PPF Banka

SECURITY PRINCIPLES FOR INTERNETBANKING OF PPF banka a. s.

The following document describes the principles for safety operation of Internetbanking of PPF banka a. s. (hereinafter "IB" only). We recommend going by all these principles with all computers where IB will be operated. PPF banka a. s. (hereinafter "Bank" only) is not responsible for any data loss, Personal Information leakage or any other points of fact that occur as a result of noncompliance with the principles introduced here.

More information on IB application, Security Principles, Security Elements or current security threats can be found on the Bank Websites in IB or you can get them in Place of Business of the Bank, on telephone number +420 222 244 255 or on e-mail address customer.service@ppfbanka.cz.

If there are terms or collocations of words with capital letters used in the text of these Security Principles, their meaning is given in the article Definition of Terms of *The General Business Conditions of PPF banka a. s.* (hereinafter "GBC" only) and/or *Business Conditions of PPF banka a. s. for the Usage of Internetbanking Services* (hereinafter „SBC" only), or the meaning specified in particular regulations of GBC and/or SBC. The current wording of GBC and SBC is available on Websites www.ppfbanka.cz.

User's support for IB is provided by a Client service, which can be contacted during working days from 8 a.m. to 5 p.m. on telephone number +420 222 244 255 or on e-mail address customer.service@ppfbank.cz. Queries sent by e-mail out of the given period of time will be answered by the Client service during the next working day.

1. SECURITY ELEMENTS AND TERMS

IB is closely connected with two internet portals:

- https://ibs.ppfbanka.cz – portal IB, and
- https://ibcc.ppfbanka.cz – portal of Certification Centre.

Security Elements for an access to IB are called Authenticators. The authenticators can be IB Username and:

a) the Certificate and PIN to Token, on which the Certificate is stored (a special device that is connected to the computer via USB port), or
b) IB Login Password and SMS code sent to the mobile phone of the User.

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

2. GENERAL SECURITY PRINCIPLES

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

IB Username, IB Login Passwords, PIN as well as Personal Information and Token serving for the access to IB or to any other interconnected part of IB (e.g. Certification Centre´s Login Name and Login Password) must be kept in the safe place.

The aim of abuse can also be the *Agreement on Internetbanking* and its supplements (hereinafter "Agreement on IB" only). Consider these documents confidential, protect them from loss and keep them in the safe place.

If you suspect that usernames, passwords or any other sensitive data could be disclosed, contact the Client service of the Bank immediately and ask to put a stop on IB or accesses into IB.

3. SECURITY PRINCIPLES FO INTERNETBANKING USAGE

Security of IB system is of such strength how strong it is its weakest link. IB system consists of bank servers, internet network, GMS network, User's computer possibly also User's mobile phone and a human factor.

The Bank servers are secured by server certificates, firewall system, protective zones, monitoring devices and further mechanisms, which create the very strong link in the whole IB system.

Communication via internet is performed by a ciphered connection between the Bank servers and the User's computer.

GSM network is utilized only for transmission of partial information, which as such cannot be abused for breaking through the IB security.

The other two links – User's computer and possibly User's mobile phone – are potentially the most vulnerable spots of the whole system because it is not the Bank but only the Client himself, or User, who is responsible for their security. The protection of a mobile phone can be relatively easily secured, we recommend having the mobile with oneself all the time and protecting the data in its memory by PIN code or other protective means, which are at disposal in the concrete apparatus.

It might be more difficult for a lay User to ensure the computer safety in such a way that nobody could install programs enabling remote-control administration including the reading of keyboard (getting the password or PIN), copying the files (of the Certificate), or faking the displayed information. Therefore special attention must be paid to the security of the User's computer and if need be the safety setting must be consulted with an expert. We recommend using antivirus/antispyware solution.

Relatively independent chapter that forms the potentially weakest link is so called human factor. It means the fact that User can disclose important parts of the security system to a potential attacker, who can later abuse them. Security of IB system (and its further parts) must be so solid that even in case of the disclosure of some sensitive information to an unauthorized person, it could not be

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

abused. The system of safety elements is created by one or several data known only to a User and by a further device for identity authentication (Token with PIN, a mobile phone with SMS code). Each User should be aware of the data sensitiveness that serves to authenticate its identity in compliance with IB usage and never disclose these data to anybody. Under no circumstances the Bank will require the disclosure of these data, with the exception of their entry into IB.

4. PHISHING

Utilize only reliable services and always make sure that you really communicate with the right provider. In access to CA and entering of orders and instructions for the Bank, check if the connection is fully secured and that you communicate with the Bank (check the validity and data in the certificate of SSL security, Bank certificates are issued by "thawte, Inc."). If you are not sure whether you really communicate with the Bank, contact the Client service of the Bank.

Choose the IB Login Passwords and PINs in such a way that they could not be easily guessed or deduced from the information about your person. The Bank never requires the entry or confirmation of these data via electronic mail. In case you are required to give such information in the name of the Bank, please, immediately contact the Client service of the Bank.

Watch out whether you are confirming the order or instruction for the Bank you entered. Sooner than you confirm it, always check if the data are correct, comparing them with an invoice, a pay slip and things like that.

Check regularly the movements on your accounts and payment card transactions. If you use a payment card for payments on internet, acquire an internet payment card. In case any discrepancy occurs, immediately contact the Bank.

Never open dubious electronic messages (messages from unknown senders, messages with foolish contents and the like), especially do not open supplements of such messages. The Bank never sends messages that were not requested and that contain references to its Websites. If you get such reference, do not react to it and, please, inform the Client service of the Bank. In case you have a suspicion that your password or PIN was disclosed, contact the Client service of the Bank and ask for putting a stop on IB.

Be attentive – never hesitate to contact the Bank in case of any doubts or strange behaviour of the computer in entering the IB or other services. Suspicious behaviour means, e.g., not coming of SMS codes, other data about the payment in SMS code, a "strange" name of the server, different visual impression or new steps during the entering (especially if they required SMS code or PIN) and things like that. If you are at a loss, contact the Client service of the Bank.

5. RECOMMENDED PROCEDURES AND SETTINGS

We recommend changing the IB Login Password and PIN regularly. In creating them, do not use easily guessed information as names, dates of birth, telephone numbers and the like.

Never tell anybody your IB Login Password and PIN and prevent everybody watching you when entering them.

Certificate of authentication of the User's identity is placed on Token, whose specification prevents its abuse without using the right PIN. The right functioning of this device requires the installment of

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

applications in the computer, which enable reading data from its memory. This, de facto, also prevents the Token to be used on foreign or public computers in a simple way. Do not forget to regularly renew the Certificate, at least once a year. The Certificate is always issued to be valid for one year. In case the User does not renew it in time, any entry into IB is not possible. In this case the Client User must come to the Place of Business of the Bank and require for User the Certification Centre´s Login Name and Login Password to generate the new Certificate.

In case of the Token loss, the Certificate must be made invalid. This can be carried out by the User in Certification Centre, or possibly by a Customer Support of the Bank.

Install the antivirus software and regularly (at least once a week) carry out its updating. Install the antispyware software and regularly (at least once a week) carry out its updating. We recommend protecting the computer by programs of "Personal firewall" types, especially in connecting to internet via a fixed line (via cable television and the like).

In using the antivirus program, pay attention to any changes in the system files, attacks of "Troyan horse" type (the virus imported, e.g., by a file connected to the mail) may occur here.

Do not use the user's profile with administrator rights for routine work, especially when you work with internet.

Do not enable the other person to connect to the network by means of your user profile. Before leaving the computer, always lock the screen or end all connections with IB. The Token that serves as a storage, must be safely stored. Always carry the mobile phone for sending SMS codes with you.

We do not recommend installing the software obtained from untrustworthy source (public libraries, supplements in electronic mail and the like). Especially, illegally obtained SW can contain so called "Troyan horses" and thus send your passwords to the author of these (illegally modified) programs. Be careful when receiving the electronic mail with supplements – viruses spread in this way often contain so called "password thieves".

Install important updates (for operational system and further software from Microsoft company: http://windowsupdate.microsoft.com).

Remember, if you enable anybody to access to your personal data or security means, you make possible for such a person to abuse these data or convey them to another person.

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