

## INTERNET BANK SERVICE

### I. GENERAL PROVISIONS

- 1.1. Internet Bank (**IB**) is a set of the Bank's services provided via the Bank's online system at [www.sb.lt](http://www.sb.lt).
- 1.2. The terms used in this document are defined in the *Terms of Electronic Services*, which form an integral and inseparable part of the *Internet Bank Service Agreement* (hereinafter, Agreement).
- 1.3. Information on how to use the IB is available by phone at 1813 (+370 37 301 337 for calls from abroad) and by email at [kc@sb.lt](mailto:kc@sb.lt).

### II. MEANS OF AUTHENTICATION

The Bank shall establish the identity of the Client/User on the basis of Means of Authentication issued by the Bank or third parties:

- 2.1. **User ID:** the login name specified in the Agreement, consisting of letters and digits, which is not changeable.
- 2.2. **Initial Password:** the digital password generated by the Bank and specified in an envelope or the Agreement. It shall be used for the first login to the IB by means of an SMS code/code generated by a code generator and shall be changed to a login password created by the User.
- 2.3. **Login Password:** a personal password created by the User after the first login to the IB by means of an SMS code/code generated by a code generator known only to the User. The User must come up with a password of 6 or more letters of the Latin alphabet, digits and/or standard characters. It is not recommended to use spaces, Lithuanian letters, or special characters in the password. For security reasons, the IB system shall ask you to change your Login Password periodically. The User can also change the Login Password in the IB.
- 2.4. Code received by **SMS** (hereinafter, **SMS**): code generated by the Bank and sent by SMS to the User's mobile telephone. SMS is used for logging in and signing Transactions in the IB.
- 2.5. **Generator:** an electronic device issued by the Bank that generates authentication/login and signature codes.
- 2.6. **Electronic Signature:** Client's signature that is formed by electronic means and which allows the identity of the signatory to be established and which has the same legal effect as a regular handwritten signature:
  - 2.6.1. **Mobile ID:** a means of authentication that allows securely and conveniently logging in to the IB and the mobile application (hereinafter, Application) and signing Transactions using a mobile telephone and mobile SIM card. A special SIM card with a mobile signature function can be obtained by visiting the mobile operator's office.
  - 2.6.2. **Smart-ID:** The Smart-ID application is a simple, secure, and smart tool that allows logging in to the IB and the Application and signing transactions. The Client/User can download the application free of charge to a **smartphone** or tablet from [AppStore](#) or [Google Play](#) stores and register an account by visiting the Bank or by using the Mobile-ID issued by a digital certification centre. There are two types of Smart-ID accounts:
    - 2.6.2.1. **Smart-ID Basic:** if, at the time of creating the account, the identity is verified by logging in to the IB using the means issued by the Bank, i.e., Generator/SMS, this application can only be used to access the Internet Bank and the Application of the Bank;
    - 2.6.2.2. **Smart-ID:** if, at the time of creating the account, the identity is verified by means of Mobile ID, the application can be used to log in to and sign documents in the IB, the Application and the electronic service provider systems integrated into the Smart-ID network.
- 2.7. **Biometrics/PIN:** a profile created by the User on the Application using the User's biometric data (facial image or fingerprint) or a numeric quick access code (PIN) created by the User on the Application.
- 2.8. **Password:** one of the means to sign Transactions as provided for in the Agreement: Electronic Signature, code generated by the Generator, SMS.

### III. LOGGING IN TO THE IB

- 3.1. To start using the IB, the Client must sign an Agreement with the Bank.
- 3.2. The following steps are required to log in to the IB:
  - 3.2.1. enter <https://e.sb.lt> in the address field of the web browser or click on the link on the Bank's website [www.sb.lt](http://www.sb.lt) - > Log in -> Internet Bank;
  - 3.2.2. Enter the User Name (ID) in the first field of the IB login window. The User ID is specified in the "User Rights" section of the Agreement. It is made up of letters and digits and can not be changed;
  - 3.2.3. In the second field of the IB login window, enter the Login Password, i.e., the SMS code received from the Bank or Generator code. When logging in for the first time, you will need to enter your Initial Password, which is either on the inside of the password envelope or specified in the Agreement (when no envelope is issued). It consists of 8 digits and is used only for the first login. When logging in with the Electronic Signature, you will need to enter your User ID in the second field of the IB login window.
- 3.3. After entering your User ID and Login Password/User ID, click on the "Log in" button.
- 3.4. In the newly opened window, enter the requested SMS code, or the code generated by the Generator, or the Electronic Signature code.

- 3.5. When logging in to the IB for the first time with an SMS code received from the Bank or a Generator code, the Initial Password must be changed in the newly opened window to a Login Password created by the User (consisting of 6 or more letters of the Latin alphabet, digits and/or standard characters). The Bank recommends that you securely store your Initial Password so that if you forget the Login Password that you have created, it can be reset to the Initial Password.

#### IV. USERS

- 4.1. By signing the Agreement, the Client may designate one or more User(s) who shall be authorised to manage the Client's bank accounts via the IB.
- 4.2. The Client may, at the time of entering into the Agreement or subsequently upon separate request, establish the following rights for the management of the User's Transactions:
- 4.2.1. the right of first signature (with a signature right, i.e., a Transaction entered and signed by the User, or a Transaction confirmed by the User and entered and signed by the User with the right of second signature and the User without signature right shall be executed);
- 4.2.2. the right of second signature (with a signature right, i.e., a Transaction can be entered and signed, but shall not be executed until it is confirmed by the User with the right of first signature, or the User with the right of second signature may enter, sign and confirm transactions up to a certain amount set for him/her, in which case no validation by the User with the right of first signature is required);
- 4.2.3. without the right to sign (without signature right, i.e., a Transaction can be entered, but shall not be executed until it is signed by the User with a signature right);
- 4.2.4. it may be provided that every Transaction must be confirmed by all/at least one User with a signature right;
- 4.2.5. the User may change the Transaction management rights for themselves and for other Users: rights of entering/confirming Transactions.

#### V. SETTING LIMITS AND ACCOUNT MANAGEMENT RIGHTS

- 5.1. The Bank shall have the right to unilaterally, or at the Client's separate request, set limits for the execution of Transactions on the Account:
- 5.1.1. single transaction limit, i.e., the maximum amount of money up to which the User may enter and/or sign one Transaction on the specified account;
- 5.1.2. daily limit, i.e., the maximum amount of money up to which the User may sign Transactions in one day on the specified account;
- 5.1.3. monthly limit, i.e., the maximum amount of money up to which the User may sign Transactions in one calendar month on the specified account.
- 5.2. At the Client's request, the following account management rights may be granted to the User:
- 5.2.1. view only, i.e., generate an account statement, view the account balance and other information;
- 5.2.2. credit only, i.e., only make transfers to the account;
- 5.2.3. debit only, i.e., only make transfers from the account;
- 5.2.4. credit and debit, i.e., make transfers to and from the account.

#### VI. ENTERING AND SIGNING TRANSACTIONS

- 6.1. Transactions are prepared by selecting the relevant IB or Application menu item and filling in the required data.
- 6.2. The User must sign the prepared Transaction by clicking the confirmation button for it to be executed. The User shall sign Transactions with the means of authentication issued to him/her by the Bank or in his/her possession, except as provided in paragraph 6.3.
- 6.3. For credit transfers between the Client's own accounts and for currency exchanges, such Transactions shall be executed by clicking the confirmation button only. This applies if the Transactions involve accounts of the same Client and the Transactions are authorised by the User with the right of first (highest) signature.
- 6.4. If the User has not confirmed the Transaction, it shall be in the list of unsigned Transactions (go to the IB menu item *Payments -> Payment statuses -> Not confirmed/Payments -> Import -> Not confirmed/Other services -> Document statuses -> Not confirmed*). A user who has entered several payment transactions can sign them all at once.
- 6.5. In the IB, Transactions are organised into four lists:
- 6.5.1. **unsigned** – Transactions entered but not confirmed by the User or Transactions not yet confirmed by other Users of the Client. The Transactions in this list affect the amount of the future balance of the accounts (go to the IB menu item *Accounts and cards -> Account overview -> More information*). The User must confirm the Transaction not more than within one hundred (100) days after its entry (otherwise it shall not be executed);
- 6.5.2. **signed** – Transactions confirmed by the User and executed at the Bank. The User may delete Transactions in this list if he/she no longer wishes them to be executed;
- 6.5.3. **rejected** – Transactions confirmed by the User that were not executed due to insufficient funds in the accounts, errors or other reasons. The User shall be informed of the rejected Transactions via the IB;
- 6.5.4. **executed** – Transactions that have been confirmed by the User and have been executed. Information on the completed payment orders is additionally available in the Account Statement (go to the IB menu item *Accounts and cards -> Statement*).

- 6.6. Transaction processing times are indicated on the Bank's website at [www.sb.lt](http://www.sb.lt).
- 6.7. We recommend that you check each time you sign Transactions that the Transaction has been successfully executed.
- 6.8. The User must check the details of the Transactions made on the account at least once a month. The Client shall notify the Bank in writing of any incorrectly executed Transactions, as well as of any other errors, discrepancies or inaccuracies.

## VII. CURRENCY EXCHANGE

- 7.1. Currency exchange transactions entered before 11:55 p.m. on weekdays are executed on the same business day. If the transaction is submitted at a later time, the exchange takes place on the next business day.
- 7.2. If the User selects and enters a currency exchange transaction at the *Contractual Rate*, the currency exchange shall be confirmed or rejected by an employee of the Bank on a weekday (during the Bank's business hours).

## VIII. IMPORT OF TRANSACTIONS

- 8.1. If the User is an employee of the Client (legal entity) or is authorised to manage the accounts of another Client (legal entity) and has an accounting software or other software on his/her computer which prepares SEPA and non-SEPA credit transfers in ISO 20022 XML format, the payment orders prepared can be imported into the IB.
- 8.2. If the Client does not have a program that prepares payment orders in the required ISO 20022 XML format, he/she can enter the payment data manually in the payroll form (IB menu item *Payments -> Payroll*).

## IX. ADDITIONAL INFORMATION

- 9.1. The Bank undertakes to block the use of the IB and the Application if the Client/User:
  - 9.1.1. submits a written request to the Bank;
  - 9.1.2. contacts the Bank by telephone at 1813 (+370 37 301 337 for calls from abroad);
  - 9.1.3. calls another telephone number indicated on the Bank's website;
  - 9.1.4. enters the Login Password/User's national identification number incorrectly five (5) times;
  - 9.1.5. enters the SMS code/Generator code incorrectly three (3) times (the Generator shall be temporarily blocked, and if the code is entered incorrectly 3 more times, it shall be blocked). If means of authentication not issued by the Bank are used, the blocking shall be performed in accordance with the requirements of third parties.
- 9.2. If the User forgets/loses the means of authentication issued by the Bank or the Bank's system blocks the use of the IB and the Application, the Client must visit any of the Bank's branches in order to unblock it.
- 9.3. Before logging in to the IB, the User must check that the web browser:
  - 9.3.1. shows the correct website address, i.e., <https://e.sb.lt>, starting with "https" and not "http".
  - 9.3.2. the website security certificate must be valid – the address bar in the browser must contain a lock symbol and the text *Siauliu Bankas AB [LT]* written in green (or in black against green background, depending on the browser used). If this symbol is missing or the browser warns you that the security certificate is not valid, do not log in to the IB and immediately notify the Bank thereof.
- 9.4. If the User does not perform any actions in the IB for five (5) minutes, a message shall be displayed for one (1) minute indicating that the session is about to end, during which time one of the two buttons can be clicked: "Continue" or "End". If the User does not click any of these buttons within one (1) minute, the session shall be closed and a message to that effect shall be displayed until the User clicks on the "I understand" button. After clicking this button, the User is redirected to the initial IB login window.

## X. HARDWARE AND SOFTWARE REQUIREMENTS

- 10.1. The Client/User wishing to use the IB needs a device with a legal, up-to-date operating system (e.g., Windows 7, Windows 8, Windows 10, or an operating system supported by other manufacturers) and the Internet connection. You must also have the latest versions of browsers fully supported by the manufacturers, e.g., Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome, Opera, Safari. The use of browsers that are no longer supported or updated, such as Microsoft Internet Explorer 10 and older, is not recommended.
- 10.2. It is the User's responsibility to ensure that the computer, software or other equipment used to log in to the IB is protected against viruses and other threats, for example, by keeping up to date the anti-virus system, the web browser and anti-spyware and firewall. Also ensure that other applications on your computer are up-to-date, especially those used by web browsers, e.g., Adobe Flash, Adobe Reader, Java.
- 10.3. Once the User has finished using the IB, he/she must log out of the system by clicking the *Log out* button (top right corner) and closing the browser.

---

Šiaulių Bankas AB