PPF Banka

SECURITY PRINCIPLES FOR THE HOMEBANKING SERVICE of PPF banka a.s.

Contents:

This document sets out principles for the secure use of the Homebanking service (hereinafter "HB") of PPF banka a.s. (hereinafter the "Bank"). We recommend applying these principles on all computers used for HB operations. The Bank accepts no responsibility for any data loss, Personal Data leakage or other events which occur if the recommendations stated below are not followed.

More information about the HB application, Security Principles, Security Elements and the latest security threats can be found on the Internet Website of the Bank and in HB itself, or can be obtained at the Bank's Places of Business, by calling +420 224 175 995, or by writing to the email address customer.service@ppfbanka.cz.

Capitalised terms or phrases used in the text of these Security Principles have the meaning specified in the article "Definition of Terms" in the *General Business Conditions of PPF banka a.s.* (hereinafter the "GBC") and/or in the *Business Conditions of PPF banka a.s. for the Use of Homebanking Services* (hereinafter the "SBC"), or, where applicable, the meaning specified in individual provisions of the GBC or SBC. The current versions of the SBC and GBC are available on the Internet Website at www.ppfbanka.cz.

User support for HB is provided by Customer Service, which you can contact on Business Days from 8.00 a.m. to 6.00 p.m. using the telephone number +420 224 175 955 or at the email address customer.service@ppfbanka.cz.

PPF banka a.s., Praha 6, Evropská 2690/17, Post Code 160 41 Czech Republic, Company ID No. 47116129, VAT No. CZ47116129
Incorporated in the Companies Register of the Municipal Court in Prague, Section B, File 1834
Tel.: (+420) 224 175 888, Fax: (+420) 224 175 980

1. SECURITY FOR HB ACCESS AND AUTHORISATION

The method by which Users log into HB is set by the System Administrator during HB administration. We recommend setting up access using Security Elements which will ensure User authentication (verification of the User's identity) and minimize the risk of abuse of HB access – a HB Username in combination with a HB Login Password.

Payment Orders and requests made to the Bank must always be Authorised using an Electronic Signature. An Electronic Signature consists of encrypted data in electronic form which is attached to submitted data and which enables the verification of a User's identity. It comprises a Signature Certificate and a Signature Key. During Authorisation a User must also enter a Password to the Signature Key.

2. GENERAL SECURITY PRINCIPLES

We recommend making use of the option to set Limits on Payment Orders for all HB Users (more information about Users, setting Limits and Authorisation Rights can be found in the SBC).

Keep Security Elements in a safe place.

Your *Agreement on Homebanking* and its annexes (hereinafter the "Agreement on HB") can also be abused, so treat these documents as confidential, protect them from being lost, and likewise keep them in a safe place.

If you suspect that any Usernames, Passwords or other sensitive data may have been disclosed, your System Administrator should immediately block Users' access to HB. Then contact the Bank's Customer Service and ask them to block HB or access to HB on the Bank's side.

3. SECURITY PRINCIPLES FOR THE USE OF HOMEBANKING

The security of the HB system is only as strong as its weakest link. The HB system consists of the Bank's servers, telecommunications technology used for connection with the Bank and data transmission (modems, the Internet etc.), the User's computer, and the human factor involved.

The Bank's servers are secured by means of server certificates, a system of firewalls, security zones, monitoring devices and other mechanisms, and thus constitute a very strong link in the HB system as a whole.

The next two links - the User's computer and the telecommunications technology used for connection with the Bank and data transmission - are potentially the most vulnerable points of the entire system, because the Bank is not and cannot be responsible for their security. This responsibility lies solely with Clients/Users themselves.

The actual transfer of data from the User's computer to the Bank and vice versa is performed via a secure channel (128-bit SSL). In addition, the data itself is also protected by encryption (1024-bit RSA algorithm) and other security features which ensure the highest possible level of security.

A more difficult issue may be for ordinary Users to secure their computers so that no-one can install programs on them allowing their remote administration, including keylogging (to obtain a password) or copying of files (Certificates). Due attention must therefore be given to the security of the User's computer, potentially including consultation with an expert about security settings. We recommend using antivirus and antispyware software.

A relatively independent issue which may also be the weakest link in security is the "human factor". This involves the fact that a User may disclose important elements of the security system to a potential attacker, who can then exploit them. The security system used for HB (and its other components) should be sufficiently robust that even if some items of sensitive information are disclosed to an unauthorised person it still cannot be abused. The system of Security Elements must always consist of one or more items of data known only to the User, along with additional means used to verify the User's identity (a Certificate and password). Every User should be aware of the sensitivity of all of the items of data used to verify the User's identity in connection with the use of HB, and should under no circumstances divulge this information. The Bank will never ask a User to provide this information other than when the User enters the relevant data into HB.

PPF banka a.s., Praha 6, Evropská 2690/17, Post Code 160 41 Czech Republic, Company ID No. 47116129, VAT No. CZ47116129
Incorporated in the Companies Register of the Municipal Court in Prague, Section B, File 1834
Tel.: (+420) 224 175 888, Fax: (+420) 224 175 980

4. PHISHING

Use only trusted services, and always make sure that you are communicating with the genuine service provider. If you have any doubts about whether you are communicating with the Bank, contact the Bank's Customer Service.

Choose HB passwords which cannot easily be guessed or deduced from personal information about you. The Bank will never ask you to enter or confirm this information via email. If you receive a request made in the Bank's name to provide such information, please notify the Bank's Customer Service of this fact.

Be careful to make sure that you are confirming the Payment Order or request to the Bank which you entered. Before confirming, always check that the information stated is correct (e.g. by cross-checking against the relevant invoice, payment slip etc.).

Regularly check the movements on your accounts and any payment card transactions. Immediately notify the Bank if you find any discrepancies.

Do not open any suspicious emails (messages from unknown senders, messages with meaningless subject lines etc.), and in particular do not open any attachments to such messages. The Bank will never send you any unsolicited messages containing links to its Internet Website. If you receive an email containing such a link, do not reply to it, and please notify the Bank's Customer Service of this fact. If you suspect that your password has been disclosed, contact the Bank's Customer Service and request the blocking of HB.

Be on the lookout – do not hesitate to contact the Bank if you have any concerns or if your computer behaves strangely when you access HB or other services. If you are not sure about any issue, contact the Bank's Customer Service.

5. RECOMMENDED PRACTICES AND SETTINGS

We recommend that you regularly change your HB Login Password (see section 1). When creating this do not use any information which could easily be guessed, such as names, dates of birth, telephone numbers etc.

Do not reveal your passwords to anyone, and make sure that no-one is watching when you enter them.

It is a good idea to keep the Signature Certificate stored on a portable data storage device (e.g. a USB flash drive), which can be kept under the User's own control. After finishing work with HB, this storage device should then be put in a safe place.

Signature Certificates are valid for one year. Before or after their Signature Certificate expires, Users must submit a request for the generation of a new Signature Certificate. If Users do not request the generation of a new Signature Certificate they will be blocked from performing the Authorisation of Payment Orders, requests and other messages to be sent to the Bank.

The Transport Certificate required for receiving messages from the Bank is also valid for one year. Before or after the Transport Certificate expires, the System Administrator must submit a request for the generation of a new Transport Certificate. If the System Administrator does not request the generation of a new Transport Certificate it will not be possible to receive encrypted messages and information from the Bank via HB (account statements, information on cleared transactions etc.).

Install antivirus software and regularly update it (at least once a week). Install antispyware software and regularly update it (at least once a week). We also recommend that you protect your computer using personal firewall software.

When using antivirus software, take note of any changes that occur in system files. These are the files which will be affected by "Trojan horse" attacks (malware which may be imported into the computer via, for example, an email attachment).

For routine work, and especially when working online, do not use a user profile with administrator rights.

PPF banka a.s., Praha 6, Evropská 2690/17, Post Code 160 41 Czech Republic, Company ID No. 47116129, VAT No. CZ47116129
Incorporated in the Companies Register of the Municipal Court in Prague, Section B, File 1834
Tel.: (+420) 224 175 888, Fax: (+420) 224 175 980

Do not allow any other person to log into HB using your user profile. Before leaving your computer always lock the screen or close the HB application.

We recommend that you do not install any software obtained from untrusted sources (public software libraries, email attachments etc.). Illegally obtained SW in particular may contain "Trojan horse" malware which will send your passwords to the author of these (illegally modified) programs. Be especially careful when you receive emails with attachments – "password stealer" viruses are often spread in this way.

Install all critical updates (for Microsoft operating systems and other software: http://windowsupdate.microsoft.com).

Keep in mind that if you allow anyone else to access your personal information or Security Elements, you are providing that person with the opportunity to exploit this data or to communicate it to a third party.

To a certain extent, setting various Limits for entering Payment Orders (Transaction Limits, Time-based Limits, or a combination of the two) can also be used to prevent abuse.

PPF banka a.s., Praha 6, Evropská 2690/17, Post Code 160 41 Czech Republic, Company ID No. 47116129, VAT No. CZ47116129
Incorporated in the Companies Register of the Municipal Court in Prague, Section B, File 1834
Tel.: (+420) 224 175 888, Fax: (+420) 224 175 980