



OPTIGA™ TPM2.0 solution: Learn how Infineon is simplifying your IoT security

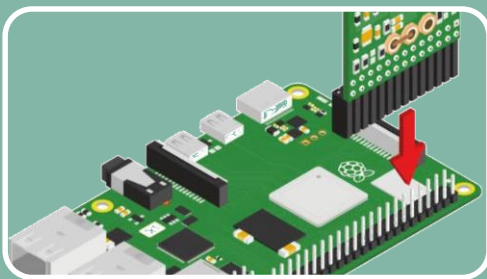
Infineon Technologies
February 2022



Agenda

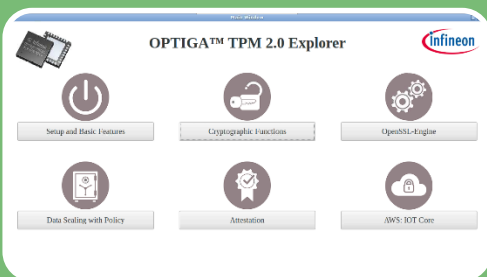
- 1 Simplifying the TPM 2.0 journey
- 2 Get started easily
- 3 TPM 2.0 is easy for beginners with the help of Graphical User Interface (GUI)
- 4 Integration is easy with ready-to-use code examples
- 5 Key takeaways

Simplifying the TPM 2.0 journey for developers



Get started easily

OPTIGA™ TPM2.0 add-on board is designed to enable the quick set up on Raspberry Pi, providing an almost plug & play integration



Learning is now easier and more engaging

Ease of installation and feature-rich GUI software to evaluate TPM basic to advanced use cases.



Ease of deployment and integration

Ready-to-use code examples for practical use cases deployment

Get TPM 2.0 up and running easier and quicker

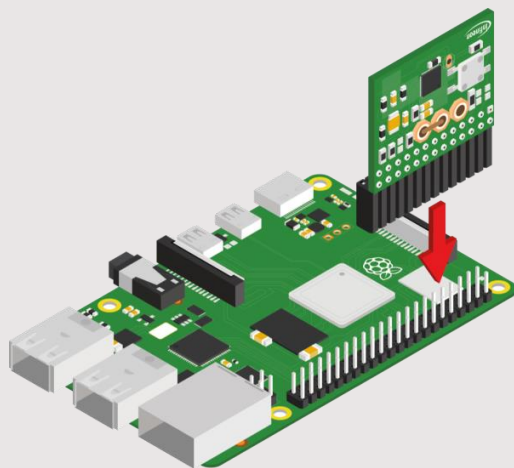
1



Setting up RPI

Connect the iridiumboard to your Raspberry Pi as illustrated and follow the instructions under:

<https://projects.raspberrypi.org/en/projects/raspberry-pi-setting-up>



2



Enabling TPM 2.0

Boot the Raspberry Pi and open the shell.
Run the following commands:

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

In the file replace:

```
#dtparam=spi=on
```

with:

```
dtparam=spi=on
```

and add this line:

```
dtoverlay=tpm-slb9670
```

Save your changes

```
sudo reboot now
```

3



Installing TPM 2.0 SW

Please follow the app note under:

<https://www.infineon.com/TPM-TSS-AppNote>

Making learning easier and more engaging

Hassle-free setup with automated installation script

Control the RPI from you laptop without additional peripheral devices

[OPTIGA TPM2.0 Explorer](#)

TPM is easy even for beginners with the help of GUI instead of CLI

Accelerate your learning by following graphical examples and step-by-step instructions in the user manual

Making interfaces not just easy to use, but also easy to learn

Easy-to-navigate interface

| | |
|---------------------------------|---|
| 1 Get TPM capability (variable) | 1 Displays variable TPM properties such as the AuthSet Values etc |
| 2 Get TPM capability (fixed) | 2 Displays fixed TPM Properties such as the manufacturer details etc |
| 3 Change Auth | 3 Changes the owner, endorsement and lookout authorization values |
| 4 TPM Clear | 4 Clear lockout, endorsement and owner authorization values as well as objects created under the respective hierarchies |
| 5 TPM Clear Disable | 5 Disables the execution of tpm2_Clear() |
| 6 TPM Clear Enable | 6 Enables the execution of tpm2_Clear() |
| 7 Dictionary Attack Settings | 7 Configure failure tries allowed, recovery time and lockout recovery |
| 8 | 8 Start up the TPM |

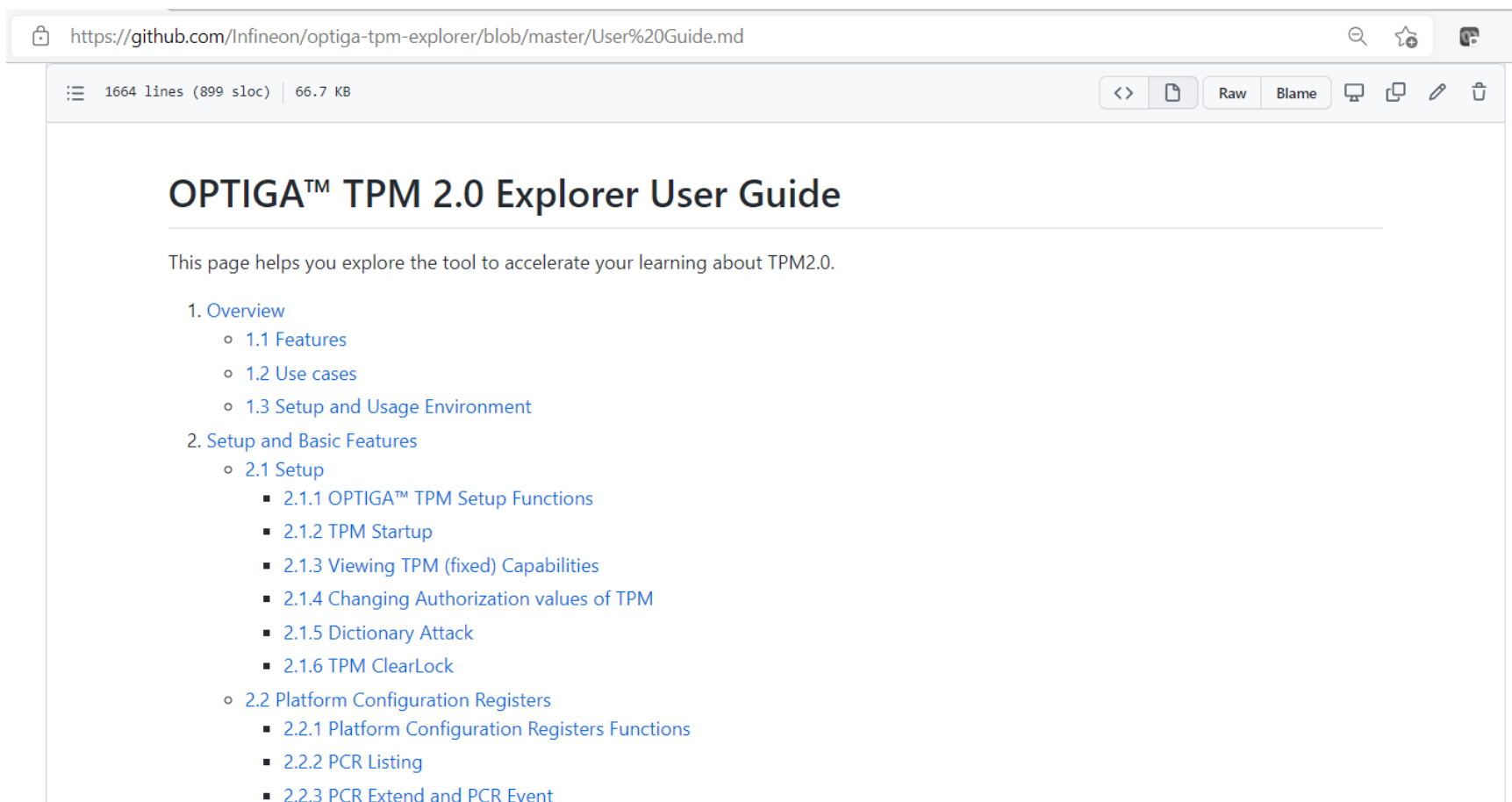
Easy to configure and read out

Easy to evaluate and study

Easy to understand security use cases

The beginner's guide to OPTIGA TPM2.0 Explorer

Learn more about the tool, how it works, and the functionalities of the OPTIGA™ TPM 2.0 by following graphical examples and simple step-by-step instructions on [Infineon GitHub repository](https://github.com/Infineon/optiga-tpm-explorer/blob/master/User%20Guide.md)

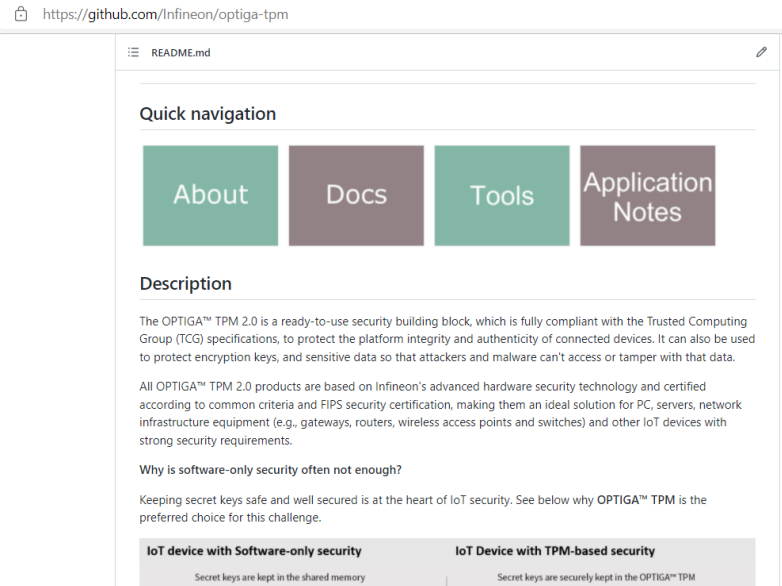


The screenshot shows a web browser displaying a GitHub repository page. The address bar shows the URL: <https://github.com/Infineon/optiga-tpm-explorer/blob/master/User%20Guide.md>. The page content includes a file size of 66.7 KB and 1664 lines (899 sloc). The main heading is "OPTIGA™ TPM 2.0 Explorer User Guide". Below the heading, there is a brief introduction: "This page helps you explore the tool to accelerate your learning about TPM2.0." followed by a table of contents with the following structure:

- 1. Overview
 - 1.1 Features
 - 1.2 Use cases
 - 1.3 Setup and Usage Environment
- 2. Setup and Basic Features
 - 2.1 Setup
 - 2.1.1 OPTIGA™ TPM Setup Functions
 - 2.1.2 TPM Startup
 - 2.1.3 Viewing TPM (fixed) Capabilities
 - 2.1.4 Changing Authorization values of TPM
 - 2.1.5 Dictionary Attack
 - 2.1.6 TPM ClearLock
 - 2.2 Platform Configuration Registers
 - 2.2.1 Platform Configuration Registers Functions
 - 2.2.2 PCR Listing
 - 2.2.3 PCR Extend and PCR Event

The OPTIGA™ TPM is easily integrated thanks to easy-to-understand materials and sample codes on GitHub

OPTIGA™ TPM knowledge base



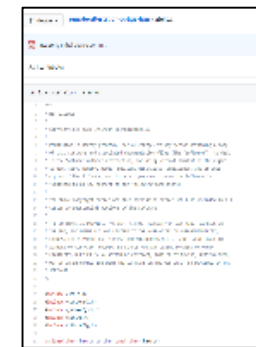
[OPTIGA™ TPM - Github link](https://github.com/Infineon/optiga-tpm)

Supported OPTIGA™ TPM common use cases

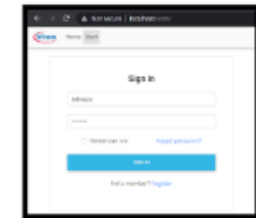
1. [AWS IoT Greengrass Hardware Security Integration](#)
2. [PKCS11 token creation](#)
3. [TPM-based remote attestation](#)
4. [TPM 2.0 integration for PSoC 6 Wi-Fi BT Prototyping Kit to enable TPM backed onboarding to AWS IoT Core](#)
5. [TPM 2.0 used with EK based onboarding](#)
6. [TPM 2.0 backed Linux Trusted and Encrypted Keys](#)
7. [TPM 2.0 in U-Boot on Raspberry Pi 4](#)
8. [Extend measurements to TPM 2.0 PCR in U-Boot on Raspberry Pi 4](#)



Appnote doc



Sample code



EVAL SW

Ready-to-use code examples for common use cases

TPM remote attestation

- › Allow remote administrator to check devices for not being manipulated or tampered with.

EK-based device onboarding

- › Use EK for strong device identity verification and onboarding

Trusted & encrypted keys

- › Secured key handling on Linux

Secured key store thru PKCS11

- › Support the use of HSM (TPM 2.0) through PKCS11 interface for secured key storage

TPM2.0 for U-Boot

- › Extend critical measurements to PCR in TPM 2.0 before transitioning to Raspbian OS

PSOC Onboarding to AWS IoT Core

- › Support the use of TPM 2.0 to securely onboard to Infineon PSoC6 embedded platform

Your personal key takeaways



A simple GUI and ready-to-use code examples make TPM operations and implementations easy, even for first-time developers



Infineon provides easy-to-use security solutions to simplify your development journey



Infineon is the trusted advisor for IoT and networking security





Part of your life. Part of tomorrow.