

ČSOB BUSINESS CONNECTOR

PROCEDURE FOR CREATING A COMMUNICATION CERTIFICATE

This guide describes how to create a communication certificate for the ČSOB Business Connector API for cases when the application supplied by the bank is not used for communication with the API, but all communication is provided from ERP or other software and only a communication certificate is needed for the functionality itself.

The process of obtaining the communication certificate itself has the following steps:

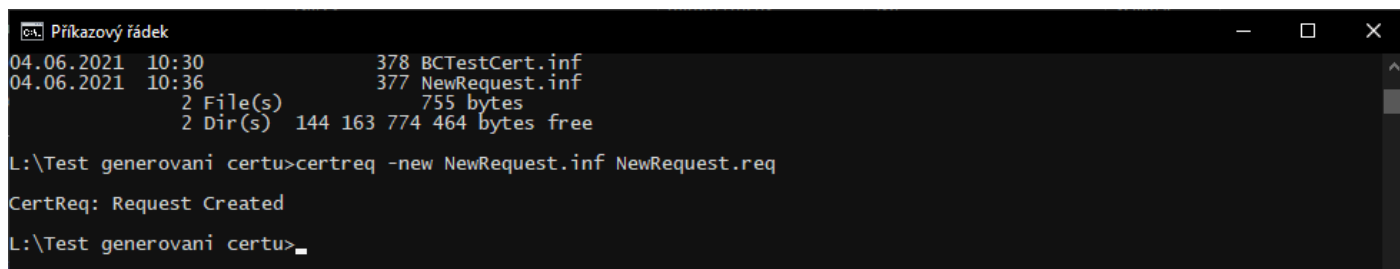
1. Creating a certificate request in the application and saving it to the computer disk.
2. Uploading a certificate request to the portal and downloading the created certificate.
3. Pairing a downloaded certificate with private keys.

The easiest way to generate communication certificates without using Business Connector is by using the Windows tool certreq.exe.

To create a certificate request, you must first create a text file with a request template following the template below. To do this, use notepad (notepad.exe, not Word for example). Note that some editors insert an invisible BOM at the beginning of the file. Save the file as ASCII or UTF-8 without the BOM.

```
[NewRequest]
Subject="CN=<BC server>, C=CZ"
KeySpec=1
HashAlgorithm=sha256
KeyLength=2048
UseExistingKeySet=FALSE
Exportable=TRUE
UserProtected=FALSE
MachineKeySet=FALSE
ProviderName="Microsoft RSA SChannel Cryptographic Provider"
ProviderType=12
RequestType=PKCS10
KeyUsage=0xa0
SMIME=False
SuppressDefaults=true
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.2
```

In the template, specify the computer name on the Subject=line after the CN= characters. The name must not contain comma character (,) or quotation marks ("). This name will be included in the name of the issued certificate. Save the template file and name it e.g. BCcert.inf in the Documents folder.



```
Príkazový řádek
04.06.2021 10:30          378 BCTestCert.inf
04.06.2021 10:36          377 NewRequest.inf
          2 File(s)          755 bytes
          2 Dir(s) 144 163 774 464 bytes free

L:\Test generovani certu>certreq -new NewRequest.inf NewRequest.req
CertReq: Request Created
L:\Test generovani certu>
```

Run the command prompt. At the command prompt, navigate to the directory where the certificate request template is stored and type "certreq -new NewRequest.inf NewRequest.req", this creates the certificate request. Upload this request to the CEB portal where it will generate a certificate.

The screenshot shows the 'Business Connector settings' page. On the left is a navigation menu with items like Security, My permissions, Personalization, Account settings, CEB Info, Business Connector, and Service administration. The main content area is titled 'Business Connector settings' and contains a 'Certificate request' form. The form has two fields: 'Certificate request *' with a 'Select file' button and a green checkmark, and 'Name *' with a text input containing 'Test certificate' and a green checkmark. Below the form are 'Back' and 'Send' buttons. At the top right, there is a user profile for 'Jiří Vohnout' and a 'Log out' link.

After logging into the service, go to Menu>Settings>Business Connector and select the Add button. Then use select File to upload the certificate request file, after pressing the Submit button a certificate will be created and ready for download.

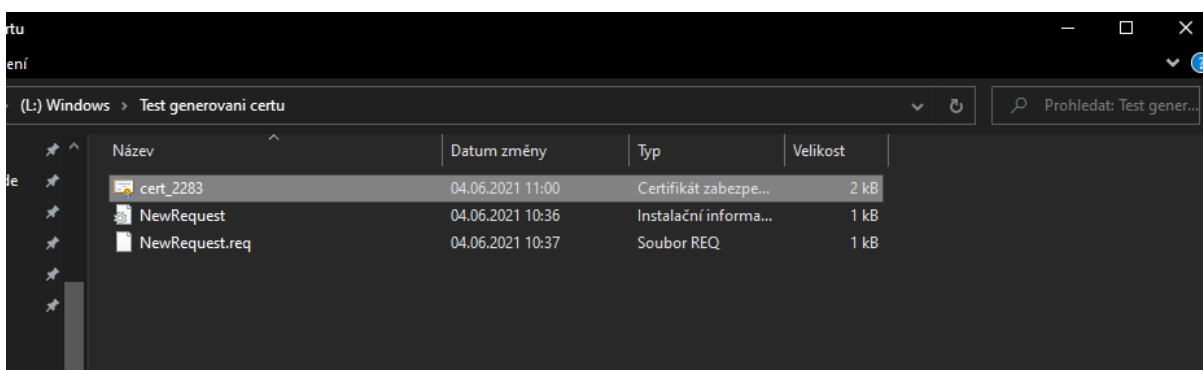
The screenshot shows the 'Business Connector settings' page after a successful certificate generation. A green message box at the top states: 'The certificate has been successfully generated. You can download the certificate file. Download certificate'. Below this is a section titled 'Your certificates' with 'Add' and 'Request certificate' buttons. A table lists the generated certificate:

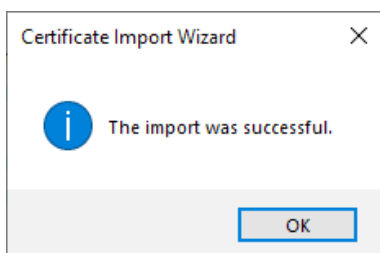
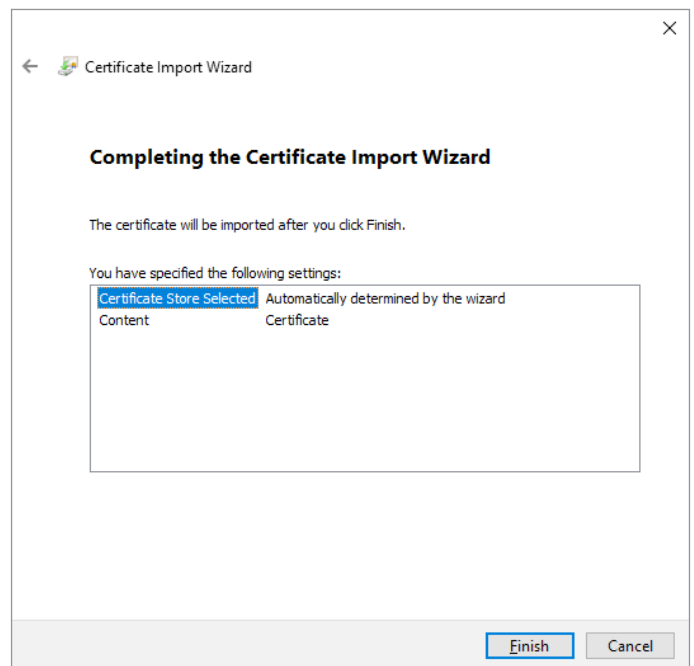
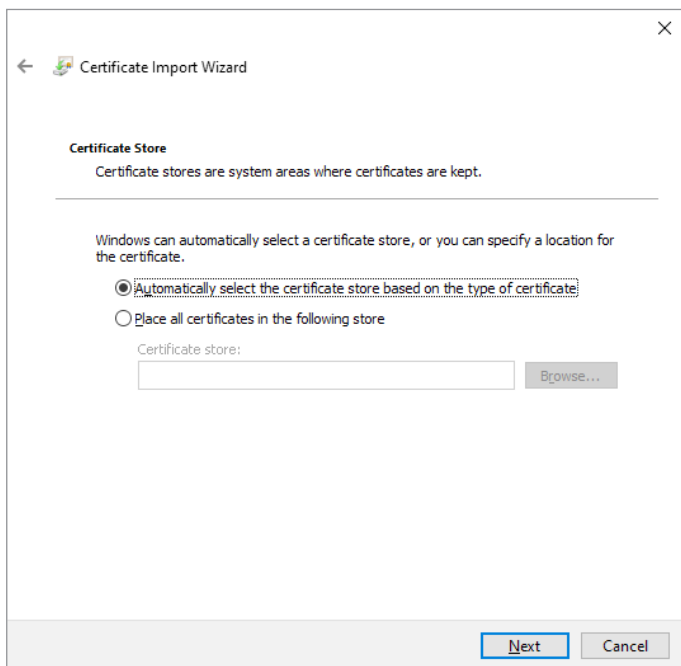
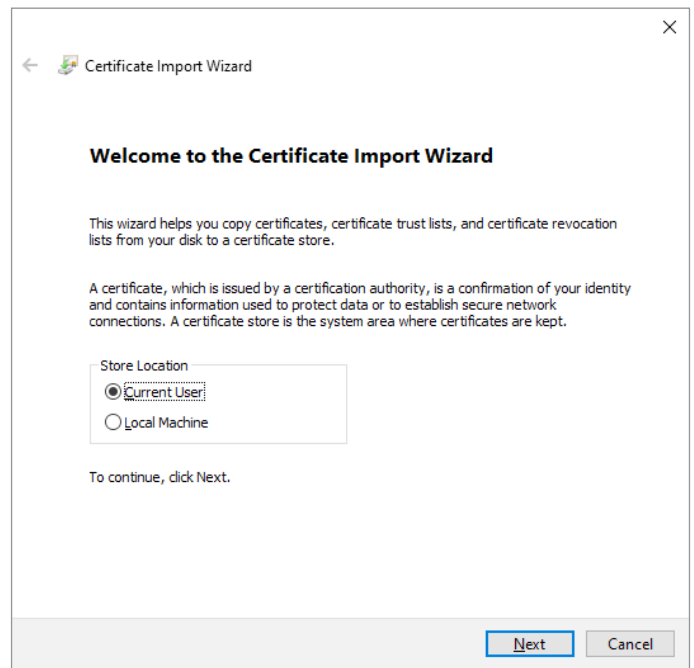
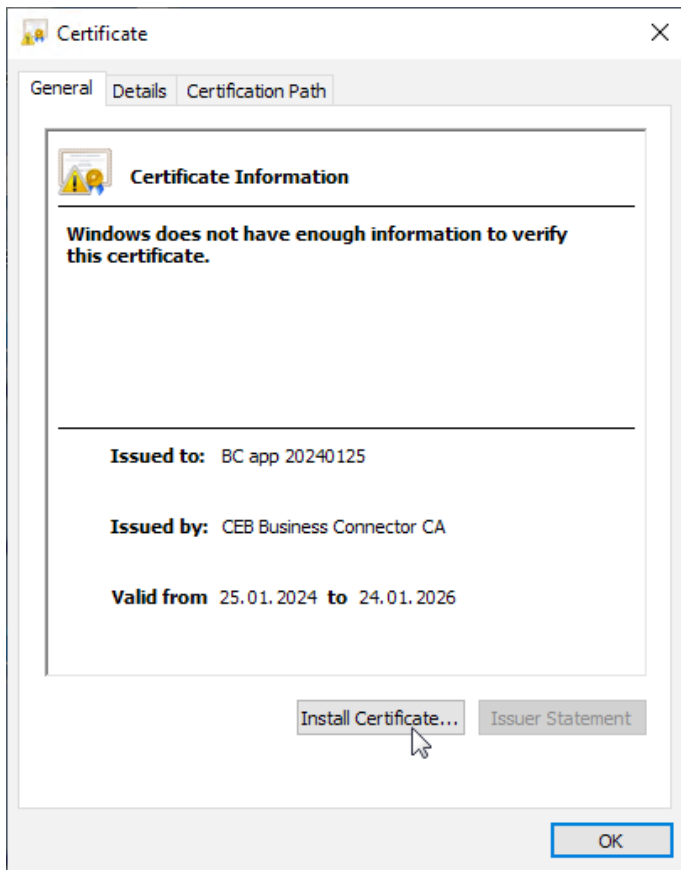
Serial num...	Name	Entity	Issuer	Valid till	Status	Download
125d	Test certificate	W2AB00KH	CEB Bus...	06.12.2020 14:01:29	active	Download ...

Below the table is a 'Scroll to top' link. The top navigation and user profile are the same as in the previous screenshot.

To function properly, the Business Connector service must be enabled on the CEB portal for the required accounts, including the settings for downloading or uploading data.

You must download the finished certificate to the same computer where the request was created and pair the private keys with the downloaded certificate. This is done by opening the certificate file.



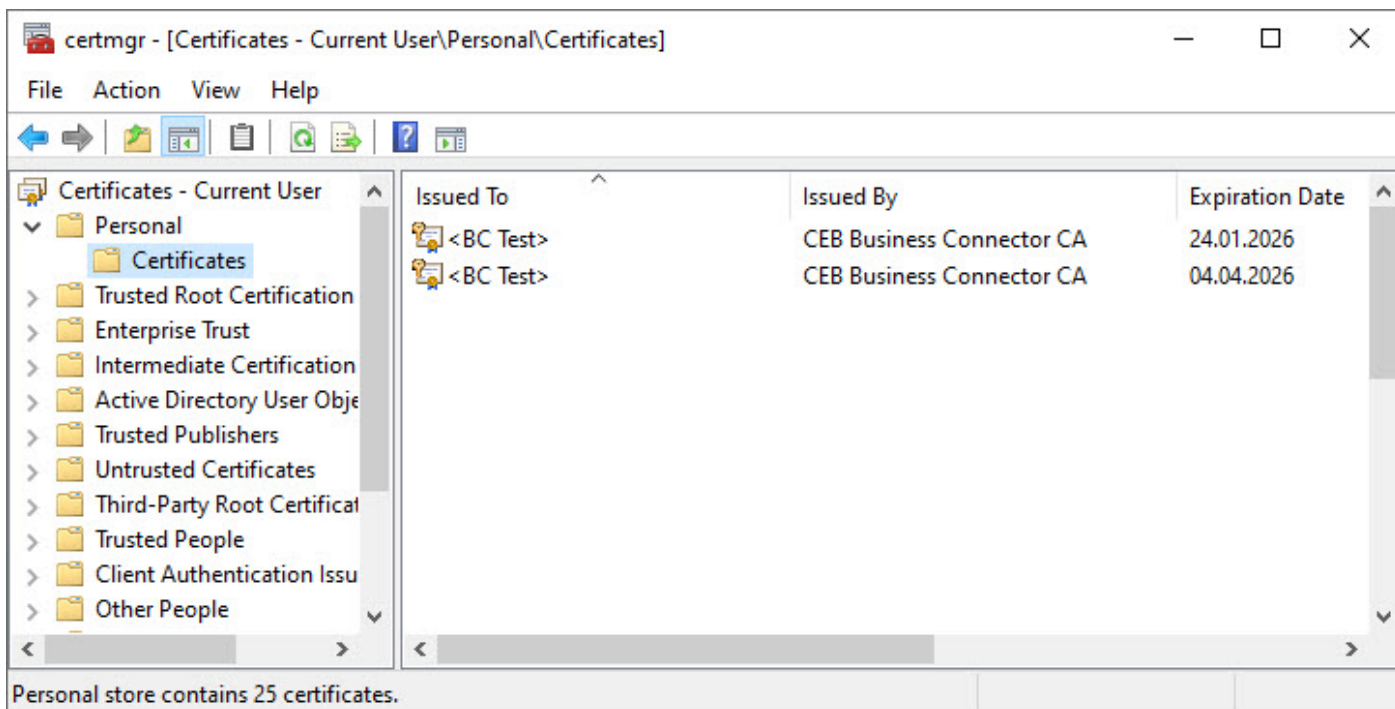


This registers the certificate in Windows and pairs it with the private key so that it can be used on that particular computer. If a certificate in PKCS #12 format is needed to register for Services, or to transfer to another PC, then follow the section. Export the certificate using the system tool.

EXPORT THE CERTIFICATE USING THE SYSTEM TOOL.

Start Manage user certificates, either through the start menu, or the certmgr command at the command prompt.

In certificate management, under Personal Certificates, find the newly created certificate.



Open this certificate and then export it, including the private keys.

