# SERVICE OF INTERNET BANK

## I. GENERAL PROVISIONS

**1.1.** Internet Bank (hereinafter – **IB**) means the Bank's services provided through the Bank's online system at www.sb.lt.
**1.2.** The concepts used in this document are defined in the *Conditions of Provision of Electronic Services* that are an integral part of the *Contract for Internet Bank Service* (hereinafter – Contract).
**1.3.** Information about use of IB is provided by phone 1813 (+370 37 301 337 from abroad) and by e-mail kc@sb.lt.

## II. IDENTITY VERIFICATION MEANS

The Bank identifies the Client/ User according to the identity verification means issued by the Bank or third parties:
**2.1.** **User ID** – the user name consisting of letters and numbers that cannot be changed indicated in the Contract.
**2.2.** **Initial Password** – a digital password generated by the Bank and indicated in the Contract or given in the envelop. It is used for the first logging-in to IB and has to be changed to the Logging-in Password created by the User.
**2.3.** **Logging-in Password** – personal password known only to the User and created by the User after the first logging-in to IB. The User has to create a password consisting of 6 or more Latin letters, numbers and/or standard symbols. It is not recommended to use spaces, Lithuanian letters or special symbols in the password. For the purpose of security, IB system will ask to change the Logging-in Password periodically. The User may change this password in IB.
**2.4.** **PIN card and code received by a text message** (hereinafter - **PIN + SMS**) – the card containing 24 codes of multiple use issued by the Bank and an additional code generated by the Bank and sent by a text message to the User's mobile phone. PIN + SMS is used to log in and to sign the transactions in IB.
**2.5.** **Generator** – an electronic device issued by the Bank that generates recognition (logging-in) and signing codes.
**2.6.** **Electronic signature** – the Client's signature that is formed using the electronic means enabling to identify the signatory. It has the same legal power as the usual handwritten signature:
2.6.1. **M-signature** – an identity verification tool that helps to log in to IB and mobile application (hereinafter – App) and to sign the transactions with the help of mobile phone and mobile SIM card. The User may get a SIM card with a function of mobile signature in the representative office of the mobile connection operator.
2.6.2. **Smart – ID**: app Smart-ID is a simple, safe and smart tool that allows accessing IB and the App and signing the transactions. The Client / the User may download free app to the **smart phone** or tablet from AppStore or Google Play store and to register the account using the means issued by the Bank: Generator, PIN + SMS or m-signature issued by digital certification centres. Smart-ID account may be of two types:
*2.6.2.1.* Smart-ID Basic – if the identity was verified at the time of the account's creation by logging to the Bank's IB, using the means issued by the Bank: Generator / PIN + SMS, this app will be available only in internet bank of the banks and in the App;
*2.6.2.2.* Smart-ID – if the identity was verified at the time of the account's creation by m-signature, this app will be available to access the Bank's IB, App and other systems of electronic service providers integrated in the network Smart-ID, and to sign the documents there.
**2.7.** **Password** – a code of one of the types of transaction signing means indicated in the Contract: electronic signature, code generated by the Generator, PIN + SMS.

## III. LOGGING-IN TO IB

**3.1.** The Client, who wants to use IB, has to sign the Contract in the Bank.
**3.2.** To access IB, the following actions have to be performed:
3.2.1. Enter address https://e.sb.lt in the browser's address line or click on the link in the Bank's website www.sb.lt -> *Log in -› Internet Bank;*
3.2.2. The username (ID) has to be entered in the first box of IB logging-in page. User ID is indicated in the Contract's section "Rights of Users". It is made from numbers and letters and cannot be changed;
3.2.3. The Logging-in Password has to be entered in the second box of IB logging-in page. At the time of the first log-in, the Initial Password indicated in the given envelop or in the Contract (when the envelop is not issued) has to be entered. It consists of 8 numbers and is used only for the first logging-in.
**3.3.** When the User ID and Logging-In Password are entered, press the button "Connect".
**3.4.** Enter the requested code from PIN card in the newly opened window (after the protective layer is removed from the requested code's number), as well as the code received by a text message or a code generated by the Generator, or a code of Electronic Signature.
**3.5.** At the time of the first log-in to IB, the Initial Password has to be changed to the Logging-in Password created by the User in the newly opened window (from 6 or more Latin letters, numbers and/or standard symbols). The Bank recommends to keep the Initial Password in a safe place so that the Logging-in Password could be restored to the Initial Password if forgotten by the User.

## IV. USERS

**4.1.** When signing the Contract, the Client may indicate one or several Users entitled to manage the Client's bank accounts in IB.

**4.2.** The Client may determine the following rights of transactions' management for the User when signing the Contract or later, by filing a separate request:

4.2.1. right of the first signature (with the right of signature, i.e., the transaction entered and signed by the User or he transaction confirmed by the User that was entered and signed by the User with the right of the second signature and the User without the right to sign will be executed);

4.2.2. right of the second signature (with the right of signature, i.e., the transaction will be entered and signed but it will not be executed until it is confirmed by the User with the right of the first signature or the User with the right of the second signature may enter, sign and confirm the transactions until the amount fixed with that User's regard is reached. In such a case, the confirmation of the User with the right of the first signature is not required);

4.2.3. without the right to sign (without the right to sign, i.e., the transaction will be but it will not be executed until it is signed by the User with the right to sign);

4.2.4. to determine that the transaction has to be confirmed by all/ at least one User with the right to sign;

4.2.5. to change the rights of transactions' management for him(her)self and other Users: rights to enter / confirm the transactions.

## V. DETERMINATION OF LIMITS AND RIGHTS OF ACCOUNT MANAGEMENT

**5.1.** The Bank has the right to determine the limits for the transactions in the account unilaterally or upon receipt of the separate request of the Client:

5.1.1. one transaction – the maximum amount of money that cannot be exceeded, when the User enters and/or signs one transaction in the specified account;

5.1.2. daily – the maximum amount of money that cannot be exceeded per one day, when the User signs the transactions in the specified account;

5.1.3. monthly – the maximum amount of money that cannot be exceeded per one month, when the User signs the transactions in the specified account.

**5.2.** The following rights of account management may be determined for the User upon the Client's request:

5.2.1. just to review – to form an account statement, to see the balance and other information;

5.2.2. just to credit– only to transfer money to the account;

5.2.3. just to debit– only to transfer money from the account;

5.2.4. to credit and debit – to transfer money to and from the account.

## VI. ENTRANCE AND SIGNING OF TRANSACTIONS

**6.1.** The transactions are prepared by choosing a respective item on the menu of IB or the App and completing the required data.

**6.2.** The User has to sign the prepared transaction by pressing the confirmation button to proceed. The User shall sign the transactions using the identity verification means that s/he has or that have been issued by the Bank, save for the exception specified in Paragraph 6.3.

**6.3.** When the credit transfers are made between the Client's accounts and when currency is exchanged, the transactions may be executed only after the confirmation button is pressed. This condition is applied if the User with the right of the first (supreme) signature takes part in the transactions of the same Client and confirms the transactions.

**6.4.** If the User does not confirm the transaction, it will be stored in the list of unsigned transactions (IB menu: *Payments -> List of payments and other transactions -> Unsigned transactions*). When the User enters several transactions, all of them may be signed at the same time.

**6.5.** IB transactions are divided into four lists:

6.5.1. **unsigned** – the entered transactions not confirmed by the User or the transactions yet not confirmed by other Users of the Client. The transactions in this list affect the future balance (IB menu: *Account's information -> Review of accounts*). The User has to confirm the transaction not later than within 100 (one hundred) days after its entrance (otherwise, it shall not be executed);

6.5.2. **signed** – the transactions confirmed by the User and executed in the Bank. The User may delete the transactions in this list if s/he does not want any more to have them executed;

6.5.3. **rejected** – the transactions confirmed by the User but not executed because of insufficient funds in the account, errors or other reasons. The User is informed about the rejected transactions in IB;

6.5.4. **executed** – the transactions confirmed by the User that were executed. Information about executed payment orders is provided additionally in the account statement, by choosing the following in IB menu *Account's information -> Statement.*

**6.6.** The times of transactions' execution are indicated on the Bank's website www.sb.lt.

**6.7.** It is recommended to check whether the transaction has been executed successfully every time after having it signed.

**6.8.** The User has to check the information about the transactions performed in the account at least once in a month.

The Client has to notify the Bank about the transactions executed improperly, about any errors, discrepancies or inaccuracies.

## VII. CURRENCY EXCHANGE

**7.1.** The currency exchange transactions entered on the working days before 23:55 are executed on the same working day. If they are entered later, the currency is exchanged on the next working day.

**7.2.** If the User selects and enters the currency exchange for the *Contractual Rate*, the currency exchange shall be confirmed or rejected by the Bank's employee on working days (Bank's working days).

## VIII. IMPORT OF TRANSACTIONS

**8.1.** If the User is the Client's (legal entity's) employee or has the permit to manage accounts of another Client (legal entity) and has an accounting software in his/her computer or another software used to prepare advance credit transfers SEPA and non-SEPA credit transfers in ISO 20022 XML format, the prepared payment orders may be imported to IB system as a single or package processing of transactions.

**8.2.** If the Client does not have any software used to prepare payment orders in the needed ISO 20022 XML format, the converter's function in IB may be used. This function converts the data sets with extensions ".mokesis" ".taresis" or ".xml" to transfers in ISO 20022 XML format.

## IX. ADDITIONAL INFORMATION

**9.1.** The Bank undertakes to block use of IB or the App if the Client/ User:

9.1.1. submits a written request during working hours of any branch of the Bank;

9.1.2. calls to 1813 (+370 37 301 337 from abroad);

9.1.3. calls other phone number provided on the Bank's website;

9.1.4. if the Logging-in Password is entered incorrectly 5 (five) times;

9.1.5. if the code from PIN card and code received as the text message/ generated by the Generator is entered incorrectly 3 (three) times, the access is blocked temporarily, and the access is blocked if the code is entered incorrectly 3 more times. If the identity verification means issued not by the Bank are used, blocking is done in accordance with the requirements of the third parties.

**9.2.** If the User forgets / loses the identity verification means issued by the Bank or the Bank's system blocks the use of IB and the App, the Client has to come to any branch of the Bank (and to have the personal identity document).

**9.3.** Before accessing IB, the User has to check whether the browser:

9.3.1. shows correct website's address - https://e.sb.lt, it has to start with *https,* not *http*.

9.3.2. the website's security certificate has to be valid – the symbol of lock has to be present in the address line of the browser, as well as green (or black in the green background – depends on the browser) note "Siauliu Bankas AB [LT]". If this note is not present or the browser warns about invalid security certificate, do not connect to IB and notify the Bank thereof immediately.

**9.4.** If the User does not perform any actions for 12 (twelve) minutes in IB, the notice about soon ending session is shown for 3 (three) minutes. During this period, it is possible to press one of the buttons: "To continue the work" or "To end the work". If the User does not press any of the buttons in 3 (three) minutes, the session is closed and the notice hereof is shown until the User presses the button "I understand". Afterwards, the User is referred to the home page of IB.

## X. REQUIREMENTS FOR HARDWARE AND SOFTWARE I

**10.1.** The Client/User, who wants to use IB, has to use the device with legal and updated operating system (e.g., Windows 7, Windows 8, Windows 10, or operating system of other manufacturers) and Internet network. Besides, the latest versions of browsers fully supported by the manufacturers have to be installed: Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome, Opera, Safari. It is not recommended to use the browsers that are not supported or updates any more, for example, Microsoft Internet Explorer 10 or older.

**10.2.** The User has to take care about protection of the computer, software or other equipment used to access IB from viruses and other threats, for example, to update regularly the antivirus system, browser, anti-spyware, and firewalls. Besides, it is necessary to update other computer applications, especially the one that use browsers (Adobe Flash, Adobe Reader, Java).

**10.3.** Having finished the work in IB, the User has to leave the system pressing the button *Sign out* in the right upper corner and to close the browser.

AB Šiaulių Bankas