OPTIGA™ Trust M Family of Products: Frequently Asked Questions

By
Robert Rozario

This article answers some of the frequently asked questions about the OPTIGA™ Trust M family and product features evaluation. It also includes useful links to the software repositories, tools, and all relevant articles. Please note that for some articles, you may need to sign up for a myinfineon account or create developer community profile.

What software do I need to evaluate the product features?

Windows users, do the following:

1. Go to Infineon website and create a myinfineon account (top right). Link

2. Download the ModusToolbox™ Software.

You may also download the Tera Term, PuTTY, Angry IP Scanner, etc. based on your needs.

Where can I find the host library for OPTIGA™ Trust M?

Go to OPTIGA™ Trust M page and navigate to OPTIGA™ Trust **>>** Design resources >> Development Tools.

Where can I find Linux host library and examples for OPTIGA™ Trust M?

Go to OPTIGA™ Trust M Linux GitHub to access the library and all relevant documents.

Is there a guide on how to test the OPTIGA™ Trust M features using the OPTIGA™ Trust M IoT Kit?

Yes. Refer to OPTIGA™ Evaluation.

How can I write specific data and certificates in OPTIGA™ Trust M board from Windows machine for prototyping?

Utilize the MCU as a USB-I2C bridge and host side python library is used to access and read/write data and certificates in OPTIGA™ TRUST M. For more information, see OPTIGA™ Windows_Application_Guide.

I would like to test OPTIGA™ Trust M Linux Library. Can you provide some suggestions on a platform and setup?

Use OPTIGA™ Linux_Test_Library guide as a reference for testing OPTIGA™ Trust M Linux Library.

Do you have some example for verified boot implementation using OPTIGA™ Trust M?

Yes. Infineon have a partnership with Thistle, which brings a verified boot implementation to a Raspberry Pi. For more information, see OPTIGA™ Trust M_Verified_Boot.

Here is a detailed guide on how to implement verified boot using Thistle software and OPTIGA™ Trust M. Link

I want to provision my own AES key in OPTIGA™ Trust M. Is it Possible?

Yes. Here is an article that describes the protected update of AES key in OPTIGA™ Trust M. Link

Is there is a limitation on the file size for AES encryption?

Theoretically, there is no limit to the amount of data that can be AES (-CBC/-ECB) encrypted. The length of the input data per command must be block size (16 byte) aligned with the AES Key being used (with a max. payload length per command = 255 bytes). Eventually, you would run into the security monitor throttling the encryption performance, as each 'Symmetric Encrypt' command issues a 'key usage' security event. Throttling starts at 128 events and becomes worst at 255 events. With those constraints (15x16 bytes per command) x 128 commands, you could encrypt ~30 kB of data before encountering performance throttling.

References

- OPTIGA™ Trust M SLS32AIA