USER GUIDE FOR HOMEBANKING OF PPF banka a.s.

Generating and Renewal of a Signing certificate

Content:

1. Introduction

Terms or phrases capitalised in this Guide have the meaning defined in the article "Definition of Terms" in the *General Business Conditions of PPF banka a.s.* (hereinafter the "GBC") and the *Business Conditions of PPF banka a.s. for the Homebanking* (hereinafter the "SBC"), in the contractual documents, or, where appropriate, the meaning specified in the individual provisions of the GBC and SBC. The current texts of the GBC and SBC can be retrieved from www.ppfbanka.cz.

2. Generating a Signing Key, Requesting the Generation of a Signing Certificate

All Users holding rights for authorization at the Bank need to request a new Signing Certificate themselves.

The Signing Key is used to encrypt documents at the client station and safeguard their secure transmission to the Bank.

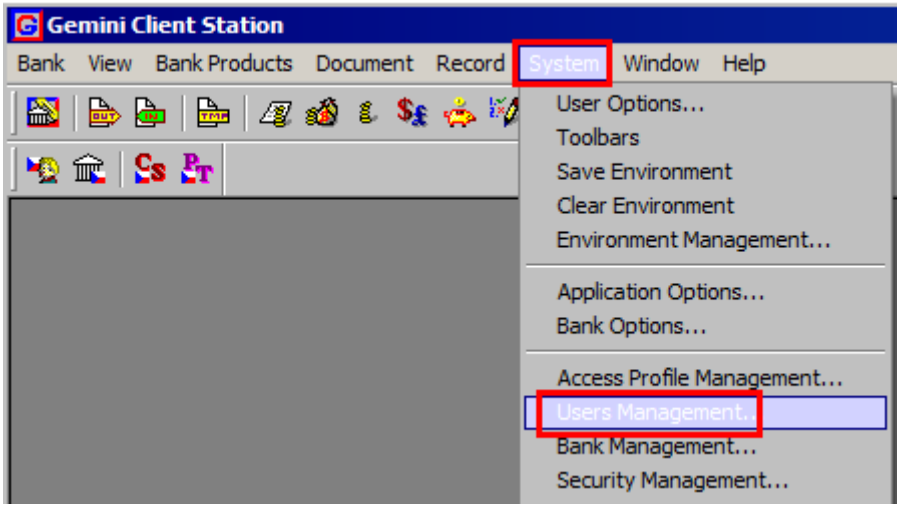
You received an envelope containing a Password for Signing Certificate verification (the envelope labelled with the User's name – inside you will find a "Password for authentication of user signing certificate") from the Bank. This is used to generate the Signing Certificate. **Keep this envelope in a safe place – you will need the Password for Signing Certificate verification to regenerate the Signing Certificate when it expires** (see point 4.).

!!! IMPORTANT !!!

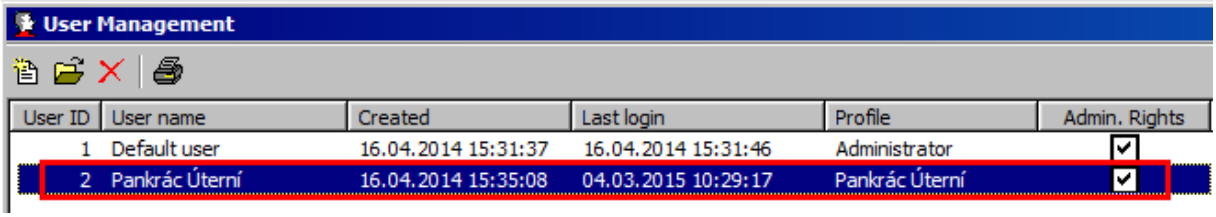
A Signing Certificate is valid for one year. Before expiration of your Transport Certificate, you can renew it according to point 5., when your Signing Certificate expires, you will need to apply for a new one. When you enter the final 14 days period of Signing Certificate validity, you will automatically be alerted to the approaching expiry of your Signing Certificate when you open HB (unless you change this setting in HB).

If your Signing Certificate expires and no new one has been generated, you will no longer be able to authorize and send encrypted documents (especially Payment Orders) to the Bank.

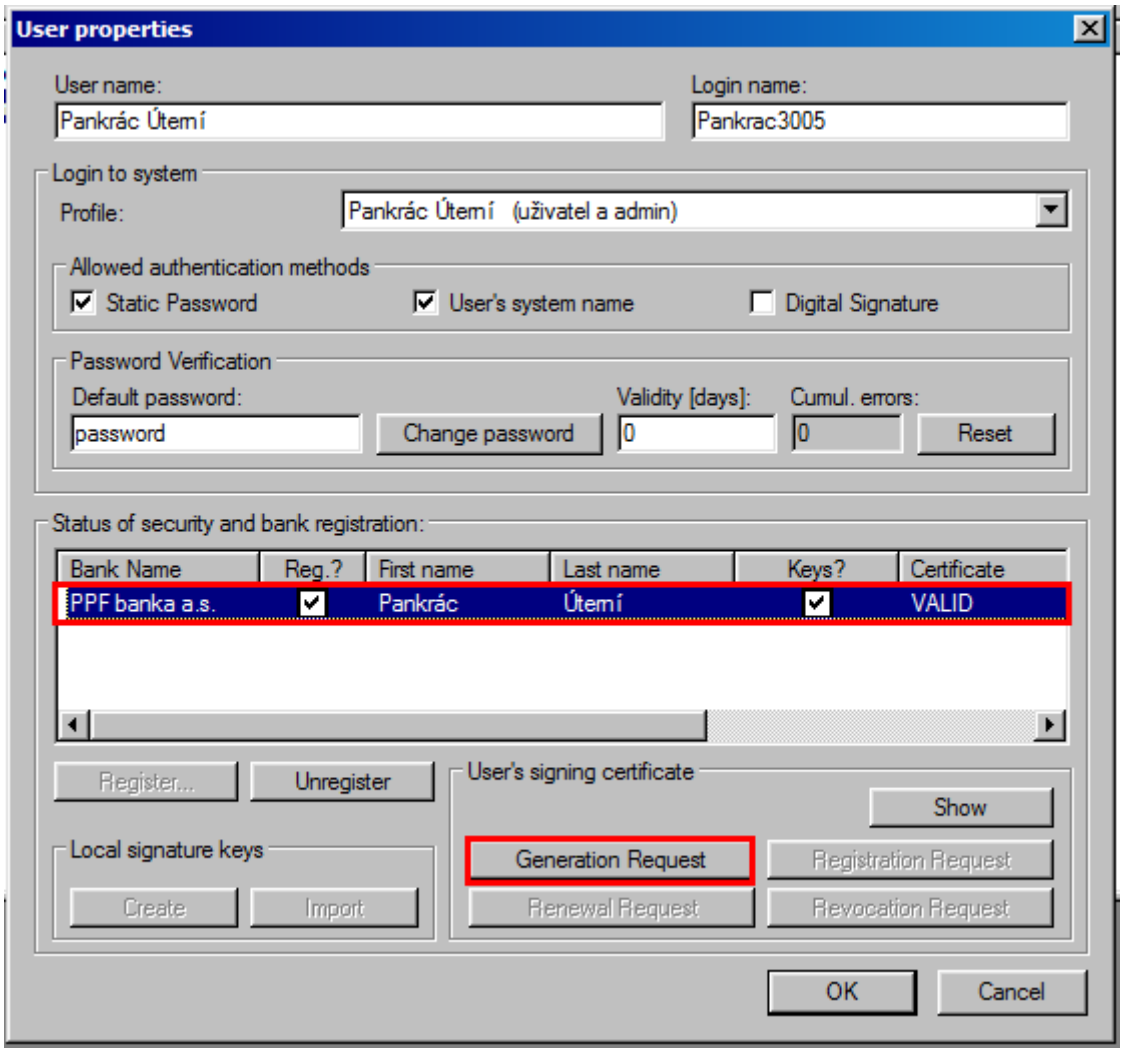
To generate a Signing Key, select **System** in the homepage bar, followed by **Users Management.**



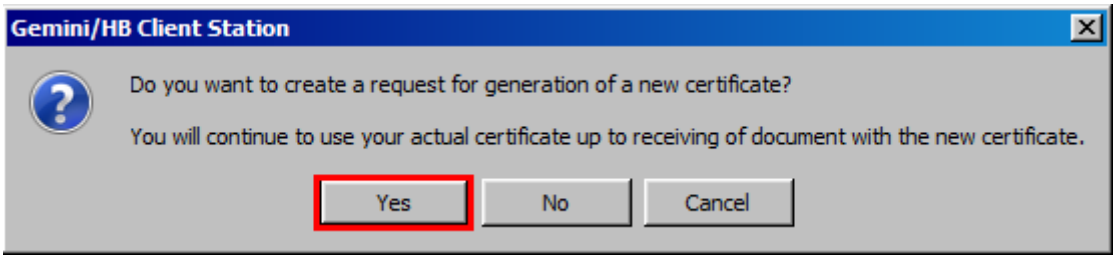
In the window that opens, click on the row with your name and press **Enter**.



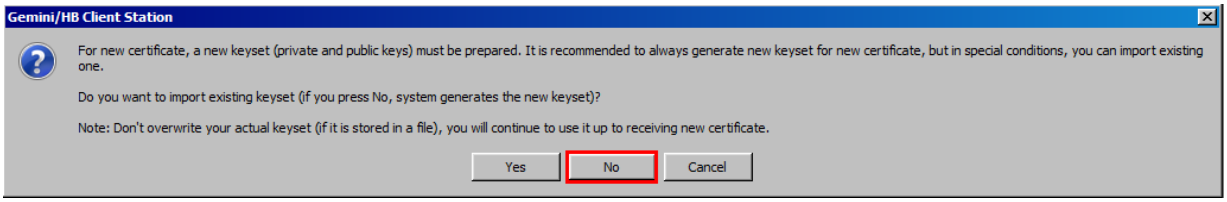
A window with User Properties is displayed. Under **Status of security and bank registration**, press on the row with your name and, under **User's signing certificate**, click the button **Generation request**.



This activates the system question **Do you want to create a request for generation of a new certificate?** – press the **Yes** button to confirm.

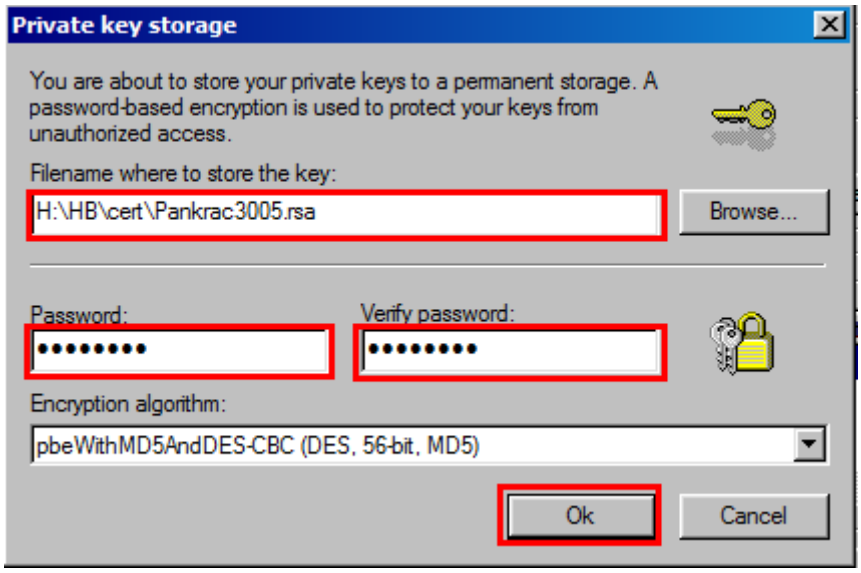


A system question is then displayed asking whether you wish to import an existing key set – refuse the import by pressing **No**.



In the next window, enter the file name and path (use the **Browse** button) to save the Signing Key. **For security reasons, we recommend saving the Signing Key on an external drive** (preferably USB) in the exclusive possession of the User, and that the User store it in a safe place whenever it is not required for authorisation in HB. **If you follow this advice, it is then essential that, when generating the Signing Certificate, you keep the external drive connected to the computer for the entire process, i.e. until you receive confirmation back from the Bank that the Signing Certificate has been successfully generated.**

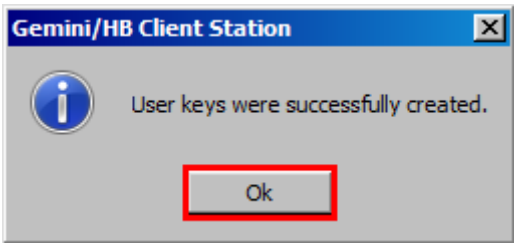
After this, enter the **Password to Signing Key** in the **Password** and **Verify password** boxes and press **Ok**.



!!! IMPORTANT !!!

The Password to Signing Key is an alphanumeric code which you set yourself and which you will then be required to enter whenever you need to authorise (sign) documents and Payment Orders sent to the Bank. Therefore, be sure to remember it.

The system message **User keys were successfully created** will appear. Close this message by pressing **Ok**.

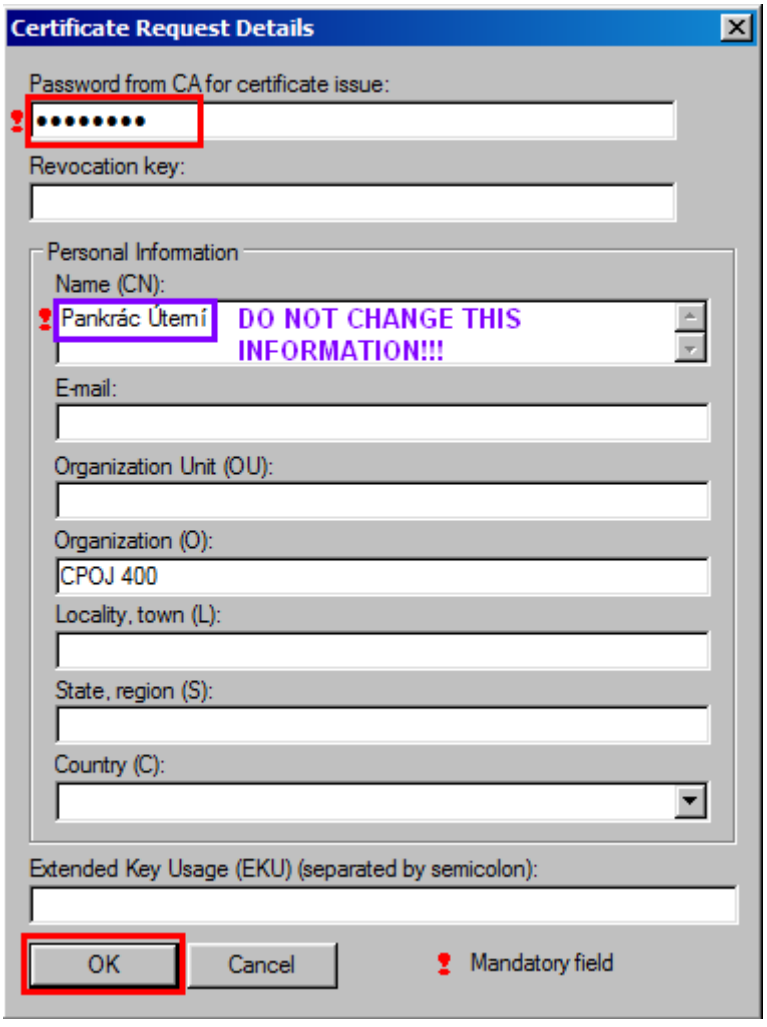


A table with the Signing Certificate request is displayed. Fill in the table as follows – **FILL IN DATA IN THE FIELD "Password from CA for certificate issue", DO NOT ALTER THE OTHER DATA**:

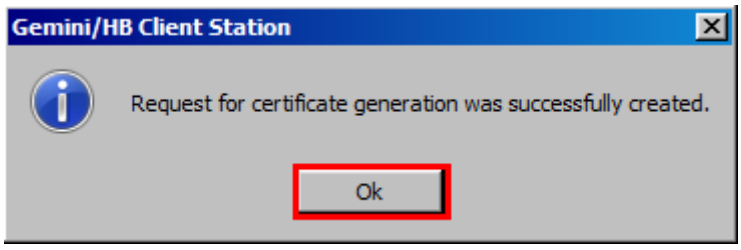
Field	Information required
Password from CA for certificate issue	Enter the **Password for Signing Certificate verification** you received in a separate envelope from the Bank (the envelope labelled with the User's name – inside you will find a "Password for authentication of user signing certificate").
Revocation key	Leave blank.
Name (CN)	The given name and surname of the User for whom the Signing Certificate is being generated is filled in automatically – **DO NOT CHANGE THIS INFORMATION!!!**

Field	Information required
E-mail (E)	Optional.
Organization Unit (OU)	Optional.
Organization (O)	Optional. The name of the Contact Person indicated in the HB documentation is automatically filled in – this may be changed.
Locality, town (L)	Optional.
State, region (S)	Optional.
Country (C)	Optional.
Extended Key Usage (EKU)	Leave blank.

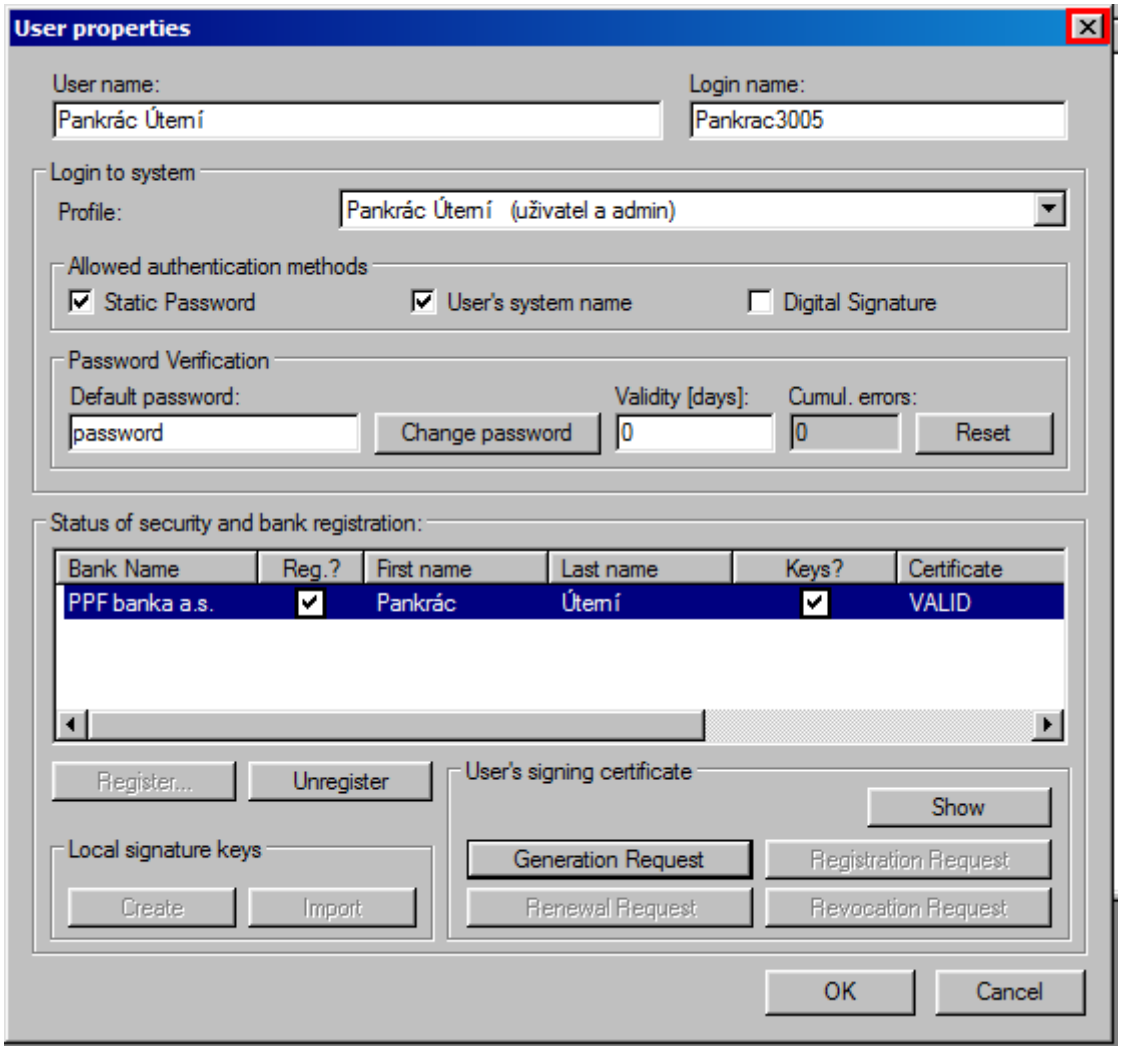
Once you have filled in the information, press **OK**.



Close the system message notifying you of the successful generation of the request by pressing **Ok**.



Close the User admin window by clicking on the cross in the top right-hand corner.



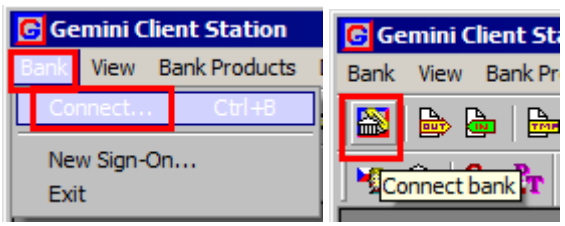
To send the Signing Certificate request and to receive the generated Signing Certificate, connect with the Bank by following the instructions in point 3.

3. Connecting with the Bank

Before connecting with the Bank, make sure that the NCM software is running on the computer you wish to use to communicate with the Bank. If NCM is on the same computer, there is no need to take any related action. If NCM is server-based, set the service to run automatically – it will run until it is closed manually.

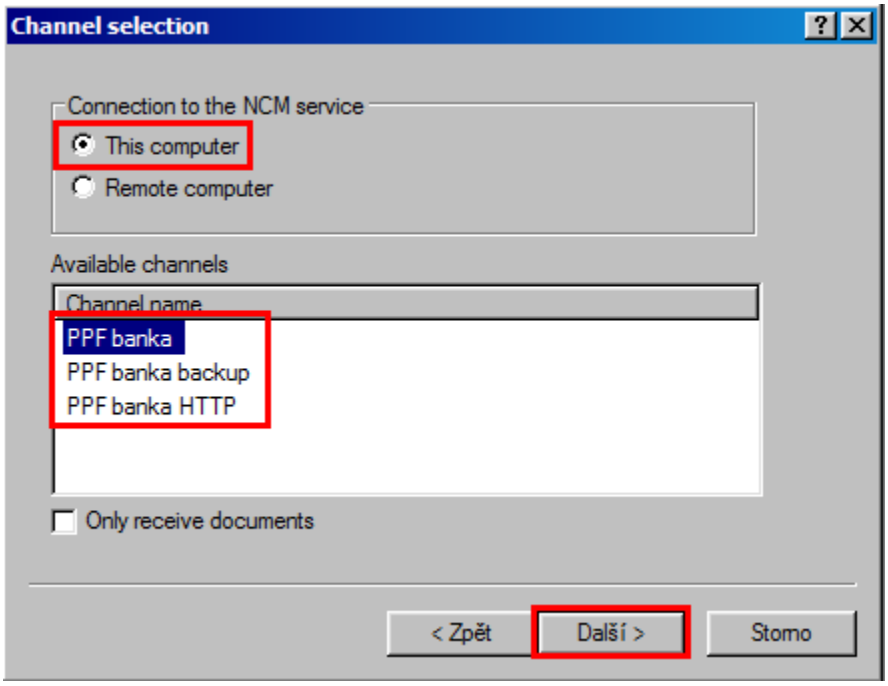
Proceed as follows to make the connection:

1. Make the connection with the Bank by selecting **Bank** from the menu, followed by **Connect**. Alternatively, click on the **Connect bank** icon under the **Bank** option, or use the shortcut **Ctrl+B**.

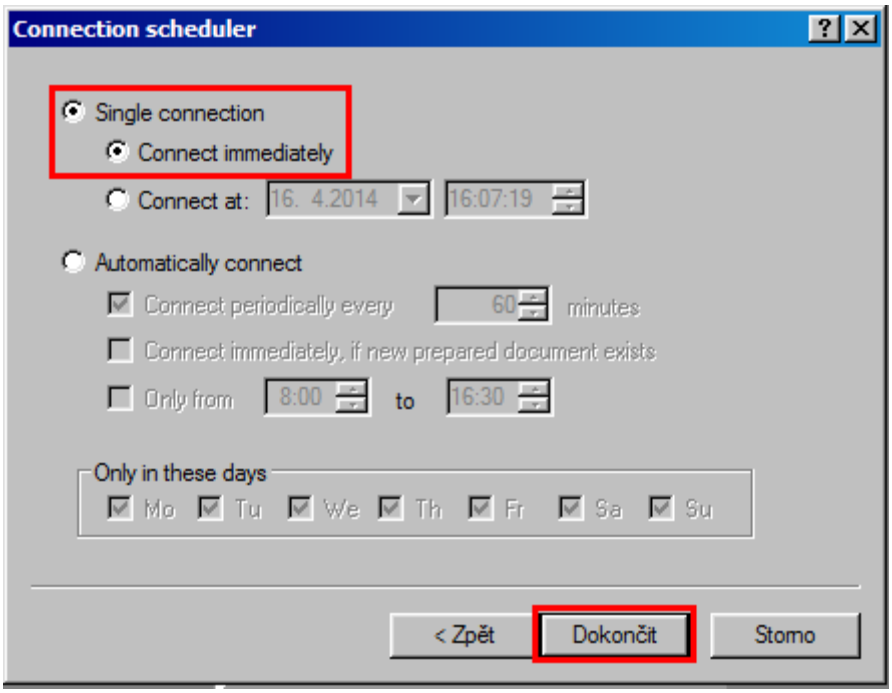


2. In the first dialogue window, select the Bank connection (NCM). In **Connection to the NCM service**, select **This computer**. In the **Available channels** part of the window, a list of defined

channels is displayed. Select the channel (the type of connection) you require. After selecting the required parameters, press **Next (Další)** to proceed to the next window.



3. In the next window, you choose what time the connection is to take place. Select **Single connection** and **Connect immediately** and press **Finish (Dokončit)**.



The GCC software, used to communicate with the Bank, will then be run. The window that is displayed presents all information on the connection in progress. If connections are made to multiple banks, in the top part of the window you need to select the bank you wish to link to. The individual parts of the window display information about documents waiting to be sent, on documents received and sent, and – at the bottom of the window – details of connection tasks.

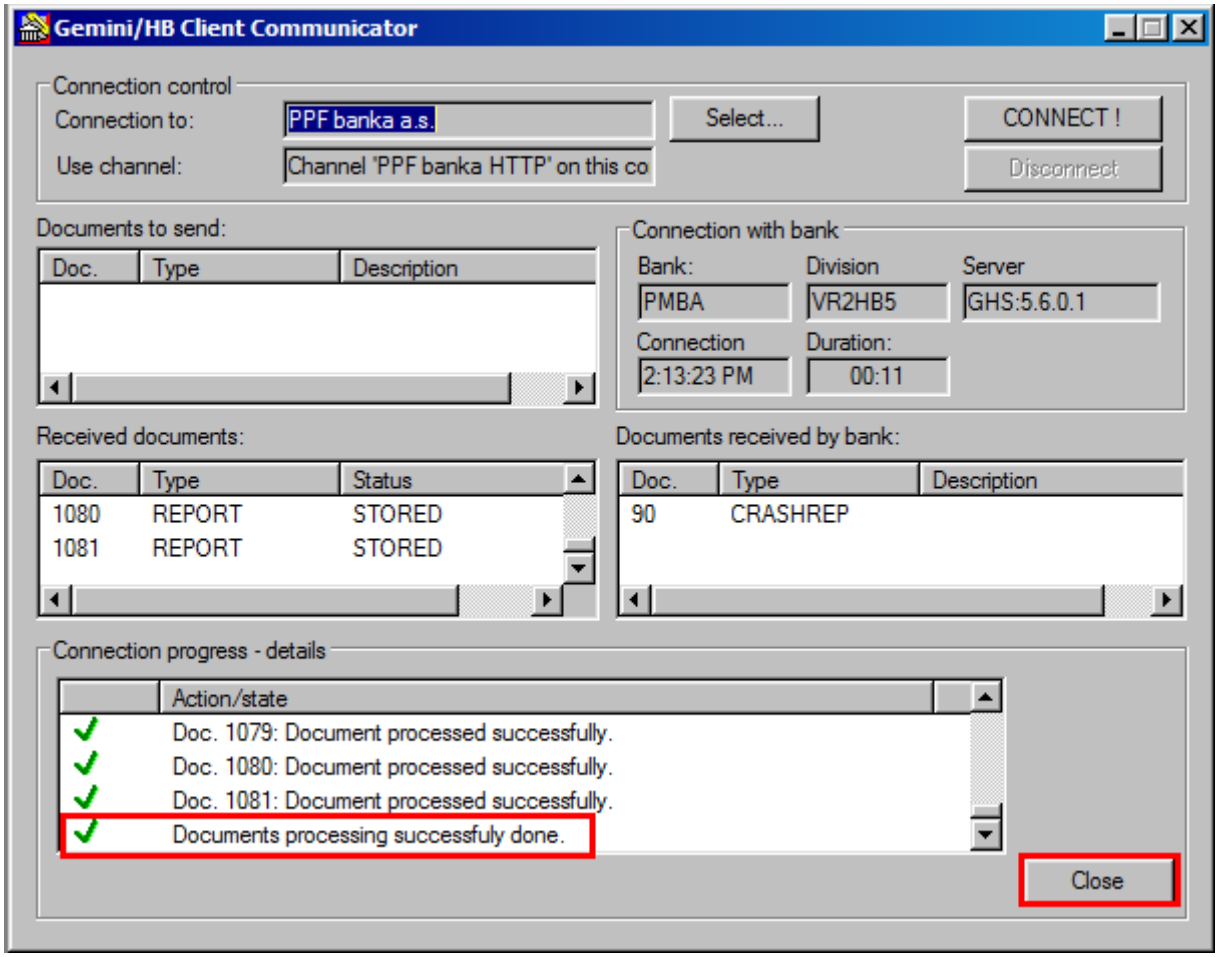
When all of the necessary documents have been successfully transmitted, the message **Documents processing successfully done** is displayed in the section **Connection progress – details**.

!!! IMPORTANT !!!

You need to connect with the Bank at least twice – once to send a Signing Certificate request, and then to receive the generated Signing Certificate.

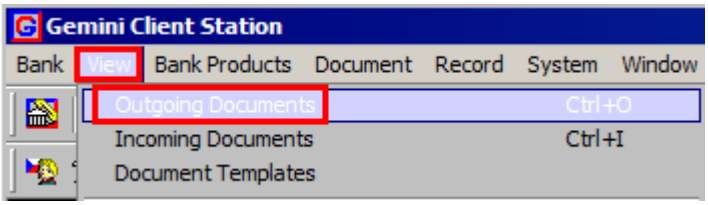
During the first connection, the request for a Signing Certificate for User Signing Keys is transmitted to the Bank. During the second connection, a Signing Certificate is delivered in the opposite direction. It is stored in accordance with the parameters entered and is used to encrypt documents sent to the Bank.

Close the window by pressing **Close**.

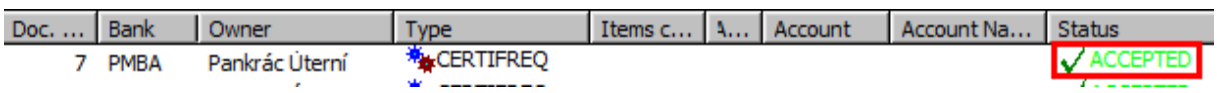


If document transmission fails, try to repeat the connection or contact Customer Support.

Check for the receipt of the generated Signing Certificate under **View** – **Outgoing documents**.



In the **CERTIFREQ** row of the **Status** column, check whether the Signing Certificate request status is **ACCEPTED**. If so, you may now use the new Signing Certificate.



If the status is **FAILED**, repeat the entire procedure and pay close attention when entering the passwords.

4. Regenerating a Signing Key and Signing Certificate

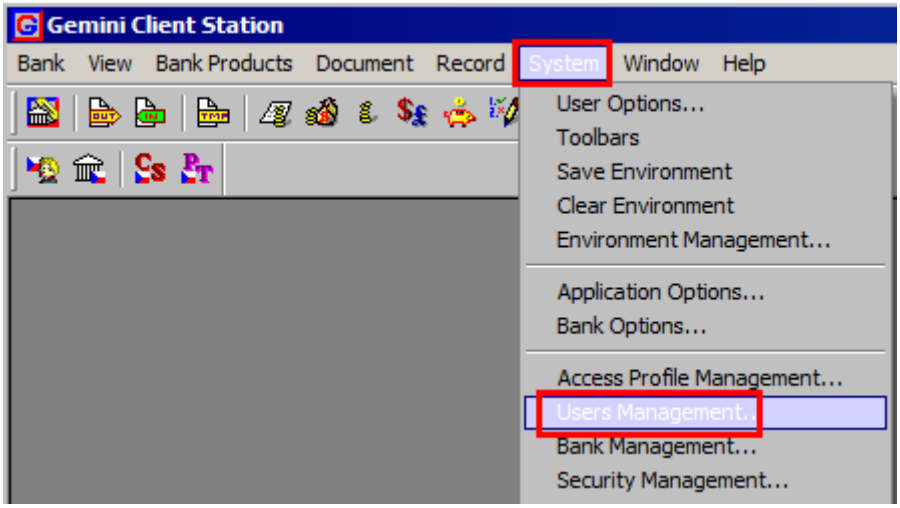
To generate a new Signing Key and to request the generation of a new Signing Certificate, follow the instructions in points 2. and 3. To generate a new Signing Certificate, use the Password for Signing Certificate you received in a separate envelope from the Bank the first time you generated a certificate. If you no longer have the Password for Signing Certificate, you must first ask the Bank to send you a new **Password for Signing Certificate verification**.

If you do not generate a new Signing Key or request the generation of a new Signing Certificate before they expire, you will not be able to authorise documents sent to the Bank (see point 2. above).

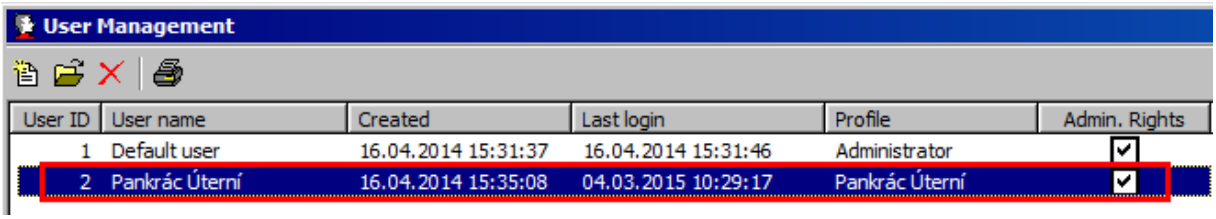
Documents sent to the Bank cannot then be authorised until a new Signing Key is generated and a new Signing Certificate has been received.

5. Renewal of a Signing Key and a Signing Certificate

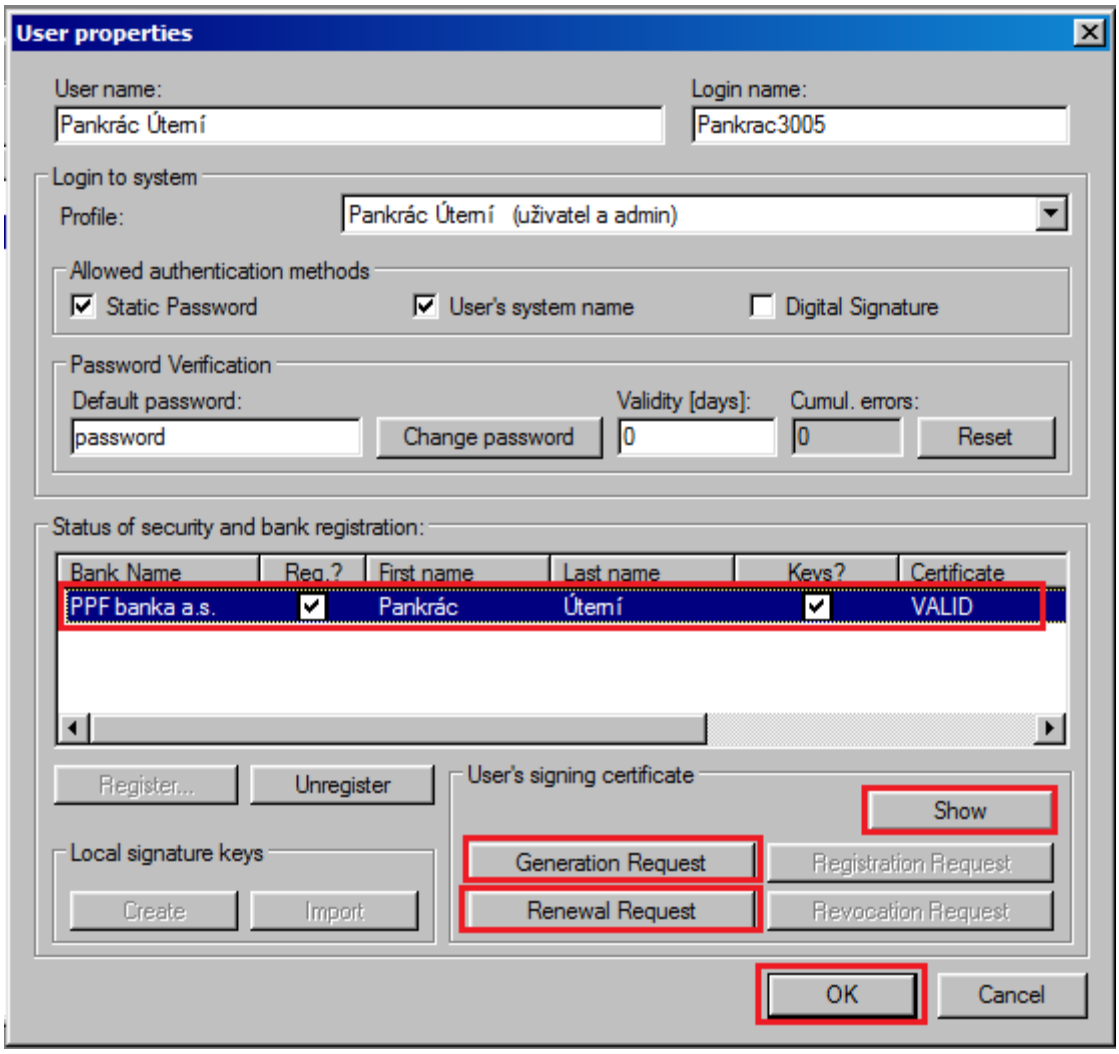
Signing Key and Signing Certificate can be renewed before their expiration. To renew a Signing Key, select **System** in the homepage bar, followed by **Users Management.**



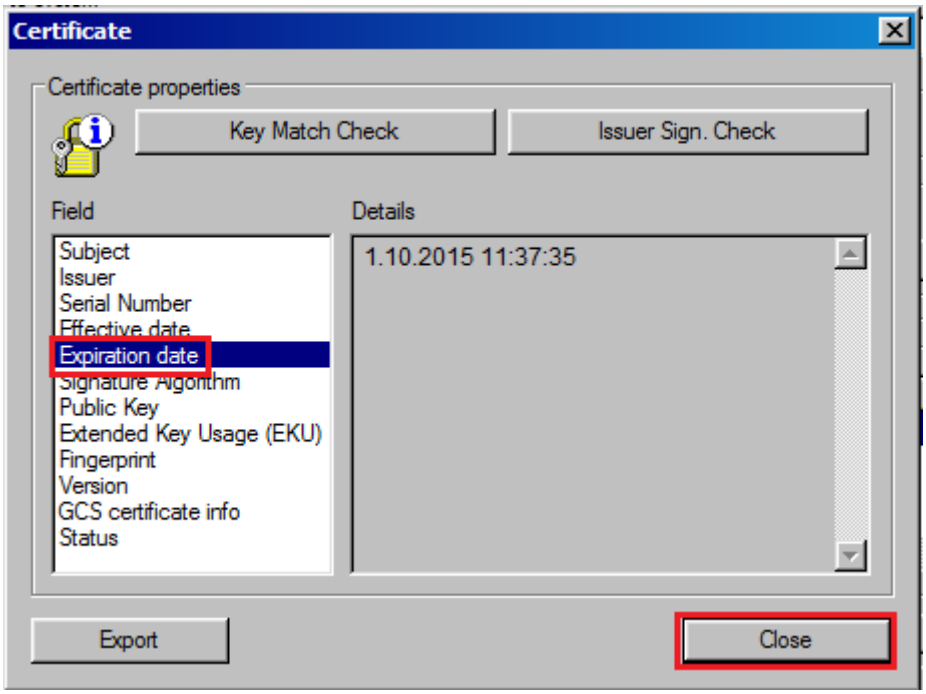
In the window that opens, click on the row with your name and press **Enter**.



A window with User Properties is displayed. Under **Status of security and bank registration**, press on the row with your name – buttons **Show**, **Generation request** and **Renewal request** are activated in part **User's signing certificate**.



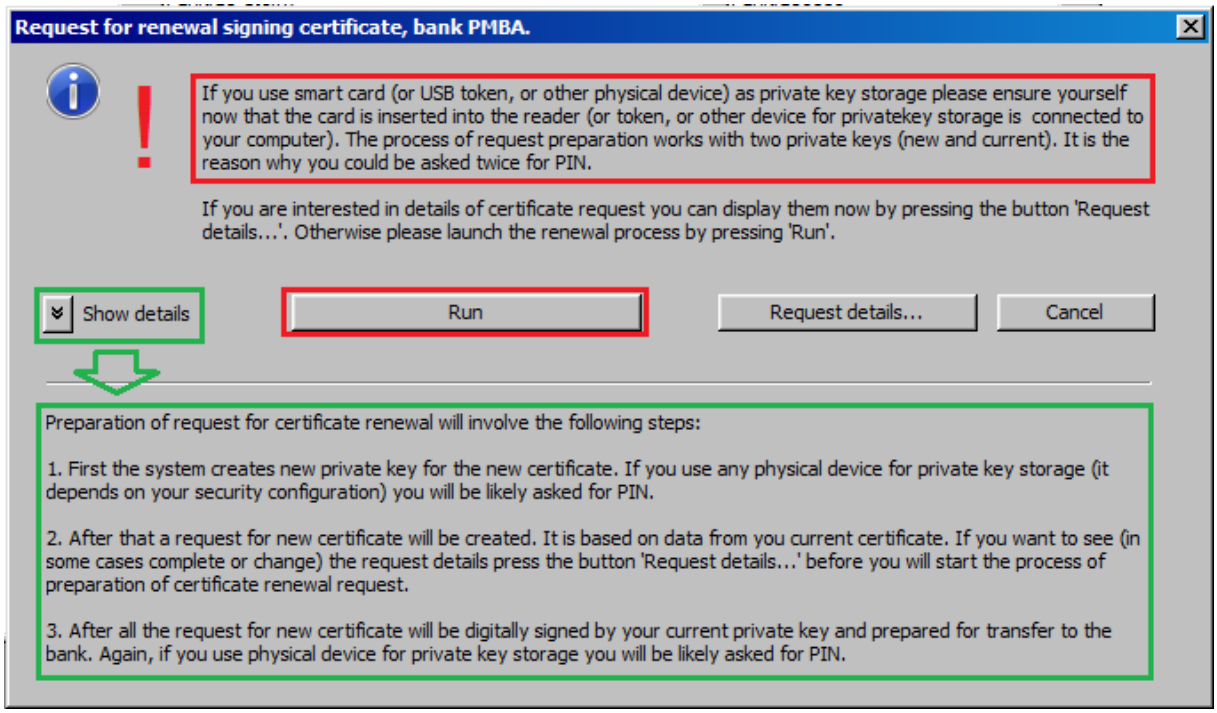
By clicking on the button **Show**, you can check validity of your Signing Certificate in the field **Expiration date**. Close this window by pressing button **Close**.



If Signing Certificate is expired, it is necessary to generate the new one – in this case continue by clicking on the button **Generation request** and then follow point 2.

In case the Signing Certificate is still valid, you can renew it by clicking on the button **Renewal request**. First, a warning on the method of setting the Signature key appears – **read this notice carefully and follow it!!!** You can also display details of Signature Certificate renewal process by clicking on the arrows at the text **Show details**.

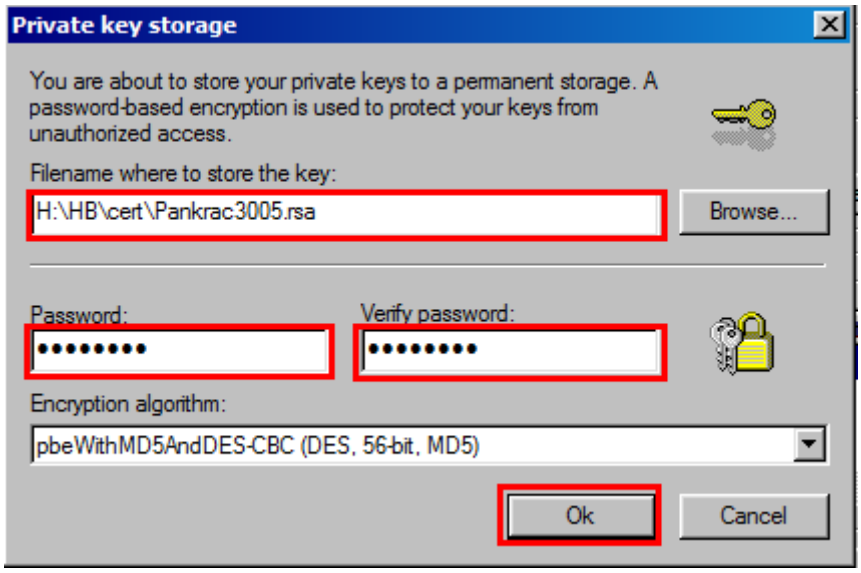
Click on the button **Run** for renewal of Signing Key and Signing Certificate.



In the next window, enter the file name and path (use the **Browse** button) to save newly generated Signing Key. **File name and/or path has to differ from the saving of existing Signing Key otherwise it will not be possible to process request for renewal!!!**

For security reasons, we recommend saving the Signing Key on an external drive (preferably USB) in the exclusive possession of the User, and that the User store it in a safe place whenever it is not required for authorisation in HB. **If you follow this advice, it is then essential that, when generating the Signing Certificate, you keep the external drive connected to the computer for the entire process, i.e. until you receive confirmation back from the Bank that the Signing Certificate has been successfully generated.**

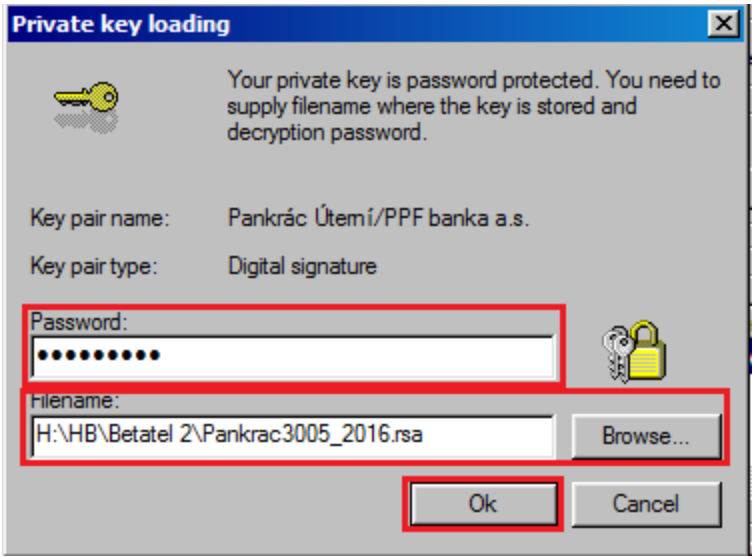
After this, enter the **Password to Signing Key** in the **Password** and **Verify password** boxes and press **Ok**.



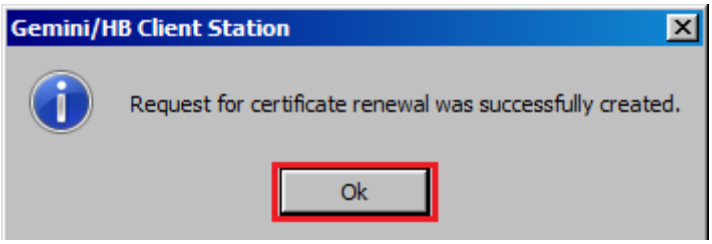
!!! IMPORTANT !!!

The Password to Signing Key is an alphanumeric code which you set yourself and which you will then be required to enter whenever you need to authorise (sign) documents and Payment Orders sent to the Bank. Therefore, be sure to remember it.

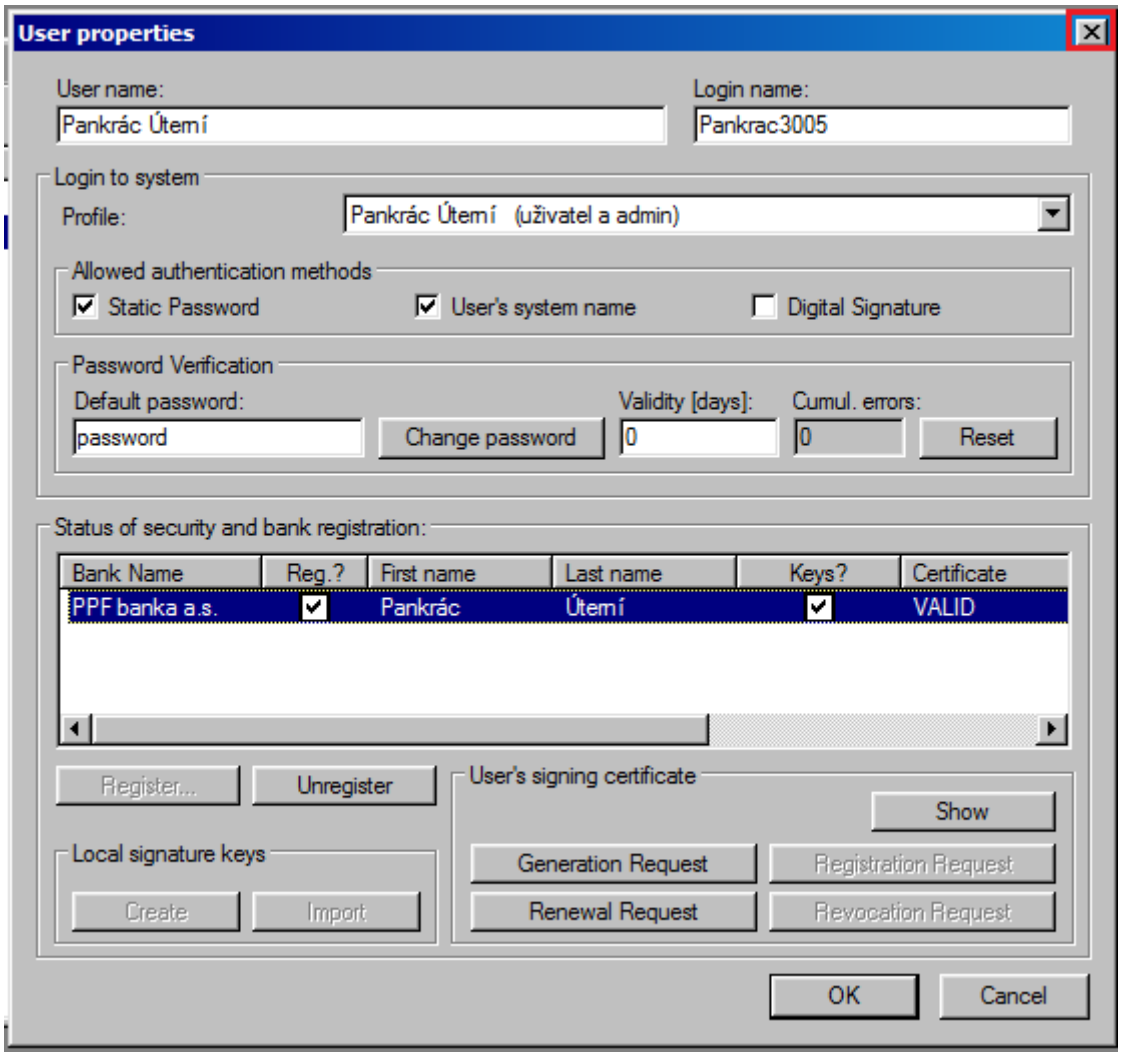
Enter current Password to Signing Key in the **Password** box and the file name and path (use the **Browse** button) to save it. Confirm entered data by clicking on the button **OK**.



Close the system message notifying you of the successful generation of the request by pressing **Ok**.

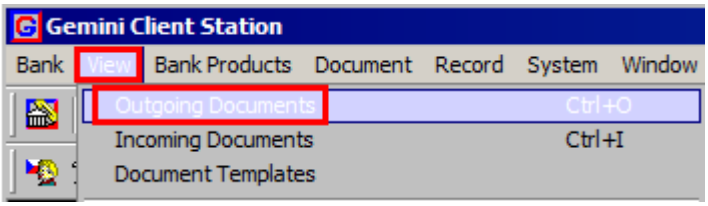


Close the User admin window by clicking on the cross in the top right-hand corner.

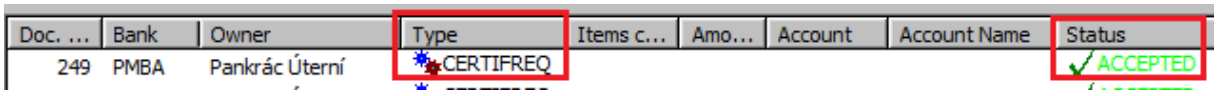


To send the Signing Certificate request and to receive the generated Signing Certificate, connect with the Bank by following the instructions in point 3.

Check for the receipt of the generated Signing Certificate under **View** – **Outgoing documents**.



In the **CERTIFREQ** row of the **Status** column, check whether the Signing Certificate request status is **ACCEPTED**. If so, you may now use the new Signing Certificate.



If the status is **FAILED**, repeat the entire procedure and pay close attention when entering the passwords.