PPF Banka

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

Contents:

This document sets out principles for the secure use of the Internetbanking service (hereinafter "IB") of PPF banka a.s. (hereinafter the "Bank"). We recommend applying these principles on all computers used for IB 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 IB application, Security Principles, Security Elements and the latest security threats can be found on the Internet Website of the Bank and in IB itself, or can be obtained at the Bank's Places of Business, by calling +420 224 175 901, 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 Internetbanking 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 IB 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 +420 224 175 901 or at the email address customer.service@ppfbanka.cz.

1. SECURITY ELEMENTS AND TERMS USED

IB is inseparably linked to two internet portals:

- https://ibs.ppfbanka.cz – the IB portal; and
- https://ibcc.ppfbanka.cz – the Certification Centre portal.

The Security Elements used for accessing IB and for the Authorisation of Payment Orders and requests made to the Bank are called "authenticators". These authenticators consist of the User's IB Username, and:

a) a Certificate and a PIN for the Certification Token on which the Certificate is stored (the Certification Token is a special device which connects to the computer via a USB port); or
b) an IB Login Password and an OTP code generated using an OTP Token; or
c) an IB Login Password and an SMS code sent to the User's mobile phone.

2. GENERAL SECURITY PRINCIPLES

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

Keep IB Usernames, IB Login Passwords, PINs, Personal Data and Tokens used for accessing IB or any of its associated parts (e.g. Certification Centre Login Names and Login Passwords) in a safe place.

Your *Agreement on Internetbanking* and its annexes (hereinafter the "Agreement on IB") 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, immediately contact the Bank's Customer Service and ask for IB or IB access to be blocked.

3. SECURITY PRINCIPLES FOR THE USE OF INTERNETBANKING

The security of the IB system is only as strong as its weakest link. The IB system consists of the Bank's servers, the Internet, the GSM network, the User's computer and potentially also mobile phone, 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 IB system as a whole.

Communication over the Internet is carried out using an encrypted connection between the Bank's server and the User's computer.

The GSM network is used only for the transmission of partial fragments of data, which cannot themselves be exploited to breach the security of IB.

The next two links – the User's computer and possibly mobile phone – 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. Mobile phones can be secured fairly easily – we recommend having the phone with you at all times and protecting the data in its memory using a PIN code and/or any other means of protection available on the given device.

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 PIN), copying of files (Certificates), or the displaying of falsified information. 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 IB (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 Certification Token with a PIN, an OTP Token with an OTP code, or a mobile phone with an SMS code). 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 IB, 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 IB.

4. PHISHING

Use only trusted services, and always make sure that you are communicating with the genuine service provider. When accessing CAs and entering Payment Orders and requests made to the Bank, check that your connection is properly secured and that you are communicating with the Bank (check the validity of the SSL certificate and the data stated in it – the Bank's certificates are issued by "thawte, Inc."). If you have any doubts about whether you are communicating with the Bank, contact the Bank's Customer Service.

Choose IB Login Passwords and PINs 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 or PIN has been disclosed, contact the Bank's Customer Service and request the blocking of IB.

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 IB or other services. Suspicious behaviour may consist, for example, of SMS codes not being delivered, different payment information being shown with an SMS code, a server with a "strange" name, a different visual appearance or new steps when logging in (especially if an SMS code or PIN is requested) etc. 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 IB Login Password and PIN. When creating these do not use any information which could easily be guessed, such as names, dates of birth, telephone numbers etc.

Do not reveal your IB Login Password or PIN to anyone, and make sure that no-one is watching when you enter them.

The Certificate used to verify a User's identity is stored on a Certification Token whose specifications prevent it from being abused by requiring the correct PIN to be entered. In order for this device to function correctly, applications must be installed on the computer allowing data to be read from its memory. This in effect also prevents the Certification Token from being easily used on third parties' computers or public computers. Remember to renew your Certificate regularly, at least once a year. Certificates are always issued with a one-year period of validity, and if they are not renewed in time the User will be denied any access to IB. In such a case, the User or Client will have to go in person to a Place of Business of the Bank and request a new Certification Centre Login Name and Login Password in order to generate a new Certificate.

If a Token is lost or if you lose the mobile phone to which SMS codes are sent, contact the Bank immediately and have User access to IB blocked.

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.

Do not allow any other person to connect to the Internet using your user profile. Before leaving your computer always lock the screen or close all connections with IB. Store your Token in a safe place. Always keep the mobile phone which you use for receiving SMS codes with you.

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 your settings can also be used to prevent abuse:

- various Limits can be set for entering Payment Orders (Transaction Limits, Time-based Limits, or a combination of the two);
- notifications of selected events can be sent to you - in particular notifications about Users logging into IB, or also about transactions performed on CAs.