УСЛУГА МОБИЛЬНОГО ПРИЛОЖЕНИЯ

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Мобильное приложение (далее – **«Приложение»**) – приложение мобильного банкинга Банка, позволяющее клиенту управлять счетами, совершать платежные операции или получить другие услуги Банка с использованием смарт-устройств. Приложение является составной частью интернет-банка.

1.2. Информация об использовании Приложения предоставляется по телефону 1813 (+370 37 301 337 при звонке из-за границы), а также по электронной почте kc@sb.lt.

II. УСЛУГИ И ФУНКЦИИ

2.1. Приложением можно пользоваться после подписания Договора об оказании услуги интернет-банка (далее – **«ИБ»**) и скачивания Приложения из интернет-магазинов Google Play (для устройств с Android) или App Store (для устройств с iOS). Минимальные требования смарт-устройства к операционной системе – Android v5.1 или iOS v9.0.

2.2. Пользователь приложения может:

2.2.1 проверить остатки счетов, забронированные или заблокированные суммы;

2.2.2. перечислить денежные средства на свои или счета других клиентов;

2.2.3. произвести стандартные или мгновенные платежи;

2.2.4. совершить операции по обмену валюты;

2.2.5. получить сообщения о поступлении средств на счет и другие сообщения;

2.2.6. просмотреть состояния выполненных платежных операций;

2.2.7. просмотреть выписки и их скачать

2.2.8. получить информацию о банке (сети подразделений банка, курсах валют, правилах), написать или позвонить в банк;

2.2.9. перенаправить номер счета.

2.3. В Приложении используются литовский, английский и русский языки. После скачивания Приложения оно открывается на том языке, который установлен в смарт-устройстве. Пользователь Приложения может установить приемлемый ему язык.

III. ПОДТВЕРЖДЕНИЕ ЛИЧНОСТИ

3.1. При подключении к Приложению Банк устанавливает личность Пользователя по предоставленным Пользователю имеющимся у Пользователя средствам аутентификации.

3.2. Первый раз к Приложению Пользователь должен подключиться с полным подключением с использованием:

3.2.1. **ID Пользователя** – указанное в *Договоре предоставления услуги интернет-банка* имя пользователя, состоящее из букв и цифр, оно является неизменным;

3.2.2. **Первичного входного пароля (далее – «Первичный пароль»)** – указанный в *Договоре предоставления услуги интернет-банка* или содержащийся в конверте (с 2014 г. конверты не выдаются) цифровой пароль, используемый: для первого подключения Пользователя к ИБ или Приложению или в случае восстановления Работником Пароля для входа в Первичный пароль. Первичный пароль после подключения к ИБ или Приложению подлежит изменению на придуманный Пользователем Пароль для входа.

3.2.3. **Пароля для входа** – созданный Пользователем после первого подключения к ИБ или Приложения либо после восстановления Работником Входного пароля на Первичный пароль личный, только Пользователю известный пароль.

3.2.4. **Мобильной подписи** (далее – **«М. подпись»**) – средство подтверждения личности, электронный аналог обычной подписи, которое с помощью мобильного телефона и СИМ-карты мобильного телефона позволяет безопасным и удобным способом подключиться к Приложению и подписать платежные операции. СИМ-карту, имеющую функцию мобильной подписи, Клиент может получить в представительстве оператора мобильной связи.

3.2.5. **Smart ID** – электронная подпись, которая создается Пользователю после бесплатной инсталляции на смарт-устройство приложения Smart-ID из интернет-магазинов AppStore или Google Play и регистрации учетной записи с использованием выданных в Банке средств аутентификации или М. подписи.

3.2.6. **ПИН-кода** – созданный Пользователем код из 4 цифр для подключения к Приложению, который может быть изменен в настройках Приложения VP.

3.3. В случае использования Пользователем М. подписи он должен указать Банку свой номер мобильного телефона, в котором установлена СИМ-карта, имеющая электронную квалифицированную подпись,

на который отправляются сгенерированные Банком коды, которые Пользователь подтверждает только ему лично известными кодами SPIN1 и SPIN2. Коды SPIN1 и SPIN2 предоставляются операторами мобильной связи, выдающими СИМ-карты. В случае изменения номера телефона Пользователь незамедлительно в письменной форме должен информировать об этом банк.

3.4. Если подключение Пользователя к ИБ заблокировано / приостановлено, подключение к Приложению также не представляется возможным. Снятие блокировки Приложения осуществляется только после прибытия Пользователем в подразделение Банка или обращения по телефону 1813 (+370 37 301 337 при звонке из-за границы) с просьбой разблокировать интернет-банк.

3.5. Пользователь должен обеспечить безопасность Средств аутентификации, хранить их в тайне, а также принимать все возможные меры по исключению возможности использования их третьими лицами или сообщения между ними.

3.6. В случае возникновения угрозы того, что средства аутентификации могут узнать третьи лица или в случае их утери, утраты, завладения ими, получения к ним доступа третьими лицами или невозможности Пользователем владения Средствами аутентификации, а также в случае утери Клиентом мобильного телефона, СИМ-карты, Пользователь обязуется без промедления информировать об этом Банк с просьбой заблокировать ИБ и Приложение. В случае, если Пользователь пользовался Smart-ID и коды Smart-ID (PIN1 и/или PIN2) стали известными третьим лицам, Пользователь должен немедленно в приложении Smart-ID удалить созданную им учетную запись, выбрав в меню приложения пункт «Удалить учетную запись» и создать новую учетную запись, во время создания которой можно будет изменить коды PIN1, PIN2. Устные сообщения о блокировке доступа к ИБ и Приложению принимаются по телефону, указанному на веб-сайте Банка www.sb.lt. Убытки, возникшие до момента отправления Банку предусмотренного уведомления о блокировке Средств аутентификации, несет Клиент. Убытки, возникшие после отправления Банку предусмотренного уведомления о блокировке Средств аутентификации, несет Банк, за исключением случаев, когда убытки возникли по умыслу или крайней неосторожности Пользователя.

3.7. Банк в целях защиты интересов Пользователя вправе по собственной инициативе заблокировать доступ к ИБ или Приложению в случае неправильного использования Средств аутентификации ряда раз, а также в случае возникновения подозрения, что данными средствами могут /могли воспользоваться третьи лица. Доступ к ИБ или Приложению блокируется в случае:

3.7.1. неправильного ввода Входного пароля 5 (пяти) раз;

3.7.2. неправильного ввода кода в приложении Smart-ID или телефоне при подтверждении кода М. подписи. Блокировка осуществляются в соответствии с требованиями третьих сторон, выдавших данные средства.

IV. ПОДКЛЮЧЕНИЕ К ПРИЛОЖЕНИЮ

4.1. При подключении к Приложению необходимо выполнить следующие действия:

4.1.1. после инсталляции Приложения на используемое устройство Пользователь должен выбрать, желает ли он получать сообщения от Банка, включая сообщения о поступлении средств на счет. Данные сообщения Пользователь может выключить/включить в любое время позднее в настройках Приложения;

4.1.2. выбрать средство аутентификации: Smart-ID или М. подпись;

4.1.3. в первом поле окна подключения ввести указанное в договоре ИБ имя ID Пользователя;

4.1.4. во втором поле окна подключения ввести Первичный пароль или Входной пароль и нажать «Подключиться»;

4.1.5. в случае подключения Пользователем со Smart-ID, активизируется приложение Smart-ID, в окне которого отображается информация об инициировании подключения к Приложению, т.е. наименование поставщика услуг (Šiaulių bankas, AO), код безопасности (xxxx). Пользователь должен убедиться, что код безопасности на экране приложения (xxxx) совпадает с номером (xxxx) в окне устройства. В случае совпадения, Пользователь должен ввести код PIN1 Smart-ID. После ввода правильного кода PIN1 автоматически завершается процесс подключения к Приложению. В случае, если код PIN1 не совпадает, Пользователь должен прервать процесс подключения путем нажатия в приложении Smart-ID кнопки «Отменить». В случае подключения с использованием М. подписи, Пользователь должен проверить полученный на телефон код и его подтвердить путем ввода кода sPIN мобильной подписи (защитный код мобильной подписи). В случае отсутствия в указанном номере мобильного телефона мобильной подписи, ее можно изменить, выбрав в Приложении «Изменить номер телефона»;

4.1.6. создать и подтвердить ПИН-код из четырех цифр, с использованием которого можно будет подключаться к Приложению коротким способом. ПИН-код действует 180 дней. После истечения срока его действия Пользователь к приложению должен подключиться полным подключением путем ввода своих ID Пользователя, входного пароля и подтверждения подключения М. подписью или Smart-ID и его изменить;

4.1.7. если устройство Пользователя поддерживает функцию отпечатка пальца, устройство предлагает ее активизировать. В случае отказа от активации данной функции Пользователь

позднее может ее включить/выключить в настройках Приложения. После включения функции сканирование отпечатка пальца Пользователя осуществляется приложив его к отведенному для этого месту на мобильном телефоне.

4.1.8. после выполнения данных действий открывается окно, подтверждающее успешное подключение к Приложению, с предложением нажать кнопку «Продолжить»;

4.1.9. в случае подключения Пользователем с Первичным входным паролем, приложение его попросит создать и подтвердить Входной пароль.

4.1.10. после подключения первый раз в следующие разы к Приложению можно подключаться коротким способом – с отпечатком пальца или придуманным ПИН-кодом.

4.2. В случае если Пользователь в течение 5 (пяти) минут не выполняет никаких действий в Приложении, сессия закрывается и отображается сообщение *Ваша сессия завершилась*. *Подключитесь заново, пожалуйста* до момента, пока Пользователь не закрывает сообщения или не прикасается к экрану устройства. После данных действий Пользователь может подключиться к Приложению с ПИН-кодом или отпечатком пальца, или полным подключением, выбрав *Подключиться другим способом*, как указано в п. 4.1.6.

4.3. После завершения работы в Приложении Пользователь должен отключиться от системы путем нажатия кнопки «Отключиться».

V. ВВОД И ПОДПИСАНИЕ ОПЕРАЦИЙ

5.1. Пользователь вправе совершать те платежные операции и получить те услуги, которые Банк разрешает совершать с использованием Приложения, включая услуги, которые Банк разрешит совершать/получать в будущем.

5.2. Пользователь в Приложении может совершать платежи между своими счетами, платежи на счета других клиентов Банка, платежи SEPA в другие Банки, экспресс платежи и обмен валюты.

5.3. Подготовка платежных поручений осуществляется путем выбора соответствующего пункта в меню Приложения и ввода требующихся данных. При заполнении платежного поручения и выборе поля Получателя в открывшемся окне вводится наименование Получателя и нажимается *Использовать* либо осуществляется поиск получателя путем ввода трех символов. С помощью поиска приводятся получатели из списка недавно выполненных платежей, списков получателей или заготовок. После обнаружения требующегося получателя и нажатия на него платежное поручение автоматически пополняется информацией о Получателе и счете Получателя.

5.4. Подготовленное платежное поручение для его выполнения Пользователь должен подписать путем нажатия кнопки подтверждения. Платежные операции подписываются Пользователем с использованием средств аутентификации (Smart-ID или кодом sPIN2 М. подписи). При выполнении переводов денежных средств между счетами клиента в Банке и выполнении обмена валюты на счете такие операции осуществляются только нажатием кнопки подтверждения без необходимости подписания их средством аутентификации. Данное условие распространяется в случае подтверждения платежной операции Пользователем, имеющим право первой подписи.

5.5. Подтверждением подписью платежной операции Пользователь заверяет, что указанные в платежном поручении данные являются правильными и на счете имеется достаточно средств для совершения операции и уплаты комиссий Банка.

5.6. Представленные Пользователем с использованием Приложения платежные поручения выполняются Банком на условиях, предусмотренных в *Правилах платежных услуг AO Šiaulių bankas*, которые публикуются по адресу www.sb.lt.

5.7. После выполнения платежных операций рекомендуем проверить, были ли подписанные операции успешно выполнены. Выполненные операции можно просмотреть в выписке со счета.

5.8. *Неподтвержденные, Отклоненные, Выполняемые* операции можно просмотреть в части состояний платежа путем нажатия колокольчика 🔔. Пользователи рабочей группы могут просмотреть и *Подтверждаемые* операции.

5.9. Сформированное в Приложении и переданное с использованием средств аутентификации платежное поручение, выполненная операция, заключенный договор и другие сообщения или заявления имеют такую же юридическую силу как и письменный документ, подписанный Пользователем (клиентом) и признаются излиянием воли Клиента и авторизацией сделок и платежных операций.

VI. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

6.1. Пользователь вправе пользоваться Приложением, если используемые им технические средства, компьютерное, программное и иное обеспечение отвечает установленным Банком требованиям. Пользователь обязуется в используемом им компьютерном, программном или ином обеспечении соблюдать все возможные меры безопасности, позволяющие совершать операции безопасным способом и исключающие раскрытие любых данных третьим лицам. Пользователь несет ответственность за последствия, которые будут связанны с недостаточной защитой используемой системы.

6.2. Пользователь должен использовать средство, в котором инсталлирована легальная, обновленная операционная система (Android или iOS) и имеется сеть интернета. Также должны быть инсталлированы поддерживаемые производителями версии браузеров - Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Safari или Android 7/0 Nougat. Рекомендуется использовать последнюю версию.

6.3. Пользователь обязан заботиться о компьютерном, программном и другом обеспечении, из которого осуществляется подключение к ИБ, защитой от вирусов и других угроз, например, постоянно обновлять антивирусную систему, браузер и антишпионские программы (англ anti-spyware) и межсетевые экраны (англ. firewall). Также позаботиться об обновлении других прикладных компьютерных программ, особое внимание обратить на программы, которые используются браузерами – Adobe Flash, Adobe Reader, Java.

6.4. Банк не несет ответственности в случае, если Пользователь не мог пользоваться Приложением по причине отсутствия у него компьютерного, программного или иного обеспечения или оно не работало, или в связи со сбоями в телекоммуникационных сетях, либо по вине компаний, оказывающих телекоммуникационные услуги, не мог воспользоваться Электронными каналами, или по причине сбоев в телекоммуникационных сетях информация была утрачена, искажена и т.п.

6.5. Банк вправе временно приостановить доступ к Приложению в связи с выполнением технических работ, работ по обновлению системы, непредусмотренными помехами или другими уважительными причинами, соответствующим образом предупредив об этом Пользователя через ИБ и /или в открытом доступе на веб-сайте Банка www.sb.lt.

AO Šiaulių bankas