OPTIGA™ Trust M Cloud ID

User guide

About this document

Scope and purpose

The scope of this document is to guide the users to retrieve their device certificates and shared secrets using the Infineon CIRRENT™ Cloud ID.

Intended audience

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

Table of contents

List of figures

1 Introduction

This document describes the process of retrieving the device certificates and shared secrets (platform binding secret and authorization reference) using the Infineon CIRRENT™ Cloud ID service. This process includes four components.

1. **The reel with OPTIGA™ Trust M Express devices:**

   Each reel contains 4000 devices. The reels are packed in individual boxes.

2. **The letter:**

   Each reel will have a sealed individual letter placed in the same box. The letter contains information such as the Reel ID, QR code, and two secret strings: the batch ID and the transport key.

   Figure 1 shows an example of such a letter.

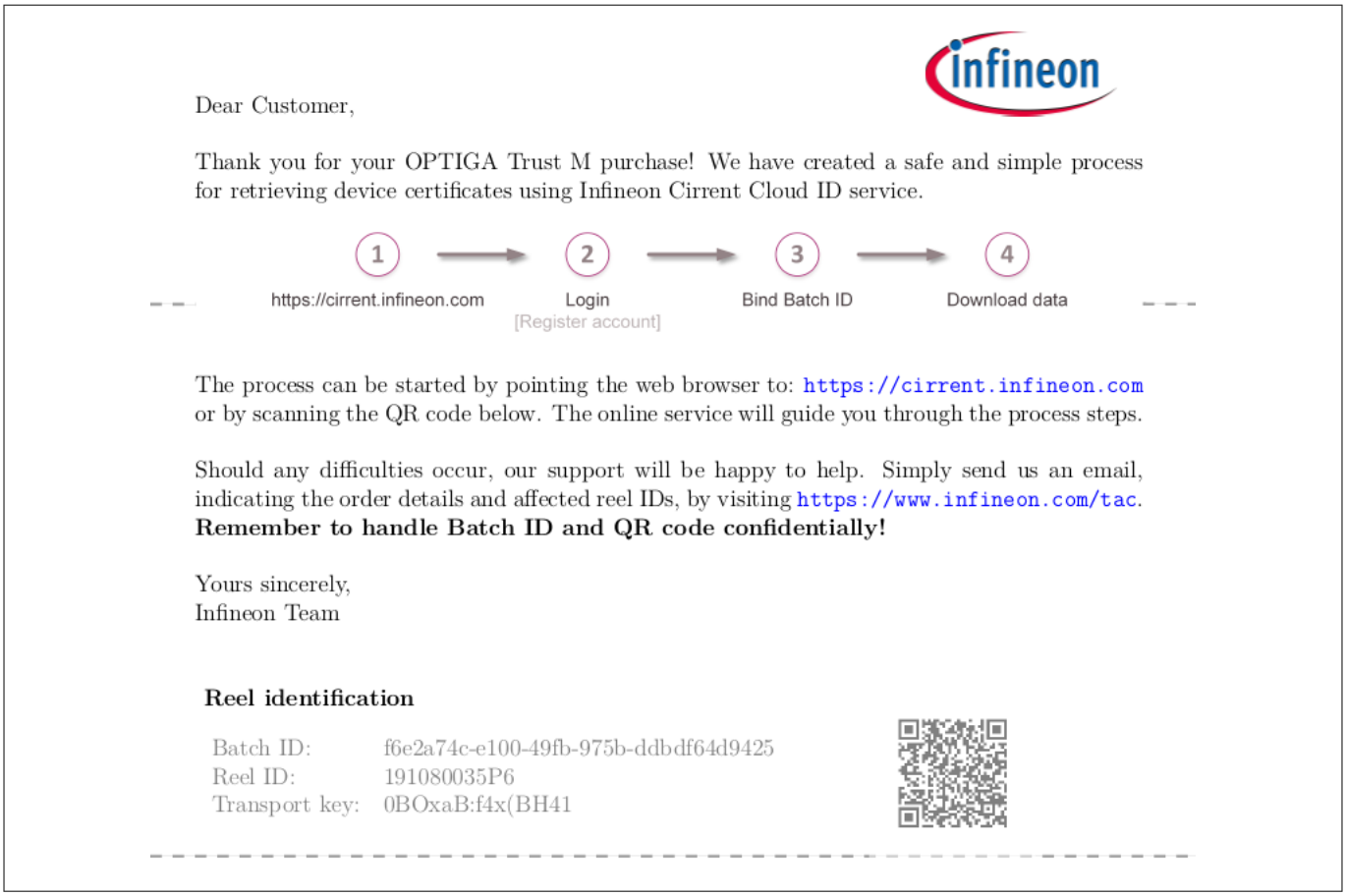


Figure 1 The letter

3. **CIRRENT™ Cloud ID:**

   This is where the customers can retrieve their device certificates and shared secrets.

4. **The Bundle file[1]:**

   The device certificates and shared secrets are packaged as a Bundle file for each reel and can be downloaded using the Infineon CIRRENT™ Cloud ID service. Refer to Chapter 2 for more information.

[1] It is possible that the bundle file contains more certificates than devices on a reel. This is due to the manner in which the reel is tested and packed. The extra certificates are from devices that are scrapped during testing and pose no risk.

2 Bundle file

A bundle file is an archive of archives. The Bundle file contains archives of device certificates and shared secrets (platform binding secret and authorization reference). Platform binding secret and authorization reference secrets are encrypted with the transport key from the letter.

The structure of the Bundle file is as shown in the Figure 2.

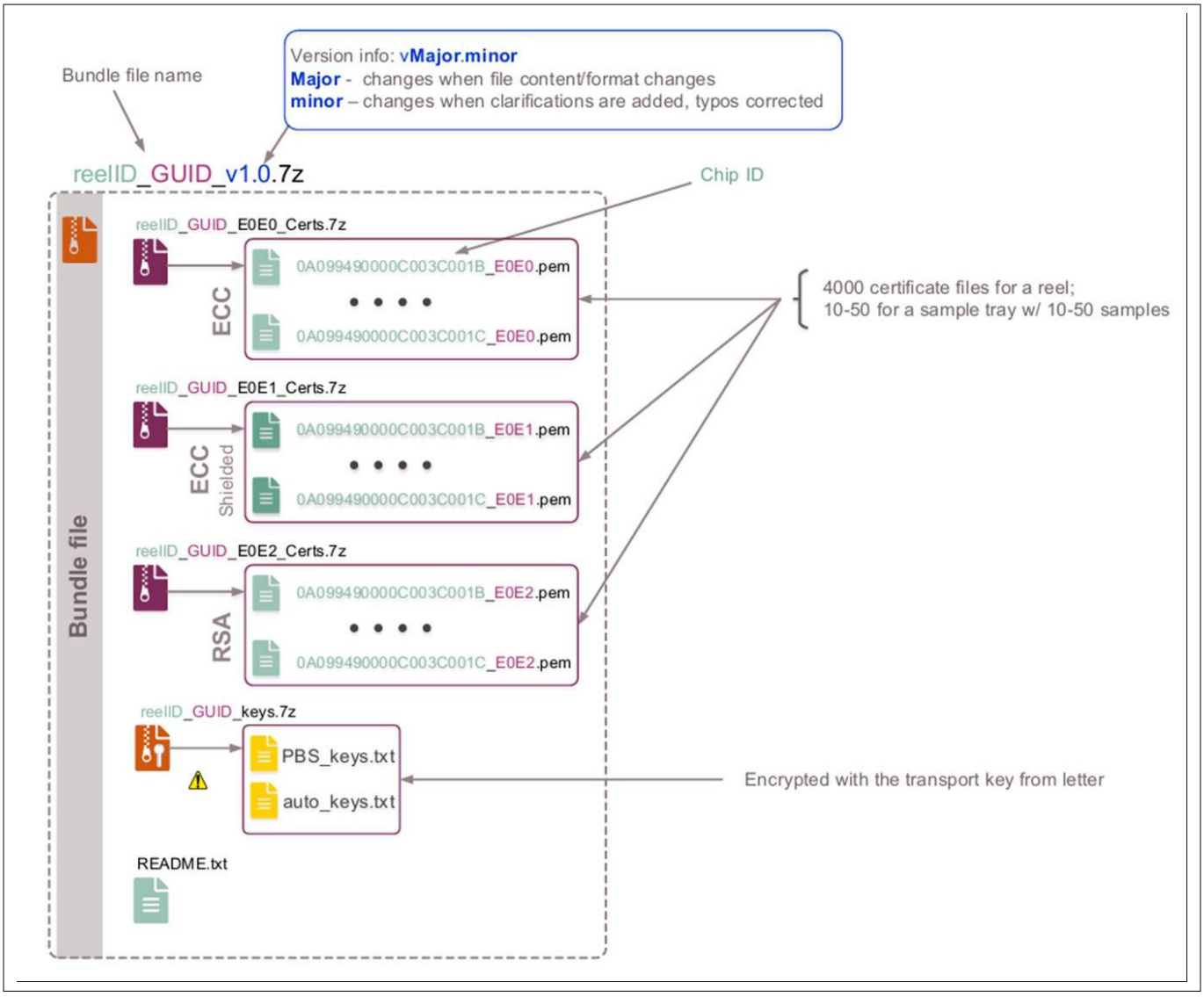


Figure 2 Bundle file structure

The Bundle file includes the following archives:

- **reelID_GUID_E0E0_Certs.7z**

  This archive contains the certificates stored in data object 0xE0E0 as device individual.pem files. To allow matching certificate to device, the individual file names adhere to the convention: chipID_E0E0.pem.

- **reelID_GUID_E0E1_Certs.7z**

  This archive contains the certificates stored in data object 0xE0E1 as device individual.pem files. To allow matching certificate to device, the individual file names adhere to the convention: chipID_E0E1.pem.

  Note: The certificate from the 0xE0E1 data object can only be used under shielded connection.

- **reelID_GUID_E0E2_Certs.7z**

  This archive contains the certificates stored in data object 0xE0E2 as device individual.pem files. To allow matching certificate to device, the individual file names adhere to the convention: chipID_E0E2.pem.
- **reelID_GUID_keys.7z**

  This file is an encrypted archive containing the platform binding secret and authorization reference secret for each chip. The decryption key is named "transport key" and is available in the reel associated letter. Platform binding secret and authorization reference secret are included in this archive as text files with 1 record/line, structured as {chipID, PBS key} and {chipID, authorization key}, respectively.

  The records are represented as hexadecimal strings.
- **PBS_keys.txt**

  This file contains a platform binding secret (PBS) that is used to establish a shielded connection between a Host MCU and OPTIGA™ Trust M. For more information, refer to [3] and [4].
- **auto_keys.txt**

  This file contains authorization reference secrets. For more information, refer to [3] and [4].
- **ChipID**

  Unique ID of the OPTIGA™. The structure of the ChipID is as follow:
  - Batch number [6 bytes] || Chip position on wafer: X-coordinate [2 bytes] || Chip position on wafer: Y-coordinate [2 bytes]

3 Bundle file retrieving flow

The following section demonstrates how to retrieve a bundle file from the CIRRENT™ Cloud ID using a web browser; alternatively, use a mobile device and the instructions from the letter.

The steps for retrieving the Bundle file from the CIRRENT™ cloud ID are as follows:

1. The OPTIGA™ Trust M Express devices are shipped with built-in device individual certificates and shared secrets.

   Note: The certificates and shared secrets are made available to the customer via the CIRRENT™ Cloud ID service.

2. Navigate to the https://cirrent.infineon.com website and either access the account with an email address or create a new account by following the instructions.

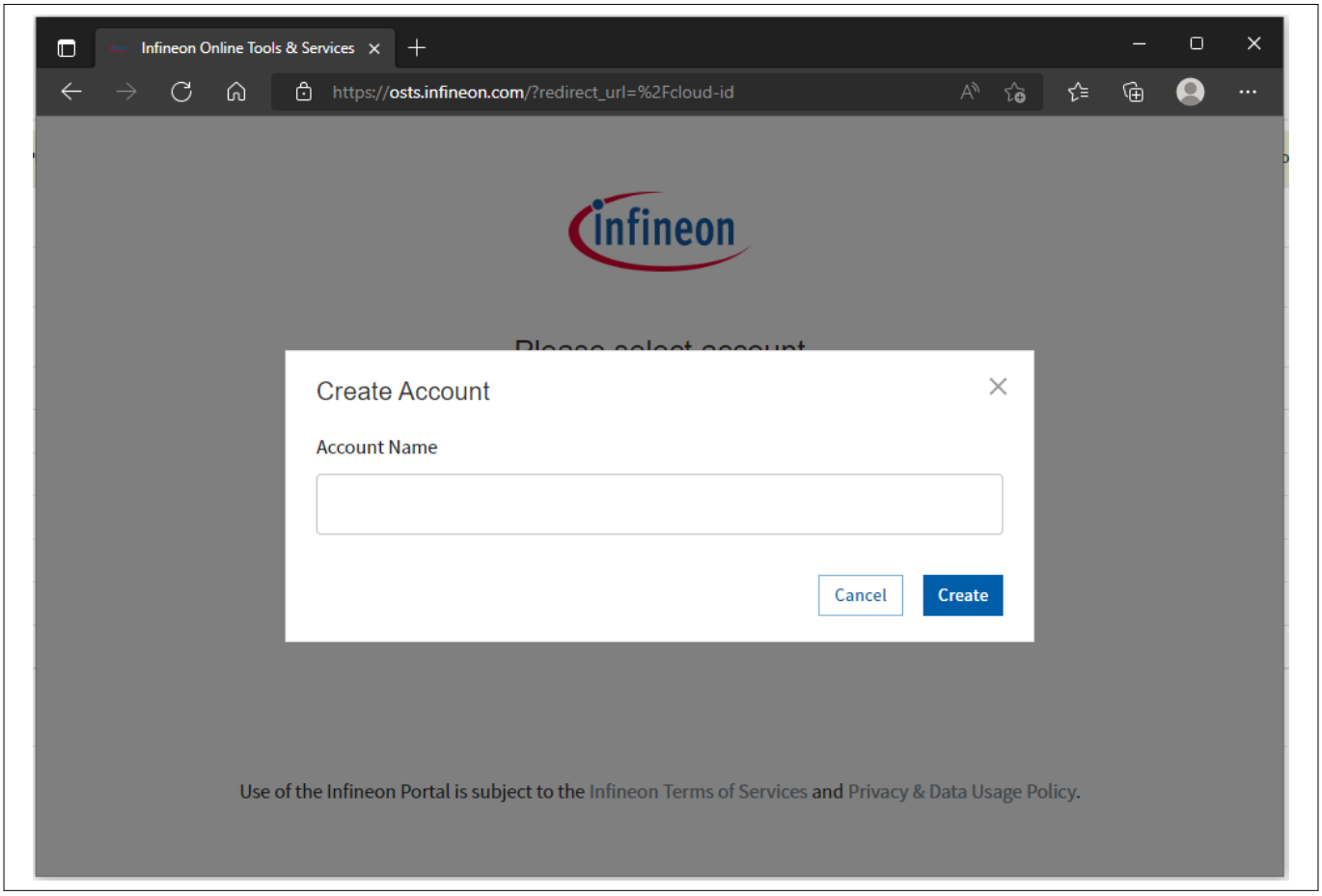
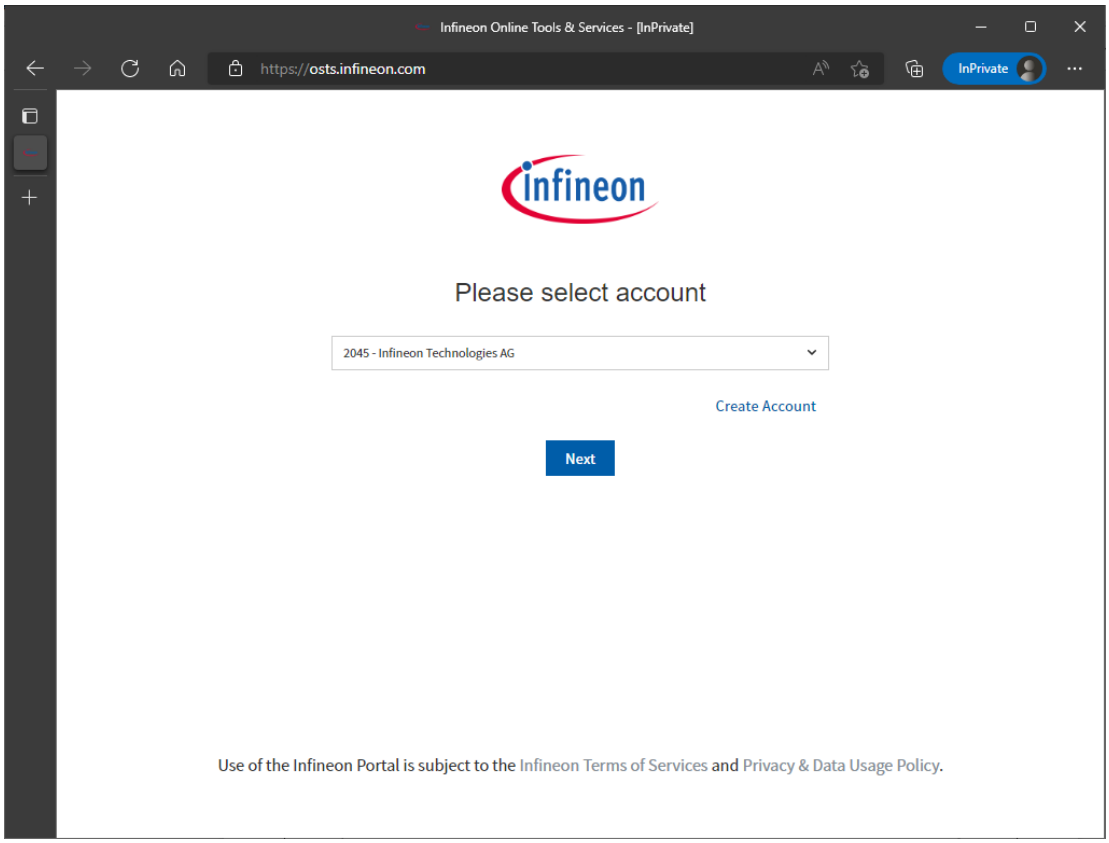


Figure 3 Creating an account with CIRRENT™

3. Login to the CIRRENT™ Console.



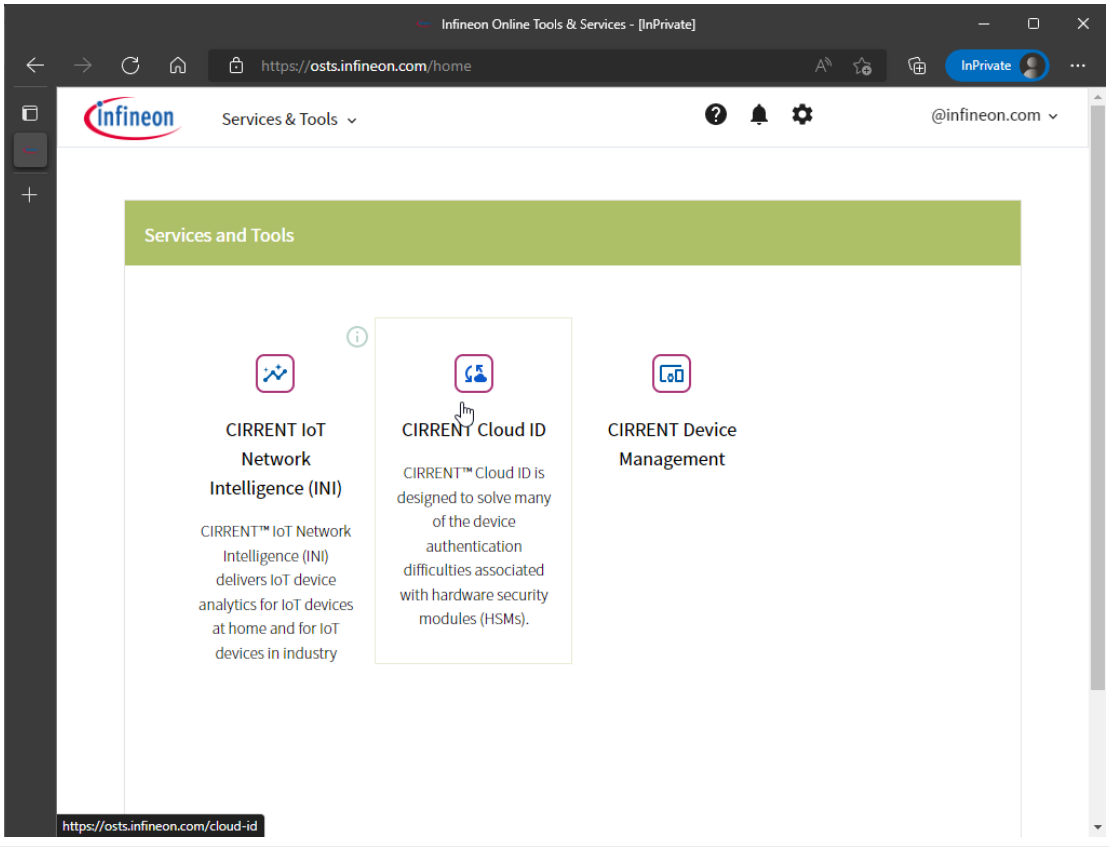


Figure 4 Login to the CIRRENT™ Cloud ID

4. Bind the ownership of the device by entering the batch ID number and Reel ID (as a passphrase) provided in the letter.

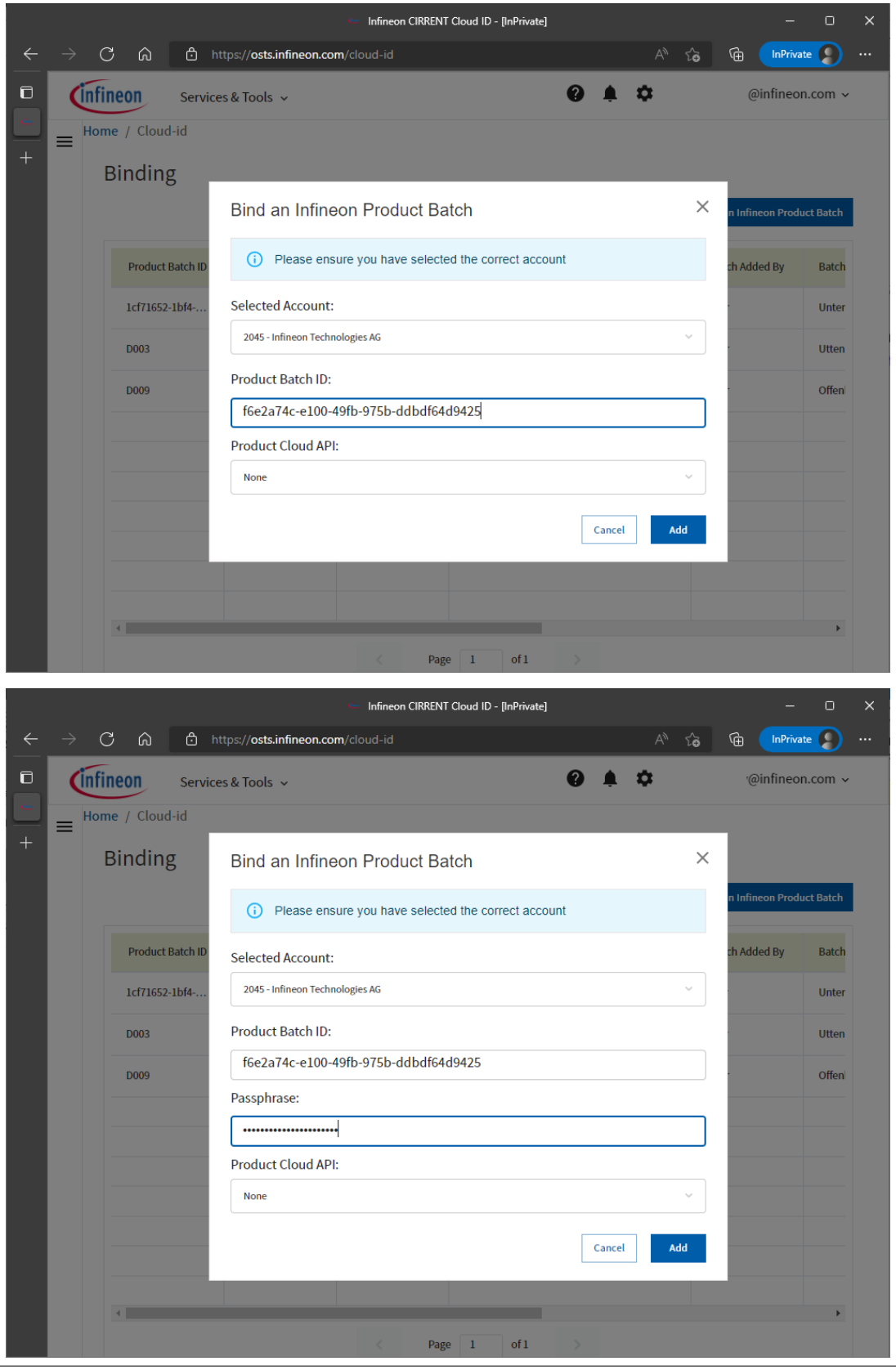


Figure 5 Binding an Infineon product batch

5. Download the Bundle file. Refer to Chapter 2 for more information about the structure of the bundle file.

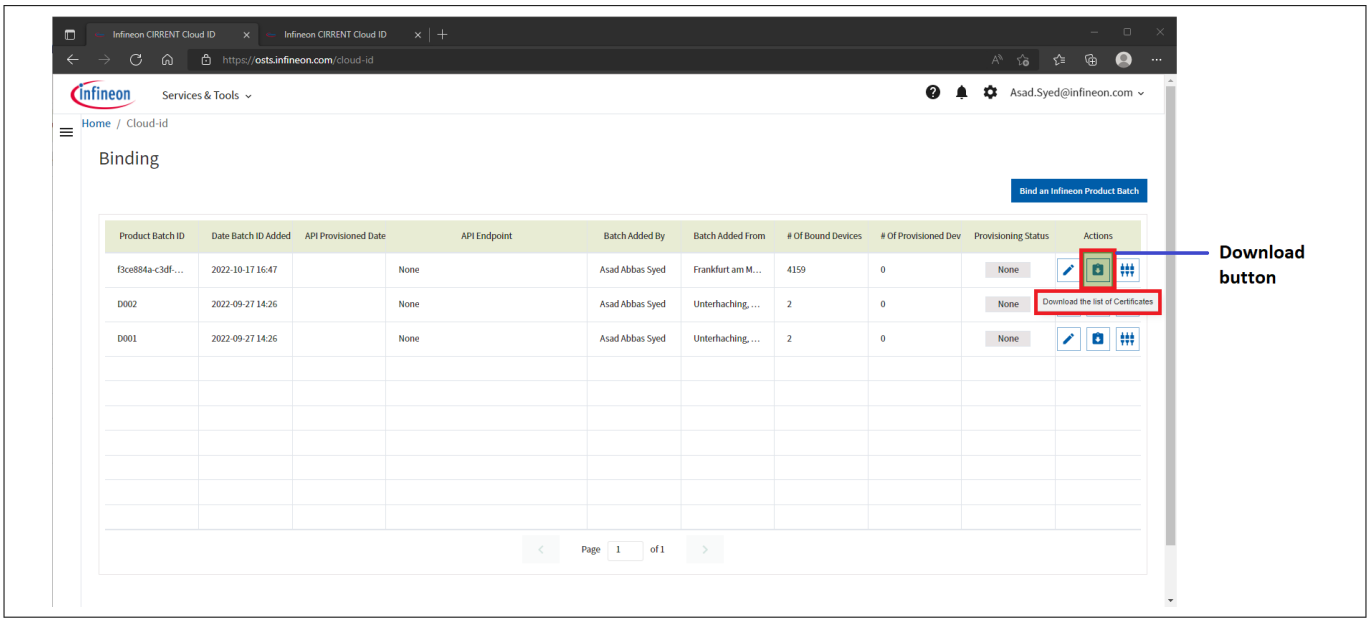


Figure 6 Downloading the Bundle file

For more information about this service, navigate to CIRRENT™ Cloud ID website [2].

4 CA certificates

The CA certificates required for end device certificate validation are as follows:

- The root CA certificates:
  http://pki.infineon.com/OptigaEccRootCA2/OptigaEccRootCA2.crt
  http://pki.infineon.com/OptigaRsaRootCA2/OptigaRsaRootCA2.crt
- The intermediate CA certificates:
  https://pki.infineon.com/OptigaTrustEccCA306/OptigaTrustEccCA306.crt
  https://pki.infineon.com/OptigaTrustRsaCA309/OptigaTrustRsaCA309.crt

References

[1] Infineon Technologies AG: *CIRRENT™ Cloud ID login*: https://documentation.infineon.com/html/cirrent-support-documentation/en/latest/cid/quick-start-cloud-id-virtual-dev-kit.html

[2] Infineon Technologies AG: *CIRRENT™ Cloud ID:* https://www.infineon.com/cms/en/design-support/service/cloud/cirrent-cloud-id/

[3] Infineon Technologies AG: *OPTIGA™ Trust M, Solution Reference Manual (Revision 3.50);* 2022-11-09

[4] Infineon Technologies AG: *OPTIGA™ Trust M, Configuration Guide (Revision 1.2);* 2022-11-09

Glossary

AC
access condition (AC)

batch ID
A unique reel identifier.

CA
certificate authority (CA)

ECC
elliptic curve cryptography (ECC)

GUID
globally unique identifier (GUID)
It has been replaced by batch ID.

ID
identification (ID)

Revision history

Reference	Description
Revision 1.2, 2022-11-09	
All	Layout change
Revision 1.1, 2022-10-20	
All	Editorial changes
Revision 1.0, 2022-10-11	
All	Initial release

Trademarks

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

Edition 2022-11-09

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-nhb1663828544673

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.