OPTIGA™ Trust M MTR

User guide

About this document

Scope and purpose

The scope of this document is to guide the users to evaluate the OPTIGA™ Trust M MTR.

Intended audience

This document is primarily intended for solution providers and system integrators.

Table of contents

List of figures

1 Introduction

To make Smart Home devices secure, reliable, and interoperable, the Connectivity Standards Alliance (CSA) came up with a new standard called Matter. This specification is supported by more than six hundred organizations including all the major Original Equipment Manufacturer (OEMs) and device manufacturers.

One of the key goals of CSA with the Matter specification is to evoke the trust in the mind of end consumer to mix and match smart home devices from multiple vendors while ensuring privacy, security, and seamless experience. This will enhance user confidence, simplify the adoption process, and stimulate market growth for both consumers and stakeholders.

Security is the primary requirement for Matter, when we mix and match devices from various vendors, we need to ensure each of them adhere to the stringent security requirement laid out by CSA in the Matter specification. To address the security concerns for Matter development we have our new offering OPTIGA™ Trust M MTR to provide the easiest way to add Matter security to your applications.

This User Guide covers all the steps required to evaluate the OPTIGA™ Trust M MTR. In case of any queries please reach out to us on the Infineon Developer Community.

2 How to evaluate OPTIGA™ Trust M MTR

There are multiple stages to evaluate the OPTIGA™ Trust M MTR, first stage is to prepare the setup, the second stage is to download the Device Attestation Certificate (DAC) and to evaluate the Matter device.

2.1 Prepare the setup

Hardware requirements

- PSoC™ 62S2 Wi-Fi BT Pioneer Kit (CY8CKIT-062S2-43012)
- OPTIGA™ Trust Adapter
- OPTIGA™ Trust M MTR Shield
- Matter Hub (for example Apple Homepod, Google Nest, etc.)
- Matter Controller (must match the selected Matter Hub, for example Apple iPhone, Android Smartphone)

Evaluation flow

Steps

1. Register and get a myInfineon account using your email, to access the relevant collateral and tools to evaluate OPTIGA™ Trust M MTR.
2. Once registered, get yourself an OPTIGA™ Trust M MTR kit from here. You will need to buy three separate pieces of hardware:
   a. PSoC™ 62S2 Wi-Fi BT Pioneer Kit
   b. OPTIGA™ Trust Adapter
   c. OPTIGA™ Trust M MTR Shield
3. Follow the guide here, to get started with the kit:
   a. Download and install ModusToolbox™ (MTB) Software, Infineon's development environment to be able to flash the kit
   b. Download the attach chip-psoc6-lock-example.hex hex-file (right-click and Save as...) from GitHub
   c. Connect the OPTIGA™ Trust M MTR Shield using the OPTIGA™ Trust Adapter
   d. Program the PSoC™62 EVM with the provided OpenOCD Command as described in GitHub
   e. Experience the Matter Demonstration

After the initial Get-Started Experience, the next step is to start developing your own application. Head over to the Matter SDK on GitHub and set up your development environment. You will find the OPTIGA™ Trust M MTR as a supported HSM and can integrate this into your device (Direct link for Matter SDK v1.1).

2.2 Download the Device Attestation Certificate

It is time to download the Device Attestation Certification (DAC) to evaluate your first Matter solution.

Steps

1. Go to the OPTIGA™ Trust M MTR product page.
2. Now go to the Infineon's Online Services Tools & Software (OSTS) website here
3. Login to the OSTS website using your myInfineon login credentials

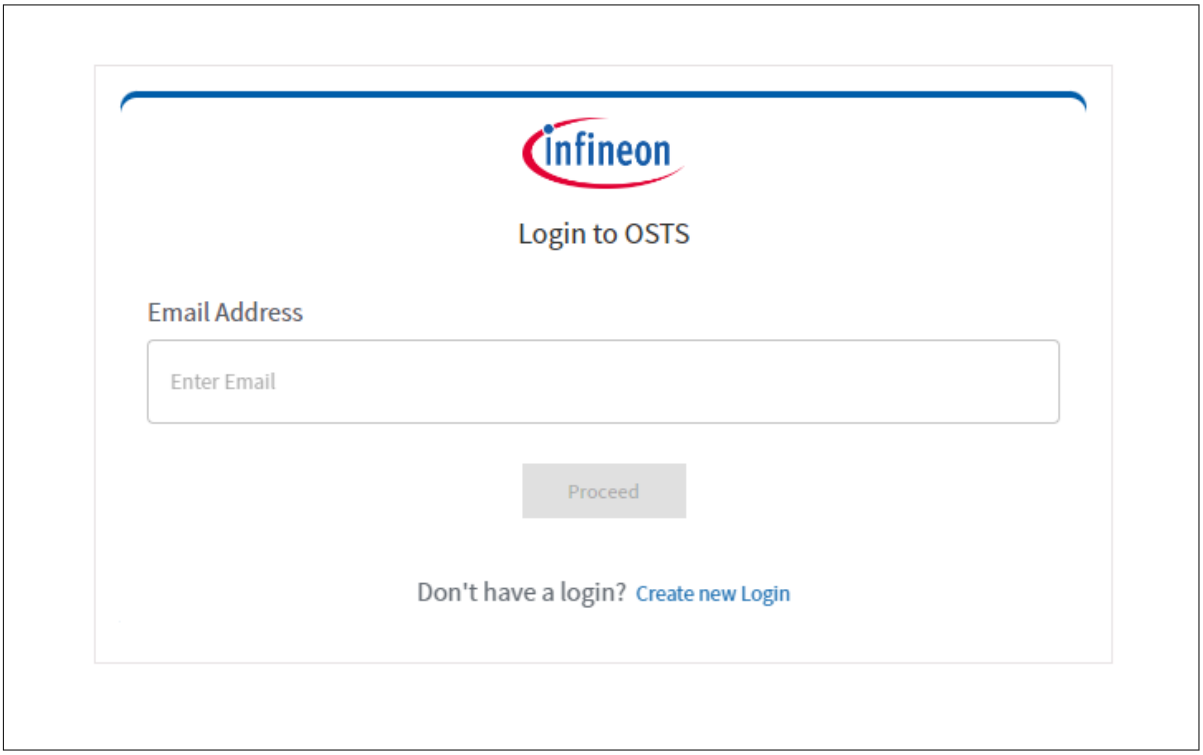

Figure 1 Login screen of OSTS webpage

4. During the first login, fill in the name of your company and choose the suitable role (please choose "Developer" for now to evaluate the OPTIGA™ Trust M MTR) and click ***Submit*** (Figure 2). Based on your chosen role, the OSTS webpage will have a customized options available to suit your needs. There are multiple other roles too like Admin etc but those are meant for production runs.

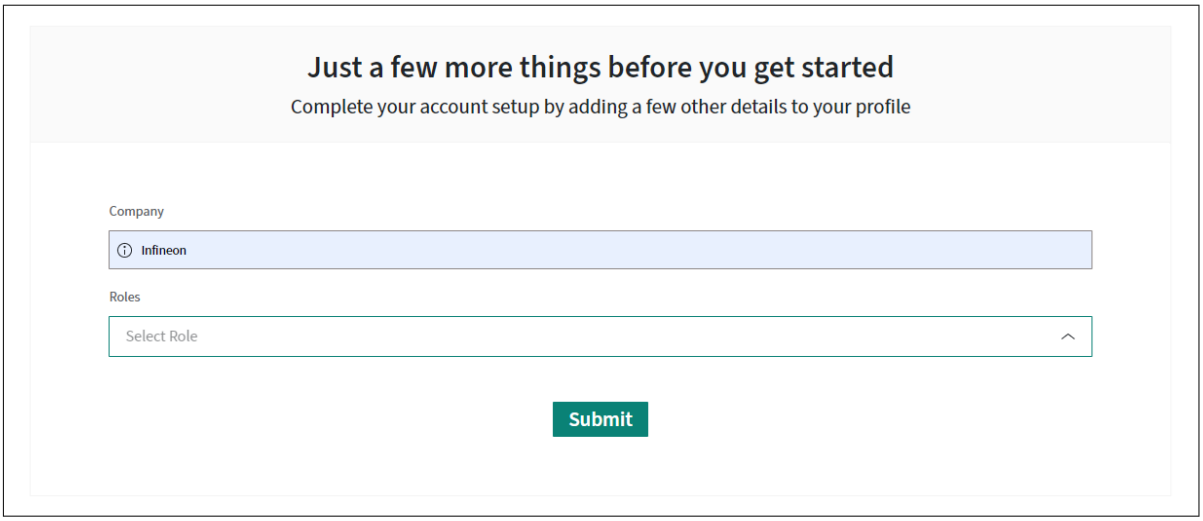

Figure 2 Login questions

5. After logging in you will see the main page (Figure 3), you can find all the related information and collateral's here on this page.

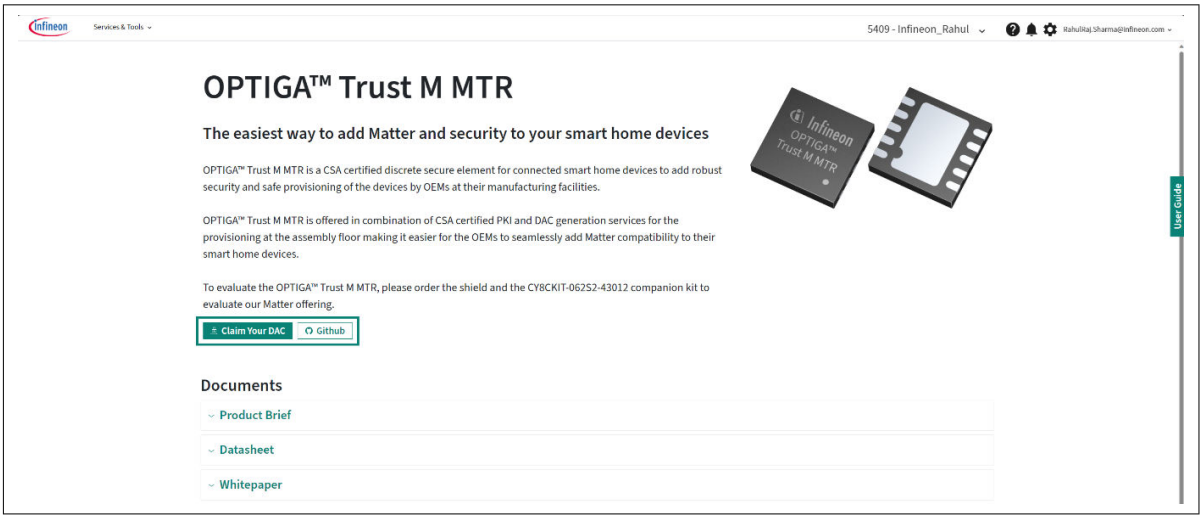

Figure 3 OPTIGA™ Trust M MTR OSTS webpage

6. You can click on the GitHub button to go to the main GitHub page, which will guide you to download all the related projects and scripts/tools.

7. Once your setup is ready, you can click on the "Claim Your DAC" button to download the device specific DAC for your system.

8. Infineon has partnered with Kudelski S.A. who acts as a CSA certified Product Attestation Authority (PAA) to generate and provide Matter DACs. All the unique DACs for each of the test sample and for the production devices will be generated by Kudelski's keySTREAM portal, and hence when the user clicks on the "Claim Your DAC" button, the user is re-directed to Kudelski's webpage to generate and download the unique DACs[1)]. Infineon provides a pop-up to inform the user that the user is getting redirected to the Kudelski's servers. When the user goes to the Kudelski's site for the first time he's asked to agree to the Privacy Policy and Terms & Conditions (Figure 4) which governs Kudelski's website. This is required to be done only once, as second time onwards the redirection will directly take the user to the DAC download page.

1 Users don't have to create a separate account with Kudelski for the evaluation of samples and shields. For the evaluation purposes, all the details are shared from the Infineon's website to the Kudelski's website

Figure 4 First re-direction to the Kudelski's webpage

9. Accept both the Privacy Policy and the Terms & Conditions on this page and click “Next” to go to the DAC Download page (Figure 5).

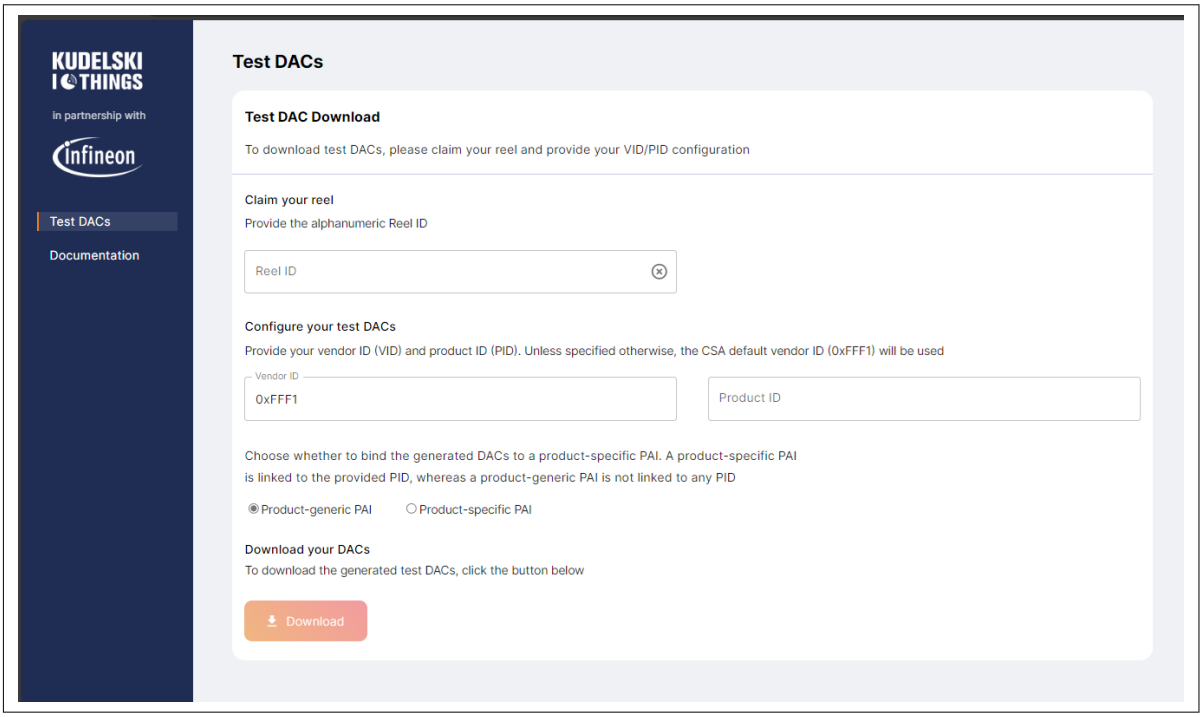

Figure 5 DAC download page

10. On the DAC Download page, user can enter Vendor ID (VID) if available, or else the tool automatically picks up the default test VID (0xFFF1).

11. Optionally, Product ID (PID) can be entered if available or can be left blank.

12. Lastly, the Reel ID (RID) should be entered, which is available on the shield box.

13. Once all the above details are entered, the user can download the test DAC[2)].

[2] Please note that the process to download DACs for the production run will be different from the process mentioned in this User Guide

14. This test DAC can be injected to the sample devices or the shield using the injection script to evaluate the Matter solution. The guidance to get started can be found here

3 How to get Production DACs for OPTIGA™ Trust M MTR

Once the evaluation is done and a product is planned to move to production then there are different requirements to get the production DAC. Following are the steps you need to follow before you can download the production DAC.

- Register with CSA and become a CSA member to get the unique Vendor ID or VID
- Register your product with CSA to get a Product ID or PID
- Register with Kudelski and follow the required vetting process to get a production account
- Once you have a production account then you can download the production DACs during the assembly of the end products using the Web UI or APIs
- A detailed guide will be provided once the client is vetted by Kudelski, and is moving to production

Revision history

Reference	Description
Revision 1.0, 2024-02-21	
	First release

Trademarks

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

Edition 2024-02-21

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about any aspect of this document?

Email:
CSSCustomerService@infineon.com

Document reference
IFX-dic1706173841858

Important notice

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenheitsgarantie").

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer's compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer's products and any use of the product of Infineon Technologies in customer's applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

Warnings

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.