EGOSECURE FULL DISK ENCRYPTION

EgoSecure FDE - Adding the SmartCard Logon certificate to YubiKey Neo

Version 15.4

Updated 01.2021

EgoSecure GmbH
Pforzheimer street 128b
76275 Ettlingen
Telephone: +49(0)7243 / 354 95-0
Telefax: +49(0)7243 / 354 95-10
E-Mail: contact@egosecure.com
Internet: www.egosecure.com

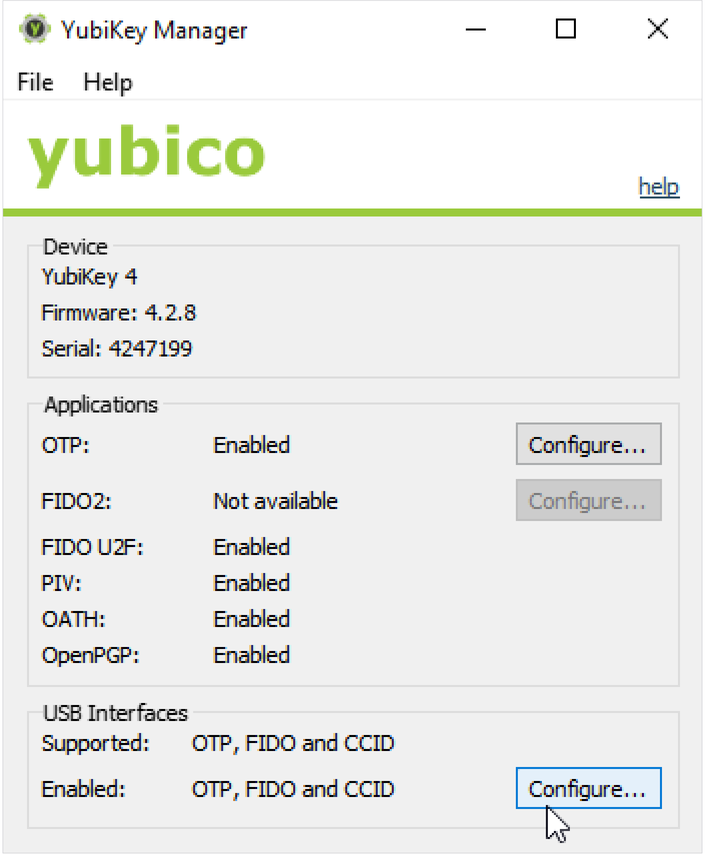
Phone and mail support
+49 (0)7243-35495-50
support-int@egosecure.com

Preparing YubiKey Neo device in the Windows PKI environment to use it for two-factor authentication

1. Download and install the following utilities:

- Yubikey Manager
- YubiKey PIV Manager

2. Start the Yubikey Manager utility.
3. Click **Configure**.



Device
YubiKey 4
Firmware: 4.2.8
Serial: 4247199

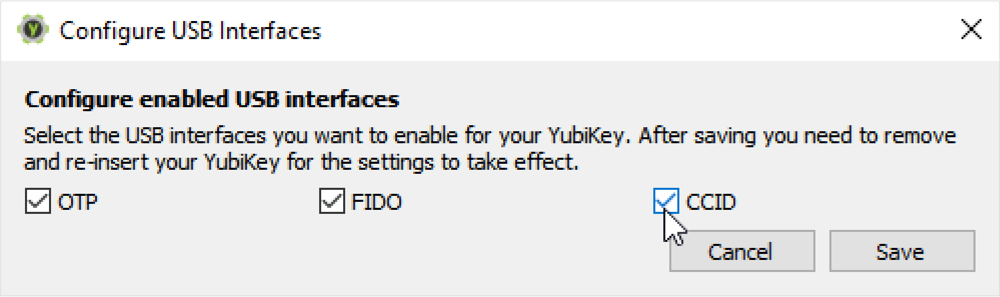
Applications

OTP:	Enabled
FIDO2:	Not available
FIDO U2F:	Enabled
PIV:	Enabled
OATH:	Enabled
OpenPGP:	Enabled

USB Interfaces
Supported: OTP, FIDO and CCID
Enabled: OTP, FIDO and CCID

→ The **Configure USB Interfaces** dialog appears.

4. Set the **CCID** check box, and click **Save**.



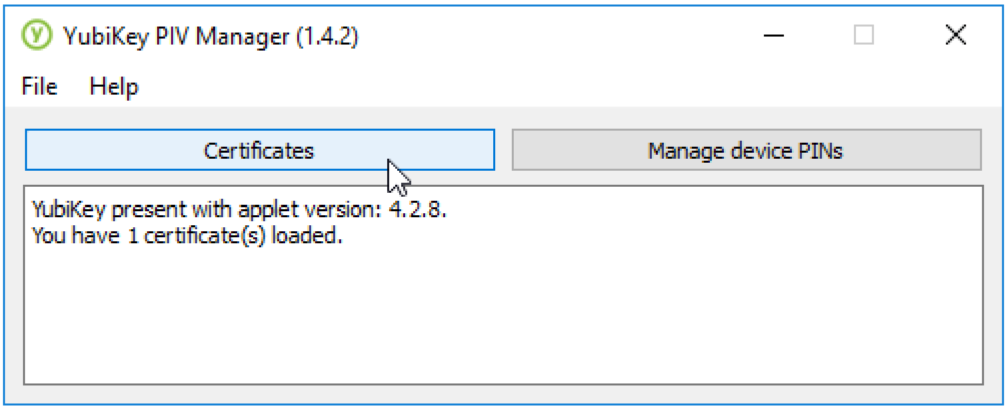
Configure enabled USB interfaces

Select the USB interfaces you want to enable for your YubiKey. After saving you need to remove and re-insert your YubiKey for the settings to take effect.

☑ OTP ☑ FIDO ☑ CCID

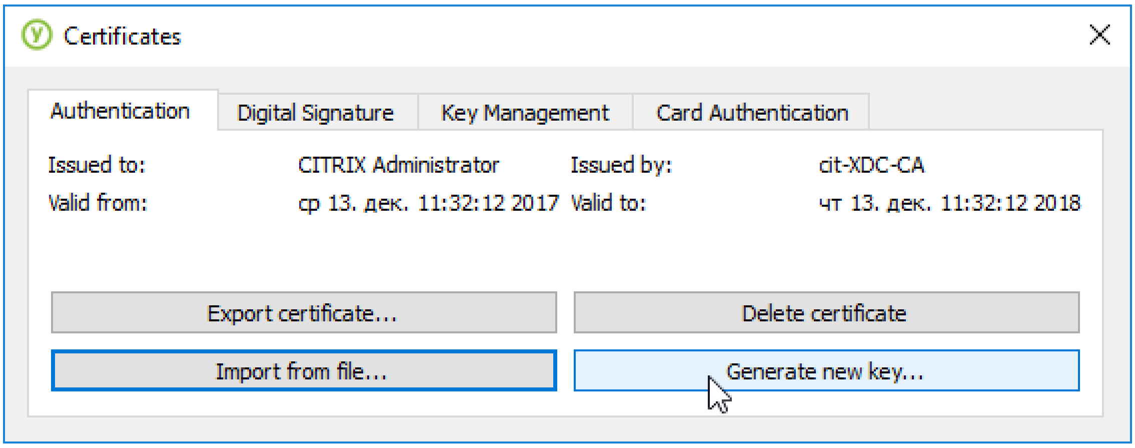
5. Unplug and re-attach **YubiKey Neo** device, and close the **Yubikey Manager** utility.

6. Open the **YubiKey PIV Manager** utility, and click the **Certificates** button.



YubiKey present with applet version: 4.2.8.
You have 1 certificate(s) loaded.

7. In the **Authentication** tab, click **Generate new key**.

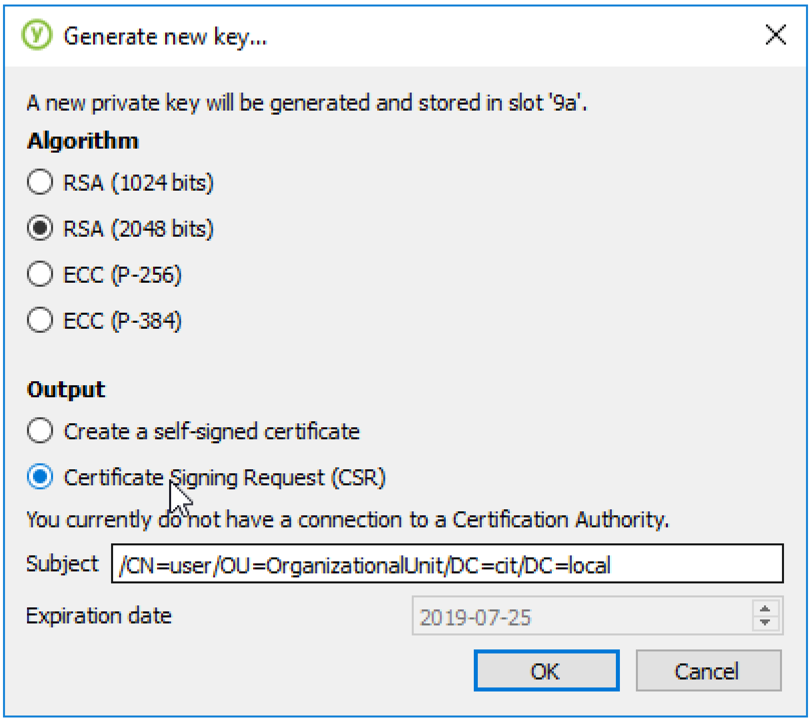


Issued to: CITRIX Administrator
Issued by: cit-XDC-CA
Valid from: ср 13. дек. 11:32:12 2017
Valid to: чт 13. дек. 11:32:12 2018

8. Select the **RSA (2048 bits)** encryption algorithm. In the **Output** panel, set the **Certificate Signing Request (CSR)** radio button.

Only certificates signed by a domain with a Certificate Authority are supported.

9. Specify the path for the subject of the user in the Active Directory.
For example, for the user who is in the Organizational unit of the `cit.local` domain, the path looks like this:
`/CN=user/OU=OrganizationUnit/DC=cit/DC=local`



Generate new key...

A new private key will be generated and stored in slot '9a'.

Algorithm

○ RSA (1024 bits)

● RSA (2048 bits)

○ ECC (P-256)

○ ECC (P-384)

Output

○ Create a self-signed certificate

● Certificate Signing Request (CSR)

You currently do not have a connection to a Certification Authority.

Subject /CN=user/OU=OrganizationalUnit/DC=cit/DC=local

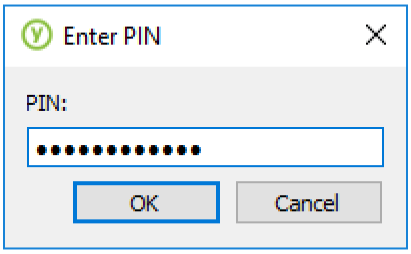
Expiration date 2019-07-25

10. Click **OK**.

→ The **Save Certificate Signing Request as** dialog appears.

11. Enter a file name to save a certificate request, and select the folder where to store the file.

12. Enter PIN for device access.



Enter PIN

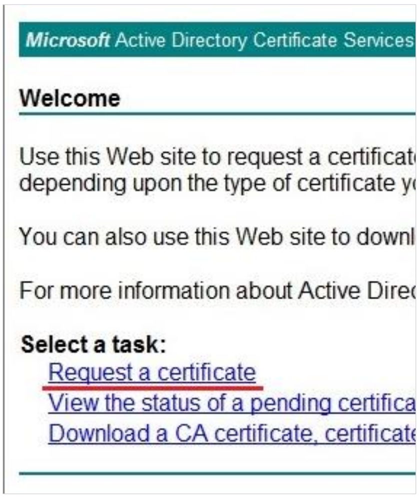
PIN: •••••••••••••

→ The private key is generated and saved to the device.

13. Deploy the PKI. For details, see the Microsoft article which describes how to configure the internal certificate authority.

14. In **Internet Explorer**, open an enterprise Certification Authority page (generally, it looks like *https://IP-adress_of_CA/certsrv* or *https://domain_name_of_certificate _authority/certsrv*). When authorization is required, enter the credentials of the user, whom the certificate must be given to.

15. Click the **Request a certificate** link.



Microsoft Active Directory Certificate Services

Welcome

Use this Web site to request a certificat
depending upon the type of certificate y

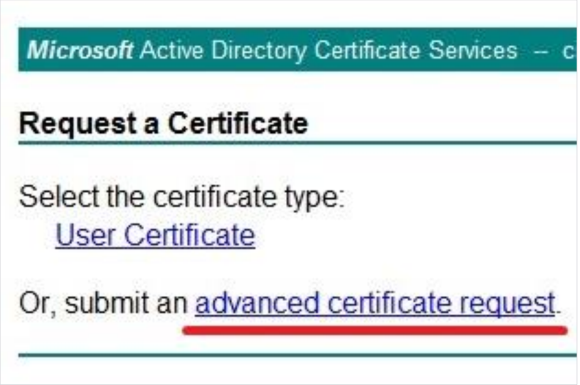
You can also use this Web site to downl

For more information about Active Direc

Select a task:

Request a certificate
View the status of a pending certifica
Download a CA certificate, certificate

16. Click the **advanced certificate request** link.



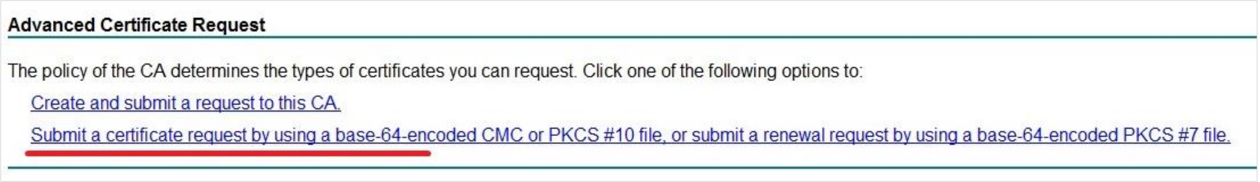
Microsoft Active Directory Certificate Services -- c

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

17. Click the link **Submit a certificate request by using a base 64-encoded CMC**…

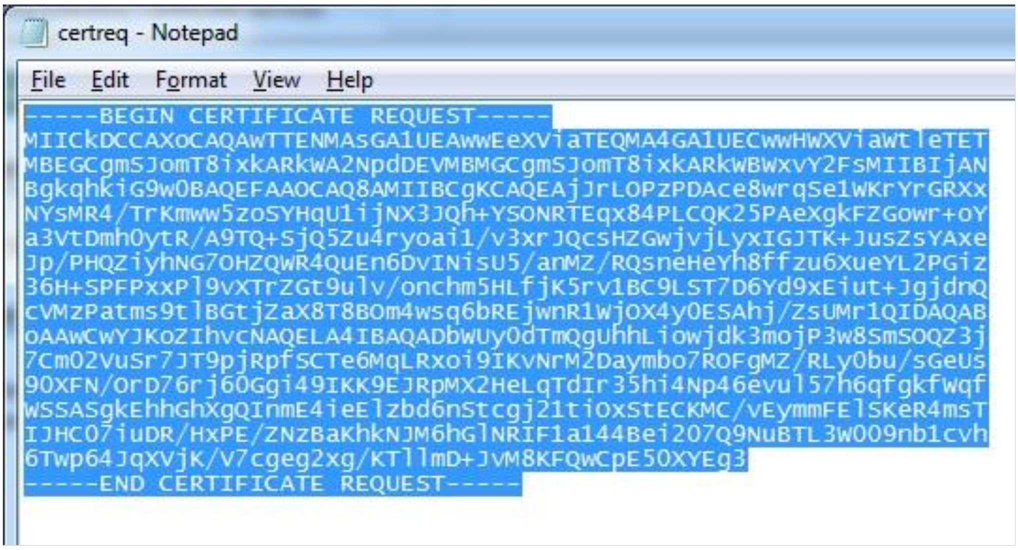


Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

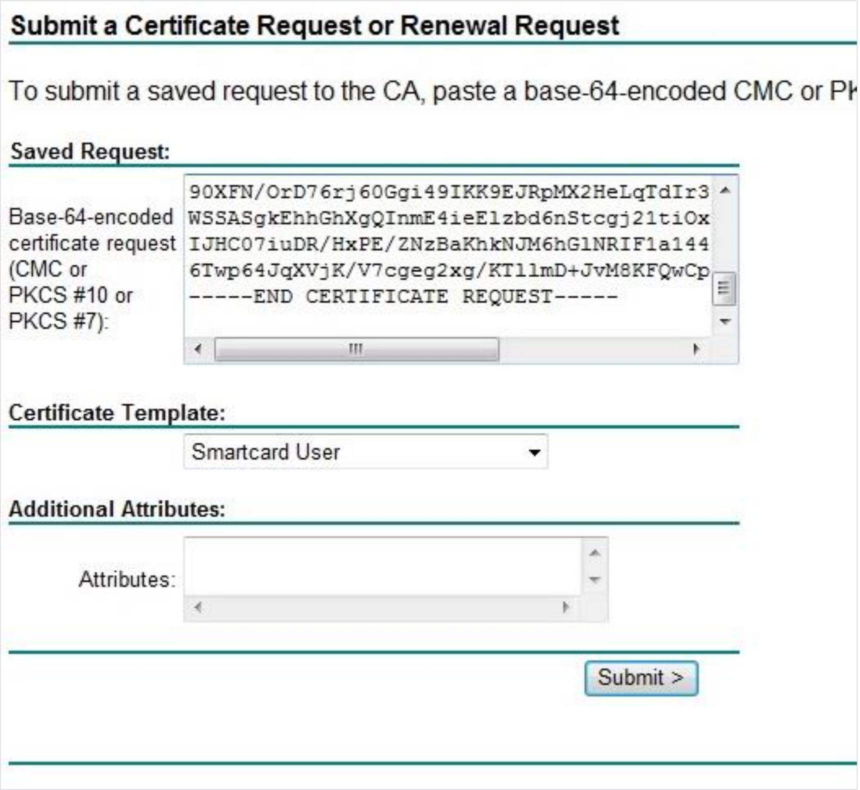
18. Open the certificate request file in any text editor (for example, Notepad), and copy its content to the clipboard.



```
-----BEGIN CERTIFICATE REQUEST-----
MIICkDCCAXoCAQAwTTENMAsGA1UEAwwEeXViaTEQMA4GA1UECwwHWXViaWtleTET
MBEGCgmSJomT8ixkARkWA2NpdDEVMBMGCgmSJomT8ixkARkWBWxvY2FsMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAjJrLOPzPDAce8wrqSe1WKrYrGRXx
NYsMR4/TrKmww5zoSYHqU1ijNX3JQh+YSONRTEqx84PLCQK25PAeXgkFZGowr+oY
a3VtDmh0ytR/A9TQ+SjQ5Zu4ryoai1/v3xrJQcsHZGwjvjLyxIGJTK+JusZsYAxe
Jp/PHQZiyhNG7OHZQWR4QuEn6DvINisU5/anMZ/RQsneHeYh8ffzu6XueYL2PGiz
36H+SPFPxxPl9vXTrZGt9ulv/onchm5HLfjK5rv1BC9LST7D6Yd9xEiut+JgjdnQ
cVMzPatms9tlBGtjZaX8T8BOm4wsq6bREjwnR1WjOX4y0ESAhj/ZsUMr1QIDAQAB
oAAwCwYJKoZIhvcNAQELA4IBAQADbWUy0dTmQgUhhLiowjdk3mojP3w8SmSOQZ3j
7CmO2VuSr7JT9pjRpfSCTe6MqLRxoi9IKvNrM2Daymbo7ROFgMZ/RLy0bu/sGeUs
90XFN/OrD76rj60Ggi49IKK9EJRpMX2HeLqTdIr35hi4Np46evul57h6qfgkfWqf
WSSASgkEhhGhXgQInmE4ieElzbd6nStcgj21tiOxStECKMC/vEymmFElSKeR4msT
IJHC07iuDR/HxPE/ZNzBaKhkNJM6hGlNRIF1a144Bei207Q9NuBTL3W009nb1cvh
6Twp64JqXVjK/V7cgeg2xg/KTllmD+JvM8KFQwCpE50XYEg3
-----END CERTIFICATE REQUEST-----
```

19. Paste information from clipboard to the **Saved Request** field. In the **Certificate Template** section, select **Smartcard User** from the drop-down list, and press the **Submit** button.

Figure 1. Submit a certificate request



Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or Pk

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
90XFN/OrD76rj60Ggi49IKK9EJRpMX2HeLqTdIr3
WSSASgkEhhGhXgQInmE4ieElzbd6nStcgj21tiOx
IJHC07iuDR/HxPE/ZNzBaKhkNJM6hGlNRIF1a144
6Twp64JqXVjK/V7cgeg2xg/KTllmD+JvM8KFQwCp
-----END CERTIFICATE REQUEST-----
```

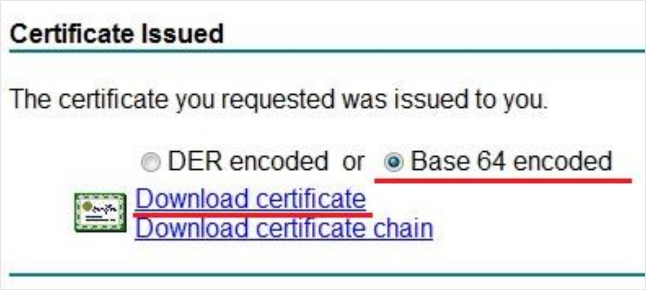
Certificate Template:

Smartcard User

Additional Attributes:

Attributes:

20. Select the **Base 64 encoded** radio button, and then click the **Download certificate** link to save the certificate in the **Base 64** format.



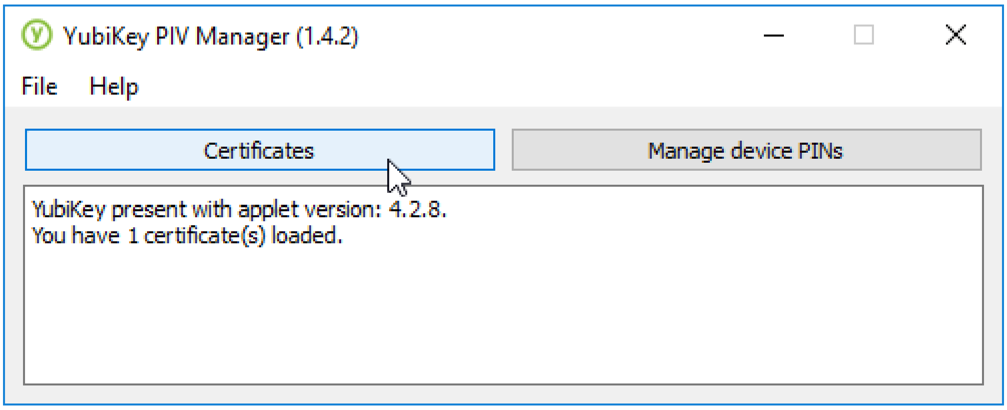
Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

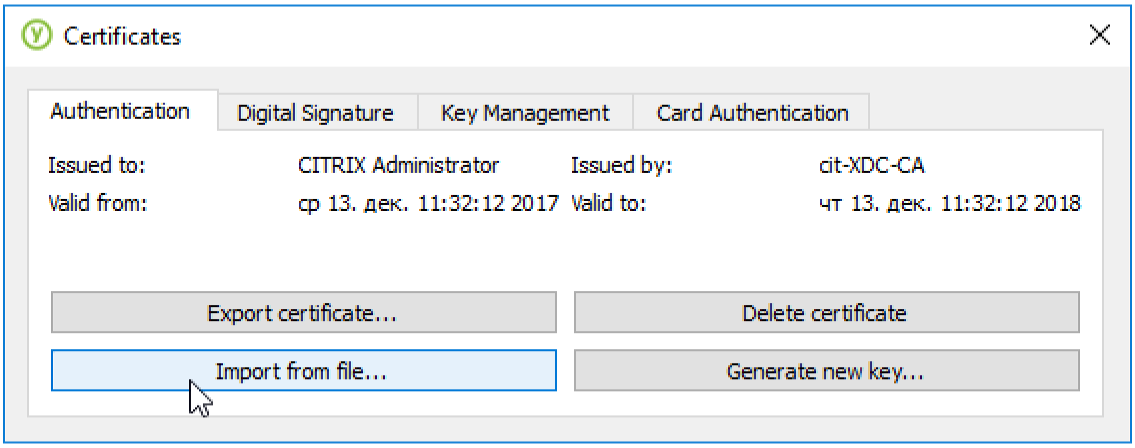
Download certificate
Download certificate chain

21. Open the **YubiKey PIV Manager** utility application, and then click the **Certificates** button.



YubiKey present with applet version: 4.2.8.
You have 1 certificate(s) loaded.

22. In the **Authentication** tab, press the **Import from file...** button to load the certificate created from file.



Issued to: CITRIX Administrator Issued by: cit-XDC-CA
Valid from: ср 13. дек. 11:32:12 2017 Valid to: чт 13. дек. 11:32:12 2018

23. Unplug and re-attach the device to use the **YubiKey Neo** device with a new certificate.

Legal Notices