Memorandum

E-resept Forskrivningsmodul

Thula – Nordic Source Solutions

Subject | Step-by-step instructions to install a new institution certificate

Date | 16/05/2022

Document version | 1.0
Document status | Customer Review

Author | Atli Sturluson
Contributor(s) | Fernando Meira

Distribution | Norsk Helsenett

File name | Memo - eResept - Step by step instructions to install a new institution certificate.docx

1 Document control

This section describes how to version, file, distribute and improve this document.

1.1 Revision tracking

This document is subject to revision control so that after each formal change a new version shall be created with a new data and revision number. At any given time the revision with the highest version number is considered the official and valid version of this document.

1.2 Document source, storage and distribution

The source of this document is maintained by Thula and stored in the Thula document repository. This document shall be distributed in PDF format only.

1.3 Revision history

Date	Version	Author/Approved by	Description
2022-05-16	1.0	Atli Sturluson	Initial version.

1.4 Reader comments

If you have any comments on the contents of this document, please send those by e-mail to the author.

1.5 Glossary

Abbreviation	Explanation or web reference
CA	Certification Authority
MMC	Microsoft Management Console
UAC	User Access Control
FM	Forskrivning Module

2 Intro

This document provides instructions in a step-by-step form for installing a new EIDAS 2.0 institution certificate, along with the Buypass trusted Root and CA certificates required for the certificate validation.

3 Gathering all required files

To proceed with the installation the following files are required:

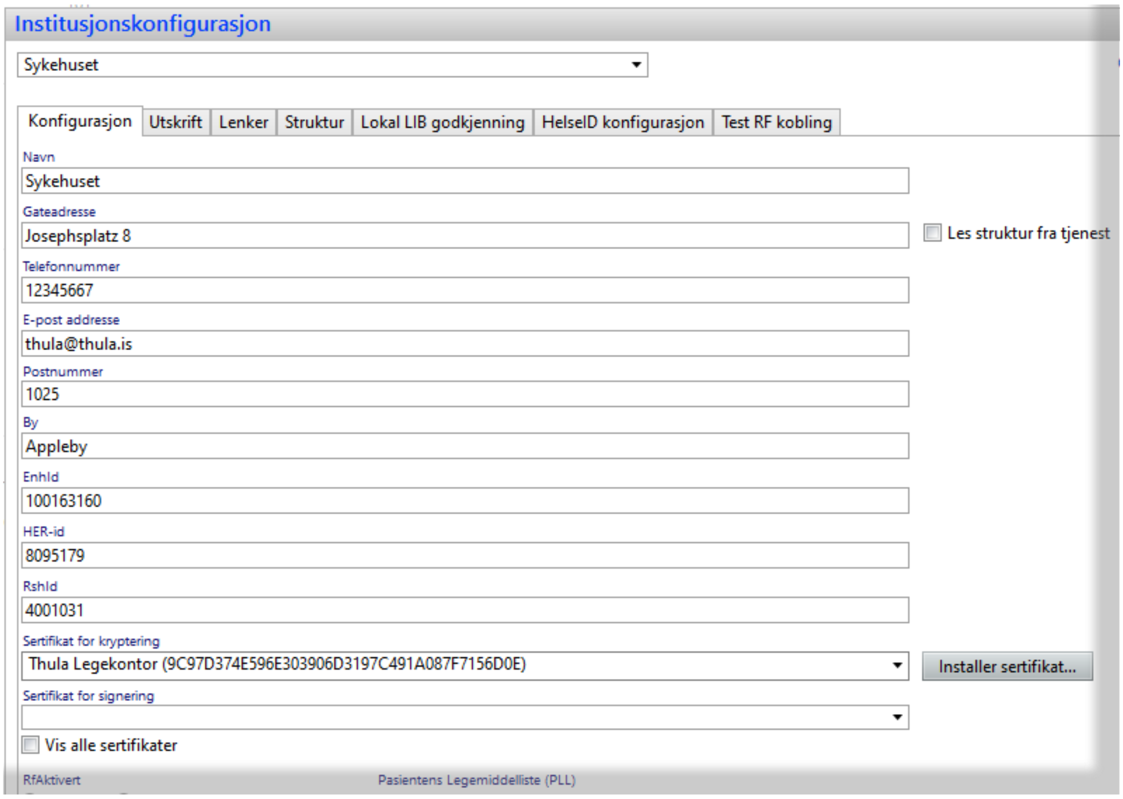
File	Description
Institution certificate for encryption	An EIDAS 2.0 certificate with a private key and where the “Key usage” property includes the value “Key Encipherment” or “Data Encipherment”
BPCl3CaG2STBS.cer	Buypass Class 3 CA G2 ST Business `Thumbprint: 23e05050c00142de0d2a50a3eed347c9b8700b4b`
BPCl3RootCaG2ST.cer	Buypass Class 3 Root CA G2 ST Business `Thumbprint: 50320a8e9af8a1e3a750afda3706a05446a0c68e`

4 Updating the institution certificate using the FM Amin client

The FM Admin client (“Systemadministrasjon”) can be used to install the new institution certificate.

To install the new certificate, the following steps are needed:

1. On the machine where the FM Server is installed, run the FM Systemadministrasjon application as a Windows administrator (right-click the Systemadministrasjon icon and select “Run as administrator”). This will open the FM Amin client. After logging in, select “Administrer organisasjonskonfigurering” to open the institution setup:



Institusjonskonfigurasjon

Sykehuset

Navn: Sykehuset

Gateadresse: Josephsplatz 8

□ Les struktur fra tjenest

Telefonnummer: 12345667

E-post addresse: thula@thula.is

Postnummer: 1025

By: Appleby

EnhId: 100163160

HER-id: 8095179

RshId: 4001031

Sertifikat for kryptering: Thula Legekontor (9C97D374E596E303906D3197C491A087F7156D0E)

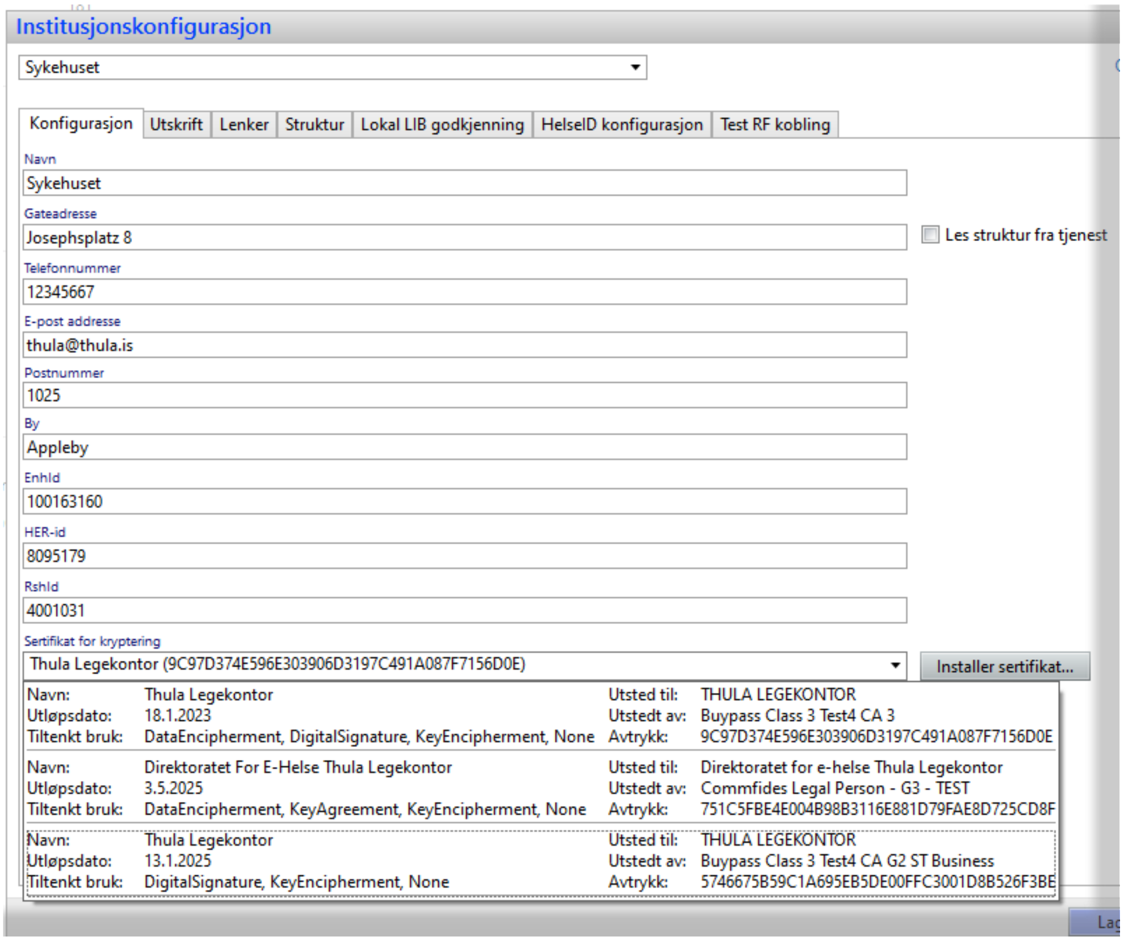
Sertifikat for signering:

□ Vis alle sertifikater

2. Click the “Installer sertifikat…” button and select the new institution certificate file. This will install the new certificate in the correct Windows certificate store and set up the required privileges to enable the FM server to use it.

3. **NOTE: this step will only work for FM version 4.11.0 or later. In older versions, the new certificate will not be available in the drop-down list. For these older versions, the procedure described in section 5 will be needed to install the Buypass root certificates and update the FM database to use the new certificate.**

   In the “Sertifikat for kryptering” combo-box , select the new certificate:



Sykehuset

Navn: Sykehuset

Gateadresse: Josephsplatz 8

□ Les struktur fra tjenest

Telefonnummer: 12345667

E-post addresse: thula@thula.is

Postnummer: 1025

By: Appleby

EnhId: 100163160

HER-id: 8095179

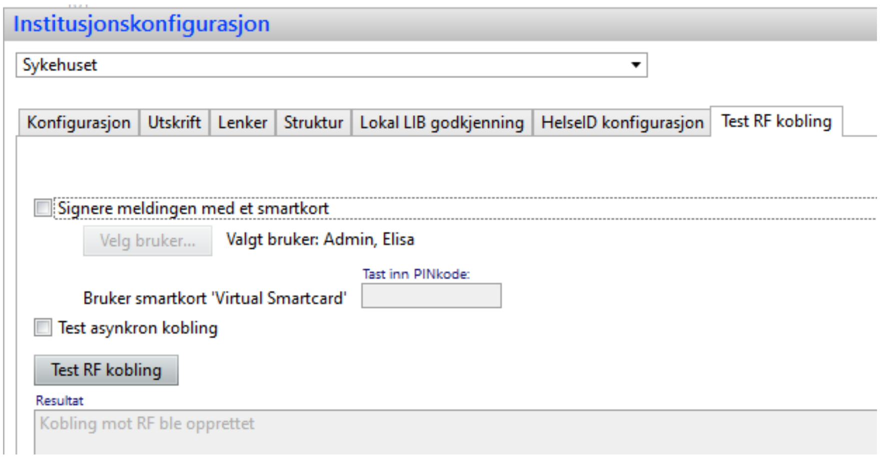
RshId: 4001031

Sertifikat for kryptering: Thula Legekontor (9C97D374E596E303906D3197C491A087F7156D0E)

Navn:	Thula Legekontor	Utsted til:	THULA LEGEKONTOR
Utløpsdato:	18.1.2023	Utstedt av:	Buypass Class 3 Test4 CA 3
Tiltenkt bruk:	DataEncipherment, DigitalSignature, KeyEncipherment, None	Avtrykk:	9C97D374E596E303906D3197C491A087F7156D0E
Navn:	Direktoratet For E-Helse Thula Legekontor	Utsted til:	Direktoratet for e-helse Thula Legekontor
Utløpsdato:	3.5.2025	Utstedt av:	Commfides Legal Person - G3 - TEST
Tiltenkt bruk:	DataEncipherment, KeyAgreement, KeyEncipherment, None	Avtrykk:	751C5FBE4E004B98B3116E881D79FAE8D725CD8F
Navn:	Thula Legekontor	Utsted til:	THULA LEGEKONTOR
Utløpsdato:	13.1.2025	Utstedt av:	Buypass Class 3 Test4 CA G2 ST Business
Tiltenkt bruk:	DigitalSignature, KeyEncipherment, None	Avtrykk:	5746675B59C1A695EB5DE00FFC3001D8B526F3BE

4. Press “Lagre” and you are done! Note that the “Sertifikat for signering” field is not relevant and can be left empty.

5. Communicating with RF using the new certificate can be tested by selecting the “Test RF kobling” tab and pressing the “Test RF kobling” button.



Sykehuset

□ Signere meldingen med et smartkort

Valgt bruker: Admin, Elisa

Bruker smartkort 'Virtual Smartcard'

Tast inn PINkode:

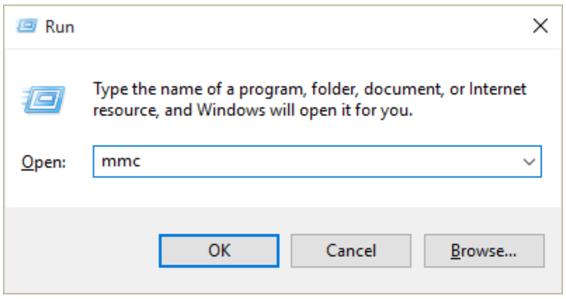
□ Test asynkron kobling

Resultat: Kobling mot RF ble opprettet

5 Manual installation of the institution and related certificates (for advanced users)

5.1 Open the Microsoft Management Console

As a user with high privileges, open the Microsoft Management Console (MMC) by running a command (START > select “Run...” or START > type “run”, depending on the version of Windows).

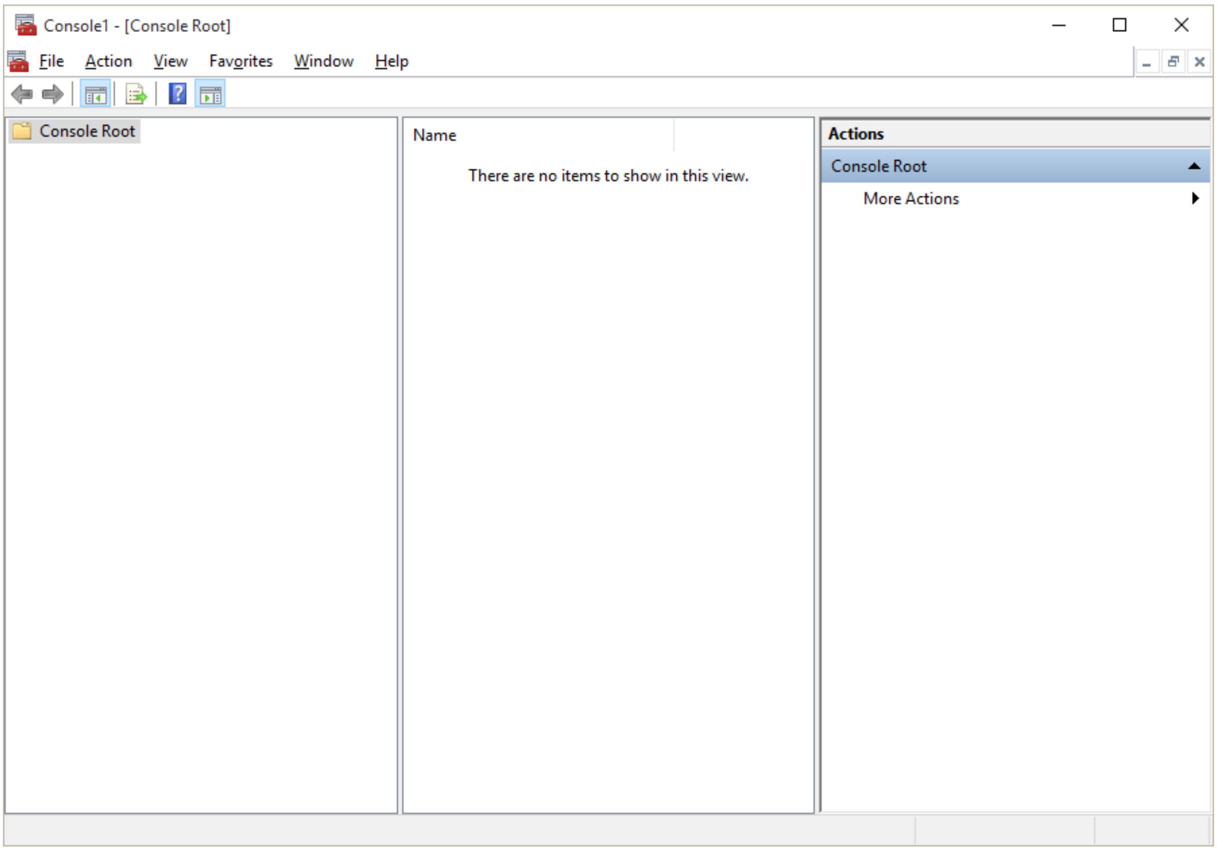


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

Depending on your UAC settings, a popup dialog may appear asking to confirm that you want to execute the MMC application. If so, select yes.

The MMC application opens empty as shown the next screenshot.

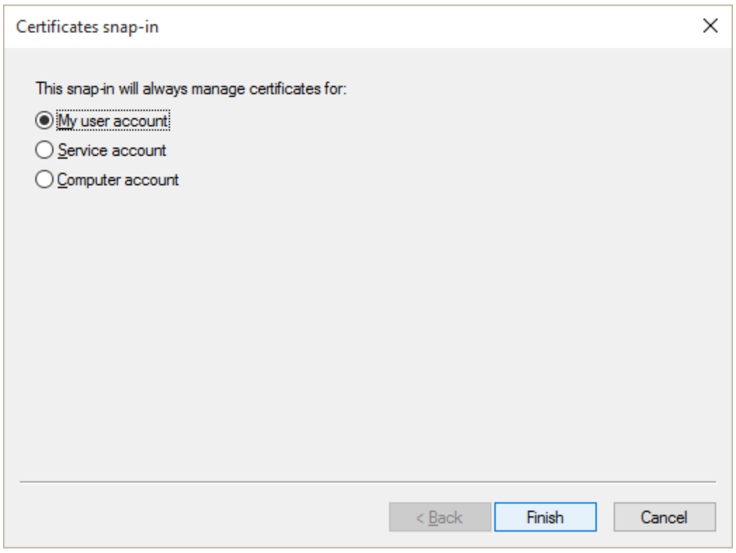


There are no items to show in this view.

Load the certificate lists by doing the following:

1. File > Add/Remove Snap-in… (or use shortcut key CTRL+M).
2. Select “Certificates” from the available snap-ins list.
3. Press the “Add >” button located between the two lists.

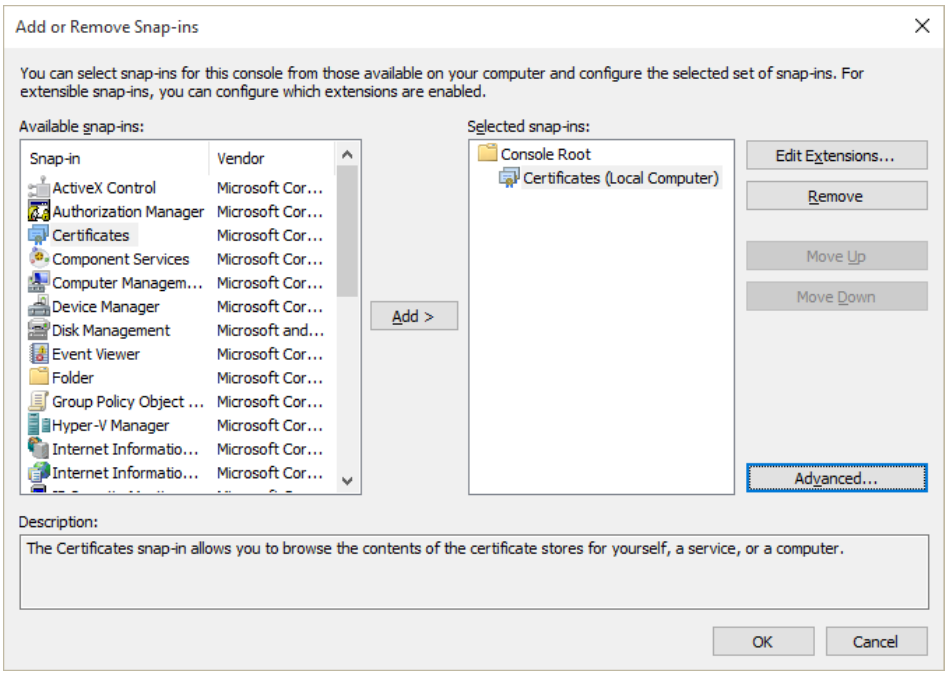
4. The following popup appears.
5. Select to manage certificates for “Computer account”.
6. A “select computer” dialog is shown. Change the default selection to “Local computer”, and press the Finish button.



This snap-in will always manage certificates for:

● My user account
○ Service account
○ Computer account

At the end of this process there should be one certificate list chosen, visible on the right-hand-side (“Selected snap-ins”) as shown the following screenshot.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Hyper-V Manager	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...

Selected snap-ins:

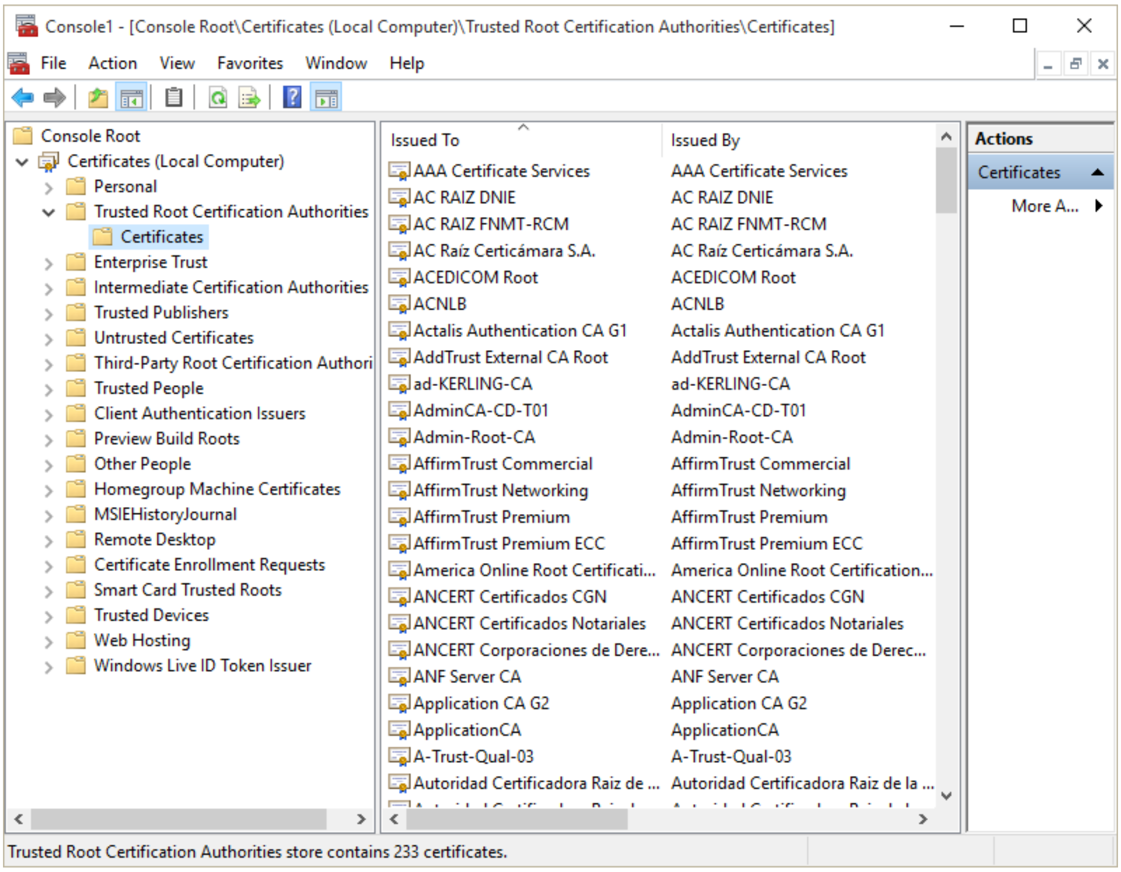
- Console Root
  - Certificates (Local Computer)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Pressing OK should show those two lists on the MMC window.

Start by expanding the list marked as “Certificates (Local Computer)” and within that list expand the “Trusted Root Certification Authorities” folder and select the inner “Certificates” folder. A list of already installed certificates should appear in the central panel, as shown in the following screenshot.


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Actions
Certificates
More A...

- Console Root
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authori
    - Trusted People
    - Client Authentication Issuers
    - Preview Build Roots
    - Other People
    - Homegroup Machine Certificates
    - MSIEHistoryJournal
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - Trusted Devices
    - Web Hosting
    - Windows Live ID Token Issuer

Issued To	Issued By
AAA Certificate Services	AAA Certificate Services
AC RAIZ DNIE	AC RAIZ DNIE
AC RAIZ FNMT-RCM	AC RAIZ FNMT-RCM
AC Raíz Certicámara S.A.	AC Raíz Certicámara S.A.
ACEDICOM Root	ACEDICOM Root
ACNLB	ACNLB
Actalis Authentication CA G1	Actalis Authentication CA G1
AddTrust External CA Root	AddTrust External CA Root
ad-KERLING-CA	ad-KERLING-CA
AdminCA-CD-T01	AdminCA-CD-T01
Admin-Root-CA	Admin-Root-CA
AffirmTrust Commercial	AffirmTrust Commercial
AffirmTrust Networking	AffirmTrust Networking
AffirmTrust Premium	AffirmTrust Premium
AffirmTrust Premium ECC	AffirmTrust Premium ECC
America Online Root Certificati...	America Online Root Certification...
ANCERT Certificados CGN	ANCERT Certificados CGN
ANCERT Certificados Notariales	ANCERT Certificados Notariales
ANCERT Corporaciones de Dere...	ANCERT Corporaciones de Derec...
ANF Server CA	ANF Server CA
Application CA G2	Application CA G2
ApplicationCA	ApplicationCA
A-Trust-Qual-03	A-Trust-Qual-03
Autoridad Certificadora Raiz de ...	Autoridad Certificadora Raiz de la ...

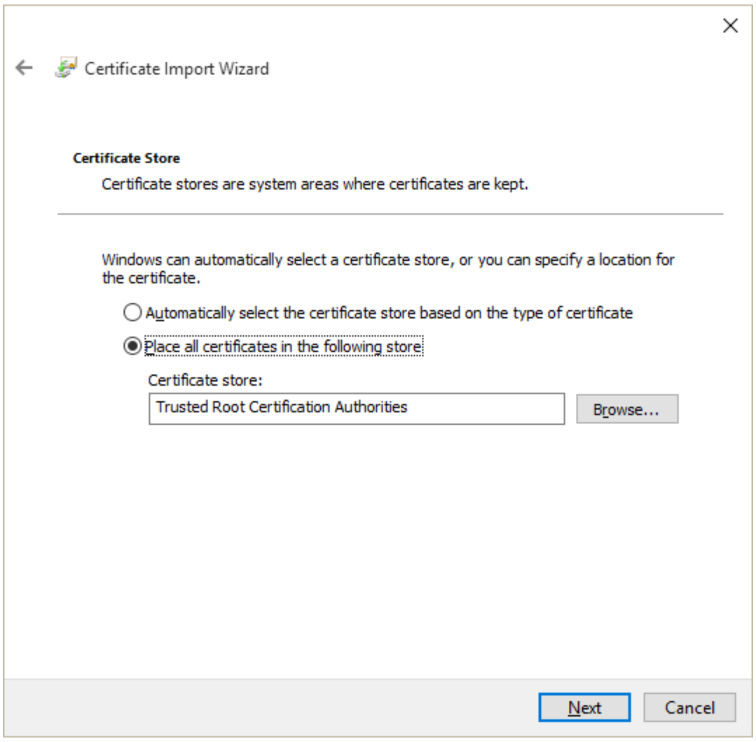
Trusted Root Certification Authorities store contains 233 certificates.

5.2 Import CA certificates

This step is only needed if the EIDAS 2.0 Buypass certificates have not already been installed on the machine.

Import the Buypass Root CA certificate by doing the following:

1. With the Certificates folder selected, inside Trusted Root Certification Authorities, open the import wizard by selecting Action > All Tasks > Import…



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

2. A welcome screen should appear with the Local Machine store pre-selected. Click “Next”.

3. Use the file dialog to select the “BPCl3RootCaG2ST.cer” file.

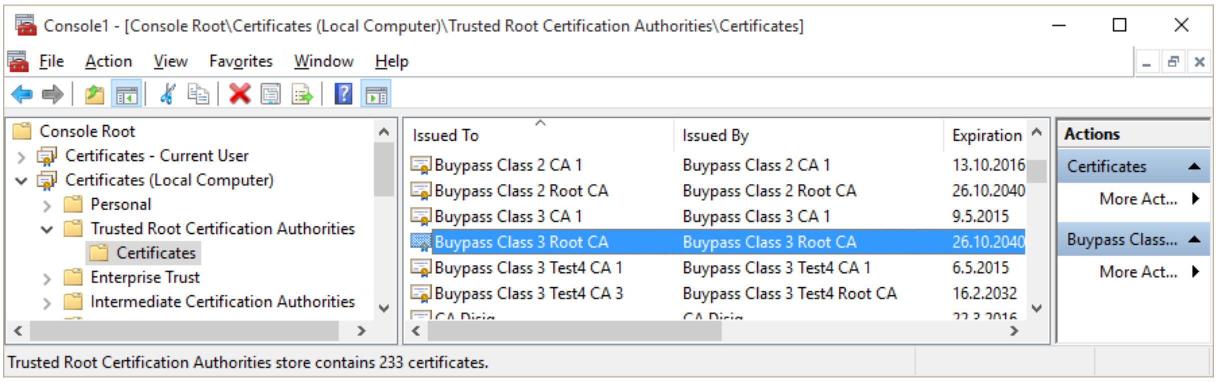
4. Press “Next” on the File to import screen.

5. A dialog to choose the Certificate Store appears. It should have preselected the option “Place all certificates in the following store” and have the working folder selected on the Certificate store textbox, i.e., it should say “Trusted Root Certification Authorities”, as in the following screenshot. If that store is not pre-selected, use the “Browse” button to select it from the list of available stores. Press “Next”.

6. A final wizard screen appears presenting the overview of the import process. Confirm that everything is as expected and press “Finish”.

7. A dialog is shown informing that the import was successful.

You should now be able to find the imported certificate in the list of installed certificates, located in the central panel of the MMC window, like in the example:



Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

Issued To	Issued By	Expiration
Buypass Class 2 CA 1	Buypass Class 2 CA 1	13.10.2016
Buypass Class 2 Root CA	Buypass Class 2 Root CA	26.10.2040
Buypass Class 3 CA 1	Buypass Class 3 CA 1	9.5.2015
Buypass Class 3 Root CA	Buypass Class 3 Root CA	26.10.2040
Buypass Class 3 Test4 CA 1	Buypass Class 3 Test4 CA 1	6.5.2015
Buypass Class 3 Test4 CA 3	Buypass Class 3 Test4 Root CA	16.2.2032
CA Disig	CA Disig	22.3.2016

Trusted Root Certification Authorities store contains 233 certificates.

To install the Buypass Class 3 CA G2 ST Business certificate, repeat all previous 7 steps but select the file named “BPCl3CaG2STBS.cer” during step 3.

5.3 Install the institution certificate

The new institution certificate should be installed in the Personal folder of the Local computer store.

It can be installed by performing the following steps:

1. Select the folder “Certificates” inside “Personal” folder in MMC. See section 5.1 on how to initialize the MMC tool.

2. Open the import wizard by selecting Action > All Tasks > Import…

3. A welcome screen should appear with the Local Machine store pre-selected. Click “Next”.

4. Use the file dialog to select the “.p12” file for the new institution encryption certificate.

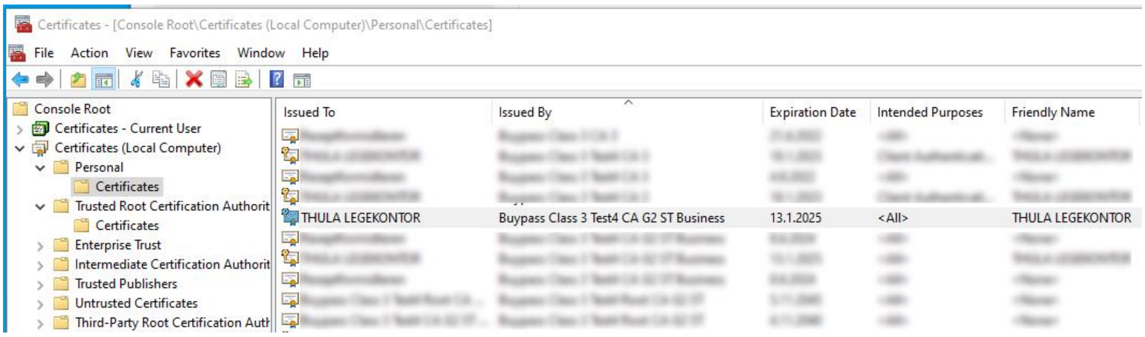
5. Press “Next” on the File to import screen.

6. A dialog to choose the Certificate Store appears. It should have pre-selected the option “Place all certificates in the following store” and have the working folder selected on the Certificate store textbox, i.e., it should say “Personal”. If not, use the “Browse” button to select the Personal folder. Press “Next”. You will be prompted for certificate password.

7. A final wizard screen appears presenting the overview of the import process. Confirm that everything is as expected and press “Finish”.

8. A dialog is shown informing that the import was successful.

The central panel of the MMC window should now include the imported certificate, as shown in the following screenshot:



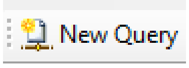
Certificates - [Console Root\Certificates (Local Computer)\Personal\Certificates]

Console Root
- Certificates - Current User
- Certificates (Local Computer)
  - Personal
    - Certificates
  - Trusted Root Certification Authorit
    - Certificates
  - Enterprise Trust
  - Intermediate Certification Authorit
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification Auth

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
THULA LEGEKONTOR	Buypass Class 3 Test4 CA G2 ST Business	13.1.2025	<All>	THULA LEGEKONTOR
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

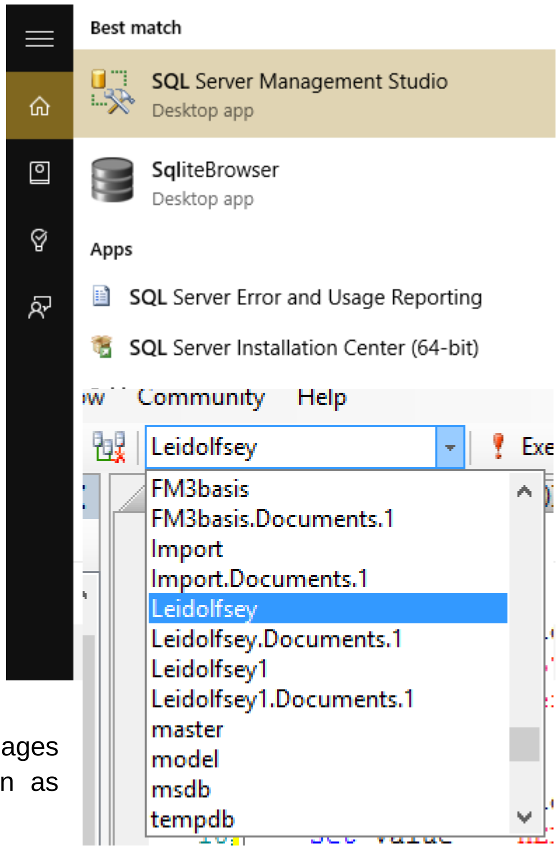
5.4 Update the FM system

When the FM Admin procedure described in section 4 has been performed (which will require FM version 4.11.0 or later), the FM database will be updated to correctly use the new certificate. Otherwise, the FM database needs to be updated manually. Follow these steps to perform the required operation:

1. Open SQL Management Studio.
2. Connect to the database used by the FM installation to be updated with a user that has write permissions on the database.
3. The next steps are divided in two depending on if you are going to be using the provided SQL file or typing in the queries manually.
4. Open a new query window by using the shortcut CTRL+N or clicking on “New query button: 

5. Select the FM database used from the combobox or execute the following script (using as example “Leidolfsey” as the FM database name):

```
use Leidolfsey
```



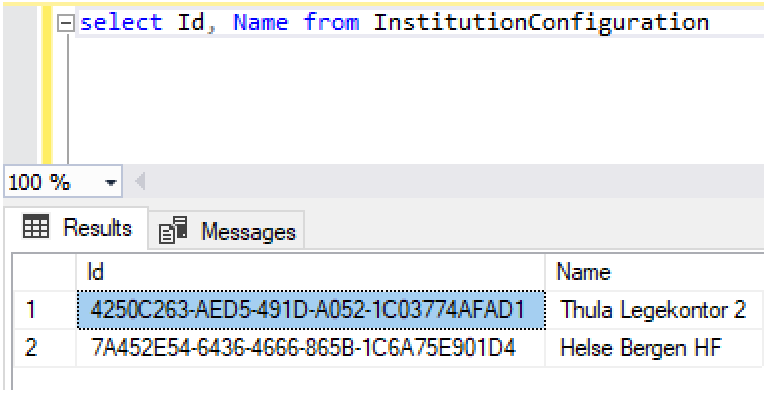
The following message should appear in messages panel and the database name should be shown as selected on the available databases combobox.

```
Command(s) completed successfully.
```

6. Erase all scripts, if any, and run the following script to see the institutions that are defined in FM:

```
select Id, Name from InstitutionConfiguration
```

This should show results similar to the following (in many cases only one row will be shown, if the FM installation only has a single institution defined):



```
select Id, Name from InstitutionConfiguration
```

	Id	Name
1	4250C263-AED5-491D-A052-1C03774AFAD1	Thula Legekontor 2
2	7A452E54-6436-4666-865B-1C6A75E901D4	Helse Bergen HF

Copy the value of the Id column for the correct institution to the clipboard.

Erase all scripts, if any, and run the following script to update the institution certificate that FM uses. The `EncryptionCertificate` should be the certificate’s thumbprint, available on the details of the certificate. The `Id` value should be the value copied from the Id column in the query results in step 6 above:

```
update InstitutionConfiguration
 set EncryptionCertificate='5746675b59c1a695eb5de00ffc3001d8b526f3be'
```

```
where Id='4250C263-AED5-491D-A052-1C03774AFAD1'
```

The following success message should appear on the messages panel:

```
(1 row(s) affected)
```

If all steps in this memo have been successfully performed, then the FM institution should be configured to use the new certificate and all certificates needed should have been installed.