



Instructions for activation and installation of the Certum Code Signing certificates on a virtual card

version 1.1

Table of contents

1. Product description	3
2. Account registration	3
3. Initiation of certificate activation	3
4. Completion of the form during activation	3
5. Verification	5
5.1. Document-based verification	5
5.2. Verification with AriadNEXT	6
5.2.1. Verification using a computer	6
5.2.2. Mobile phone verification	9
6. Access emails to the SimplySign service	9
7. Installation of the Simply Sign app	9
8. Activation of access to SimplySign service	9
9. Reading the QR code	11
10. Import the certificate from the Simply Sign Desktop level	11

1. Product description

Certum Standard Code Signing is a certificate for digitally signing software code. The certificate is stored on a Simply Sign virtual card.

2. Account registration

To purchase a certificate, you need to create an account in the Certum store and then select the product you want to buy. To create an account, please follow this link: <https://sklep.certum.pl/customer/account/login/> and then follow the displayed steps. If you already have an account, please log in.

3. Initiation of certificate activation

Once you have placed your order, initiate the activation of your certificate from the [Certificate Activation](#) tab.

In order to do so, locate the appropriate certificate on the list and then click the [Activate](#) icon.

Service name	Order date	Order Number	Payment state
Standard Code Signing, 1 year Issue	May 6, 2020		Payment booked Inactive certificate Activate

The Service Activation window will pop up with the [Key generation via the SimplySign service](#) option automatically selected. Click [Next](#).

Kody elektroniczne

Aktywacja

1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi: Standard Code Signing SimplySign, 1 rok Wydanie

Wybierz sposób dostarczenia kluczy dla certyfikatu

generowanie kluczy na karcie przez usługę SimplySign

[Dalej >>](#)

4. Completion of the form during activation

The next step is to complete the certification request form with the data that will be contained in the certificate. Please note that the fields with an asterisk * are mandatory. After filling in the data, click [Next](#)

Applicant data:

Name * Dominik
Surname * Lowczyński
Phone * 123456789
Email * dominik.lowczyński@assecods.pl
Registration Number

Certificate Data: If you want to issue a certificate for maximum validity period, don't fill „end of validity” field

Common name * Asseco Data Systems S.A.
Hash function RSA-SHA256

End of validity 2022-02-19

Business category * Business entity
Organization * Asseco Data Systems S.A.
Organizational unit Certum
Registration Number * 0000421310
Street and house number
Locality * Gdynia
Postal code
Country * Poland
State
Jurisdiction of incorporation locality name
Jurisdiction of incorporation country name * Poland
Jurisdiction of incorporation state or province name

Previous Next

Note! If you enter your email address in the Email field, a verification link will be sent to the address provided. If you do not want to verify your email address, leave this field empty!

Having clicked Next, carefully verify that the information entered is correct and choose the manner in which Certum’s team will confirm your Identity. Telephone and document-based verification is available.

Please check Your data. After activation correction is not possible.

Certificate Structure:

Subject CN=Asseco Data Systems, O=Asseco Data Systems S.A., OU=Certum, L=Gdynia, C=PL

Verification method *
 verification using subscriber documents
 verification via phone number

The contact phone number used for the phone verification of the certified organization has to match the number found in qualified sources of information such as public business and organization registers. In the event of a phone number mismatch, the verification will be carried out using documents.

Terms of Use

BEFORE SENDING TO CERTUM A REQUEST TO ISSUE CERTIFICATE, OR ACCEPTING CERTIFICATE OR THE FIRST USE OF IT, PLEASE READ THE TEXT OF THESE „TERMS OF USE FOR NON-QUALIFIED CERTIFICATES” REFERRED TO AS „TERMS OF USE”. IF YOU DO NOT ACCEPT THESE TERMS OF USE, DO NOT SEND THE REQUEST TO ISSUE CERTIFICATE, DO NOT ACCEPT IT AND DO NOT USE IT.

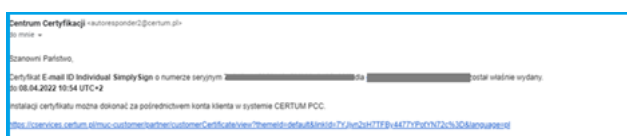
THESE TERMS OF USE BECOMES EFFECTIVE FROM THE MOMENT OF SUBMITTING THE CERTIFICATE REQUEST TO „CERTUM - Certification Authority” (HEREINAFTER „CERTUM”) AND ARE VALID UNTIL THE END OF CERTIFICATE VALIDITY PERIOD OR UNTIL THE CERTIFICATE REVOCATION. SENDING THE CERTIFICATE REQUEST MEANS THAT YOU WANT CERTUM TO REVIEW THE APPLICATION AND ISSUE THE CERTIFICATE, AND MEANS THAT YOU

I agree to Terms of Use *
 I declare and confirm that I am aware of the fact that the certificate may expose my personal data to the extent it has been indicated for inclusion in the certificate. I also confirm that all activities carried out using this certificate may, at my discretion, be available without restriction, in particular with regard to location. The use of the certificate is not affected by Asseco Data Systems S.A., provider of security services. *
 I confirm that I am of age *
 I hereby confirm the accuracy of my personal data included in the application for the certificate. *

Previous Activate

After the activation is completed, you will receive an email with a verification link, using which you must confirm access to the email address entered in the form.

An email with an activation link will be sent to the email address you provided. Click on the link or paste it into your browser to verify the email address associated with the certificate.



After clicking on the link, the you will be redirected to Certum's website, where you need to click on the [Verify](#) icon.

Once the email address has been successfully verified, the certificate will be available in the [Certificate Management](#) tab.

Confirmation of the correctness of the completed process is the receipt of two emails to the address associated with the store account with further steps to be taken.

NOTE: regardless of the address to which the certificate was activated, the email will always come to the email address associated with the Certum store account.

5. Verification

Depending on which verification method you have chosen, you will receive an email with verification instructions.

Note: If you entered an email address in the data for the certificate (in step 4), an authentication message will be sent to the email after activation. One of the conditions of issuing the certificate will be clicking on the verification link.

5.1. Document-based verification

Issuance of the Standard Code Signing certificate requires verification of the Subscriber/Organisation identity. For this purpose, the person requesting the certificate should provide [Certum](#) with the following documents:

Verification of the identity of a private person requesting a certificate on their own behalf:

- confirmation of identity at a Registration Desk or Identity Confirmation Point (details: <https://shop.certum.eu/certum-reseller-points-map>) or
- notary confirmation of identity or for faster issuance
- a copy of an identity document of the ordering person (ID card, passport, driver's license, permanent residence card). The copy should be a complete copy of the document (both sides).

Identity can also be confirmed with a valid qualified certificate issued for the Subscriber by [Certum](#).

Verification of the identity of a person requesting a certificate on behalf of an organization:

1.

- confirmation of identity at a Registration Desk or Identity Confirmation Point (details: <https://shop.certum.eu/certum-reseller-points-map>) or
- notary confirmation of identity or for faster issuance
- a copy of an identity document of the ordering person (ID card, passport, driver's license, permanent residence card). The copy should be a complete copy of the document (both sides).

Identity can also be confirmed with a valid qualified certificate issued for the Subscriber by [Certum](#).

And

2. power of attorney or authorization confirming the relationship of the person ordering the certificate with the organization - when the ordering party is not listed in the relevant register as a person authorized to represent the company,
3. company registration document - when the company is not listed in the KRS/GUS/CEiDG register

In justified cases, [Certum](#) may ask you to send additional documents necessary for proper verification.

Please send all the documents collected to [Certum](#) in one of the following ways:

- by e-mail as a password-protected file to the address: ccp@certum.pl (recommended form),

In order to determine how to transfer your password, please contact the Certum technical support line

- by fax to: +48 91 4257 422
- by post to:

Certum
ul. Bajeczna 13
71-838 Szczecin

5.2. Verification with AriadNEXT

The entire process is performed using a computer or other device with access to a camera, from a maintenance-free interface. During scanning, the document Data are automatically extracted and analyzed as well as compared to the Owner's face. The process is based on comparison of a facial image with a photo extracted from an identity document. The biometric solution ensures that the User is present during the identity confirmation. The entire process is live, in real time, and does not require sending documents, they are only scanned during the process to extract the data needed for verification and

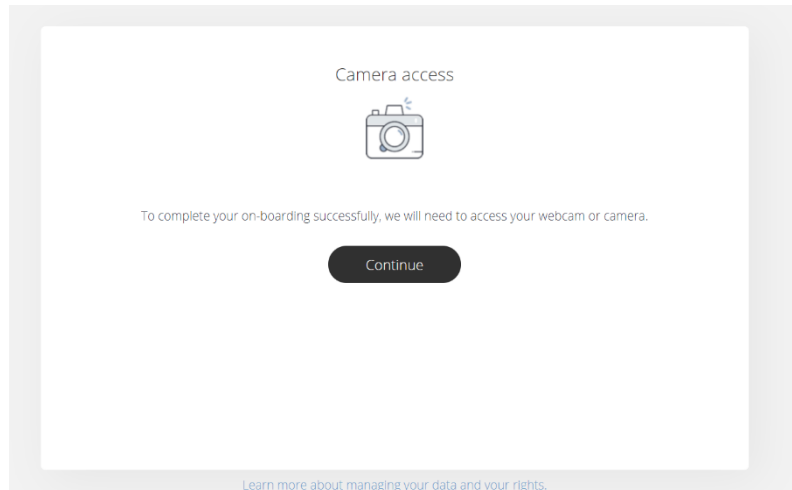
What does the process during certificate activation look like?

- In the certificate activation process, when selecting an identity verification method, select the method: **Automatic identity verification**
- After submitting the application, the User receives a unique link to the indicated email address
- After clicking on the link, the User is taken to the Certum screen on which the Automatic Verification process can be started. The User will then receive a link that initiates verification.
- Depending on the device on which the verification is performed, the process is different.

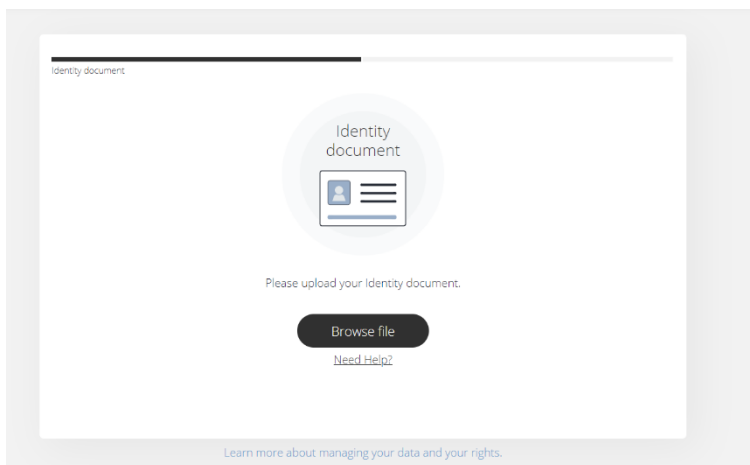
5.2.1. Verification using a computer

Step 1 — Document verification

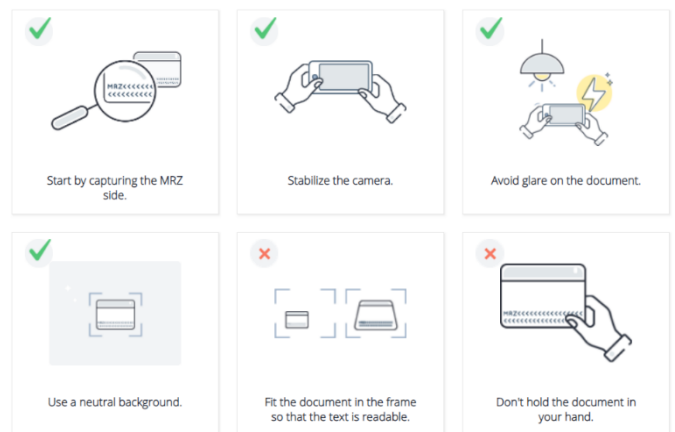
After clicking the link to initiate verification, you will be prompted to turn on your camera, so your identity can be verified. Click "Continue" and proceed to the next step.



You will then be asked to upload a photo of your identification document. The photo provided should be taken according to the guidelines provided during the process.



How to take a good picture of a document.

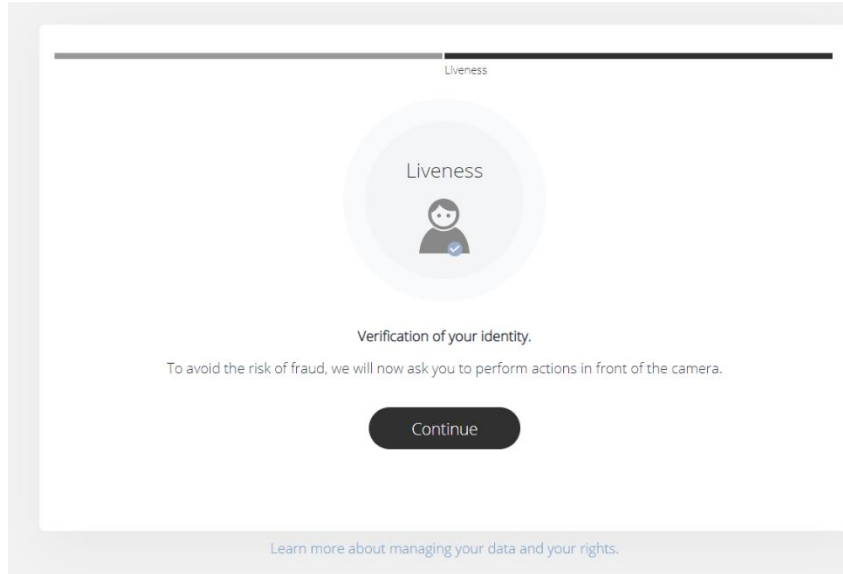


I understand

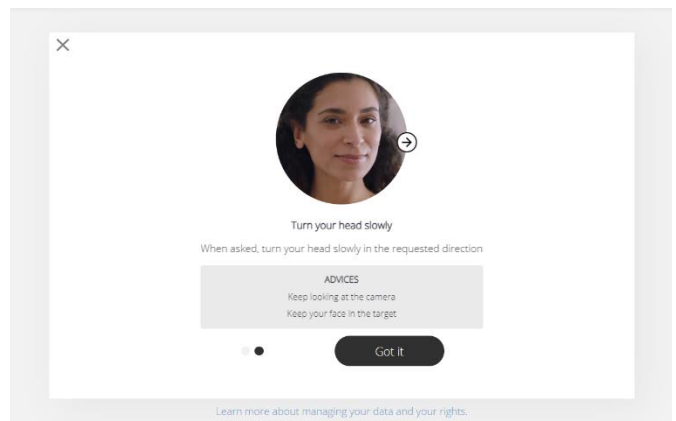
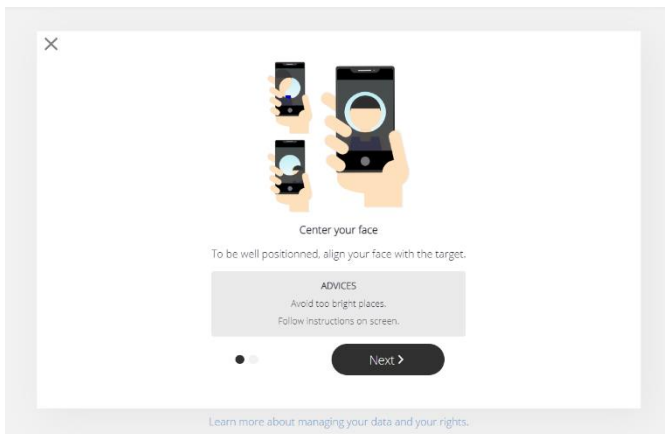
Once the data are submitted, the system will process it for approximately 12 seconds to extract the data from the document. After this process, the document image will be deleted.

Step 2 — Facial comparison

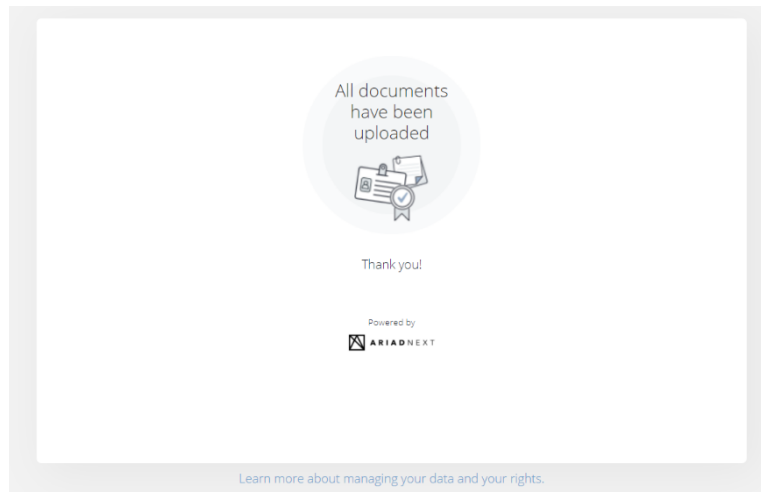
During this step you will be asked to move your face in front of the camera. This biometric solution will ensure that the User is present during the identity confirmation and is the holder of the document.



Performing this step requires you to point your face toward the center of the camera and then move your head toward the right side, looking at the camera the entire time.



After completing this step, a screen indicating that the verification was successful will be displayed. Your certificate will be issued shortly.



5.2.2. Mobile phone verification

The verification process is similar, but in step one, the user does not provide a pre-made photo but takes one live during the process.

Note: In the case of an order placed by a traditional transfer, it is also necessary to register the payment in order to issue the certificate.

6. Access emails to the SimplySign service

Once the certificate has been issued, the Certum system sends the following email messages to the user. At the same time, an account is automatically created for the user who does not have an account in the Simply Sign app. The account is created using the email address of the store account.

a) Confirmation of creating the certificate:

Certificate request has been created

b) Secret code (activation code) needed to recover access to the service

Secret for regaining access to the SimplySign service

c) Recovering access to the service

Regaining access to the SimplySign service

7. Installation of the Simply Sign app

Note: This process is dedicated to users who do not have a Simply Sign account or app. If you have an account with an email address linked to the Certum shop and have the app installed go to the section [Certificate Import](#)

In order to fully activate the service, you will need both the mobile app and the Desktop app:

To download the mobile app, use the links below:

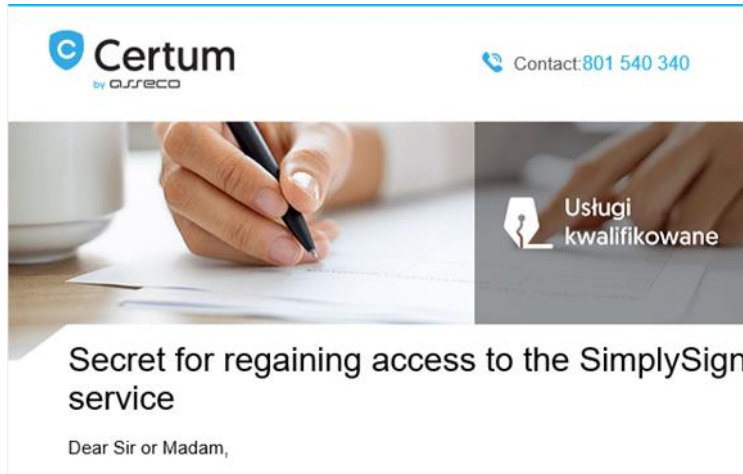
- App for Android phones: Google Play Store: download
- App for iOS phones: App Store: download

To download the PC app, use this link: <https://simplysign.certum.pl/pobierz/>

Make sure you have selected the correct version for your operating system.

8. Activation of access to SimplySign service

In the first step, open the email [Secret for recovering access to the SimplySign service](#). Copy the Secret activation code it contains. It will be required to run the Simply Sign mobile app.



Then open the email titled [Recovering access to the SimplySign service](#). Click on the link [Certum Service](#). Next, a window will open in which you should enter the Secret activation code you copied earlier. Then click the [Send](#) button

Regaining access to the SimplySign service

Dear Sir or Madam,

In order to regain your access to the SimplySign service and the generator of one-time authorization passwords Token, required for logging in / authorization in the Certum service, please follow the instructions below:

- 1. Launch the SimplySign app on your mobile device**
(using this app you should scan the QR code necessary for the authorization of unlocking of the SimplySign service and the generator of one-time authorization passwords Token)
- 2. Prepare the 6 character activation code, which you obtained via the Certum Technical Support.**
- 3. Begin the procedure of recovering access to the SimplySign service by clicking on the link:**

Certum service: <https://model.simplysign.weboznosci.pl/arc/app/resetseed?token=8786d294ac486823556e95b23988333d02ba5ec9e5d3956d5c51e8c474ac70fb>
(Click or copy the link to the web browser and regain access to SimplySign)

Odzyskiwanie dostępu do usługi SimplySign (Recovering access to the SimplySign service)

* Podaj sekret podany przez operatora (Enter secret provided by operator)

A QR code will be displayed, which must be read using the Simply Sign mobile app.

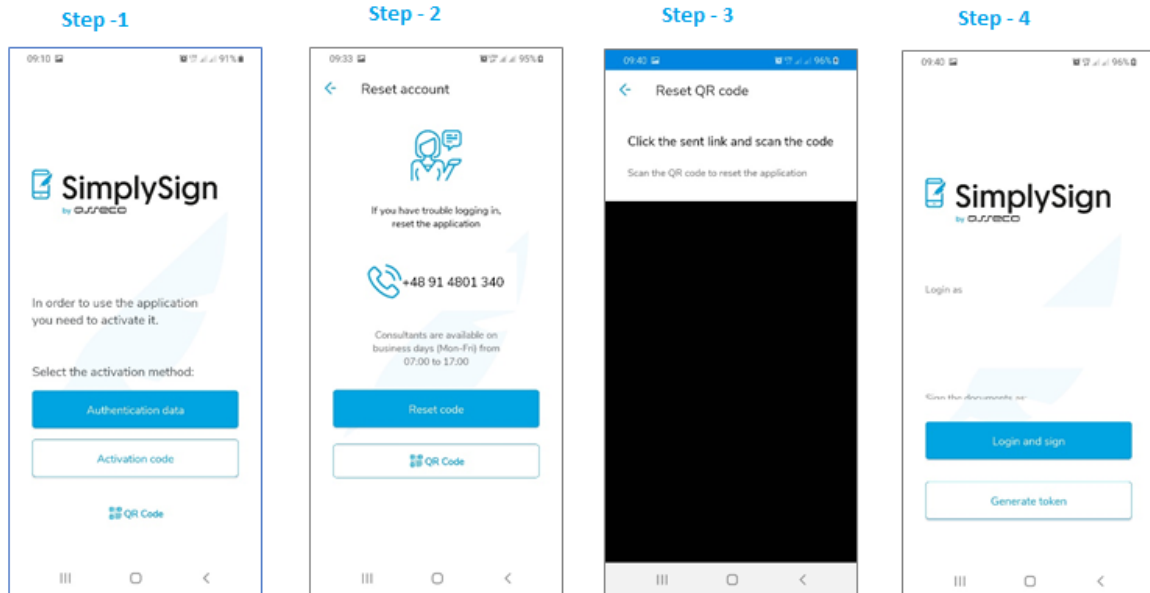


9. Reading the QR code

To read the QR code, follow these steps:

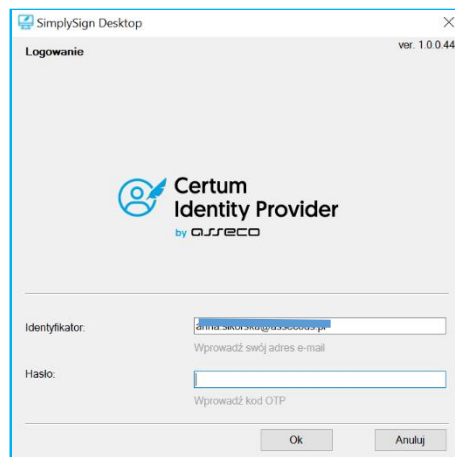
- Run the previously installed SimplySign mobile app
- Click on the QR CODE button
- Allow access to the camera and read the QR CODE value from the browser screen

Once you have completed these steps, the app is ready to run



10. Import the certificate from the Simply Sign Desktop level

To import the certificate ID, you need to open the SimplySign app on your computer. To log in, generate an OTP code (token) in the SimplySign Desktop app, then type it in the Password field. Proceed in this way each time to start the app.



In order to import the certificate, right-click the SimplySign icon in the right-hand corner of the taskbar and then select: [Managing certificates](#) -> [List of certificates](#). Once this command is completed, a window with a list of available certificates will open.

Right-click the certificate you wish to export and choose [Show certificate](#). The details of the certificate will be displayed and the [Install certificate](#) command will be available. Select this command.

The Import Wizard window will then open. Perform the import as the [Current User](#) and Continue. In the next window, select [Automatically select a certificate store](#) and continue.

The final step will be to close the Import Wizard. A confirmation of successful completion of all steps will be a pop-up window stating that the import was successful.