

Installation Guide for CUG Certificate for use with DKMANet

Contents

How to start the installation.....	1
The installation process.....	1
Finding the certificate on your pc.....	3
Making a backup copy.....	5
Easy access to certificate from DKMANet login.....	6
Getting access to DKMANet.....	8
Removing an old certificate.....	9

How to start the installation

When the Danish Medicines Agency issues a Closed User Group (CUG) certificate to you, you will receive both an email and an ordinary letter by mail. The email contains a short installation guide and the link to the certificate administration tool that you need in order to start the installation. The letter contains the installation code that you will be asked to enter during the installation process.

In order to start the installation, please find both the letter and the email - it was sent from dkmanet@dkma.dk - and click the link in step 3 of the email. The installation should run correctly in recent versions of most browsers, but if you experience any problems we recommend using Mozilla Firefox or Google Chrome: start the browser and copy the link from the email to the address line in the browser window if you need to use a different browser than the one set as standard on your pc.

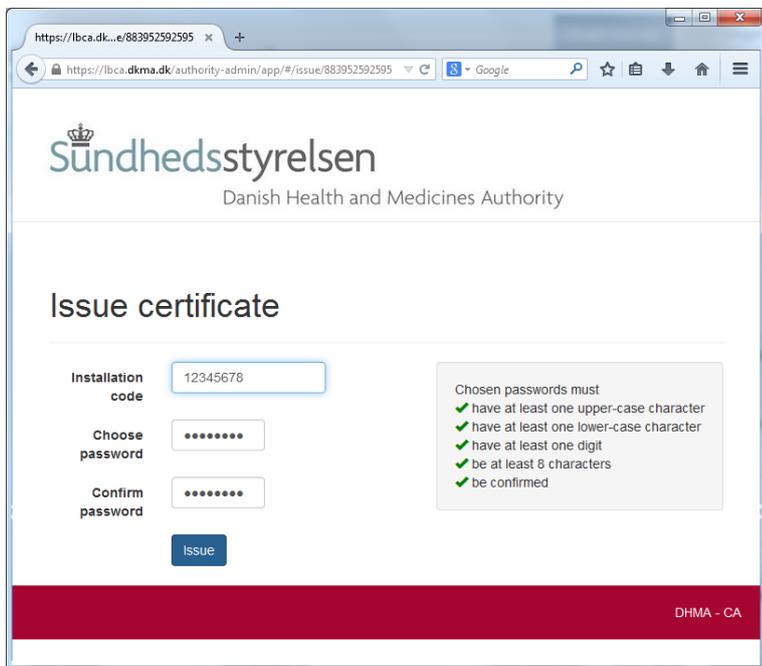
The installation process

When you follow the link from the email, a window like the one below opens. Please enter the installation code from the ordinary letter in the entry field "Installation code":

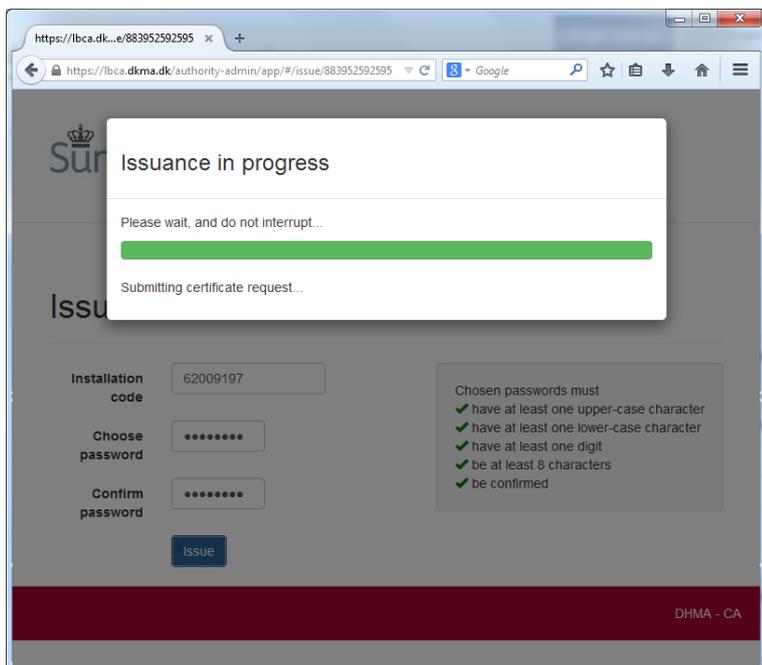
The screenshot shows a web browser window displaying the 'Issue certificate' page. The page header includes the logo for Sundhedsstyrelsen (Danish Health and Medicines Authority). The form contains the following elements:

- Installation code:** A text input field with a placeholder '8 digits'.
- Choose password:** A text input field.
- Confirm password:** A text input field.
- Issue:** A blue button.
- Password requirements:** A list of requirements with red 'X' icons:
 - have at least one upper-case character
 - have at least one lower-case character
 - have at least one digit
 - be at least 8 characters
 - be confirmed

Then you need to decide on a personal password that you will be asked to supply each time you use the certificate to log in to DKMANet. The password will be known only by you - it is not stored in DKMA systems in any form. The password should be easy for you to remember and difficult for others to guess, and it needs to comply with the requirements given on the screen. The requirements will be ticked off one by one as they are fulfilled. Please type the password into both remaining fields on the screen and click the "Issue" button.



When you see the following window, please wait.



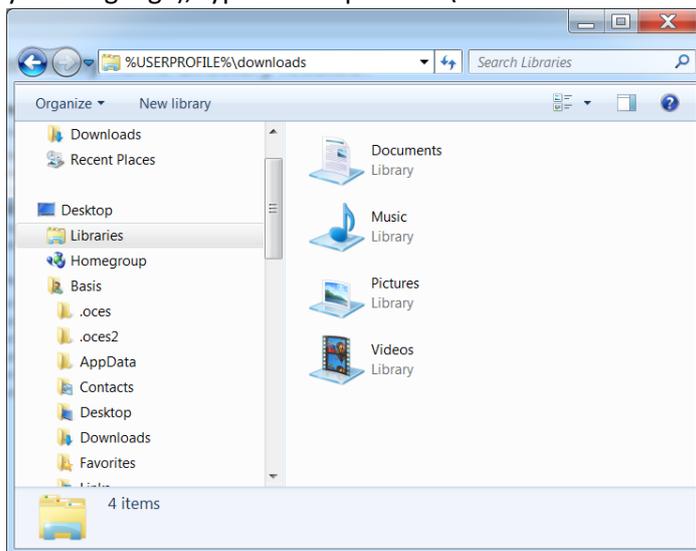
In Firefox you will then be prompted to either open or save the file - please select "save".

Finding the certificate on your pc

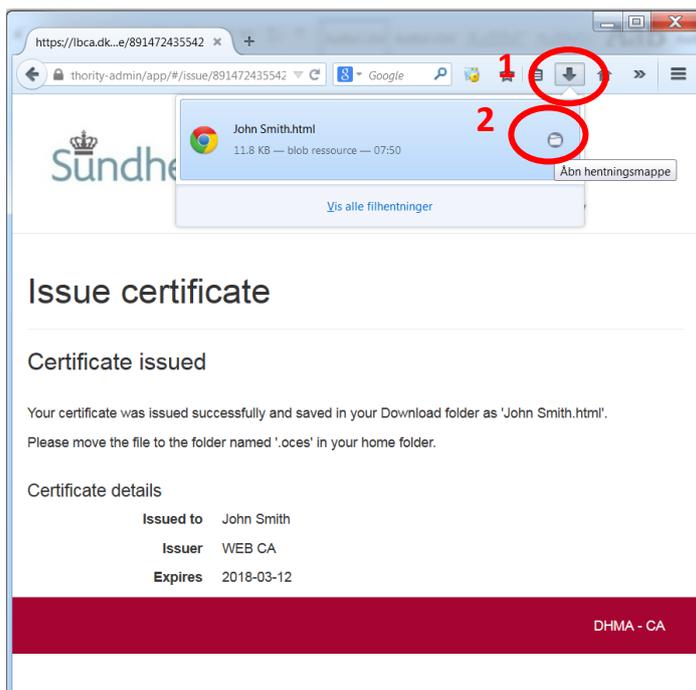
The certificate will be saved as an HTML file in the “downloads” folder on your pc. The file carries your name as it was indicated on the “Order for Closed User Group Certificate” sent to DKMA, e.g. “John Smith.html”.

Please note that the name of the “downloads” folder depends on the language of your Windows (or other) operating system. If you do not know the folder name in the language of your operating system, it may be difficult to use Explorer to browse your way to the folder. Here are a number of alternative ways of opening the “downloads” folder in an Explorer window:

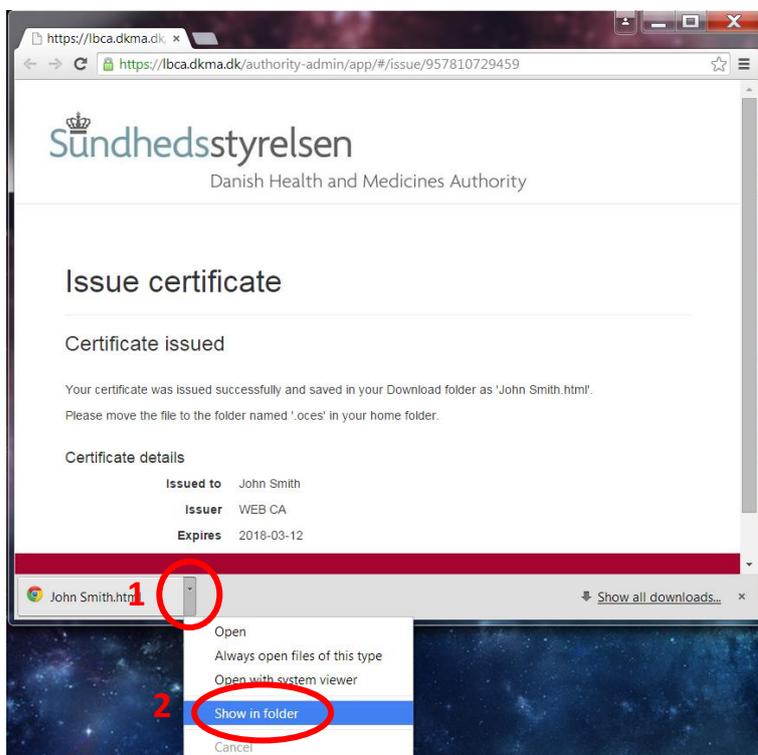
1. Open an Explorer window, e.g. by clicking the Windows Start button and then “Documents” (in your language), type “%userprofile%\downloads” into the address line, and press ENTER:



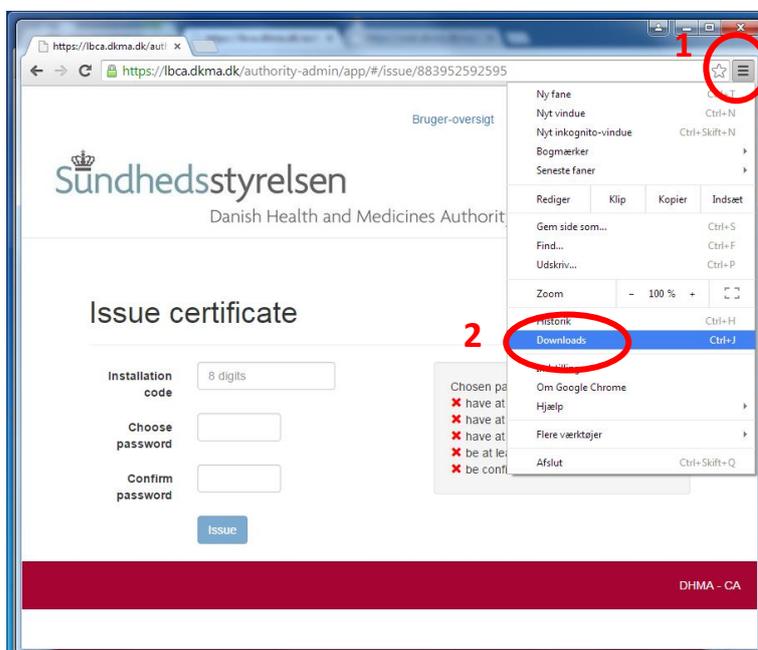
2. If you use Firefox: in your browser window, select to see the downloaded file in the downloads folder:



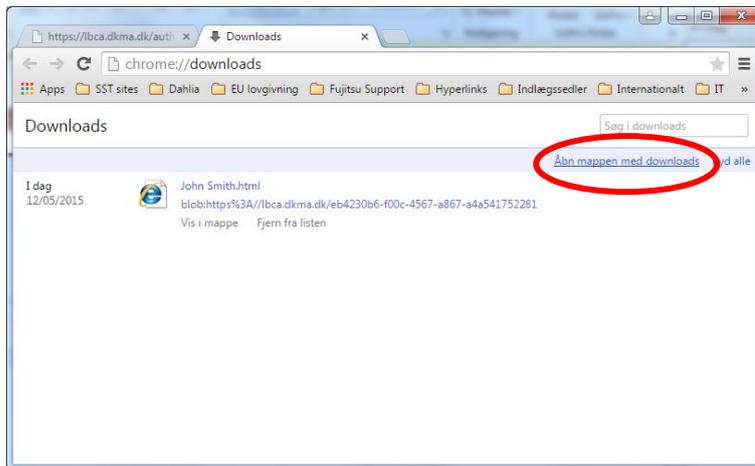
3. If you use Google Chrome: if you still have the file link at the bottom of the browser window, click the small down arrow and select "Show in folder":



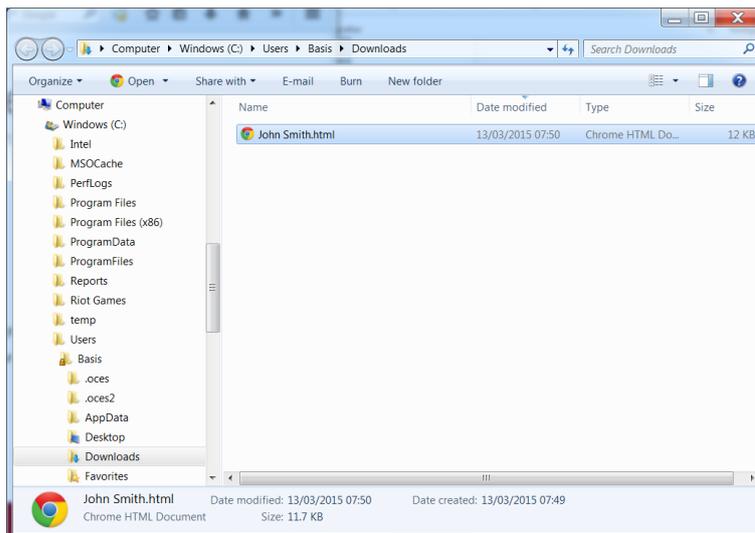
4. If you use Google Chrome: first select to see all downloads:



Then click on the link to open the downloads folder:



- Using any of these methods, you should end up with the “downloads” folder open and the certificate HTML file shown in the Explorer window:



Please note that as the certificate is stored in a file and not “installed” in the true sense of that word, you are able to rename the certificate. This may be convenient if you will need access to DKMANet for different companies using different certificates.

Making a backup copy

Before you start using your certificate, you should make a backup copy of it in a secure location, e.g. on a network drive that is regularly backed up or on an external backup device.

For that purpose, the certificate file is just like any other file: take a copy of it and save the copy in a secure location.

Easy access to certificate from DKMANet login

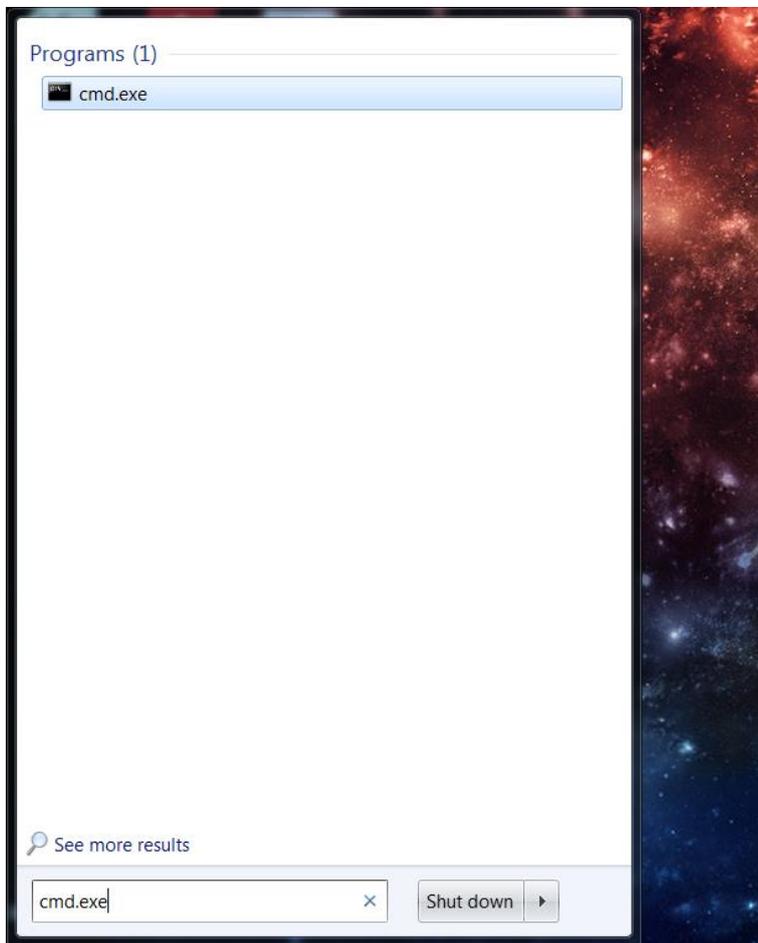
The login box at DKMANet.dk allows you to select the certificate you want to use for login. There is a “Browse” button that will allow you to select the certificate file from the downloads folder, but the login box automatically displays any certificate found in the “.oces” folder on your pc.

If you have already been using a certificate to log in to DKMANet, the “.oces” folder will already exist on your pc (like it does in the screen shot above), as a sibling folder on the same level as the downloads folder. In that case simply copy (or move) the certificate HTML file from the downloads folder to the “.oces” folder.

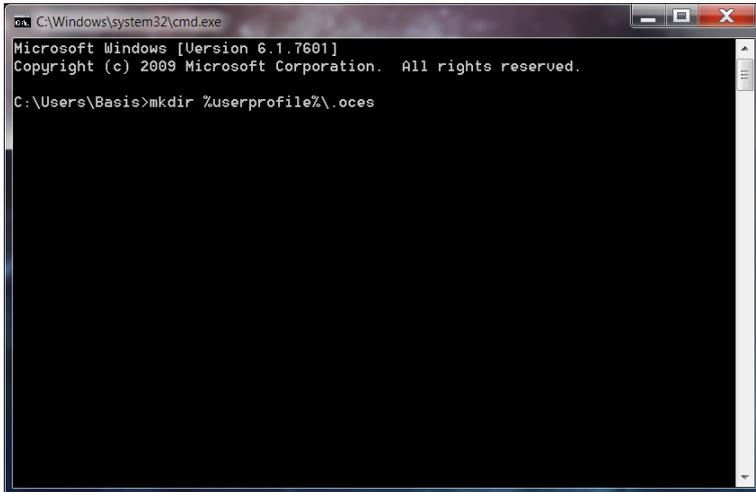
If there is no “.oces” folder on your pc, you have to create it first, before copying the certificate file. This is a bit difficult, because Windows Explorer does not allow you to give a new folder a name that starts with a period (“.”).

The easiest way to create the “.oces” folder in the correct location is to use the Command Prompt:

Click the Windows Start button, type “cmd.exe” into the search field, and press ENTER:



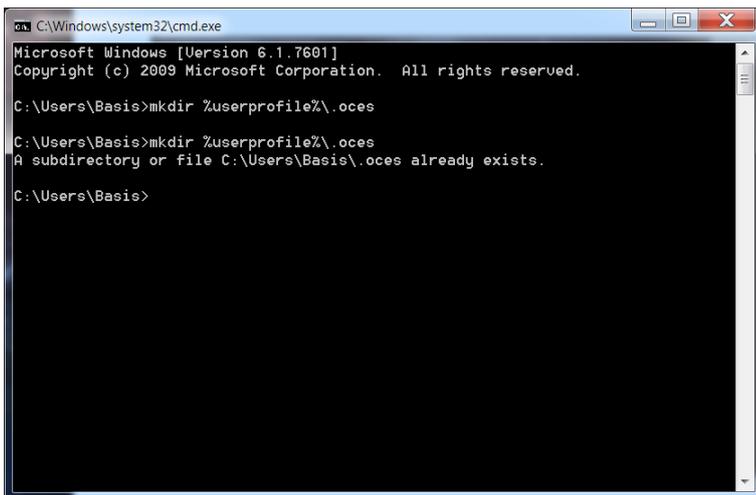
In the Command Prompt window that opens, type “mkdir %userprofile%\.oces” and press ENTER:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Basis>mkdir %userprofile%\.oces
```

If the “.oces” folder should already exist, the command will have no effect:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Basis>mkdir %userprofile%\.oces
C:\Users\Basis>mkdir %userprofile%\.oces
A subdirectory or file C:\Users\Basis\.oces already exists.

C:\Users\Basis>
```

Then close the window by clicking the red cross or by typing “exit” and pressing ENTER.

You can now copy or move the certificate HTML file from the downloads folder to the “.oces” folder.

If you cannot locate the “.oces” folder, you can find and open it by opening an Explorer window (e.g. click the Windows Start button and then “Documents” in your language), typing “%userprofile%\.oces” in the address line and pressing ENTER. You should now have two open Explorer windows and be able to copy the certificate HTML file between them.

Getting access to DKMANet

The certificate allows for a secure identification of yourself, but access to DKMANet also requires a corresponding user account specifying which data you are allowed to access.

Existing users

If the certificate is issued as a replacement for an existing or “lost” certificate, you will already have a user account on DKMANet.

If we have been aware of that fact when we issued the certificate, the internal identification number of the certificate, the RID number, will be identical to the one in the previous certificate, and you should be able to log on to the existing user account with the new certificate right away.

If we have not been aware that the certificate was intended to replace an existing one, the new certificate will have a different RID number from the one currently indicated in your user account. This means that the user account should be updated – the only change needed is the new RID number – before you can use the new certificate. If you are the Security Administrator for your company on DKMANet, please inform the Danish Medicines Agency of the new RID number by email: dkmanet@dkma.dk and we will update your user account. If you are an ordinary user or administrator (CU or CA user account type), the update must be made by your Security Administrator (it can also be made by a CA user if you have a CU account).

Please see below for instructions on how to find the RID number of your new certificate.

New users

If you are a new user or if the certificate should be used with a new user account on DKMANet, the appropriate user account needs to be created, including the RID number of the certificate, before you can access DKMANet.

If you are to be the Security Administrator for the company on DKMANet, you need to fill in and send to us the form for appointment of Security Administrator that you can find on our web site (link in the bottom coloured box to the right): <http://laegemiddelstyrelsen.dk/en/reimbursement/prices/notification-of-prices-and-range>. Please observe the details about authorization to sign for the company etc. indicated on page two of the form.

When we have received the form, we will create the user account for you and let you know when you can access DKMANet.

If you are to be an ordinary user or administrator (CU or CA user account type), the Security Administrator for the company must create the user account for you using the “User administration” page on DKMANet.

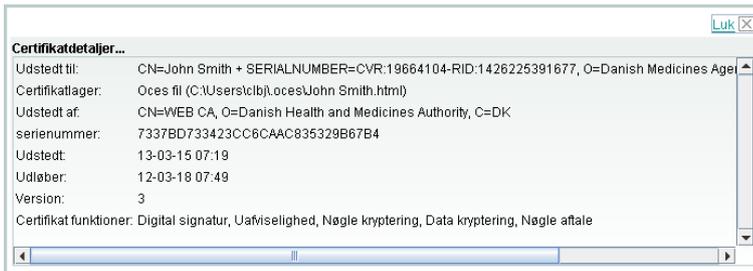
Please note that with a newly created user account you will not be able to log in to DKMANet until the day following the creation of the account.

On all new user accounts the RID number of the certificate must be indicated. You can find the RID number of your new certificate in the following way.

Finding the RID number

In order to find the RID number of the new certificate, after you have completed the installation of it, please go to the login page of DKMANet, but click the “Details” button instead of “OK” after choosing the HTML file.

When you have supplied the password, you will get a dialogue box like the following, with the RID number (13 digits) listed in the first line:



Removing an old certificate

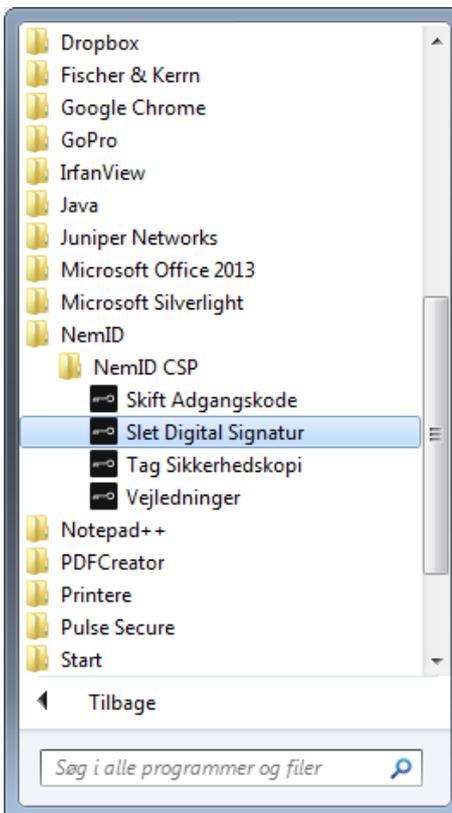
If the new certificate is a replacement for an existing CUG certificate of the previously used type, we recommend that you remove the old certificate - **after** making sure that you are able to log in to DKMANet with the new certificate.

Unless you remove the old certificate, it will continue to be presented in the DKMANet login box, even after it has expired.

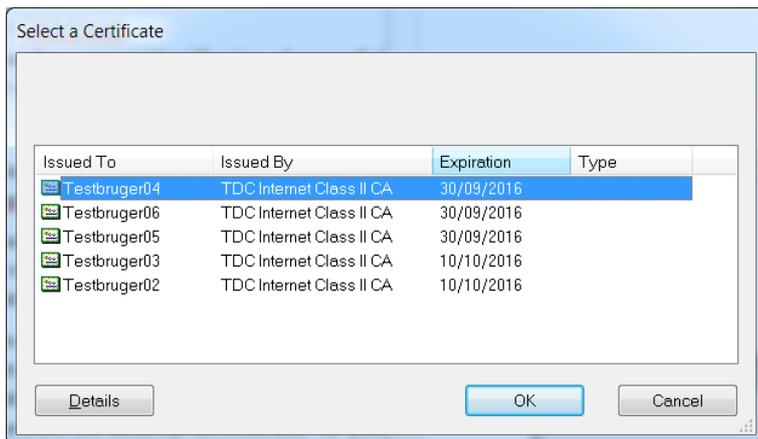
The previously used type of certificate is installed in your computer's certificate store. In order to remove an old certificate you should start the tool that was installed together with the certificate:

Click the Windows Start button and select "All Programs" in your language.

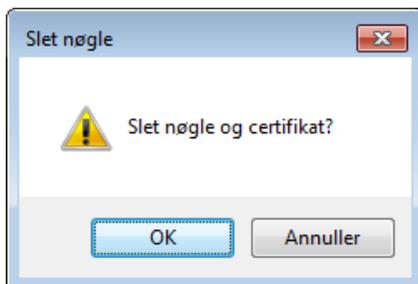
Find and click the "NemID" program group, then "NemID CSP" and finally "Slet Digital Signatur" ("Delete Digital Signature"):



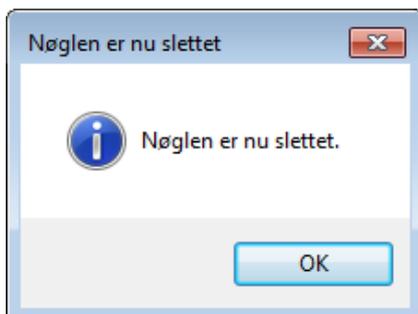
This will open a small window with a list of installed certificates. The CUG certificates of the old type are listed with the text "TDC Internet Class II CA" in the second column:



Select the certificate to be deleted in the list and click OK. Also click OK in the window which prompts you to confirm the deletion:



You will receive a confirmation that the certificate has been deleted:



You may also safely delete all backup copies you may have taken of the old certificate.