Iridium - SPI TPM

Evaluation Board for OPTIGA™ Trusted Platform Module

Devices

- IRIDIUM9670 TPM1.2 LINUX
- IRIDIUM9670 TPM2.0 LINUX
- IRIDIUM SLI 9670 TPM2.0
- IRIDIUM SLM 9670 TPM2.0

Board Rev. 1.0

About this document

Scope and purpose

This document describes the evaluation board for the Infineon OPTIGA™ TPM devices OPTIGA™ SLB 9670 TPM1.2 and OPTIGA™ SLx 9670 TPM2.0

Note: *OPTIGA™ TPM SLx 9670 TPM2.0 refers to OPTIGA™ TPM SLB 9670VQ2.0, OPTIGA™ TPM SLI 9670AQ2.0, or OPTIGA™ TPM SLM 9670AQ2.0.*

The Iridium – SPI TPM board can be used to evaluate the functionality of the OPTIGA™ TPM SLB 9670 TPM1.2 and OPTIGA™ TPM SLx 9670 TPM2.0 Trusted Platform Module (TPM) in a target system environment.

The Iridium - SPI TPM evaluation board is dedicated for use on a Raspberry Pi® Board. It contains a 26-pin Raspberry Pi® 1 header, compatible with Raspberry Pi® 40-pin header.

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™ TPM SLB 9670 TPM1.2 or OPTIGA™ TPM SLx 9670 TPM2.0 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™ TPM SLB 9670 TPM1.2 or OPTIGA™ TPM SLx 9670 TPM2.0 in PG-VQFN-32-13 package is the main part of the Iridium - SPI TPM evaluation board with Board Rev. 1.0.

The pinnings of the OPTIGA™ SLB 9670 TPM1.2 and OPTIGA™ SLx 9670 TPM2.0 are compliant to the TCG [7], [8], [9], [10], [11].

1.2 Features

- OPTIGA™ TPM SLB 9670 TPM1.2 or OPTIGA™ TPM SLx 9670 TPM2.0 Trusted Platform Module
- PG-VQFN-32-13 package
- Serial Peripheral Interface (SPI)
- 26-pin Raspberry Pi® 1 header, compatible with Raspberry Pi® 2 & 3 40-pin header
- 3.3 V or 1.8 V power supply
- Reset button
- Reset input from evaluation board or from Raspberry Pi®

1.3 Scope and Purpose

The OPTIGA™ TPM SLB 9670 TPM1.2 and OPTIGA™ TPM SLx 9670 TPM2.0 use a SPI interface to communicate with the host. The OPTIGA™ TPM SLB 9670 TPM1.2 and OPTIGA™ TPM SLx 9670 TPM2.0 product families with SPI interface consists of 4 different products:

- OPTIGA™ TPM SLB 9670 TPM1.2 standard security applications
- OPTIGA™ TPM SLB 9670 TPM2.0 standard security applications
- OPTIGA™ TPM SLI 9670 TPM2.0 automotive security applications
- OPTIGA™ TPM SLM 9670 TPM2.0 industrial security applications

We refer with TPM to all of the above 4 members of the OPTIGA™ TPM1.2 and OPTIGA™ TPM2.0 product families with SPI interface. Whereas the OPTIGA™ TPM SLB 9670 TPM1.2 is a fully TCG compliant TPM product with CC (EAL4+) certification, the OPTIGA™ TPM SLx 9670 TPM2.0 products have additionally FIPS certification. The OPTIGA™ TPM SLx 9670 TPM2.0 products standard, automotive and industrial differ with regards to supported temperature range, lifetime, quality grades, test environment, qualification and reliability to fit the target applications requirements. For more details and an overview of all Infineon OPTIGA™ TPM products refer to Infineon's website [1] and the according OPTIGA™ TPM Datasheets [2][3][4][5]. More information about the OPTIGA™ TPM in general and how to integrate it into a platform can be found in the corresponding specifications of the Trusted Computing Group (TCG) in reference [6].

Iridium – SPI TPM boards:

Supported TPM	Order type	Order number:
OPTIGA™ TPM SLB 9670 TPM1.2	IRIDIUM9670 TPM1.2 LINUX	SP001596596
OPTIGA™ TPM SLB 9670 TPM2.0	IRIDIUM9670 TPM2.0 LINUX	SP001596592
OPTIGA™ TPM SLI 9670 TPM2.0	IRIDIUM SLI 9670 TPM2.0	SP004232000
OPTIGA™ TPM SLM 9670 TPM2.0	IRIDIUM SLM 9670 TPM2.0	SP004232004

Table 1 List of available Iridium –SPI TPM boards

2 Schematics and Layout

2.1 Iridium – SPI TPM Schematics

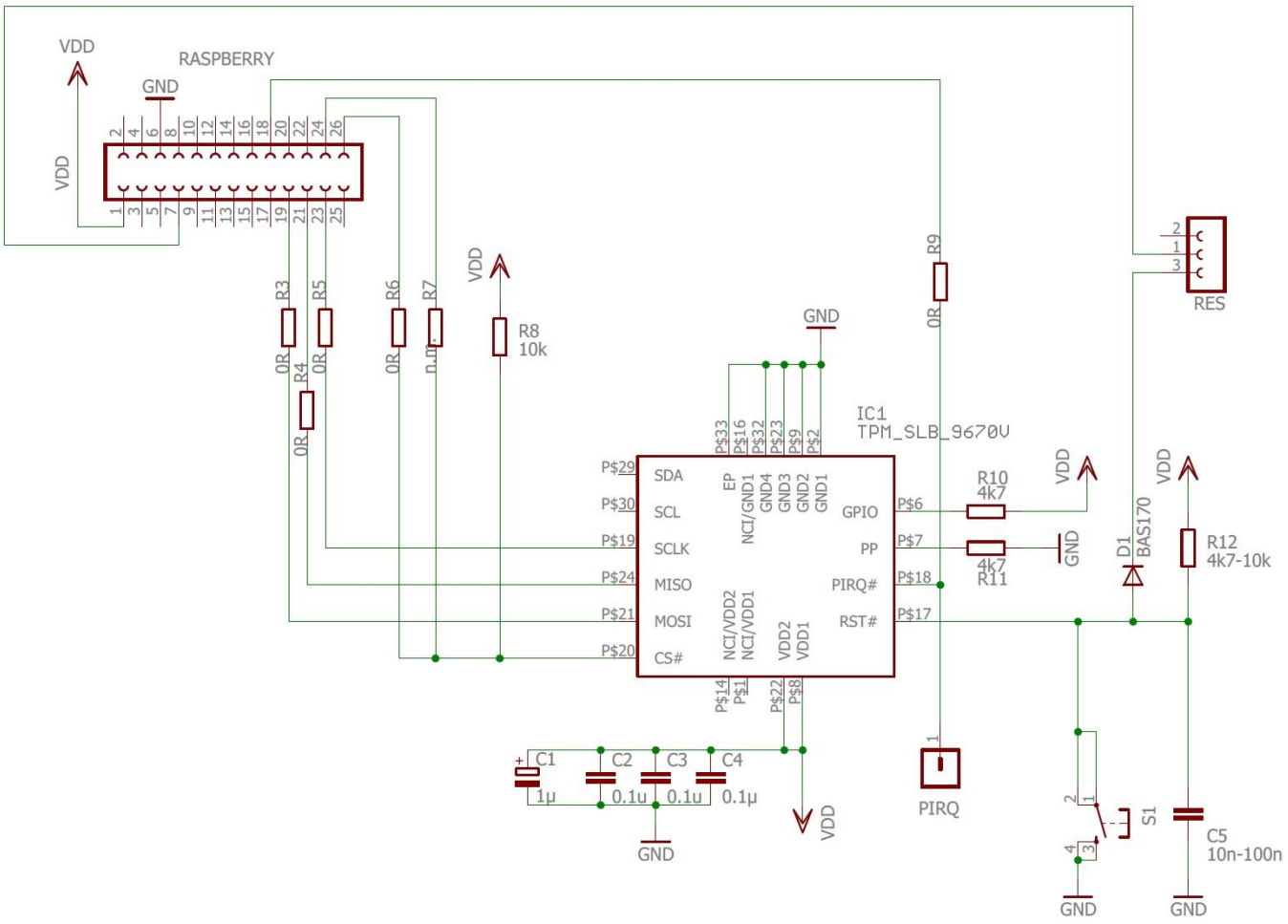


Figure 1 Iridium - SPI TPM schematics.

2.2 Iridium – SPI TPM Board Layout

2.2.1 Placement of components

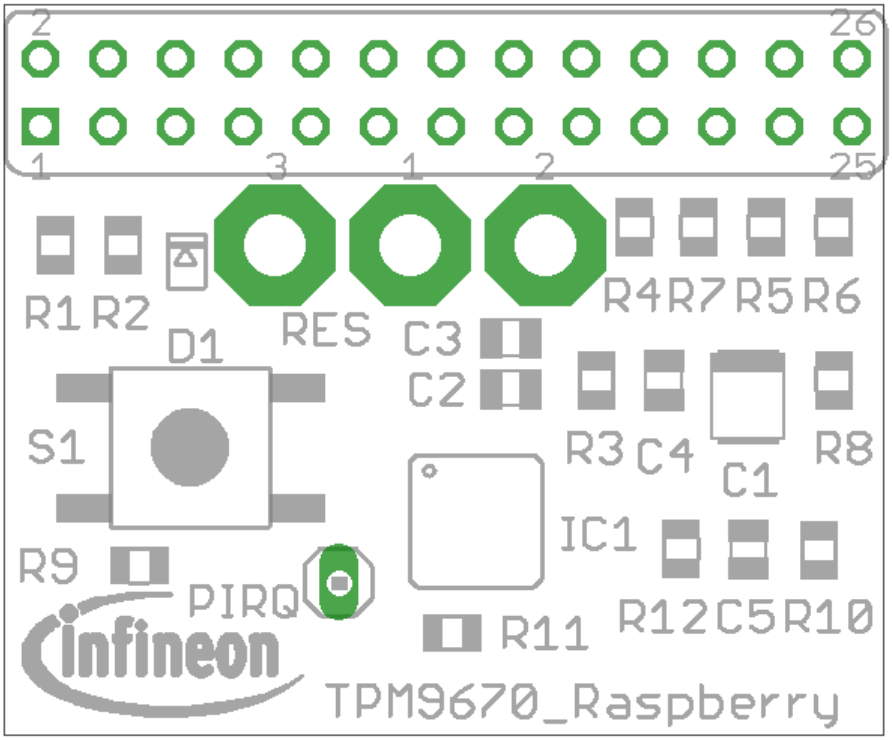


Figure 2 **Top view of Iridium - SPI TPM board**

2.2.2 Layout of the component side

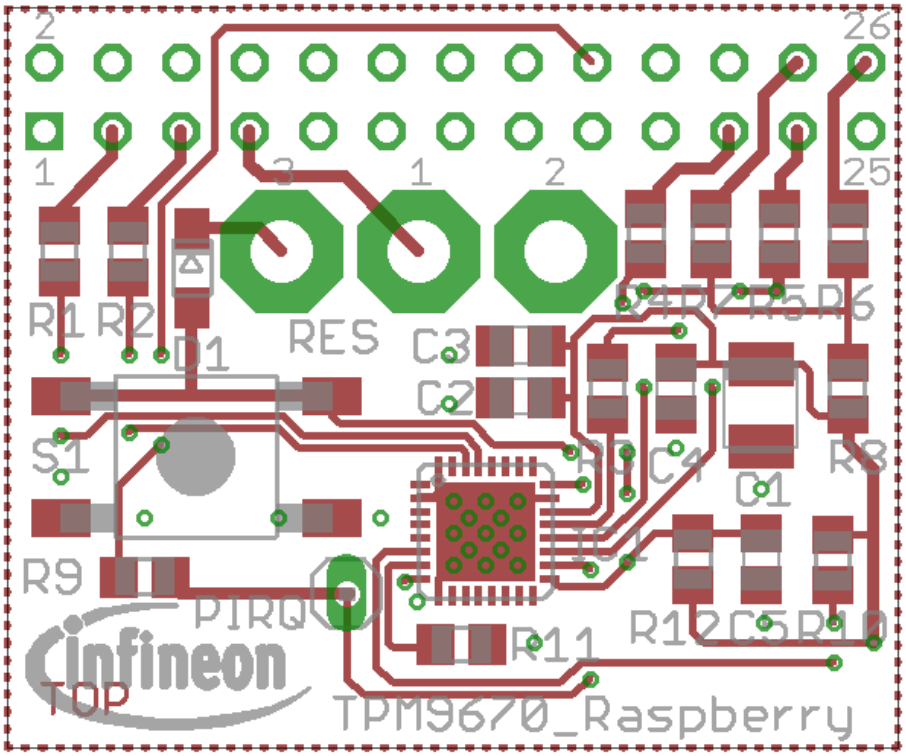


Figure 3 **Layout on top view of Iridium - SPI TPM board**

2.2.3 Layout of the solder side

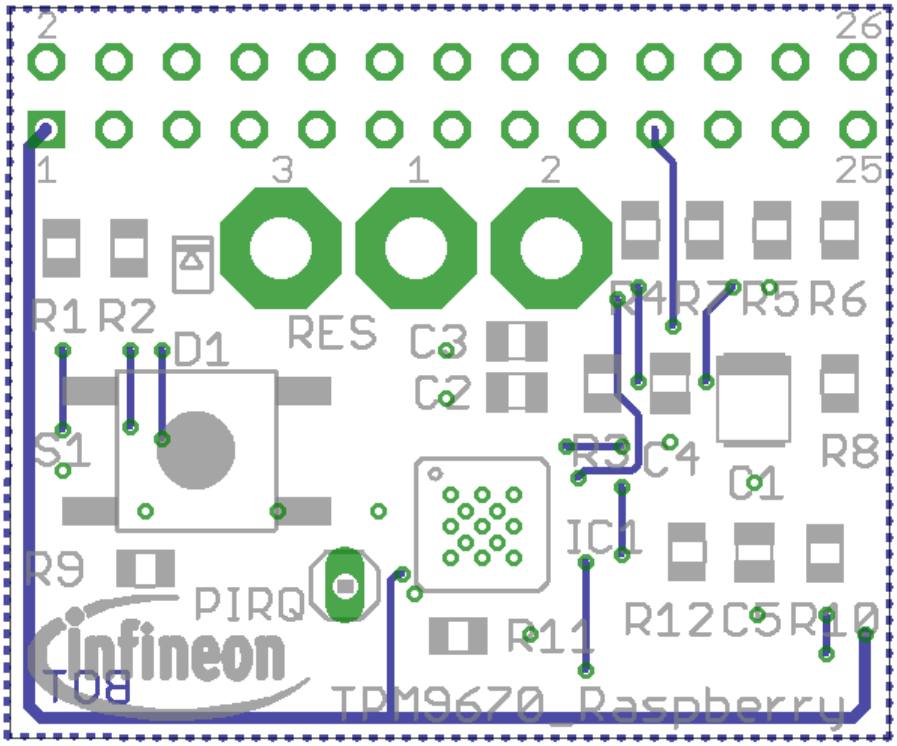


Figure 4 Layout of solder side of Iridium - SPI TPM board

3 Iridium – SPI TPM Board Details

3.1 Iridium – SPI TPM Board Dimensions

- ~ 34 x 33 mm (including Raspberry Pi® connector)
- Thickness: ~ 12 mm

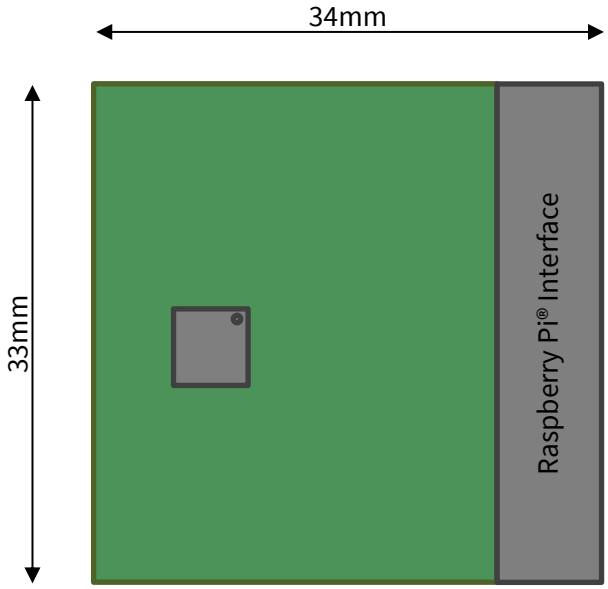
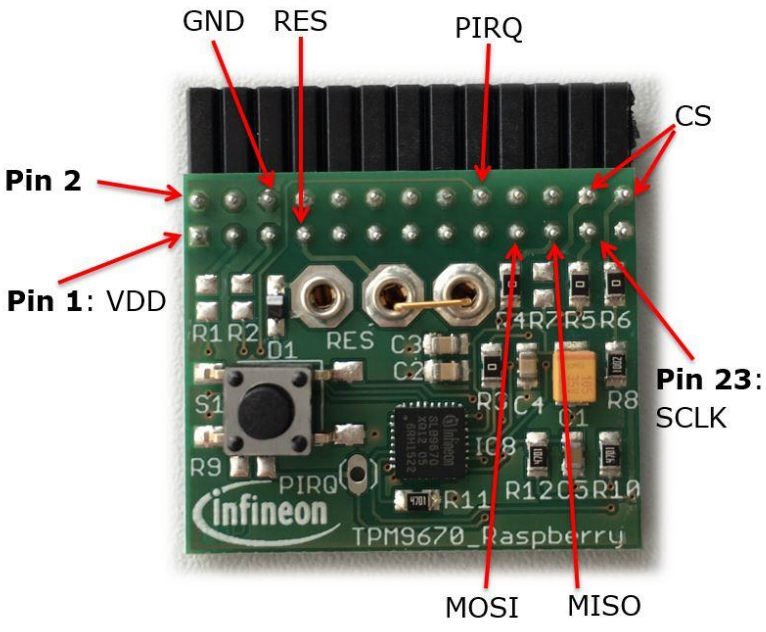


Figure 5 Iridium – SPI TPM board (Board Rev. 1.0)

3.2 Iridium – SPI TPM Board – Pin Configuration



Signal	Pin	Pin	Signal
VDD	1	2	-
-	3	4	-
-	5	6	GND
RES	7	8	-
-	9	10	-
-	11	12	-
-	13	14	-
-	15	16	-
-	17	18	PIRQ
MOSI	19	20	-
MISO	21	22	-
SCLK	23	24	CS (optional)
-	25	26	CS (default)

Figure 6 Iridium – SPI TPM board - Pin Configuration

4 Iridium – SPI TPM Board Connectors

Figure 7 Board connection Iridium - SPI TPM board on a Raspberry Pi® 3

4.1 Reset input from evaluation board

An optional Reset input source from the Raspberry Pi® board can be selected with the Reset Jumper RES.

RES Pins connected	Reset can be initiated by the host
1-2	No
3-1	Yes

Table 2 Reset input configuration

5 Board Ordering

Sales Code / Ordering Code:

Sales Code	Ordering Code
IRIDIUM9670 TPM1.2 LINUX	SP001596596
IRIDIUM9670 TPM2.0 LINUX	SP001596592
IRIDIUM SLI 9670 TPM2.0	SP004232000
IRIDIUM SLM 9670 TPM2.0	SP004232004

Table 3 Iridium – SPI TPM board ordering information

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] Data Sheet of Trusted Platform Module SLI 9670VQ2.0 TCG, Rev 1.1, 2019-02-21

[5] Data Sheet of Trusted Platform Module SLM 9670VQ2.0 TCG, Rev 1.0, 2019-04-08

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

[7] “TCG PC Client TPM Interface Specification (TIS)”, Version 1.3, 2013-03-21, TCG

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

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

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

[11] “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 – Iridium - 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.