Member Portal / Issuer Portal

Section “CA Services”
User Manual

Introduction

This document describes the procedure for an EDMS Participant to interact with a certification authority the functions of which are performed by the Moscow Exchange within the framework of the Electronic Document Management System (the "EDMS CA").

The interaction of the EDMS Participant with the EDMS CA is carried out through the section "CA Services" of the Member Portal (the "MP") or the Issuer Portal (the "IP").

The EDMS Participant has an opportunity to manage all the main stages of the life cycle of certificates of electronic signature verification keys (the "CESVK") used in the EDMS:

- initial creation of CESVK;
- scheduled/unscheduled replacement of CESVK;
- creation of a new CESVK in connection with changes to the existing CESVK.

The functions of the section "CA Services" provides the EDMS Participant with the opportunity to obtain information about the installation keys for the CIPF "Validata CSP", about the CESVKs created for the EDMS Participant, as well as the opportunity to pay for the services of the EDMS CA and update the CESVK of counterparties and the EDMS CA at the workplace of the EDMS Participant.

Gaining Access to the Section "CA Services" in the MP/IP

The procedure for obtaining access to the MP is described in the document "Member Portal User Guide" (https://moex.com/a1676).

The procedure for obtaining access to the IP is described in the document "Instruction on the Procedure for Using the Issuer Portal Information Support" (https://www.moex.com/s20).

Requirements to the Workplace of the EDMS Participant

To interact with the EDMS CA through the MP/IP, the EDMS Participant needs:

- a PC compatible with IBM type PC AT (processor type Pentium and higher) running 32-bit and 64-bit versions of Microsoft Windows operating systems (version 7 or higher) on the x86 or x64 platform;
- browser: Yandex Browser, Atom Browser, Microsoft Edge, Mozilla Firefox or Google Chrome (Google Chrome requires access to the Chrome store);
- browser plugin MoexBrowserPlugin (plugin installation instructions can be found at: https://moex.com/a1676).

If the EDMS Participant plans to manage cryptographic keys on the same PC on which he/she has access to the MP/IP, the following programmes shall be additionally installed on this PC:

- for work with CESVK using certified CIPF (GOST cryptography) – the software package of the ASP "Validata Client" and CIPF "Validata CSP" (https://moex.com/s1292);
- to work with CESVK using non-certified CIPF (RSA cryptography) – the software package "MOEX EDI Cryptoprotection" (https://www.moex.com/s1293).

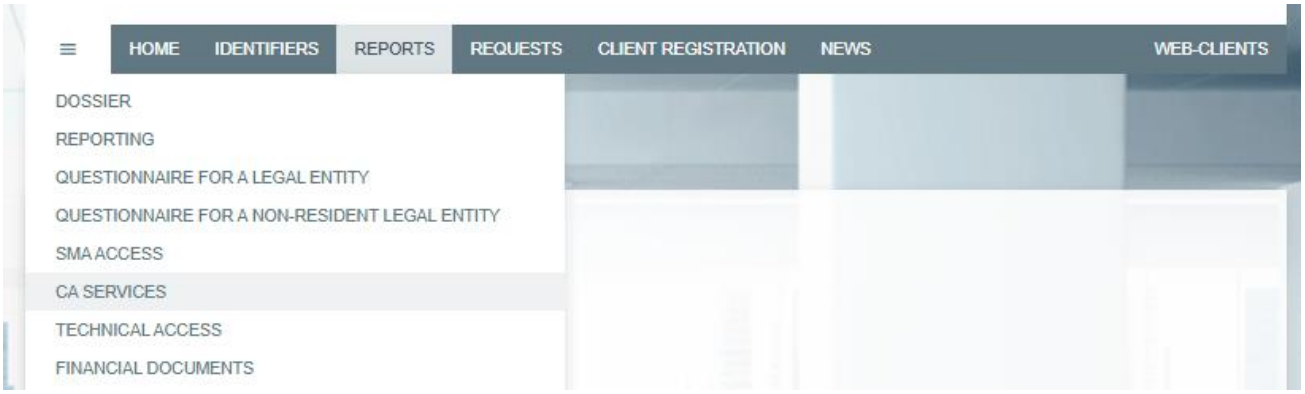
Otherwise, cryptographic keys shall be managed on a separate PC by the security administrator of the EDMS Participant. On such a PC, the software specified in the previous paragraph shall be installed.

IMPORTANT!

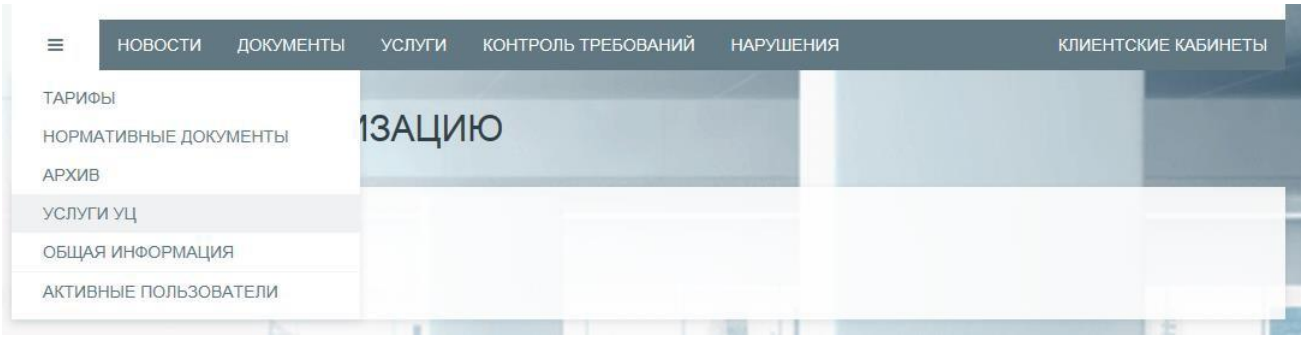
1. The browser plugin MoexBrowserPlugin requires the mandatory installation of the 32-bit version of the software package ASP “Validata Client” (GOST cryptography) or “MOEX EDI Cryptoprotection” (RSA cryptography), including for 64-bit versions of Microsoft Windows operating systems.
2. It is allowed to install simultaneously 32-bit and 64-bit versions of the software packages ASP “Validata Client” or “MOEX EDI Cryptoprotection” on one PC.

Getting Started with the Section “CA Services”

Entrance to the section “CA Services” in the MP: Member Portal → “Three strips” → “CA Services”



Entrance to the section “CA Services” in the IP: Issuer Portal → “Three strips” → “CA Services”



If some of the buttons in the section “CA Services” are inactive, this means that the plugin MoexBrowserPlugin is not configured on this PC.

“Act on Software” Menu Item

The act of granting the right to use the software is a document on the basis of which the EDMS Participant is granted the rights to use the software CIPF “Validata CSP”, ASP “Validata Client” and “ASP Client MOEX EDI Cryptoprotection”.

The act contains information about the registration numbers for the provided software (if any) and the installation key for the CIPF “Validata CSP”.

This menu item allows the EDMS Participant, first of all, to quickly obtain information about the installation key for the CIPF “Validata CSP”.

“Initial Creation of Certificate” Menu Item

Creation of a new CESVK upon initial generation, loss or expiry of a working key is possible only if the EDMS Participant provides the Moscow Exchange with documents drawn up in accordance with the requirements of the Rules for Electronic Document Management (Application for the Creation of CESVK (the “Application”) and a Power of Attorney for the owner of the CESVK (https://moex.com/s1288)).

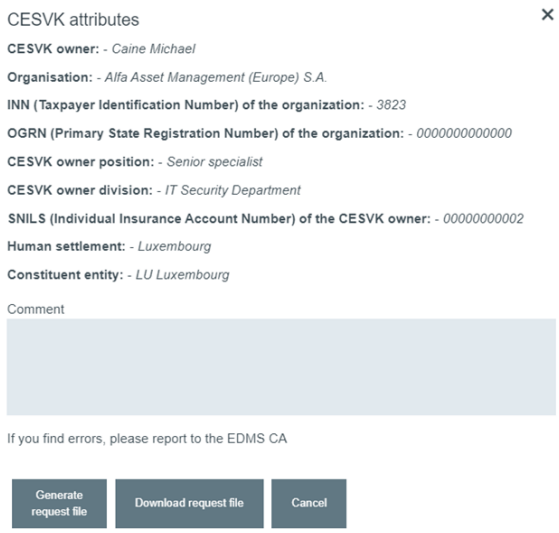
For each Application, a separate information line is displayed containing the full name of the owner of CESVK and the current processing status of this Application.

CERTIFICATE OWNER	DATE OF RECEIVING THE APPLICATION TO THE CA	KEY TYPE	APPLICATION PROCESSING STATUS	
Caine Michael	07.09.2023	GOST	Request received. Processing in progress	
Smith John	06.09.2023	RSA	Certificate Issued	
Caine Michael	06.09.2023	GOST	Application received. Request for creation of CESVK is pending	

To create a new CESVK corresponding to the selected Application in the “Initial Creation of Certificate” section, you shall click the icon “Generate a request to create a new CESVK”.

CERTIFICATE OWNER	DATE OF RECEIVING THE APPLICATION TO THE CA	KEY TYPE	APPLICATION PROCESSING STATUS	
Smith John	06.09.2023	RSA	Application received. Request for creation of CESVK is pending	

1. In the window that opens, you need to check the attributes (details) for the created CESVK. If all the data is correct, you can generate your new working key and a request to create CESVK directly on this PC. To do this, click the button “Generate request file”. Otherwise, click the “Cancel” button and contact the CA to resolve the error.

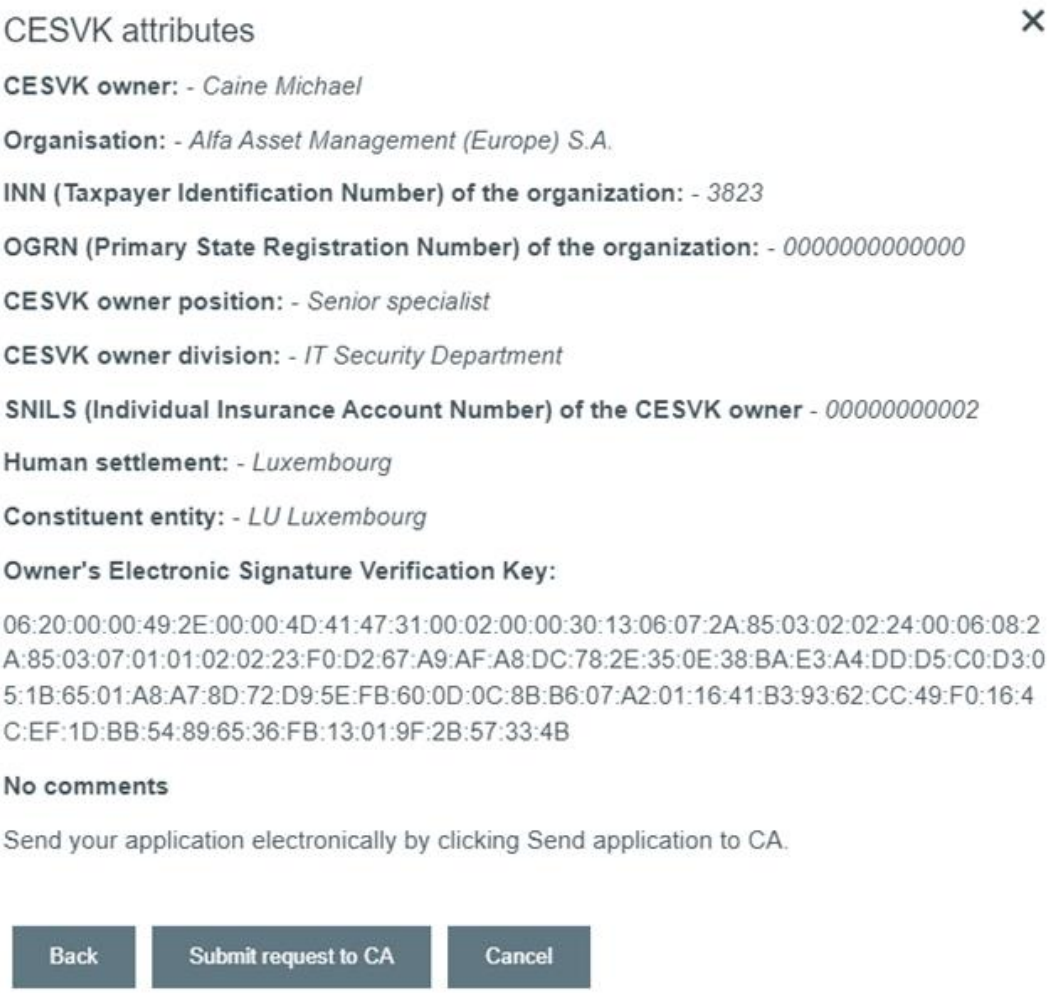


A new working key will be written to the key medium specified in the “CIPF Configuration Programme” (flash drive, ruToken, eToken, registry reader, etc.). The “default” media is a flash drive (removable disk reader). When generating a key, a dialogue box will be displayed for entering a password for the key. If you do not plan to additionally protect your key with a password, or plan to do so later, click “OK” without entering any information.

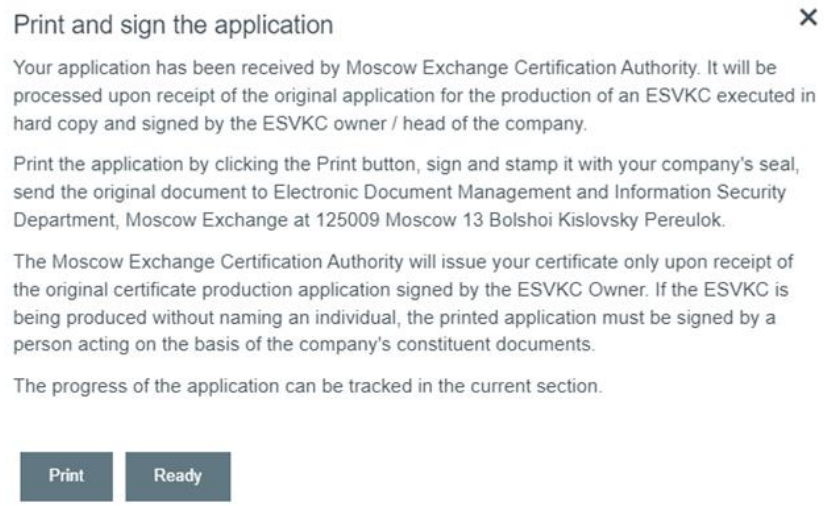
IMPORTANT! If the password for the secret key is lost, it will be impossible to recover this key. In this case, the EDMS Participant shall go through the procedure for the initial creation of a certificate again.

If no software packages for working with certificates (ASP "Validata Client" or "MOEX EDI Cryptoprotection") are installed on this PC of the EDMS Participant, and a dedicated security administrator is responsible for the creation of cryptographic keys in the organisation of the EDMS Participant, click the button "Download request file" and upload the request file generated by the security administrator on a specialised computer designed to generate cryptographic keys.

2. Check the data that will be used in the EDMS CA to form the CESVK. If there are no comments, click the button "Submit request to CA".

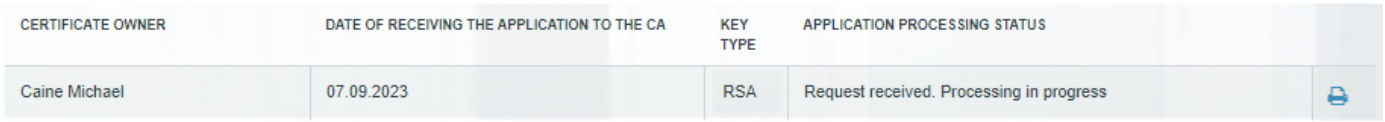


3. Click the "Print" button, print the request for the creation of CESVK on paper, sign it with the certificate owner, certify it with the seal of the organisation and send this document to: Moscow Exchange, 13 Bolshoy Kislovsky pereulok, Moscow 125009.

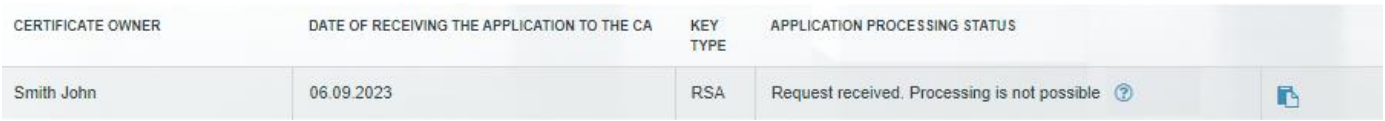


IMPORTANT! Your request will be processed by the EDMS CA only after receiving the sent document.

4. After clicking on the "Done" button, the status of the Application will change to "Request received. Processing in progress".

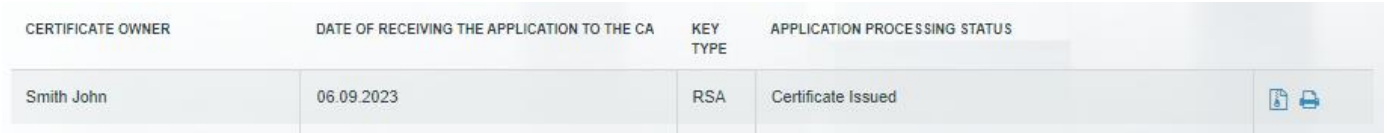


When the status changes to "Request received. Processing is not possible", you can see the reason for the refusal of the EDMS CA by placing the cursor on the icon with the sign "**?**". For a detailed explanation of the reason for the refusal, you need to contact the EDMS CA.

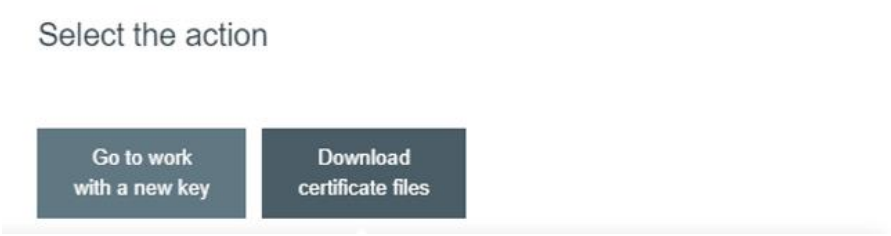


5. After the EDMS CA processing of the request sent by the user and creating a new CESVK based on the received request, the status of the Application will change to "Certificate issued".

Click the icon "Upload the archive to form the storeprofile".



6. In the new dialog box, click the button "Go to work with a new key" if a new working key was created on this PC. If a working key was created on a specialised computer designed to create cryptographic keys by the security administrator, you can click the button "Download certificate files" to transfer the CESVK to a specialised PC and configure the store profile on this PC in manual mode.



IMPORTANT! Each click on the button "Go to work with a new key" causes the formation of a new profile. The profile name is generated at the moment the button is clicked and has the following format: <Organisation name>_<User name>_YYYYMMdd_HHmmss.

7. To print an invoice for the creation of CESVK, click the icon "Download the invoice for the creation of a CESVK".

“Scheduled certificate replacement” Menu Item

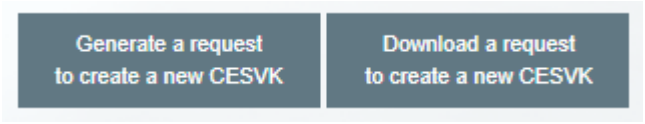
Using this menu item, you can create a new CESVK in case of a scheduled/unscheduled replacement of a valid certificate.

The page corresponding to this menu item displays all requests for the creation of a new CESVK (the “Requests”).

For each Request, a separate information line is displayed containing information about the owner of the created CESVK and the status of its processing.

CERTIFICATE OWNER	DATE OF RECEIVING THE APPLICATION TO THE CA	KEY TYPE	APPLICATION PROCESSING STATUS	
Caine Michael	07.09.2023	RSA	Certificate Issued	
Smith John	06.09.2023	RSA	Certificate Issued	

You can generate your new working key and a request to create CESVK directly on this PC. To do this, click the button “Generate a request to create a new CESVK”.



1. The screen will display a list of profiles that are configured in the Certificate Store on your PC. If the electronic signature key for the profile is valid, the icon will be displayed in the left column: “Generation of a new key and a request for the creation of a CESVK” . Click the icon .

2. Click the button “Submit request to CA”.

3. A new working key will be written to the key medium specified in the “CIPF Configuration Programme” (flash drive, ruToken, eToken, registry reader, etc.). The “default” media is a flash drive (removable disk reader). When generating a key, a dialogue box will be displayed for entering a password for the key. If you do not plan to additionally protect your key with a password, or plan to do so later, click “OK” without entering any information.

4. On the page with the list of Requests, a line for a new request will appear with the status “Request received. Processing in progress”.

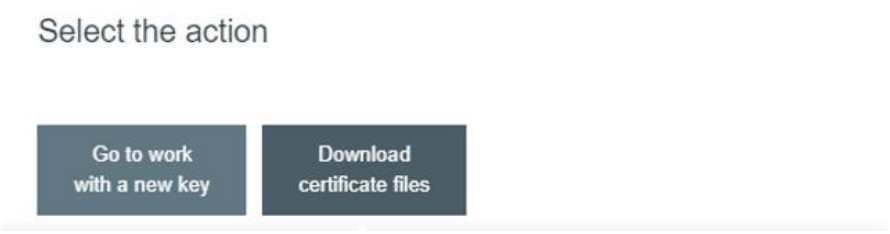
CERTIFICATE OWNER	DATE OF RECEIVING THE APPLICATION TO THE CA	KEY TYPE	APPLICATION PROCESSING STATUS
Caine Michael	07.09.2023	RSA	Request received. Processing in progress

5. After the EDMS CA processing of the request sent by the user and creating a new CESVK based on the received request, the status of the Request will change to “Certificate issued”. Click the icon “Download working certificate”.

CERTIFICATE OWNER	DATE OF RECEIVING THE APPLICATION TO THE CA	KEY TYPE	APPLICATION PROCESSING STATUS	
Caine Michael	07.09.2023	RSA	Certificate Issued	

When the status changes to “Request received. Processing is not possible”, you can see the reason for the refusal of the EDMS CA by placing the cursor on the icon with the sign “**?**”. For a detailed explanation of the reason for the refusal, you need to contact the EDMS CA.

6. In the new dialog box, click the button “Go to work with a new key” if a new working key was created on this PC. If a working key was created on a specialised computer designed to create cryptographic keys by the security administrator, you can click the button “Download certificate files” to transfer the CESVK to a specialised PC and configure the store profile in manual mode.



7. When you click the button “Go to work with a new key”, a list of profiles will appear. Click the icon for the profile where you want to install the new working certificate. A new dialogue box will display the result of the installation of new working certificate.

IMPORTANT! The installation of new working certificate does not remove the previous working certificate from the certificate store. If you need to return to the old certificate, you can do this using the “Certificate Store” programme by means of declaring the old certificate as working.

If this PC does not have software packages for working with qualified or non-qualified certificates (ASP “Validata Client” or “MOEX EDI Cryptoprotection”), while a dedicated security administrator is responsible for the creation of cryptographic keys in the organisation of the EDMS Participant, at the first stage click the button “Download a request to create a new CESVK” and download the request file generated by the security administrator on a specialised computer designed to create cryptographic keys.

8. To print an invoice for the creation of CESVK, click the icon “Download the invoice for the creation of a CESVK”.

"Changing certificate details" Menu Item

Using this menu item, you can create a new CESVK if you need to change the data specified in the certificate.

The cost of the service for creating such a certificate is lower than in the case of a scheduled/unscheduled replacement, but the expiration date of the electronic signature key, in this case, is set as the expiration date of the previous key.

On the page corresponding to this menu item, all requests for creating a new CESVK (Requests) are displayed.

For each Request, a separate information line is displayed containing the information on the owner of CESVK and the Request processing status.

To create a new CESVK with changed data, you need to:

1. Download on page https://www.moex.com/s1288 an Application form for the creation of CESVK, enter all relevant data, taking into account the intended changes, save the file to your hard drive. With the help of the "Certificate Store" programme, it is necessary to sign the generated file on the user's current working key (menu item "Service" – "ES installation", then "Attached signature"), select the saved file with the application, click "Next", specify "*Organisation name,* changing certificate details" as the file name, then check the box "Add certificate in the EP", click "Next" and "Done".

2. The generated file with the ".p7s" extension shall be sent as an attachment via electronic mail to the address pki@moex.com. Please indicate "*Name of the organisation,* _changing certificate details" in the subject line.

3. Generate/create your new secret key using the utilities **xpki1tst.exe** for GOST cryptography or **rpki1tst.exe** for RSA cryptography, which are located at "Command line utility for use in EDMS" at https://www.moex.com/a7978, in a ZIP archive in the **xml_req** folder.

These utilities allow you to create new keys for the user's electronic signature and encryption, as well as a request to create a CESVK in the form of an XML file.

Examples of running the utility

For GOST cryptography: 32bit:

xpki1tst.exe -manage -xmlreq -minimal -2012 >Request.xml or

64bit:

xpki1tstx64.exe -manage -xmlreq -minimal -2012 >Request.xml

As a result of the operation of the utility, the key of electronic signature and encryption will be written to the key medium specified in the "CIPF Configuration Programme" (flash drive, ruToken, eToken, etc.), and the request for the initial creation of the CESVK in the form of an XML file (Request.xml) – to the current store.

For RSA cryptography: 32bit:

rpki1tst.exe -manage -xmlreq -minimal >Request.xml

or 64bit:

rpki1tstx64.exe -manage -xmlreq -minimal >Request.xml

As a result of the operation of the utility, the key of electronic signature and encryption will be written to the catalogue C:\Users\.....\AppData\Roaming\Microsoft\Crypto\RSA and the request for the initial creation of the CESVK in the form of an XML file (Request.xml) – to the current store.

4. It is necessary to sign the request file (Request.xml) generated with the help of the utilities through the user's current working key using the "Certificate Store" programme (menu item "Service" – "ES installation", then "Attached signature"), select the saved request file, click "Next", specify "*Organisation name_c*hanging certificate details_request file" as the file name, then check the box "Add certificate in the EP", click "Next" and "Done".

5. The generated and signed request file with the ".p7s" extension shall be uploaded to the MP/IP using the button "Upload a request to create a new CESVK" in the "CA Services" section – "Changing certificate details".

6. Further procedure for working with Requests is identical to those specified in section "Scheduled certificate replacement" (see above).

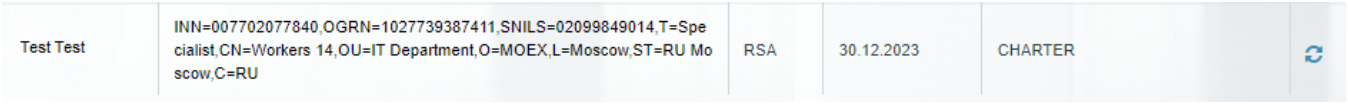
In the "Comments" field, you shall specify changes for the new certificate.

“Update of Certificates” Menu Item

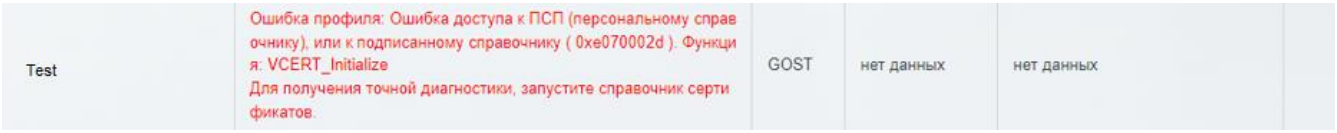
Using this menu item, you can update the certificates of employees of the Moscow Exchange Group and other EDMS Participants in the local certificate store of your PC.

The page corresponding to this menu item displays information about the profiles of the Certificate Store for this PC.

For each profile, its name and information on the working certificate are displayed. Updateable profiles have an icon “Update Profile Certificates”.



If the integrity of the profile is violated and/or the secret key of the electronic signature for the profile has expired, then the corresponding information will be displayed for the profile.



Click the icon , select the update option “Update counterparty certificates now”.

The update will be performed for the selected profile of your PC.

The “Upload counterparty certificates” option is designed to obtain the files necessary for updating with a view to their subsequent use when updating in the “Certificate Store” programme. Such an update can be performed both on this PC and on any other PC where the “Certificate Store” is installed and configured.

“List of Certificates” Menu Item

Using this menu item, you can get information on all the CESVK created by the EDMS CA for your organisation.

For each CESVK, the following information is displayed: CESVK owner, expiration date of the secret key, expiration date of the power of attorney for the CESVK owner, information on the scopes of CESVK.

CERTIFICATE OWNER	KEY IS VALID UNTIL	THE POWER OF ATTORNEY IS VALID UNTIL
Smith John	05.09.2024	06.09.2030

To the Attention of the Security Administrator of the EDMS Participant

The organisation of the EDMS Participant may implement a policy of centralised management of cryptographic keys. In this case, the cryptographic keys are created by the security administrator on a dedicated computer intended for the creation of cryptographic keys.

In case of centralised management of cryptographic keys, the computer through which the MP/IP is logged in may not have ASP "Validata Client" or "MOEX EDI Cryptoprotection" software packages installed.

For the initial generation of secret cryptographic keys, the security administrator shall use the **xpki1tst.exe** utility for GOST cryptography or the **rpki1tst.exe** utility for RSA cryptography, which are located at "Command line utility for use in EDMS" at https://www.moex.com/a7978, in a ZIP archive in the xml_req folder.

These utilities allow you to create keys for the user's electronic signature and encryption, as well as a request to initially create a CESVK in the form of an XML file. The request generated using the utility shall be loaded into the MP/IP.

Examples of running the utility

For GOST cryptography: 32bit:

xpki1tst.exe -manage -xmlreq -minimal -2012 >Request.xml or

64bit:

xpki1tstx64.exe -manage -xmlreq -minimal -2012 >Request.xml

As a result of the operation of the utility, the keys of electronic signature and encryption will be written to the key medium specified in the "CIPF Configuration Programme" (flash drive, ruToken, eToken, etc.), and the request for the initial creation of the CESVK in the form of an XML file (Request.xml) – to the current store.

For RSA cryptography:

32bit:

rpki1tst.exe -manage -xmlreq -minimal >Request.xml or

64bit:

rpki1tstx64.exe -manage -xmlreq -minimal >Request.xml

As a result of the operation of the utility, the keys of electronic signature and encryption will be written to the catalogue C:\Users\.....\AppData\Roaming\Microsoft\Crypto\RSA and the request for the initial creation of the CESVK in the form of an XML file (Request.xml) – to the current sore.

In case of scheduled/unscheduled replacement of certificates, the security administrator shall use the "Certificate Store" programme to generate new cryptographic keys.

After creating a new certificate in the EDMS CA, the security administrator may upload from the MP the files necessary for the creation of the local certificate store (user's working certificate, user's counterparty certificates, root certificates and lists of revoked certificates of the EDMS CA) and create a working profile for the user through the "Certificate Store" on the specific PC.