

Регистрационный № 134

**ИНСТРУКЦИЯ
ПО ПРИМЕНЕНИЮ E-TOKEN ПРИ ПОЛЬЗОВАНИИ УСЛУГОЙ ИНТЕРНЕТ
- БАНКИНГА «SAM.ONLINE»**

1. Общие положения

- 1.1. Настоящая Инструкция регламентирует порядок использования E-TOKEN в системе интернет – банкинга «SAM.online».
- 1.2. E-TOKEN представляют собой устройства для защищенного хранения закрытых ключей ЭЦП клиента. Главное достоинство E-TOKEN — защищенное хранение и неизвлекаемость (невозможность считывания) закрытого ключа ЭЦП. Закрытый ключ ЭЦП хранится в защищенной памяти E-TOKEN и ни при каких условиях не может быть считан из него.
- 1.3. E-TOKEN марки SafeNet iKey 1032 предназначен для работы на следующих платформах: Windows 95, 98, NT, 2000, XP, 2003 и 7.

2. Установка драйвера для E-TOKEN для Windows

- 2.1. Драйвер необходим для работы с E-TOKEN в системе интернет - банкинга «SAM.online».

Внимание!

Не вставлять E-TOKEN в USB-порт компьютера до установки драйвера. Во время установки драйвера все приложения должны быть закрыты во избежание ошибки разделения файлов. Для установки драйвера пользователю необходимы права администратора системы.

- 2.2. Для установки драйвера запустите установочный файл iKeyAll.exe, который вы получили на диске от сотрудника банка. На экране появится следующее окно:



Рис.1

Для продолжения нажмите кнопку «Next» (Рис.1)

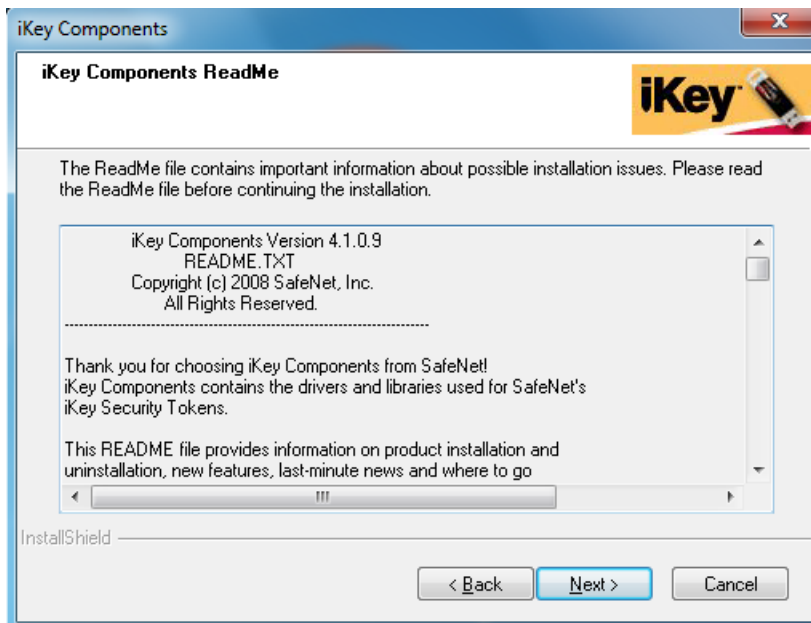


Рис.2

После ознакомления с файлом Readme нажмите кнопку «Next» (Рис.2)



Рис.3

Далее появляется окно с лицензионным соглашением (Рис.3). После ознакомления с ним нажмите кнопку «Yes»

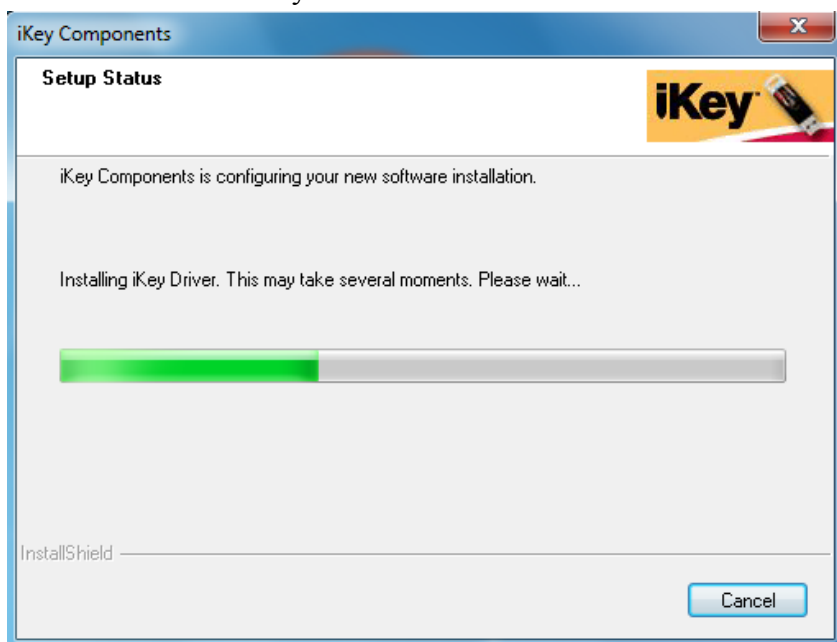


Рис.4

Подождите, пока установочная программа установит необходимые компоненты на ваш компьютер (Рис.4)

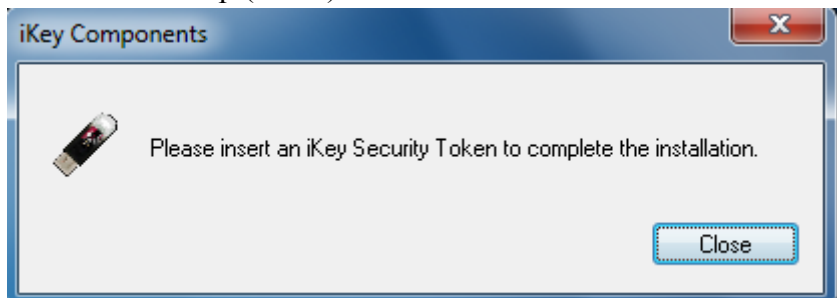


Рис.5

Далее программа попросит вас вставить E-TOKEN в USB-порт (Рис.5). После того, как вы вставите E-TOKEN, выйдет следующее окно:

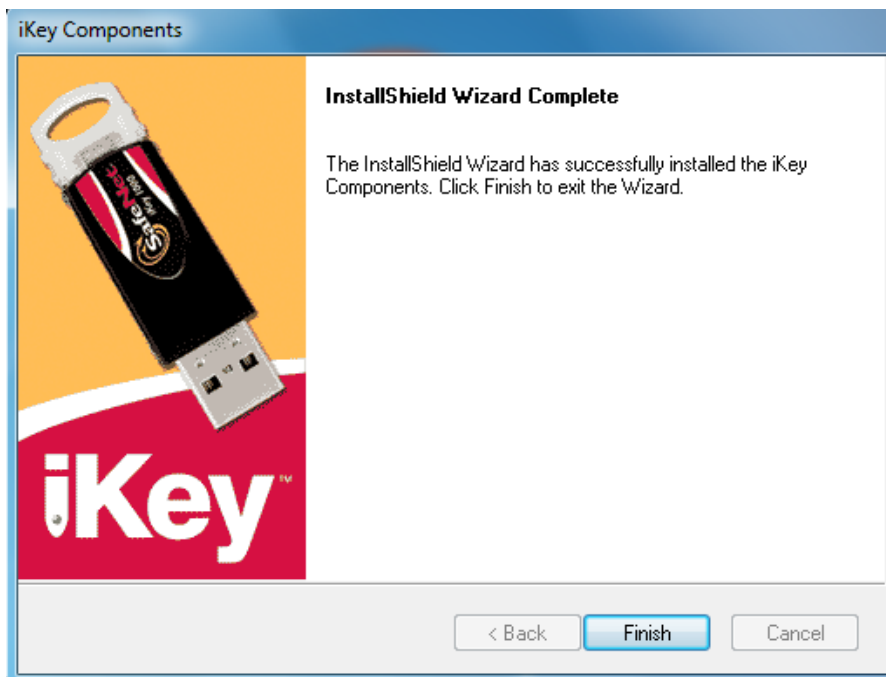


Рис.6

Нажмите кнопку «Finish» для окончания работы программы установки драйвера (Рис.6)

3. Подтверждение документов в интернет – банке «SAM.online»

3.1. Для подтверждения платежа, совершаемого с помощью дистанционного доступа необходимо вставить E-TOKEN в USB-порт, набрать платеж и отправить в банк. Перед отправкой система запросит у вас пароль. В появившемся окне нужно ввести пароль к закрытому ключу, который был ранее установлен пользователем при установке закрытого ключа в память E-TOKEN (Рис.7).

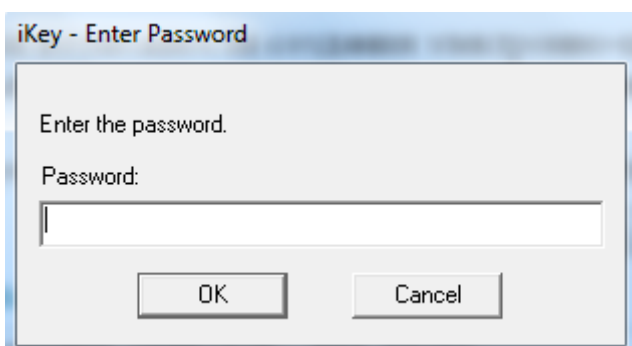


Рис. 7

4. Эксплуатация и хранение E-TOKEN

- 4.1. E-TOKEN являются чувствительными электронными устройствами. При их хранении и эксплуатации пользователю необходимо соблюдать ряд правил и требований, при нарушении которых указанные устройства могут выйти из строя.
- 4.2. Следующие правила эксплуатации и хранения обеспечат длительный срок службы E-TOKEN, а также сохранность конфиденциальной информации пользователя.
 - Необходимо оберегать E-TOKEN от сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т.п.).
 - E-TOKEN необходимо оберегать от воздействия высоких и низких температур. При резкой смене температур (вносе охлажденного устройства с мороза в теплое помещение) не рекомендуется использовать E-TOKEN в течение 3 часов во избежание повреждений из-за сконденсированной на электронной схеме влаги. Необходимо оберегать E-TOKEN от попадания на них прямых солнечных лучей.

- Необходимо оберегать E-TOKEN от воздействия влаги и агрессивных сред.
- Недопустимо воздействие на E-TOKEN сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества.
- При подключении E-TOKEN к компьютеру не прилагайте излишних усилий.
- E-TOKEN в нерабочее время необходимо всегда держать закрытым во избежание попадания на разъем E-TOKEN пыли, грязи, влаги и т.п. При засорении разъема E-TOKEN нужно принять меры для его очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо.
- Не разбирайте E-TOKEN
- Необходимо избегать скачков напряжения питания компьютера и USB-шины при подключенном USB-порте, а также не извлекать E-TOKEN из USB-порта во время записи и считывания.
- В случае неисправности или неправильного функционирования E-TOKEN обращайтесь в Банк.

5. Меры предосторожности при работе с E-TOKEN

- 5.1. Не допускается передача E-TOKEN третьим лицам. Не сообщайте третьим лицам пароль от ключей ЭЦП!
- 5.2. В случае утери (хищения) или повреждения E-TOKEN необходимо немедленно связаться с банком.
- 5.3. Не допускается постоянное бесконтрольное подключение к компьютеру E-TOKEN. E-TOKEN должен быть подключен к компьютеру только на время работы с системой "SAM.online".
- 5.4. Клиенту необходимо строго соблюдать порядок работы в системе "SAM.online", а именно:
- соблюдать регламент доступа к компьютеру, к E-TOKEN с закрытыми ключами ЭЦП;
 - использовать системное и прикладное ПО, полученное из доверенных источников, а также регулярно обновлять указанное ПО;
 - использовать и регулярно обновлять специализированное ПО для защиты информации — антивирусное ПО, средства защиты от несанкционированного доступа, персональные межсетевые экраны и пр.;
- соблюдать правила информационной безопасности при работе в Интернете — не посещать подозрительные сайты, не устанавливать программы из недоверенных источников, не открывать файлы от неизвестных отправителей и пр.;
 - немедленно информировать банк о внештатных ситуациях и подозрениях на нарушение безопасности рабочего места (заражение компьютера вирусом или трояном).

6. Смена пароля к закрытому ключу

- 6.1. Для смены пароля доступа к закрытому ключу необходимо в правой нижней части экрана найти иконку драйвера iKey, нажать на иконку правой клавишей мыши и выбрать «Open», как на рисунке 8. В появившемся окне выберите вкладку «User Tools» (Рис.9) и нажмите кнопку «Change Password».

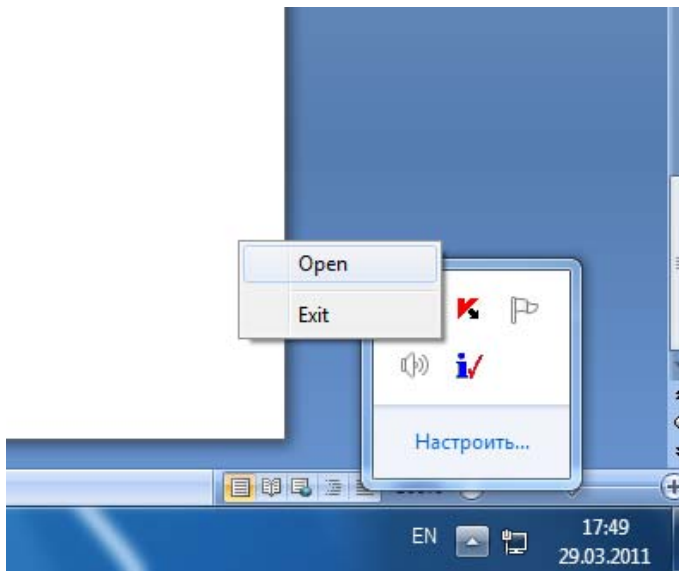


Рис.8

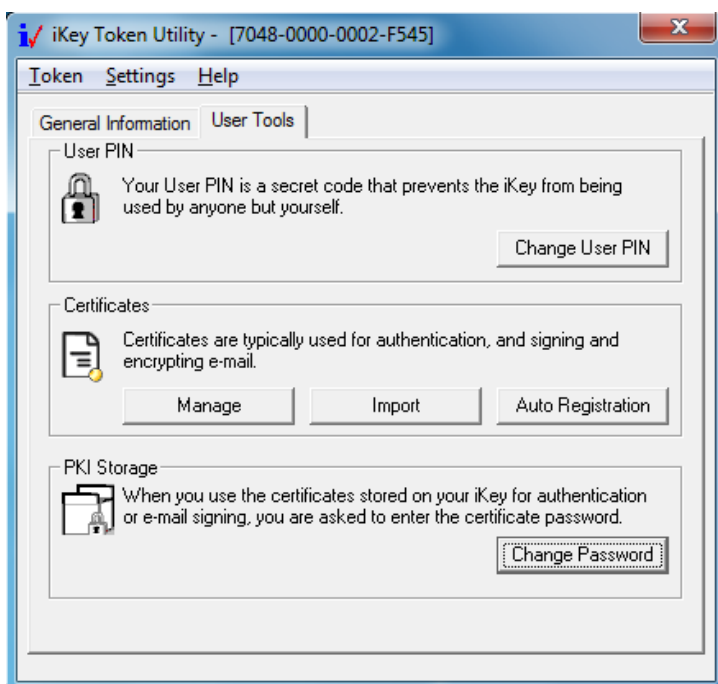


Рис.9

Далее, в первом поле необходимо ввести действующий пароль, а в двух следующих полях – новый пароль (Рис.10).

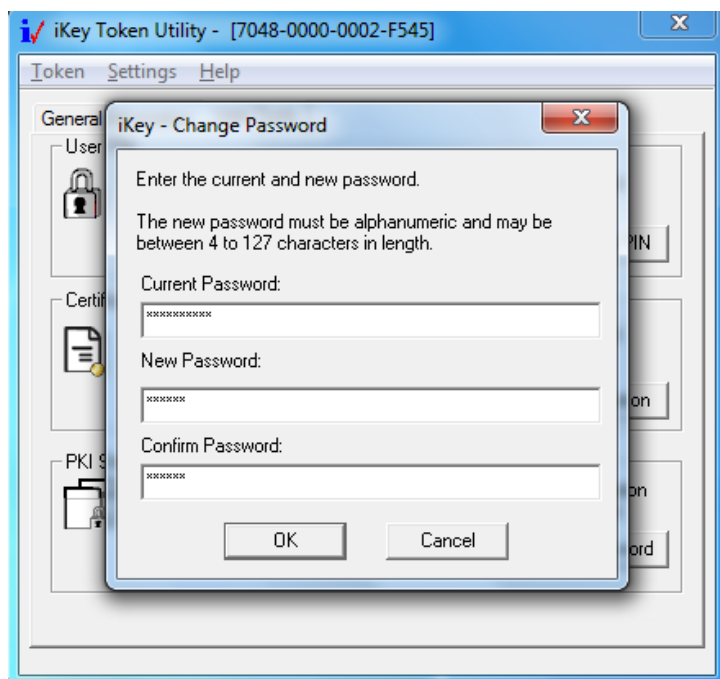


Рис. 10

Важно!

Для того чтобы Ваш пароль был безопасным:

- пароль не должен состоять из одних цифр;
- пароль не должен быть слишком коротким и состоять из символов, находящихся на одной линии на клавиатуре;
- пароль должен содержать в себе как заглавные, так и строчные буквы, цифры и знаки препинания;
- пароль не должен быть значимым словом (Ваше имя, дата рождения, номер машины или телефона и т.д.), которое можно легко подобрать или угадать.

Важно!

Неправильно ввести пароль к ключу, который находится в Хранилище ключей E-TOKEN, можно не более 5 раз подряд. После этого ключ блокируется. Чтобы разблокировать ключ, вам необходимо обратиться к обслуживающему вас сотруднику банка.

Внесено:

И.о. начальника Службы внутреннего контроля и безопасности
Ким А.А.

Согласовано:

Начальник Операционного Департамента Валиев Т.З.

Начальник Департамента информационных технологий Каменский В.Н.

Начальник Юридической службы
Нурмурадова Э.С.

Юридическая экспертиза проведена.