DigiCert® On-Boarding Guidelines for Product Manufacturers to the CI Plus Portal

Version 1.9

digicert®

Legal Notice

DigiCert, Inc.
2801 North Thanksgiving Way, Suite 500
Lehi, UT 84043
https://www.digicert.com

Table of Contents

CHAPTER 1

1 Introduction

This chapter includes the following topics:

1.1 About these Guidelines

This document is a guideline for product manufacturers (TV sets or CAM devices) and describes the process flow leading to on-boarding to the CI Plus portal.

On-boarding describes the process where the Licensee has to complete several tasks to get access to the CI Plus portal to order Device ID credentials from DigiCert, which is the CI Plus Trust Authority.

If you are a component manufacturer (firmware, software, or chips), you should read *DigiCert® Guidelines for Becoming a CI Plus Component Manufacturer Licensee*, which is also available on DigiCert's web site:

https://knowledge.digicert.com/support/device-certificate-services.html

1.2 About Accessing the CI Plus Portal

As Product Manufacturers, the Licensee uses the CI Plus portal to place purchase orders, to download the resulting Device ID credentials, and to decrypt the downloaded files. Up to ten employees of the Licensee can be provided access to the CI Plus portal. Access to the portal for these administrators is secured by a Brand Administrator certificate. This credential authenticates the administrator to the portal and secures all communication with it. For security reasons, this credential must be stored on a security token.

The Brand Administrator certificate is provisioned by DigiCert PKI Platform. DigiCert PKI is a public key infrastructure (PKI) platform that combines software, encryption technologies, and services to enables enterprises to protect the security of their Internet communications and business transactions. PKI uses digital certificates, public- key cryptography, and Certification Authorities (CA) to create an enterprise-wide network security architecture that protects against intrusion, such as hackers who steal passwords or intercept email messages and credit card transactions.

Once you have received the initial Brand Administrator certificate, you will typically only need to use DigiCert PKI to create and manage additional Brand Administrators (that is, to add, remove, or edit administrators). You do this through the DigiCert PKI administration portal, PKI Manager. If you wish to review the functionality of PKI Manager or learn how to issue other types of certificates using DigiCert PKI, contact your DigiCert representative.

1.2.1 Security Tokens

For security reasons, the Brand Administrator credential must be stored on a security token. The security token provides greater protection of the Brand Administrator's private key, compared to the protection afforded by a browser. The private key, once downloaded to the token, can never be removed or backed up, which ensures that the private key on the token cannot be duplicated. In addition, the token can be locked away in a secure location when not in use.

As part of the on-boarding process, you will need to obtain security tokens for your Brand Administrators. The supported token is Aladdin eToken Pro. Refer to the token manufacturer's web site for a local reseller, supplier, or contact the manufacturer to get information in your area.

You will need one token for testing, and one production token for each Brand Administrator that you will allow to access the CI Plus portal and manage Device IDs. Once you have obtained the security tokens, install them on the computers that the Brand Administrators will use when accessing the CI Plus portal. Refer to the token manufacturer's documentation for installation procedures.

1.2.2 PKI Client

PKI Client is DigiCert's certificate management tool. Brand Administrators will use PKI Client to enroll for, store, and access PKI certificates (specifically, the Brand Administrator certificate). Brand Administrators will be prompted to install PKI Client when picking up the Brand Administrator certificate.

1.3 On-boarding Overview

The process for on-boarding a Product Manufacturer begins when a Product Manufacturer contacts DigiCert for information. Contact DigiCert at:

- Website: https://www.websecurity.symantec.com/pki/ci-plus-device
- Email: ciplus@digicert.com

Include a telephone number if you want DigiCert to contact you about specific questions.

DigiCert will provide the Product Manufacturer with additional information including pricing, initial licensing agreements, and this on-boarding document.

Table 1-1 describes the general process for on-boarding Product Manufacturers. Note that some of these steps can be done in parallel. Refer to the resources listed after each step for additional details about the step.

Module Manufacturers who want to register Standard (non-ECP) Device Types, supporting both CI Plus Roots of Trust, have to follow the Standard Device Type registration process.

Product Manufacturers who want to register ECP Device Types need to follow additional steps. These steps are tagged, "For ECP only". ECP Device Types are Host and CICAM devices that have been designed and manufactured in accordance to the ECP Specification.

Table 1-1 On-boarding Process Checklist

Task	Performed by	Refer to	Status
Obtain and complete the initial agreements: • Interim License Agreement (ILA) • [For ECP only] ILA Addendum for ECP • Certificate Service Agreement (CSA)	Product Manufacturer	See "About the Initial Documents" on page 10.	
Pay the on-boarding fee	Product Manufacturer	N/A	
Obtain and complete the Brand Administrator authorization form: • Authorization of PKI Administrator • Official company register or DUNS number	Product Manufacturer	See "About the Initial Documents" on page 10.	
Product Manufacturer authentication begins	DigiCert	N/A	
Obtain security tokens	Product Manufacturer	See "Security Tokens" on page 6.	

Task	Performed by	Refer to	Status
Provide customer with CIPLock Tool and test package	DigiCert	N/A	
Obtain the initial Brand Administrator certificate	Product Manufacturer	See "Obtaining a Brand Administrator Certificate" on page 17.	
Revoking Brand Administrators	Product Manufacturer	See "Revoking a Brand Administrator Certificate" on page 20.	
Obtain and complete the CI Plus Company/Brand On-boarding Form	Product Manufacturer	See "Creating the Portal Account" on page 21.	
Create the CI Plus portal account	DigiCert	N/A	
Send a test Device Type to the CI Plus Test House (Eurofins)	Product Manufacturer	N/A	
Send the applicable CI Plus Robustness Certification Checklist and the Registration Application forms to DigiCert	Product Manufacturer	See "Configuring the Device Type" on page 22.	
Add the defined Device Type to the CI Plus portal account	DigiCert	N/A	

Once these steps are completed, the Brand Administrators can access the CI Plus portal to place purchase orders and to download the resulting Device ID credentials.

1.4 Additional On-boarding for ECP

The process for on-boarding as an ECP Product Manufacturer when you are already on-boarded as a Product Manufacturer follows:

1. Contact DigiCert to begin the on-boarding process for ECP:

   Website: https://www.websecurity.symantec.com/pki/ci-plus-device
   Email: ciplus@digicert.com
   Include a telephone number if you want DigiCert to contact you about specific questions.

2. If the current signed version of the *Interim License Agreement* is older than 2018, the Product Manufacturer must renew their license agreement prematurely by obtaining and completing the 2018 *Interim License Agreement*.

   In this case, the manufacturer does not pay a license fee or an on-boarding fee. The 2018 *Interim License Agreement* shall be dated with the same dates as the Product Manufacturer's current *Interim License Agreement*.

3. Obtain and complete the *ILA Addendum for ECP*.

   ECP Product Manufacturers already on-boarded for Standard (non-ECP) Device Types do not pay a license fee or an on-boarding fee. The *ILA Addendum for ECP* and any subsequent annual renewals shall be dated with the same dates as the Product Manufacturer's current *Interim License Agreement*.

CHAPTER 2

2 Obtaining and Completing the Initial Documents

This chapter includes the following topics:

2.1 About the Initial Documents

DigiCert is a Trusted Agent of CI Plus, and is authorized to collect and sign forms as part of the on-boarding process. As the first task in the on-boarding process, the Product Manufacturer must complete the following initial documents and return them to DigiCert:

- Initial Agreements:
  - Interim License Agreement (ILA) (Product Manufacturers wishing to register ECP Device Types must provide a 2018 *Interim License Agreement* or newer)
  - ILA Addendum for ECP (only for Product Manufacturers wishing to register ECP Device Types)
  - Certificate Supply Agreement (CSA)
- Brand Administrator Authorization Form (Authorization of PKI Administrator and excerpt of an official company register or DUNS number)

2.2 Initial Agreements

The Licensee should send the Interim License Agreement (ILA), the Certificate Supply Agreement (CSA), and (for Licensees wishing to register ECP Device Types) the ILA Addendum for ECP to DigiCert at:

DigiCert, Inc.
Attn: Legal Department
2801 North Thanksgiving Way Suite 500
Lehi, Utah 84043

Email: legal@digicert.com

Reference telephone number (for couriered items): 1-800-896-7973

For questions, email: ciplus@digicert.com. To ensure proper delivery, include CI Plus in the subject line of all email communications.

The Licensee must return the completed and signed documents to DigiCert for archiving and audit purposes.

2.2.1 Interim License Agreement

The CI Plus Device Interim License Agreement entitles Licensees to access and use certain security elements, authentication certificates, specifications, software, and test materials to develop and manufacture compliant Hosts and/or Modules. The Agreement is by and between CI Plus LLP ("CI Plus TA"), a United Kingdom limited liability company, and the Licensee.

Obtain the Interim License Agreement template from the DigiCert web site at: https://knowledge.digicert.com/support/device-certificate-services.html

The ILA contains the main part of the Interim License Agreement and the following exhibits that define additional processes and procedures:

Note: These exhibits include a copy of the CI Plus Robustness Certification Checklist for reference purposes. The Licensee does not need to complete this form until ready to configure the Device Type.

See "Configuring the Device Type" on page 22.

- Exhibit A: Device Type
- Exhibit B: Robustness Rules
- Exhibit C: Compliance Rules for Host Device
- Exhibit D: Compliance Rules for CICAM Device
- Exhibit E: URI Mapping Table
- Exhibit G: Robustness Rules Checklist
- Exhibit H: Confidentiality Agreement
- Exhibit I: Fee schedule
- Exhibit J: Registration Procedure
- Exhibit K: Change Procedure
- Exhibit L: Revocation Procedure
- Exhibit M: Informative Flow Chart describing Arbitration Process

The Licensee completes the first page, marks a checkbox in the Licensed Product section, signs two copies of the ILA (by an authorized official), and sends the completed form to DigiCert. The Licensee must submit all pages of the agreement, even if they are not completed.

DigiCert is the CI Plus Trusted Agent and is authorized to collect this form as part of the on-boarding process. DigiCert is entitled to sign the License Agreement on behalf of CI Plus and a copy is sent back to the Licensee.

2.2.2 ILA Addendum for ECP

The (optional) ILA Addendum for ECP entitles Licensees to access and use certain security elements, authentication certificates, specifications, software to develop and manufacture ECP Hosts and/ or Modules, compliant with the CI Plus ECP Specification. The Agreement is by and between CI Plus LLP ("CI Plus TA"), a United Kingdom limited liability company, and the Licensee.

The ILA Addendum for ECP is an addendum to the ILA and cannot stand alone.

Obtain the ILA Addendum for ECP template from the DigiCert web site at: https://knowledge.digicert.com/support/device-certificate-services.html

The ILA Addendum for ECP contains an addendum of the main part of the Interim License Agreement and the following exhibits that define additional processes and procedures:

Note: These exhibits include a copy of the ECP Robustness Rules Checklist for reference purposes. The Licensee does not need to complete this form until ready to configure the Device Type.

See "Configuring the Device Type" on page 22.

- Exhibit ECP_B: Robustness Rules for ECP Devices
- Exhibit ECP_C: Compliance Rules for ECP Host Devices
- Exhibit ECP_D: Additional Compliance Rules for ECP CICAM Devices
- Exhibit ECP_E: URI Mapping Table for ECP
- Exhibit ECP_G: Robustness Checklist for ECP Devices

The Licensee completes the first page of the Addendum (which must be filled-out identically to the first page of the ILA), signs two copies of the Addendum (by an authorized official), and sends the completed form to DigiCert. The Licensee must submit all pages of the agreement, even if they are not completed.

DigiCert countersigns the ILA Addendum for ECP and a copy is sent back to the Licensee.

2.2.3 Certificate Supply Agreement

The DigiCert Certificate Supply Agreement entitles Licensees to place orders for certificate batches for the CI Plus system at the CI Plus portal operated by DigiCert. The Agreement is between DigiCert, Inc. an Irish limited liability company, and the Licensee.

The Certificate Supply Agreement can be downloaded from DigiCert's web site at: https://knowledge.digicert.com/support/device-certificate-services.html

The Licensee signs two copies of the CSA by an authorized official and sends them to DigiCert. DigiCert countersigns the Certificate Supply Agreement and a copy is sent back to the Licensee.

2.3 Brand Administrator Authorization Form

Once the Interim License Agreement and Certificate Supply Agreement are received at DigiCert and the Licensee has paid the on-boarding fee, DigiCert will begin the CI Plus account set-up process. At that time, DigiCert uses the information from the following forms to authenticate and verify all Licensees requesting a CI Plus account, as well as the administrators allowed to access the CI Plus portal and manage Device IDs.

The Licensee must complete separate Brand Administrator authorization form. However, only the initial Brand Administrator authorization is required as part of the on-boarding process. The Licensee can provide these documents for other Brand Administrators as they are added to the CI Plus account.

The Licensee must also submit updated Brand Administrator authorization form, if a Brand Administrator's contact information is updated.

Note: The official company register or Dun & Bradstreet (DUNS) number is only needed during the on-boarding process.

The Licensee should send the Brand Administrator authorization form to DigiCert at:

Email: ciplus@digicert.com. To ensure proper delivery, include CI Plus in the subject line of all email communications.

2.3.1 Authorization of PKI Administrator Form

The Authorization of PKI Administrator Form provides authorization by the Licensee that the listed administrators are allowed to access the CI Plus portal and manage Device IDs.

Obtain the Authorization of PKI Administrator Form from the DigiCert web site at: https://knowledge.digicert.com/support/device-certificate-services.html

An authorized official of the Licensee completes and signs the Authorization of PKI Administrator Form and sends the completed form to DigiCert.

2.3.2 Official Company Register or DUNS Number

An excerpt from the official company register or Dun & Bradstreet (DUNS) number provides proof of the existence of the Licensee organization. Send this excerpt or DUNS number to DigiCert.

CHAPTER 3

3 Testing the Device Technology

When the Interim License Agreement and the Certificate Supply Agreement have been signed and returned to DigiCert and the on-boarding fee paid, DigiCert will send the Licensee a test set containing test versions of the following items:

- Device ID credentials
- Test Brand Administrator credentials: The Test Brand Administrator PKCS#12 file (the file with extension .p12 contains a certificate and the corresponding private key)
- For CICAM manufacturers, the test set also contains:
    - 10 CICAM Test Devices certificates and keysCI Plus Test Root CA certificate
    - CI Plus Test Brand CA certificate
    - CI Plus 2nd Root Test Root CA certificate
    - CI Plus 2nd Root Test Brand CA certificate
    - 1 CICAM 2nd Root Test Device certificate and key with security level = Standard
    - 1 CICAM 2nd Root Test Device certificate and key with security level = ECP
    - Test license constants used for both Roots of Trust (for production license constants, each Root of Trust will use different values)
    - Readme pdf file with more information about the certificates
    - CICAM CI Plus License Specification
    - CI Plus CICAM Revocation Test Requirements
    - Revocation test material
    - Additional revocation test material from 2nd Root of Trust
- For Host manufacturers, the test set also contains:
    - 11 Host Test Device certificates and keys
    - CI Plus Test Root CA certificate
    - 2 CI Plus Test Brand CA certificates
    - CI Plus 2nd Root Test Root CA certificate
    - CI Plus 2nd Root Test Brand CA certificate
    - 4 Host 2nd Root Test Device certificates and keys with security level = 1 (ECP)
    - Test license constants used for both Roots of Trust (for production license constants each Root of Trust will use different values)
    - Readme pdf file with more information about the certificates
    - Host CI Plus License Specification

CHAPTER 4

4 Managing Brand Administrators

This chapter includes the following topics:

4.1 About the Brand Administrator

Access to the CI Plus portal is limited to Brand Administrators of the Licensee. Brand Administrators have a credential (a Brand Administrator certificate issues by DigiCert) on a security token that allows them to access the portal, to place purchase orders, to download the resulting certificate batch files (with the Device ID certificates/private keys), and to decrypt the downloaded file. The Brand Administrator certificate authenticates the Brand Administrator to the CI Plus portal and secures all communication with it. DigiCert will provide the Licensee with up to 10 Brand Administrator certificates. The price of up to 10 certificates is included in the annual hosting fee.

Before a Brand Administrator can be issued a certificate, the Brand Administrators have to be authenticated and verified by DigiCert. At this point, the Licensee has already provided contact information for the initial Brand Administrator, which DigiCert will use to authenticate and verify the initial Brand Administrator and issue the initial Brand Administrator certificate. However, the Licensee must provide contact information for each additional Brand Administrator listed in Brand Administrator authorization form.

See “Brand Administrator Authorization Form” on page 13.

Brand Administrator certificates are issued using DigiCert PKI Platform (DPP). DigiCert representative will start enrollment of the Brand Admin(s) as listed in Admin Authorization from on CI Plus Service PKI account. After the initial Brand Administrator is approved and has received the Brand Administrator certificate, he or she has to finish enrollment finally.

The Brand Administrator certificate must be stored on a security token.

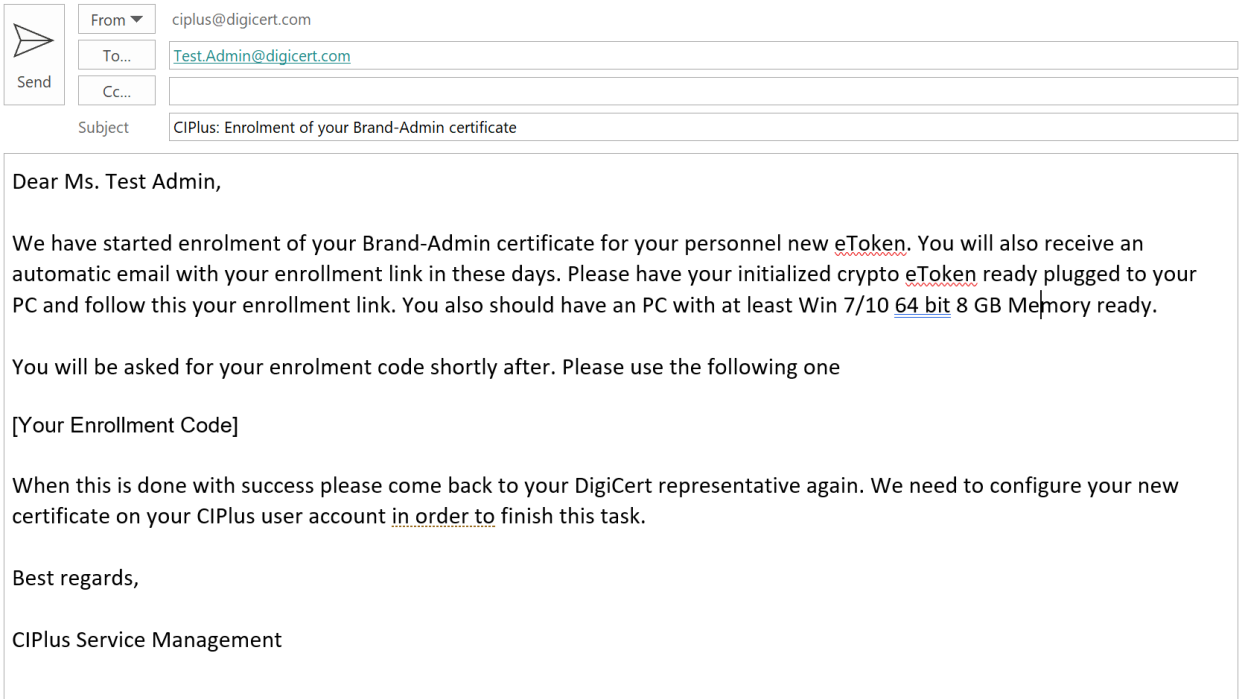
See “Security Tokens” on page 6.

4.2 Obtaining a Brand Administrator Certificate

To obtain a Brand Administrator certificate, a request must be made through PKI Manager, and the request must be authenticated and verified by DigiCert. Each Brand Administrator request will be made by your DigiCert representative.

Once the updated contact information for each Brand Administrator, as listed in Brand Administrator authorization form has been received per email and the request is approved, the new Brand Administrator will receive 2 separate emails

1. Email with personnel enrollment code.



Send

From: ciplus@digicert.com

To: Test.Admin@digicert.com

Cc:

Subject: CIPlus: Enrolment of your Brand-Admin certificate

Dear Ms. Test Admin,

We have started enrolment of your Brand-Admin certificate for your personnel new eToken. You will also receive an automatic email with your enrollment link in these days. Please have your initialized crypto eToken ready plugged to your PC and follow this your enrollment link. You also should have an PC with at least Win 7/10 64 bit 8 GB Memory ready.

You will be asked for your enrolment code shortly after. Please use the following one

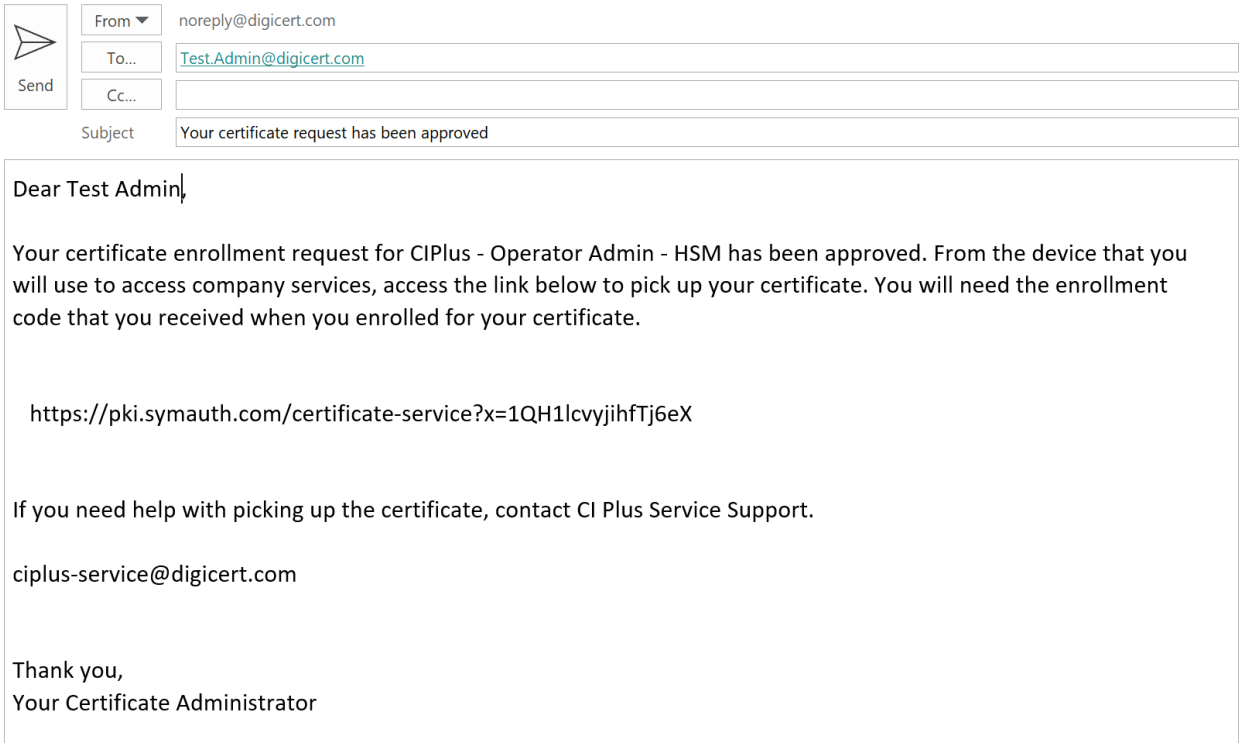
[Your Enrollment Code]

When this is done with success please come back to your DigiCert representative again. We need to configure your new certificate on your CIPlus user account in order to finish this task.

Best regards,

CIPlus Service Management

2. Email with personnel enrollment link sent automatically by DigiCert's CIPlus Service PKI account.



Send

From noreply@digicert.com

To... Test.Admin@digicert.com

Cc...

Subject Your certificate request has been approved

Dear Test Admin,

Your certificate enrollment request for CIPlus - Operator Admin - HSM has been approved. From the device that you will use to access company services, access the link below to pick up your certificate. You will need the enrollment code that you received when you enrolled for your certificate.

https://pki.symauth.com/certificate-service?x=1QH1lcvyjihfTj6eX

If you need help with picking up the certificate, contact CI Plus Service Support.

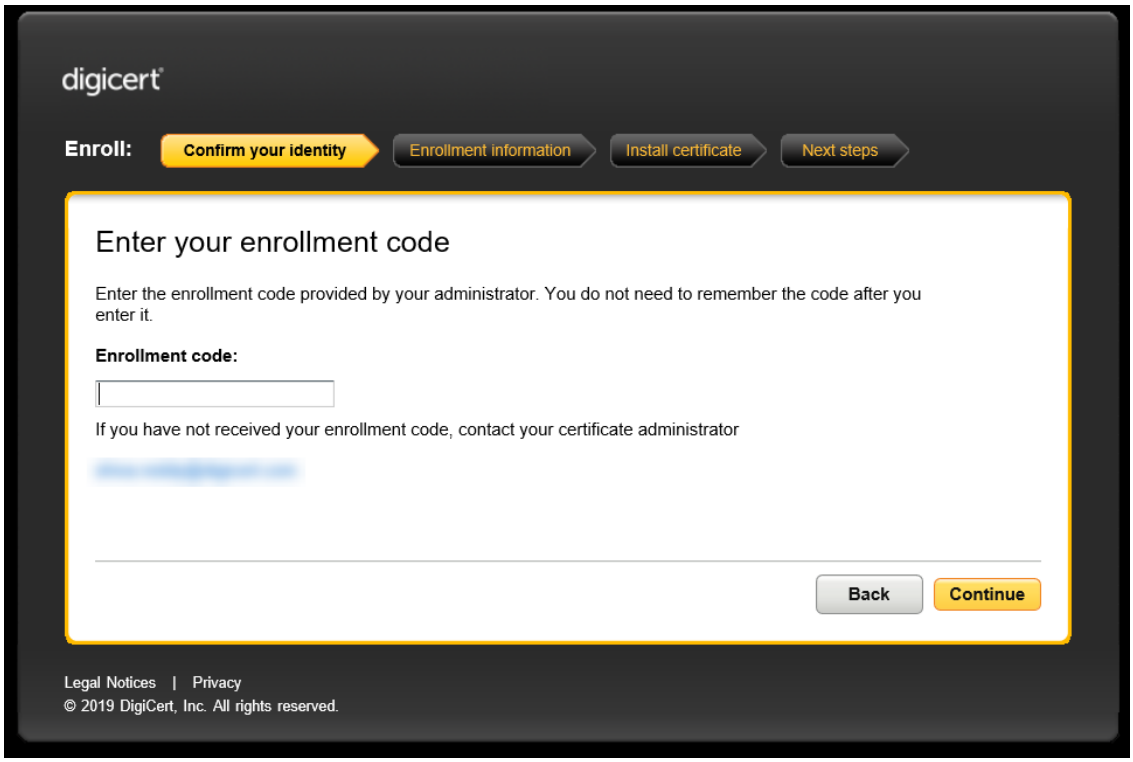
ciplus-service@digicert.com

Thank you,
Your Certificate Administrator

At that point, the new Brand Administrator should complete the following steps to obtain a Brand Administrator certificate.

1. Ensure that the security token is inserted correctly.
2. Click the link in the enrollment email or enter the enrollment link into your browser's URL bar. The PKI Certificate Service enrollment page displays.
3. Microsoft browser MS IE 11.0 will work without any further addons. In case of you are using browsers Firefox or Chrome please assure to have been installed the appropriate addons for PKI Client as follows in advance.

   a) Firefox: https://addons.mozilla.org/en-GB/firefox/addon/symantec-mpkic-extension/
   b) Chrome: https://chrome.google.com/webstore/detail/symantec-authentication-c/mbclaggcfknjpjmdbgpdahdoodbjoceh



4. Enter your enrollment code (from the enrolment email above) and click *Continue*.
5. You may see several prompts, depending upon how your system is configured:

   - If PKI Client is not already installed, you will be prompted to install it. PKI Client is DigiCert's certificate management tool. You must install PKI Client to pick up the Brand Administrator certificate.
   - If you have not used PKI Client before, you will be prompted to set a PIN. You will use this PIN any time you access the certificates on PKI Client.
   - If you have used PKI Client before, you will be asked for the PIN you set previously.
   - If the token is not inserted, you will be prompted to insert it. Insert the security token and click Refresh.

You will see a confirmation message stating that the certificate was installed successfully.

Although you now have a Brand Administrator certificate on the token, you will not have access to the CI Plus portal until the following steps are completed:

- For the initial Brand Administrator, the CI Plus portal account must be created. See "About Preparing the CI Plus Portal Account" on page 21.
- For all Brand Administrators, the Brand Administrator certificate must be registered with the CI Plus portal. The Brand Administrator must give notice to DigiCert that token enrollment has been finished. DigiCert will register the certificate shortly after the Brand Administrator picks up the certificate (the certificate is not

generated until the certificate is picked up). The Brand Administrator will receive an email stating that the certificate has been registered and that the administrator has access to the CI Plus portal.

4.3 Revoking a Brand Administrator Certificate

In some situations, a Brand Administrator certificate has to be revoked (for example, the certificate was issued to the wrong administrator, the administrator has left the Licensee's organization, or the Brand Administrator certificate has been lost or compromised).

You can request that an administrator be revoked from the CI Plus portal.

See "Additional Files in the Portal Account" on page 38.

Download document Brand Administrator Revocation form from this document download page. This form has to complete and signed shipped to address stated in the form below.

To speed up the process, a signed and scanned copy of this document can initially be provided by email to DigiCert representative. However, the Licensee must return the completed and signed paper-based documents to DigiCert for archiving and audit purposes.

This request may take up to 1 business day to complete. Once the certificate is revoked, the Brand Administrator will not be able to log into the CI Plus portal, place purchase orders, or download certificate batches. You can issue a replacement certificate to the Brand Administrator, if appropriate.

Email: ciplus@digicert.com. To ensure proper delivery, include CI Plus in the subject line of all email communications in order to go in touch with your DigiCert representative person of the CIPlus LLP.

CHAPTER 5

5 Preparing the CI Plus Portal Account

This chapter includes the following topics:

5.1 About Preparing the CI Plus Portal Account

Preparing the CI Plus portal account consists of two steps:

- See "Creating the Portal Account" on page 21.
- See "Configuring the Device Type" on page 22.

Note that requesting additional Brand Administrators is independent of the CI Plus portal. The initial Brand Administrator can request additional Brand Administrators at any time before, during, or after the CI Plus portal is ready.

5.2 Creating the Portal Account

After the initial Brand Administrator certificate is picked up, but before the initial Brand Administrator can access the CI Plus portal to order and download Device ID credentials, DigiCert must create the CI Plus portal account. Before DigiCert can create the CI Plus portal account, the Licensee must send a completed CI Plus Company/Brand On-boarding Form (available on the DigiCert web site at https://knowledge.digicert.com/support/device-certificate-services.html) to DigiCert Enterprise Authentication at the following address. This form provides DigiCert with account-specific information needed to create the CI Plus account.

DigiCert, Inc.
CIPlus Services
Unit 21 Beckett Way
Park West Business Park
Dublin 12
D12 C9YE, Ireland

Courier contact phone number (Post office): +353 1 255 2935

Email: ciplus@digicert.com

Once DigiCert receives this form, the CI Plus portal account will be created, and DigiCert will send the portal account link to the Licensee.

The Brand Administrators will then be able to log into the portal and test their login credential on the security token; however, they are not yet able to place purchase orders until the Device Type has been configured and the Registration Application and CI Plus Robustness Certification Checklist have been provided to DigiCert.

5.3 Configuring the Device Type

Before ordering credentials associated with a certain Device Type, the Licensee has to complete the following tasks for each Device Type:

- Device Type needs to be validated by the CI Plus Test House (Eurofins Digital Testing) against a given list of criteria, unless the Licensee has self-test rights in which case the Device Type needs to be validated by the Licensee.
- Licensee has to complete and provide the applicable CI Plus Robustness Certification Checklist to DigiCert (Exhibit ECP_G of the ILA Addendum for ECP for ECP Device Types, Exhibit G of the Interim License Agreement for Standard Device Types)
- Licensee has to complete and provide a Registration Application form containing information for DigiCert that is required to configure the new Device Type. This form has to be signed by the Test House prior to the submission to DigiCert, unless the Licensee has self-test rights for the Device Type being registered.

The Product Manufacturer must complete the applicable CI Plus Robustness Certification Checklist (Exhibit G or Exhibit ECP_G) and the Registration Application and return them to DigiCert at:

DigiCert, Inc.
CIPlus Services
Unit 21 Beckett Way
Park West Business Park
Dublin 12
D12 C9YE, Ireland

Courier contact phone number (Post office): +353 1 255 2935

Email: ciplus@digicert.com

To speed up the on-boarding process, a signed and scanned copy of these forms can initially be provided by email to DigiCert. However, the Licensee must return the completed and signed paper-based forms to DigiCert for archiving and audit purposes.

5.3.1 CI Plus Robustness Certification Checklist

For Standard Device Types, the CI Plus Robustness Certification Checklist (Exhibit G of the ILA) documents the result of a completed self-assessment, done by the Licensee.

The Robustness Certification Checklist form can be found on the CI Plus section of DigiCert's website.

https://knowledge.digicert.com/support/device-certificate-services.html

The Licensee signs the Robustness Certification Checklist by an authorized official and sends it to the address listed above.

5.3.2 CI Plus Robustness Checklist for ECP

For ECP Device Types, the CI Plus Robustness Checklist for ECP (Exhibit ECP_G of the ILA Addendum for ECP) documents the result of a completed self-assessment, done by the Licensee.

The CI Plus Robustness Checklist for ECP form can be found on the CI Plus section of DigiCert's website.

https://knowledge.digicert.com/support/device-certificate-services.html

The Licensee signs the CI Plus Robustness Checklist for ECP by an authorised official and sends it to the address listed above.

5.3.3 Registration Application Form for a New Device Type

In case of Normal Registration (as defined in the ILA) the Registration Application is the result of a physical product test of a device submitted by a Licensee to the official CI Plus Test House Eurofins Digital Testing. The Test House also confirms that the appropriate Robustness Checklist for the new Device Type (Exhibit G of the ILA for Standard Device Types, Exhibit ECP_G of the ILA Addendum for ECP Device Types) is completed correctly and signed by the Licensee. The Licensee then has to provide the Robustness Checklist and the Registration Application form signed by the Licensee and by the Test House to DigiCert to verify that the product meets the requirements as specified by CI Plus.

In case of Self-Test Registration, the Licensee has to provide the Registration Application form (signed only by Licensee) together with a self-test report and the signed Robustness Checklist to DigiCert. Hereby the Licensee assures that the product meets the requirements as specified by CI Plus.

The Registration Application form provides the necessary information to configure a new Device Type on the portal for the Licensee's account.

The Registration Application form can be found at DigiCert's website.

https://knowledge.digicert.com/support/device-certificate-services.html

5.4 Accessing the CI Plus Portal

Once the CI Plus Robustness Certification Checklist and the CI Plus Registration Application form have been reviewed successfully, DigiCert will then include the Device Type on an approved list in the Licensee's portal account.

At this point, the Brand Administrators can access the CI Plus portal to place purchase orders and to download the resulting Device ID credentials. The remainder of this document describes how to use the CI Plus portal and its associated tools to obtain and work with batches of Device IDs.

CHAPTER 6

6 Placing Purchase Orders

This chapter includes the following topics:

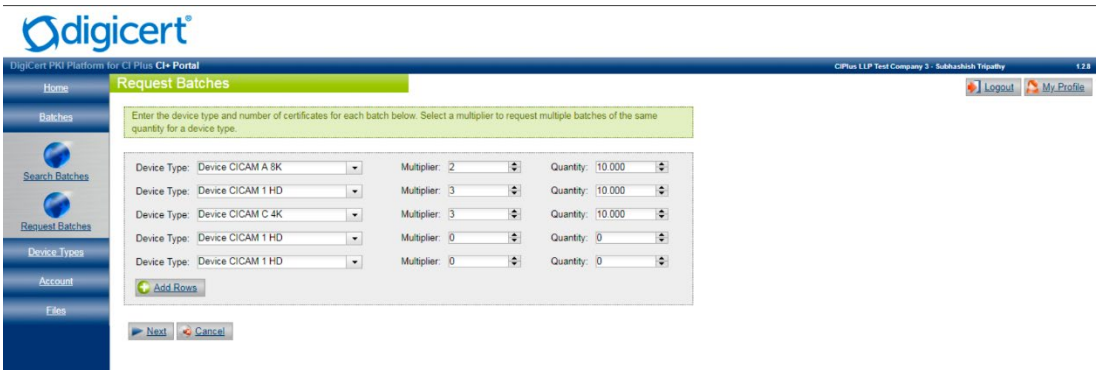
6.1 About Placing Purchase Orders

Once a new Device Type has been configured in the CI Plus portal, DigiCert will accept purchase orders for Device Type credentials. The resulting credentials can then be downloaded from the CI Plus portal. The credentials are provided as a compressed archive file which has been encrypted with the Licensee Brand Administrators' certificates in order to avoid unauthorized usage. The file is called a certificate batch.

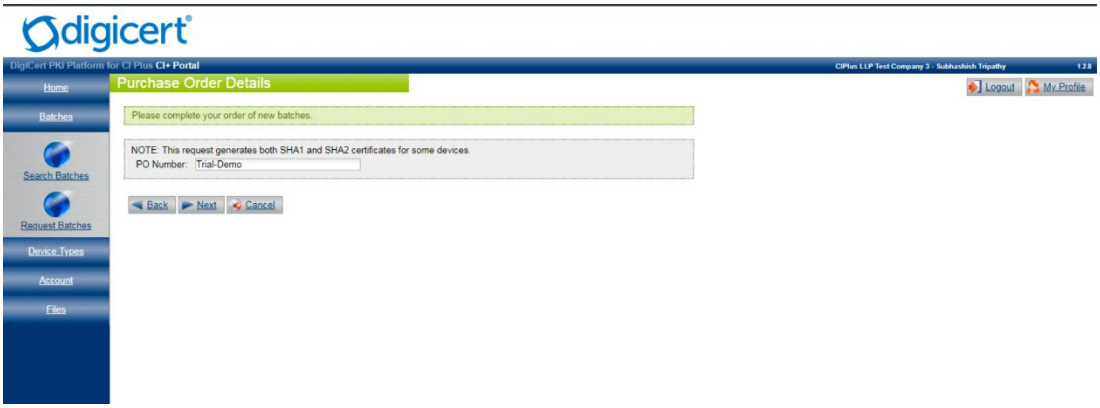
To place purchase orders:

1. Log into the CI Plus portal using the Brand Administrator certificate on the security token. The link to the CI Plus portal is provided by the DigiCert representative once the CI Plus portal account has been configured and access has been granted.
2. Select **Request Batches** and enter the batch request information:
    - Select the Device Type.
    - To request multiple batches of the same quantity for this Device Type, select a batch multiplier.
    - Select the batch quantity (number of devices these certificates are for).
    - Note that for devices supporting the 2 Roots of Trust, batches of SHA-1 certificates (for CI Plus Root of Trust) and batches of SHA-2 certificates (for CI Plus 2nd Root of Trust) will be automatically generated.

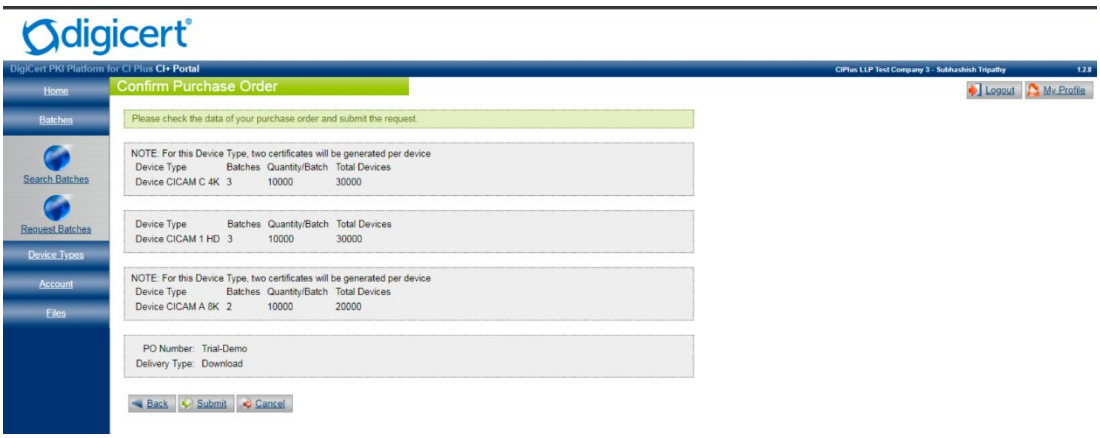
Complete a new row for each different Device Type or for each different quantity for the same Device Type.



3. Click Next.
4. Enter a purchase order (PO) number, if desired. This number is your own reference number, and will appear on the DigiCert invoice so that you can track this purchase order in your invoicing process. Use a unique number for each purchase order.

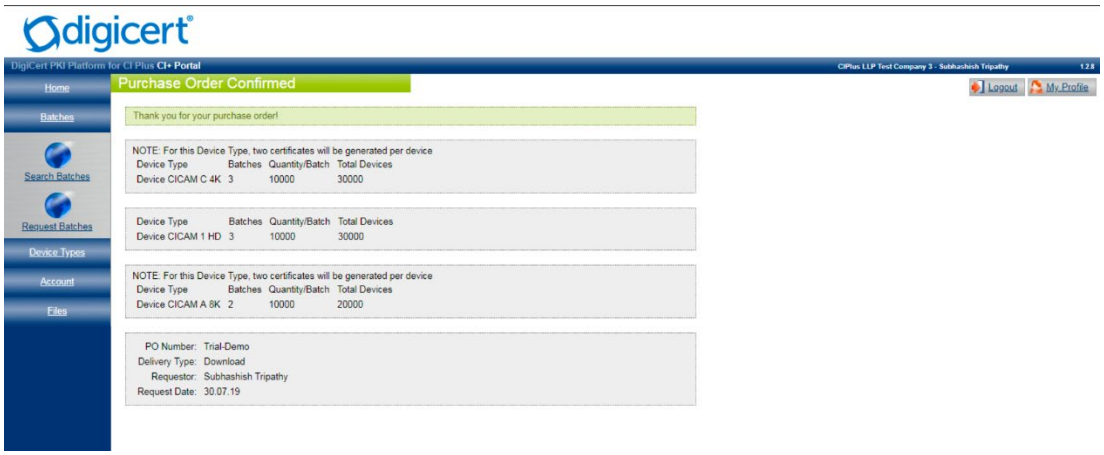


5. Click Next to view a summary of your purchase order. Device Types that support the two Roots of Trust will be provisioned with two certificates per device, as reflected in the summary.



6. Review the order and click Submit.

   DigiCert will process the order and notify you when the certificate batch file is ready for download.



CHAPTER 7

7 Certificate Batches and the CIPLock Tool

This chapter includes the following topics:

7.1 About the CIPLock Tool

Due to the sensitive nature of the production Device ID credentials, they are provided only in an encrypted manner. The provision of these credentials is done in batches that are encrypted and made available in each Licensee's CI Plus portal account. A batch itself is a zip archive that contains the Device IDs (certificate and associated private key).

The batch files contain X.509 certificates in binary DER format with corresponding private keys. All files are compressed into a zip archive which then has been encrypted with all Brand Administrator certificates of a particular Licensee. This file then has been signed with a DigiCert signing certificate in order to allow signature verification and detect any modifications that occurred after file generation.

To work with certificate batches, DigiCert provides the CIPLock tool, that verifies and decrypts them.

7.2 Obtaining Certificate Batches

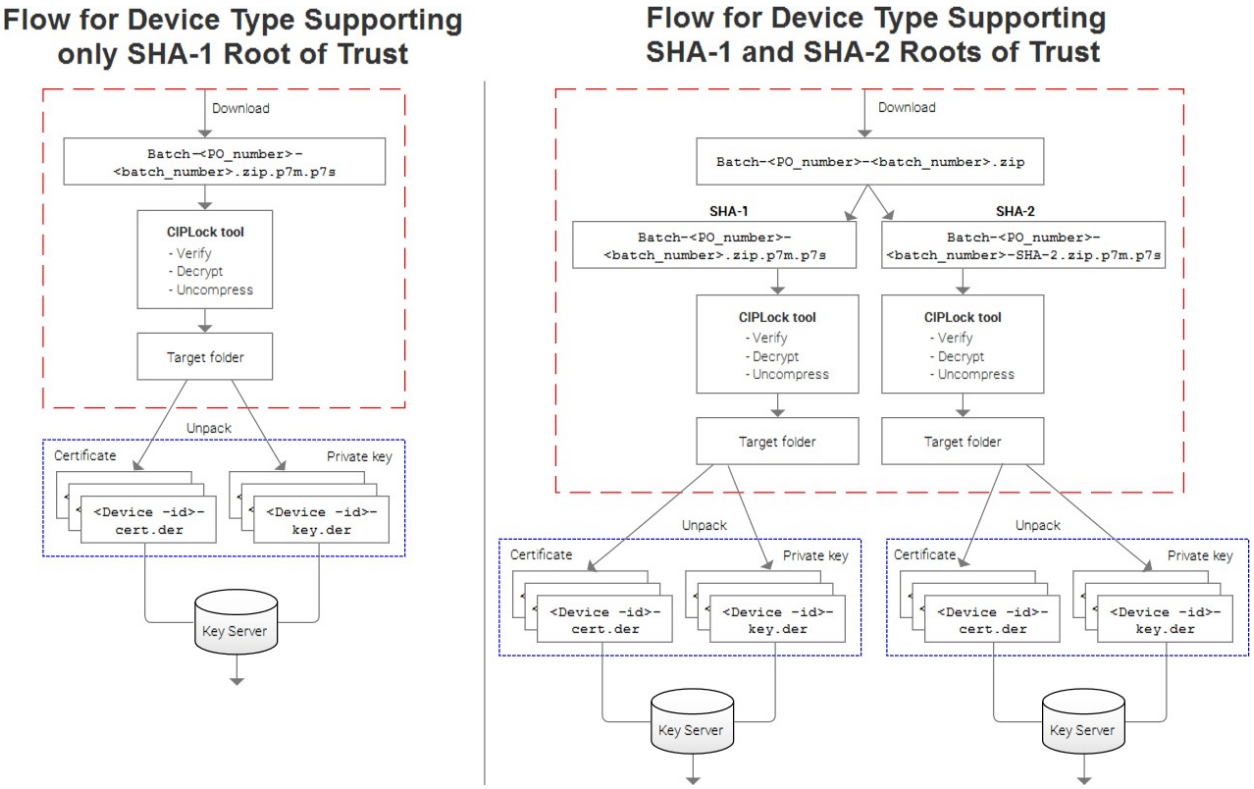
When a purchase order has been approved and released by DigiCert, the certificates are issued and a zip file archive per batch is created for each Root of Trust supported by the Device Type. Each archive is then encrypted with the Decrypt Officials credentials of a particular Licensee, signed by a DigiCert certificate and made available for download in the Licensee's portal account. When the batch file has been created successfully, an automatic email notification is sent to all Brand Administrators that informs them about the new file and its availability for download.

To download the batch file(s), the Brand Administrator logs into the portal and goes to the Batches section. The download can be started by selecting the download icon.

See “Batch File Structure” on page 29.

7.3 Batch File Structure

The following diagram gives an overview of a batch file structure:



7.3.1 Additional File Checks

DigiCert recommends that the following checks are made after batch download.

- File name: SHA-1, SHA-2, or Dual (SHA-1 + SHA-2)
- File size
- File integrity
- File encryption

File Name – SHA-1

The file name convention for the batch file is:

Batch-<PO_number>-<batch_number>.zip.p7m.p7s

For example: Batch-1234567890-1.zip.p7m.p7s

Check that the PO number in the file name refers to the purchase order.

File Name – SHA-2

The file name convention for the batch files is:

Batch-<PO_number>-<batch_number>-SHA-2.zip.p7m.p7s

For example: Batch-1234567890-1-SHA-2.zip.p7m.p7s

Check that the PO number in the file name refers to the purchase order.

File Name – Dual (SHA-1 + SHA-2)

The file name convention for the batch file is:

Batch-<PO_number>-<batch_number>.zip, which contains Batch-<PO_number>-<batchnumber>.zip.p7m.p7s and Batch-<PO number>-<batch number>-SHA-2.zip.p7m.p7s

For example: The downloadable file is Batch-PO2-1.zip, which contains Batch-PO2-1.zip.p7m.p7s (contains 10k cert/key pairs) and Batch-PO2-1-SHA-2.zip.p7m.p7s (contains 10k cert/key pairs)

Check that the PO number in the file name refers to the purchase order.

File Size

Plan for about 24 MB of data for 10,000 certificates. Verify that the file size approximately matches the requested number of certificates.

File Integrity

Verify the PKCS#7 signature to confirm the integrity of the downloaded file and check that the signer certificate has been issued by DigiCert and that it has not been revoked. These checks can be done with the help of the CIPLock tool or any other tool that is able to verify PKCS#7 signatures and signer certificates.

File Encryption

Verify that you are in possession of a matching decryption key/certificate to decrypt the downloaded file. The easiest way to do this is to decrypt the file with the help of the CIPLock tool.

7.4 CIPLock Tool

DigiCert provides the CIPLock tool which can be used to verify and decrypt the certificate batch files. Due to export restrictions the tool is based on publicly available cryptographic components that have to be downloaded and installed before the tool itself can be used to decrypt the batch files. The CIPLock install link can be found in the Licensee's Portal account where also an explanation about the preconditions is provided.

The tool has the following options:

- Verify, decrypt and unpacking (decompress)
- Verify only
- Decrypt and unpack only (but no verify)

You must run the verify, decrypt, and unpack options in online mode, or you will get an error message that the software is unable to verify the signature and then aborts the operation.

Installing the CIPLock Tool

Complete the following steps to install the CIPLock tool.

1. Verify the machine requirements:

   - The CIPLock tool will run only on machines with a Windows operating system.
   - Due to the expected maximum file size of the Device ID batch files the machine where the CIPLock tool will be installed requires at least 2 GB of physical memory.
   - The machine must have an active Internet connection when you install the CIPLock tool. Once installed, you will also be able to run it in offline mode.

2. Acquire security tokens.

   See “Security Tokens” on page 6.

3. Install the third-party applications. Refer to the instructions on the following web page to download and install the third-party applications you will need in order to run the CIPLock tool: https://ciplus.pki.digicert.com/CIPLock/.
4. If you will use the CIPLock tool to decrypt the test set provided by DigiCert (as part of testing the test set), you must import the CI Plus Test Root CA certificate and the CI Plus Test Brand CA certificate onto the security token designated for the testing.
5. Click the Install and launch CIPLock link on the web page listed in step to launch the CIPLock tool for the first time. Once you have launched it for the first time, a CIPLock tool icon is added to your desktop and to the Welcome page of the CI Plus portal.

7.4.1 Running the CIPLock Tool

Use the following procedures to run the CIPLock tool to verify and decrypt certificate batches.

1. Verify that the token containing the Brand Administrator certificate is inserted correctly and that the Brand Administrator certificate is valid.

   If testing the test set provided by DigiCert, use the test security token containing the test Brand Administrator credentials.

2. Open the CIPLock tool by double-clicking the CIPLock tool on your desktop, or by clicking the Launch CIPLock tool link on the Welcome page of the CI Plus portal (available by clicking Home in the left pane of the CI Plus portal).
3. In the first field, browse to the encrypted certificate batch file.
4. Select an action to perform on the certificate batch file:

   - Select **Verify, decrypt, and unpack** to verify the signature of the certificate that signed the batch file, decrypt the private keys and certificates in the batch file, and write them to the target directory, in unencrypted format. This option can only be performed if there is an active Internet connection to validate the status of the signing certificate.
   - Select **Verify only** to verify the signature of the certificate that signed the batch file. This option can only be performed if there is an active Internet connection to validate the status of the signing certificate.
   - Select **Decrypt and unpack** only to decrypt the private keys and certificates in the batch file, and write them to the target directory, in unencrypted format. This option can be used when in offline mode, and it will skip the signature verification (which requires an Internet connection to validate the status of the signing certificate). When this option has been selected the tool will grey out the steps that are skipped in the process.

5. Enter the target directory in the second field.
6. Click Open and process archive.
7. If an option with decryption has been selected, a dialogue will show up, asking for the PIN of the security token.
8. The result should be a directory containing files with the naming convention xxx-key.der and xxx-cert.der. These are the certificates and corresponding private key files.

7.4.2 Using CIPLock Tool on Multiple Machines

You can use the CIPLock tool on multiple machines, as long as you have inserted the token containing the Brand Administrator certificate. However, PKI Client must be installed on each machine that will run the CIPLock tool. The latest version of PKI Client is always available on PKI Manager.

1. Access PKI Manager.
2. Click the Resources icon in the left side of the footer.
3. Click Download under DigiCert® PKI Client, click Save, and save the resulting .zip file to a temporary location.

   If you will install PKI Client on another machine, copy the resulting .zip file to a temporary location on the machine where you will install it.

4. Unzip the file.
5. Install PKI Client:

   - On Windows machines, double-click the PKI Client .msi file.
   - On Mac machines, open a Command Prompt (Finder D> Applications > Utilities > Terminal) and enter the following command:
   - installer -pkg DigiCert-PKI-Client-x64.2.6.x.pkg -target /
   - Follow the prompts to complete the installation.

Refer to *DigiCert® PKI Client Administrator's Guide* (provided in the PKI Client.zip file) for complete details on installing and configuring PKI Client.

CHAPTER 8

8 CI Plus Portal Overview

This appendix includes the following topics:

- About this Overview
- Device Types
- Configuration
- Additional Files in the Portal Account

8.1 About this Overview

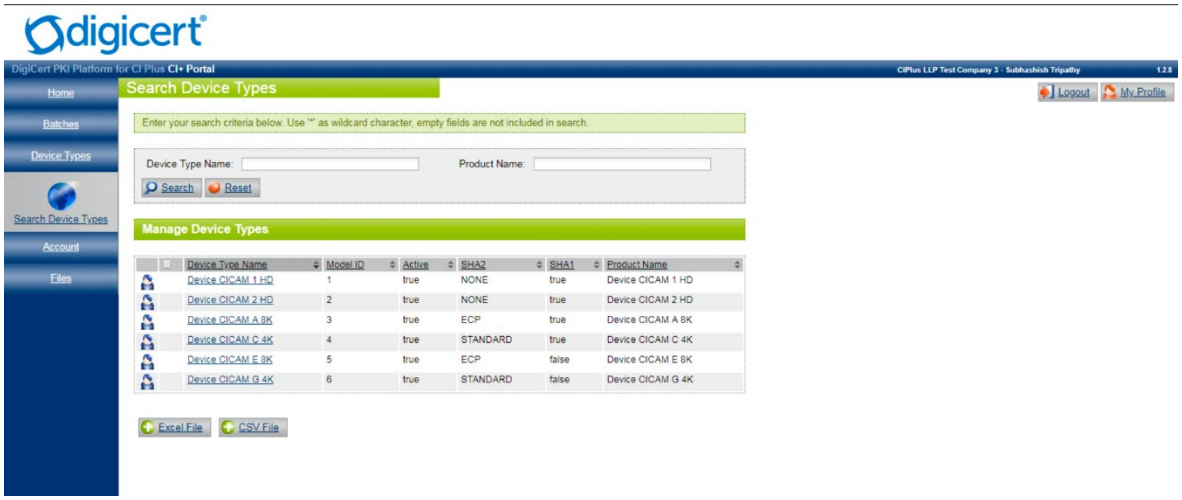
The CI Plus portal offers other resources and tools in addition to placing purchase orders and downloading certificate batches. This appendix provides an overview of the portions of the CI Plus portal not described earlier.

- See "About Placing Purchase Orders" on page 25.
- See "About the CIPLock Tool" on page 28.

8.2 Device Types

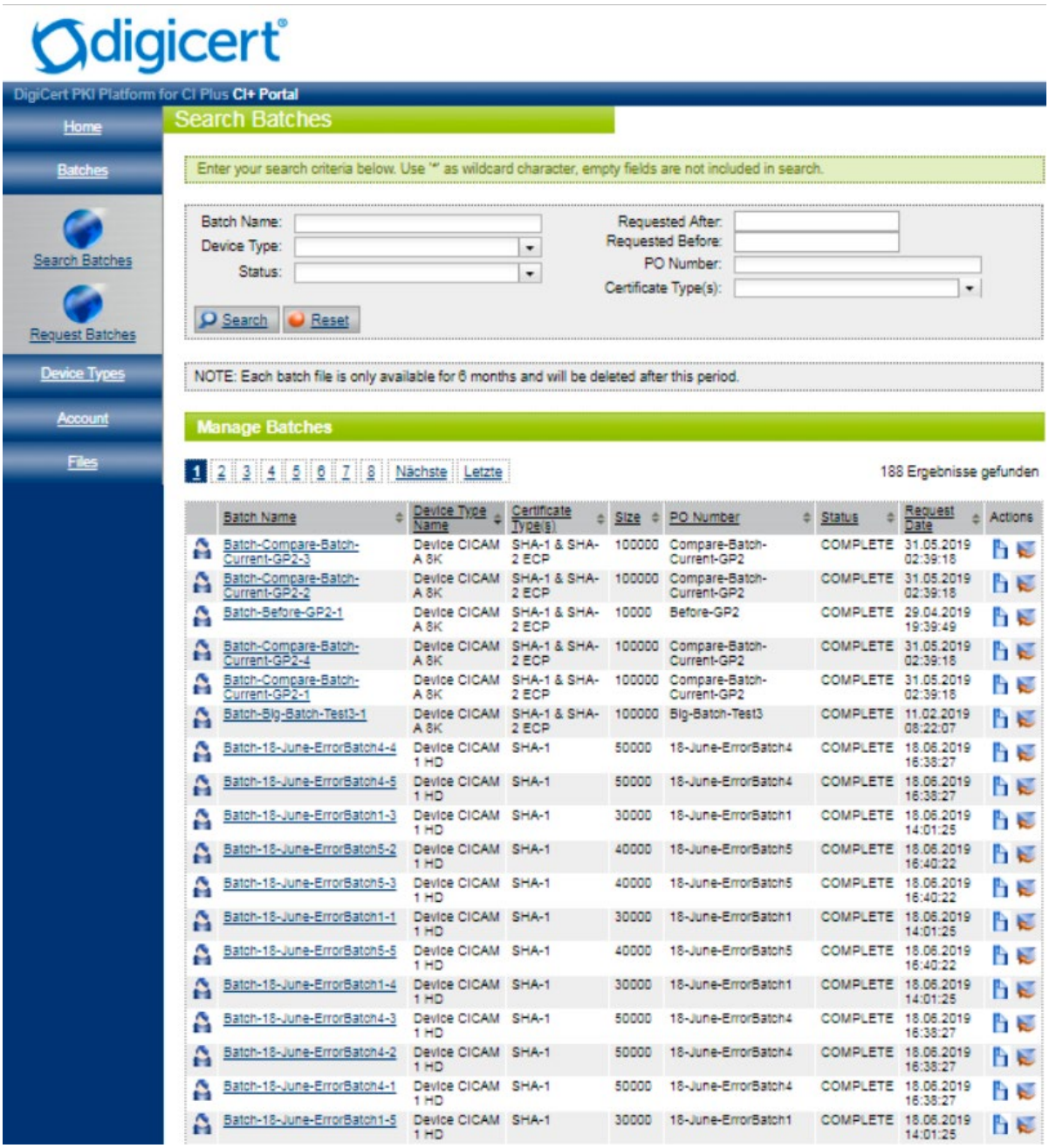
The Search Device Types page provides an overview of the configured Device Types in a Licensee's portal account. A new Device Type will be configured by DigiCert whenever Device has been tested successfully (either through the Test House or self-testing), and the Licensee has returned the completed and signed Registration Application form and Robustness Certification.

See "Configuring the Device Type" on page 22.



8.2.1 Batches

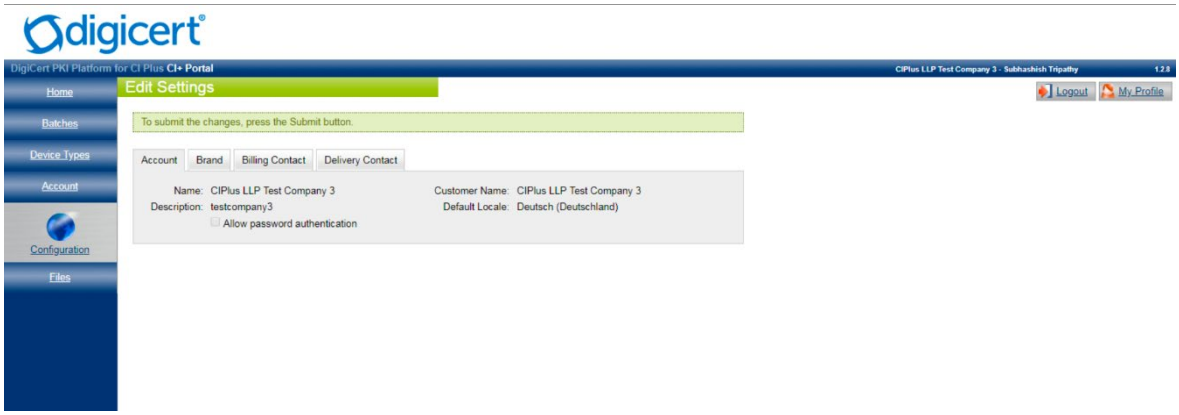
The **Search Batches** page provides an overview of the requested batches of certificates. The batches can be searched by various parameters, e.g. Device Type or Certificate Type.



8.3 Configuration

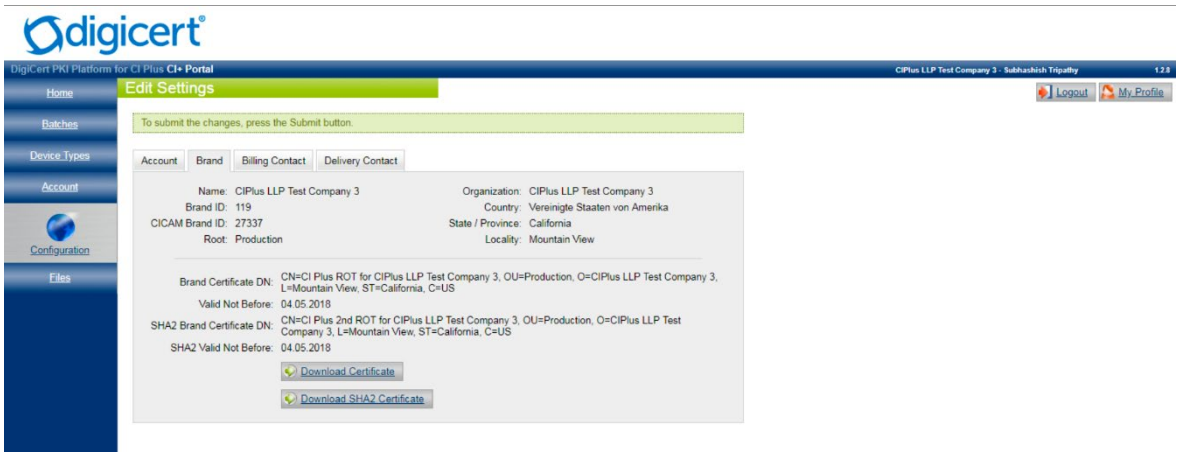
The Configuration page provides an overview of the account details, delivery contact and billing contact. In addition, on this page the Brand CA certificate of the Licensee is also made available for download.

By default, the page opens to the Accounts tab. The Accounts tab gives information about the account details, such as Account name and additional description.



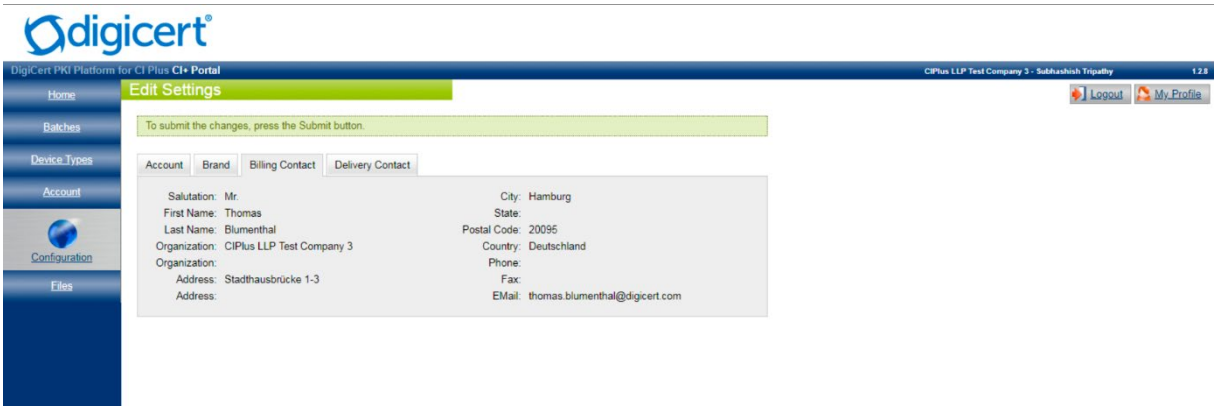
8.3.1 Brand CA Certificate

In the Brand tab, the Brand CA certificate is provided for download. The Licensee must select Download Certificate to download the Brand CA certificate.



8.3.2 Billing Contact

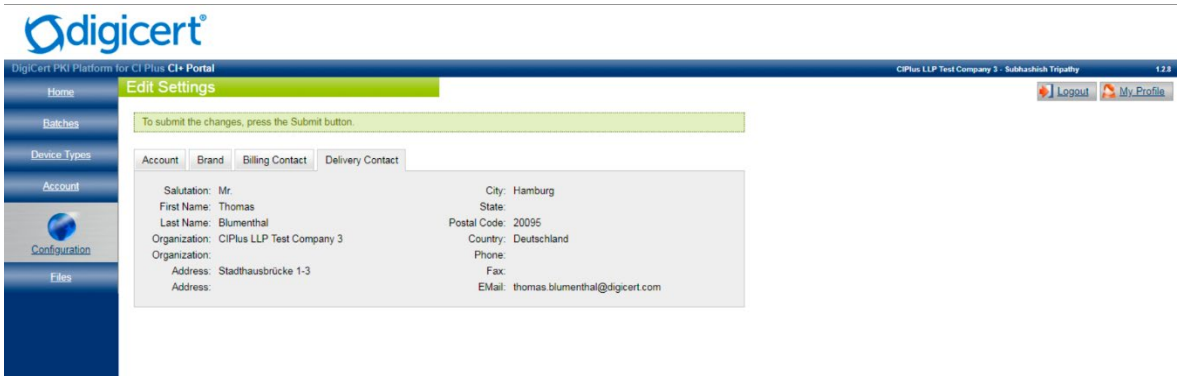
In the Billing Contact tab, the contact for the billing of ordered Device IDs is configured. If this contact should be changed, an updated and signed Brand On-Boarding form has to be provided to DigiCert.



8.3.3 Delivery Contact

In the Delivery Contact tab, the contact for the delivery of additional physical documents or items is configured. This delivery contact is optional.

If the delivery contact details should be changed, an updated and signed Brand On-Boarding form has to be provided to DigiCert.



8.4 Additional Files in the Portal Account

The CI Plus portal also provides a section where additional files can be downloaded by the Licensee. In particular the following files are available:

- CI Plus Root CA certificate. The Root CA certificate is the uppermost certificate in the CA certificate hierarchy. The Root CA certificate issues the brand CA certificate for each manufacturer/Licensee. It might be used by a Licensee during the verification process of the Device ID credential.
- CI Plus 2nd Root CA certificate. The 2nd Root CA certificate is the uppermost certificate in the new CA certificate hierarchy for the CI Plus 2nd Root of Trust. The 2nd Root CA certificate issues the 2nd Root brand CA certificate for each manufacturer/Licensee. It might be used by a Licensee during the verification process of the 2nd Root Device ID credential.

Note: Both Root CA certificates are valid until 2099. This may lead to an error message if the certificate is opened in a standard browser (the expiration date may be displayed as a date in the past).

- CI Plus Production License Constants. The Production License Constants contain the keys used in the CI Plus scheme. They have to be handled with uppermost care and are highly confidential. Unauthorized access to the License Constants is not permitted and would eventually compromise the CI Plus security.
- CI Plus 2nd Root of Trust Production License Constants. These Production License Constants contain the keys used in the CI Plus 2nd Root scheme. They have to be handled with uppermost care and are highly confidential. Unauthorized access to the License Constants is not permitted and would eventually compromise the CI Plus security.
- CI Plus License Specification - Addendum for Production. This is an addendum to the License specification and describes the algorithms to compute various production keys. This document has to be kept confidential and any unauthorized access or publication is not permitted.
- CI Plus Device ID Forecast form. The forecast form has to be used by the Licensees to notify DigiCert about the monthly required number of Device ID credentials and covers a three-month sliding window. The forecast is non- binding which means that there is no obligation of the Licensee to request the forecasted number of Device ID credentials. However, it is used by DigiCert for the monthly capacity planning and is the basis for the SLA in terms of delivery time for the ordered credentials.

- CI Plus Brand Administrator Revocation form. In some situations, a Brand Administrator certificate has to be revoked (for example, the certificate was issued to the wrong administrator, the administrator has left the Licensee's organization, or the Brand Administrator certificate has been lost or compromised.). To revoke a Brand Administrator, complete the revocation request form and send it to DigiCert at:

  DigiCert, Inc.
  CIPlus Services
  Unit 21 Beckett Way
  Park West Business Park
  Dublin 12
  D12 C9YE, Ireland

  Courier contact phone number (Post office): +353 1 255 2935

  Email: ciplus@digicert.com. To ensure proper delivery, include CI Plus in the subject line of all email communications.

To speed up the revocation process, a signed and scanned copy can initially be provided by email to DigiCert. However, the Licensee must return the completed and signed paper-based forms to DigiCert for archiving and audit purposes.

This request may take up to 1 business day to complete. Once the certificate is revoked, the Brand Administrator will not be able to log into the CI Plus portal, place purchase orders, or download certificate batches. You can issue a replacement certificate to the Brand Administrator, if appropriate.