

## USER GUIDE FOR HOMEBANKING OF PPF banka a.s.

Generating and Renewal of a Signing certificate



### **Content:**

1.	Introduction	3
2.	Generating a Signing Key, Requesting the Generation of a Signing Certificate	3
3.	Connecting with the Bank	7
4.	Regenerating a Signing Key and Signing Certificate	. 10
5.	Renewal of a Signing Key and a Signing Certificate	. 10



### 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 <u>www.ppfbanka.cz</u>.

## 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. <u>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.).</u>

#### !!! IMPORTANT !!!

A Signing Certificate is valid for one year. Before expiration of your Transport Certificate, you can renew it according to point <u>5.</u>, 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.

	🔁 User Management								
"B 🚅 🗙 🎒									
	User ID	User name	Created	Last login	Profile	Admin. Rights			
I	1	Default user	16.04.2014 15:31:37	16.04.2014 15:31:46	Administrator				
l	2	Pankrác Úterní	16.04.2014 15:35:08	04.03.2015 10:29:17	Pankrác Úterní				



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**.

r propercies					
User name:			Log	jin name:	
Pankrác Útem í			Par	nkrac3005	
ogin to system					
Profile:	Pa	nkrác Útemí	(uživatel a admin)		
Allowed authoritizati	mathada				
Static Password	on methous	V Hear's	austem name	Digital Sig	esture
I♥ Static Password		It Users	system name	Digital big	nature
Password Verification	n				
Default password:			Validity (day	/s]: Cumul. er	rors:
password		Change pa	issword 0	0	Reset
Status of security and	bank registr	ation:			
Bank Name	Reg.?	First name	Last name	Keys?	Certificate
PPF banka a.s.	<b>V</b>	Pankrác	Útemí	Image: A state of the state	VALID
•					
Register	Upregiet	~   User	r's signing certificate		
Hegister	Onregist				Show
			Constition Request	Registr	stien Request
Local signature keys			Generation Request	negisu	adonmequest
Local signature keys					
- Local signature keys	Import		Renewal Request	Revoc	ation Request
Create	Import		Renewal Request	Revoc	ation 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.

Gemini/HB Client Station								
?	Do you want to create a request for generation of a new certificate? You will continue to use your actual certificate up to receiving of document with the new certificate.							
	Yes	No	Cancel					

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

Gemini/H	HB Client Station
?	For new certificate, a new keyset (private and public keys) must be prepared. It is recommended to always generate new keyset for new certificate, but in special conditions, you can import existing one.
	Do you want to import existing keyset (if you press No, system generates the new keyset)?
	Note: Don't overwrite your actual keyset (if it is stored in a file), you will continue to use it up to receiving new certificate.
	Yes No Cancel



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**.

Private key storage	×
You are about to store your private keys to a permanent storage. A password-based encryption is used to protect your keys from unauthorized access.	<b></b>
Filename where to store the key:	
H:\HB\cert\Pankrac3005.rsa	Browse
·	
Password: Verify password:	a <mark>O</mark>
••••••	
Encryption algorithm:	•
pbeWithMD5AndDES-CBC (DES, 56-bit, MD5)	•
Ok	Cancel

#### !!! 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 – <u>FILL IN DATA IN</u> <u>THE FIELD "Password from CA for certificate issue", DO NOT ALTER THE OTHER DATA</u>:

Field	Information required
Password from CA for certificate issue	Enter the <b>Password for Signing Certificate verification</b> 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 – <u>DO NOT</u> <u>CHANGE THIS INFORMATION!!!</u>



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.

Certificate Request Details
Password from CA for certificate issue:
2
Revocation key:
Personal Information Name (CN):
Pankrác Útemí DO NOT CHANGE THIS
INFORMATION!!!
E-mail:
Organization Unit (OU):
Organization (O):
CPOJ 400
Locality, town (L):
State, region (S):
Country (C):
Extended Key Usage (EKU) (separated by semicolog):
OK Cancel 2 Mandatory field

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.

Jser name:			Log	gin name:	
Pankrác Útemí			Pa	ankrac3005	
ogin to system					
Profile:	Par	nkrác Útemí (	uživatel a admin)		
Allewed authoriticativ	en methodo				
Allowed authenticatio	on methous		wetern name	Digital Si	an sture
			system name	) Di Digitar Dij	griduore
Password Verification	1				
Default password:			Validity (da	iys]: Cumul. e	errors:
password		Change pas	sword 0	0	Reset
Status of security and I	hank registra	ation:			
Deels News	Dec 2	Dark serves	Lastana	Kaua 2	Catificate
Bank Name	Reg.?	First name	Last name	Keys?	Certificate
Bank Name PPF banka a.s.	Reg.?	First name Pankrác	Last name Útemí	Keys?	Certificate VALID
Bank Name PPF banka a.s.	Reg.?	First name Pankrác	Last name Útemí	Keys?	Certificate VALID
Bank Name PPF banka a.s.	Reg.?	First name Pankrác	Last name Útemí	Keys?	Certificate VALID
Bank Name PPF banka a.s.	Reg.?	First name Pankrác	Last name Útemí	Keys?	Certificate VALID
Bank Name PPF banka a.s.	Reg.?	First name Pankrác	Last name Útemí s signing certificate —	Keys?	Certificate VALID
Bank Name PPF banka a.s.	Reg.?	First name Pankrác	Last name Útemí s signing certificate —	Keys?	Certificate VALID
Bank Name PPF banka a.s.  Fregister Local signature keys	Reg.?	First name Pankrác	Last name Útemí s signing certificate — Generation Request	Keys?	Certificate VALID
Bank Name PPF banka a.s.  Hegister Local signature keys	Reg.?	First name Pankrác er User's	Last name Útemí s signing certificate – Generation Request	Keys?	Certificate VALID
Bank Name PPF banka a.s.  Hegister Local signature keys Create	Reg.?	First name Pankrác er User's	Last name Útemí s signing certificate Generation Request Renewal Request	Keys?	Certificate VALID Show tration Request
Bank Name PPF banka a.s.  Fregister Local signature keys Create	Reg.?	First name Pankrác	Last name Útemí s signing certificate Generation Request Renewal Request	Keys?	Certificate VALID Show tration Request cation Request

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

### 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.

Channel selection	? ×
Connection to the NCM service This computer Remote computer	
Available channels	
PPF banka PPF banka backup PPF banka HTTP	
Only receive documents	
< Zpět Další > S	tomo

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)**.

Connection scheduler	? ×
Single connection	
Connect immediately	
C Connect at: 16. 4.2014 🔽 16:07:19 😴	
C Automatically connect	
Connect periodically every 60 🚔 minutes	
Connect immediately, if new prepared document exists	
Conly from 8:00 😴 to 16:30 😴	
Only in these days	
🗹 Mo 🗹 Tu 🕅 We 🗹 Th 💌 Fr 🗹 Sa 🗹 Su	
< Znět Dokončit	Stomo
	otomo

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**.

Gemini/HB Client Communicator				
Connection control Connection to: PPF banka a.s. Use channel: Channel 'PPF banka H	TTP' on this co	Select		CONNECT ! Disconnect
Documents to send: Doc. Type Description	Ba Pi Co Pi Co 2:	nnection with I nk: MBA nnection 13:23 PM	bank Division VR2HB5 Duration: 00:11	Server GHS:5.6.0.1
Received documents:	Docu		ed by bank:	Description
1080 REPORT STORED 1081 REPORT STORED	90	CRASI	HREP	
Connection progress - details				
Action/state  Control	uccessfully. uccessfully. uccessfully. done.			

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.

📴 Gemini Client Station									
Bank	View	Bank Products	Document	Record	System	Window			
1 🔜 1	0 U	tgoing Document	s		Ctrl-	+O			
	Inc	coming Document	s		Ctrl+	+I			
- Mg 1	Do	cument Template	s						

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.

Doc	Bank	Owner	Туре	Items c	A	Account	Account Na	Status
7	PMBA	Pankrác Úterní	CERTIFREQ					ACCEPTED
			*					1

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 <u>2</u>, and <u>3</u>. 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 <u>2</u>. 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.

📱 U:	ser	Management				
<b>è</b>	Ĵ.	×   S				
User	· ID	User name	Created	Last login	Profile	Admin. Rights
	1	Default user	16.04.2014 15:31:37	16.04.2014 15:31:46	Administrator	
	2	Pankrác Úterní	16.04.2014 15:35:08	04.03.2015 10:29:17	Pankrác Úterní	

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**.



er properties					
User name:			Log	in name:	
Pankrác Útemí			Par	nkrac3005	
login to system					
Profile:	P	ankrác Úterní (	(uživatel a admin)		•
Allowed authenticat	on method	s	water eare	Diatal Sia	
Je Static Password		I♥ Users :	system name	I Digital Sig	inature
Password Verification	n				
Default password:			Validity [day	rs]: Cumul.er	rrors:
password		Change pas	sword 0	Jo	Reset
Bank Name PPF banka a.s.	Reg.?	First name Pankrác	Last name Útemí	Kevs?	Certificate VALID
L .					
					F
Register	Unregis	ter User	s signing certificate —		
				L	Show
Local signature key:	3		Generation Request	Regist	ration Request
Create	Impor		Renewal Request	Revoc	ation Request
				OK	Crowd
				UK	Cancel

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**.

Certificate				×
Certificate properties Key Match C	Check	lssuer	Sign. Check	
Subject Issuer Serial Number Effective date Signature Algorithm Public Key Extended Key Usage (EKU) Fingerprint Version GCS certificate info Status	1.10.2015 11:	37:35		×
Export			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 – <u>read this notice</u> <u>carefully and follow it!!!</u> 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.

Request for rene	ewal signing certificate, bank PMBA.	×						
If you use smart card (or USB token, or other physical device) as private key storage please ensure yourself now that the card is inserted into the reader (or token, or other device for privatekey storage is connected to your computer). The process of request preparation works with two private keys (new and current). It is the reason why you could be asked twice for PIN.								
If you are interested in details of certificate request you can display them now by pressing the button 'Request details'. Otherwise please launch the renewal process by pressing 'Run'.								
Show detai	ils Run Request details Cancel							
Preparation of	request for certificate renewal will involve the following steps:							
1. First the syst depends on you	1. First the system creates new private key for the new certificate. If you use any physical device for private key storage (it depends on your security configuration) you will be likely asked for PIN.							
2. After that a request for new certificate will be created. It is based on data from you current certificate. If you want to see (in some cases complete or change) the request details press the button 'Request details' before you will start the process of preparation of certificate renewal request.								
3. After all the bank. Again, if	request for new certificate will be digitally signed by your current private key and prepared for transfer to the you use physical device for private key storage you will be likely asked for PIN.							

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

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**.



PPF	Banka

Private key storage	×
You are about to store your private keys to a permanent storage. A password-based encryption is used to protect your keys from unauthorized access.	<b>=</b> 0
Filename where to store the key:	
H:\HB\cert\Pankrac3005.rsa	Browse
Password: Verify password:	<b>2</b>
Encryption algorithm:	
pbeWithMD5AndDES-CBC (DES, 56-bit, MD5)	•
Ok	Cancel

#### **!!! 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**.

Private key load	ing	×				
<b>*</b>	Your private key is password protected. You need to supply filename where the key is stored and decryption password.					
Key pair name:	Pankrác Útem í/PPF banka a.s.					
Key pair type:	Digital signature					
Password:		P				
Hiename: H:\HB\Betatel 2\	Pankrac3005_2016.rsa	Browse				
	Ok	Cancel				

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.



er properties					
User name:			Logir	name:	
Pankrác Útemí			Panl	krac3005	
Login to system					
Profile	Pankr	ác Útemí (u	živatel a admin)		
Tronic.	1. 0	Jo otonni ya	Ervator a daminy		
Allowed authentication	n methods				
Static Password		User's sy	stem name	🗖 Digital Sig	nature
Password Verification					
Default password:			Validity (days	1: Cumul. en	rors:
password		Change pass	word 0	0	Reset
				,	
Status or security and b	ank registration	n:			
Bank Name	Reg.? Firs	t name	Last name	Keys?	Certificate
PPF banka a.s.	✓ Par	ikrac	Utemi	Ľ	VALID
•					
Register	Unregister	User's	signing certificate		
					Show
Local signature keys		G	eneration Request	Registr	ation Request
Create	Incont		Descrived Description		- Very Discourses
	Import		Kenewai Kequesi	nevoo	ation nequest
					_

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.

G Gemini Client Station									
Bank	View	Bank Products	Document	Record	System	Window			
	0	itgoing Document	s		Ctrl-	ю			
	Inc	coming Document	s		Ctrl+	+I			
<b>1 1</b>	Do	cument Template	s						

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.

Doc	Bank	Owner	Туре	Items c	Amo	Account	Account Name	Status
249	PMBA	Pankrác Úterní	CERTIFREQ					✓ ACCEPTED
1			*					1

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