Инструкция пользователя системы электронного банкинга StarAccess

Использование мобильного приложения «Google Authenticator»
для генерации одноразовых паролей (OTP)

Версия 3.
Дата: 23.01.2017

1. Общие положения.

В инструкции используются следующие термины и сокращения:

StarAccess – система электронного банкинга StarAccess.
Банк – АО "УкрСиббанк".
Клиент – юридическое лицо или физическое лицо – субъект хозяйствования (в т.ч. предприниматели) – клиент банка, эксплуатирующий StarAccess.
Пользователь – сотрудник клиента, который работает в StarAccess.
АРМ – автоматизированное рабочее место клиента системы электронного банкинга StarAccess.
Google Authenticator – приложение, которое используется для создания кодов (одноразовых паролей) двухэтапной аутентификации. Приложение доступно для смартфонов с ОС Android, iOS, BlackBerry. Это альтернативный способ получения OTP, который может использоваться при двухфакторной аутентификации и/или подтверждении документов в StarAccess. Основным способом подтверждения является SMS или OTP-токен.

В StarAccess реализована поддержка приложения "Google Authenticator" для получения (генерации) одноразовых паролей (OTP) непосредственно на смартфоне Пользователя и подтверждения операций без необходимости получения OTP в SMS. Пользователи самостоятельно принимают решение об использовании данного альтернативного способа, и в любой момент могут вернуться к основному.

Внимание! Сервис доступен только клиентам, которым подключена опция многофакторной аутентификации и/или подтверждения документов и способ получения паролей (OTP) в SMS на безопасный номер мобильного телефона (регистрируется сотрудником Банка в карточке Клиента в StarAccess на основании «Заявления на активацию/деактивацию "SMS-OTP" в системе StarAccess». Для замены/добавления номера мобильного телефона необходимо обратиться в обслуживающее отделение Банка и подписать указанное заявление).

2. Работа с Google Authenticator.

2.1. Установка Google Authenticator.

Установить приложение Google Authenticator (Рис.1) на свой смартфон можно из Google PlayMarket либо Apple AppStore. Общую информацию о приложении, а также ссылку "Как установить Google Authenticator", можно посмотреть после входа в StarAccess в разделе: "Мои данные" / "Google Authenticator" (Рис.2) по ссылке «Как установить Google Authenticator?» (открывает в новом окне соответствующую страницу справки Google).

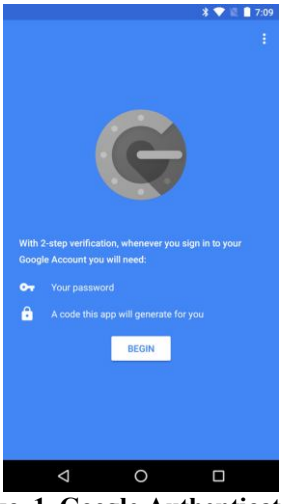

Рис. 1. Google Authenticator

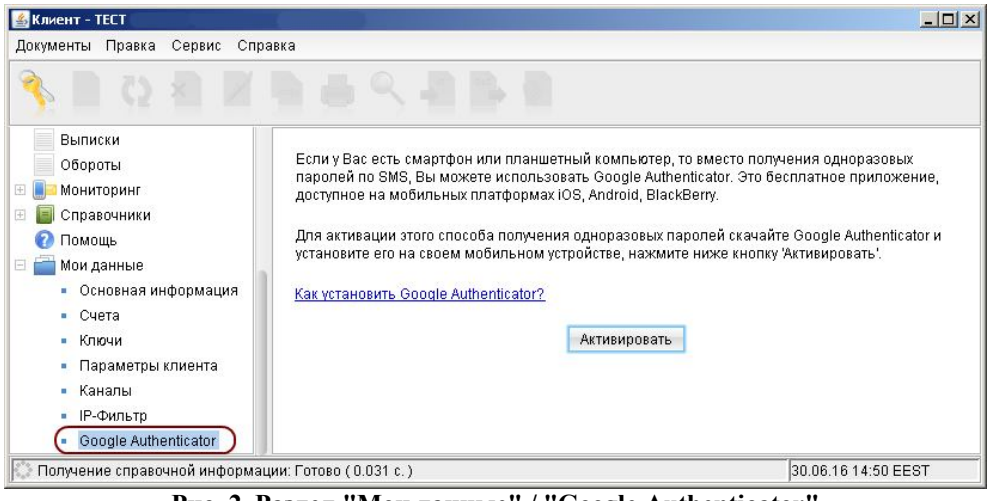

Рис. 2. Раздел "Мои данные" / "Google Authenticator"

2.2. Активация Google Authenticator.

Для активации Google Authenticator, в разделе "Мои данные" / "Google Authenticator" (Рис.2.):

- нажать кнопку "Активировать". В результате будет выполнен переход на «Шаг 1. "Подтверждение"» (Рис.3), а пользователю будет отправлен OTP в SMS на зарегистрированный в StarAccess номер мобильного телефона.

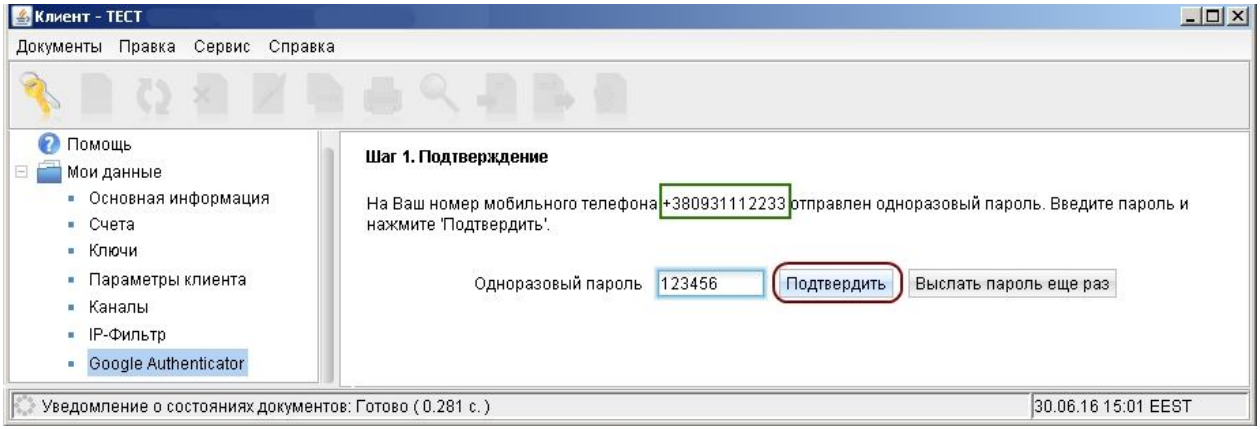

Рис. 3. Шаг 1. "Подтверждение".

- ввести OTP из SMS и нажать кнопку "Подтвердить" (Рис.3). При успешном подтверждении будет выполнен переход на следующий шаг "Сканировать код" (Рис.4).

Внимание! Если введен OTP, срок действия которого истек (аналогично сроку действия OTP для подтверждения документов или многофакторной аутентификации), на экран будет выведено сообщение с ошибкой и выполнена повторная отправка SMS с новым OTP. Если SMS по каким-либо причинам не получен, необходимо нажать кнопку "Выслать пароль еще раз". Если Пользователь неверно ввел OTP заданное в StarAccess количество раз подряд, работа учетной записи Пользователя блокируется, необходимо обратиться в обслуживающее отделение для разблокировки.

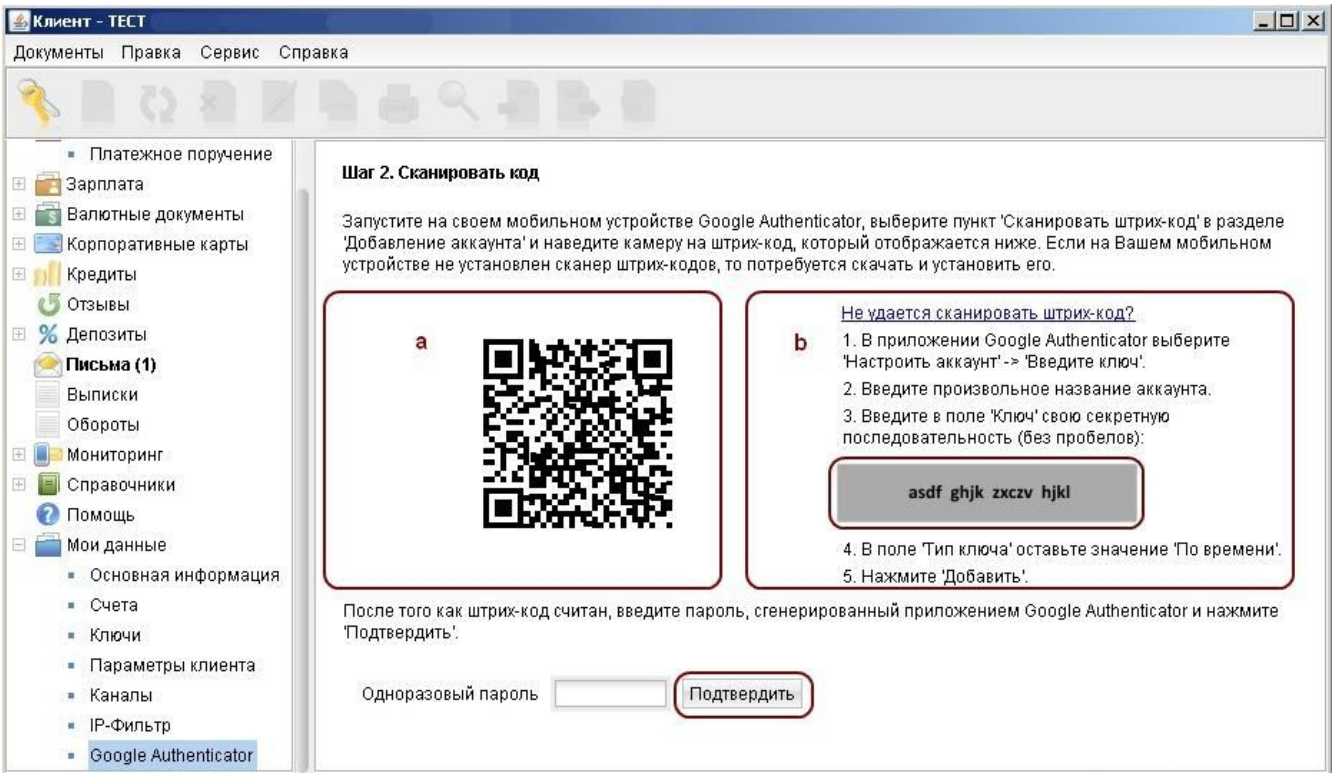

Рис 4. Сканирование кода для создания учетной записи.

- запустить приложение Google Authenticator на смартфоне и добавить новую учетную запись (в разделе «Добавление аккаунта»):
    a. выбрать пункт «Сканировать штрих-код» (в разделе «Добавление аккаунта»), сканировать штрих-код (Рис.4, блок a);
    b. если не удается сканировать щтрих-код, в настройках учетной записи выбрать пункт «Введите ключ», а в StarAccess нажать ссылку "Не удается сканировать штрих-код?" и ввести ключ вручную, следуя дальнейшим инструкциям (Рис.4, блок b).
- вести OTP в поле «Одноразовый пароль» в StarAccess, сгенерированный приложением Google Authenticator, нажать кнопку "Подтвердить" (Рис.4).

Внимание! Если после ввода одноразового пароля, сгенерированного приложением Google Authenticator, возникает ошибка "Неверный одноразовый пароль. Повторите попытку", необходимо выполнить синхронизацию времени в приложении:

1. Откройте главное меню приложения Google Authenticator.
2. Зайдите в **Настройки**.
3. Нажмите **Коррекция времени для кодов**.
4. Выберите **Синхронизировать**.

После успешного подтверждения отображается информация о завершении активации (Рис.5). Данная информация будет отображаться и при последующих входах в StarAccess.

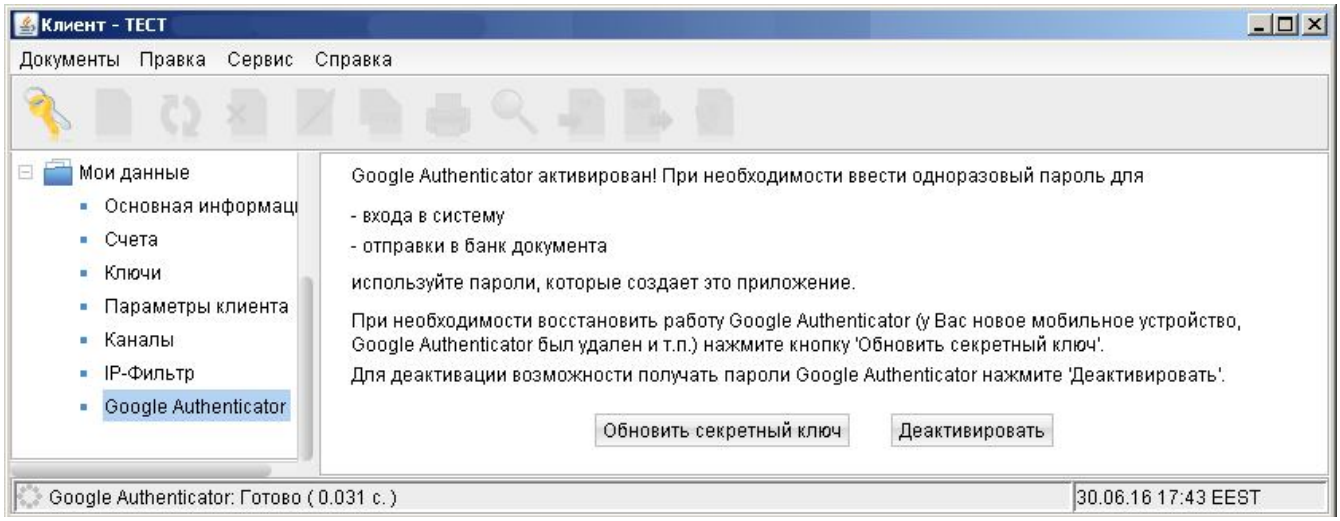

Рис. 5. Завершение активации.

Внимание! Каждый Пользователь одновременно может иметь только одну учетную запись Google Authenticator в StarAccess.

2.3. Деактивация Google Authenticator.

Для деактивации способа получения OTP с помощью Google Authenticator необходимо нажать кнопку "Деактивировать" в разделе "Мои данные" / "Google Authenticator" (Рис.5). Далее следует Шаг 1. "Подтверждение" (Рис.3). При успешном выполнении секретная последовательность удаляется, на экран выводится сообщение (Рис.6), выполняется переход в раздел "Мои данные" / "Google Authenticator" (Рис.2), Google Authenticator деактивирован. Для повторной активации Google Authenticator, необходимо выполнить действия, указанные в Разделе 2.2. данной Инструкции.

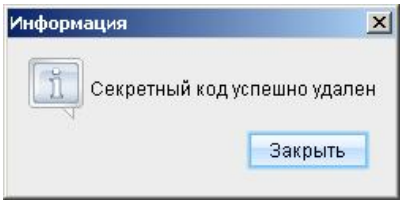

Рис.6. Удаление секретной последовательности.

2.4. Обновление секретного ключа Google Authenticator.

У Пользователя может возникнуть необходимость обновить секретную последовательность (секретный ключ) Google Authenticator (например, при повторной установке мобильного приложения, смене устройства и т.п.). В данном случае, необходимо перейти в раздел "Мои данные" / "Google Authenticator" и нажать кнопку "Обновить секретный ключ". По сути, процедура обновления аналогична активации новой учетной записи Google Authenticator (см. Раздел 2.2.). После корректного выполнения всех действий, указанных в Разделе 2.2., старая секретная последовательность удаляется, а новая активируется. Если процесс обновления по каким-либо причинам не завершен (выполнен переход в другое меню, осуществлен выход из StarAccess и т.д.), текущая секретная последовательность (секретный ключ) останется без изменений.

3. Дополнительная информация.

Способ получения паролей Google Authenticator **устанавливается по умолчанию при подтверждении входа в StarAccess и/или подтверждении документов**. При этом у пользователя остается возможность выбрать любой другой из доступных способов получения пароля: SMS или OTP-токен (Рис.7).

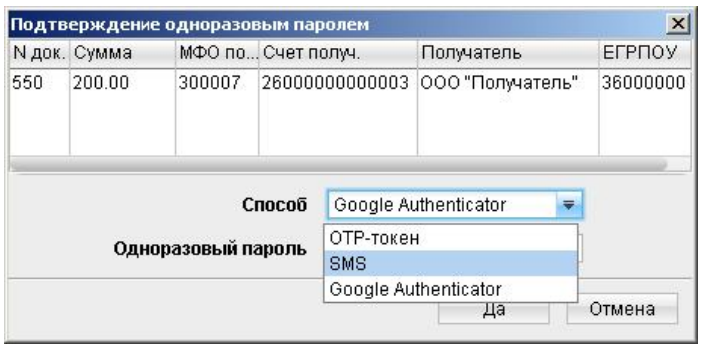

Рис. 7. Выбор способа получения пароля при подтверждении документа.