User manual

registration of a new client in the Internet version of Raiffeisen Business Online system

(for legal entities)

Raiffeisen Business Online support service (Mon-Fri 8:00-22:00, Sat-Sun 8:00-20:00) clientbank.support@raiffeisen.ua	Calls from abroad	Support service for foreign currency transactions (Mon-Fri 9:00-18:00)
0 800 505 770 **0 800 400 470** **+ 38 (044) 495 41 40** (in Kyiv and from abroad)	**+38 (044) 230 99 98** (acc. to tariffs of provider)	**0 800 400 425** **0 800 500 025** **+38 (044) 299 10 99** (in Kyiv and from abroad)

Ukraine, 01011, 4a Generala Almazova St., Kyiv, Ukraine https://raiffeisen.ua/

CONTENTS

1. INTRODUCTION 2
1.1. Features of the generation and registration of ES keys 2
1.2. Use of file and hardware storages for storing ES keys 3
2. Registration in the system with the generation of an advanced ES key 3
2.6.1. Generation of an advanced electronic signature key for an Accountant "without signature rights" 6
2.8. Activation of the advanced ES key 9
2.8.1. If the ES key "with signature rights" is generated in the name of the Authorized person with the first signature level: 10
2.8.2. If the ES key "with signature rights" is generated in the name of an Authorized person with the second or other signature level: 10
2.8.3. If the ES key "without signature rights" is generated: 11
3. Registration in the system using the existing qualified ES key 11
4. Service messages 17

1. INTRODUCTION

This instruction regulates the procedure for registration in the Raiffeisen Business Online System (hereinafter – the System or RBO).

Working with the System is available in the following web browsers:

- Microsoft Edge of the latest current version,
- Mozilla FireFox 15.0 and higher,
- Opera 15.0 and higher,
- Safari 6.0 and higher,
- Google Chrome 29.0 and higher.

Before registering in the system, you must configure your browser so that you can choose a location to save files before downloading them and **make sure** you disabled saving logins and passwords in the browser.

1.1. Features of the generation and registration of electronic signature keys

There are two ways to register:

a) registration in the system using the **advanced electronic signature key** generated by the system during registration (advanced ES /bank's ES key);
b) registration using an existing **qualified electronic signature key** (qualified ES/QES key).

Please note! For the advanced electronic signature keys (bank's ES key) the validity period is 24 months.

The list of qualified electronic trust service providers whose QES keys are supported by the system is available for review on the bank's website at https://raiffeisen.ua/uk/aem/biznesu/onlain-servisy/raiffeisen-business-online.html#faq, in the section of the page:

- useful information / instructions and training materials for the web-version.

Please note! Before registering a qualified electronic signature key, make sure that such key meets the requirements of the system:

- QES keys issued to an individual or individual entrepreneur or self-employed person (NOT to an authorized person of the company) are automatically rejected by the System when you try to register with such a QES key,

- QES keys of the "electronic seal" type (NOT "electronic signature") are rejected by the system automatically when trying to register with such a QES key.

1.2. Use of file and hardware storages for storing ES keys

There are two ways to store AES/QES keys. When registering and generating a new AES/QES key, such a key can be saved:

- in the file storage,
- in hardware storage.

Attention! The system Internet-version and Mobile application support the use of hardware storages of the following types:

Channel	Hardware storage name	Manufacturer	Manufacturer's official website	Additional information
WEB	**"Crystal-1"** ("IIT E.key Crystal -1")	**IIT JSC** (Institute of Informational Technologies JSC)	https://iit.com.ua/	USB-device, in a plastic or a metal case
	"Almaz-1K" ("IIT E.key Almaz-1K")			
Mobile + WEB	**"Almaz-1K"** ("IIT E.key Almaz-1K") (Bluetooth-device)			• A plastic keychain, • User's device should support the wireless interface Bluetooth 4.0 (and more recent)
WEB	**SecureToken-337F**	**AVTOR LLC**	https://avtor.ua/	• USB-device, in a plastic case, • Has an additional FLASH-drive
	SecureToken-338KF			
	SecureToken-338M			USB-device, in a plastic case
	SecureToken-338S			USB-device, in a metal case
	SecureToken-338MF			• USB-device, in a plastic case, • additional mechanic confirmation of the transactions' carrying out
Mobile + WEB	**SecureToken-338HD** (Bluetooth-device)			• Plastic keychain, USB-device, • User's device should support the wireless interface Bluetooth 5.0 (and more recent)
	SecureToken-338MB (Bluetooth-device)			• Plastic keychain, USB-device, • User's device should support the wireless interface Bluetooth 5.0 (and more recent)
WEB	**CryptoCard-337**			• Smart-card, • In order to use it, a card reader should be available
	CryptoCard-338			

Also, information about hardware storage is available on the official website of the State Enterprise "DIIA" (https://ca.diia.gov.ua/).

Before starting the registration:

- of the new advanced ES key that you plan to save to the hardware storage,
- of the existing qualified ES key that you store in the hardware storage,
- make sure that the required library installation packages are installed on your device.

When further using the system and logging in to the system on another device, if you store the qualified ES key in the hardware storage:

- make sure that the required library installation packages are installed in your device.

2. Registration in the system with the generation of new advanced ES key

2.1. To register, go to the link **https://rbo.raiffeisen.ua**, where the authorization window in the system will open (Fig. 1):

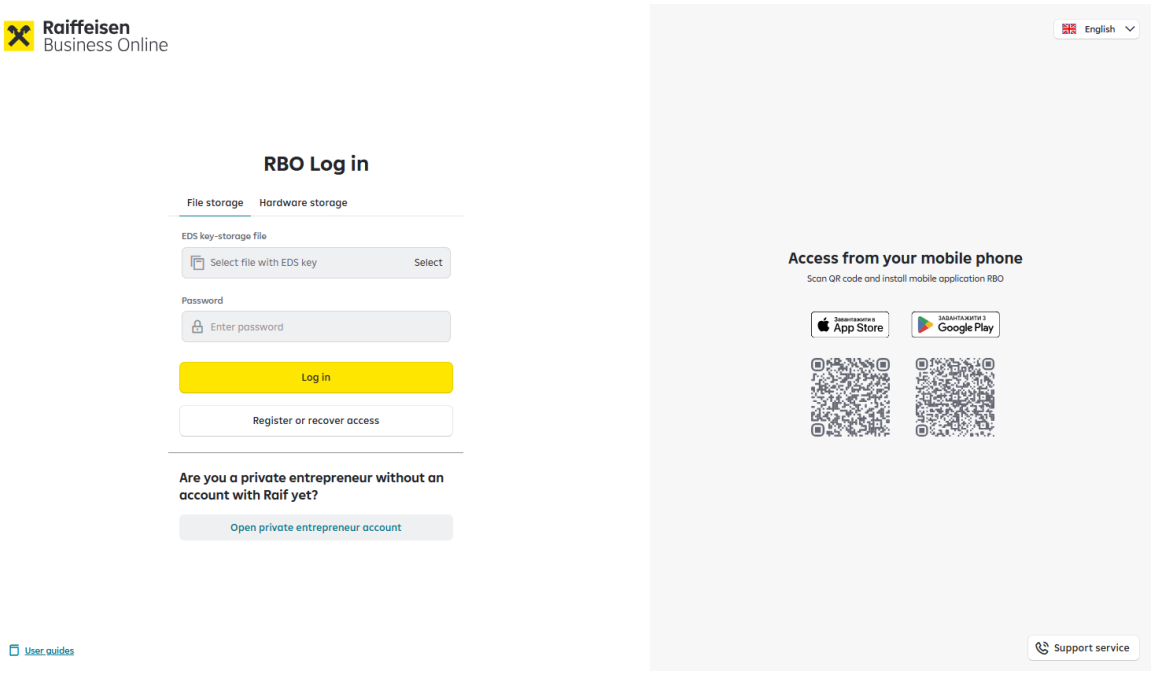
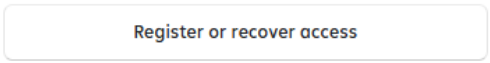


Fig. 1

2.2. To start the registration procedure, click the "**Register or recover access"** button.



2.3. After clicking the "Register or recover access" button, the "**Step 1: Choose the key you want to use for the registration"** form will automatically open (Fig. 2):

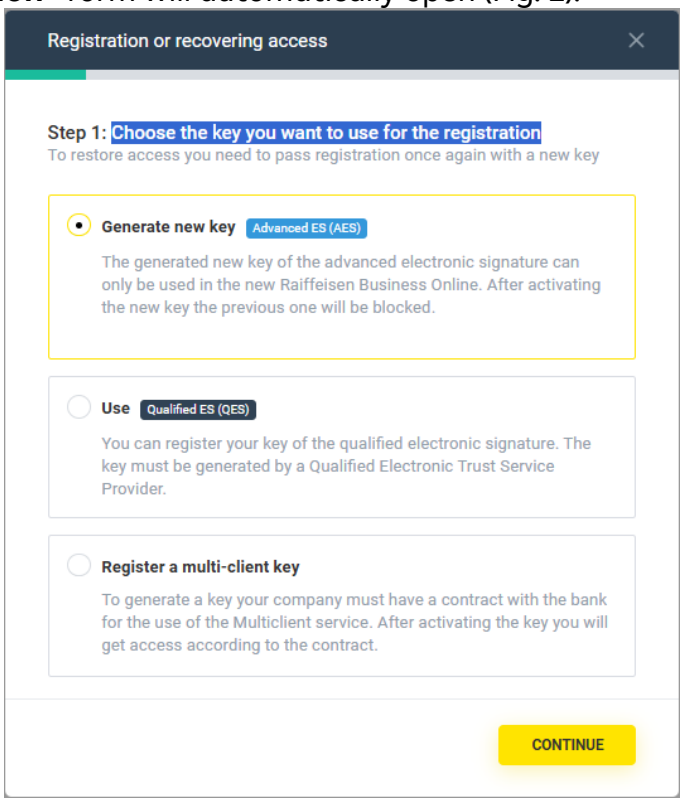


Fig. 2.

To register in the system using the advanced ES key generated by the system during registration, select the option "Generate new key (Advanced ES (AES))" and click the button CONTINUE.

2.4. In the next step, "**Step 2: Selecting a key storage"**, you must select the media on which the key will be stored. If you choose hardware storage, select the storage and enter the password.

ATTENTION! To work with hardware storage, the installation packages of the libraries must be updated on your device. If the libraries are not installed or they are outdated, the system will offer to install or update the necessary libraries (Fig. 3).

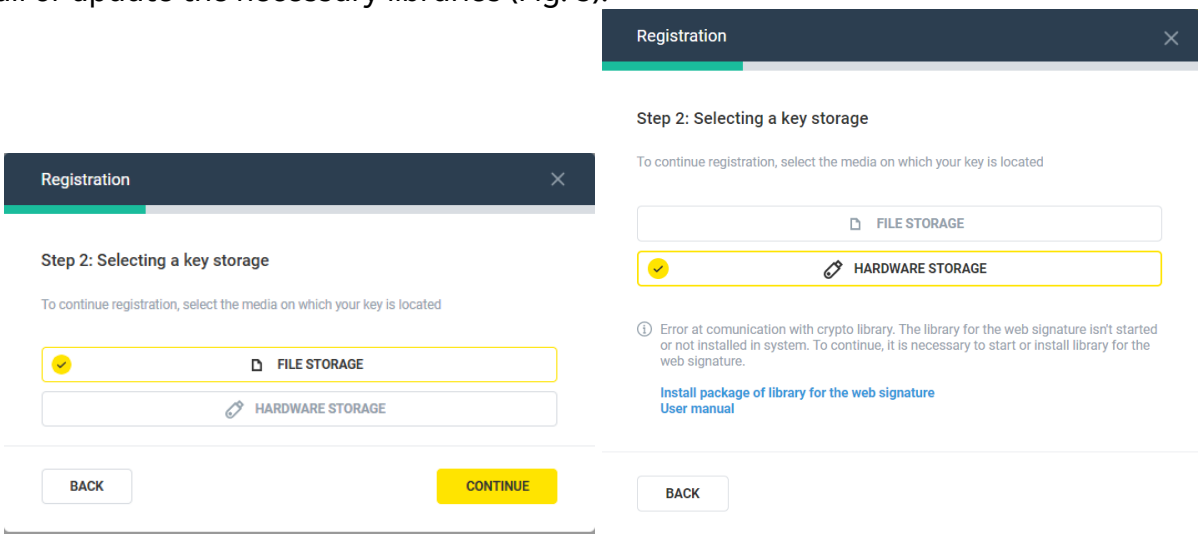


Fig. 3

2.5. At the next stage "**Step 3: Enter Client data**", the client and each of the client's authorized person (if any) must personally fill out the registration form, for which they must select the "LEGAL ENTITY" tab and fill in the fields marked with «*» with information about the client (Fig. 4):

In this form:

- **Country of state registration of the legal entity** – select the country code and name from the drop-down list. To do this, enter the name of the country in full or in part. The field is mandatory;
- **EDRPOU code** – the EDRPOU code can contain 8 digits. This field is mandatory;
- **Name of the organization** – name of the company in Ukrainian (abbreviated name may be used). The field must not exceed 40 characters.

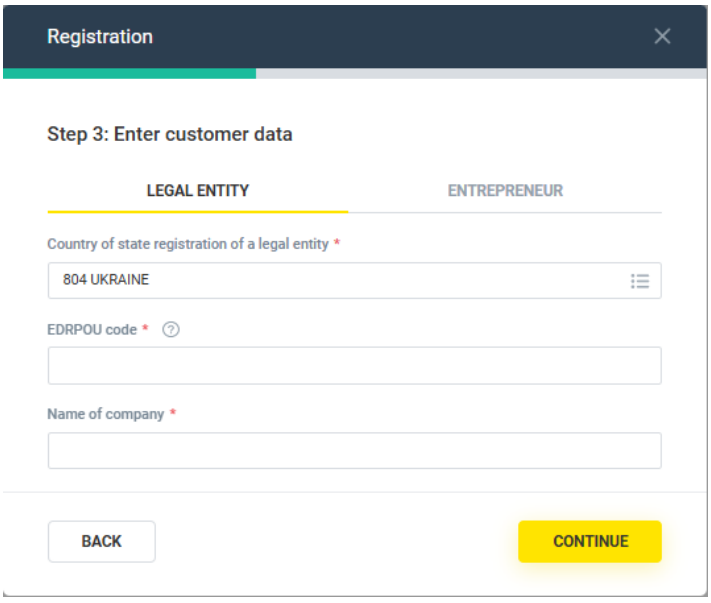
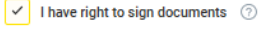


Fig. 4

2.6. At the next stage "**Step 4: Enter User data", information about the client's authorized person is filled in** (Fig. 5).

The form allows you to enter data if:
The registration is performed personally by an **authorized person with the right to sign** settlement documents, in which case the checkbox 

must be **checked**;

2.6.1. Generation of an advanced electronic signature key for an accountant "without signature rights"

The form allows you to enter data if:
The registration is performed personally by an **authorized person without the right to sign** settlement documents, in which case the checkbox ☐ I have right to sign documents must **NOT be checked.**

ATTENTION! Registration in the system of authorized persons without signature right must be carried out after the bank confirms the application for activation of the electronic signature key of the client's authorized person with the right of first signature.

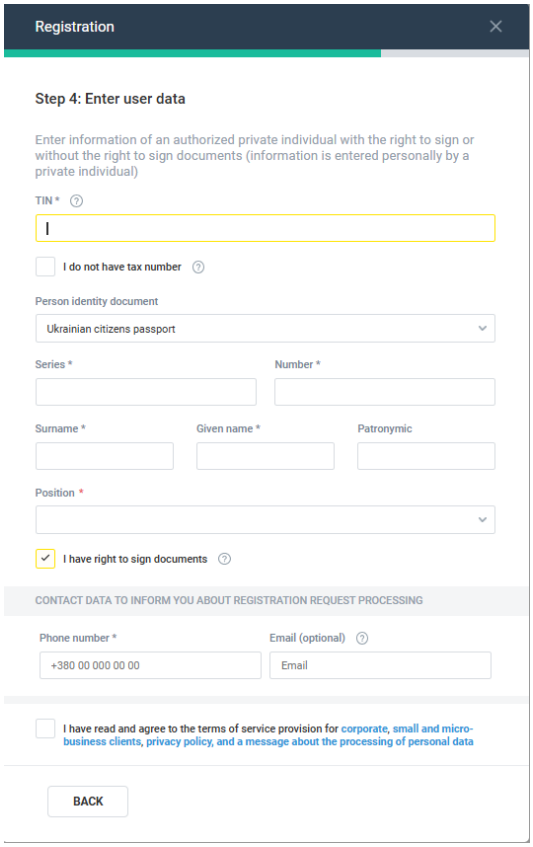


Fig. 5

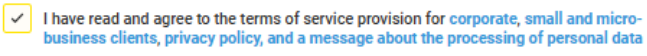
All data about the authorized person shall be filled in by such person independently:

- **TIN of the authorized person** – registration number of the taxpayer's account card (identification code). Must contain 10 digits. The field is required to be filled in unless the check box "I do not have a TIN" is checked.

ATTENTION! If the authorized person does not have a TIN, you must check the check box ☑ I do not have tax number.

- **Identity document** – select the type of identity document from the list.
- **Series** – available only if the document type "Passport of a citizen of Ukraine" is selected. Must contain 2 cyrillic characters.
- **Number** – if you have selected a document of the "Passport of a citizen of Ukraine" type, it must contain 6 digits. If the document of the "Passport of a citizen of Ukraine in the form of an ID card" type is selected, it must contain 9 or 12 digits.
- **Surname, First Name, Patronymic** – full name of the authorized person (the "Patronymic" field is not mandatory unless the user doesn't have a "Patronymic" according to the passport document).
- **Position** – the position of the authorized person (select a position from the fixed drop-down list, or select the "Specify manually" position). The position of the authorized person with signature rights shall be indicated. It must coincide with the information contained in the documents of the client's file (if such information is available in the client's file at the time of registration).
- **"I am authorized to sign settlement documents"** – filled in automatically for the authorized person with signature rights. In case of registration of an authorized person without signature rights, the checkbox ☑ I have right to sign documents must be unchecked. After registering an authorized person without signature rights, such person will not be able to

use the key of the advanced electronic signature to sign electronic settlement documents. At the same time, he/she will be able to log in to the system, create and store electronic settlement documents, etc.

- **Contact phone number** – you must specify the number with the international code of Ukraine (the code is indicated in the field) and the city code/mobile operator code.
- **E-mail** – it should be entered in the format example@mail.com. The authorized non-resident person who has selected a international passport, permanent or temporary residence permit, type of the temporary residence in the form of an ID card, Certificate of refugee a citizen of Ukraine, or another type of document in the "Person identity document" field must necessarily indicate the e-mail.
- **Field** 

– The authorized person must check the box. To read the terms of the consent, please follow the link on the form. The checkbox is required to be filled in.

After filling out the form, click the button 

.

2.7. At the next step "**Step 5: Save the key**", the form for generating the advanced ES key by the system will be opened (Fig. 6):

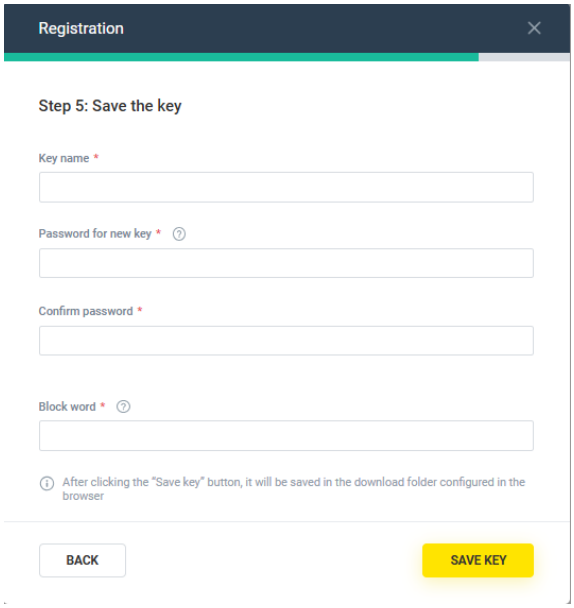


Fig. 6

If you chose a file medium for saving in step 2, you must fill in the following fields:

- **Key name** – can be any word or phrase;
- **Password** – must contain at least one uppercase Latin letter, at least one lowercase Latin letter, one digit, a special character (e.g. !, ;, %, :, ?, *, (,), +, -, _, =) and be at least 8 characters long.

ATTENTION! Be sure to check the language of the keyboard where you enter the key password. Pressing the same keys in different input languages has different meanings and different special characters.

- **Repeat the password** – the passwords must be the same;
- **Blocking word** – any word that is necessary to identify the client\authorized person when contacting the bank's support service by phone to block the personal electronic signature

key of the client\authorized person (in case of its loss, damage or compromise). **The specified blocking word must be memorized**.

After filling out the form, click the button SAVE KEY.

After clicking the "**Save a key"** button, the system will generate an electronic signature key, which the web browser will offer you to save. With the appropriate browser settings, your key can be automatically saved to the appropriate directory (by default, to the "Downloads" folder).

ATTENTION! Be sure to memorize the location where your ES key will be saved. No one else has this information except the user who is registering. If you have forgotten the path to the key file, you must re-register with the generation of a new ES key.

If hardware storage was selected for saving in step 2, the following fields must be filled in (Fig. 7):

- **Hardware storage** – select the hardware storage to save the key from the list;
- **Checkbox for using the device with administration rights** – used for hardware storages of the Crystal-1 type;
- **Administrator password for the device** – enter the administrator password. The field is displayed only for hardware storages of the Crystal-1 type, provided that the Device with administrator rights checkbox is selected;
- **Password** – must contain at least one uppercase Latin letter, at least one lowercase Latin letter, one digit, a special character (for example !, ;, %, :, ?, *, (,), +, -, _, =) and be at least 8 characters long.

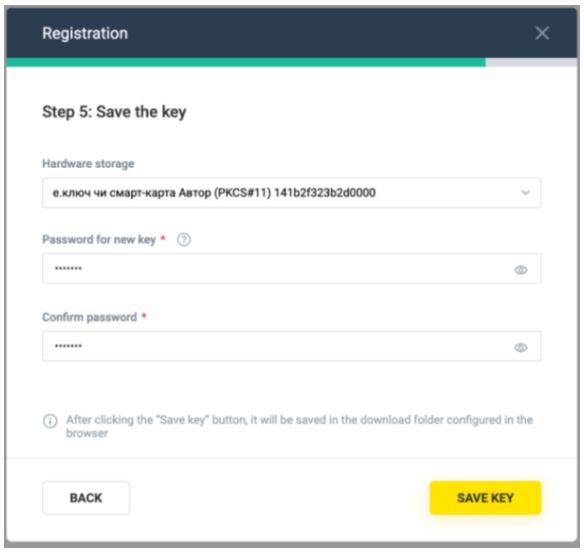


Fig. 7

ATTENTION! Be sure to check the language of the keyboard where you enter the key password. Pressing the same keys in different input languages has different meanings and special characters.

- **Repeat the password** – the passwords must be the same;
- **Blocking word** – any word that is necessary to identify the client\authorized person when contacting the bank's support service by phone to block the personal electronic signature key of the client\authorized person (in case of its loss, damage or compromise).
  The specified blocking word must be memorized.

After saving the ES key, the system will offer to print the application (Fig. 8).

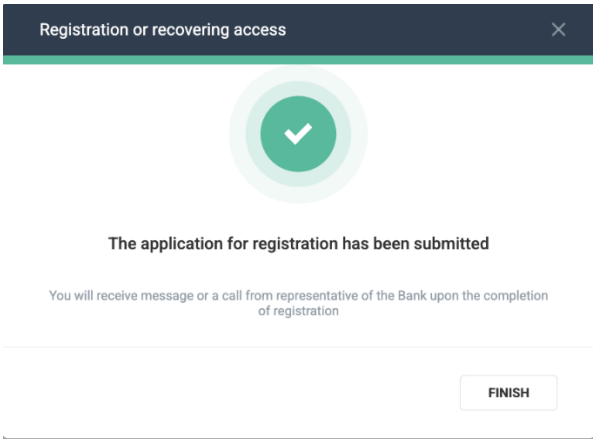


Fig. 8

To print the Application, click the button PRINT THE APPLICATION FOR REGISTRATION.

To save the Application, click the button SAVE THE APPLICATION FOR REGISTRATION.

After printing/saving the Application for Registration of the Client's Public ES Key, click the "Finish" button.
After these actions, the registration procedure will be completed.

The key will be activated no later than the next business day from the date of submission of the duly executed Application and documents to the Bank (Fig. 8), personally to the Bank's branch or remote channel.

After saving the electronic signature key for an Authorized person without the right to sign settlement documents, the system will automatically open a window indicating successful registration (Fig. 9).

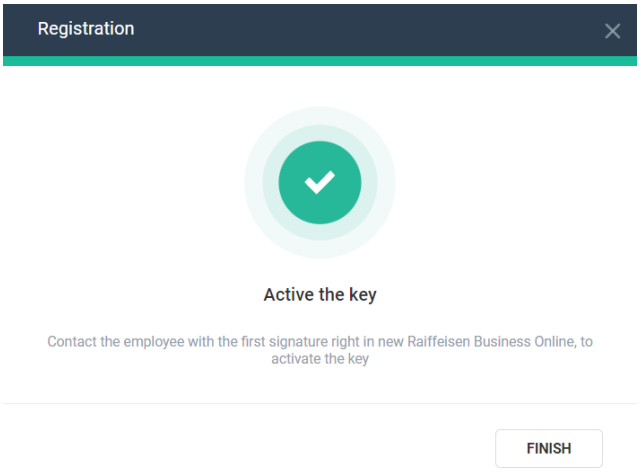


Fig. 9

2.8. Activation of the advanced ES key

ATTENTION! The validity period of the application for activation of the electronic signature keys of the client's authorized persons with signature rights is 30 days from the date of their generation.

To activate the advanced ES key, the following steps are required:

2.8.1. The ES key "with signature rights" is generated in the name of the authorized person with the first signature level:

(1) Print and sign the application form (Fig. 10) in two fields:
- "Достовірність заведених даних підтверджую"/"I hereby confirm the accuracy of the provided data" – signature,
- "Керівник клієнта"/"CEO of the Client" – date of filling, signature, surname/name/patronymic.

(2) Submit the following documents in person to any branch of the Bank:
a) signed application (you can print the application yourself or at the bank's branch),
b) the original passport document, the details of which were indicated when filling out the application,
c) documents confirming the powers of the authorized person with signature rights (if they are not available in the client's file in the bank).

The key will be activated no later than the next business day after submission of the duly executed application and documents to the bank's branch.

ATTENTION! If you have difficulties visiting the bank's branches, the application for registration of the advanced electronic signature key can be submitted to the bank remotely:
(option #1) If you are a private client of the bank, call the technical support service for consultation and transfer of the application via Raiffeisen Online Chat, or
(option #2) Save and sign the application with your qualified ES key (QES) and send it to the virtual branch address raif.business@raiffeisen.ua:
- **Please note!** You can sign the application with your qualified key issued to you as an authorized person of the company, or with your personal qualified key issued to you as an individual.

To learn more about how to submit the application remotely, please follow the link.

2.8.2. The ES key "with signature rights" is generated in the name of an authorized person with the second or other signature level:

(1) Print and sign the application form (Fig. 10) in two fields:
- "Достовірність заведених даних підтверджую"/"I hereby confirm the accuracy of the provided data" – signature,
- "Керівник клієнта"/"CEO of the Client" – date of filling, signature, surname/name/patronymic.

(2) Submit the following documents in person to any branch of the bank:
a) application, which must be signed by the authorized person and the client's manager,
b) the original passport document, the details of which were indicated when filling out the application,
c) documents confirming the powers of the manager/authorized person with signature rights (if they are not available in the client's file with the bank).

The key will be activated no later than the next business day after submission of the duly completed application and documents to the bank's branch.

ATTENTION! If you have difficulties visiting the bank's branches, the application for registration of the advanced electronic signature key can be submitted to the bank remotely:

(option #1) If you are a private client of the bank, please call the technical support service for consultation and submission of the application via Raiffeisen Online chat:

- **Please note!** In order to submit the application via Raiffeisen Online chat, such application must be pre-signed by the customer's manager using a qualified key (QES).

(option #2) Save and sign the application with your qualified key (QES) and send it to the address of the virtual branch raif.business@raiffeisen.ua:

- **Please note!** In order to send the application to raif.business@raiffeisen.ua, such application must be pre-signed by the client's manager using the qualified key of such manager.

To learn more about how to submit the application remotely, please follow the link.

2.8.3. If the ES key "without signature rights" is generated:

ATTENTION! To activate the electronic signature key, you must contact the manager/authorized person registered in the system with the right of first signature.

The application for registration of the electronic signature key "without signature rights" is confirmed in the system independently by the manager / authorized person registered in the system with the right of first signature (the bank does not participate in the activation of keys "without signature rights").

Заявка № 160133758417 від 28.07.2023 р.

НА РЕЄСТРАЦІЮ ВІДКРИТОГО КЛЮЧА ЕЦП КЛІЄНТА У СИСТЕМІ «РАЙФФАЙЗЕН БІЗНЕС ОНЛАЙН» АТ «РАЙФФАЙЗЕН БАНК»

Відомості про клієнта	
Найменування клієнта	ТОВ "Тест"
ЄДРПОУ	11224455
Країна реєстрації	УКРАЇНА
Телефон	+38 (056) 123-11-11
E-mail	test@gmail.com
Відомості про власника відкритого ключа ЕЦП	
Посада	Директор
Прізвище	Петров
Ім'я	Петро
По-батькові	Петрович
Код ІПН	3322556688
Посвідчення особи	Паспорт громадянина України
Серія та номер	СК 112311
Відомості про відкритий ключ ЕЦП	
Серійний номер сертифікату	743C079FCF88D1020400000868F00004A7C0100
Представлення відкритого ключа ЕЦП у 16-ковому вигляді	02 C5 8E BB D4 AE C9 0D 82 E9 A7 3D 8A 12 86 5D 16 44 AB 78 FB 76 3A 8A 1C A5 CC FE 17 0D 21 CF 01

Достовірність заведених даних підтверджую Personal signature of the owner of the ES key
(особистий підпис)

Керівник клієнта
Data / Signature of CEO of the Client / Name, Surname of CEO of the Client
(Дата, підпис, П.І.Б.)

Відбиток печатки (за наявності)

Уповноважений представник Банку
_____ / _____ / _____
(Дата, підпис, П.І.Б.)

Відбиток печатки Банку

Fig. 10

3. Registration in the system using the existing qualified ES key

3.1. To register, go to the link **https://rbo.raiffeisen.ua**, where the authorization window in the system will open (Fig. 11):

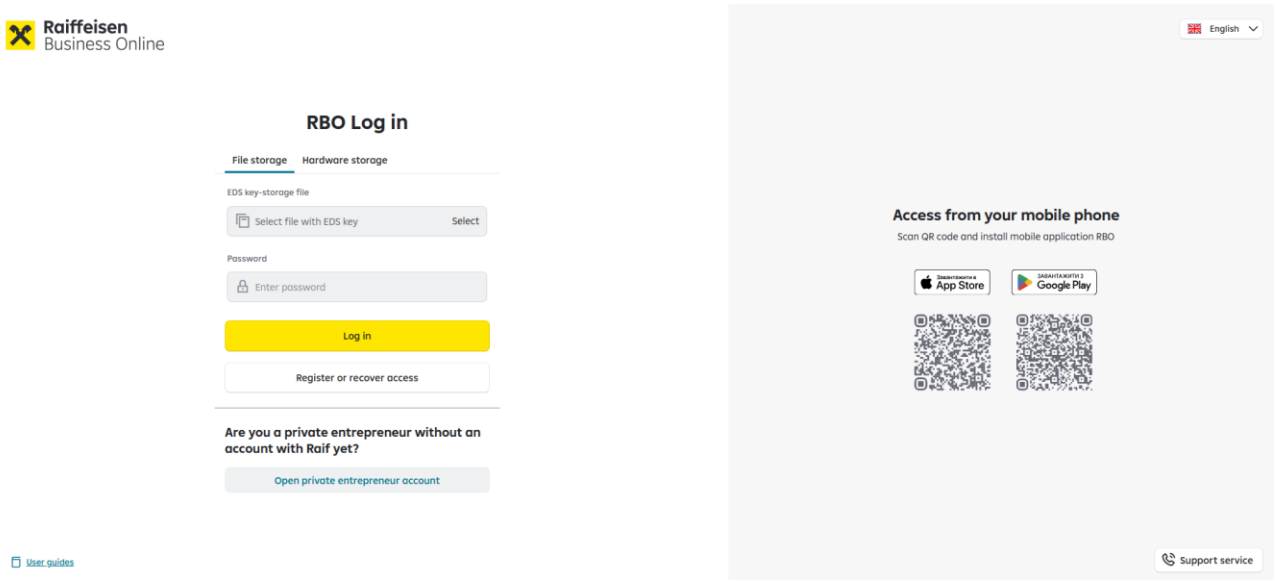
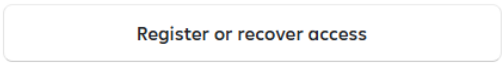


Fig. 11

3.2. To start the registration procedure, click the "**Register or recover access"** button.



3.3. After clicking the "Register or recover access" button, the "**Step 1: Choose the key you want to use for the registration**" form will automatically open (Fig. 12):

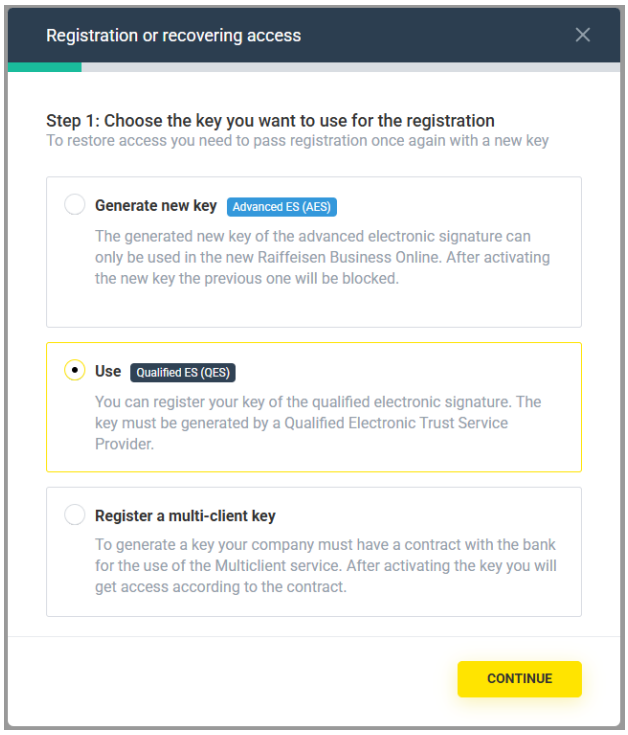


Fig. 12

To register in the system using the qualified ES key, you must select the appropriate option "Use Qualified ES (QES)" and click the button 

.

3.4. In the next step, "**Step 2: Selecting a key storage**", you must select the media on which the key will be stored. If you choose hardware storage, select the storage and enter the password.

ATTENTION! To work with hardware storage, the installation packages of libraries must be updated on your device. If the libraries are not installed or they are outdated, the system will offer to install or update the necessary libraries (Fig. 13).

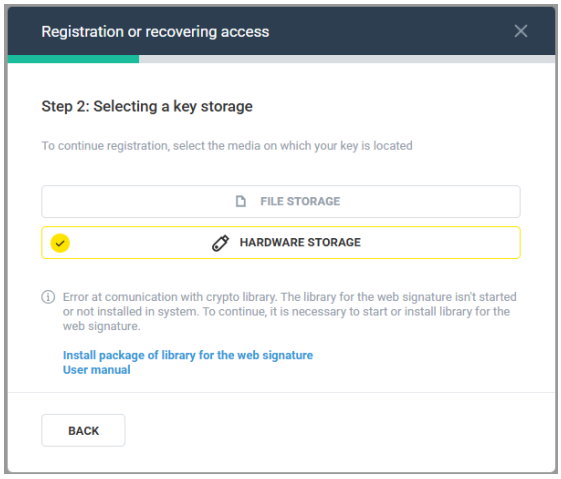


Fig. 13

3.5. After clicking the "Continue" button, the "**Step 3: Use EDS key"** form will open to select the file with the qualified ES key and enter the password (Fig. 14).

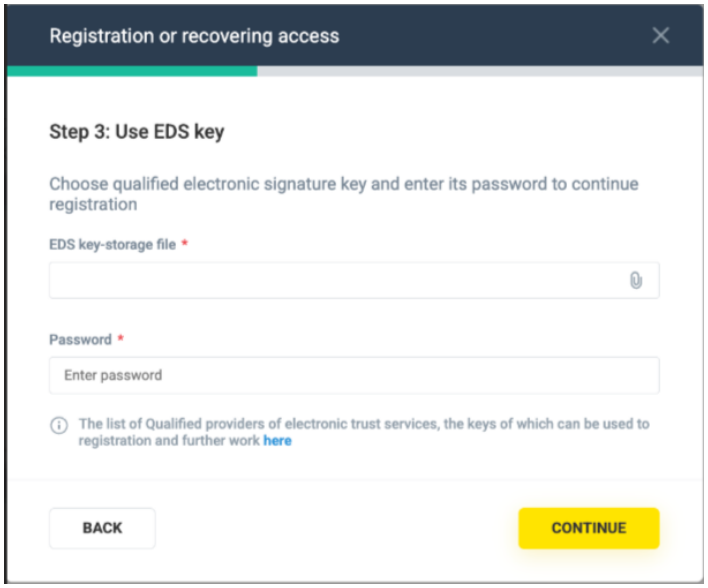


Fig. 14

After filling out the form, click the button CONTINUE.

3.6. In the form "**Step 4: Check customer data"**, the client's data will be pre-filled automatically in accordance with the data of the qualified ES key certificate (Fig. 15).

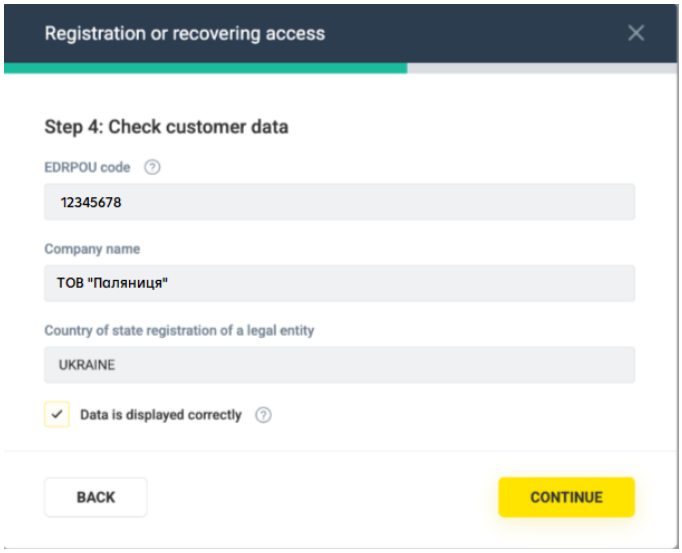


Fig. 15

At the same time, you need to confirm the data by selecting the "Data is displayed correctly" checkbox and click the button CONTINUE.

ATTENTION! If the data does not match the data displayed on the screen, you must contact a qualified electronic trust service provider to update the qualified ES key.

3.7. At the next step "**Step 5: Enter user data**", information about the client's authorized person is filled in (Fig. 16):

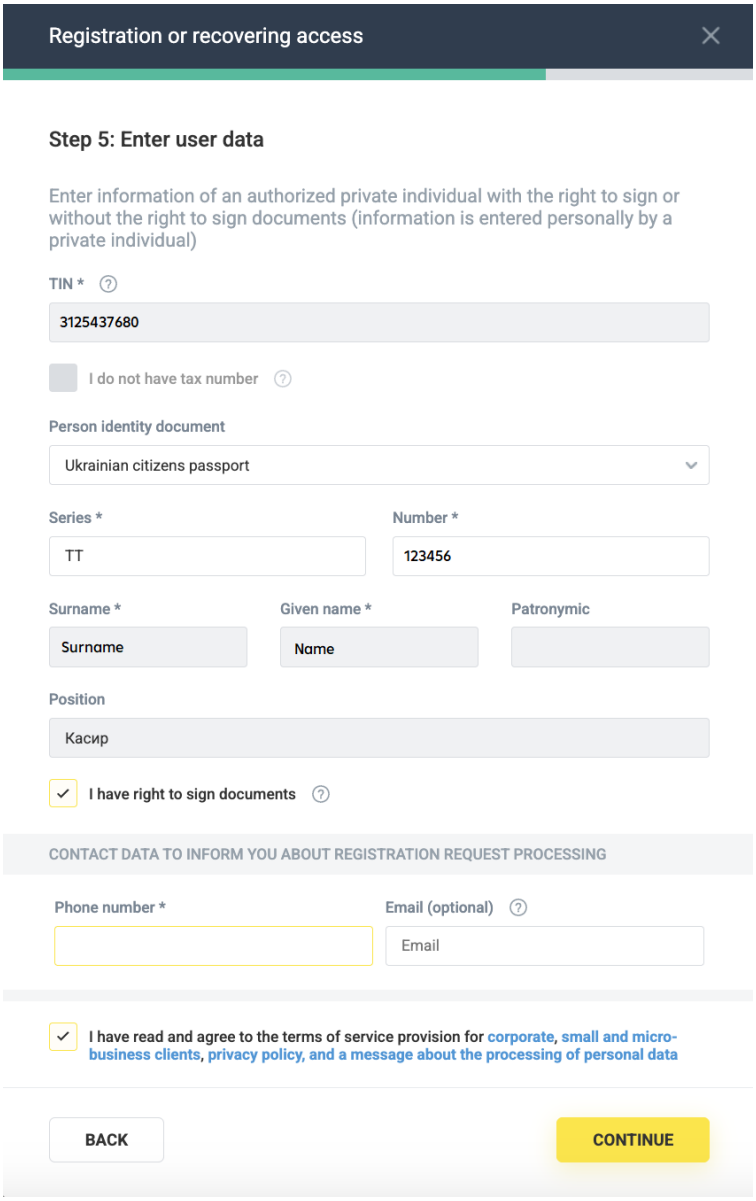


Fig. 16

Fill in the following fields in the form:

- **Person identity document** – select the type of identity document from the list;
- **Series** – available only if the document of the "Passport of a citizen of Ukraine" type is selected. Must contain 2 cyrillic characters;
- **Number** – if the document of the "Passport of a citizen of Ukraine" type is selected, it must contain 6 digits. If the document of the "Passport of a citizen of Ukraine in the form of an ID card" type is selected, it must contain 9 or 12 digits;
- **Surname, Given name, Patronymic** – full name of the authorized person automatically filled from the data of the qualified ES key (without editing rights);
- **Position** – the role of the authorized person, automatically filled from the data of the qualified ES key (without editing rights);
- **"I have right to sign documents"** – is filled in automatically for the authorized person with signature rights. In case of registration of an authorized person without signature rights, the checkbox 

must be unchecked. After registration, an authorized person without signature rights will not be able to use a qualified ES key to sign electronic settlement documents. At the same time, he/she will be able to log in to the system, create and store electronic settlement documents, etc;

- **Phone number** – you must specify the number with the international code of Ukraine (code specified in the field) and the city code/mobile operator code;
- **Email** – must be specified in the format example@mail.com;
  An authorized non-resident person who has chosen a foreign passport document, a permanent or temporary residence permit, a temporary certificate of a citizen of Ukraine, or another type of document in the identity document field must provide an e-mail;
- **"I have read and agree to the terms of service provision for corporate, small and micro business clients, privacy policy, and a message about the processing of personal data"** – the authorized person should check the box. To familiarize yourself with the terms of the consent, follow the link on the form. The checkbox is required to be filled in.

ATTENTION! Registration of the qualified electronic signature key without signature rights in the system shall be carried out after the bank confirms the application for activation of the key of the authorized person of the client with the right of 1st (first) signature.

3.8. At the next stage "**Step 5. Enter block word"**, the form will contain only a field for entering the block word.

- **Block word** – any word required for identifying the client/authorized person during a phone call to the bank's support service to block the personal ES key of the client/authorized person (in case of loss, damage, or compromise). **This block word must be remembered.**

After clicking the "Next" button, **if the qualified ES key certificate does not contain any restrictions on the rights of the client/authorized person (by type of document, amount of transactions, etc.),** the system will automatically open a message about the successful registration (Fig. 18).

After processing such an application, the bank shall send a notification of registration (activation) of the qualified ES key to the mobile phone number or e-mail address of the client/authorized person of the client specified by such client/authorized person during registration in the system to enable the client to start using the system.

To complete the registration, click the button FINISH.

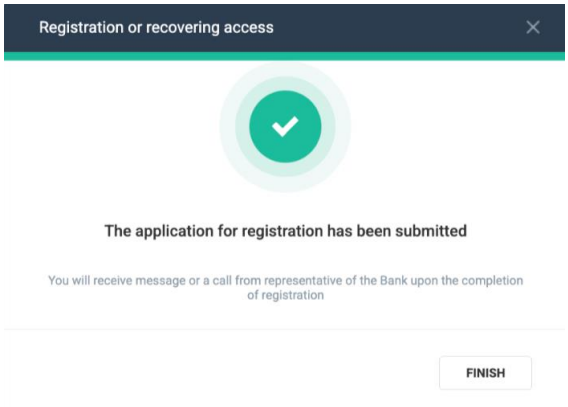


Fig. 18

After clicking the "Next" button for an Authorized person without the right to sign settlement documents, the system will automatically open a window on successful registration (Fig. 19).

Click the "Finish" button, after which the registration procedure will be completed.

To activate the ES key, you must contact the Authorized person registered in the system with the right of 1st (first) signature.

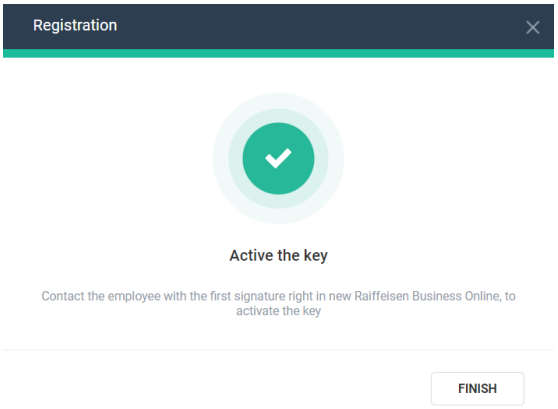


Fig. 19

4. Service messages

4.1. The system displays a message to the user in case of unsuccessful registration or authorization (login):

MESSAGES	WHAT DOES IT MEAN?
Key error Maybe your key has not been activated yet. Otherwise generate a new key by clicking "Register or recover access" or contact the support service	- the ES key with which you are trying to log in has expired, - the ES key isn't yet activated, - the ES key is NOT registered in the system, please, register your ES key in RBO first,
Key expired Create a new key by pressing "Register or renew access". If you still have any questions, contact the support service for help	- the validity period of the ES key has expired,
Key error Generate a new key by clicking "Register or recover access" or contact the support service	- the ES key is damaged or has an incorrect format, - the ES key is blocked or activation has been canceled,
Invalid password or key Please try selecting the key and entering the password again. If the error keeps occuring, click "Register or recover access" or contact the support service	- the password for the ES key is incorrect, - the personal secret key file does not meet the requirements of the system (incorrect key, QES seal),
Your IP-adress {user-ip} has been banned Please contact your administrator	- settings for allowed/blocked IP addresses for login have been configured; please check the settings,
Access is blocked Please contact support for help	- access has been blocked for the company under which the user is registered in RBO,
Something went wrong Please try again or contact the support service	- other reasons, for example, the company's account in the system was blocked or transferred to the archive, or other technical reasons.

4.2. The system displays a message to the user about the expiration of the ES keys

Automatically configured system notifications inform you about the expiration date of advanced ES and qualified ES keys:

- the text of the message about the expiration of the advanced ES key contains a link to a YouTube video instruction,
- if the key you used to log in to the system expires in less than 30 days, the system will inform you about it (Fig. 20, Fig. 21):

Message displayed in the system regarding the advanced ES and qualified ES keys, daily, starting from the 30th day until the expiration date of the key:

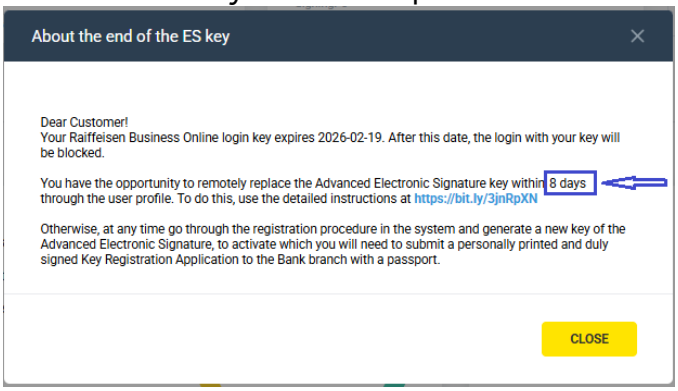


Fig. 20

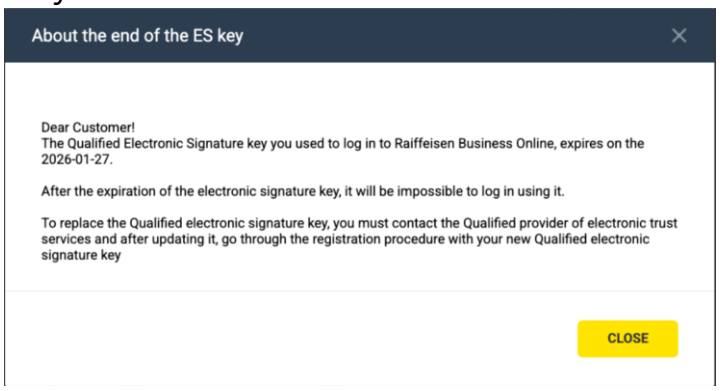


Fig. 21

SMS – a message sent 7 days before the key expiration date

Do 01.08.23 neobkhidno zminyty klyuch Banku u RBO. Zminit klyuch dystantsijno u profili korystuvacha. Navchalne video: https://bit.ly/3jnRpXN Detali 0800505770

Do 01.08.23 zminit klyuch KEP dlya vkhodu v RBO ta projdit povtornu reyestratsiyu. Navchalne video: https://rb.gy/rjkx38 Detali 0800505770

Viber or e-mail – a message sent 7 days before the key expiration date

Шановний клієнте!
Термін дії Вашого ключа Удосконаленого електронного підпису (ключ банку) у Raiffeisen Business Online закінчується 01.08.20234.
Після цієї дати вхід до системи з цим ключем буде обмежено.
Змініть ключ банку дистанційно у профілі користувача.
Скористайтесь відео-інструкцією за посиланням.

У разі додаткових питань звертайтесь до:
☎ Служба підтримки RBO: 0800505770, 0800400470, 0444954140 (у Києві та з-за кордону), clientbank.support@raiffeisen.ua (пн-пт 8:00-22:00, сб-нд 8:00-20:00)
☎ Інформаційний центр: 0800505045, 0800400445, 0445902498 (у Києві та з-за кордону)
З повагою, Райффайзен Банк

Шановний клієнте!
Термін дії Вашого ключа Кваліфікованого електронного підпису (КЕП) у Raiffeisen Business Online закінчується 01.08.2023.
Після цієї дати вхід до системи з цим ключем буде обмежено.
Для заміни ключа КЕП необхідно звернутись до Кваліфікованого надавача електронних довірчих послуг та після його оновлення пройти процедуру реєстрації з Вашим новим ключем КЕП у Raiffeisen Business Online.
Скористайтесь відео-інструкцією за посиланням.

У разі додаткових питань звертайтесь до:
☎ Служба підтримки RBO: 0800505770, 0800400470, 0444954140 (у Києві та з-за кордону), clientbank.support@raiffeisen.ua (пн-пт 8:00-22:00, сб-нд 8:00-20:00)
☎ Інформаційний центр: 0800505045, 0800400445, 0445902498 (у Києві та з-за кордону)
З повагою, Райффайзен Банк

We wish you successful work.
It is more convenient with Raif!