#### **Guidelines for Generation of the User keys and issue of E-Signature Certificate for Direct Integration Subsystem**

1. **Install CryptoPro CSP client module**

To work with e-signature certificates in Direct Integration remote banking subsystem, CryptoPro CSP software, **version 4.х or higher**, shall be installed on the client side. The Client shall buy this software on its own (information about the recent version of the software is available at the developer’s website: <https://www.cryptopro.ru/products/csp_5_0>). If the specified software is installed on the client side, go to section 2 of these Guidelines for Generation of the User E-Signature Certificate

* 1. Start CryptoPro CSP installation wizard – CSPSetup.exe.



* 1. Press *Install* button.



* 1. Wait until the installation is over.



* 1. Press *OK* button.

Attention! To work with JaCarta 2 GOST crypto tokens, use CryptoPro CSP version 4.0.9963:



1. **Generate a request for the user e-signature certificate on the Client side**

**!Important!**

Before generating of a request check the following operational system settings: the language of programs that do not support Unicode – is «Russian (Russia)».



The Client’s user e-signature certificates are generated and installed on a separate page at <https://www.bankline.ru/servlets/ibc-new?pagename=GenCert>

To test interaction between the Client and the Bank using Direct Integration remote banking subsystem, the system users can use the Subsystem test rig and generate a test certificate at <https://www6.bankline.ru/servlets/ibc-test-new?pagename=GenCert>

Sequence of actions:

* 1. Make sure that the plug-in for work with pre-installed CryptoPRO CSP is set up. Download and run the RequCertPlugin plug-in installer if necessary.



You could check if the RequCertPlugin has been installed and the current version of the plugin by launching the Control panel -> Programs and features.



* 1. Enter the data received from the Bank (employees): Client Code (for example, 1234567890), User Code (for example, 1234567890iii) and user full name (for example, Ivanov Ivan Ivanovich) and press *Log in* button. IMPORTANT: The Client Code and the User Code shall be obtained from the Bank employee. The entered data are case-sensitive.



* 1. Check the filled client data.

While using file exchange (FTPs, Transit 2.0 channels) the field Type of Certificate («Тип сертификата») must contain the value For signature and encryption («Для подписи и шифрования»).

If all the data is correct, press *Generate request* button. If the filled data is incorrect, press *Back* button and address the Bank employee.



* 1. In the displayed Key Generation screen, keep GOST Cryptoprovider and press *OK*  button.



* 1. In CryptoPro CSP screen, choose the media type (registry, local / removable disk / crypto token) and press *OK*.



* 1. Technical procedure of cryptographic key generation starts. Move mouse pointer, press keys when the indicator is displayed.



* 1. Upon completion of key generation, a password for the container with the key is requested. Think out, remember and enter the password two times:



* 1. The keys are stored on the media, and the following screen is displayed in My Account:



* 1. Your request is sent to the Bank – the certificate shall be issued by the Bank’s Certification Authority. Press *Return to the certificate generation request page*.
	2. The request will be displayed on the right of the screen in *Certificate requests* section.



* 1. Inform the Bank’s contact person about completion of the user certificate request procedure. The Bank employees will issue the user certificate and notify you.
1. **Install and print the user certificate on the client side**

Once the Bank notifies you of the certificate issue, the certificate shall be installed on the client side.

To do this, login the service page (to generate work certificate – <https://www.bankline.ru/servlets/ibc-new?pagename=GenCert>; to generate test certificate – <https://www6.bankline.ru/servlets/ibc-test-new?pagename=GenCert>) – similarly to Clause 2.1. of this instruction.

* 1. In *Certificate request* section, choose the certificate and press *Install* button.



* 1. An input window appears for you to enter the password for the container with the key:



* 1. Enter the password for the container used in Clause 2.7.

Important! Subject to agreement with your security department, the entered password can be saved and not entered any more. To save the password tick *Save password*.

* 1. Press *OK* so that the window confirming installation of the certificate appears.



* 1. In case of work via Internet Explorer: if the confirmation window does not appear, this means that the browser blocks installation of the certificate. To unblock the installation, go to the browser security setting from My Account (Internet Options-> Security), add website address to Legitimate (click green tick sign, press *Sites* button, press *Add* button). Then, move the security indicator for Legitimate Sites to Low, press *OK* and restart the browser.

Attention! Having installed the certificate, do not forget to return the security level of Legitimate Sites to the one that was installed before implementation of this instruction item.

* 1. Press *Understand*.

After installation, select the certificate – *Print Act report* button will appear.

The system forms the Act automatically. Print the Acknowledgement Report (the report is automatically printed in two (2) copies), sign it and submit to the Bank employee.

The Act could be signed electronically using the channel that allow using of enhanced qualified electronic signature (for example, EDW system Kontur Diadok).

After confirmation of the certificate by the Bank employee, the certificate will become confirmed meaning it is ready for use.



1. **Installation of the bank and certification authority certificates on the client side**
	1. To complete settings of the client workplace, install the Bank and Certification Authority certificates and the certificate revocation list on the Client’s user computer which will be used to interact with the Bank. The specified certificates with open keys of the Bank and the Certification Authority and the revocation list are available as individual files on the website of the Bank (for live environment – at <https://api.rosbank.ru/doc/sertifikaty-prod.zip/d>, for test environment – at <https://api.rosbank.ru/doc/sertifikaty-test.zip/d>).
	2. To install the Certification Authority certificate (certCA\_2012\_256.cer) to *Trusted root certification authorities*. To do this, open in Microsoft Edge *Settings and other* *→ Settings → Privacy, Search and Service → Security → Certificates managing → Trusted root certification authorities*. Add the certificate using *Import...* button (or click the certificate file and press *Install*). Make sure that the Certification Authority certificate is displayed at *Trusted root certification authorities*.
	3. Install the certificate of the Bank (cert\_h2h\_rb\_ib.cer). To do this, open in Microsoft Edge *Settings and other* *→ Settings → Privacy, Search and Service → Security → Certificates managing → Trusted root certification authorities*. Add the certificate using *Import...* button (or click the certificate file and press *Install*). Make sure that the Bank certificate is displayed at *Other users*.
	4. Install the revocation list received from the Bank (for the live environment - file 01032019\_2012256.crl? for the test environment – file crl2012256.crl). To do this, click the file with the mouse right button and choose *Install revocation list (CRL)*.
	5. Check if the certificate of the user is ready for work:
* open the properties of the user certificate, on the "General" tab there is a phrase: "There is a private key for this certificate".



* there are no warnings about the absence of certificates on the "Certification Path" tab.



When all the above actions are performed, the certificate of the Bank and the Certification Authority is installed on the client side, and all installed certificates are ready for use.

1. **Add a new organisation to the holding**

The issued certificate is linked to the organisation which code is used to login this My Account. However, it can be set to sign documents of other organisations. To do this, tick the required certificate in Certificate requests list and press *Add organisation* button.



In the appeared screen, enter the code of the client to be included in the holding (the client authorising this user to sign documents on its behalf according to the assigned signature level) and press *Print report*.



Fill the name of the client in each of two copies of the printed report (not filled automatically).

Submit both copies of the signed and sealed report to the Bank to authorise this user to sign documents on behalf of the added organisation.

The system forms the Act automatically. Fill the name of the client in each of two copies of the printed report (not filled automatically), sign them and submit both copies to the Bank’s authorised employee in order to authorise this user to sign documents on behalf of the added organisation.

The Act could be signed electronically using the channel that allow using of enhanced qualified electronic signature (for example, EDW system Kontur Diadok).