

UniCredit Bank Application user manual for Windows

Click on the link below for moving to appropriate section:

1. [Installation](#)
2. [Digital keys generating \(ruToken\)](#)
3. [Digital keys generating \(eToken\)](#)
4. [Documents signing](#)
5. [Links and contacts](#)

System requirements

For correct work of Business.Online system components user's PC must respond to the following requirements:

- Windows 8.1 or higher (32 or 64 bit)
- One or several supported internet browsers: Google Chrome (version 49 or higher), Opera (version 25 or higher), Yandex Browser, Internet Explorer (version 9 or higher), Microsoft Edge (for Windows 10 only).

Attention! It is strictly recommended to use the newest versions of browsers to ensure that your application components are as compatible as possible, and safe.

Pop-up windows must be turned on in the browser.

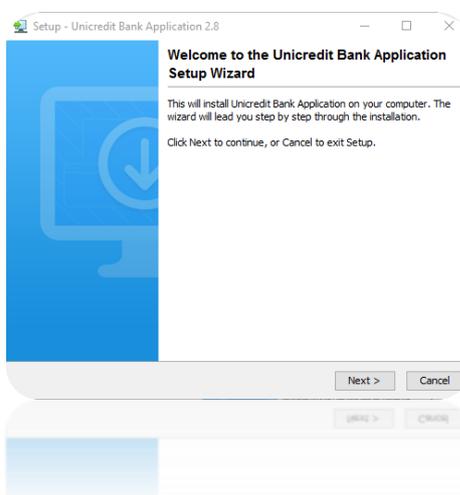
- Windows administrator user account for correct first installation of components. Administrative rights are not required for further work.

Application installation:

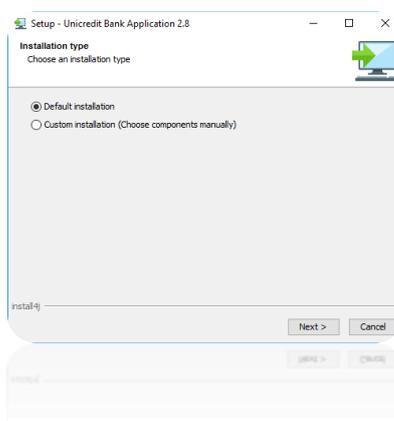
1. Download and save [UCBApp.exe](#) file
2. Open a folder where the file from the previous paragraph has been saved (**Downloads** by default), click on it with the right mouse button and choose **Run as administrator**.
Attention! Administrative rights are strictly required for the correct application installation!
3. Installation window will appear. Select preferred language and click **OK**.



4. Click **Next** in the following window

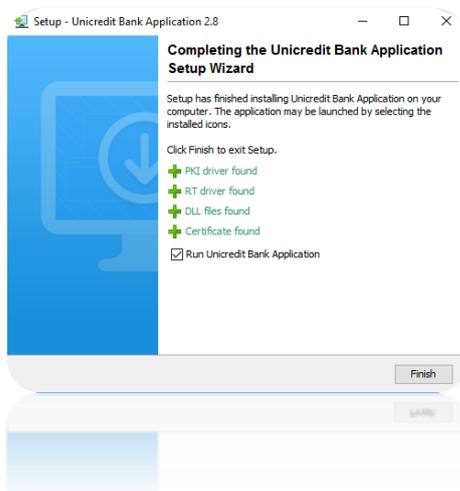


5. Select **Default installation** and click **Next**. Continue clicking on **Next** if the requests appear during the installation process



6. After the installation is complete, you will see a list of successfully installed components.

Attention! In case when one or few of the components were installed with errors, please restart the installation again and make sure it runs with the administrative rights.



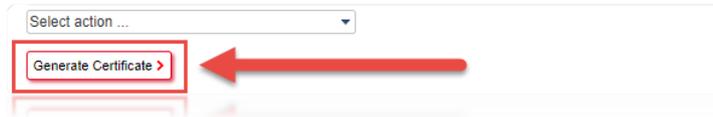
7. Signature software has been successfully installed on your PC. Click **Finish**.

DSK generation (ruToken):

1. Make sure **UniCredit Bank Application** is installed and launched. Red icon in Windows system tray indicates this:



2. Go to <https://gws.unicredit.ru/> and log in to the system using login (sent by the Bank via email) and password (sent by the Bank via SMS. Open **Settings**, then **Maintain A&A devices**. Plug your ruToken into PC. Click on **Generate Certificate**".



3. A new window for certificate creation will appear.

Create new key

Key owner: Awesome John | 0 USB[Rutoken ECP <no la... ?

Key: Awesome John_140518_134943

Rutoken DS (USB): "Awesome John_140518_134943"

Password: ●●●●●● [?] [?]

[Create] [Exit]

4. The program will set a way to the key and order you to type a password (1) for the token. Enter the password for the token and click on Create (3). You can check your password by clicking on the button (2).

Create new key

Key owner: Awesome John | 0 USB[Rutoken ECP <no la... ?

Key: Awesome John_140518_134943

Rutoken DS (USB): "Awesome John_140518_134943"

Password: ●●●●●● [?] [?]

[Create] [Exit]

5. When generation is over, you will see a confirmation message:

Settings > Maintain A&A devices

AUTHENTICATION & AUTHORIZATION DEVICE MANAGEMENT

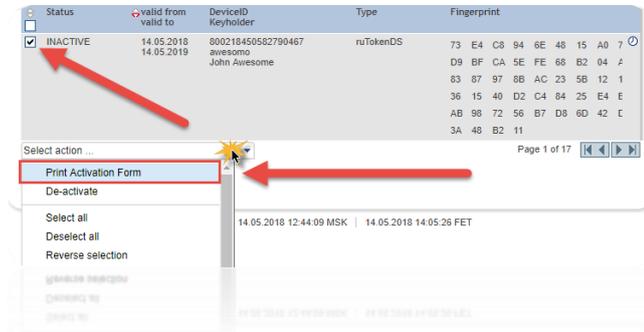
Your new key has been created! Please print and sign the activation form!

Overview of digital keys

Key storage location	Awesome John_140518_135920	Reset		
Status	valid from 14.05.2018 valid to 14.05.2019	DeviceID Keyholder 800215450582790467 awesome John Awesome	Type ruTokenDS	Fingerprint 73 E4 C8 94 6E 48 15 A0 7 D9 BF CA 5E FE 68 B2 04 F 83 87 97 8B AC 23 5B 12 1 36 15 40 D2 C4 84 25 E4 E AB 98 72 56 B7 D8 6D 42 E 3A 48 B2 11

- To activate your new certificate, please, mark it (near **Inactive**) and select Print activation form from the dropdown list (**Select action...**). Certificate print form will be opened in a new browser window.

Attention! Pop-up windows must be turned on in the browser.



- You need to print the activation form in duplicate, fill in your passport data, put a signature and deliver it to the Bank office.

Attention! The Bank is activates digital signature keys within two business days since they have been received. In case it does not happen, please, contact your account manager.

DSK generation (eToken):

1. You'd better change token's default password (**1234567890**) before digital signature key generation. You will a window offering you to change your default password when eToken is connected to PC for the first time.
Password must respond to the following requirements: uppercase and lowercase letters, digits.
2. Make sure UniCredit Bank Application is installed and launched. Red icon in Windows system tray indicates this



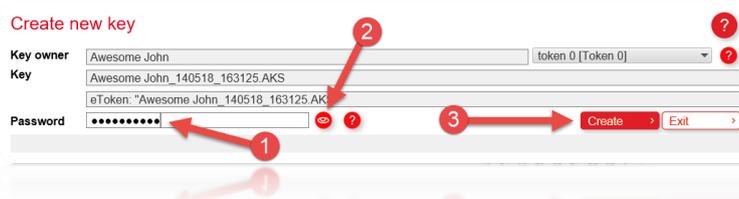
3. Go to <https://gws.unicredit.ru/> and log into the system using login (sent by the Bank via email) and password (sent by the Bank via SMS. Open **Settings**, then **Maintain A&A devices**. Plug your ruToken into PC. Click on **Generate Certificate**.



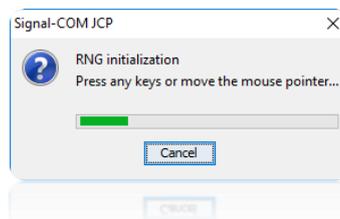
4. A new window for certificate creation will appear.



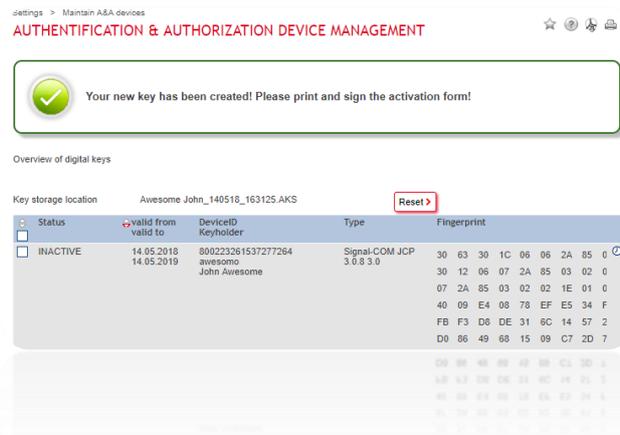
5. The program will set a way to the key and order you to type a password (1) for the token. Enter the password for the token and click on Create (3). You can check your password by clicking on the button (2).



6. RNG initialization window will appear. Please, move mouse pointer within with window or press any keys randomly until the progress bar is full.

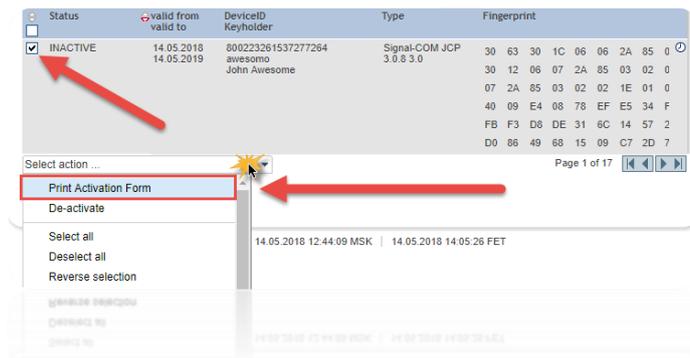


7. When generating is over, you will see a confirmation message:



8. To activate your new certificate, please, mark it (near **Inactive**) and select Print activation form from the dropdown list (**Select action...**). Certificate print form will be opened in a new browser window.

Attention! Pop-up windows must be turned on in the browser.

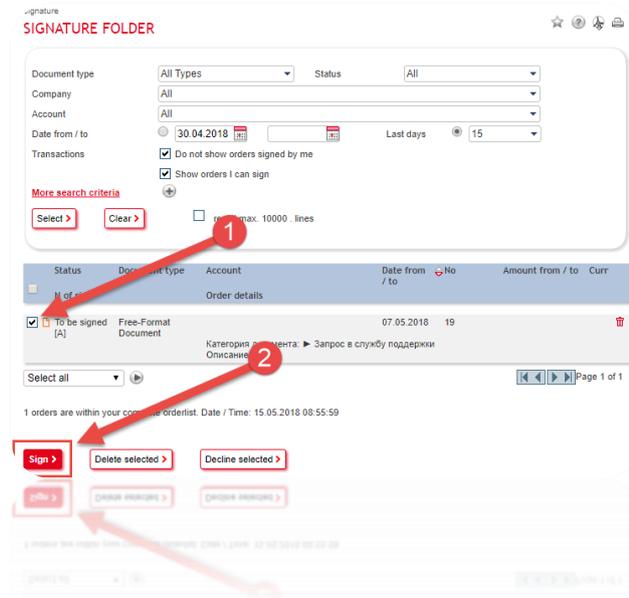


9. You need to print the activation form in duplicate, fill in your passport data, put a signature and deliver it to the Bank office.

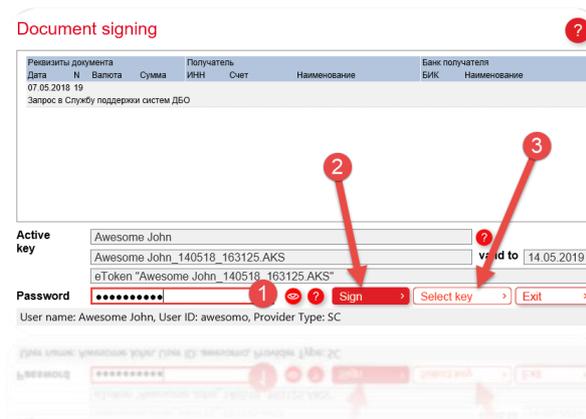
Attention! The Bank is activating digital signature keys within two business days since they have been received. In case it does not happen, please, contact your account manager.

Documents signing:

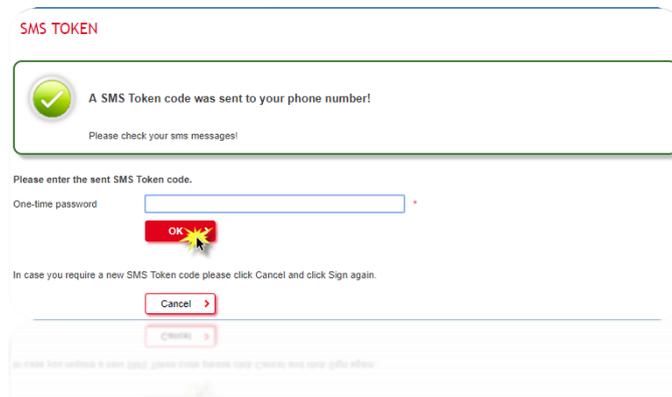
1. Create and save necessary documents within **Business.Online** banking system. Open **Signature** folder.
2. Check if UniCredit Bank Application is installed and running now.
3. Make sure the documents awaiting for signature are all marked. Plug your token (USB device) into your PC.
Click **Sign** button.



4. A new window for signing will open. The program will set a way to the key and order you to type a password (1) for the token. If it does not happen, please, click **Select key** (3) and choose a path to the key storage (eToken/ruToken). Enter password for the token (default for eToken: **1234567890**; default for ruToken: **12345678**) and click on **Sign** (2).



5. If password for the token is entered correctly, you will see a message saying that SMS with the additional authentication code has been sent to your mobile phone. You need to enter that code on the next window. In case you are using secondary authentication method, a code from the scratch card will be asked.



6. In case the additional authentication code is entered correctly, the documents will be totally signed and sent to the Bank for the further processing.

List of results

Status	Order type Information Message	Account	Date	Amount	Curr
Signed	Free-Format Document Категория документа: Запрос в службу поддержки Описание: 123 You finally signed this order		07.05.2018		

Links and contacts:

[Customer technical support portal](#)

[Log into Business.Online](#)

In case of any technical difficulties, please, contact us via one of the phones:

+ 7 (495) 258-72-32

8 (800) 700-99-32

Or via e-mail: support@unicredit.ru / 911@unicredit.ru

For organizational matters, please, contact call center via one of the phones:

+7 (495) 725-25-44 (*in the voice menu press 2*)

8 (800) 700-73-00 (*in the voice menu press 4 then 2*)