OPTIGA™ TPM Application Note

Integration of an OPTIGA™ TPM SLx 9670 TPM2.0 with SPI Interface in a Raspberry Pi® 4 Linux environment

Devices

- OPTIGA™ TPM SLB 9670 TPM2.0
- OPTIGA™ TPM SLI 9670 TPM2.0
- OPTIGA™ TPM SLM 9670 TPM2.0

About this document

Scope and purpose

This document explains how the OPTIGA™ TPM SLx 9670 TPM2.0 can be used on a Raspberry Pi® 4. The same setup also works and has been tested on a Raspberry Pi® 3. However, in this document we refer to "Raspberry Pi® 4". The Linux kernel described in this document is version 4.19.50. This kernel has integrated TPM 2.0 driver support, which simplifies TPM setup with the Raspberry Pi® 4. This Application Note shows how fast and simple the TPM 2.0 setup is, even with basic Linux knowledge.

The OPTIGA™ TPM SLx 9670 TPM2.0 uses a SPI interface to communicate with the Raspberry Pi®. The OPTIGA™ TPM SLx 9670 TPM2.0 product family with SPI interface consists of 3 different products:

- 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 "OPTIGA™ TPM SLx 9670 TPM2.0" to all of the above 3 members of the OPTIGA™ TPM 2.0 product family with SPI interface.

OPTIGA™ TPM SLx 9670 TPM2.0 products are fully TCG compliant TPM products with CC (EAL4+) and 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 refer to Infineon's website [1]. Since all 3 OPTIGA™ TPM SLx 9670 TPM2.0 products are fully TCG compliant with regards to the SPI and software interface, the described steps to integrate a TPM 2.0 in a Raspberry Pi® 4 Linux environment are the same and valid for all 3 variants. We are referring in this document also to the OPTIGA™ TPM SLx 9670 TPM2.0 by using simply "TPM". An overview of all Infineon OPTIGA™ TPM products can be found on Infineon's website [2]. More information about the 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 [3].

The described steps to integrate an OPTIGA™ TPM in a Raspberry Pi® 4 Linux environment can be performed with one of the Infineon Iridium SLx 9670 TPM2.0 SPI Boards, listed in the Table below.

Iridium Boards:

Supported TPM	Order type	Order number:
OPTIGA™ TPM SLB 9670 TPM2.0	IRIDIUM 9670 TPM2.0	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

The 3 Infineon Iridium Boards are referred in the following as "Infineon Iridium SLx 9670 TPM2.0 SPI Board"

Intended audience

This document is intended for customers who want to increase the security level of their embedded platforms using a TPM 2.0 and like to evaluate how to start with the TPM software integration for their target applications.

OPTIGA™ TPM Application Note
OPTIGA™ TPM SLx 9670 TPM2.0 in a Raspberry Pi® 4
Table of contents

Table of contents

1 Introduction

1.1 Motivation

Two of the basic principles of information security when exchanging data are confidentiality and authenticity. While the first one is obvious to almost everyone, the second one often does not get the appropriate amount of attention. Authenticity is just as important as confidentiality, because for example the highest confidentiality of secret data is worth nothing in case the secret data come from or is shared with the wrong communication partner.

A TPM adds additional security features to a platform, which will not only help in gaining confidentiality but also authenticity of exchanged data or a communication partner.

One of the most important features to achieve these goals is that sensitive data such as cryptographic keys or secrets can be stored inside the TPM, where the data is protected by the TPM's hardware from unauthorized access or manipulation. This allows confidentiality of the data on a high level. But in addition to this protection, the data can also be bound to a single TPM and thus to the platform hosting this TPM. This in turn can be used to bring in another authenticity factor, since only the platform or user operating the correct TPM is able to provide the correct authentication secret required to access the protected sensitive data.

Another basic feature of the TPM is that it can function as a starting point for establishing a root of trust, which allows the detection of unauthorized modifications to a platform's hardware or software.

Additionally, the TPM can be used to perform several cryptographic operations on data in hardware, decreasing the vulnerability to several kinds of attacks, such as reading out unencrypted sensitive data from the platform's memory.

1.2 Scope

This document is intended for users to help them getting familiar how to use a subset of the TPM's functionalities on embedded platforms running Linux. The final goal in this document is to interact with the TPM 2.0 to be able to run the test scripts provided in the GitHub project [4].

The topics described in this document are:

- The Evaluation Board (Figure 1) with its expansion header for the Raspberry Pi® 4 [5].

- Usage of a TPM 2.0 on a Raspberry Pi® 4.

This document has been generated using kernel version 4.19.50.

In this application note we use a Raspberry Pi® 4 Linux distribution based on Debian® to describe the system setup and the application of the TPM 2.0. If not explicitly said otherwise, the application note refers to specific versions of the required Linux packages to prevent compatibility problems. The mentioned versions were publicly available and downloaded at the time of release from the specified links and repositories.

1.3 Acronyms and Abbreviations

Acronym	Explanation
BIOS	Basic Input / Output System
EK	Endorsement Key
FTD	Flattened Device Tree
LTS	Long Term Support
PCR	Platform Configuration Register
RNG	Random Number Generator
RPi	Raspberry Pi ®
SoC	System on a Chip
SPI	Serial Peripheral Interface
SRK	Storage Root Key
SSH	Secure Shell
SSL	Secure Sockets Layer
TCG	Trusted Computing Group
TCS	TCG Core Services
TCSD	TCS Daemon
TLS	Transport Layer Security
TPM	Trusted Platform Module
TSS	TCG Software Stack
UEFI	Unified Extensible Firmware Interface
VPN	Virtual Private Network

2   Hardware Setup

The required hardware to perform the steps described in this document consists of:

- Developer PC: This platform is used for installing the Raspian image following the steps provided in this guide [8].
- Infineon Iridium SLx 9670 TPM2.0 SPI Board. This board contains the Infineon OPTIGA™ TPM SLx 9670 TPM2.0 mounted on an easy-to-use hardware board, which can be attached to the Raspberry Pi® 4.
- Raspberry Pi® 4:
    - Raspberry Pi® 4
    - Micro SD Card[1] with at least 8 GB
    - USB-C USB cable for power supply
- MicroSD-Card Reader (for the developer PC)

2.1   Infineon Iridium SLx 9670 TPM2.0 SPI Board

The Infineon Iridium SLx 9670 TPM2.0 SPI Board can be connected to a Raspberry Pi® 4 via its extension header. For data transfer the board uses the SPI bus. The board is shown in Figure 2.
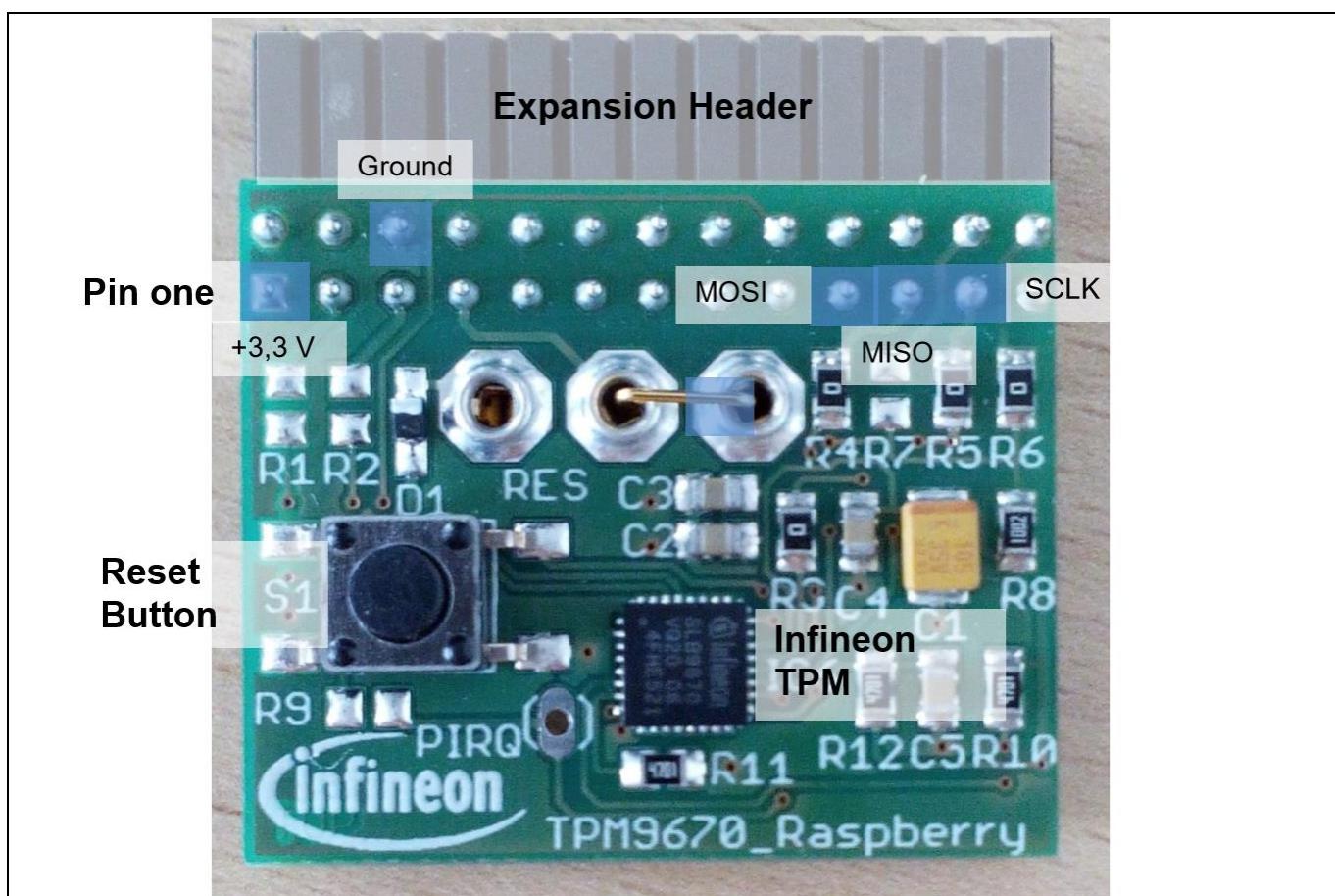
Figure 1   Infineon Iridium SLx 9670 TPM2.0 SPI Board

---

[1] Some card models may not work.

On the top is the Raspberry Pi® Header with 26 pins. The board contains a reset circuit on board, which pulls the reset line of the TPM to GND for the right amount of time after VCC becomes available. The reset of the module is active low and can also be set by connecting reset and ground via the reset button.

The Raspberry Pi® 4 Header has VDD, GND, MOSI, MISO and SCLK at the following pins:

Pin	1	6	19	21	23
Signal	VDD, 3.3 V	GND	MOSI	MISO	SCLK

Figure 2   Infineon Iridium SLx 9670 TPM2.0 SPI Board on Raspberry Pi® 4

3 Software Setup

This section describes all necessary steps needed to use the TPM 2.0 with a Raspberry Pi® 4.

3.1 On the Raspberry Pi® 4

Insert the flashed SD card and boot the Raspberry Pi® 4.

Open the file config.txt in an editor.

Code Listing 1

```
001        $ sudo nano /boot/config.txt
```

In this file insert two lines from Code Listing 2:

Code Listing 2

```
001        $ dtparam=spi=on
002        $ dtoverlay=tpm-slb9670
```

Save the file and exit the editor.

Reboot the Raspberry Pi® 4 for the changes to take effect.

Code Listing 3

```
001        $ sudo reboot now
```

After the reboot your Raspberry Pi® 4 should be able to communicate with the Iridium board.

3.2 Testing the TPM

Follow the next steps accordingly:

To use the Infineon Iridium SLx 9670 TPM2.0 SPI Board, run Embedded Linux TPM Toolbox 2 (ELTT2) on GitHub [7] and follow the steps provided in the ReadMe.

In order to integrate the OPTIGA™ TPM SLx 9670 TPM2.0 into your application, consider using open source TPM2 Software Stack (TSS) [4]. This software stack is available on GitHub.

In case you have questions or further specific interest in OPTIGA™ TPM, please get in touch with your local sales.

References

[1]   https://www.infineon.com/cms/de/product/evaluation-boards/iridium9670-tpm2.0-linux/

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

[3]   https://trustedcomputinggroup.org/resource/tpm-main-specification/

[4]   https://github.com/tpm2-software

[5]   https://www.raspberrypi.org/

[6]   https://www.raspberrypi.org/downloads/raspbian/

[7]   https://github.com/Infineon/eltt2

[8]   https://www.raspberrypi.org/documentation/installation/installing-images/README.md

Revision history

Page or Reference	Description of change
Revision 1.0, 2019-07-19	
	Initial Release

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