Production environment keys

To work in the NSD EDC system the user's computer must have the following certificates and keys installed:

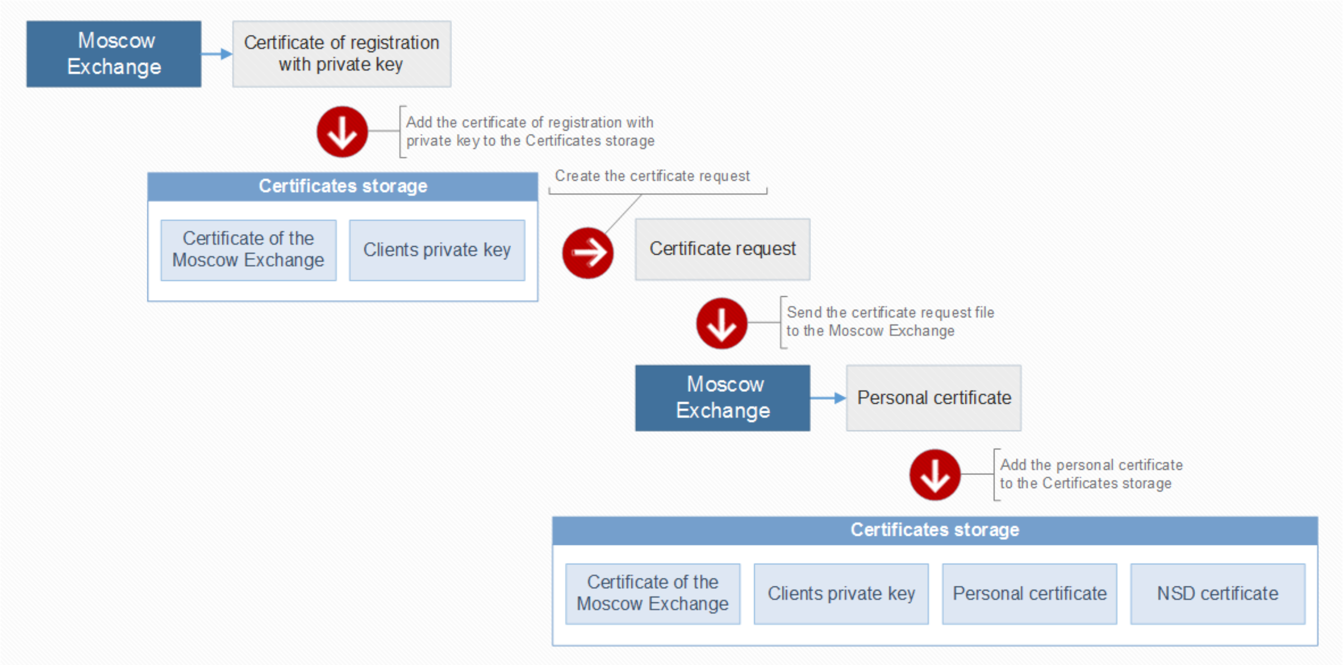
- NSD certificate (public key) to encrypt messages sent from the client to the repository;
- Clients certificate with public and private keys, used for creating digital signature to messages sent from the client to the repository and for decrypting messages sent from the repository to the client;
- Root certificate of the Moscow Stock Exchange (Certification Authority, hereinafter CA).

On this page:

Further information:

- Creating profiles

Scheme 1 shows the general procedure of installing certificates and keys.


Moscow Exchange
Certificate of registration with private key
Add the certificate of registration with private key to the Certificates storage
Certificates storage
Certificate of the Moscow Exchange
Clients private key
Create the certificate request
Certificate request
Send the certificate request file to the Moscow Exchange
Moscow Exchange
Personal certificate
Add the personal certificate to the Certificates storage
Certificates storage
Certificate of the Moscow Exchange
Clients private key
Personal certificate
NSD certificate

Scheme 1 – the general procedure of installing certificates

Obtaining a certificate

From the Moscow Exchange you obtain a certificate of registration document and a CD disk, comprising of:

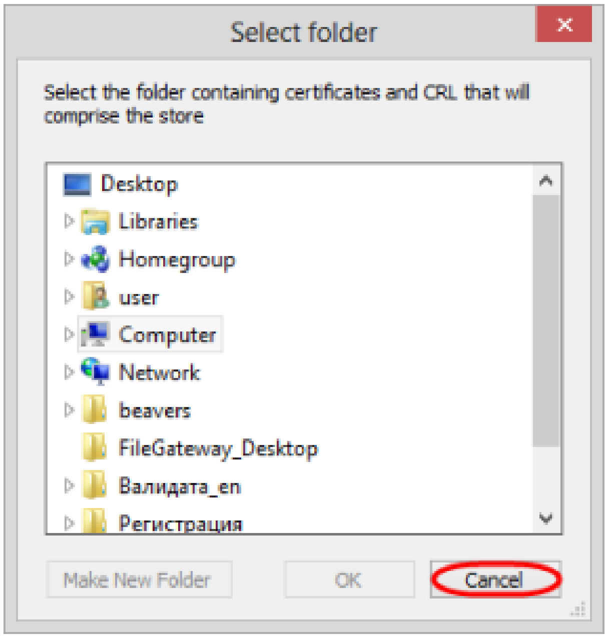
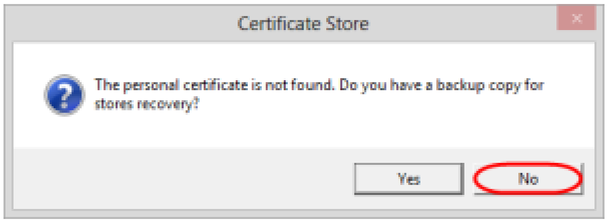
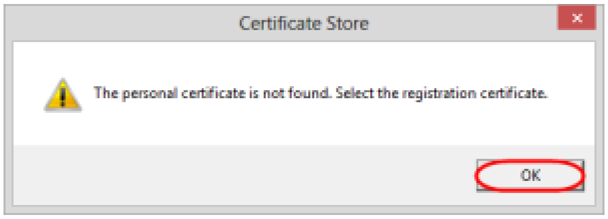
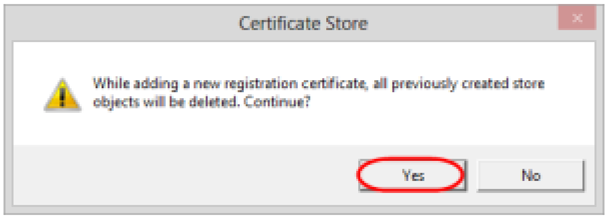
- software (MOEX EDS DSSK: Certificates storage, MOEX EDS DSSK: Java API);
- certificate of registration with private key.

> The key and the certificate of registration are not intended to provide security of the transmitted information. They will be added to the Certificates storage for the generation of the private and public key and creating of a request to issue a certificate for the Moscow Exchange. The key and the registration certificate are to be copied to the root folder on any external drive, such as a usb-stick.

Certificate of registration are used for:

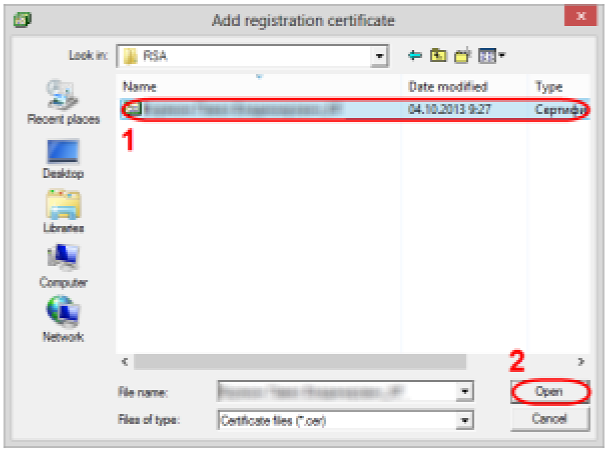
1. generation of user's private and public key;
2. creation of a request to issue a public key certificate.

Depending where the certificate is stored (external hard drive or a computer), the order they are added to the Certificates storage and making a request will differ.

	If the key and the certificate of registration are stored on the user's computer	
1 Step	During the first start a window will open informing you that you need to insert an external drive. As the key and the certificate of registration are located on your computer, skip this step and click **Cancel**	
2 Step	During the initial connection the user only has a certificate of registration, so skip this step by clicking **Cancel**	 Select folder Select the folder containing certificates and CRL that will comprise the store Desktop Libraries Homegroup user Computer Network beavers FileGateway_Desktop Валидата_en Регистрация Make New Folder OK Cancel
3 Step	Next the storage will be automatically checked for the presence of a personal certificate. During the first start a personal certificate and copies of storagies are not available. Skip step by clicking **No**	 Certificate Store The personal certificate is not found. Do you have a backup copy for stores recovery?
4 Step	Then the screen will sequentially display windows for selecting the certificate of registration, where you need to click **OK** and **Yes** respectively	 Certificate Store The personal certificate is not found. Select the registration certificate.  Certificate Store While adding a new registration certificate, all previously created store objects will be deleted. Continue?

5
Step

The window for adding a certificate of registration will appear, where you need to select the certificate file and click **Open**. The registration key will be imported automatically (provided that it is next to a certificate, in the same folder)



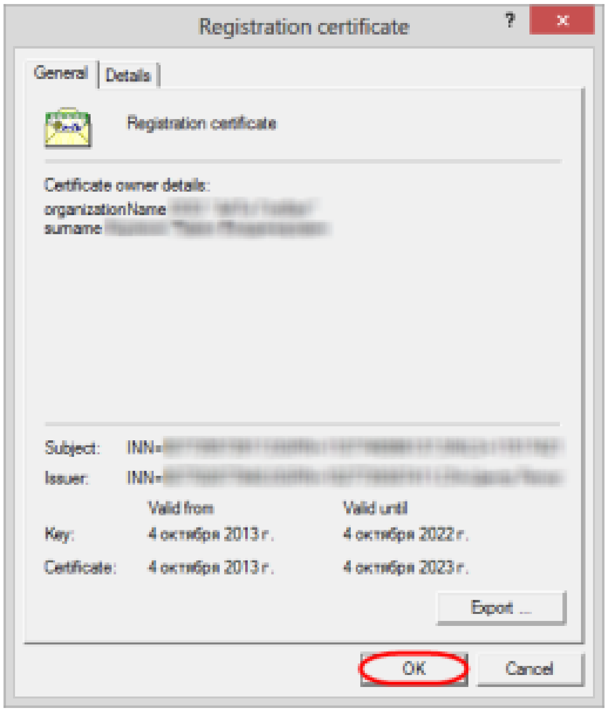
6
Step

Next, the screen displays information about adding certificates of registration

The certificate of registration will serve as a basis for creating a personal and local storage. The personal storage is confirmed with an electronic signature using the registration key.

The personal storage will display the certificate of Moscow Exchange, and the user's registration certificate under Certificate of registration

Click **OK** to continue working in the storage



Registration certificate

Certificate owner details:
organizationName
surname

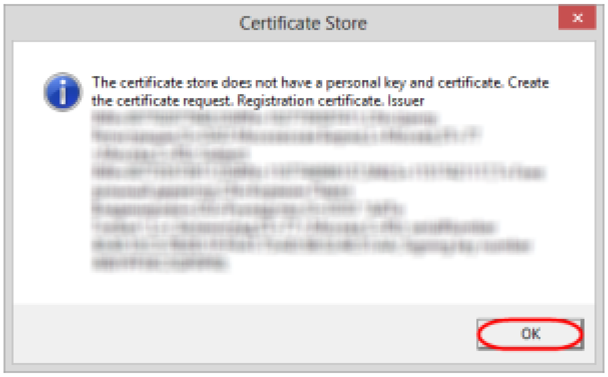
Subject: INN=
Issuer: INN=

	Valid from	Valid until
Key:	4 октября 2013 г.	4 октября 2022 г.
Certificate:	4 октября 2013 г.	4 октября 2023 г.

7
Step

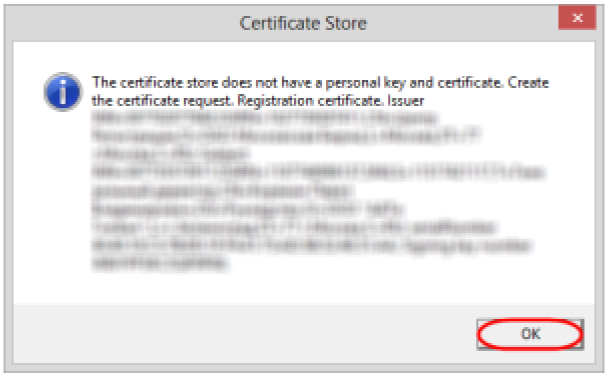
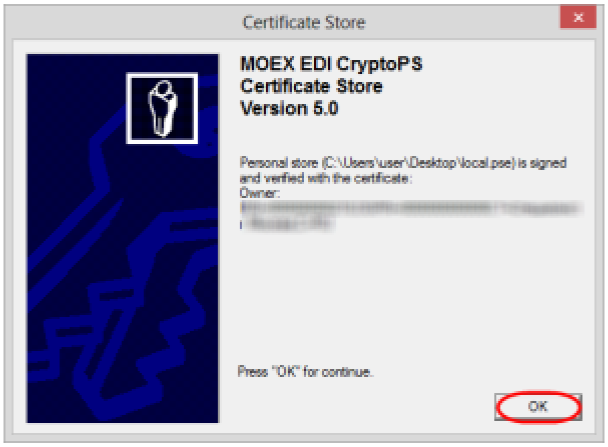
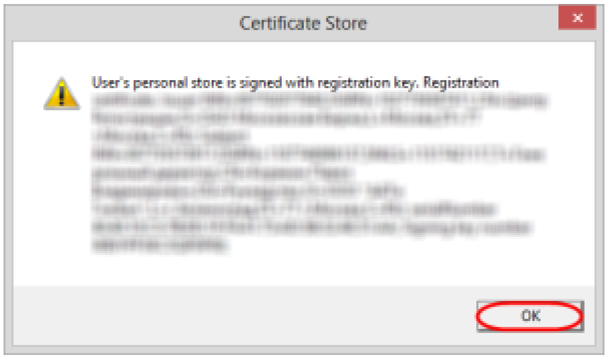
Next, you will need to generate your public and private key and a request for their confirmation by the Moscow Stock Exchange by clicking **OK**

If the registration certificate and keys are stored on the computer, the request and the private keys will be generated automatically



The certificate store does not have a personal key and certificate. Create the certificate request. Registration certificate. Issuer

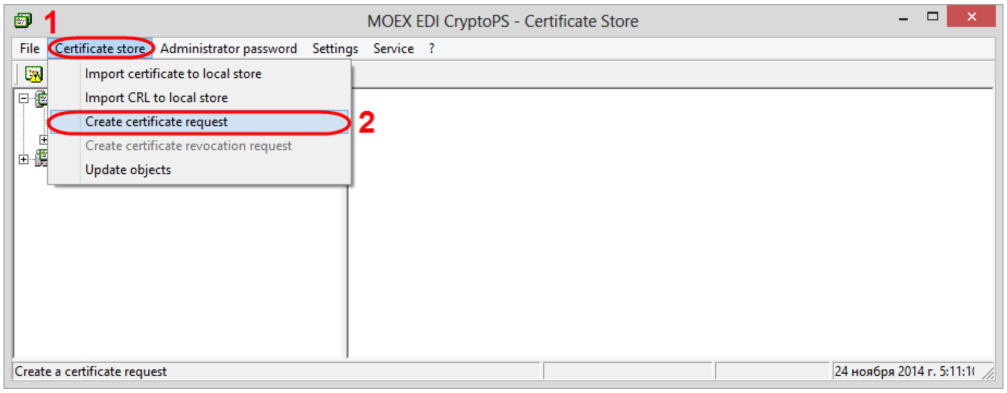
If the key and the certificate of registration are stored on an external drive

1 Step	Before you begin, insert an external drive in the usb-port on your computer, then run the Certificates storage. This opens a window where you will need to select device containing the key and certificate of registration and click **OK**	
2 Step	As a result the key and the certificate of registration will be added automatically. The screen will display a message containing information about the added files, where you need to click **OK**	 Certificate Store The certificate store does not have a personal key and certificate. Create the certificate request. Registration certificate. Issuer [redacted] OK
3 Step	The certificate of registration will serve as a basis for creating a personal and local storage (profile). The personal storage is confirmed with an electronic signature using the registration key. The personal storage will display the certificate of Moscow Exchange, and the user's registration certificate in **Certificates of registration** section	 Certificate Store **MOEX EDI CryptoPS** **Certificate Store** **Version 5.0** Personal store (C:\Users\user\Desktop\local.pse) is signed and verified with the certificate: Owner: [redacted] Press "OK" for continue. OK
4 Step	Next, a message will appear informing you that the personal storage is protected with the registration certificate. In this window you need to click **OK** to create private keys and make a request for their confirmation (see Generation of user keys and creating a request)	 Certificate Store User's personal store is signed with registration key. Registration [redacted] OK

Public and private key are created simultaneously with the request to the Certification Authority to issue a certificate. Keys cannot be used to protect information transmitted until they are certified by the Certification Authority (the Moscow Exchange). Therefore, a request is made for their confirmation, which contains information about the generated public key (Fig. 2) and information about the user, automatically added from the certificate of registration. The Moscow Exchange (CA) responds with an email containing certificate signed by the CA root certificate.

If the certificate of registration are stored on the computer, after **step 7** in the table above, Certificates storage will automatically generate user's private and public keys and a request to issue a **public key certificate** (Fig. 2).

If the certificate of registration are stored on an external drive, to generate keys and make a request select the   **(Certificates storage in the menu)** (Fig. 1.1)   **(Generate certificate request)** (Fig. 1.2), or click an icon on the toolbar.

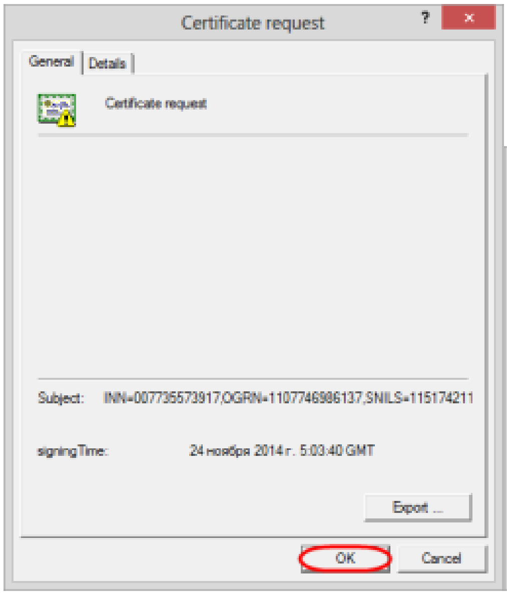

1
MOEX EDI CryptoPS - Certificate Store
File
Certificate store
Administrator password
Settings
Service
?
Import certificate to local store
Import CRL to local store
Create certificate request
2
Create certificate revocation request
Update objects

Create a certificate request

24 ноября 2014 г. 5:11:1(

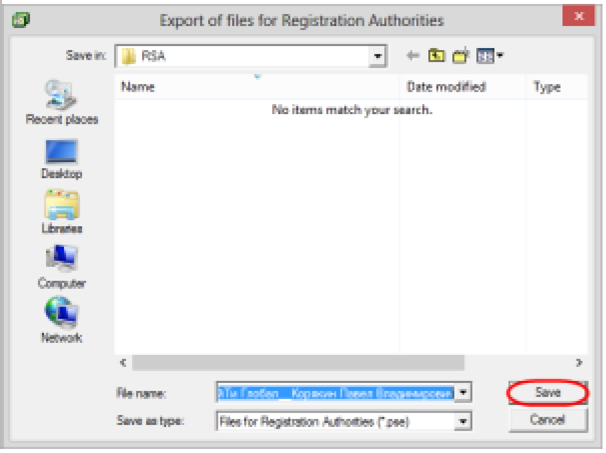
Fig. 1 – generation of a request

In the **Certificate request** dialog box, click **OK** (Figure 2). This will open the **Export files for the Registration Centers**, where you should select a folder to which the request will be saved and click the **Save** button (Fig. 3).



Subject: INN=007735573917,OGRN=1107746986137,SNILS=115174211

signingTime: 24 ноября 2014 г. 5:03:40 GMT



Save in: RSA

No items match your search.

File name: [illegible]

Save as type: Files for Registration Authorities (*.pse)

Fig. 2 – request parameters

Fig. 3 – export files

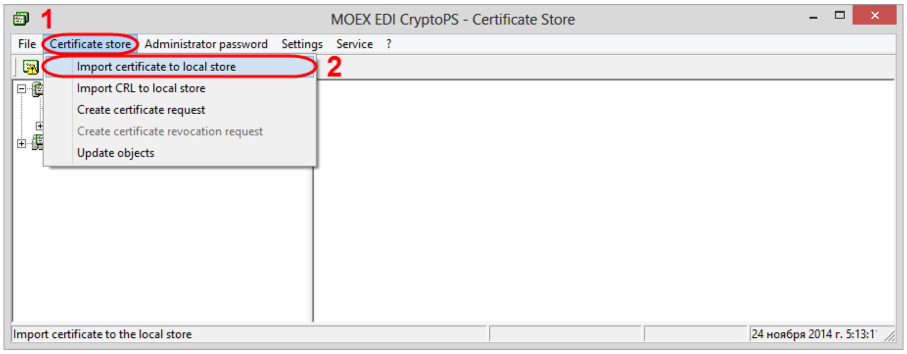
The resulting request (a *.pse file) needs to be compressed and sent to pki@moex.com, with a scanned and signed registration certificate (document) attached. The subject field should specify the **name of the organization** and the required **scope of the certificate** (for example, the **Oblachnye Investitsii CJSC – exchange market EDI, stock market EDI**). The Moscow Exchange will respond with a letter with an attached ZIP-file of the certificate. This certificate must be added to the Certificates storage.

⚠ The resulting certificate is valid only for the **generated public and private key** that is stored on the user's computer. **Therefore, a certificate from the Moscow Exchange must be added to the Certificates storage installed on the same computer, where the certificate issue request was generated!**

Adding a certificate to the Certificates storage

To add a certificate to the Certificates storage:

1. run Certificates storage menu using the **Start menuAll Programs   (MOEX EDS DSSK) (Certificates storage)**;
2. select   **(Certificates storage)**   **(Import Certificate)** to the local storage (see Figure 4). This will open a window to select the certificate file (Fig. 5);


1
MOEX EDI CryptoPS - Certificate Store
File
Certificate store
Administrator password
Settings
Service
?
Import certificate to local store
2
Import CRL to local store
Create certificate request
Create certificate revocation request
Update objects
Import certificate to the local store
24 ноября 2014 г. 5:13:1

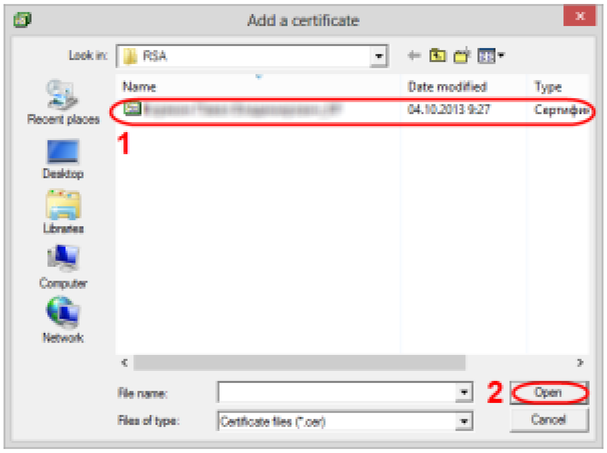
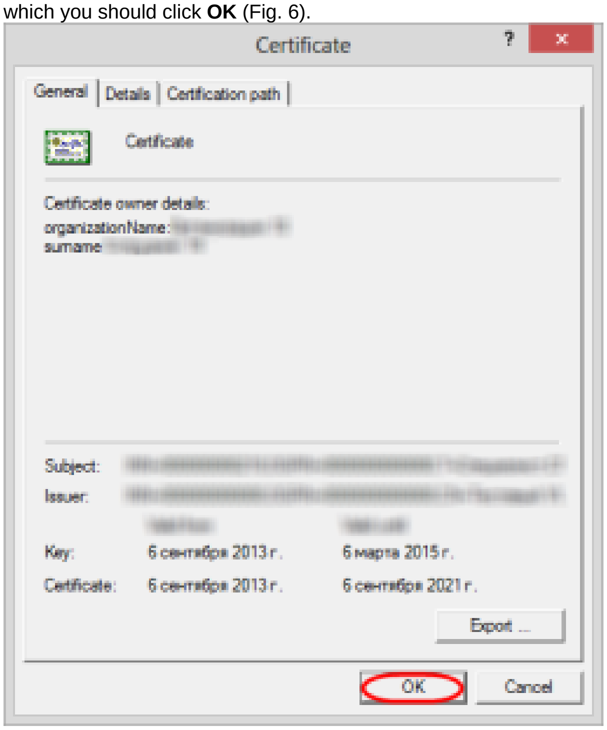


Fig. 4 – starting to import file

Fig. 5 – selecting a certificate

3. select the certificate file (see Fig. 5.1) and click **OK** (see Fig. 5.2). Before adding a window will open displaying the certificate to be added, in which you should click **OK** (Fig. 6).



Certificate

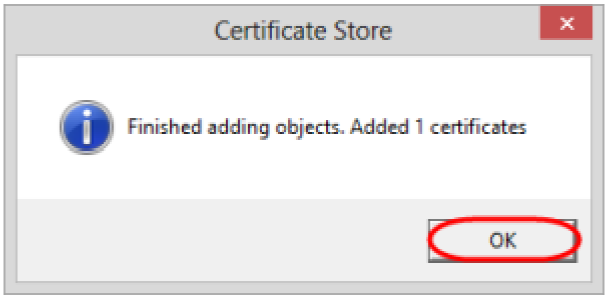
Certificate owner details:
organizationName: [redacted]
surname [redacted]

Subject: [redacted]
Issuer: [redacted]

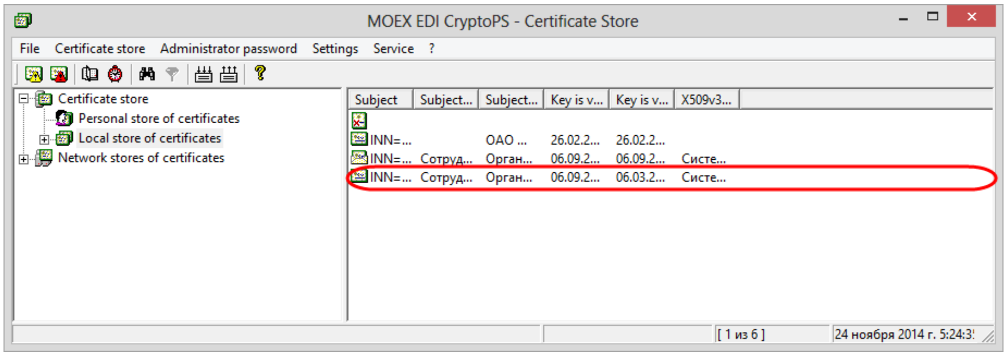
	[redacted]	[redacted]
Key:	6 сентября 2013 г.	6 марта 2015 г.
Certificate:	6 сентября 2013 г.	6 сентября 2021 г.

Fig. 6 – information about the certificate to be added

This will open a window informing the certificate was successfully added to the Certificates storage, where you need to click **OK** (Fig. 7). Example of adding a certificate is presented in Fig. 8.



Finished adding objects. Added 1 certificates

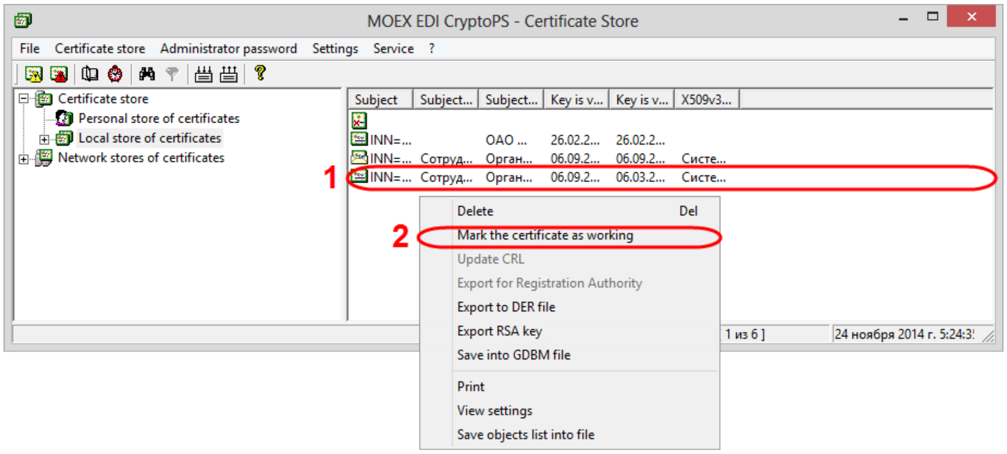

MOEX EDI CryptoPS - Certificate Store
File
Certificate store
Administrator password
Settings
Service
?
Certificate store
Personal store of certificates
Local store of certificates
Network stores of certificates

Subject	Subject...	Subject...	Key is v...	Key is v...	X509v3...
INN=...		OAO ...	26.02.2...	26.02.2...	
INN=...	Сотруд...	Орган...	06.09.2...	06.09.2...	Систе...
INN=...	Сотруд...	Орган...	06.09.2...	06.03.2...	Систе...

[1 из 6] 24 ноября 2014 г. 5:24:3!

Fig. 7 – informative message Fig. 8 – example of adding a certificate

Then the certificate must be set as **default**. To do this, select the added certificate, right-click on the shortcut menu, and select **(Make certificate workable)** (Fig. 9).


MOEX EDI CryptoPS - Certificate Store
File
Certificate store
Administrator password
Settings
Service
?
Certificate store
Personal store of certificates
Local store of certificates
Network stores of certificates
1
2
Delete Del
Mark the certificate as working
Update CRL
Export for Registration Authority
Export to DER file
Export RSA key
Save into GDBM file
Print
View settings
Save objects list into file

Subject	Subject...	Subject...	Key is v...	Key is v...	X509v3...
INN=...		OAO ...	26.02.2...	26.02.2...	
INN=...	Сотруд...	Орган...	06.09.2...	06.09.2...	Систе...
INN=...	Сотруд...	Орган...	06.09.2...	06.03.2...	Систе...

1 из 6] 24 ноября 2014 г. 5:24:3!

Fig. 9 – selecting the working certificate

After adding a personal certificate to the Certificates storage, the personal storage is signed on the member's personal certificate. The generation of a digital signature for sent messages is ensured by the private key.

ⓘ Settings will be automatically applied to 64-bit Certificates storage.

⚠ The information for further preparation of the computer and the configuration of the installed components is presented in the following articles:

- How to obtain the.cer file;
- File decryption;
- Web-client performance check.