Equipment Certificate – Instructions

Instructions for Windows users.

Table of Contents

1. Introduction

Electronic certificates consist of a **Private Key** and a **Public Key**.

The private key is generated by the certificate holder and is the core component of the certificate.
It must **never be shared** with anyone other than those authorised to manage the certificate on behalf of the company.

The public key is issued by **Auðkenni** together with the intermediate certificate *Fullgilt auðkenni* and may be shared freely, for example with banks.

When applying for an **Equipment Certificate (Búnaðarskilríki)**, the applicant must generate a **CSR (Certificate Signing Request)**. The CSR is used to produce the public key. At the same time as the CSR is created, the private key is generated on the same computer.

Applicants who do not feel confident creating a CSR themselves may request **Auðkenni** to generate it on their behalf for a small fee. In that case, the applicant selects the option:
"I want Auðkenni to generate the CSR."

Auðkenni recommends that applicants generate the CSR themselves. This process is easier than many expect, and detailed instructions are provided later in this document.

How do I apply for an Equipment Certificate?

The application process is as follows:
The applicant completes the Equipment Certificate application form on the Auðkenni website:
https://www.audkenni.is/en/information/company-registration-certificate/application-for-equipment-certificate

In the application, the applicant must specify:

- a **Technical Contact**, and
- an **Authorised Representative / company signatory**.

Regarding the CSR, two options are available:

1. The applicant generates the CSR themselves and enters it into the application form (**recommended by Auðkenni**).
2. The applicant chooses to have **Auðkenni** generate the CSR.

Option 1: The applicant generates the CSR
Once the application is approved, **Auðkenni** generates the public key for the certificate.
Auðkenni sends a **.cer file** containing the public key to the Technical Contact.

If the intermediate certificate *Fullgilt auðkenni* and the root certificate *Íslandsrót* are not already installed on the computer, they must be installed first. Detailed instructions are provided later in this document.

The applicant runs the **.cer file** containing the public key **on the same computer where the CSR was generated**.
The installation wizard completes the process by binding the public key to the existing private key and installing the certificate into the computer's certificate store.

At this point, the certificate is installed on the computer.
The certificate can then be exported to a **.pfx file** and installed on additional machines if required.

Option 2: Auðkenni generates the CSR
Once the application is approved, **Auðkenni** generates both the private key and the public key for the certificate.
Auðkenni sends the Technical Contact a **.pfx file** via a secure file transfer.
The file contains:

- the private key
- the public key
- the intermediate certificate (*Fullgilt auðkenni*)
- the root certificate (*Íslandsrót*)

The file is protected with a password generated by Auðkenni, which is provided to the Technical Contact.
The applicant runs the **.pfx file** on the computer where the certificate is to be installed.
The installation wizard completes the process and installs the certificate into the computer's certificate store.
The certificate may be installed on additional machines if required.

2. Completing the application form, generating the CSR, and creating the private key

The applicant must complete the application form.

An **Authorised Representative** must have signed authority for the company or hold a valid power of attorney.
The **Technical Contact** is the person to whom Auðkenni sends the Equipment Certificate.
Emails are sent to the email addresses of both the Authorised Representative and the Technical Contact.
Both must click the **"CONFIRM EMAIL ADDRESS"** link contained in the emails.
Auðkenni verifies the signing authority of the Authorised Representative.
The application document is then sent to the Authorised Representative for **electronic signature**.
If signing authority is confirmed, the application document is signed, and both the Authorised Representative and the Technical Contact have confirmed their email addresses, the application is approved and the certificate is sent to the Technical Contact.

CSR (Certificate Signing Request)
(This section can be skipped if the applicant has chosen to have Auðkenni generate the CSR.)
The CSR is the core component of the certificate.
When the CSR is generated, the certificate's **private key** is created at the same time. The private key is automatically stored in the computer's certificate store under **Certificate Enrolment Requests**.
Once Auðkenni issues the public key based on the CSR, it is installed on the same computer where the CSR was created.
During the installation process, the system automatically locates the private key, resulting in a certificate that contains both the private and public keys.

CSR configuration ("recipe")
When the application form is completed, a configuration file (referred to here as a "recipe") for the CSR is generated.
The applicant must enter the company's **kennitala** and select a **Common Name (CN)** for the certificate.
The Common Name (CN) is displayed when viewing the certificate in the computer's certificate store, so it should clearly describe the certificate.

The CN, the company's kennitala, and the company name (retrieved from the national registry), along with additional information, are used to generate the CSR configuration.
This configuration is displayed in **Step 2** of the application form.

Below is an example of such a configuration:

```
cd\
c:
mkdir csr
cd csr
chcp 1252
echo [NewRequest] > 5210002790.inf
echo Subject = "CN=Auðkenni-Prófun;SERIALNUMBER=5210002790;O=Auðkenni ehf." >> 5210002790.inf
echo X500NameFlags = 0x40000000 >> 5210002790.inf
echo KeySpec = 1 >> 5210002790.inf
echo KeyLength = 2048 >> 5210002790.inf
echo Exportable = TRUE >> 5210002790.inf
echo MachineKeySet = FALSE >> 5210002790.inf
echo SMIME = False >> 5210002790.inf
echo PrivateKeyArchive = FALSE >> 5210002790.inf
echo UserProtected = FALSE >> 5210002790.inf
echo UseExistingKeySet = FALSE >> 5210002790.inf
echo ProviderName = "Microsoft RSA SChannel Cryptographic Provider" >> 5210002790.inf
echo ProviderType = 12 >> 5210002790.inf
echo RequestType = PKCS10 >> 5210002790.inf
echo KeyUsage = 0xe0>> 5210002790.inf
echo HashAlgorithm = sha256 >> 5210002790.inf
cmd /c "certreq -new 5210002790.inf 5210002790.txt
del 5210002790.inf
type 5210002790.txt
CSR framleitt!
```

The applicant must copy this text, open the **Command Prompt (cmd)** on the computer, and paste the text into the window.
It is recommended to use **Ctrl+V** to paste.

To open the Command Prompt, press the **Windows key** (to the left of the space bar), type **cmd**, and press **Enter**.

As soon as the configuration text is pasted into the Command Prompt window, the process starts automatically.
This process generates the **private key** and displays the **CSR** on the screen.
The CSR is also saved as a text file in a folder named **csr** on the **C:** drive of the computer.
The file is named using the company's **kennitala**.
The CSR must then be copied and pasted into the application form, after which the applicant can proceed to the next step.

Below is an example of what a CSR looks like:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDrDCCApQCAQAwUjEmMCQGA1UECgwdVGVycmEgdW1odmVyZmlzw75qw7NudXN0
YSBoZi4xEzARBgNVBAUTCjQxMDI4MzAzNDkxEzARBgNVBAMMCkFyaW9uLUxhdW4w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC3039YoT/g1VzWtlcj2iuH
jNxi4CgUaI3MGcMq6SbCZSrPLOp2tYEme+RF8sujX3I1AwjxMASzgMLe8RRaN6Mt
YpsZ5BRM4OYN1FL+PGspG0v9ks0fC5j9Fk40sswRqebR6cAJR13Xi5hsEohrtOwn
lQ0HCi8uhUNOyIpTj/WpCafEd/YchhZdxnjEbx8nlpVkcsngdFaR3fIrXpeOqicJ
+HgQOeI6OeA1Kq4KbxPmPiI5AMxJhlvKmW2KceYFpRmsvnH/UgHBxBi85iJOYFvu
rZAx4SY8FkX/K7DZVGwXC2NkCE92mnySqukqi69DuKzY24k5Z2zmfwy1KQ2LNMuV
AgMBAAGgggETMBwGCisGAQQBgjcNAgMxDhYMMTAuMC4xOTA0NC4yMD4GCSqGSIb3
DQEJDjExMC8wDgYDVR0PAQH/TESTDAgXgMB0GA1UdDgQWBBSAPsM2r+xI1/nd17n7
wooLqqarCzA/BgkrBgEEAYI3FRQxMjAwAgEJDBVBSy1CSk9TU0kuYXVka2Vubmku
aXMMC0FVREtFTk5JXHNnDAdjZXJ0cmVxMHIGCisGAQQBgjcNAgIxZDBiAgEBHloA
TQBpAGMAcgBvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAgAEMA
cgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZABlAHIDAQAwDQYJ
KoZIhvcNAQELBQADggEBAEIHqE683DUycpZnGcozoKJG1uNZy8+k7xgHHtMrMLsA
plewklWgBIS/1zEzaEanMIrnT+2V3fHMZEp86N6+FL5LM2XIs+b4Bk52C/UP/z6S
2R6M4dHdqRY1bpPQhc07IwUXjLpmAlwF0xL+kyFA16mfZ01k4pzu1gN4y0MXsMWq
bzeOC92vgUvqBwNkyfL+psn1Ly9i2pjVvd1f7eTxkZ/R39yenbMl3OsXmzJQuFjt
JRUqjSZSKCIYluUuzRNwtaXlb1I6REYp08DXwI4XlQn/iidg/sdm+P+mP+OdMRH6
Nx2wIttPQ1Cty9/FGDs097QGqcnSCg4EnJi3+IkpavY=
-----END NEW CERTIFICATE REQUEST-----
```

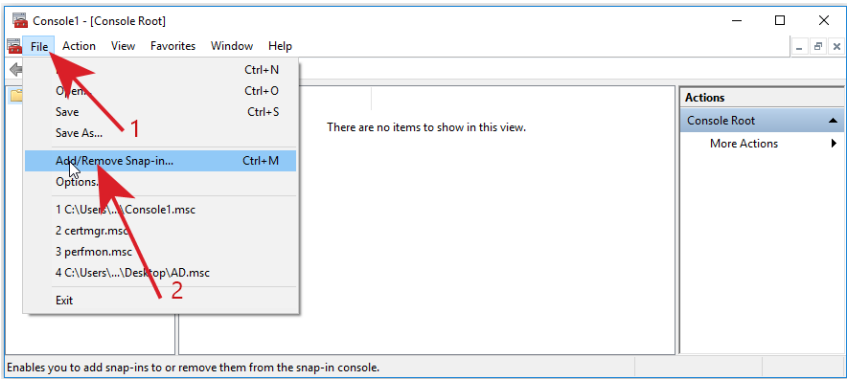
3. Installing the Íslandsrót root certificate and the Fullgilt auðkenni intermediate certificate

For the Equipment Certificate to function correctly, both the **Íslandsrót root certificate** and the **Fullgilt auðkenni intermediate certificate** must be installed on the computer.
If Equipment Certificates have not previously been used on the computer, it is likely that Íslandsrót and the intermediate certificate (*Fullgilt auðkenni*) need to be installed.
The safest approach is to check the computer's certificate store to verify whether these certificates are already present.

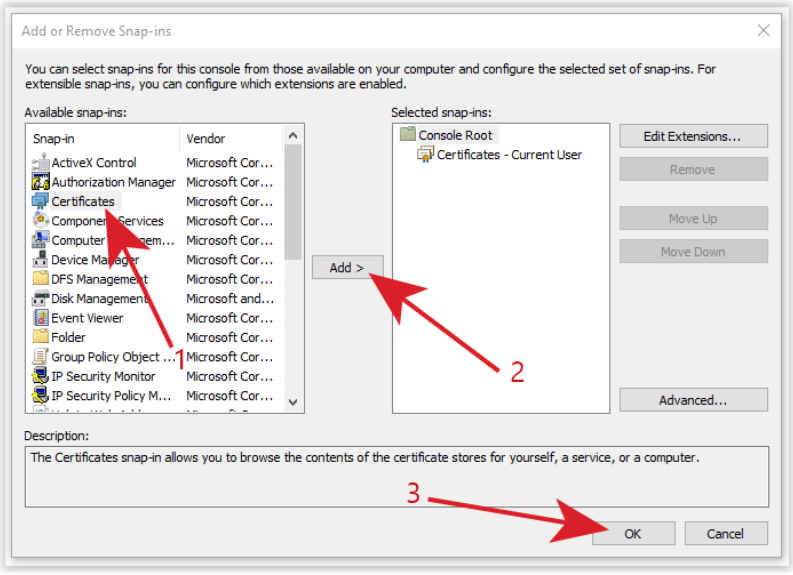
Checking the certificate store using Microsoft Management Console (MMC)
The **Microsoft Management Console (MMC)** is used to view the computer's certificate store.

To start MMC:
1. Press the **Windows key** (to the left of the space bar).
2. Type **mmc** without selecting anything.
3. The **mmc** icon should appear – click it**.**
4. MMC opens and displays the **Console** window.

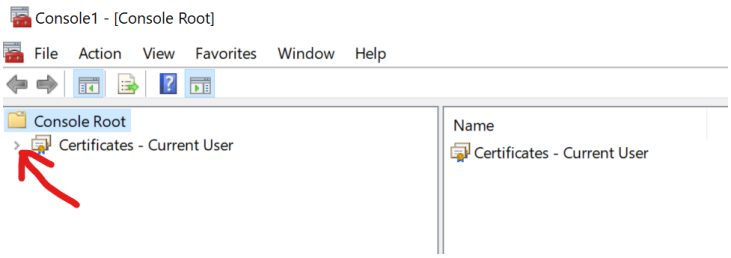
Adding the Certificates snap-in
In the Console window:
1. Select **File**. **2.** Select **Add/Remove Snap-in…**
The **Add or Remove Snap-ins** windows opens.



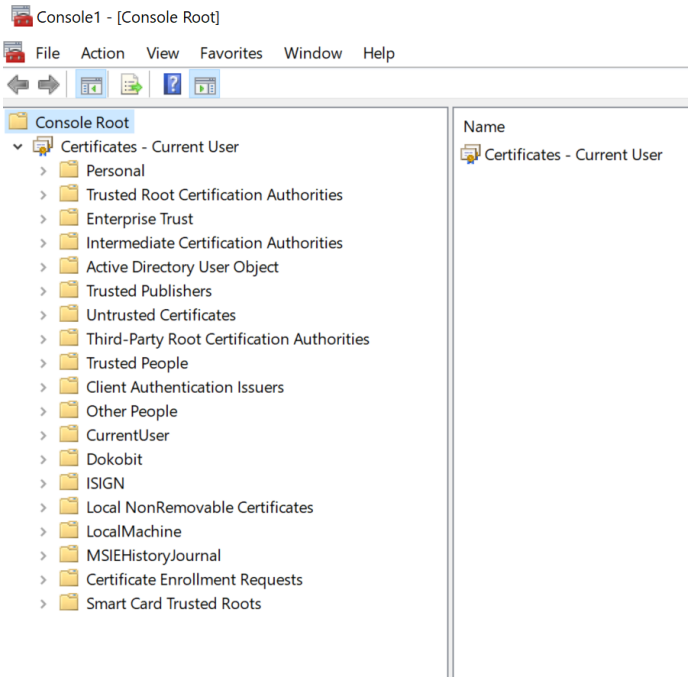
The **Add or Remove Snap-ins** windows opens.
1. Select **Certificates**. **2.** Click **Add >** **3.** Click **OK**



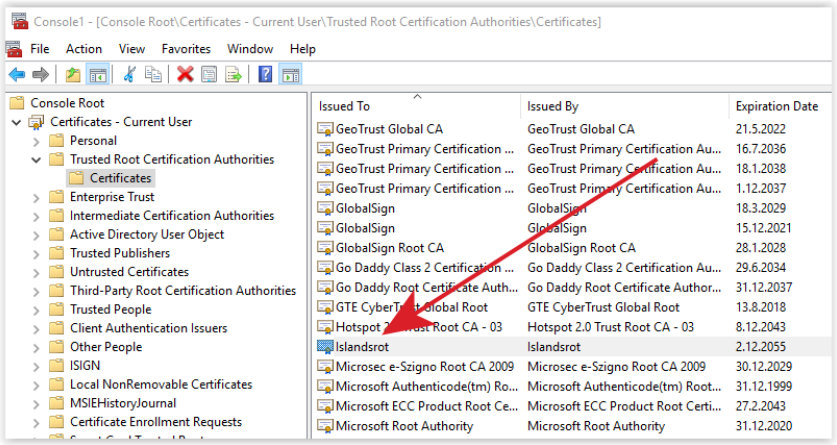
The **Add or Remove Snap-ins** window closes, and **Certificates** is now visible in the Console window.



Verifying certificate installation
Click the arrow to the left of **Certificates** under **Console Root** to expand the tree structure.

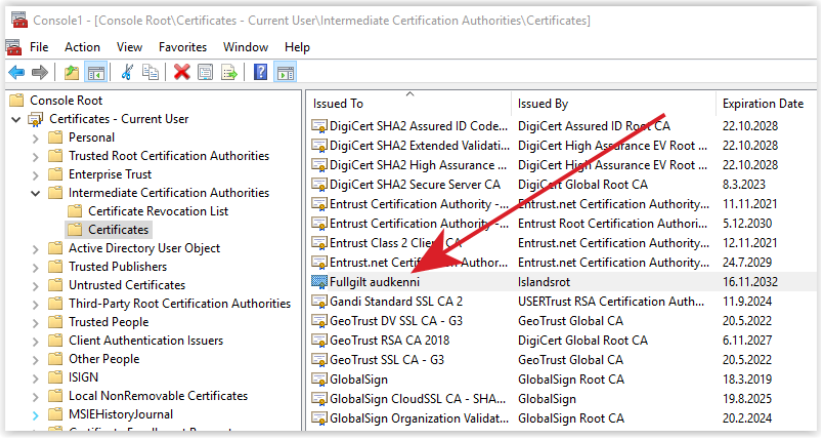


Root certificate – Íslandsrót must be located under: **Trusted Root Certification Authorities / Certificates**



Note: It is normal for many other certificates to be present in this location.

The **Fullgilt auðkenni** intermediate certificate must be located under Intermediate Certification Authorities/Certificates



If certificates have previously been used on the computer, these certificates may already be installed.
If you are unsure, it is recommended to install them anyway – installing them again will not cause any issues.

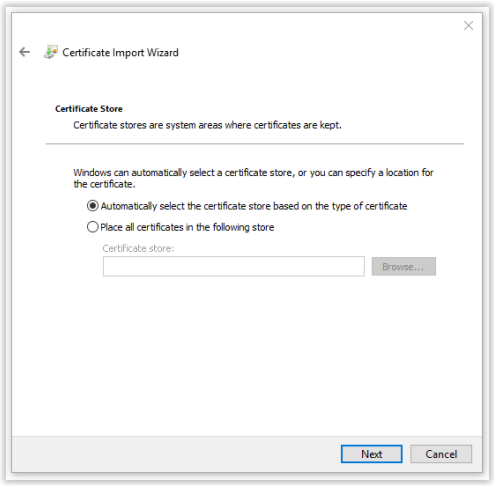
Downloading the certificates
Both certificates can be downloaded from the Auðkenni website:
https://www.audkenni.is/en/information/company-registration-certificate/audkenni-credential-chain
Both certificates must be installed. The installation process is the same for each certificate.

Installing a certificate

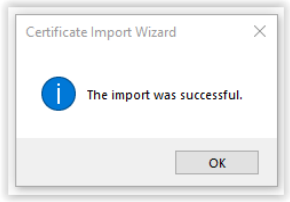
1. Save the **.cer** file to the computer.
2. Right-click the file and select **Install Certificate**.

The **Certificate Import Wizard** opens.

1. Click **Next**.
2. Select **Automatically select the certificate store based on the type of certificate**.
3. Click **Next**.



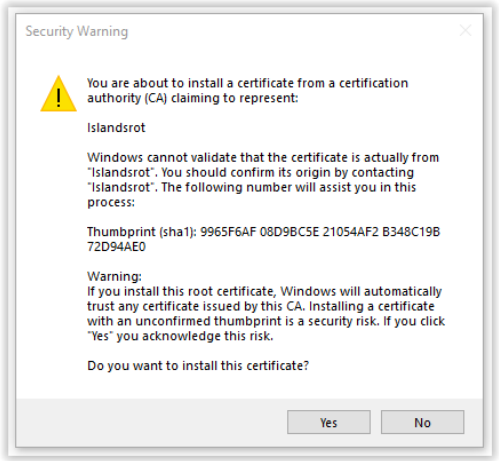
The **Completing the Certificate Import Wizard** screen appears. Click **Finish**.
After a short moment, a message appears stating: **"The import was successful."**



Trust confirmation for Íslandsrót
When installing the **Íslandsrót** root certificate for the first time, a warning message appears asking whether you want to trust the root certificate.

Click **Yes** to trust the root certificate.

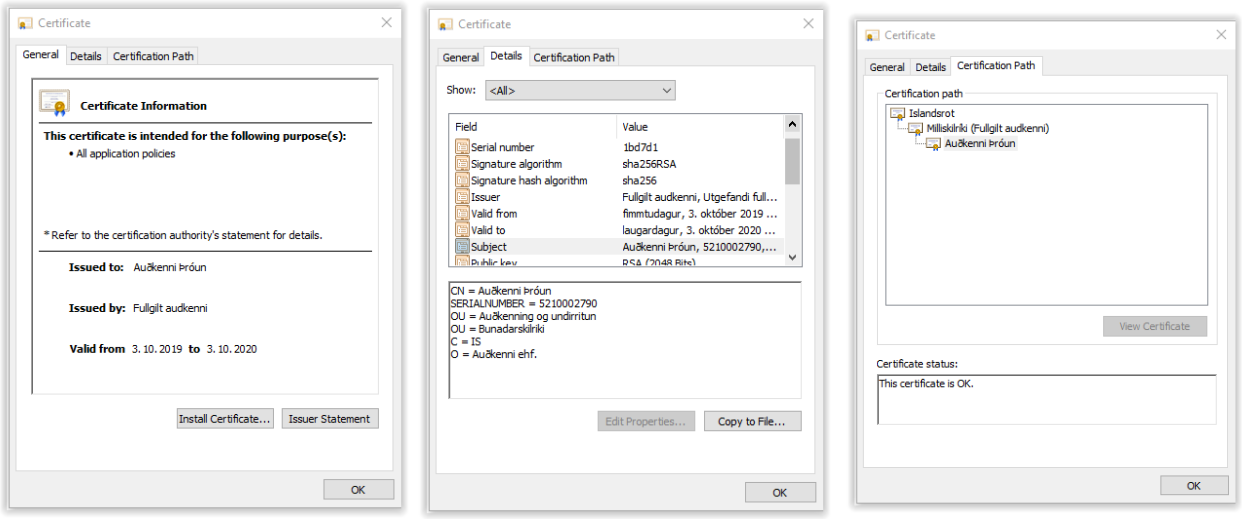
If **Yes** is not selected, the computer will not trust Íslandsrót, and the Equipment Certificate will not function on this computer.



4. Installing the Equipment Certificate on the computer

The **Technical Contact** should have received a **.cer file** from **Auðkenni**.
This file may be shared with banks and other parties, as it does **not** contain the private key of the certificate. Some banks request this file when setting up a new Equipment Certificate.
The **.cer file must be installed on the same computer where the CSR was generated**.
During installation, the public key locates the existing private key on the computer. Together, they form a complete Equipment Certificate.

Viewing the certificate file
The file can be viewed by double-clicking it. It should appear similar to the example shown below.

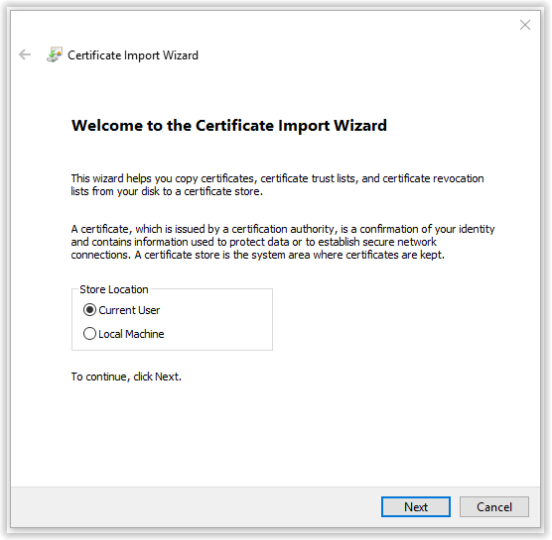


Installing the certificate
Right-click the **.cer** file, select **Install Certificate.** The **Certificate Import Wizard** opens.

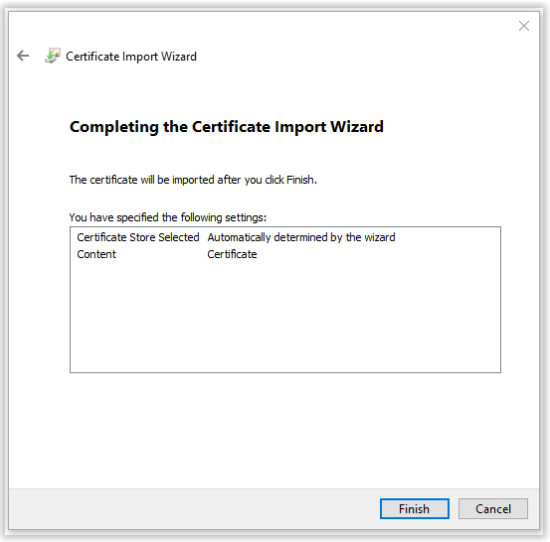
Certificate Import Wizard
You can choose between the **Current User** or **Local Machine** certificate store.

In the CSR instructions, the **Current User** store was used. For consistency, **the same option must be selected here**.

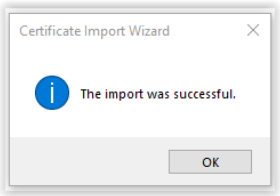
Select **Current User**, Click **Next**.



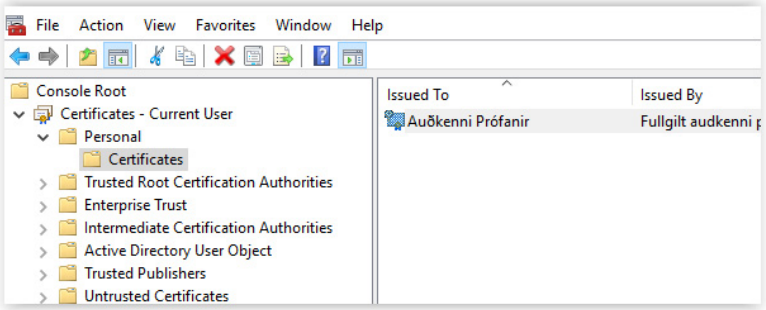
Select **Automatically select the certificate store based on the type of certificate,** click **Next.**



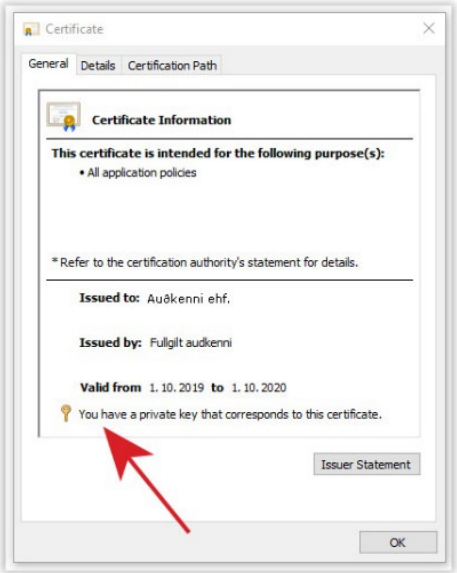
After a few seconds, a confirmation message appears. Click **OK** to close the message. The Equipment Certificate is now installed on this computer.



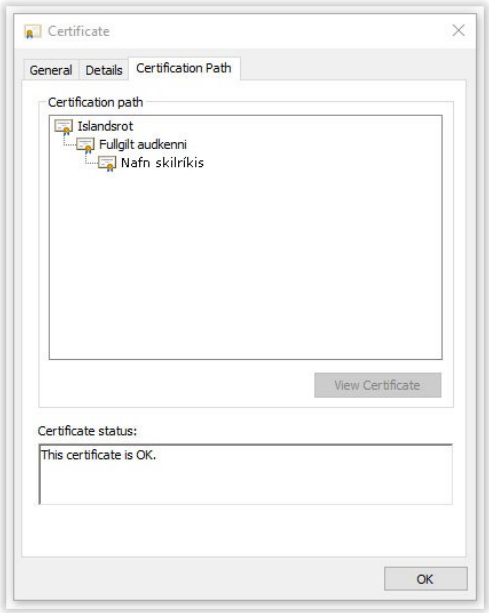
To ensure that everything is correctly installed, it is recommended to verify the certificate. The certificate should be located under: **Personal/Certificates**.



Tvísmelltu á skilríkið og þá færðu þessa mynd:



Double-click the certificate and You should see the following message:
"You have a private key that corresponds to this certificate."
This confirms that the private key and public key are correctly linked.



Verifying the certification path
Select the **Certification Path** tab.
The certification path should appear as follows:
Íslandsrót → Fullgilt auðkenni → Your certificate

If a red cross appears over **Íslandsrót** or **Fullgilt auðkenni**, the corresponding certificate must be installed on the computer.

If everything appears correct, the certificate can now be exported to a **.pfx file** and installed on additional computers if required.

Instructions for exporting the certificate are provided in the next section.

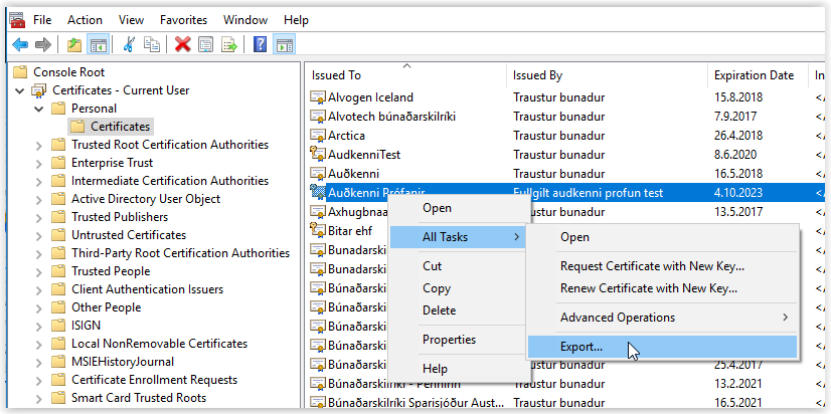
5. Installing the certificate on additional computers – exporting the Equipment Certificate to a .pfx file

If the Equipment Certificate needs to be installed on additional computers, it can be exported to a **.pfx file**.
The **.pfx file** contains:

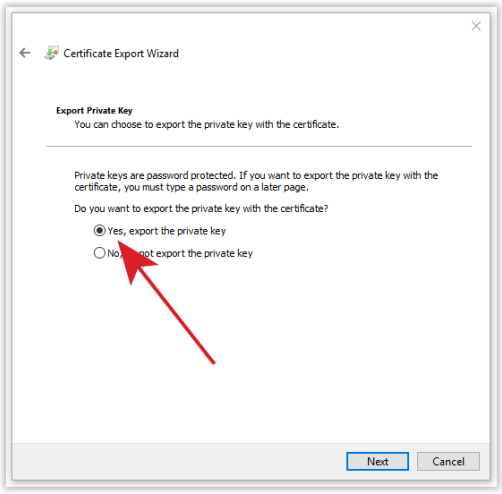
- the private key
- the public key
- the intermediate certificate (*Fullgilt auðkenni*)
- the root certificate (*Íslandsrót*)

Exporting the certificate
In the **MMC Console**, locate the Equipment Certificate under:
Personal / Certificates

1. Right-click the Equipment Certificate.
2. Select **All Tasks** > **Export…**

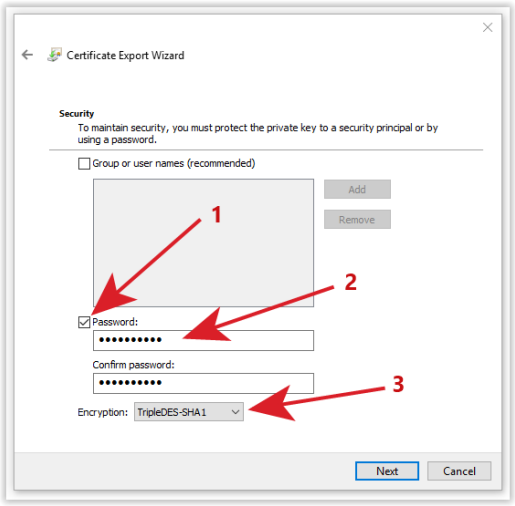


The **Certificate Export Wizard** opens: Click **Next.** Select **Yes, export the private key.**



Click **Next**

Export file format and security
1. Select **Password:**
2. Enter a **strong password**.
   (This password protects the file and is required when installing the certificate on another computer)
3. Under **Encryption**, keep the default setting: **TripleDES-SHA1**

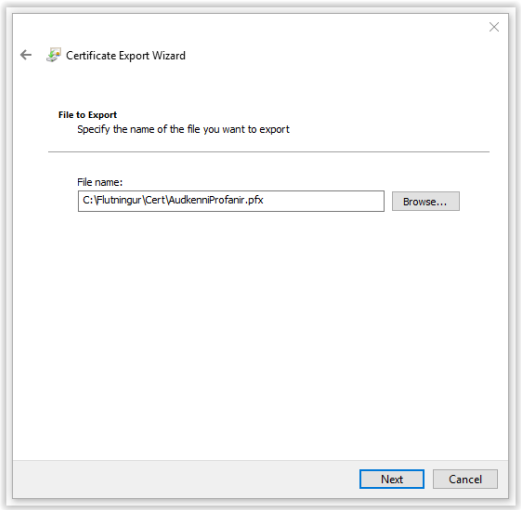


Click **Next.**

Selecting file location

1. Click **Browse**.
2. Choose where the certificate file should be saved and enter a file name.
3. Click **Save**.

The selected file path and name are displayed in the **File name** field of the Certificate Export Wizard.



Completing the export

1. Click **Next**.
2. Click **Finish**.

A confirmation message appears stating:
"The export was successful."
Click **OK**.
Both windows close, and the Equipment Certificate, including the full certificate chain, is now saved as a **.pfx file** at the selected location.

Installing the certificate on another computer
To install the certificate on another computer:

1. Double-click the **.pfx file**.
2. The **Certificate Import Wizard** opens.
3. Keep all settings at their default values and click **Next** twice.
4. Enter the password that was created during export.
5. Click **Next** twice.
6. Click **Finish**.

The Equipment Certificate, including *Íslandsrót* and *Fullgilt auðkenni*, is now installed on the computer.

6. Accounting systems and banks

If you use the Equipment Certificate for communication between an accounting system and banks, it is recommended to contact the banks you are integrating with.
Some banks need to be informed when a new Equipment Certificate is issued, and some may request a copy of the certificate's public key.
In such cases, it is acceptable to send the **.cer file**, as it does not contain the private key.

7. Login using electronic certificates on websites

Service providers that use electronic certificates for login to their websites must install an Equipment Certificate, and **Auðkenni** must register the certificate's public key in its systems.
Login **will not work** unless the service provider provides **Auðkenni** with a copy of the certificate's public key.
If a service provider installs a new Equipment Certificate, a copy of the **new public key must be sent to Auðkenni**.

8. Support

If you encounter issues and these instructions do not resolve them, you can contact **Auðkenni**:

- **Telephone:** +354 530 0000
- **Email:** audkenni@audkenni.is