3, 4 conditions:

• X1 floating:	GPIO input, high level,
• X1 signal level:	GPIO input / output level.

Additional: The board has resistors to establish the connection to GPIO pins (R10, R11, R12) – see also Figure 2.

8 Board Ordering

Sales Code / Ordering Code:

Sales Code	Ordering Code	OPN
TPM 72 FW15.21 XENON	SP005679617	TPM72FW1521XENONTOBO1

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 V4.1.0

Part ID	Value	Footprint	Description	Supplier
PCB	-	-	Xenon - SPI TPM V4.1.0 PCB	IFX
IC1 (U1)	OPTIGA™ TPM SLB 9672VU2.0 FW15.xx	PG-UQFN-32-1,-2	TPM controller	IFX
C2, C3	100nF	C_0402	Ceramic capacitor	-
C3	1µF	C_0805	Ceramic capacitor	-
R10, R11, R12	0 Ohm	SMD 0402	Optional, see 4.1	-
X2	-	-	Samtec ASP-159359-05 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 OPTIGA™ TPM SLB 9672 TPM2.0, for Devices FW15.xx, Rev 1.1, 2022-01-20

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

[4] “Trusted Platform Module Library (Part 1-4)”, Family 2.0, Level 00, Rev. 01.59, November 8, 2019, TCG

[5] “TCG PC Client Platform TPM Profile (PTP) Specification”, Family 2.0, Level 00, Rev. 01.05 v14, September 4, 2020, TCG

Revision history

Reference	Description
Revision 1.2, 2022-02-07	
all	Initial public version
Revision 1.1, 2021-11-03	
Table 2	Update to FW15.21
Revision 1.0, 2021-02-24	
all	First released version

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

Edition 2022-02-07

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email: cssscustomerservice@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 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.