ON-LINE BANKING SERVICE

I. GENERAL PROVISIONS

1. On-line banking (the OB) is the service of the Bank's services, provided aftwer having logged via the Bank's online s ystem www.sb.lt.
2. *Definitions used in this document* are defined in the Terms and Conditions of Electronic Services which are integral and inseparable part of *On-line banking service agreement* (the Agreement).
3. Information on using the On-line banking (the OB) is provided by calling 1813 (370 37 301 337 calling from abroad), as well as by e-mail kc@sb.lt.

II. AUTHENTICATION FACILITIES

The Bank identifies the Customer/User's identity according to the identity verification means issued by the Bank or third parties:

2.1. **User ID:** the login name specified in the Agreement, consisting of alphanumeric characters, which remains unchanged.

2.2. **Original password:** the digital password generated by the Bank, specified in the envelope or in the Agreement. It is used only for the first login to the OB and must be changed by the User-invented password.

2.3. **Login password:** the personal password invented by the User, known only to the User, after the first login to the OB. The User must invent the password of 6 or more Latin alphabet letters, numbers and/or standard characters. It is not recommended to use spaces, Lithuanian letters or special characters in the password. For security purposes, the OB system will ask you periodically to change your login password. The User can also change the login password on the OB.

2.4. PIN card + code received via SMS (the **PIN + SMS**): a 24-password code reusable card issued by the Bank to the User and additional Bank-generated password sent to User's mobile telephone via SMS message. PIN + SMS is used for login and signing the transactions in the OB and mobile application (the Apps);

2.5. **Generator:** electronic device issued by the Bank generating the identification (login) and signing codes.

2.6. **Electronic signature:** a signature held by the Customer, which is formed by electronic means which allow identification of the signatory and has the same legal power as a standard handwritten signature:

2.6.1. **M.signature**: this is an identity authentication instrument that allows one to safely and conveniently login to OB, Apps and sign transactions with the help of a mobile phone and a mobile connection SIM card. A special SIM card with a mobile signature function can be obtained by the Customer upon arrival at the mobile operator's representative office. M. signature works on almost all mobile phones manufactured after 2004; the phone does not have to be smart or support data communication service (on-line);

2.6.2. **„Smart – ID":** The Smart-ID App is a simple, secure and smart instrument for login to OB and signing up transactions. The Customer / User can download the apps for free **to the smartphone** or tablet from the AppStore or Google Play stores and register the account using the instruments provided by the Bank: Generators, PIN + SMS or M.signature or E.signature issued by Digital Certification Centres.

Smart-ID accounts are of two types:

2.6.2.1. "Smart-ID Basic": if, at the time of creating the account, the identity will be confirmed by loging to the Bank's on-line banking using the instruments issued by the Bank': Generator / PIN + SMS, then this app could only be used for the banks' onl-line banking;

2.6.2.2. "Smart-ID": if, at the time of creating the account, the identity will be confirmed by M.signature, E.signature, then this app will allow login to the Bank's on-line banking and to electronic service provider systems integrated into the Smart-ID network and to sign the documents therein.

2.6.3. **E. signature:** a chip personal identity card (issued from 2009 by the Migration Department) or a USB storage medium (issued by the State Enterprise Centre of Registers), which has qualified certificates to securely login to the OB and sign transactions. E.signature cannot be used on mobile devices. The Customer / User's computer must be additionally prepared for the use of the E.signature.

2.7. **Password:** type of code of one of the transaction signing instrument specified in the Agreement: electronic signature, code generated by the Generator, PIN+SMS

III. LOGIN TO OB

3.1. The Customer, wishing to use the OB, must sign the Agreement with the Bank.

3.2. When connecting to the OB, you need to do the following:

3.2.1. In the address bar of the web browser enter the address https://online.sb.lt or click on the link on the Bank's website www.sb.lt -> Internet banking -> *On-line banking;*

3.2.2. Enter the User Name (ID) in the first box of the OB login window. The User ID is specified in the User Rights clause of the Agreement. It is composed of letters and numbers and is unchanged;

3.2.3. In the second OB login field, enter the login password. When logged in for the first time, you must enter an original password that is specified inside the password envelope or printed in the Agreement (when the envelope is not issued). It consists of 8 digits and is used only for the first login.

3.3. After entering the User ID and login password, click on the Login button.

3.4. In the newly opened window, enter the requested code from the PIN card (before that you need to remove the security layer of the code number requested) and the code received by SIM message, generated by the Generator, or the Electronic Signature.
3.5. When connecting to the OB for the first time, in the newly opened window, you must change the original login password to the User-invented login password (from 6 or more Latin alphabet letters, numbers and/or standard characters). The Bank recommends to safely retain the original password so that if the User forgets the invented login password it could be restored to the original password.

IV. USERS

4.1. By signing the Agreement, the Customer may specify one or several Users who are entitled to manage the Customer's bank accounts via the OB.
4.2. The Customer, upon entering into the Agreement or later, upon submission of a separate request, may establish the following User's Transaction management rights:
4.2.1. without the right to sign (without the right of signature, i.e. the Transaction will only be entered and will not be executed until signed by the User with the signature right);
4.2.2. the right of the first signature (with the right of the main signature, i.e. entered and signed Transaction will be executed: it is sufficient to be signed by the User having the first signature right);
4.2.3. the right of the second signature (with the right of signature, i.e the Transaction will be entered and signed, but will not be executed until it is signed by the User having the right of the first signature);
4.2.4. to determine that each Transaction must be validated by all/at least one first signature User;
4.2.5. to modify the Transactions management rights for himself and other Users: Transaction entering/confirmation rights.

V. DETERMINATION OF LIMITS AND ACCOUNT MANAGEMENT RIGHTS

5.1. The Bank has the right, unilaterally, or upon receipt of a separate request by the Customer, to establish the limits for ongoing Transactions in the account:
5.1.1. for one transaction: the maximum amount of money, within which the User can enter and/or sign one Transaction from the specified account;
5.1.2. for the day: the maximum amount of money within which the User can sign Transactions within one day from the specified account;
5.1.3. for the month: the maximum amount of money within which the User can sign Transactions within one calendar month from the specified account.
5.2. At the request of the Customer, the following account management rights may be granted to the User:
5.2.1. only to view: to create an account statement, view account balance and other information;
5.2.2. only to credit: to make funds transfers into the account only;
5.2.3. only to debit: to make funds transfers from the account only;
5.2.4. to credit and debit: to make funds transfers to and from the account.

VI. ENTERING AND SIGNING THE TRANSACTIONS

6.1. Transactions are prepared by selecting the appropriate item in the OB or the App menu and filling in the required data.
6.2. The User must sign the prepared Transaction by clicking on the Confirmation button to execute it. The User signs the Transactions by the identity verification means held or issued by the Bank, except what is provided in p ar. 6.3.
6.3. In the case of credit transfers between Customer's own accounts and currency exchange, such Transactions shall only be executed by pressing the Confirm button. This condition applies if the Transactions are attended by the accounts of the same Client and the Transactions are approved by the User with the right of first (highest) signature.
6.4. If the User has not confirmed the Transaction, this Transaction will be in the unsigned Transaction list (in the OB menu item, select *Payments -> Payment and other Transaction List -> Not Signed transactions*). User who has entered several Transactions can sign them all at once.
6.5. In the OB, Transactions are divided into four lists:
6.5.1. **Unsigned:** entered Transactions not approved by the User, or other Transactions not yet approved by the Customer's Users. Transactions in this list affect the amount of the future balance of the accounts (in the OB menu item *Account information -> Summary of Accounts*). User must validate the Transaction with the password no more than within 100 (one hundred) days after its entering (otherwise it will not be executed);
6.5.2. **Signed**: User-verified Transactions, which are executed at the Bank. Transactions in this list may be deleted by the User if they are no longer required to be executed;
6.5.3. **Rejected:** User-verified Transactions that were not executed due to insufficient funds in the accounts, errors found or for other reasons. About rejected Transactions User is notified in the OB;
6.5.4. **Completed:** User verified Transactions that have been executed. Information about executed payment instructions is additionally provided in the Account statement, by selecting *Account information -> Statement i*n the OB menu item.
6.5. Transaction execution times are specified on the Bank's website www.sb.lt .
6.6. We recommend that each time when you sign the Transaction, to verify that the Transaction has been successfully executed.

6.7. User must verify at least once a month the information on Transactions executed in the account. The Customer must notify the Bank in writing about inadequately executed Transactions, as well as any other errors, inconsistencies or inaccuracies.

VII. CURRENCY EXCHANGE

7.1. Currency exchange Transactions entered on the Bank's business days before 23:40 are executed on the same Bank's business day. If submitted later, the exchange will be executed on the following Bank's business day.
7.2. If the User chooses and enters exchange at *Contractual Exchange Rate*, this exchange is confirmed or rejected by the Bank's employee on the Bank's business days (during the Bank's business hours).

VIII. TRANSACTION IMPORT

8.1. If the User is an employee of the Customer (legal entity) or has the permission to manage the accounts of another Customer (legal entity) and has an accounting program or other software on its own computer system which prepares credit transfers SEPA and credit transfers not SEPA in advance in ISO 20022 XML format, then such User can import the prepared payment instructions into the OB system by the chosen execution method: single/ batch transaction processing.
8.2. If the Customer does not have programs that prepare payment instructions in the required ISO 20022 XML format, he can use the converter function in the IB. This function is used to convert datasets with extensions: .mokesis, .taresis or .xml to transfers in ISO 20022 XML format.

IX. ADDITIONAL INFORMATION

9. The Bank undertakes to block the use of the OB and the App if the Customer/User:
9.1.1. Submits a written request after arriving to the Bank's office during Bank's working time;
9.1.2. Calls 1813 (+370 37 301 337 from abroad);
9.1.3. Calls another telephone number given on the Bank's website;
9.1.4. Incorrectly enters the login password for 5 (five) times;
9.1.5. 3 (three) times incorrectly enters the code from PIN card, SMS message/ generated by the Generator, it will be temporarily blocked, and after incorrectly entering the code 3 times afterwards - it will be blocked. Using the Identity authentication instrument issued not by the Bank, the blocking is carried out in accordance with the requirements of third parties.
9.2. If User forgets/loses the identity verification instrument(s) issued by the Bank or if the Bank system blocks the use of the OB and the App the Customer must arrive at any branch of the Bank (with a personal identity document)
9.3. Before login to the OB, the User must check whether in the web browser:
9.3.1. a correct website address is shown: https://online.sb.lt/, it must begin with „https", not with „http";
9.3.2. the page security certificate must be valid: the address line of the browser must have a lock symbol and words "Siauliu Bankas AB [LT]" should be green (or black on a green background, depending on the browser). If the words are missing or the browser warns about invalid security certificate, do not login to the OB and immediately notify the Bank.
9.4. After 12 (twelve) minutes of no User's action on the OB, the message is displayed for 3 (three) minutes that the session will end immediately, one of the two buttons can be pressed during this time: Continue Work or Finish Work. If within 3 (three) minutes the User does not press any of these buttons, the session closes and the message is displayed until the User has pressed the I Understood button. After clicking this button, the User is directed to the initial OB login window.

X. HARDWARE AND SOFTWARE REQUIREMENTS

10. Customer/ User wishing to use OB must use an instrument that has a legal, updated operating system installed (for example, Windows 7, Windows 8, Windows
10.1. or other operating system supported by other manufacturers) and has excess to the Internet network. The latest, fully supported browser versions of Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome, Opera, or Safari must also be installed. Unsupported and non-upgradable browsers, such as Microsoft Internet Explorer 10 and earlier, are not recommended.
10.2. User must take care of hardware, software or other equipment that connects to the OB, protection against viruses and other threats. For example, keep an updated antivirus system, web browser, and anti-spyware and firewall software. Also make sure that other applications on your computer are upgraded, especially to pay attention to the software used by web browsers: Adobe Flash, Adobe Reader, Java.
10.3. User must log out from the system after finishing his work on the OB by clicking the *Exit* button (in the upper right corner) and close the browser.