

SERVICE OF MOBILE APPLICATION

I. GENERAL PROVISIONS

- 1.1. Mobile application (hereinafter – **App**) means a mobile banking app of the Bank that allows the client to control bills, to perform payment operations, or to receive other services of the Bank through smart devices. An App is a constituent of Internet Bank.
- 1.2. Information about use of the App is provided by phone 1813 (+370 37 301 337 from abroad) and by e-mail kc@sb.lt.

II. SERVICES AND FUNCTIONS

- 2.1. The App may be used having signed the Contract for Internet Bank Service (hereinafter – **IB**) and having downloaded the App from Google Play (in case of Android devices) or App Store (in case of iOS devices). The minimal requirements for the smart device's operating system are Android v5.1 or iOS v9.0.
- 2.2. The App's user may:
 - 2.2.1. review account balances, reserved and blocked amounts;
 - 2.2.2. transfer money to own accounts or those of other clients;
 - 2.2.3. make ordinary or instantaneous payments;
 - 2.2.4. exchange currency;
 - 2.2.5. receive notifications about received amounts or other notifications;
 - 2.2.6. review statuses of performed payment operations;
 - 2.2.7. review and download statements;
 - 2.2.8. receive information about the bank (network of bank's units, exchange rates, rules), write or call the bank;
 - 2.2.9. forward the account number.
- 2.3. The App uses the Lithuanian, English and Russian languages. When the App is downloaded, it is opened in the language set in the smart device. The App user may set the desired language.

III. IDENTITY VERIFICATION

- 3.1. When logging to the App, the Bank identifies the User according to the identity verification means granted to the User/ held by the User.
- 3.2. The User has to log in to the App using the full logging-in data for the first time:
 - 3.2.1. **User ID** – the user name consisting of letters and numbers that cannot be changed indicated in the Contract for Internet Bank Service;
 - 3.2.2. **Initial logging-in password (hereinafter – Initial Password)** – a digital password indicated in the Contract for Internet Bank Service or given in the envelop (no envelops have been issued since 2014 that is used for the first logging-in to IB, App or when the Employee restores the Logging-in Password to the Initial Password. The Initial Password has to be changed to the Logging-in Password created by the User when IB or App is connected to.
 - 3.2.3. **Logging-in Password** – personal password known only to the User and created by the User after the first logging-in to IB, App or after restoration of the Logging-in Password to the Initial Password by the Employee.
 - 3.2.4. **Mobile signature** (hereinafter – **m-signature**) – electronic identity verification tool equivalent to ordinary signature that helps to log in to the App and to sign payment 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.
 - 3.2.5. **Smart ID** – electronic signature that is created when the User downloads free Smart-ID app to his/her smart device from [AppStore](#) or [Google Play](#) and registers the account using the identity verification means issued by the Bank or by m-signature.
 - 3.2.6. **PIN code** – a code of 4 digits created for the User to connect to the App. It may be changed in the App's settings ^{VP}.
- 3.3. If the User uses m-signature, the User has to give his/her mobile phone number to the Bank, where the SIM card with qualified electronic signature is inserted. The codes generated by the Bank are sent there and the User has to confirm them by personally known codes SPIN1 and SPIN2. Codes SPIN1 and SPIN2 are issued by the mobile connection operators who issue SIM cards. If the phone number changes, the User has to notify the Bank thereof in writing without delay.


- 3.4. If the User's access to IB is blocked or suspended, the App cannot be accessed, too. The App may be unblocked when the User comes to the Bank's unit or calls 1813 (+370 37 301 337 from abroad) asking to unblock the Internet Bank.
- 3.5. The User has to ensure safety of identity verification means, to store and keep them confidential, and to undertake all the possible measures to prevent the access and use of them by third parties.
- 3.6. In case of hazard that the identity verification means may be learnt or have been learnt by third parties, or if identity verification means are lost, overtaken by third parties, or the User cannot use them because of any other reasons, also if the User loses the mobile phone, SIM card, the User undertakes to notify the Bank thereof without delay and to ask to block IB and the App. If the User was using Smart- ID and Smart- ID codes (PIN1 and/or PIN2) were learnt by third parties, the User has to delete his/her account from Smart- ID app immediately, by choosing the item "Delete the account" in the app's menu, and to create a new account, where PIN1, PIN2 codes will be changed. Oral notifications to block IB and the App may be accepted by phone available on the Bank's website www.sb.lt. The losses incurred before the Bank's confirmation about blocked identity verification means shall fall under the responsibility of the User. The losses incurred after the Bank's notification to block identity verification means shall be assumed by the Bank, unless the losses were caused by deliberate actions or gross negligence of the User.
- 3.7. In order to protect the User's interests, the Bank shall have the right to block IB or App on own initiative, if the identity verification means have been entered incorrectly several times, and if suspicion arises that these means can/could be used by third parties. IB and App are blocked if:
 - 3.7.1. the Logging-in Password is entered incorrectly 5 (five) times;
 - 3.7.2. incorrect code is entered in Smart- ID app or phone, when m-signature is verified. The blocking takes place in accordance with the requirements of third parties that have issued these means.

IV. LOGGING-IN TO THE APP

- 4.1. In order to log in to the App, the following actions have to be performed:
 - 4.1.1. When the App is downloaded in the used device, the User chooses whether s/he wants to receive the Bank's notifications, including the notifications about money that enters the account. The User may turn on/off these notifications at any time later in the App's settings;
 - 4.1.2. The identity verification measure is chosen: Smart- ID or m-signature;
 - 4.1.3. The User ID provided in the IB contract is entered in the log-in box;
 - 4.1.4. The Initial Password or Logging-in Password is entered in the second box and button "Log in" is pressed;
 - 4.1.5. If the User uses Smart- ID, app Smart- ID is activated and the logging-in information appears on the screen, i.e., name of the service provider (Šiaulių Bankas, AB), security code (xxxx). The User has to make sure that the security code on the app's screen (xxxx) is the same as on the device's screen (xxxx). If they are the same, the User has to enter Smart- ID PIN1 code. If the correct PIN1 code is entered, the logging-in process is finished automatically. If PIN1 code differs, the User has to cancel the process by pressing button "Cancel" of Smart- ID app. If m-signature is used, the User has to check and verify the code received by phone entering sPIN (mobile signature's security) code. If the indicated mobile phone number does not have mobile signature, it may be changed using the setting "Change the phone number" in the App;
 - 4.1.6. Four-digit PIN code is created and confirmed. It will be used to log-in to the App quickly in the future. PIN code is valid for 180 days. When it expires, the User may log in to the App using the full data, such as User ID, password, and by confirming logging-in by m-signature or Smart- ID, and change the code then;
 - 4.1.7. If the User's device supports the fingerprint function, it is suggested to activate it. If the function is not activated, the User may turn it on/off later in the App's settings. When the function is turned on, the User's fingerprint is scanned by putting it on certain place of the mobile phone.
 - 4.1.8. After these actions, the window is opened informing about successful logging-in to the App and it is suggested to press button "Continue";
 - 4.1.9. If the User uses the Initial Password, s/he will be asked to create and confirm a Logging-in Password;
 - 4.1.10. After the first log in, later brief logging-in may be used (by fingerprint or created PIN code).
- 4.2. If the User does not do any actions in the App for 5 (five) minutes, the session is closed, showing the notification *Your session has expired. Please log in again*, until the User closes the notification or touches the screen. Afterwards, the User may access the App by PIN code, fingerprint, or using the full logging-in data, selecting *Log in otherwise*, as provided in par. 4.1.6.
- 4.3. Having finished the work in the App, the User has to leave the system pressing the button "Sign out".

V. ENTRANCE AND SIGNING OF TRANSACTIONS

- 5.1. The User has the right to perform the payment transactions and to receive the services allowed by the Bank for the App, including the services that the Bank will permit to perform/receive in the future.

- 5.2. The User is able to make payments between own accounts, payments to accounts of other Bank's clients, SEPA payments to other banks, instantaneous payments, and to exchange currency.
- 5.3. The payment orders are prepared by choosing a respective item on the menu and completing the required data. When the payment order is filled in and the Beneficiary's box is chosen, the Beneficiary's name is entered into the opened window and the button *Apply* is pressed; or the beneficiary may be found by entering three symbols into the search line. The beneficiaries can be found among the recent payments or from template payments. When the necessary beneficiary is found and pressed, the data of the Beneficiary and Beneficiary's account are entered automatically into the payment order.
- 5.4. The User has to sign the prepared payment order by pressing the confirmation button to proceed. The User signs the payment transactions using the available identity verification means (Smart- ID or m-signature's sPIN2 code). When the payments are made to the client's account in the Bank and the currency is exchanged in the account, the transactions are processed only after the confirmation button is pressed, without need for identity verification measure. This condition is applied if the payment transaction is confirmed by the User, who has the right of the first signature.
- 5.5. By signing the payment transaction, the User guarantees correctness of the data on the payment order and sufficient funds to perform the transaction and to pay the Bank's fees.
- 5.6. The Bank performs the payments by the App under the conditions of *Rules of Payment Services of Šiaulių Bank*, which are available at www.sb.lt.
- 5.7. When the payment transactions are made, it is recommended to check whether the signed transactions have been fulfilled successfully. The performed transactions may be reviewed in the account statement.
- 5.8. *Not confirmed*, *Rejected* transactions or transactions that are *Processed* may be reviewed in the section of payment status, by pressing a bell sign . The Users of the work group may also review the transactions that are being confirmed.
- 5.9. The payment order formed and transmitted by the App, the performed transaction, the made contract and other notifications or statements made with the help of identity verification means have the same legal power as written documents signed by the User (client). They are regarded as the will expressed by the Client and authorisation of transactions and payments.

VI. REQUIREMENTS FOR HARDWARE AND SOFTWARE

- 6.1. The User has the right to use the App if the technical means, hardware, software and other equipment used by the User satisfy the Bank's requirements. The User undertakes to apply all the possible safeguards in his/her computer, software or other equipment that would enable safe transactions, without disclosing any data to third parties. The User shall be responsible for the consequences related to insufficient protection of the used system.
- 6.2. The User has to use the device with legal updated operating system (Android or iOS) and Internet connection. Besides, the browsers supported by the manufacturers have to be installed: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Safari or Android 7.0 Nougat. It is recommended to use the newest.
- 6.3. The User has to take care about protection of the computer, software or other equipment used to access the App from viruses and other threats, for example, to regularly update 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).
- 6.4. The Bank shall not be held liable for the User's inability to use the App because of absence of the needed computer, software or other equipment, its failure, faults in telecommunications networks, because of the fault of companies providing telecommunications services, or because of lost, deteriorated information due to disorders in the telecommunications networks, etc.
- 6.5. The Bank has the right to suspend the use of the App temporarily because of technical, system's updating works, unforeseen hindrances or other important reasons, provided the User has been notified thereof appropriately via IB and/or on the Bank's website www.sb.lt.