OPTIGA™ TPM SLB 9673 RaspberryPi® Evaluation Board - I2C TPM HAT

Evaluation Board for OPTIGA™ Trusted Platform Module

Devices

- OPTIGA™ TPM SLB 9673 FW 26.xx

Board Rev. 3.2

About this document

Scope and purpose

This document describes the Evaluation Board for Infineon OPTIGA™ TPM devices, OPTIGA™ SLB 9673 TPM2.0 Firmware 26.xx.

This board can be used to evaluate the functionality of the OPTIGA™ TPM SLB 9673 TPM2.0 Firmware 26.xx Trusted Platform Module (TPM) in a target system environment.

The OPTIGA™ TPM SLB 9673 RaspberryPi® Evaluation Board – I2C 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 to help customers 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 9673 TPM2.0 FW 26.xx 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 9673 FW 26.xx in PG-UQFN-32-1,-2 package is the main component of the RaspberryPi® I2C TPM evaluation board with Board Rev. 3.2.

The functionality and the pinning of the OPTIGA™ TPM SLB 9673 FW 26.xx complies with the TCG PC Client Platform TPM Profile Specification for TPM 2.0 (TCG, 2020)

1.2 Features

- OPTIGA™ TPM SLB 9673 FW 26.xx Trusted Platform Module
- PG-UQFN-32-1,-2 package
- Inter-Integrated Circuit (I2C)
- 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 for 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 9673 FW 26.xx use an I2C interface to communicate with the host. The OPTIGA™ TPM SLB 9673 product family with I2C consists two different products:

- OPTIGA™ TPM SLB 9673 FW26, TPM with enhanced security features for IoT
    - OPN: SLB9673**X**U20FW2610XTMA1
- OPTIGA™ TPM SLB 9673 FW16, TPM with enhanced security features for IoT with enhanced temperature range
    - OPN: SLB9673**A**U20FW2610XTMA1

The OPTIGA™ TPM SLB 9673 is a fully TCG compliant TPM product with CC (EAL4+) certification and additional FIPS certification. The OPTIGA™ TPM SLB 9673 products differ with regards to supported temperature range reliability 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]. 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)[2].

[1] Data Sheet of Trusted Platform Module SLB 9673 TCG, FW 26

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

2 Schematics , Layout and Dimensions

2.1 Schematic

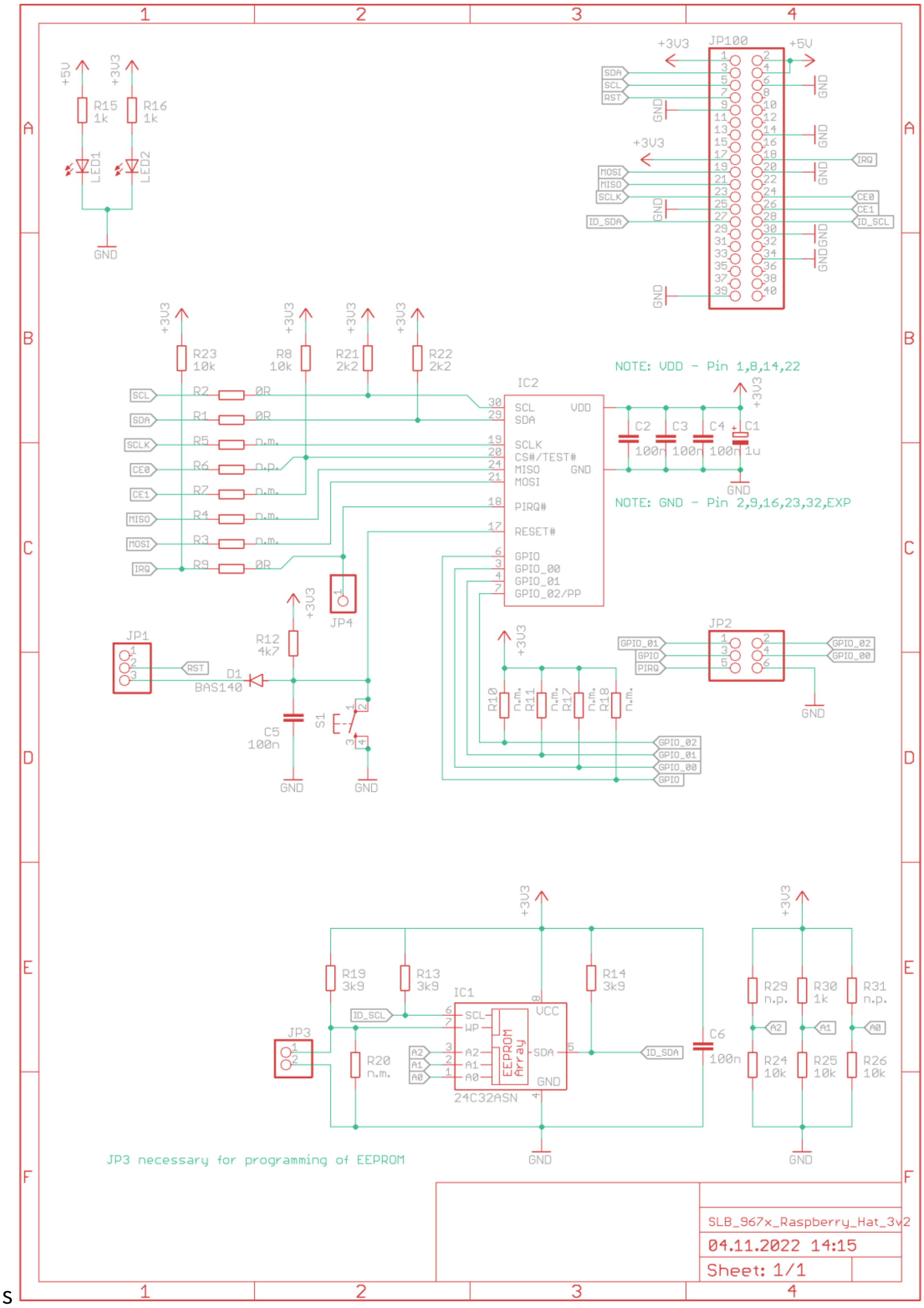

Figure 1 OPTIGA™ TPM SLB 9673 RaspberryPi® Evaluation board - I2C TPM HAT Schematic.

2.2 Placement and Board Layout

2.2.1 Placement of components

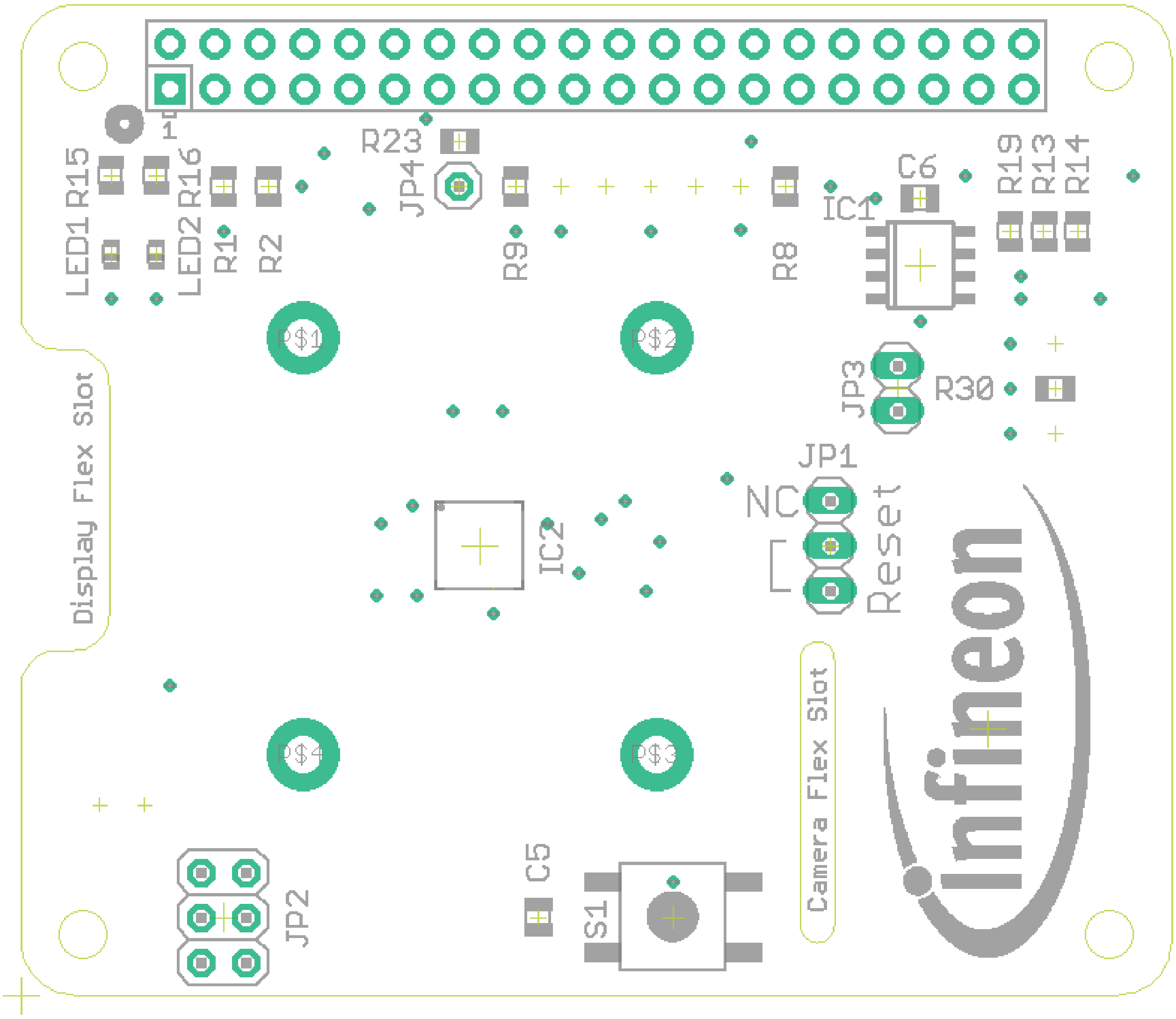

Figure 2 Top view, placing of the components

2.2.2 Layout: Top view

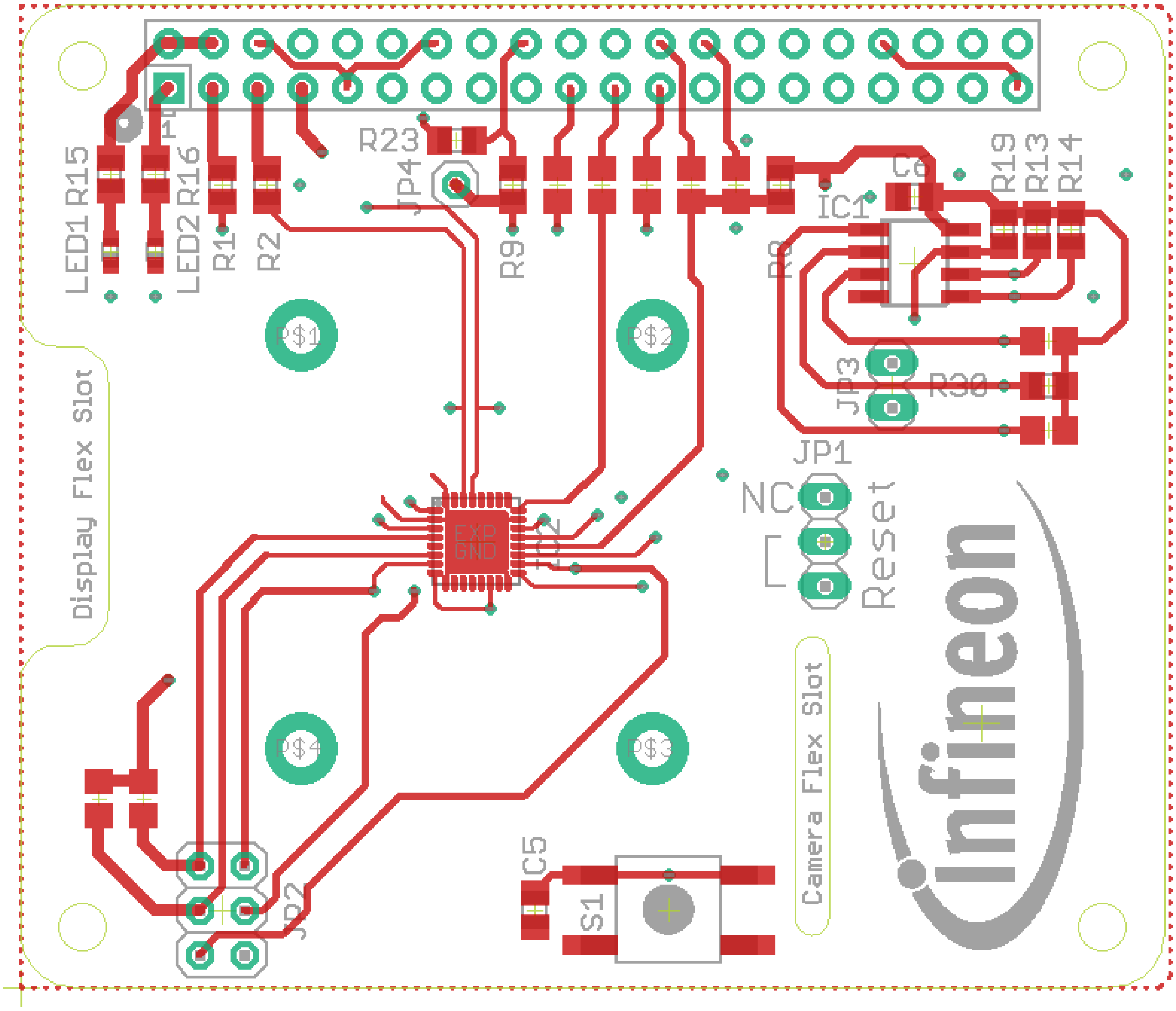

Figure 3 Top view of the Evaluation Board

2.2.3 Layout: Bottom view

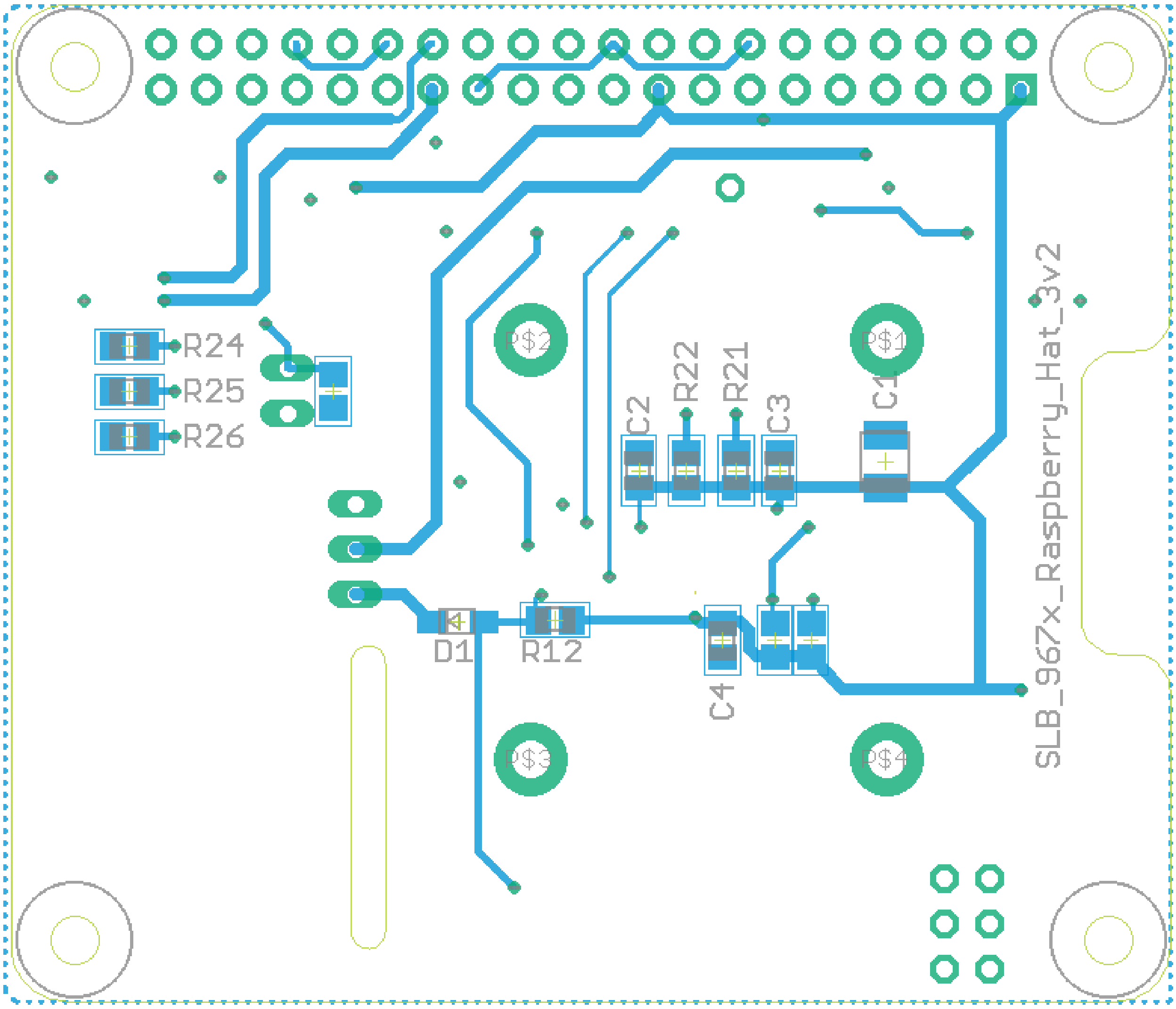

Figure 4 Bottom view of the Evaluation Board

2.3 Board Dimensions

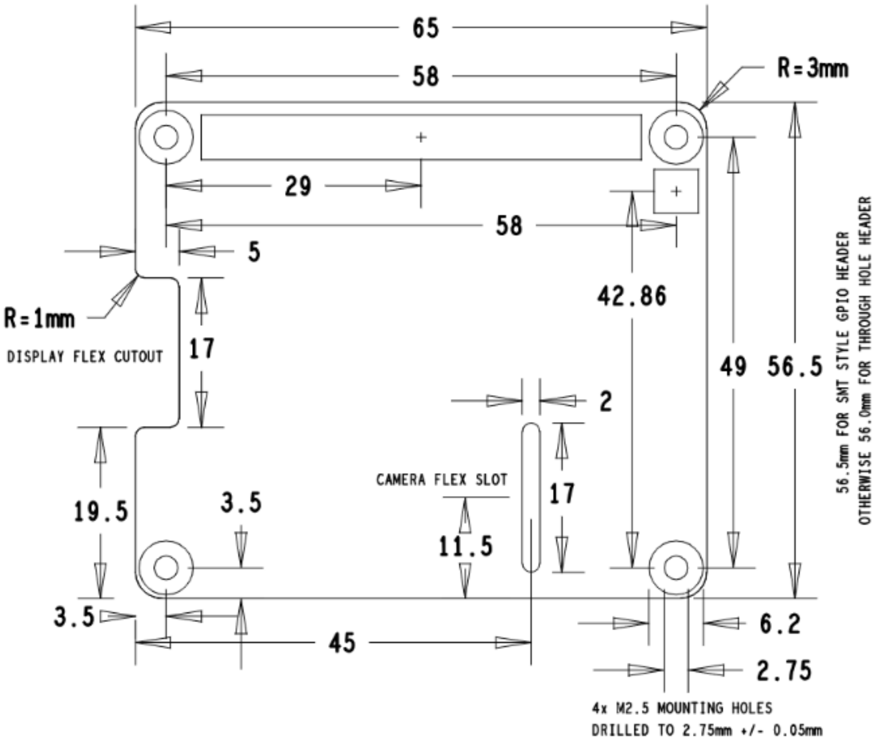

Figure 5 OPTIGA™ TPM SLB 9673 RaspberryPi® Evaluation board - I2C TPM HAT, following the HAT specification [1], Picture by Raspberry Pi (Trading) Ltd., (Raspberry Pi (Trading) Ltd.).

[1] https://github.com/raspberrypi/hats/blob/master/hat-board-mechanical.pdf

3 Evaluation Board Image

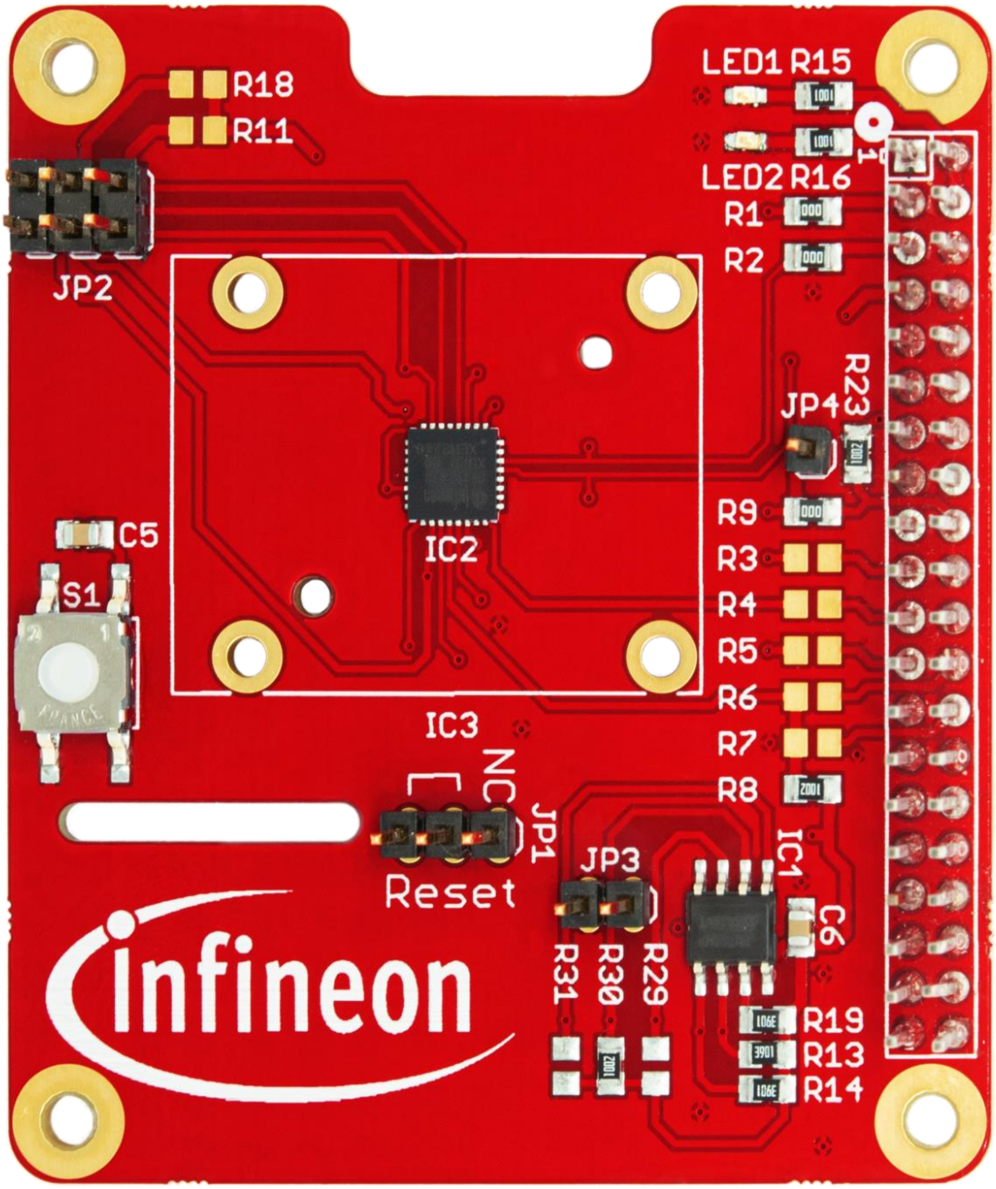

Figure 6 OPTIGA™ TPM SLB 9673 RaspberryPi® Evaluation board – I2C TPM HAT

4 Reset inputs from the evaluation board

The evaluation board contains two reset sources for the SLB9673 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 SLB9673. 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
2-3	Yes

Table 1 Reset input configuration

5 Board Ordering

Sales Code / Ordering Code

OPN	Description	Ordering Code	Status
TPM9673FW2613RPIEBTOBO1	OPTIGA™ TPM SLB 9673 RaspberryPi® Evaluation board I2C FW 26.xx	SP006005648	active and preferred

Table 2 Board ordering information

6 Appendix: Issue in I2C hardware on the RaspberryPi®'s SoC

The I2C hardware peripheral on a RaspberryPi® SoC has two hardware issues. Both issues can hinder the communication with the TPM chip.

6.1 I2C clk stability

The I2C CLK frequency of the hardware periphial is unstable. The reason is that it is internally hard-linked to the CPU frequency. If the RaspberryPi® enters a power saving mode and reduceds the CPU clock frequency, the I2C clock frequency will decrease by the same factor.

Workaround 1: Configure a fixed CPU clock frequency.

Workaround 2: Use a soft-I2C implementation instead of the hardware periphial.

6.2 Clockstretching

The I2C clockstretching mechanism is sometimes ignored by the I2C-Master periphial of the RaspberryPi®. If the clockstretching length of a slave needs only x <= T freq/2.

Workaround 1: Useage of soft-I2C.

6.3 Recommendation for the SLB9673 with RaspberryPi®

Selection of the soft-i2c driver in Device Tree Overlays.

Note that the Device Tree Overlay embedded in this evaluation board's EEPROM as well as the Device Tree Overlay of the RaspberryPi® OS Linux Kernel both use the soft-i2c driver.

7 Revision history

Reference	Description
Revision	
1.2	Update SP number and OPN
1.1	Initial version OPTIGA™ TPM SLB 9673 RaspberryPi® Evaluation board – I2C TPM HAT

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

Edition 2023-11-02
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.