OPTIGA™ TPM SLB 9672
RaspberryPi® Evaluation Board - SPI TPM HAT

Evaluation Board for OPTIGA™ Trusted Platform Module

Devices

- OPTIGA™ TPM SLB 9672 FW 15.xx
- OPTIGA™ TPM SLB 9672 FW 16.xx

Board Rev. 3.2

About this document

Scope and purpose

This document describes the Evaluation Board for Infineon OPTIGA™ TPM devices, OPTIGA™ SLB 9672 TPM2.0 Firmware 15.xx and Firmware 16.xx.

This board can be used to evaluate the functionality of the OPTIGA™ TPM SLB 9672 TPM2.0 Firmware 15.xx and 16.xx Trusted Platform Module (TPM) in a target system environment.

The OPTIGA™ TPM SLB 9672 RaspberryPi® Evaluation Board - SPI TPM HAT is designed for use on a RaspberryPi® (Version 2 or higher is required). It contains a 40-pin RaspberryPi® header and follows the RaspberryPi® HAT specification.

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 9672 TPM2.0 FW 15.xx and FW16.xx 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 9672 FW 15.xx and FW 16.xx in PG-UQFN-32-1,-2 package is the main component of the RaspberryPi® SPI TPM evaluation board with Board Rev. 3.2.

The functionality and the pinning of the OPTIGA™ TPM SLB 9672 FW 15.xx and FW 16.xx complies with the Trusted Platform Module Library (Part 1-4), Family 2.0, Level 00, Rev. 01.59, November 8, 2019 including Errata for TCG Trusted Platform Libary, Family 2.0, Level 00, Rev. 01.59, November 8, 2019, Errata Version 1.1, June 18, 2020 as well as TCG PC Client Platform TPM Profile (PTP) Specification, Family 2.0, Level 00, Rev. 01.05 v14, September 4, 2020 including Errata for PC Client Platform TPM Profile for TPM 2.0 Version 1.05 Revision 14, Errata Version 1.0, September 04, 2020.

1.2 Features

- OPTIGA™ TPM SLB 9672 FW 15.xx or FW 16.xx Trusted Platform Module
- PG-UQFN-32-1,-2 package
- Serial Peripheral Interface (SPI)
- Fulfills the RaspberryPi®HAT specification with automated loading of the necessary device-tree overlay [1]
- Stackable 40-pin header, compatible with RaspberryPi® 2, 3, 4, Zero and Zero2
- 3.3 V or 1.8 V power supply
- Reset button
- Reset input from the TPM from evaluation board button or from the RaspberryPi® GPIO

[1] https://github.com/raspberrypi/hats

1.3 Scope and Purpose

The OPTIGA™ TPM SLB 9672 FW 15.xx and 16.xx use an SPI interface to communicate with the host. The OPTIGA™ TPM SLB 9672 product family with SPI consists of four different products:

- OPTIGA™ TPM SLB 9672 FW15, TPM for computing platforms (PC and Server)
    - OPN: SLB9672**VU**20FW**15**21XTMA1
- OPTIGA™ TPM SLB 9672 FW15, TPM for computing platforms (PC and Server) with enhanced temperature range
    - OPN: SLB9672**XU**20FW**15**21XTMA1
- OPTIGA™ TPM SLB 9672 FW16, TPM with enhanced security features for IoT
    - OPN: SLB9672**XU**20FW**16**10XTMA1
- OPTIGA™ TPM SLB 9672 FW16, TPM with enhanced security features for IoT with enhanced temperature range
    - OPN: SLB9672**AU**20FW**16**10XTMA1

The OPTIGA™ TPM SLB 9672 is a fully TCG compliant TPM product with CC (EAL4+) certification and additionally FIPS certification. The OPTIGA™ TPM SLB 9672 products differ with regards to supported temperature range to fit the target applications requirements. For more details and an overview of all Infineon OPTIGA™ TPM products visit the Infineon website and the according OPTIGA™ TPM Datasheets [1] [2]. 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)[3].

[1] Data Sheet of Trusted Platform Module SLB 9672 TCG, FW 15

[2] Data Sheet of Trusted Platform Module SLB 9672 TCG, FW 16

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

2 Schematics , Layout and Dimensions

2.1 Schematic

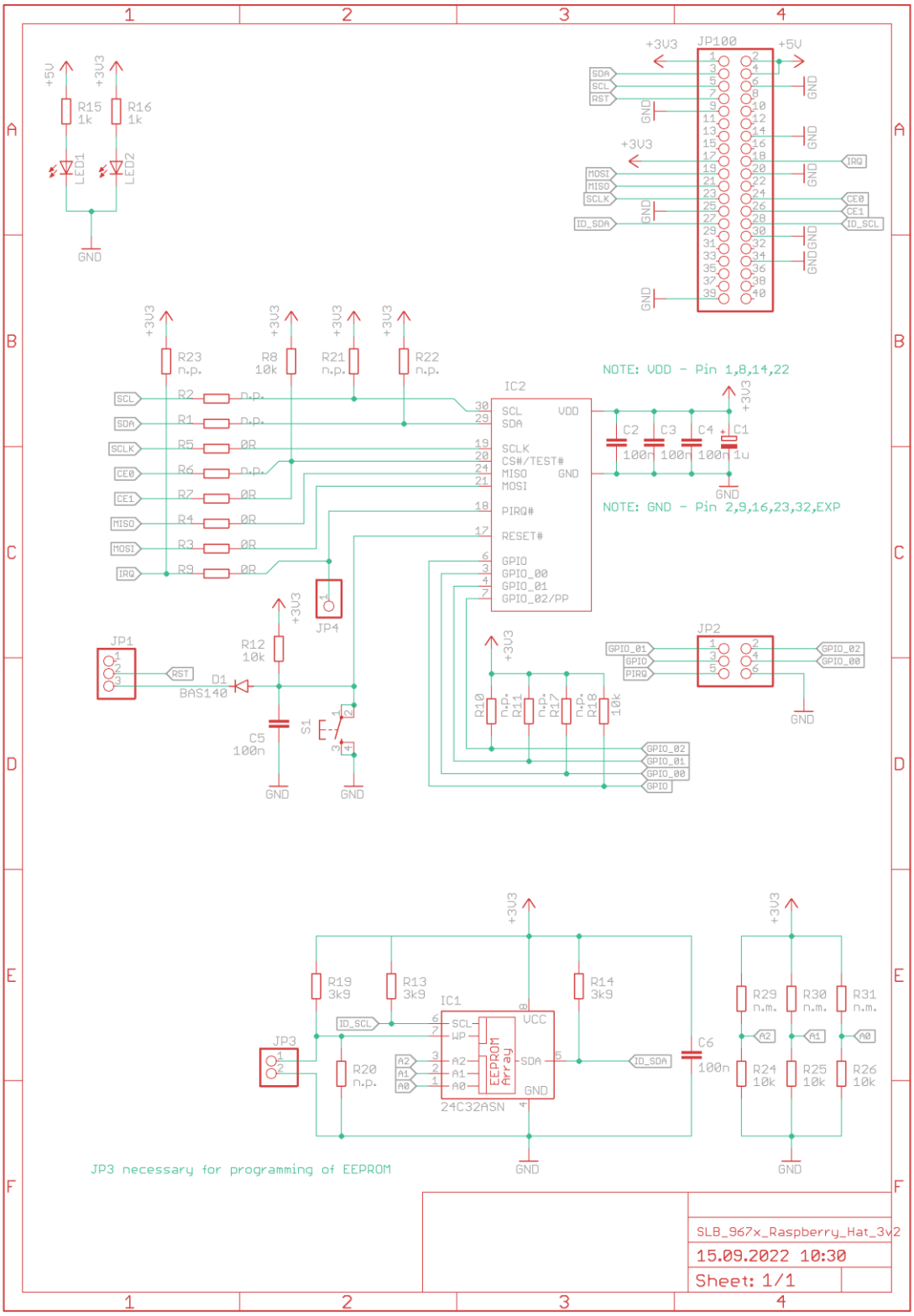

Figure 1 Schematic of OPTIGA™ TPM SLB 9672 RaspberryPi® Evaluation board.

2.2 Placement and Board Layout

2.2.1 Placement of components

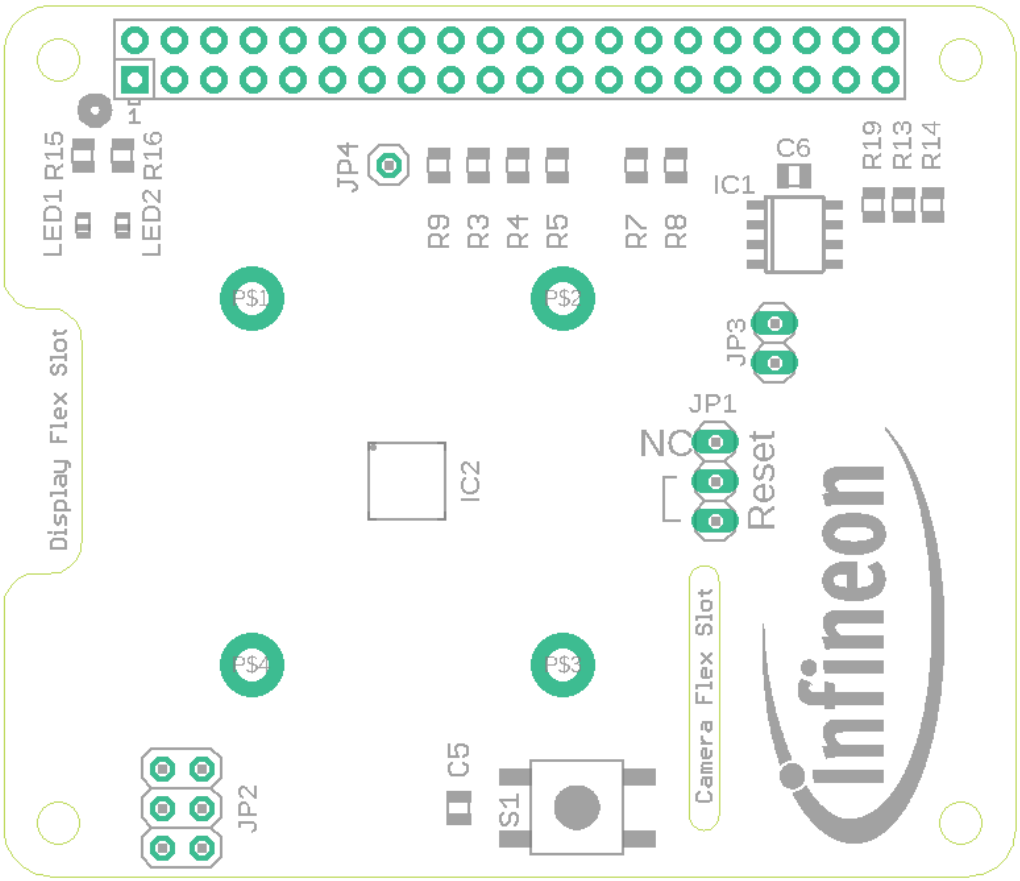

Figure 2 Component placement of OPTIGA™ TPM SLB 9672 RaspberryPi® Evaluation board ,Top.

2.2.2 Layout: Top view

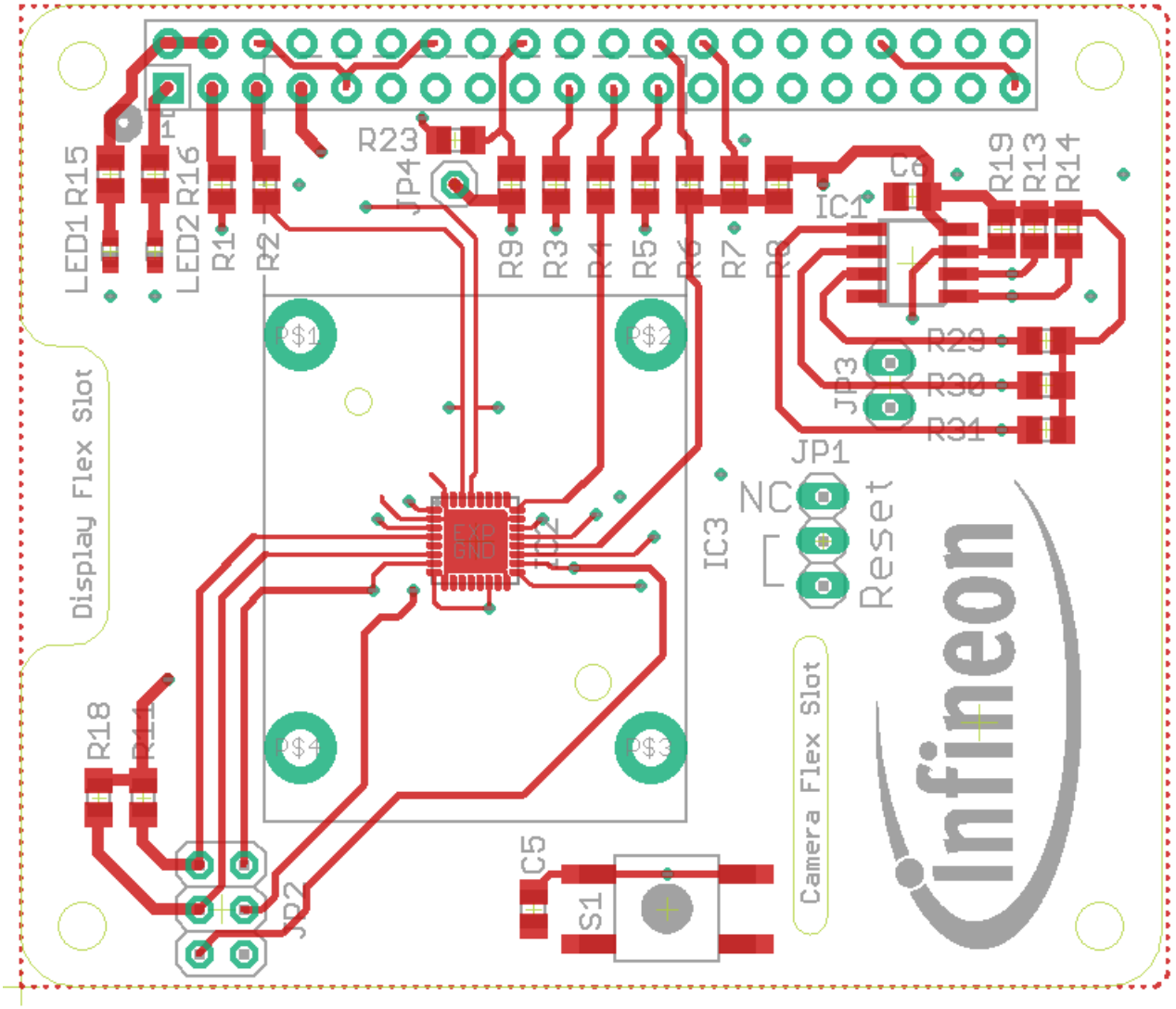

Figure 3 Top side routing of OPTIGA™ TPM SLB 9672 RaspberryPi® Evaluation board

2.2.3 Layout: Bottom view

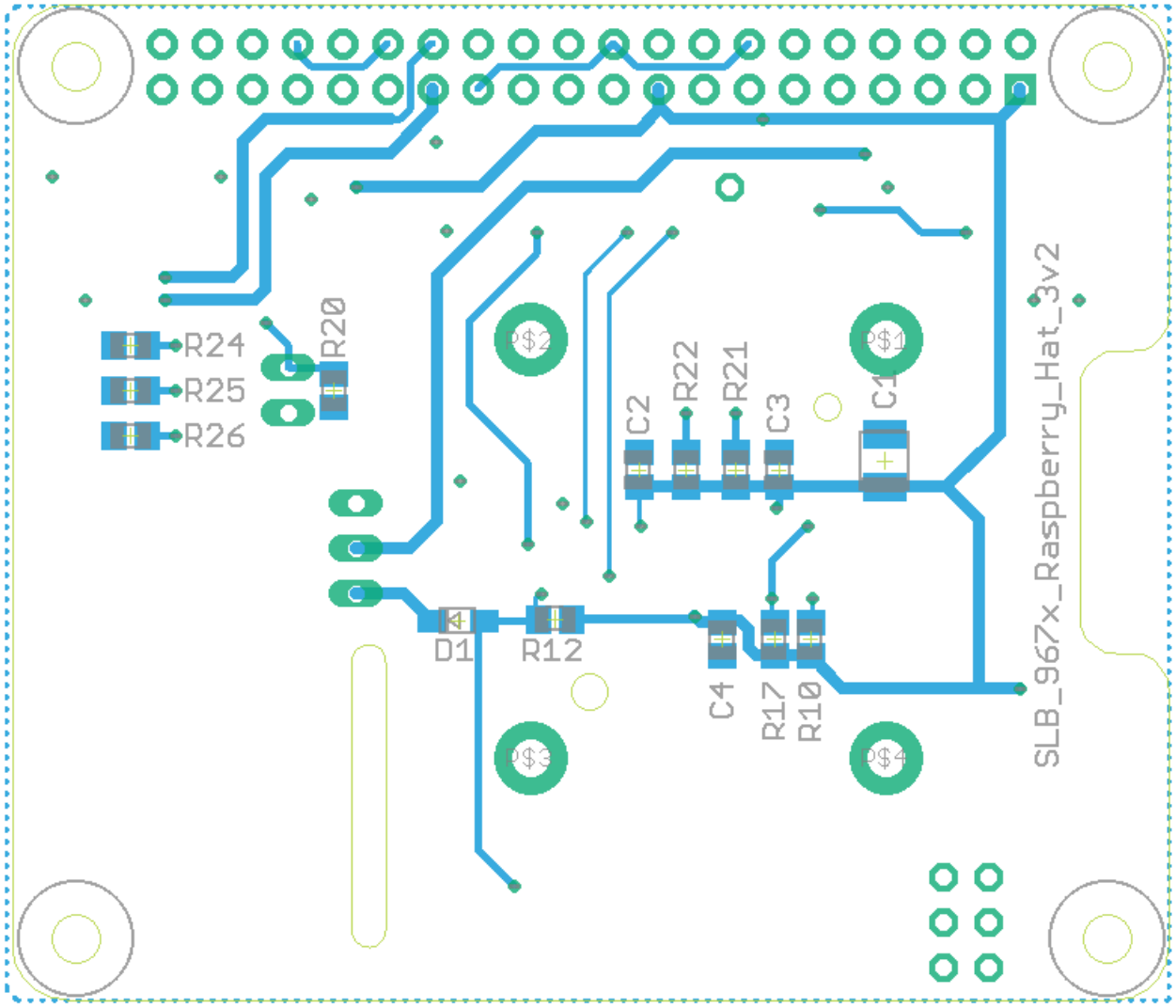

Figure 4 Bottom side routing of OPTIGA™ TPM SLB 9672 RaspberryPi® Evaluation board

2.3 Board Dimensions

Following the HAT specification , Picture by RaspberryPi® (Trading) Ltd.

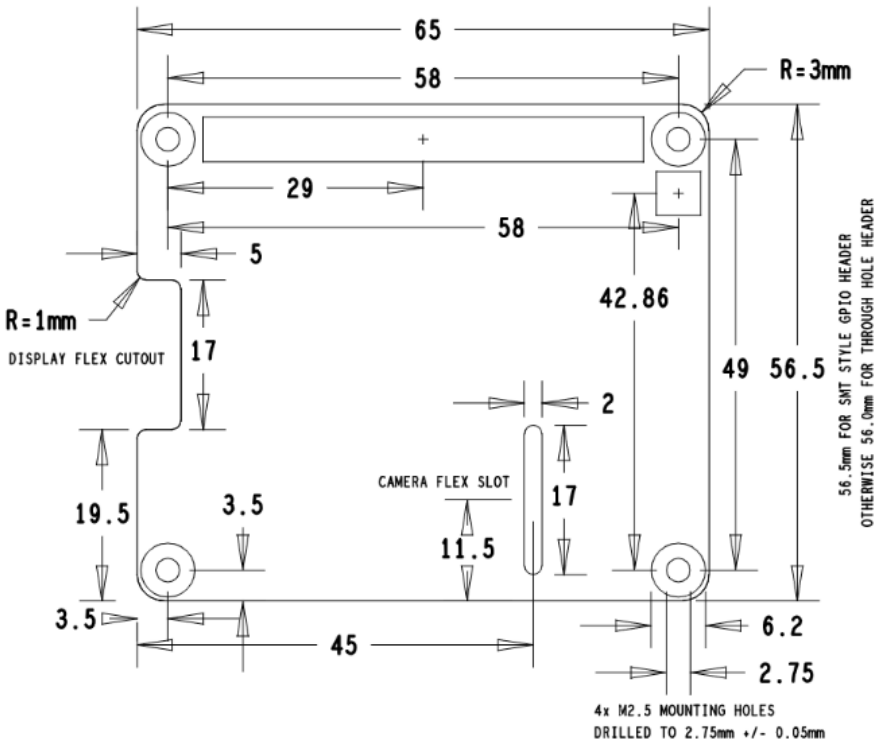

Figure 5 Board dimensions of OPTIGA™ TPM SLB 9672 RaspberryPi® Evaluation board

3 Evaluation Board Image

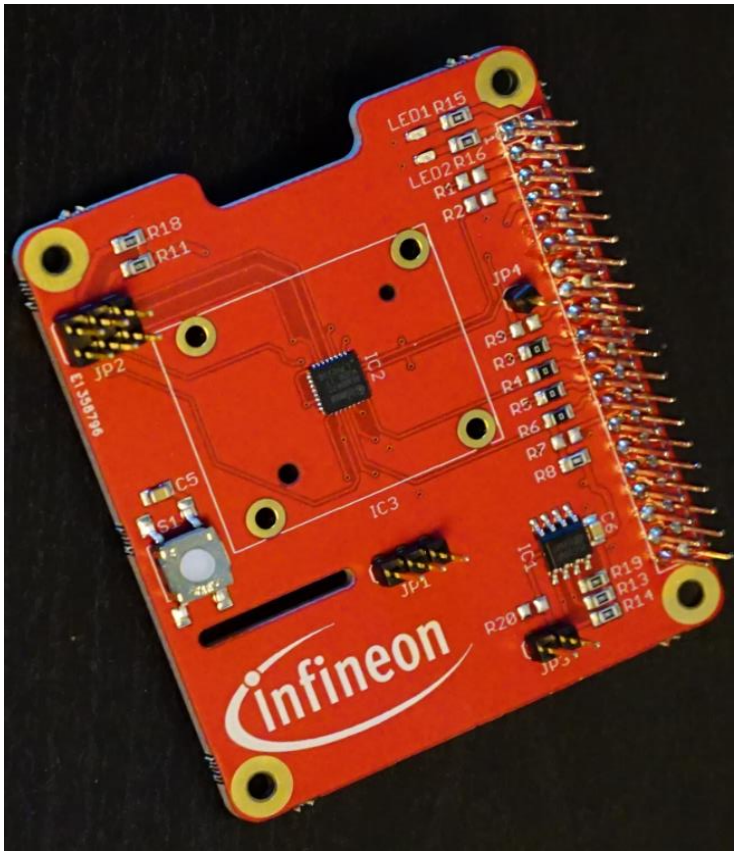

Figure 6 Picture of OPTIGA™ TPM SLB 9672 RaspberryPi® Evaluation board

4 Reset inputs from the evaluation board

The evaluation board contains two reset sources for the SLB9672 TPM chip.

4.1 Physical user button S1

The physical user button S1 will perform a reset of the TPM immediately. This reset respects the reset timing as described in the datasheet.

4.2 Reset via RaspberryPi® GPIO

The RaspberryPi® Board itself can act as an additional reset source for the SLB9672. It can be enabled using a jumper on JP1. The reset signal is expected on pin 7 of the RaspberryPi® header which corresponds to GPIO4.

JP1 Pins connected	Reset can be initiated by the host over the RaspberryPi®
1-2	No (Park position)
2-3	Yes
No connections	No

Table 1 Reset input configuration

5 Board Ordering

Sales Code / Ordering Code

OPN	Description	Ordering Code	Status
TPM9672FW1521RPIEB TOBO1	OPTIGA™ TPM SLB 9672 RaspberryPi® Evaluation board SPI FW 15.xx	SP005741189	not recommended for new designs
TPM9672FW1610RPIEB TOBO1	OPTIGA™ TPM SLB 9672 RaspberryPi® Evaluation board SPI FW 16.xx	SP005741187	active and preferred

Table 2 Board ordering information

6 Revision history

Reference	Description
Revision 1.1	
1.1	Fix typos
1.0	Initial version – OPTIGA™ TPM SLB 9672 RaspberryPi® Evaluation board - SPI TPM HAT

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.