OPTIGA™ Trust M MTR Production Flow

User guide

Document release reference: Z8F80754836-A

About this document

Scope and purpose

The scope of this document is to guide the users to setting up account with Kudelski IoT KeySTREAM™ portal and production DACs for OPTIGA™ Trust M MTR.

Intended audience

This document is primarily intended for use by the customers.

Table of contents

About this document 1
Table of contents 2
List of figures 3
1 Introduction 4
2 Steps to go to production with OPTIGA™ Trust M MTR 5
3 Setting up an account with Kudelski IoT KeySTREAM™ 6
4 Process to download the production DACs 10
5 Summary 12
Glossary 13
Revision history 14
Disclaimer 15

List of figures

Figure 1 Process to setup production account with Kudelski 5
Figure 2 How to start the process to get the production account 6
Figure 3 Signing NDA 6
Figure 4 Email to review and sign the NDA 7
Figure 5 NDA under review by Kudelski 7
Figure 6 Account setup 8
Figure 7 Provide details to create a production account 8
Figure 8 Provide PAI details 8
Figure 9 Kudelski reviewing the contract 9
Figure 10 Account setup and activation done 9
Figure 11 Claiming the reel 10
Figure 12 Provide details to claim a reel 10
Figure 13 Systems tab 11
Figure 14 Click on the download to get the DACs 11
Figure 15 Complete process to get the production DACs 12

1 Introduction

Today's smart home devices are ubiquitous and there are multiple ecosystems driving these smart home devices. With the proliferation of multiple ecosystems, users are confused about whether the new smart home device works with the ecosystem at their home and how secure the device will be.

To solve this, the Connectivity Standards Alliance (CSA) developed a new standard called Matter. Matter not only ensures that the devices are highly secure, but it also enables cross-ecosystem compatibility and gives peace of mind to the user.

The Matter logo on the box of a consumer product tells a customer that they can mix and match any set of smart home devices without any concerns about compatibility and security.

This user guide is aimed at developers and engineers who are using OPTIGA™ Trust M MTR to add Matter compatibility to their design. The steps to evaluate and test OPTIGA™ Trust M MTR are already covered in the User Guide. This guide outlines the steps to be taken when transitioning to a mass production environment. In case of any queries please reach out to Infineon Developer Community.

2 Steps to go to production with OPTIGA™ Trust M MTR

Following the evaluation phase, a customer-Kudelski non-disclosure agreement (NDA) and contract are required to move to production. Both documents govern the customer's use of Kudelski's Product Attestation Authority (PAA) services.

The below steps need to be followed to go to production:

1. Become a CSA member

The CSA is a governing body that is developing, promoting, and certifying (amongst others) the Matter smart home standard. The customer needs to be a CSA member to go into production with any end equipment compliant with Matter. Obtaining a unique Vendor Identification (VID) through a CSA membership is a mandatory requirement, essential for multiple stages of the process, including onboarding with Kudelski, acquiring Device Attestation Certificates (DAC), and ultimately, achieving certification.

2. Sign an NDA with Kudelski

An NDA is required to start production onboarding of customers on the Kudelski portal.

3. Setup an account with Kudelski

After an NDA you need to provide all the information required on the Kudelski portal for setting up your account. This will allow Kudelski to vet the customer as required by CSA and create an account to download production DACs (refer to Figure 1 for a pictorial representation of the process, more information is also given in Chapter 3).

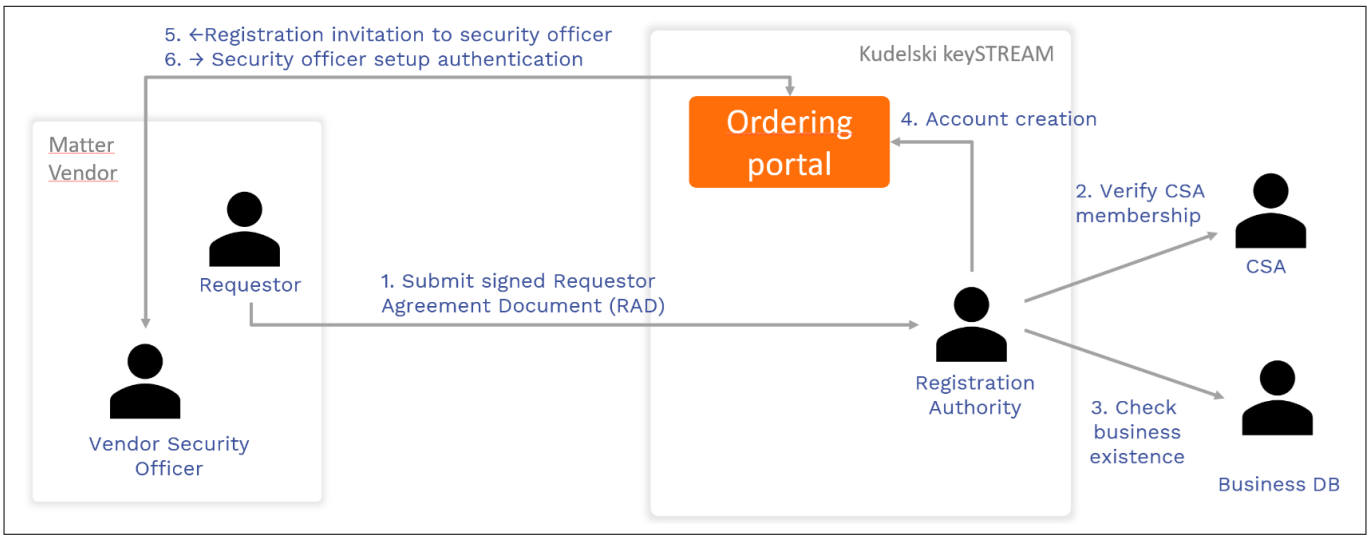

Figure 1 Process to setup production account with Kudelski

4. Sign a contract with Kudelski

Once the account setup is completed, sign the final contract with Kudelski. After that, the customer's account will be activated to download the production DACs.

5. Appoint a security officer

A security officer is required to coordinate between Kudelski and the customer. The security officer is responsible for the communication, sharing of keys and certificates, and other security-related tasks. A security officer ensures that the entire system remains secure by following all the best practices and auditing the systems and procedures to find any vulnerabilities.

3 Setting up an account with Kudelski IoT KeySTREAM™

To initiate the production process, you need to complete the necessary legal agreements and setup steps with Kudelski and the CSA. This section guides you through the process of signing the Non-Disclosure Agreement (NDA), contract, and creating a Product Attestation Intermediate (PAI) to obtain a Certification Declaration (CD) and ultimately download production DACs.

1. Go to the Kudelski Dashboard and click on the “Continue” button on the Production Setup box

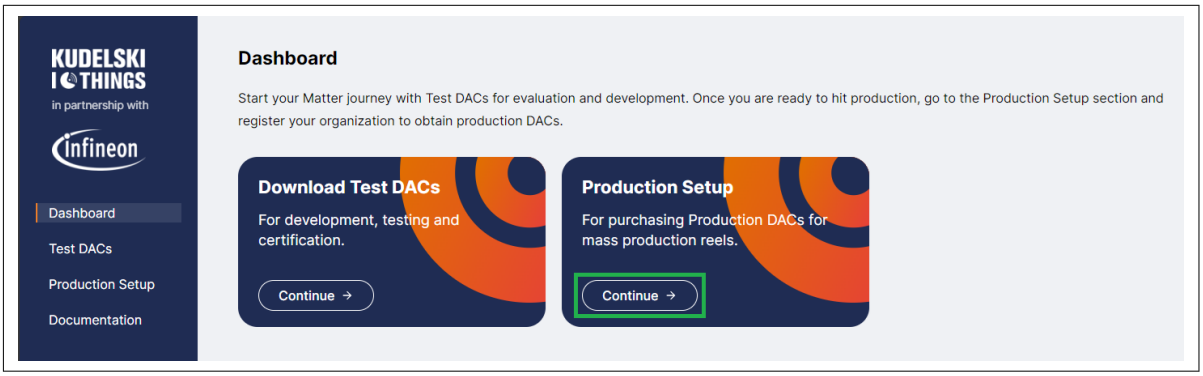

Figure 2 How to start the process to get the production account

2. Once the Continue button is clicked, an NDA form needs to be signed. Click on the “Sign NDA” button and the status will change to “Awaiting Signature”. This NDA is signed between Kudelski and the customer

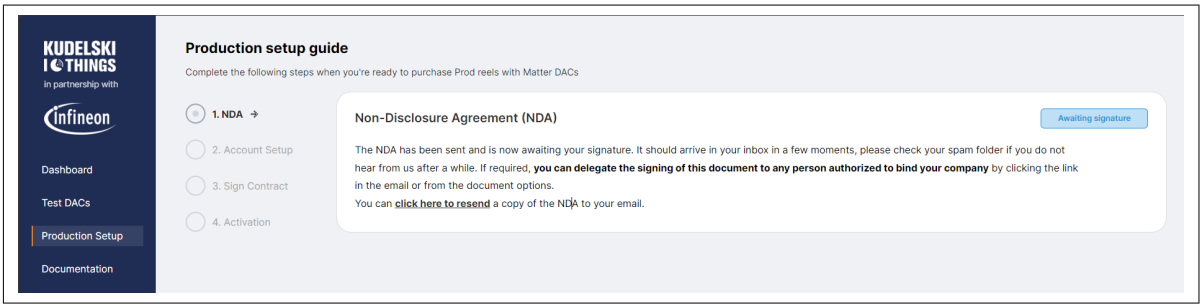

Figure 3 Signing NDA

3. Customer will receive an email from Kudelski with the NDA form, click on “Review and sign” it will open the NDA form, fill the details and click submit

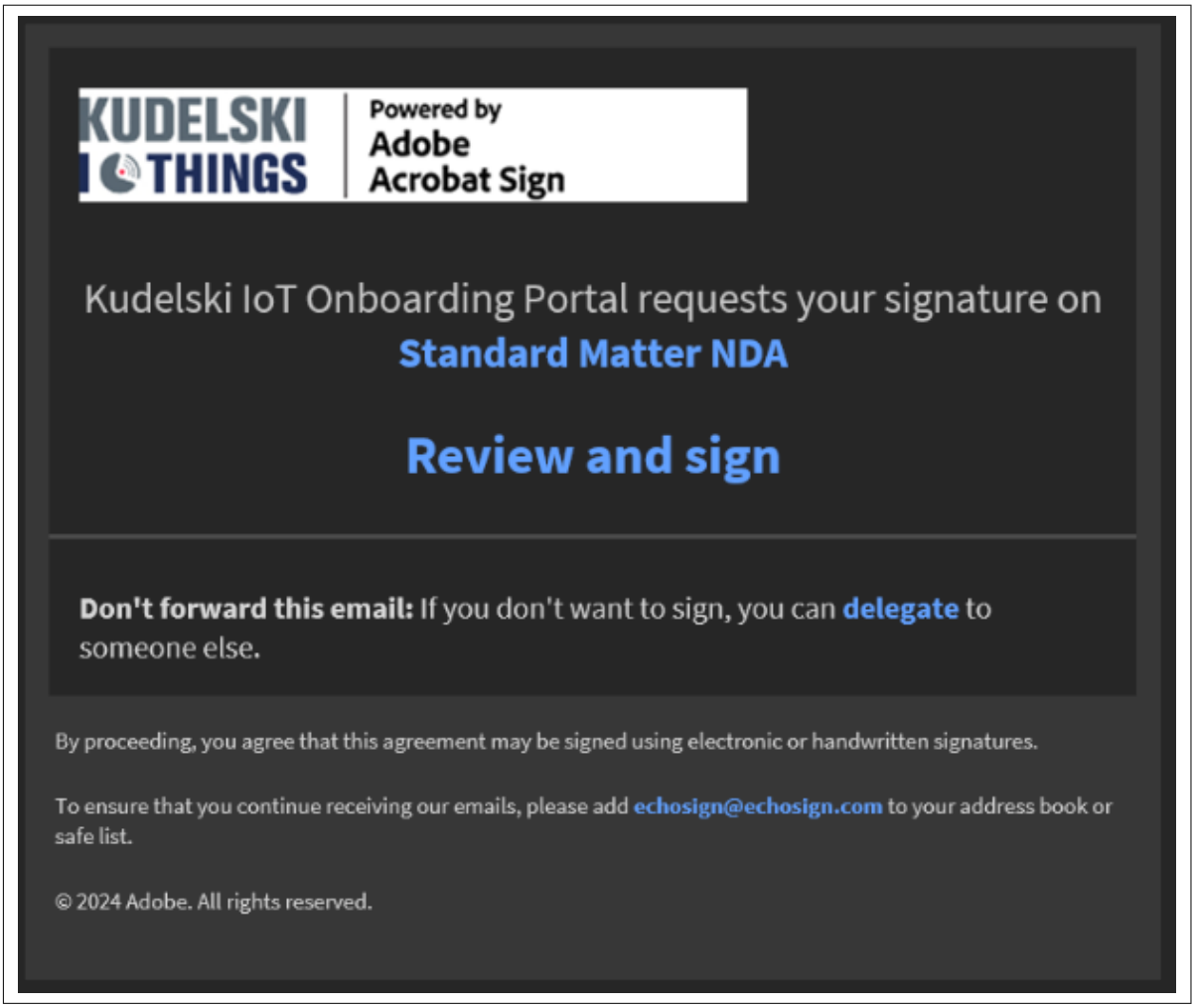

Figure 4 Email to review and sign the NDA

4. Once the NDA is signed, the form will go into “In Review” mode. At this stage, the form is with Kudelski to review and sign the form

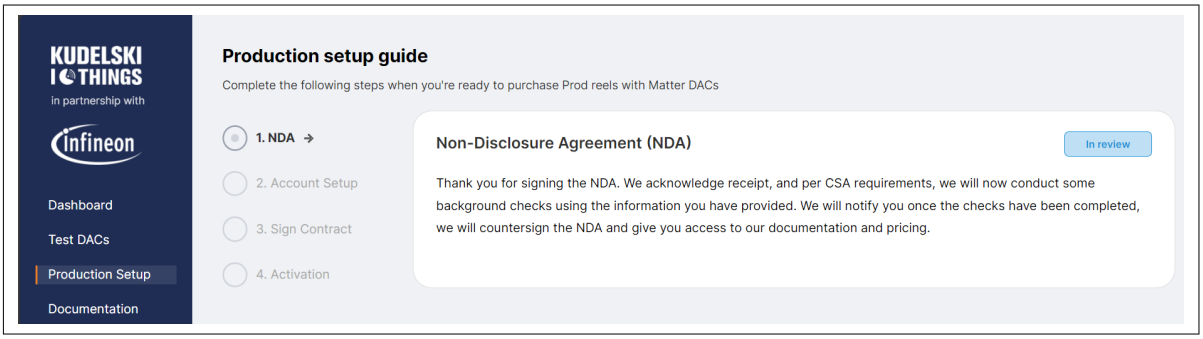

Figure 5 NDA under review by Kudelski

5. When the NDA is reviewed and signed by Kudelski, it will be sent back to the customer for counter signature. The status will be shown as “Awaiting”
6. After completing step 5, the account will go into the “Access pending” mode. The customer can go to “Account Setup” and initiate the setup of the account once access is granted
7. On the account setup page, click on the “Start Account Setup” button

3 Setting up an account with Kudelski IoT KeySTREAM™

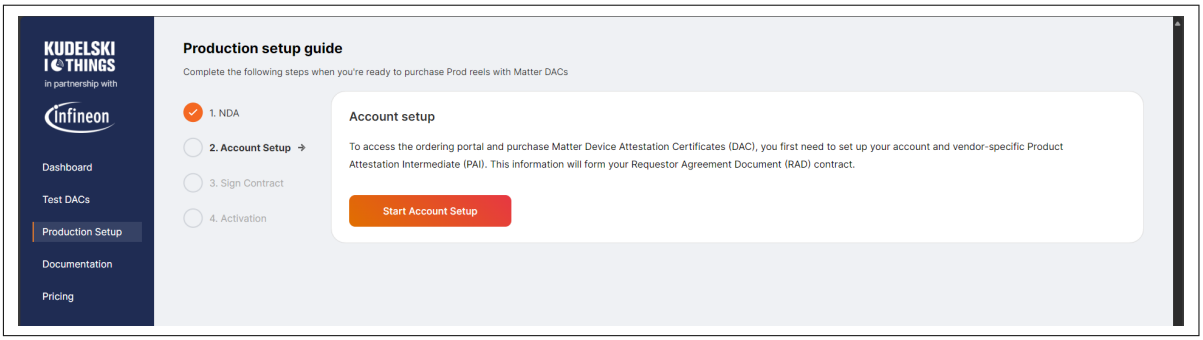

Figure 6 Account setup

8. Fill all the required details on the next page and click on the “Next” button

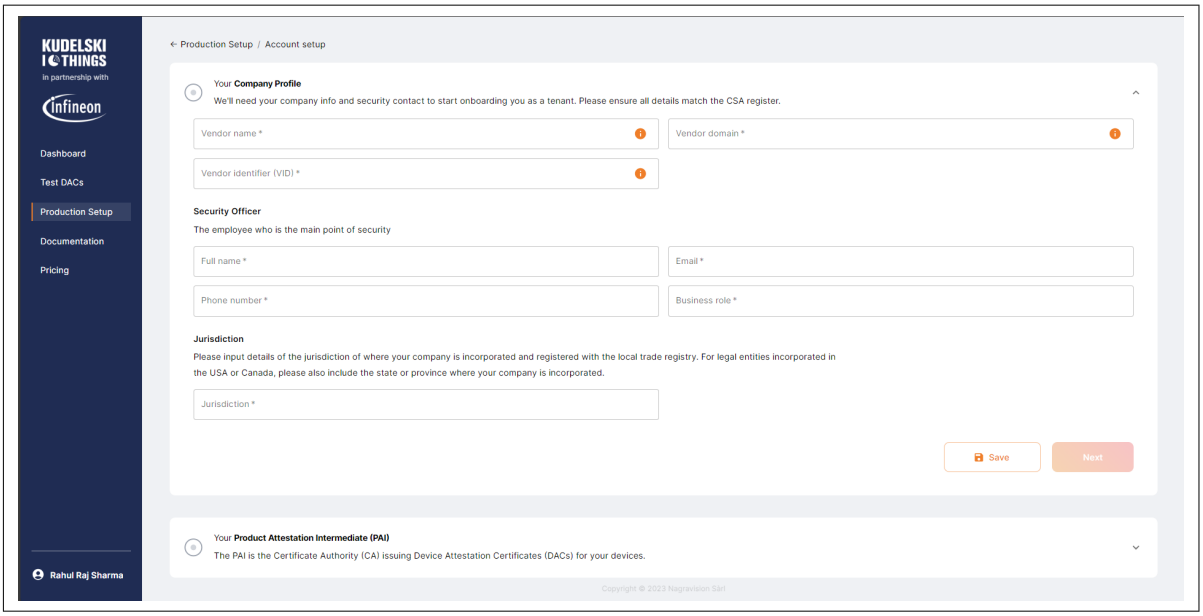

Figure 7 Provide details to create a production account

9. Fill all the required details on this page and click on the “Review and submit” button

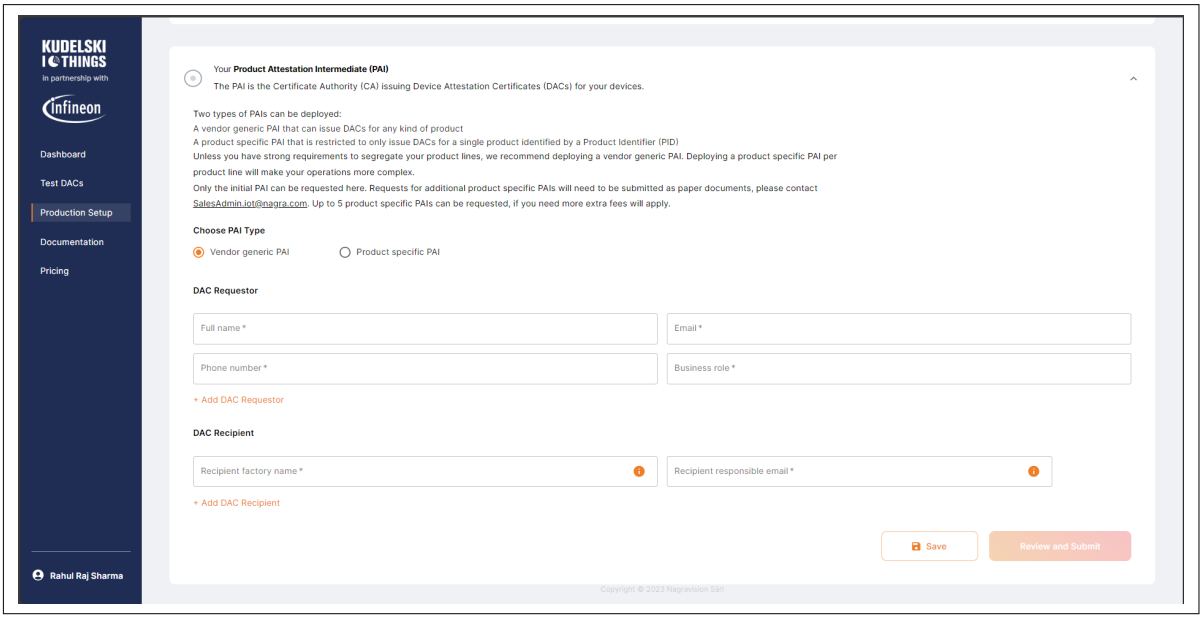

Figure 8 Provide PAI details

10. Customer will receive the contract on their registered email ID, this contract needs to be signed by the customer
11. Once signed, the contract will go back to Kudelski for review

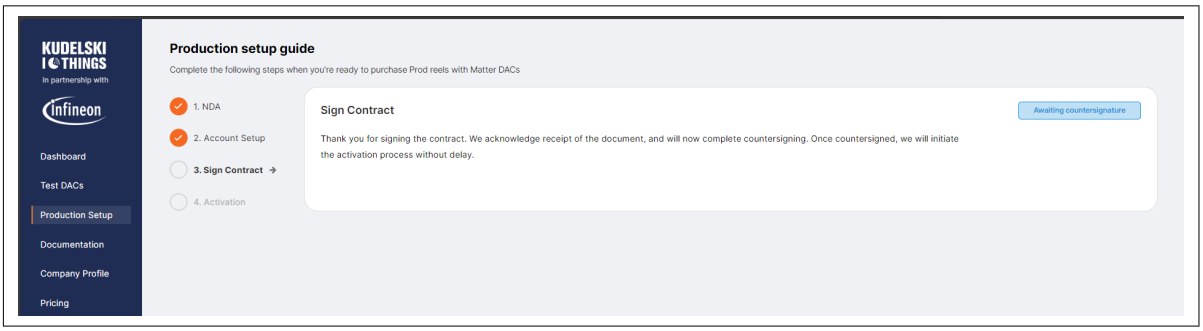

Figure 9 Kudelski reviewing the contract

12. The next step will be activation, this will be done by Kudelski to enable the customer to download the production DACs

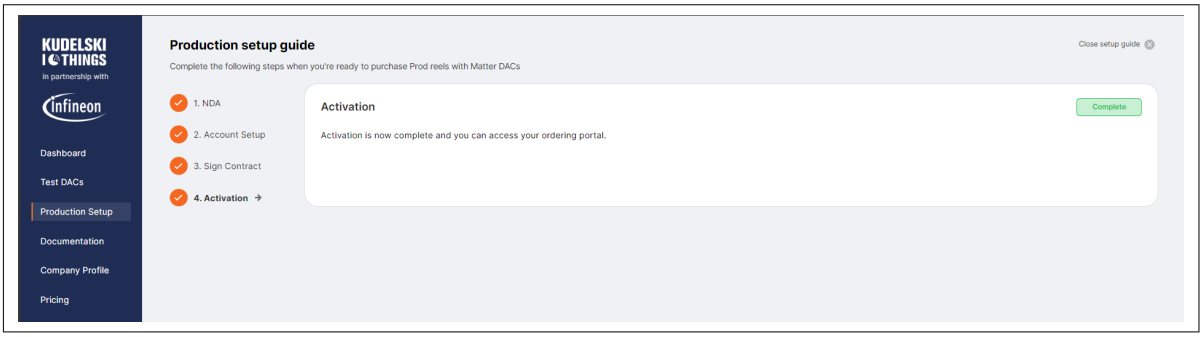

Figure 10 Account setup and activation done

13. Upon activation, proceed to the Kudelski IoT KeySTREAM™ portal to configure the Product Attestation Intermediate (PAI) and submit a request to Kudelski, which will facilitate the creation of the specified PAI
14. After the Product Attestation Intermediate (PAI) is created, the customer must submit a request to the CSA to generate a Certification Declaration (CD)

4 Process to download the production DACs

The Kudelski will send log in details with all the required information once the account is activated.

Follow the below steps to download the DACs from Kudelski IoT KeySTREAM™ portal:

1. Using the log in credentials, customer can log in to the production environment of Kudelski directly, the production environment does not require users to use the Infineon OSTS platform to log in to the Kudelski portal

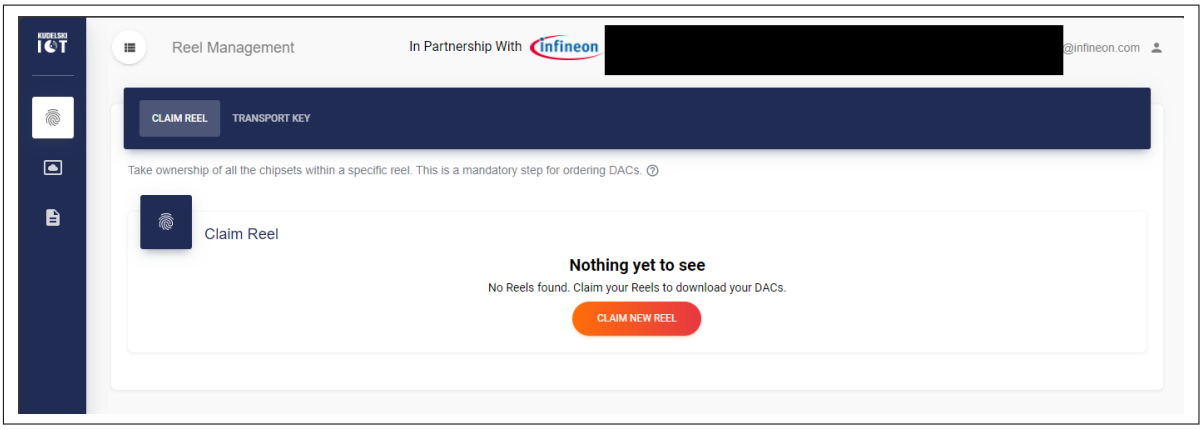

Figure 11 Claiming the reel

2. Now click on the “CLAIM NEW REEL” button to claim the reels of OPTIGA™ Trust M MTR. Once this button is clicked it will open a pop-up asking for more information about the reel

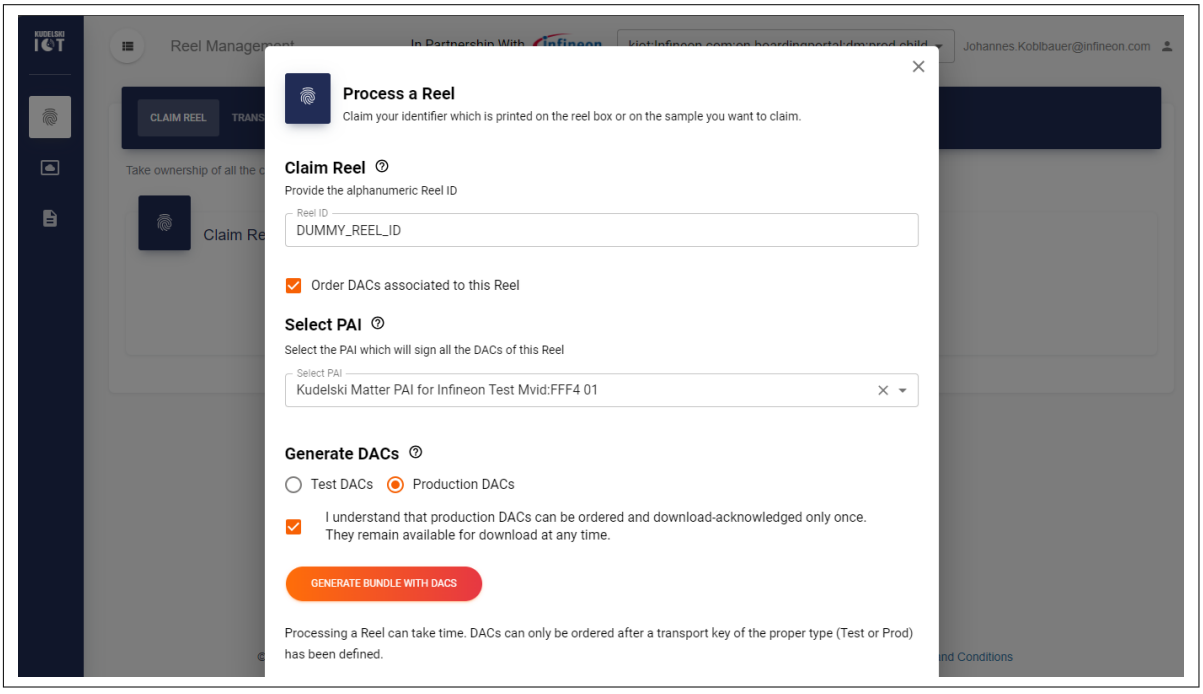

Figure 12 Provide details to claim a reel

3. Fill the Reel ID and select relevant options and click on the “GENERATE BUNDLE WITH DACS” button to download the bundle file for the given reel. Each bundle file will contain at least 4,000 unique DACs
4. These DACs can be injected using the injection script which runs on Linux. Please follow the guide available on the GitHub page “OPTIGA™ Trust M MTR: Matter Provisioning”, to inject the Matter DACs into the devices using a Raspberry Pi 4. The script here needs to be suitable and accordingly modified to run on the manufacturing setup to inject the DACs during the final assembly of the end products
5. To track the usage, customer can go to the “System” tab to see the list of claimed Reels

4 Process to download the production DACs

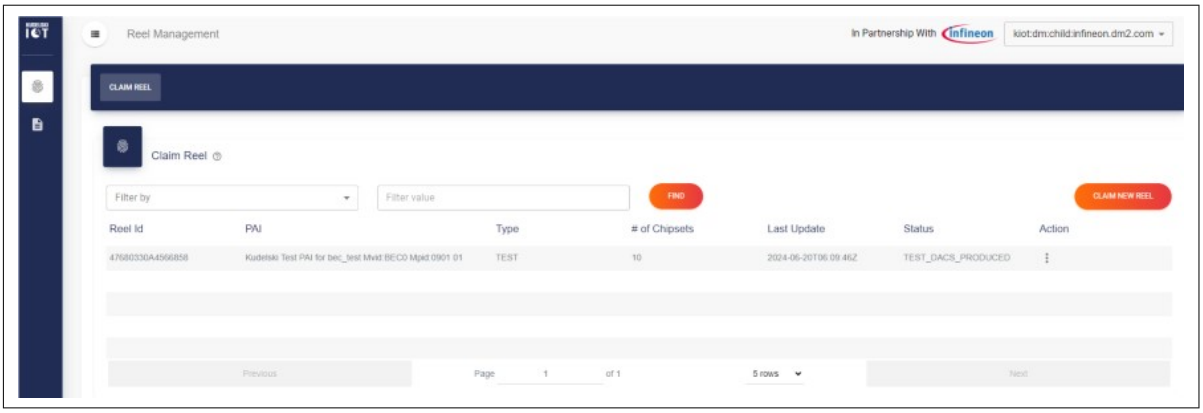

Figure 13 Systems tab

6. Click on the “Action” menu to download the DACs

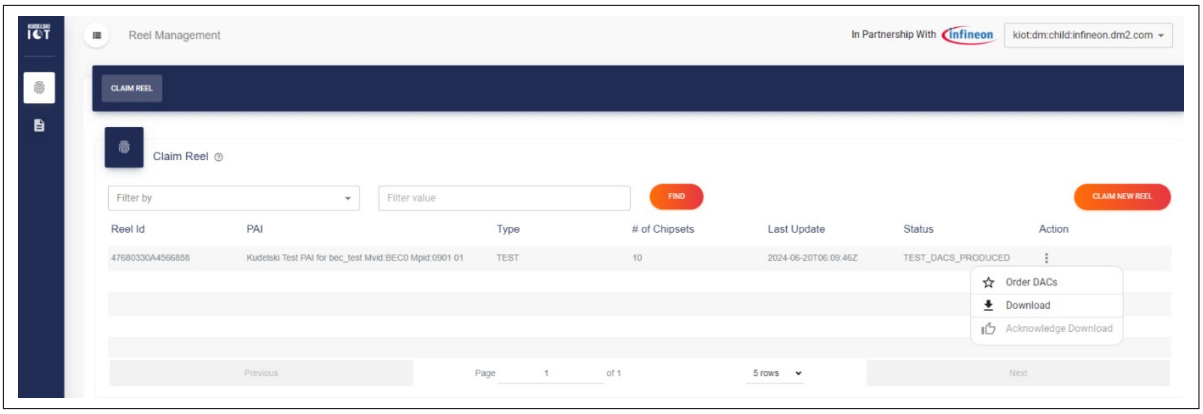

Figure 14 Click on the download to get the DACs

***Note**: The detailed information is available on the Kudelski KeySTREAM™ portal, that explain all the options available on the portal and how to use them.*

5 Summary

This document explains all the steps required to go to production by setting up a production account with our partner Kudelski to use their KeySTREAM™ portal and gives all the steps to claim reels and download the production DACs for the OPTIGA™ Trust M MTR reels.

Figure 15 encapsulates all the steps involved to go into production, starting from setting up an account to downloading and injecting the DACs into the secure elements during the production.

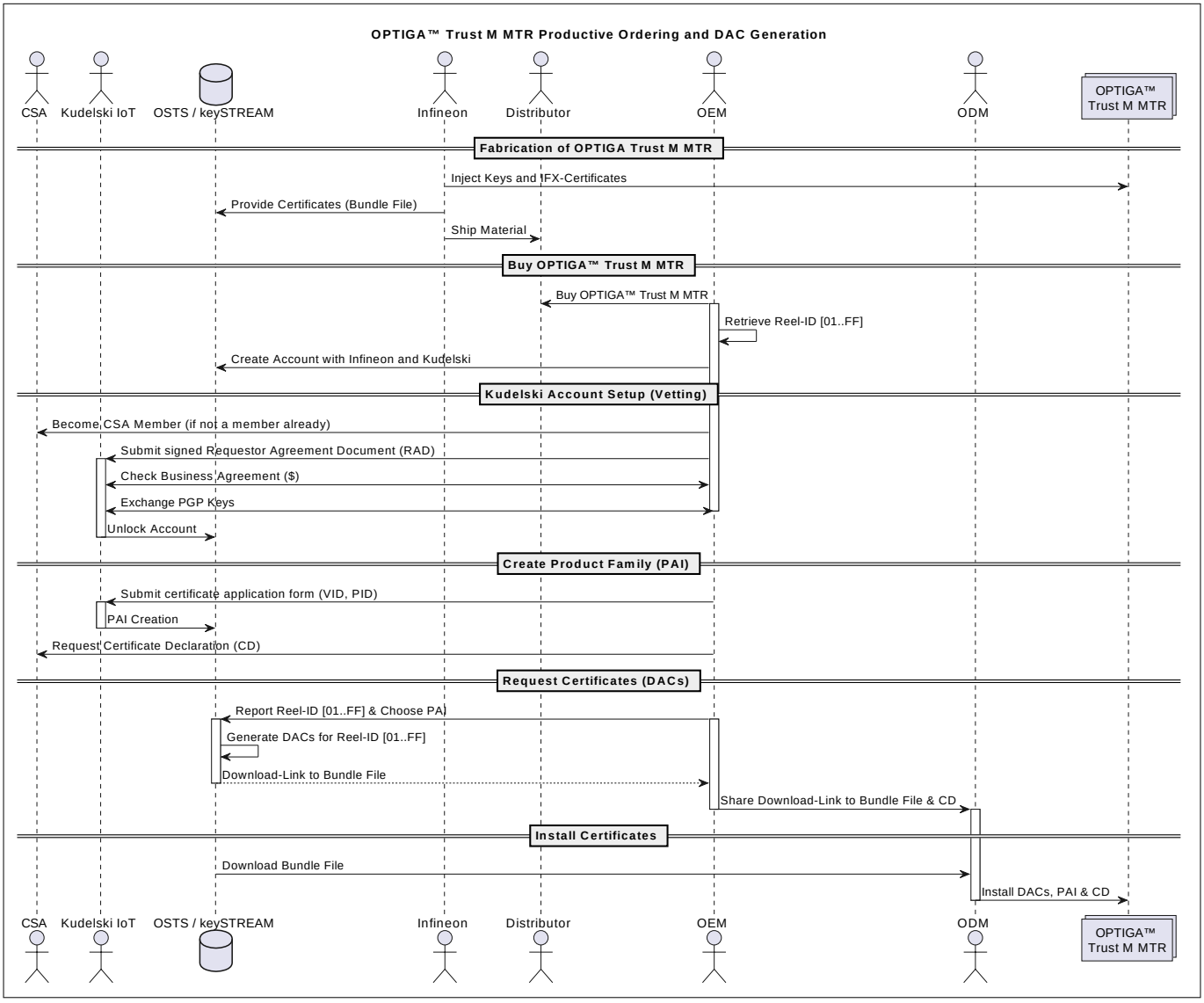

Figure 15 Complete process to get the production DACs

Glossary

CA
certificate authority (CA)

CD
Certification Declaration (CD)

CSA
Connectivity Standards Alliance (CSA)
A global organization that develops, promotes, and certifies open standards for the Internet of Things (IoT).

DAC
Device Attestation Certificate (DAC)

IoT
Internet of Things (IoT)

NDA
non-disclosure agreement (NDA)
A legal contract or part of a contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to.

OEM
original equipment manufacturer (OEM)

OSTS
Online Software Tools and Services (OSTS)

PAA
Product Attestation Authority (PAA)

PAI
Product Attestation Intermediate (PAI)

PID
product identification number (PID)

RAD
Requestor Agreement Document (RAD)

VID
vendor identification (VID)

Revision history

Reference	Description
Revision 1.0, 2025-01-31	
All	Initial release

Trademarks

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

Edition 2025-01-31

Published by

Infineon Technologies AG

81726 Munich, Germany

© 2025 Infineon Technologies AG

All Rights Reserved.

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

Email:
CSSCustomerService@infineon.com

Document reference
IFX-uwf1733833398057

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.