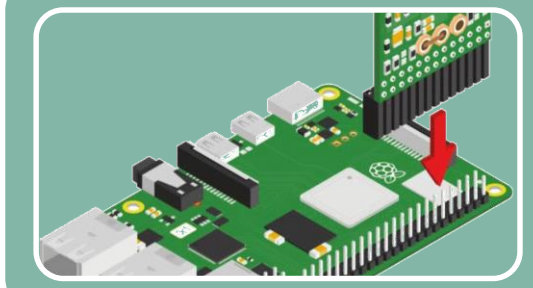
OPTIGA™ TPM2.0 solution:
Learn how Infineon is simplifying your IoT security

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.

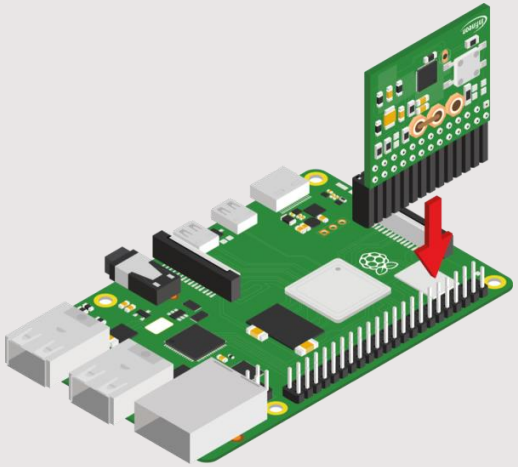
Ease of deployment and integration

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

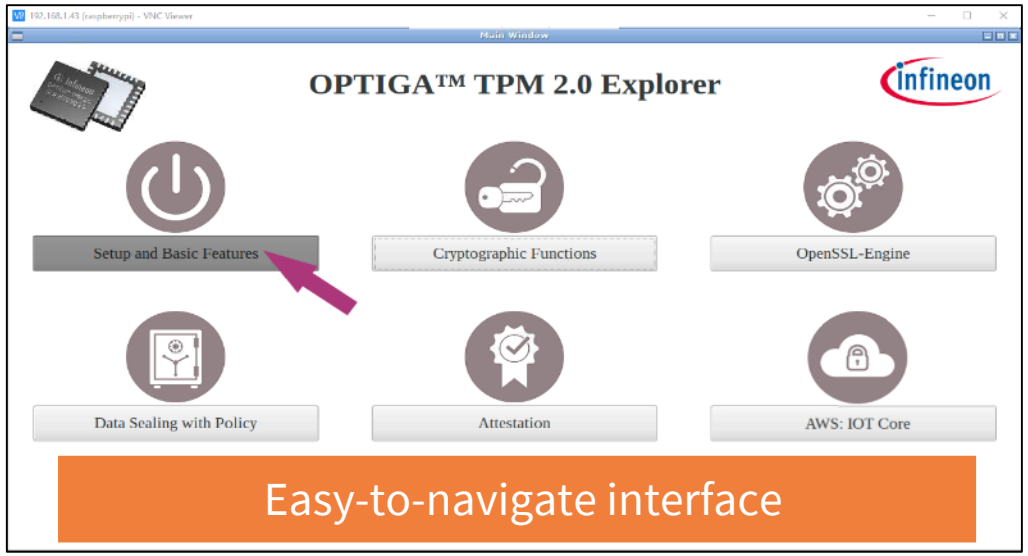
Control the RPI from you laptop without additional peripheral devices

OPTIGA TPM2.0 Explorer

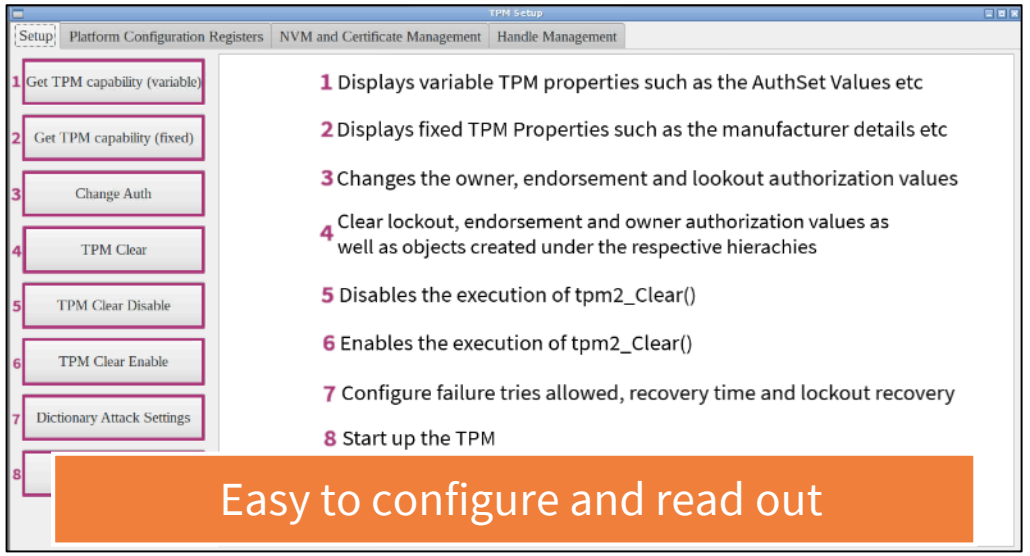
TPM is easy even for beginners with the help of GUI instead of CLI

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

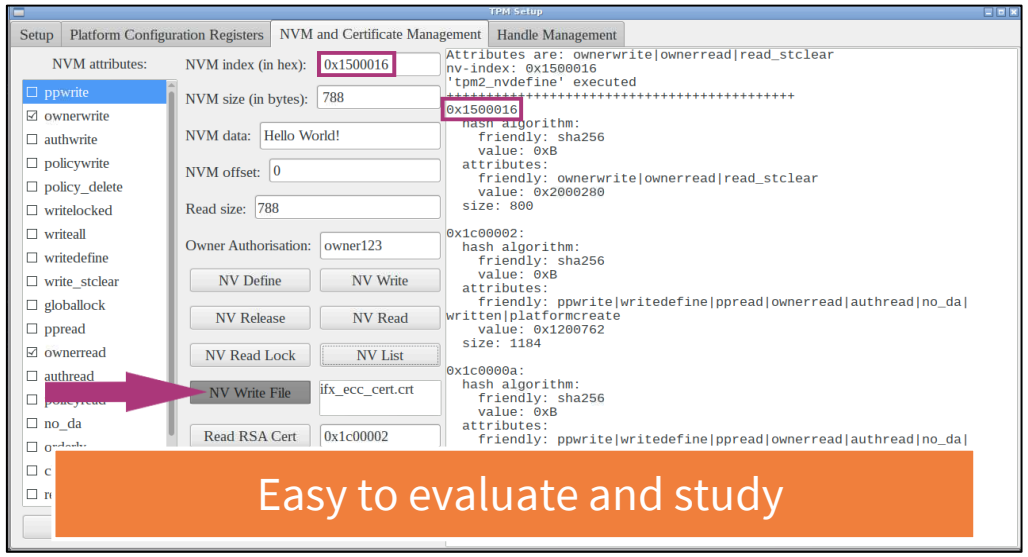
Making interfaces not just easy to use, but also easy to learn



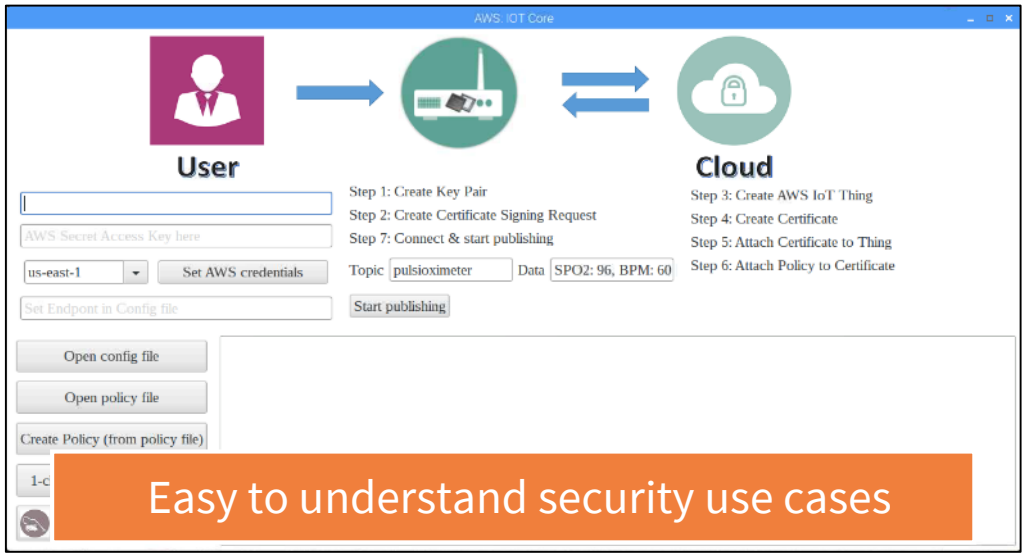
Easy-to-navigate interface



Easy to configure and read out



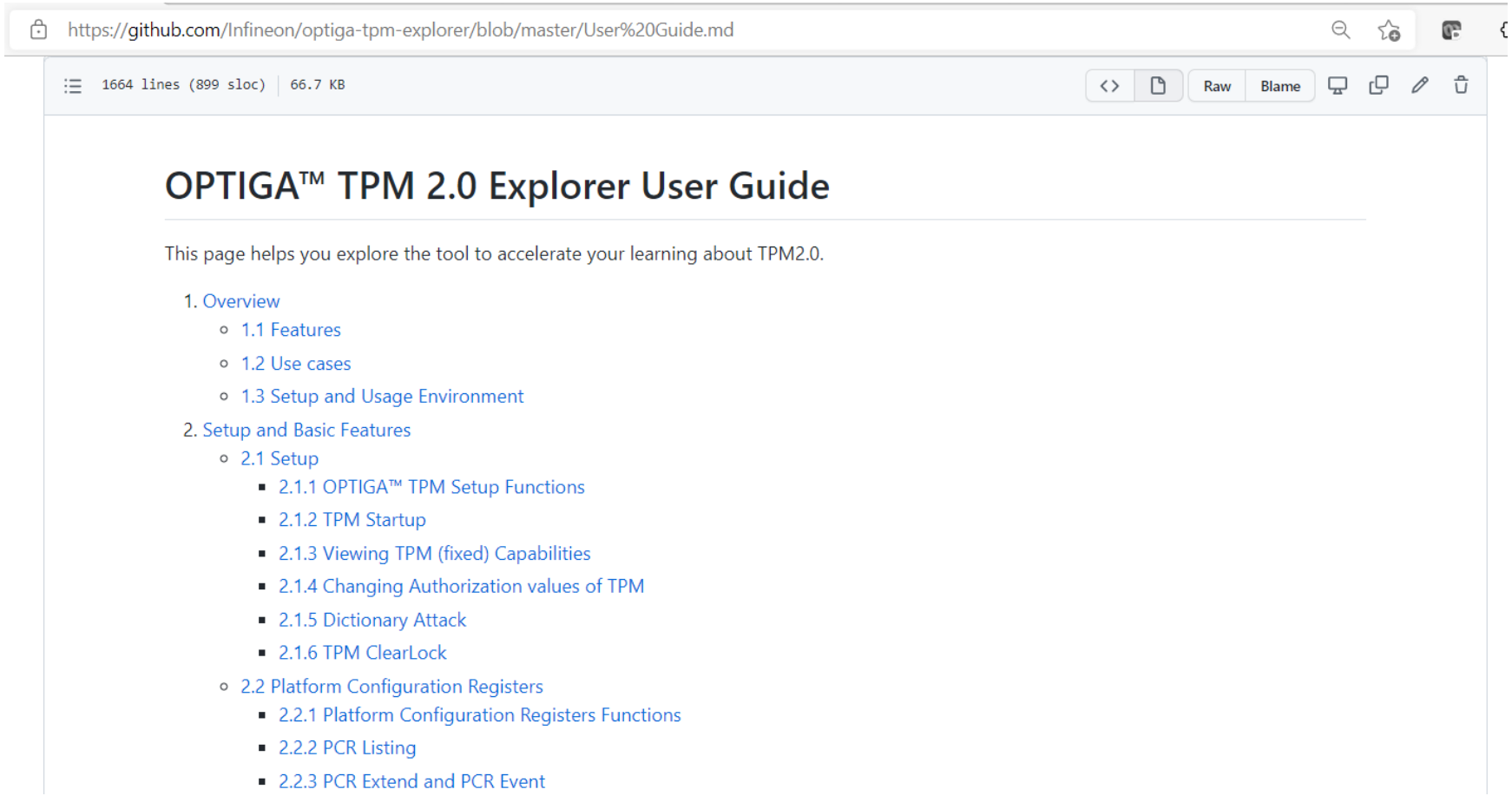
Easy to evaluate and study



Easy to understand security use cases

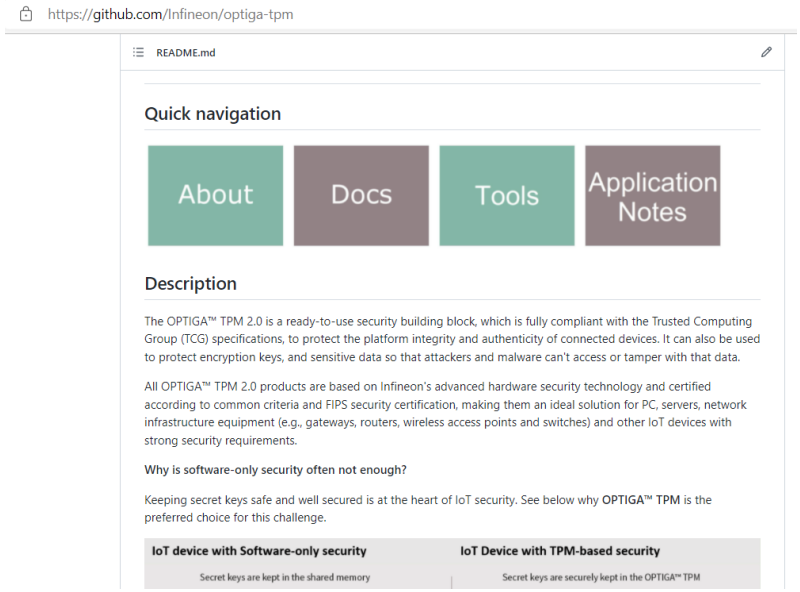
The beginner’s guide to OPTIGA TPM2.0 Explorer

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]



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]

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.