APPROVED
by Internal Order of AO Mizuho Bank (Moscow)
dated October 17, 2025 No. 100/25
President A.I. Malyshev

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 40601D00C99450EB8BEAF69867AF066C
Владелец: МАЛЫШЕВ АЛЕКСАНДР ИЛЬИЧ
Действителен: с 14.02.2025 до 14.12.2037

AO Mizuho Bank (Moscow)

Instruction on key primary generation and planned regeneration

Moscow, 2025

Contents

1. Primary generation of electronic signature key certificate 3
1.1. Primary generation to bank key medium RUTOKEN 3
1.2. Primary generation to Client's own key media (USB-flash) 6
1.3. Log in and completesignature key registration 10
2. Scheduled re-generation of electronic signature key certificate 12
2.1. Planned re-generation to bank key medium RUTOKEN 12
2.2. Planned re-generation to Client's own key media (USB-Flash) 16
2.3. Log in and complete abonent signature key registration 19

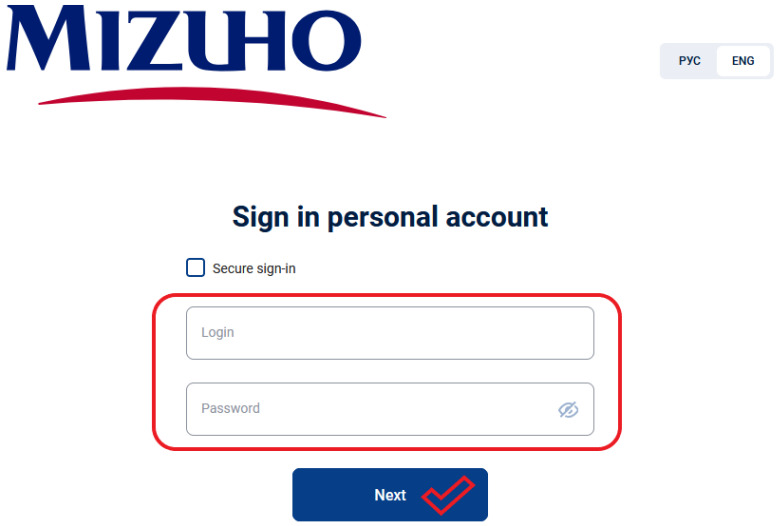
1. Primary generation of electronic signature key certificate

1.1. Primary generation to bank key medium RUTOKEN

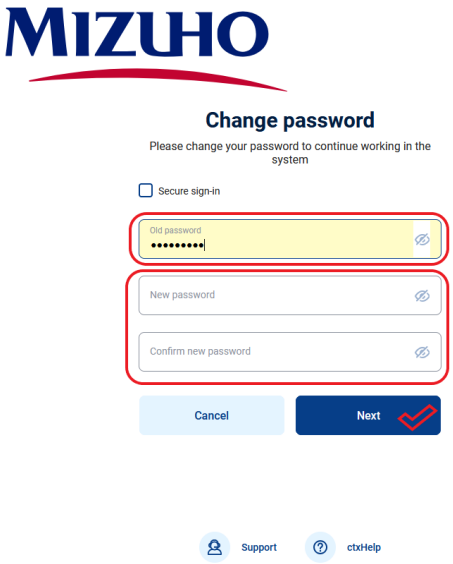
1) Install **RUTOKEN** key received in the Bank to the USB port of the computer

2) Open your browser Microsoft Edge/Google Chrome/Mozilla Firefox and click **https://online.mhcbr.ru/**

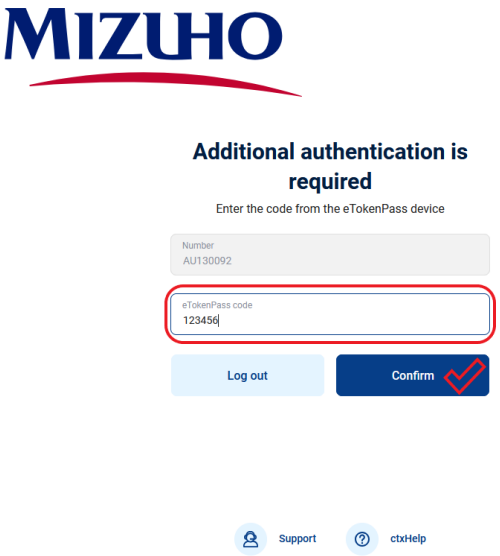
3) Enter the Login and Password, click **«Next»:**



4) A window with the need to change the password will be opened - enter **Old password (the original password provided by the Bank), New password and Confirm the new password,** then click **«Next»:**



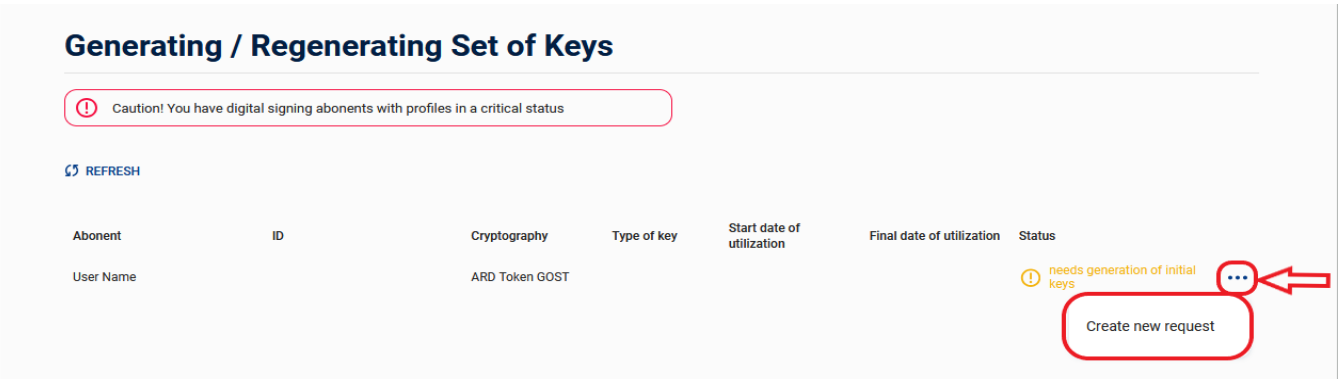
5) In case you use a stand-alone one-time password generator **eToken PASS**, an additional authentication window will appear. You must press the button once on the **eToken** device and enter the code generated by the device:



eToken PASS

ATTENTION! THIS DEVICE IS USED ONLY ONCE AT EACH LOGON. **IF THE BUTTON IS PRESSED REPEATEDLY, IT WILL BE OUT OF SYNC AND THE DEVICE WILL BE LOCKED!**

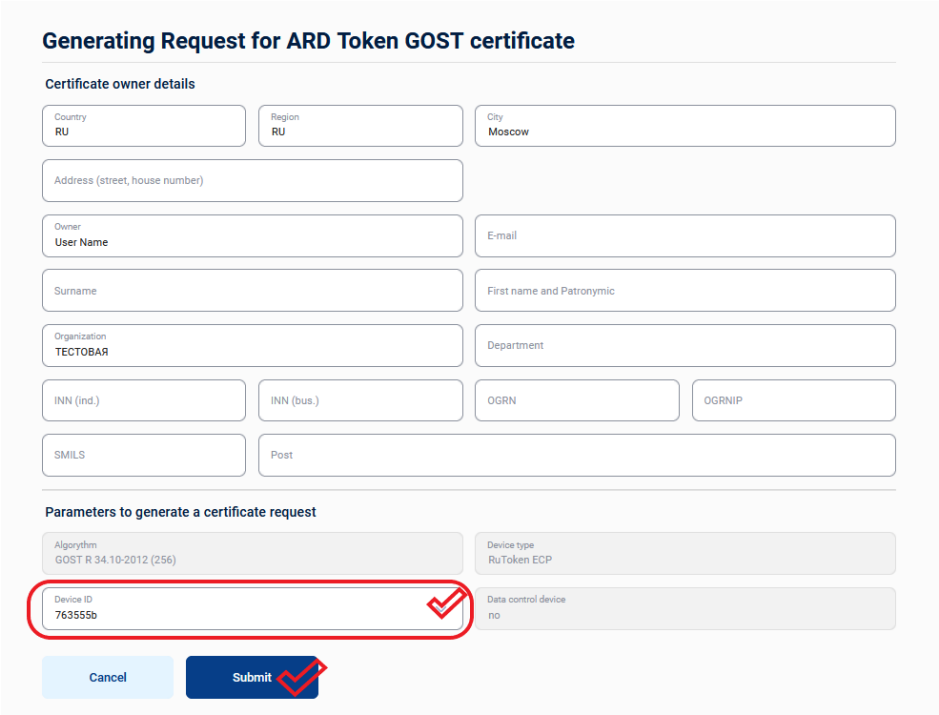
6) The information window for needs generation of intial keys, click **«…»**, select **«Create New Request»:**



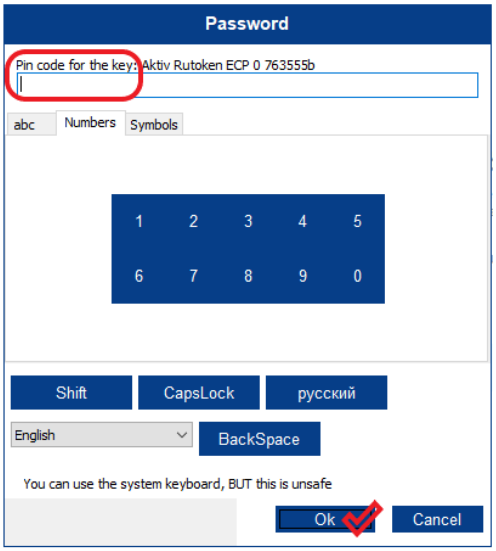
Attention! At this stage, the **received RUTOKEN** must be installed on the USB port**.**

RUTOKEN

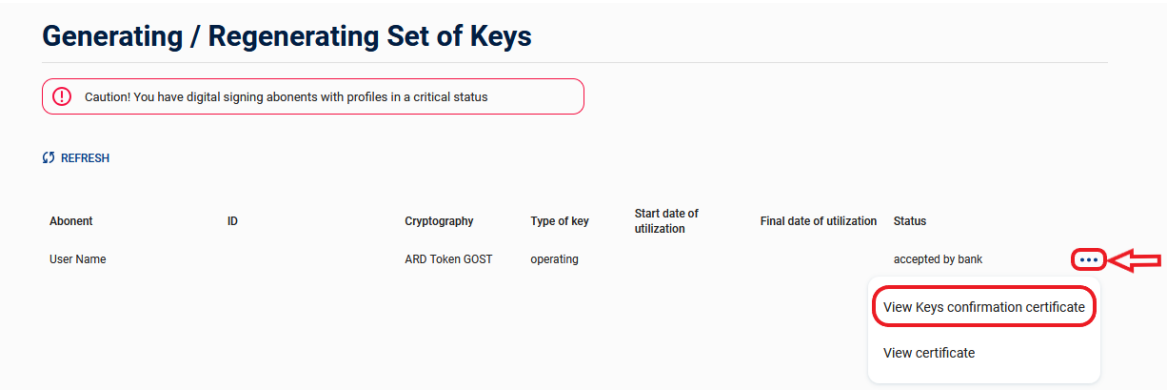
7) In the opened window click on "**Device ID**" and pull up the number of the key received in **the RUTOKEN Key** Bank, click **«Submit»:**



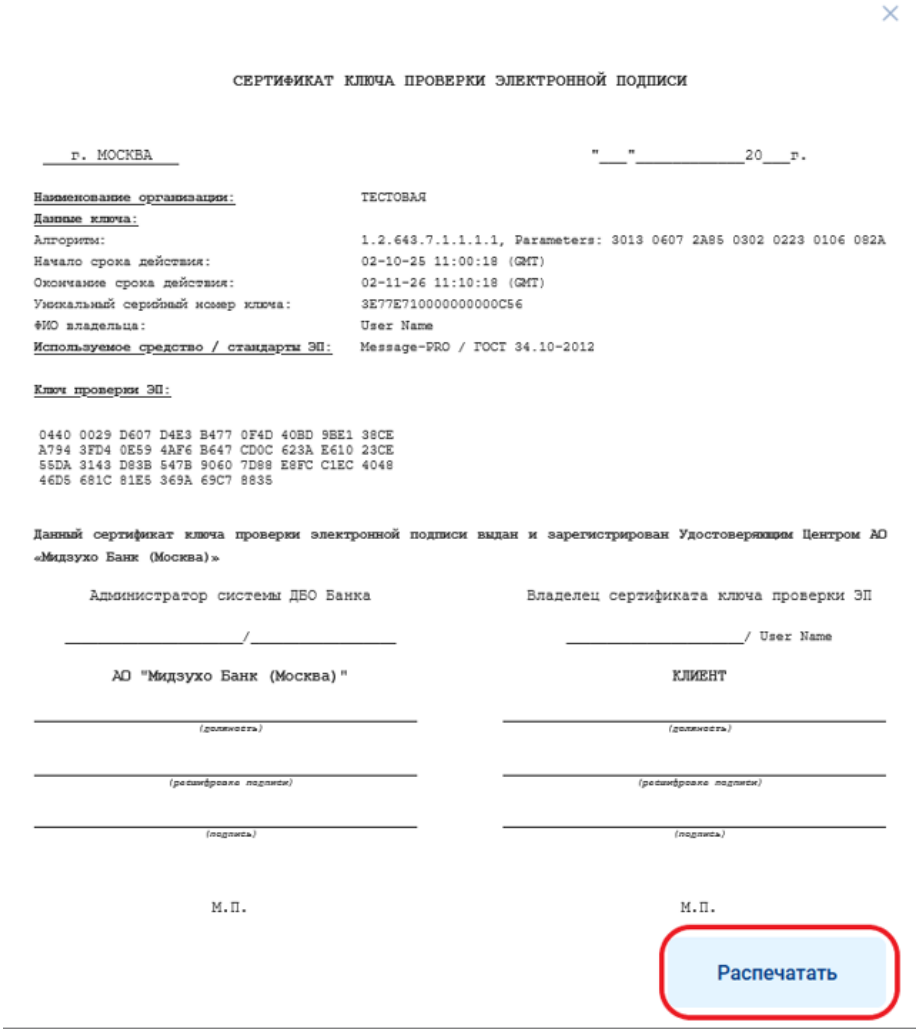
8) Next it's necessary to enter **the PIN CODE** code from **the RUTOKEN** key **(indicated on the password form,** then click **"Ok":**



9) The status key will change to 'Accepted by bank". Click **«...»** and select **«View Key Confirmation Certificate»:**



10) The Electronic Signature Key Certificate window opens, and select **«Print»:**



СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

г. МОСКВА "___"_____20___г.

Наименование организации:	ТЕСТОВАЯ
Данные ключа:	
Алгоритм:	1.2.643.7.1.1.1.1, Parameters: 3013 0607 2A85 0302 0223 0106 082A
Начало срока действия:	02-10-25 11:00:18 (GMT)
Окончание срока действия:	02-11-26 11:10:18 (GMT)
Уникальный серийный номер ключа:	3E77E710000000000C56
ФИО владельца:	User Name
Используемое средство / стандарты ЭП:	Message-PRO / ГОСТ 34.10-2012

Ключ проверки ЭП:

0440 0029 D607 D4E3 B477 0F4D 40BD 9BE1 38CE
A794 3FD4 0E59 4AF6 B647 CD0C 623A E610 23CE
55DA 3143 D83B 547B 9060 7D88 E8FC C1EC 4048
46D5 681C 81E5 369A 69C7 8835

Данный сертификат ключа проверки электронной подписи выдан и зарегистрирован Удостоверяющим Центром АО «Мидзухо Банк (Москва)»

Администратор системы ДБО Банка	Владелец сертификата ключа проверки ЭП
_____/_____	_____/ User Name
АО "Мидзухо Банк (Москва)"	КЛИЕНТ
_____ (должность)	_____ (должность)
_____ (расшифровка подписи)	_____ (расшифровка подписи)
_____ (подпись)	_____ (подпись)
М.П.	М.П.

Распечатать

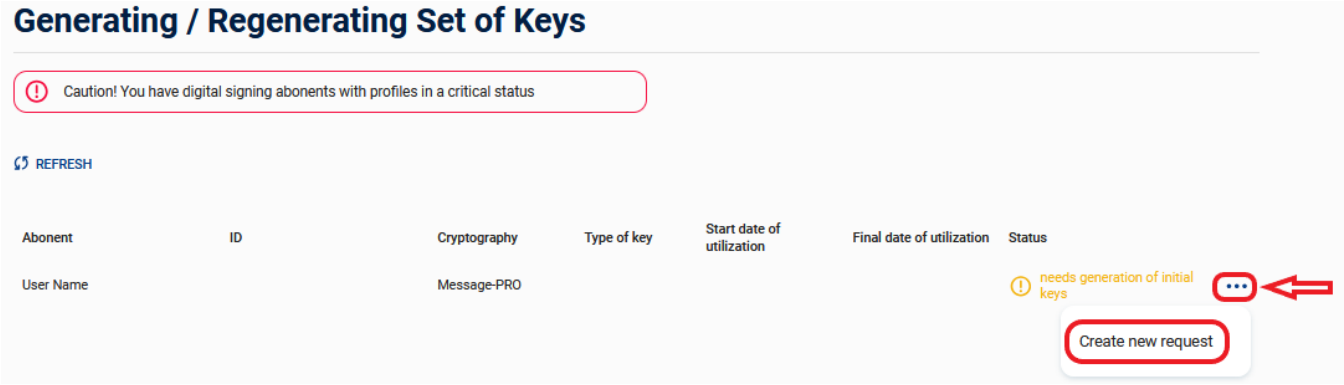
The Electronic Signature Verification Key Certificate Form shall be printed in duplicate, signed by the Key Owner, the Head of the Organization, or by an authorized person under the Power of Attorney, if applicable (all fields of the CLIENT unit shall be filled in: position, decryption, signature). The seal of the organization is printed, if any.

For compliance check of the signature and the seal to a sample in a card with samples of signatures, the signed scanned forms can be directed to mail of technical support of RBS *support@mhcb.ru*.

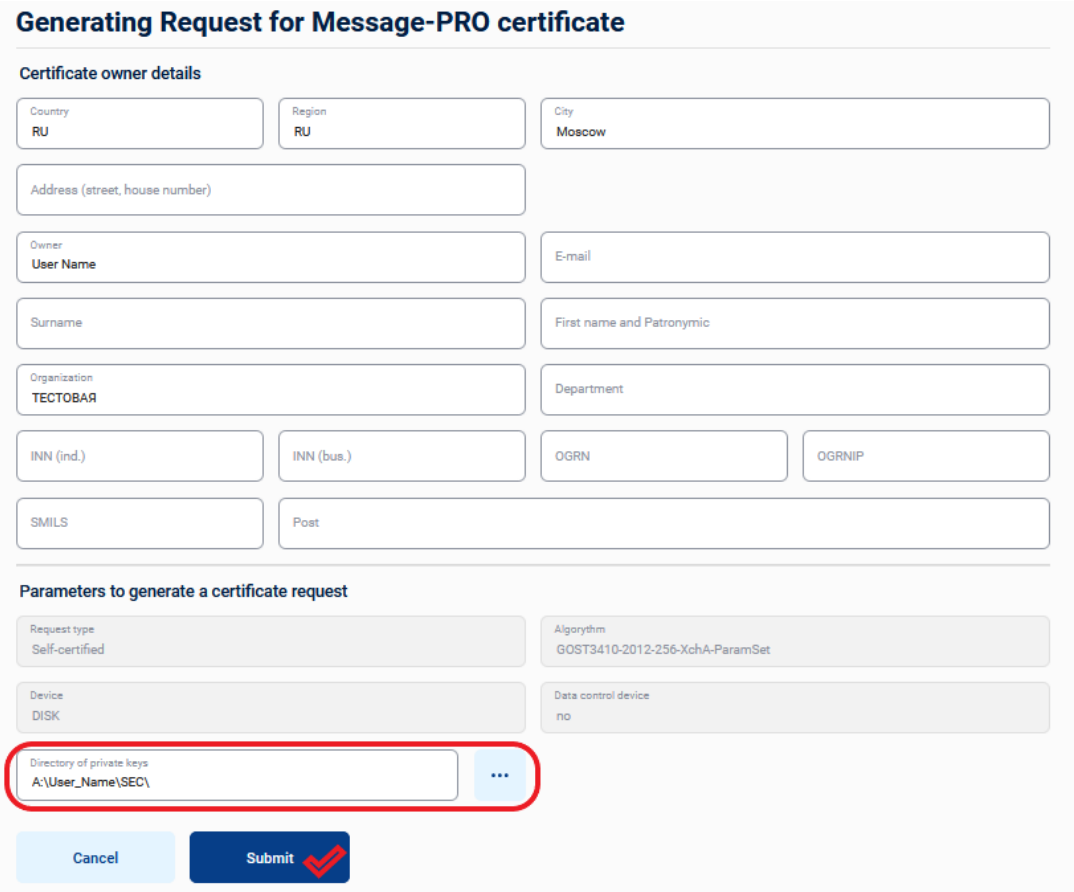
Signed forms must be submitted to the Bank for activation and granting access to the RBS.

1.2. Primary generation to Client's own key media (USB-flash)

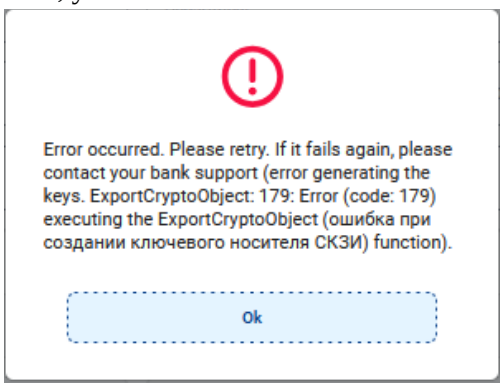
1) To record electronic keys to the **Client's own key storage media (USB-flash**) after authorization in the RBS with the Login and Password**,** click on **«...»** and select **«Create new request»:**



2) Specify the path to save the directory of private keys by changing the letter of drive A to the letter of the connected USB-flash (e.g. F:\) and click **Submit:**



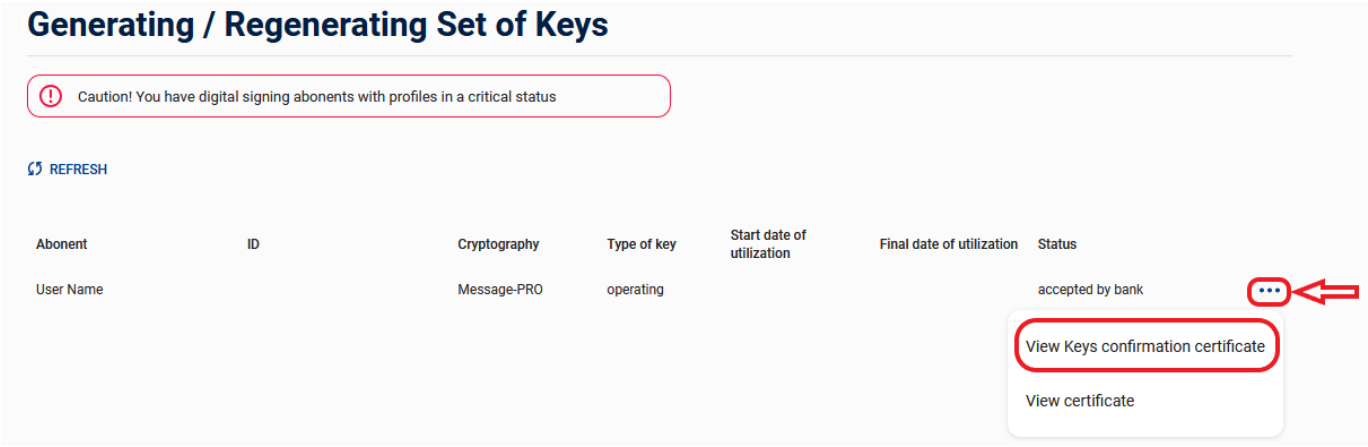
! If you do not change the drive letter, you will see this error:



Click "..." and specify the path to save the secret key directory of the USB-flash key media you are using (e.g. F :\or other), then click **Submit.**

If the biological sensor displays random numbers, press the orange circles to initialize it until the indicator bar is 100% full.

3) The status of the key will change to “Accepted by bank”. Click **«...»** and select **«View Keys Confirmation Certificate»:**



4) «The Electronic Signature Key Certificate» window opens, and select **«Print»:**

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

г. МОСКВА "___"_____20___г.

Наименование организации:	ТЕСТОВАЯ
Данные ключа:	
Алгоритм:	1.2.643.7.1.1.1.1, Parameters: 3013 0607 2A85 0302 0223 0106 082A
Начало срока действия:	02-10-25 11:00:18 (GMT)
Окончание срока действия:	02-11-26 11:10:18 (GMT)
Уникальный серийный номер ключа:	3E77E710000000000C56
ФИО владельца:	User Name
Используемое средство / стандарты ЭП:	Message-PRO / ГОСТ 34.10-2012

Ключ проверки ЭП:

0440 0029 D607 D4E3 B477 0F4D 40BD 9BE1 38CE
A794 3FD4 0E59 4AF6 B647 CD0C 623A E610 23CE
55DA 3143 D83B 547B 9060 7D88 E8FC C1EC 4048
46D5 681C 81E5 369A 69C7 8835

Данный сертификат ключа проверки электронной подписи выдан и зарегистрирован Удостоверяющим Центром АО «Мидзухо Банк (Москва)»

Администратор системы ДБО Банка	Владелец сертификата ключа проверки ЭП
_____/_____	_____/ User Name
АО "Мидзухо Банк (Москва)"	КЛИЕНТ
_____ (должность)	_____ (должность)
_____ (расшифровка подписи)	_____ (расшифровка подписи)
_____ (подпись)	_____ (подпись)
М.П.	М.П.

Распечатать

The Electronic Signature Verification Key Certificate Form shall be printed in duplicate, signed by the key owner and the Head of the Organization, or by an authorized person under the Power of Attorney, if applicable (all fields of the CLIENT unit shall be filled in: position, decryption, signature). The seal of the organization is printed, if any.

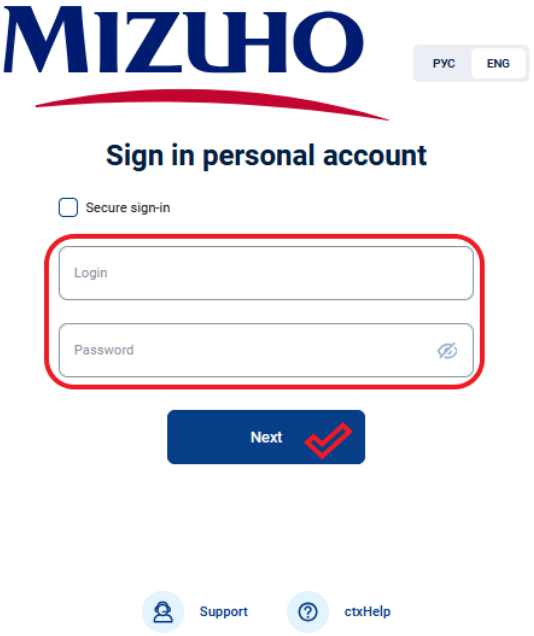
For check of compliance of the sign and seal to a sample in a card with samples of signatures, the signed scanned forms can be directed to mail of technical support of RBS *support@mhcb.ru*.

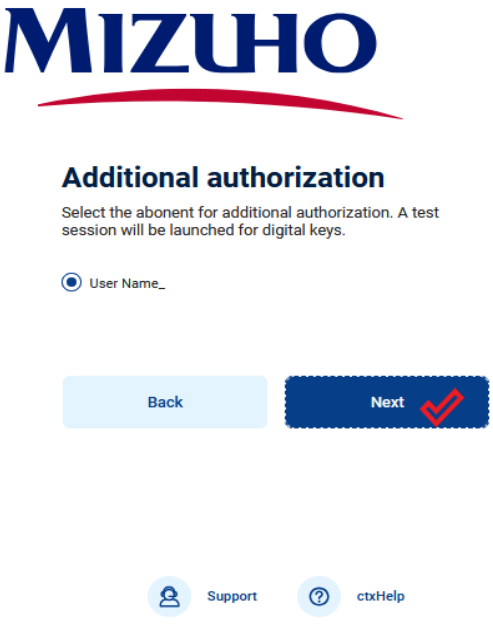
5) Signed forms must be submitted to the Bank for activation and granting access to the RBS.

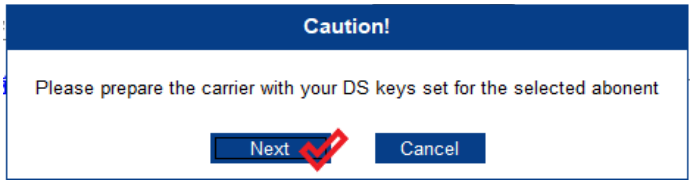
1.3. Log in and signature key registration completion

1) The administrator of the Bank's RBS, having received the originals of the Electronic Signature Public Key Certificates forms, completes the registration of the new abonent key.

2) Log in with Login and Password, click **«Next»:**



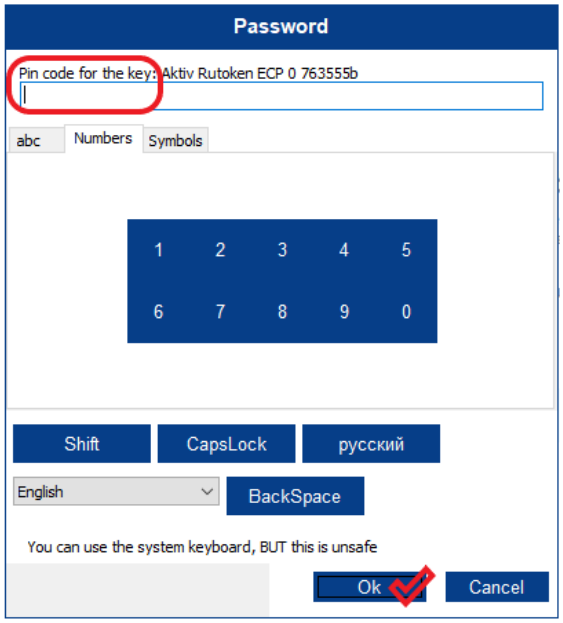




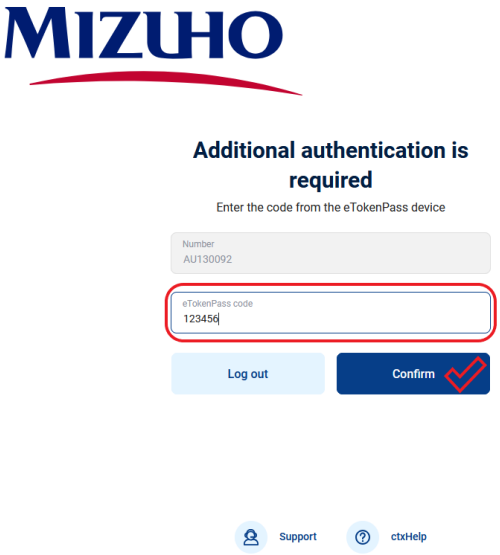
At this stage, the **RUTOKEN** or other key media received from the Bank must be installed.

3) Enter the **PIN CODE** from the RUTOKEN key received from the Bank (indicated on the password form):

IMPORTANT! PIN CODE-CODE IS INDICATED <u>ON THE PASSWORD FORM!</u>



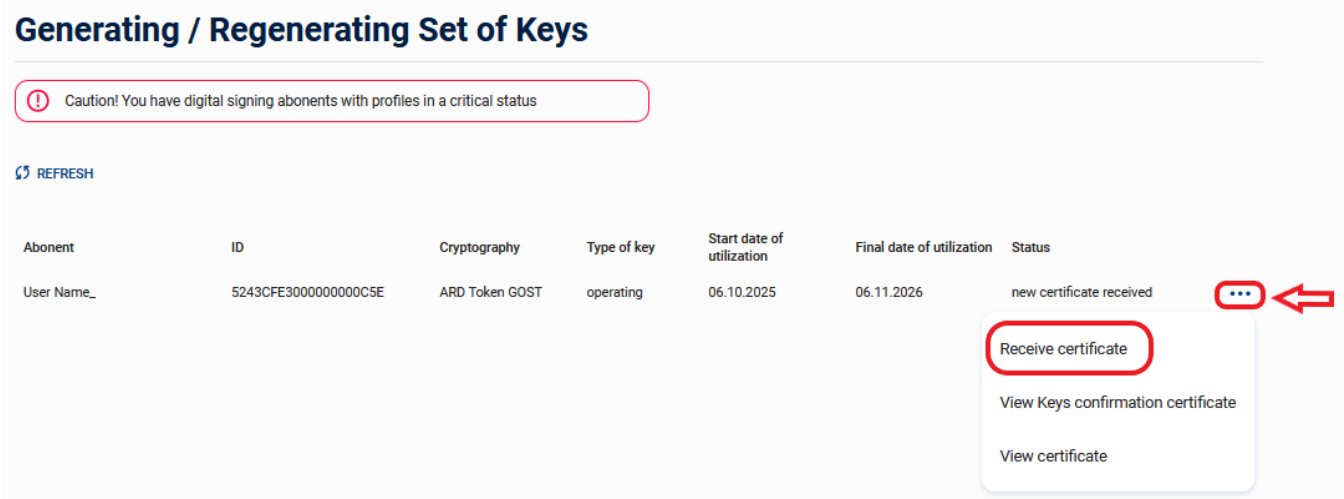
4) In case you use a stand-alone one-time password generator **eToken PASS**, you must press the button on the device **<u>once</u>** and enter the code generated by the device:



eToken PASS

ATTENTION! THIS DEVICE IS USED ONLY ONCE AT EACH LOGON. **IF THE BUTTON IS PRESSED REPEATEDLY, IT WILL BE OUT OF SYNC AND THE DEVICE WILL BE LOCKED!**

5) The key status will change to «New Certificate Received». Click **«…»** and select **«Receive Certificate»:**



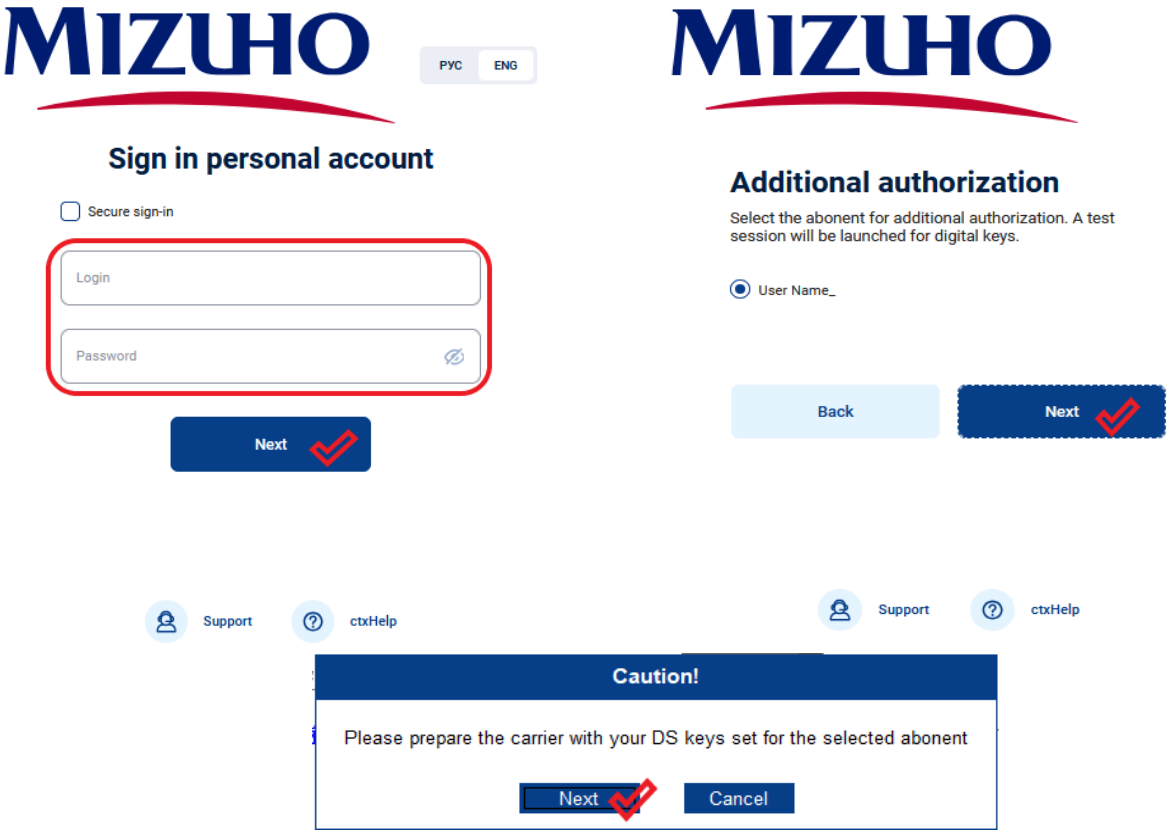
The procedure for generating keys on this is completed, and you can start working in RBS.

2. Scheduled regeneration of electronic signature key certificate

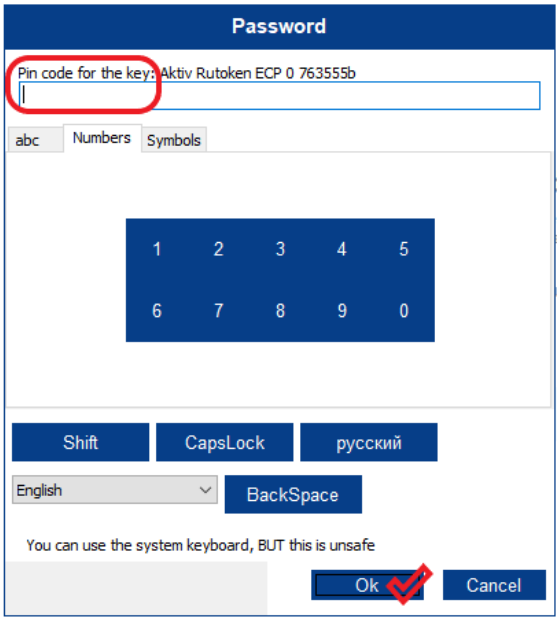
2.1. Planned regeneration to bank key medium RUTOKEN

1) Open your browser Microsoft Edge/Google Chrome/Mozilla Firefox and go to **https://online.mhcbr.ru**

2) Install the **key RUTOKEN media** received in the bank into the USB port of the computer, login to the system using the Login and Password, click **«Next»:**

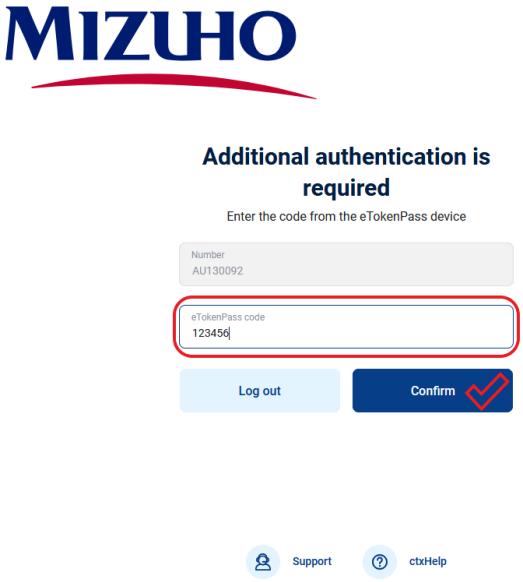


3) Enter **PIN CODE** from RUTOKEN key **(specified on the password form):**



Click **«Ok».**

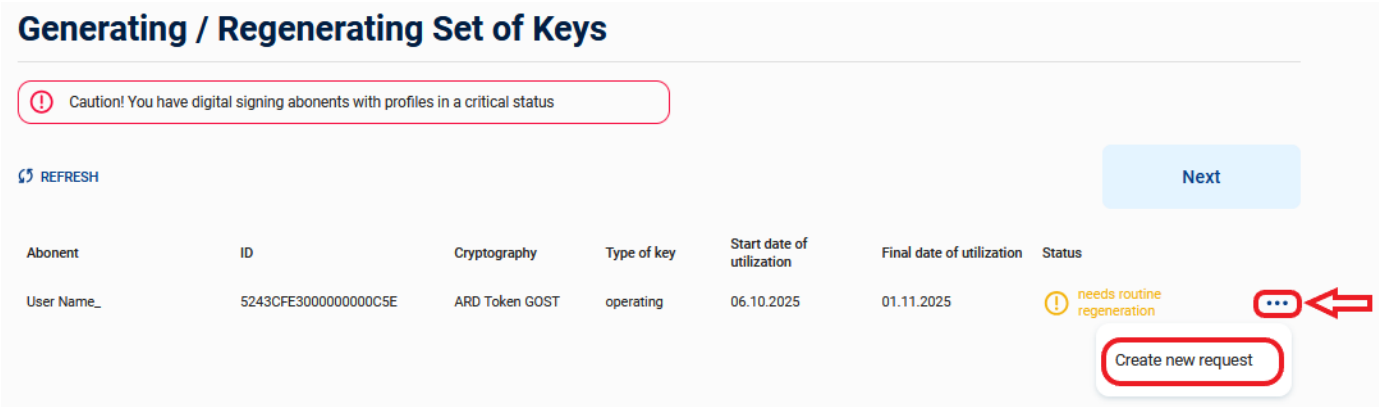
4) If you use a stand-alone one-time password generator **eToken PASS**, an additional authentication window will appear. You must press the button once on the **eToken** device and enter the code generated by the device:



eToken PASS

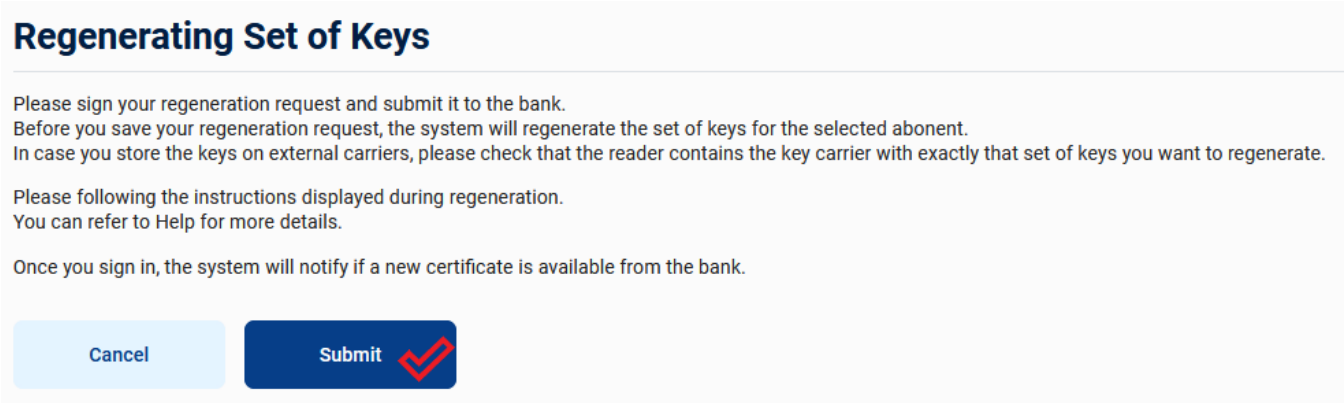
ATTENTION! THIS DEVICE IS USED ONLY ONCE AT EACH LOGON. **IF THE BUTTON IS PRESSED REPEATEDLY, IT WILL BE OUT OF SYNC AND THE DEVICE WILL BE LOCKED!**

5) The information window about the need to perform Planned key re-generation opens, click on **«…»** and select **«Create new request»:**

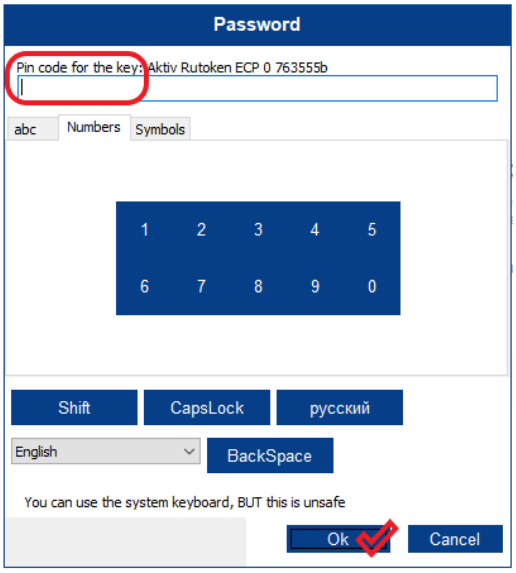


Important! If you click Next or want to generate an electronic signature key certificate on an unscheduled basis, you can do so from the **User Profile-Security-Generate/ReGenerate Key Set** menu**.**

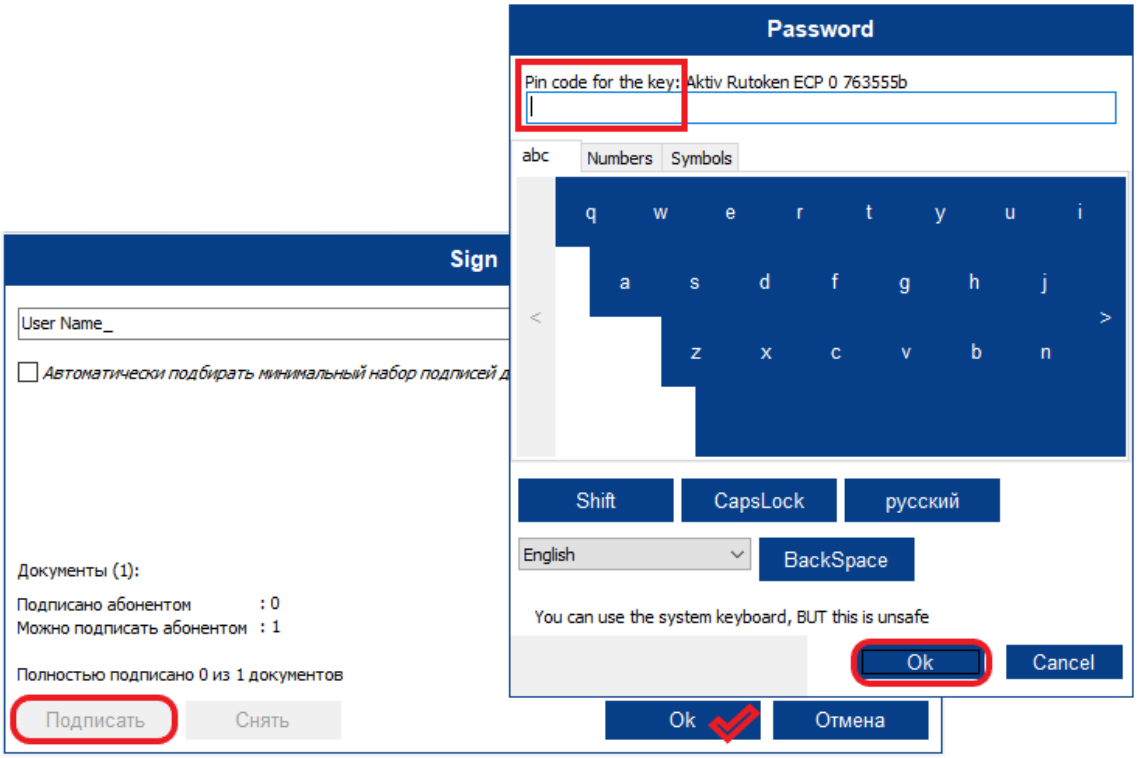
6) The «Regenerate Set of Keys» window opens, and click **«Submit»:**



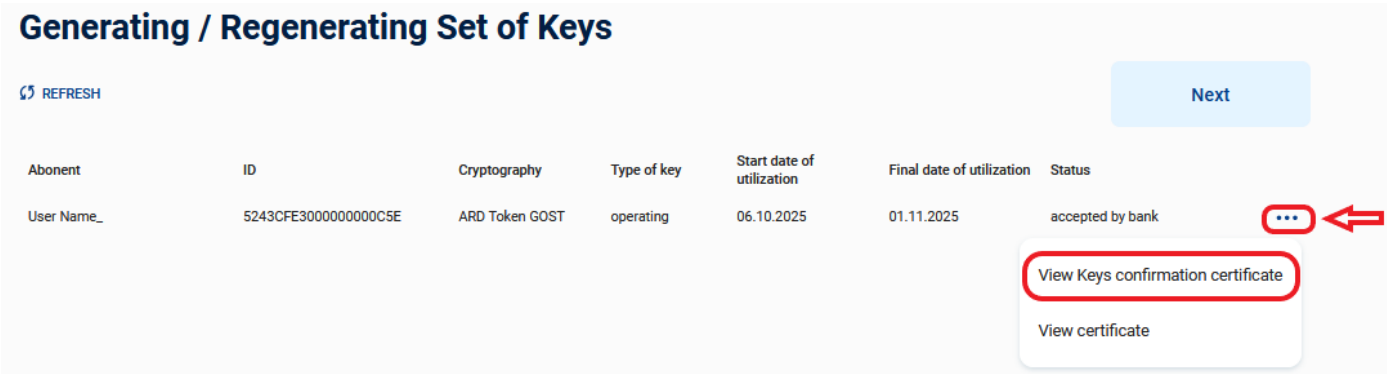
7) Enter **PIN CODE** from RUTOKEN key (specified on the password form), "**OK**"



8) Press «**Sign**» button, re-enter **PIN CODE** from RUTOKEN key, then "**Ok**"**Ok.**"



9) The status of the key will be changed to 'Accepted by bank'. Click **«…»**, select **View Key Confirmation Certificate:**



10) The «Electronic Signature Key Certificate» window opens, and select **«Print»:**

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

г. МОСКВА "___"_____20___г.

Наименование организации:	ТЕСТОВАЯ
Данные ключа:	
Алгоритм:	1.2.643.7.1.1.1.1, Parameters: 3013 0607 2A85 0302 0223 0106 082A
Начало срока действия:	02-10-25 11:00:18 (GMT)
Окончание срока действия:	02-11-26 11:10:18 (GMT)
Уникальный серийный номер ключа:	3E77E710000000000C56
ФИО владельца:	User Name
Используемое средство / стандарты ЭП:	Message-PRO / ГОСТ 34.10-2012

Ключ проверки ЭП:

0440 0029 D607 D4E3 B477 0F4D 40BD 9BE1 38CE
A794 3FD4 0E59 4AF6 B647 CD0C 623A E610 23CE
55DA 3143 D83B 547B 9060 7D88 E8FC C1EC 4048
46D5 681C 81E5 369A 69C7 8835

Данный сертификат ключа проверки электронной подписи выдан и зарегистрирован Удостоверяющим Центром АО «Мидзухо Банк (Москва)»

Администратор системы ДБО Банка	Владелец сертификата ключа проверки ЭП
_____/_____	_____/ User Name
АО "Мидзухо Банк (Москва)"	КЛИЕНТ
_____ (должность)	_____ (должность)
_____ (расшифровка подписи)	_____ (расшифровка подписи)
_____ (подпись)	_____ (подпись)
М.П.	М.П.

Распечатать

The Electronic Signature Verification Key Certificate Form shall be printed in duplicate, signed by the key owner and the Head of the Organization, or by an authorized person under the Power of Attorney, if applicable (all fields of the CLIENT unit shall be filled in: position, decryption, signature). The press of the organization is printed, if any.

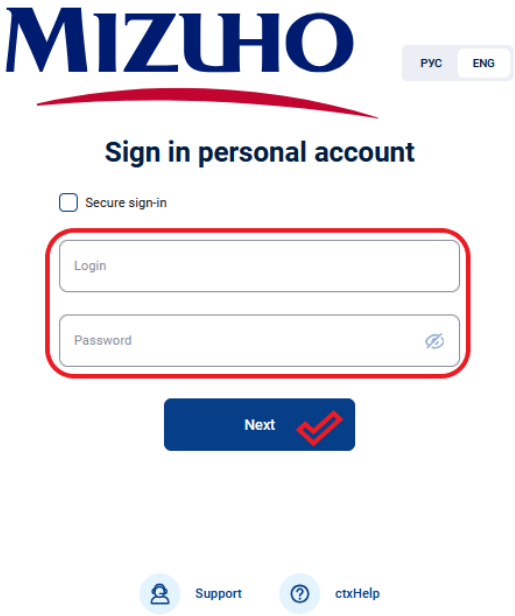
For check of compliance of the sign and seal to a sample in a card with samples of signatures, the signed scanned forms can be directed to mail of technical support of RBS *support@mhcb.ru*.

11) Signed forms must be submitted to the Bank for activation and granting access to the RBS.

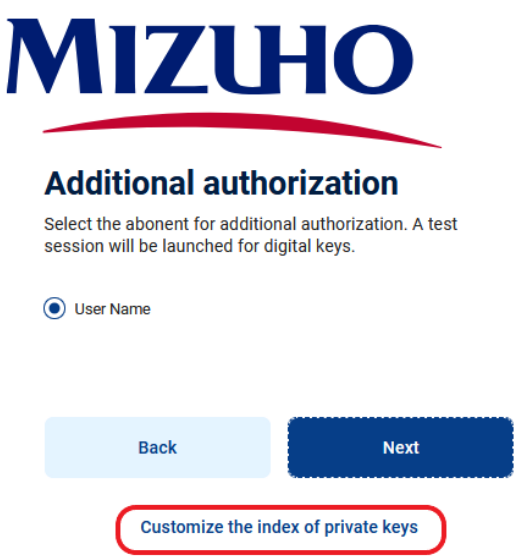
2.2. Planned regeneration to Client's own key media (USB-Flash)

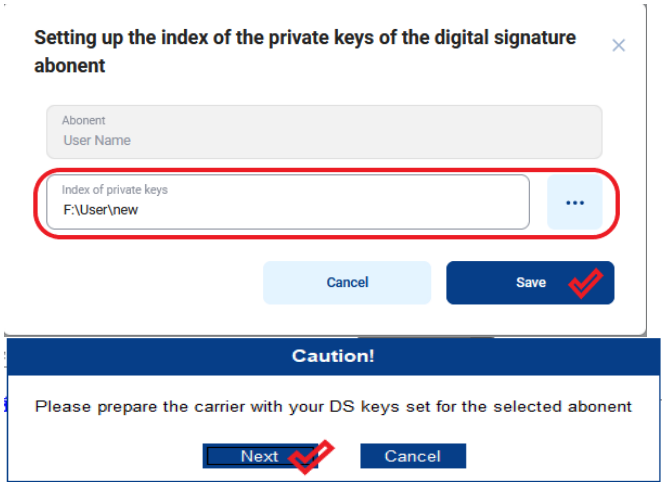
1) Open Microsoft Edge/Google Chrome/Mozilla Firefox and go to https://online.mhcbr.ru

2) Install your own USB-Flash key media into the USB port of your computer and log in using Login and Password, click **«Next»:**



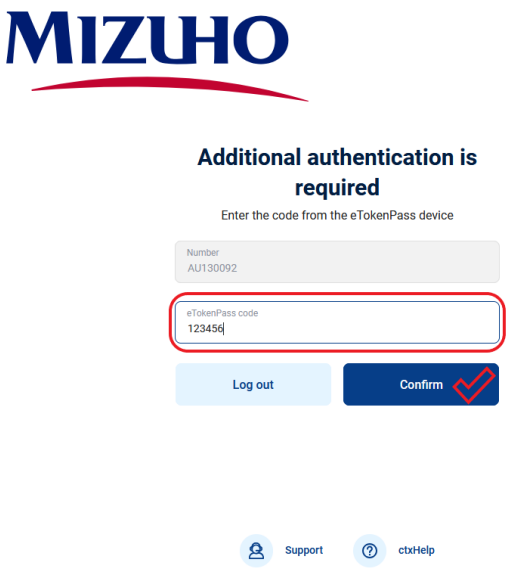
3) Then **Set up the directory of private keys** and specify the path where the electronic keys are stored on the connected **USB-flash** in line "directory of secret keys":





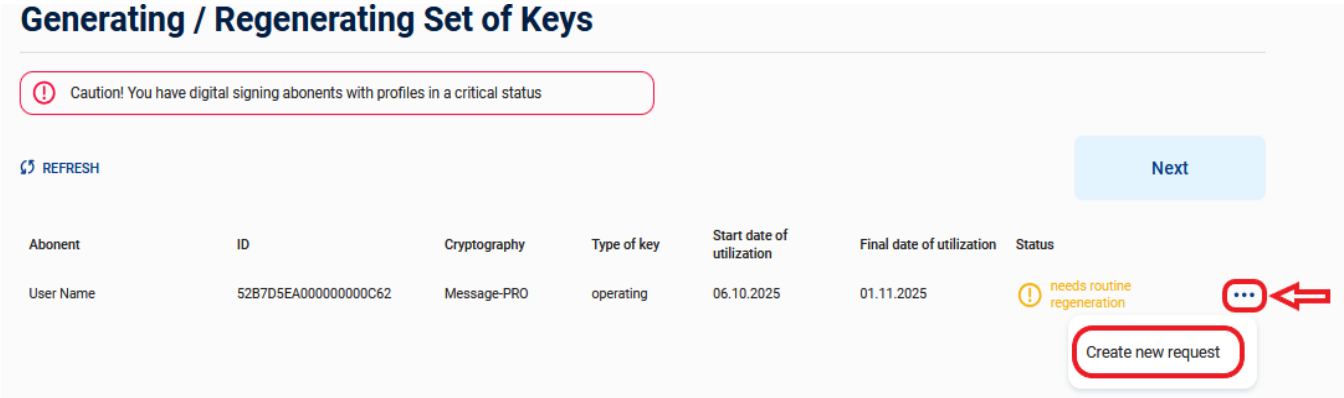
Click **«Save», «Next»,**

4) In case you use a stand-alone one-time password generator **eToken PASS**, an additional authentication window appears. You must press the button once on the **eToken** PASS device and enter the code generated by the device:



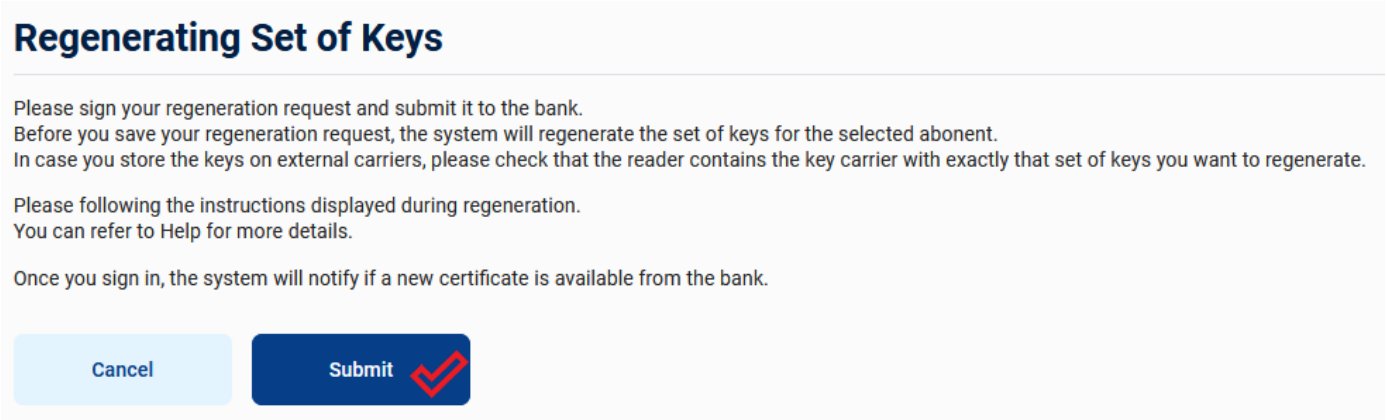
eToken PASS

5) Opens the information window about whether to perform a Planned Key Re-Generation. Click **«…»** and select **«Create New Request»:**

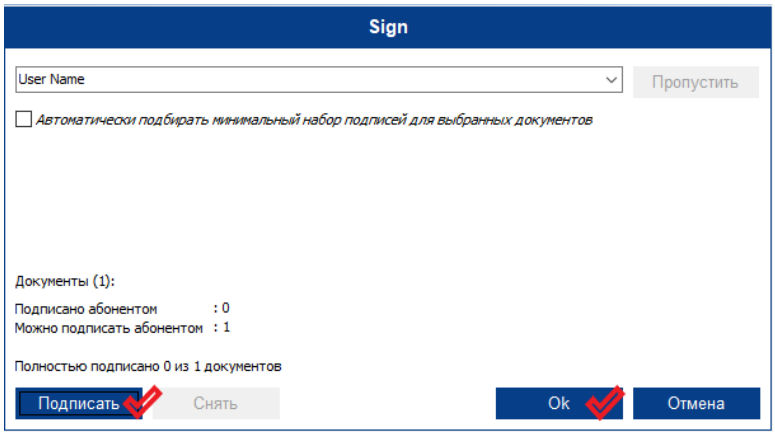


Important! If you click Next or want to generate an electronic signature key certificate on an unscheduled basis, you can do so from the **User Profile-Security-Generate/ReGenerate Key Set** menu**.**

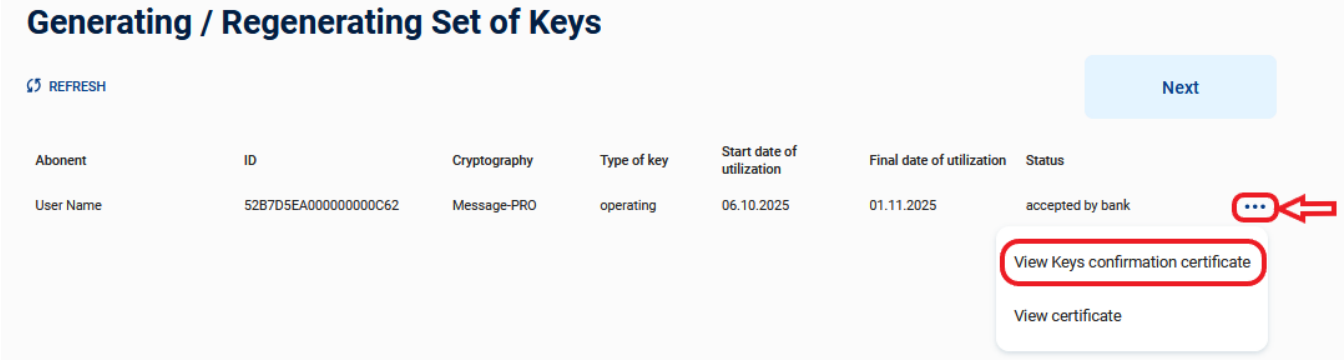
6) The «Regenerate Set of Keys» window opens, and click **«Submit»:**



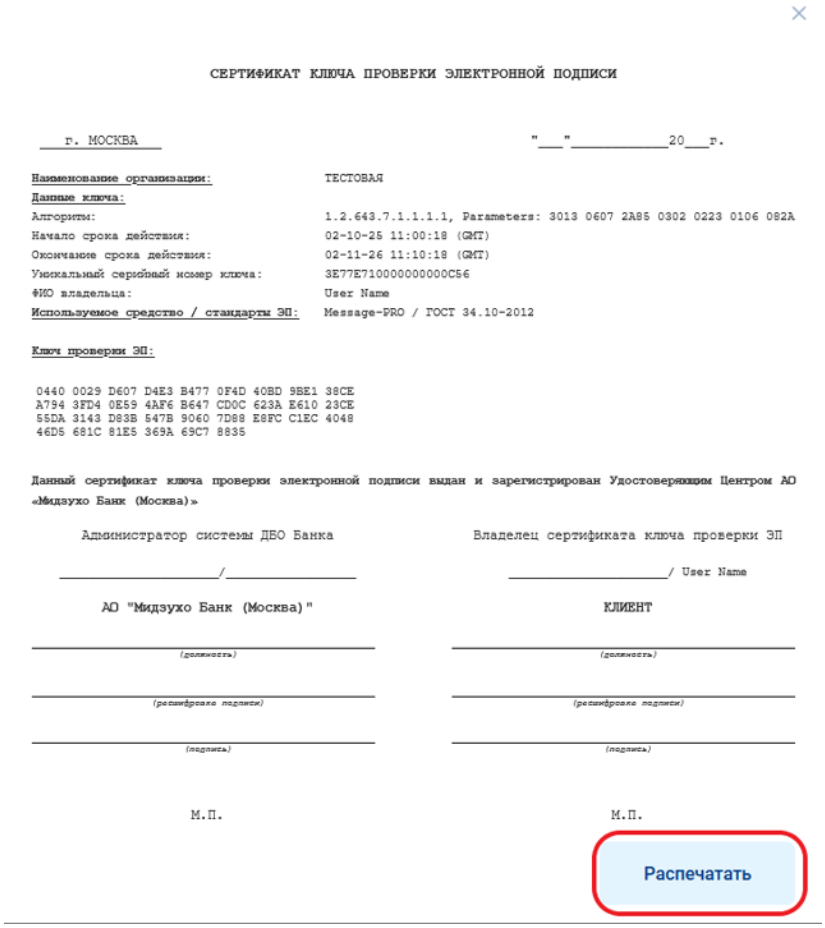
7) Click «**Sign»,** then **click «Ok».**



8) The status of the key will be changed to "Accepted by bank". Click **«...»** and select **«View Keys Confirmation Certificate»:**



9) The «Electronic Signature Key Certificate» window opens, and select **«Print»:**



СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

г. МОСКВА "___"_____20___г.

Наименование организации: ТЕСТОВАЯ
Данные ключа:
Алгоритм: 1.2.643.7.1.1.1.1, Parameters: 3013 0607 2A85 0302 0223 0106 082A
Начало срока действия: 02-10-25 11:00:18 (GMT)
Окончание срока действия: 02-11-26 11:10:18 (GMT)
Уникальный серийный номер ключа: 3E77E710000000000C56
ФИО владельца: User Name
Используемое средство / стандарты ЭП: Message-PRO / ГОСТ 34.10-2012

Ключ проверки ЭП:

0440 0029 D607 D4E3 B477 0F4D 40BD 9BE1 38CE
A794 3FD4 0E59 4AF6 B647 CD0C 623A E610 23CE
55DA 3143 D83B 547B 9060 7D88 E8FC C1EC 4048
46D5 681C 81E5 369A 69C7 8835

Данный сертификат ключа проверки электронной подписи выдан и зарегистрирован Удостоверяющим Центром АО «Мидзухо Банк (Москва)»

Администратор системы ДБО Банка
_____/_____
АО "Мидзухо Банк (Москва)"
_____ (должность)
_____ (расшифровка подписи)
_____ (подпись)
М.П.

Владелец сертификата ключа проверки ЭП
_____/ User Name
КЛИЕНТ
_____ (должность)
_____ (расшифровка подписи)
_____ (подпись)
М.П.

Распечатать

The Electronic Signature Verification Key Certificate Form shall be printed in duplicate, signed by the key owner and the Head of the Organization, or by an authorized person under the Power of Attorney, if applicable (all fields of the CLIENT unit shall be filled in: position, decryption, signature). The press of the organization is printed, if any.

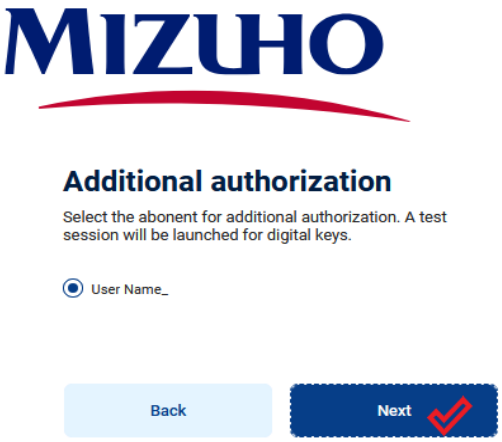
For check of compliance of the sign and seal to a sample in a card with samples of signatures, the signed scanned forms can be directed to mail of technical support of RBS *support@mhcb.ru*.

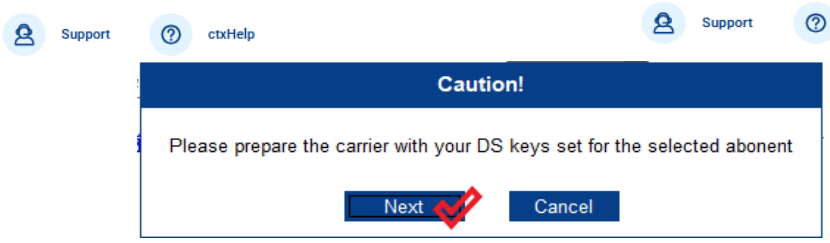
10) Signed forms must be submitted to the Bank for activation and granting access to the RBS.

2.3. Log in and complete abonent signature key registration

1) The administrator of the Bank's RBS, having received the originals of the Electronic Signature Public Key Certificates forms, completes registration of the abonent's key certificate.

2) Log in with Login and Password, click **«Next»:**

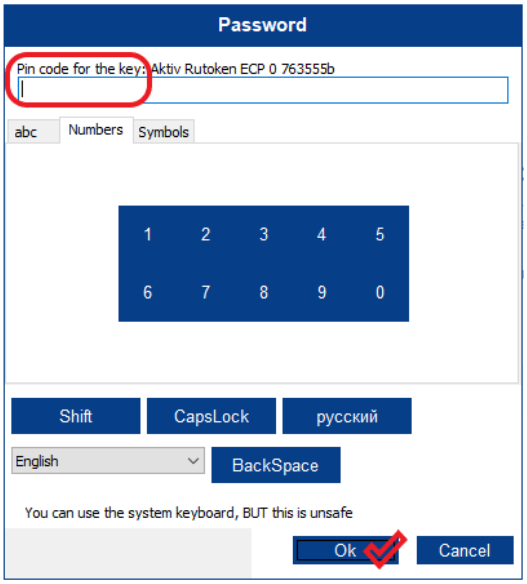




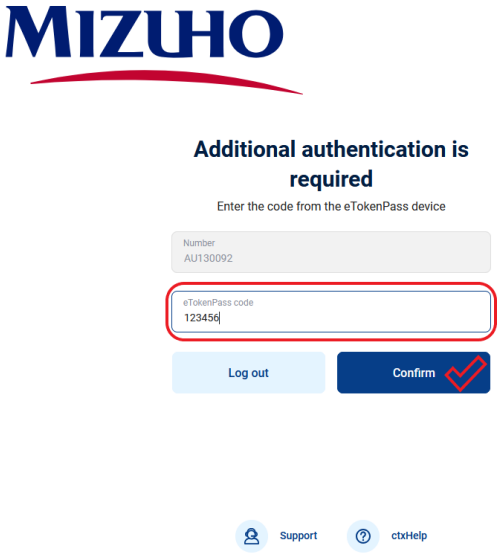
At this stage, the **RUTOKEN** or other key media received from the Bank must be installed.

RUTOKEN

3) Enter the **PIN CODE** of the RUTOKEN key received from the Bank (specified on the password form):



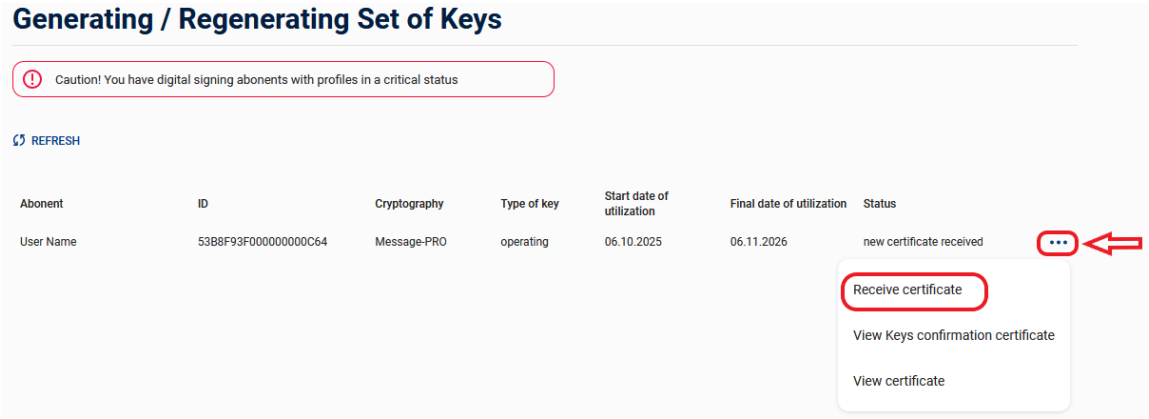
4) In case you use a stand-alone one-time password generator **eToken PASS**, you must press the button on the device **once** and enter the code generated by the device:



eToken PASS

ATTENTION! THIS DEVICE IS USED ONLY ONCE AT EACH LOGON. **IF THE BUTTON IS PRESSED REPEATEDLY, IT WILL BE OUT OF SYNC AND THE DEVICE WILL BE LOCKED!**

5) The key status will change to "New Certificate Received". Click **«…»** and select **«Receive Certificate»:**



The procedure for generating keys on this is completed, and you can start working in RBS.