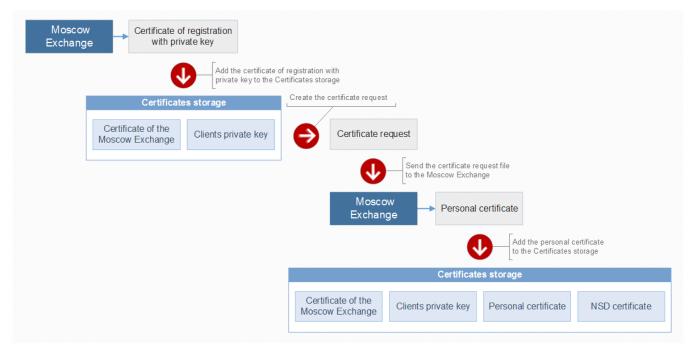
## **Production environment keys**

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:	
<ul><li>Obtaining a certificate</li><li>Adding a certificate to the Certificates storage</li></ul>	
Further information:	
Creating profiles	

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



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 use	er's computer
1 Step	During the first start a window will open informing you that you need to are located on your computer, skip this step and click <b>Cancel</b>	o insert an external drive. As the key and the certificate of registration
2 Step	During the initial connection the user only has a certificate of registration, so skip this step by clicking <b>Cancel</b>	Select folder Select the folder containing certificates and CRL that will comprise the store
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 <b>No</b>	Certificate Store
<b>4</b> Step	Then the screen will sequentially display windows for selecting the certificate of registration, where you need to click <b>OK</b> and <b>Yes</b> respectively	Certificate Store

C	The window for adding a certificate of registration will appear, where you need to select the certificate file and click <b>Open</b> . The registration	Add registration certificate
<b>D</b> Step	key will be imported automatically (provided that it is next to a certificate, in the same folder)	Lookin: RSA
		Computer Computer Network: File name: Files of type: Cetificate files (*.cer) Cancel
6	Next, the screen displays information about adding certificates of registration	Registration certificate ? ×
<b>U</b> Step	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.	General Details Registration certificate
	The personal storage will display the certificate of Moscow Exchange, and the user's registration certificate under Certificate of registration	Certificate owner details: organizationName sumame
	Click <b>OK</b> to continue working in the storage	
		Subject: INN= Issuer: INN= Valid from Valid until Key: 4 октября 2013 г. 4 октября 2022 г. Cetificate: 4 октября 2013 г. 4 октября 2023 г. Бирот
		OK Cancel
7	Next, you will need to generate your public and private key and a request for their confirmation by the Moscow Stock Exchange by clicking <b>OK</b>	Certificate Store
Step	f 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
		ОК
	If the key and the certificate of registration are stored on an exte	ernal drive

1	Before you begin, insert an external drive in the usb-port on your comp you will need to select device containing the key and certificate of regi	
Step		
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 <b>OK</b>	Certificate Store
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 <b>Certificates of registration</b> section	Certificate Store         MOEX EDI CryptoPS Certificate Store Version 5.0         Personal store (C:\Users\user\Desktop\local pse) is signed and vertice Umaric         Version         Press "0K" for continue.
<b>4</b> 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 <b>OK</b> 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

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.

<b>1</b>	1	MOEX EDI CryptoPS - Certificate Store
File	Certificate store Administrator password Setting	js Service ?
8	Import certificate to local store	
<b>-</b>	Import CRL to local store	
	Create certificate request	2
	Create certificate revocation request	
±-	Update objects	
Creat	e a certificate request	24 ноября 2014 г. 5:11:11

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).

Certificate request ? ×					
ieneral Details					
Certificate request					
	<b>a</b>	Expor	t of files for Registration Aut	horities	
	Save in:	🕌 RSA	•	+ 🗈 💣 💷	
	23	Name	*	Date modified	Туре
	Recent places		No items match your	search.	
	Desktop				
	Librates				
Subject: INN=007735573917,OGRN=1107746986137,SNILS=115174211	1				
	Computer				
signingTime: 24 ноября 2014 г. 5:03:40 GMT	Network				
Export		۲.			
		Rename:	аТи Глобел_Корякин Певел Вла		Save
OK Cancel		Save as type:	Files for Registration Authorities ("p	se) 💌	Cance

Fig. 2 – request parameters

/!\

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);

<b>1</b>			Counter DC Countier			_ 🗆 🗙
-			CryptoPS - Certifica	ate store		
	inistrator password Settings	-				
Import certificate     Import CRL to loc     Create certificate     Create certificate     Update objects	al store	2				
Import certificate to the local :	store Add a certi	ficate		×		24 ноября 2014 г. 5:13:1
	Add a certi	licate		_		
Look in: 🎽 RSA		•	+ 🗈 🖆 💷 -			
Ca Name			Date modified	Туре		
Recent places	ere Tasa Pragmanian	- P	04.10.2013 9:27	Сертифио		
I Deaktop Librariez Computer Original Network						
File name: Files of type Fig. 4 — starting to		)	• 2 4	Open Cancel	Fig. 5 – sele	ecting 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).

	Certifi	cate	
General De	tails Certification path		
	Certificate		
Certificate or organization sumame	wner details: Name:		
Subject:	No. concentration of the		Naganasa (P Taringgal (P
			Naganasa (2 Tacinggal (1
	6 сентября 2013 г.	6 марта 2015 г.	Name of Street o
lssuer: Key:	6 сентября 2013 г. 6 сентября 2013 г.	6 марта 2015 г. 6 сентября 2021 г	hummer (F Terrinue) Y
lssuer: Key:		6 сентября 2021 г	Export

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.

Certificate	Store	
Finished adding objects	. Added 1 certificates	
	ОК	
<b>9</b>	MOEX EDI CryptoPS - Certificate Store	- 🗆 🗙
File Certificate store Administrator password Settin	igs Service ?	
🛐 🍱 🕼 🧶 🗰 💎   📇 💾 🎖		
🖃 😰 Certificate store	Subject Subject Subject Key is v Key is v X509v3	
	₩ ■ INN= OAO 26.02.2 26.02.2	
Even store of certificates	САО 20.02.2 20.02.2 INN= Сотруд Орган 06.09.2 06.09.2 Систе	
	(ПNN= Сотруд Орган 06.09.2 06.03.2 Систе	
		24
	[1из6]	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).

<b>1</b>		MOEX	EDI Cry	ptoPS - Ce	ertificate S	Store				×
File Certificate store Administrator password	Settin	gs Service	?							
🖼 🖼 🕼 🧶 🚜 💎   旹 旹   ?										
E- D Certificate store	_	Subject	Subject.	Subject	Key is v	Key is v	X509v3			
Personal store of certificates     Decal store of certificates     Decal store of certificates     Decal store of certificates	4		Сотруд.	Орган		06.09.2				
	1			Орган	06.09.2	00.03.2				~
			-	elete			Del			
		2		lark the certif	ficate as wor	rking	$ \rightarrow$			
				pdate CRL kport for Regi	istration Aut	hority				
				port to DER f		inomy				
				kport RSA key			1	из 61	24 ноября 2014 г. 5:24:	21
				ave into GDB				N5 0 ]	24 H0x0px 2014 1. 5.24.	. <b>3</b> . ///
			Р	rint						
			v	iew settings						
			S	ave objects li	st into file					

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.