# OPTIGA™ TPM Demo User Manual

## Remote Attestation

26 Nov, 2020

Revision 1.0

www.infineon.com

# About this document

### Scope and purpose

The remote attestation demo shows how an OPTIGA™ TPM can be used to perform authentication and to protect the IMA measurement. This document describes how to and run the demo. For detailed setup guide please refer to the application note.

Remote attestation is a mechanism to enable a remote system (server) to determine the integrity of a platform of another system (Raspberry Pi®). In a Linux-based system, a security feature known as the Integrity Measurement Architecture (IMA) can be used to capture platform measurements. Together with TPM a hardware-based security and its set of attestation features, it can be used to perform authentication and to protect IMA measurements.

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

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. An overview of all Infineon OPTIGA™ TPM products can be found on Infineon's website [1][2]. More information on TPM specification can be found on Trusted Computing Group (TCG) in reference [3].

### 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 the implementation of TPM-based remote attestation for their target applications.

# Table of Contents

# 1 Prerequisites

For more information, including detailed setup guide, can be found in the OPTIGA™ TPM Application Note – Remote Attestation.

# 2 Operation Guide

This section describes all necessary steps to perform remote attestation.

| | |
|---|---|
| **Step 1** | Run Server. |
| **Step 2** | Provision TPM. |
| **Step 3** | Run Device Scripts. |

Table 1: Operation guide

## 2.1 Run Server

For better user experience and quicker response time, it is possible to host the server on a separate machine or remote server. The guide for server hosting is not covered in this document.

Run server on Raspberry Pi®:

```
$ cd ifx_tpmremoteattestation/server/target
$ sudo java -jar server-0.0.1-SNAPSHOT.jar
```

The server is ready for operation once you see the following message:

```
...
2020-06-10 22:37:51.856  INFO 12828 --- [           main]
o.s.m.s.b.SimpleBrokerMessageHandler     : Started.
2020-06-10 22:37:52.414  INFO 12828 --- [           main]
o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat started on port(s): 443
(https) 80 (http) with context path ''
2020-06-10 22:37:52.418  INFO 12828 --- [           main]
com.ifx.server.ServerApplication         : Started ServerApplication in 91.269
seconds (JVM running for 98.966)
```

View the webpage (https://localhost) using Raspberry Pi® OS built-in web browser. A warning message may appear, it is expected since server is using a self-signed certificate. Bypass the warning and proceed as usual. Slower loading time is expected on Raspberry Pi® 3.

### 5.1.1 Sign in Page

On the upper menu bar, click on “Start” to open the sign in page (Figure 1). Sign in using the following default user account to open a self-explanatory dashboard page.

| | |
|---|---|
| **Username** | infineon |
| **Password** | password |

Table 2: User account

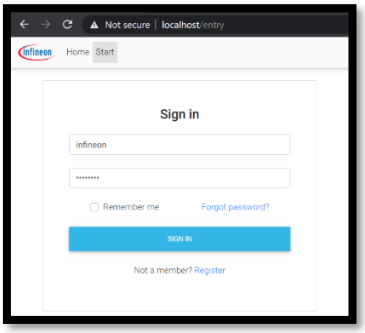


Figure 1: Sign in

### 5.1.2 Dashboard Page

The dashboard page comprises the following sections (Figure 2).

| | | |
|---|---|---|
| **Certificate Authority** | The Infineon root certificate. | |
| **Device** | The information of a connected device. | |
| | **EK Certificate** | An Infineon issued TPM certificate. |
| | **EK Verification** | TPM certificate verification. This is done by using Infineon root certificate. |
| | **AK Name** | The name (digest) of an Attestation Key. |
| | **AK Public Key** | The public information of an Attestation Key. |
| **Expected Platform Measurement** | The measurement of a good/healthy platform. | |
| | **SHA-1 PCR Bank** | TPM SHA-1 PCR bank indexes. |
| | **SHA-256 PCR Bank** | TPM SHA-256 PCR bank indexes. |
| | **Qualification Data** | A server generated random nonce to provide anti-replay protection. |
| | **PCR Values** | A list of PCR values. |
| | **Runtime Measurement List** | A list of measured files (IMA log) containing the file name, path, hash value, and which PCR it is extended to. |
| **Device Attestation** | This section contains a platform measurement (TPM quote, quote’s signature, and IMA log) and the outcome of verification. | |
| | **Compute** | Use a received IMA log only as a sorting reference to rearrange the expected IMA log before computing its digest. The digest is later used for verifying the quote’s PCRs digest. |
| | **Quote** | The breakdown of a quote. |
| | | **AK Name** — The name (digest) of a signing key. |
| | | **TPM Clock** — 64-bit value of time TPM has been powered on in millisecond. |

| | | | |
|---|---|---|---|
| | | **TPM Firmware Version** | Firmware version. |
| | | **Qualification Data** | A server generated random nonce to provide anti-replay protection. |
| | | **SHA-1 PCR Bank** | TPM SHA-1 PCR bank indexes. |
| | | **SHA-256 PCR Bank** | TPM SHA-256 PCR bank indexes. |
| | | **PCRs Digest** | A value obtained by hashing all PCR values together. |

Table 3: Dashboard

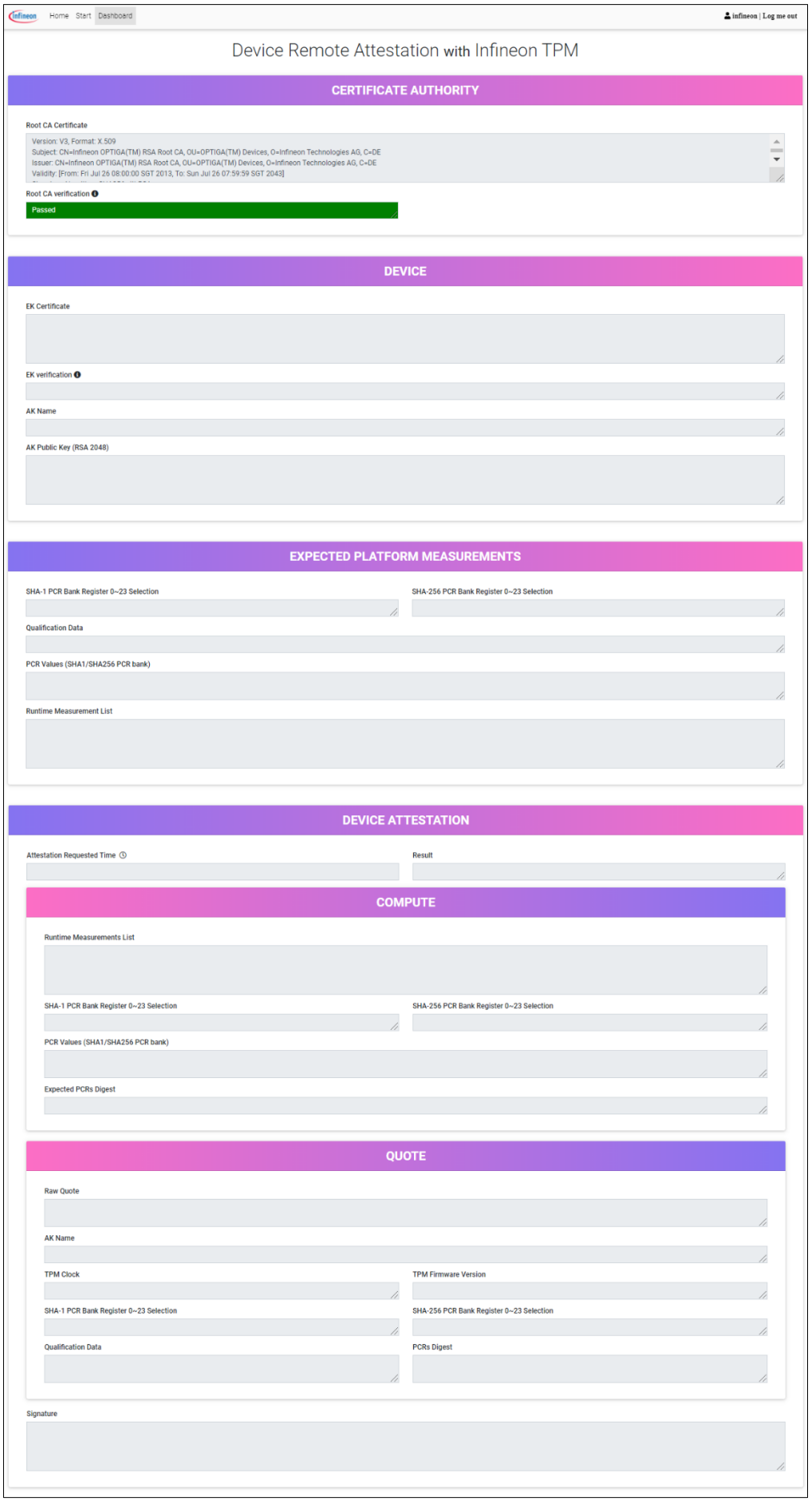


Figure 2: Dashboard

## 2.2 Provision TPM

Following steps are executed on Raspberry Pi®.

Perform a TPM clear on the platform hierarchy:

```
$ sudo chmod a+rw /dev/tpm0
$ sudo chmod a+rw /dev/tpmrm0
$ tpm2_clear -c p
```

Generate TCG profile compliant endorsement key (EK) and store it as persistent key:

```
$ tpm2_createek -G rsa -u ek.pub -c ek.ctx
$ tpm2_evictcontrol -C o -c ek.ctx 0x81010001
```

Generate attestation key (AK) and store it as persistent key:

```
$ tpm2_createak -C 0x81010001 -c ak.ctx -G rsa -g sha256 -s rsassa -u ak.pub -n
ak.name
$ tpm2_evictcontrol -C o -c ak.ctx 0x81000002
```

Verify generated keys by reading TPM persistent handles:

```
$ tpm2_getcap handles-persistent
-  0x81000002
-  0x81010001
```

## 2.3 Run Device Scripts

Navigate to directory:

```
$ cd ifx_tpmremoteattestation_client/
```

The *config.cfg* is a configuration file. View the file for more information.

Navigate to directory:

```
$ cd ifx_tpmremoteattestation_client/bin
```

Execute following scripts sequentially:

| | |
|---|---|
| **0_prep.sh** | Authorize non-privileged access to the TPM device node. |
| **1_cleanup.sh** | Erase non-essential files and restore *config.cfg*. |
| **2_pcr.sh** | Read TPM PCRs and the IMA log. |
| **3_attune.sh** | Register a good platform measurement to a server. |
| **4_atelic.sh** | Ask for a server encrypted challenge. |
| **5_credential.sh** | Decrypt the challenge using the tool *tpm2_activatecredential*. |
| **6_quote.sh** | Generate a quote and a signature using the tool *tpm2_quote*. Skip step **6_quote-bad.sh** if this script is executed. |
| **6_quote-bad.sh** | This is to trigger a failure using an invalid challenge. Skip **6_quote.sh** if this script is executed. |
| **7_attest.sh** | Send the quote, signature, and the latest IMA log to a server to perform attestation. |

Table 4: Device scripts

# References


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

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

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

# Revision history

| Page or Reference | Description of change |
|---|---|
| **Revision 1.0, 2020-11-26** | |
| | Initial Release |
| | |

**Infineon Technologies AG**

81726 Munich
Germany

Published by
Infineon Technologies AG