Система «iBank 2»
Руководство по работе с USB-токенами «iBank 2 Key»
Руководство пользователя

Содержание

Предисловие 3
Общие сведения о USB-токенах «iBank 2 Key» 4
Установка драйвера для USB-токенов «iBank 2 Key» 5
Работа с USB-токеном «iBank 2 Key» 8
Использование USB-токена «iBank 2 Key» при регистрации и управлении ключами 8
Вход в систему 10
Эксплуатация и хранение USB-токенов «iBank 2 Key» 11

Предисловие

Настоящий документ является руководством по использованию USB-токенов «iBank2 Key» системы электронного банкинга «iBank 2».

В разделе Общие сведения о USB -токенах «iBank2 Key» рассмотрено назначение USB-токенов «iBank 2 Key» и представлена информация о платформах, поддерживающих USB-токены.

Информация об установке драйвера USB-токена «iBank2 Key» представлена в разделе Установка драйвера для USB –токенов «iBank2 Key».

Использование USB-токена «iBank2 Key» при работе с системой электронного банкинга «iBank2» подробно рассмотрено в разделах Использование USB -токена «iBank2 Key» при регистрации и управлении ключами и Вход в систему.

Правила хранения и эксплуатации USB-токена «iBank2 Key» подробно рассмотрены в разделе Эксплуатация и хранение USB -токенов «iBank2 Key» .

Общие сведения о USB-токенах «iBank 2 Key»

USB-токен «iBank 2 Key» — это аппаратное USB-устройство, состоящее из PC/SC-совместимого USB-картридера и SIM-карты, в которой реализованы все российские криптоалгоритмы и имеется защищенная область памяти, позволяющая хранить до 64-х секретных ключей ЭЦП.

Рис. 1. USB-токен «iBank 2 Key»

В USB-токене «iBank 2 Key» реализованы следующие криптографические функции:

- аппаратный криптографически стойкий генератор случайных чисел;
- генерация пары ключей ЭЦП;
- формирование и проверка ЭЦП по ГОСТ Р34.10-2001 (эллиптические кривые);
- генерация ключей шифрования;
- шифрование и расшифрование в соответствии с ГОСТ 28147-89;
- формирование и проверка имитовставки (последовательности данных фиксированной длины, получаемой по определенному правилу из открытых данных и секретного ключа и добавляемой к данным для обеспечения имитозащиты) в соответствии с ГОСТ 28147-89;
- вычисление хеш-функции в соответствии с ГОСТ Р34.11-94.

Формирование ЭЦП клиента в соответствии с ГОСТ Р34.10-2001 непосредственно внутри SIMкарты токена: на вход токен принимает электронный документ, на выходе выдает ЭЦП под данным документом. При этом время формирования токеном ЭЦП приблизительно равно 0,5 сек.

USB-токены «iBank 2 Key» корректно работают на следующих платформах:

- Для операционных систем Windows XP Professional / XP Home / 2000 Server / Server 2003 / 2000 Professional / Vista используется Java 6.
- Для операционных систем Mac OS X 10.4.8 или старше используется Java 5

Секретный ключ ЭЦП генерируется самим токеном, хранится в защищенной памяти токена и никогда, никем и ни при каких условиях не может быть считан из токена.

Для использования функций криптографической защиты в «iBank 2 Key» системы электронного банкинга «iBank 2» встроена поддержка криптобиблиотеки СКЗИ «Криптомодуль-С» компании «Терна СБ», сертифицированных ФСБ (сертификат соответствия рег. № СФ/1141009 от 14 мая 2007 года).

Установка драйвера для USB-токенов «iBank 2 Key»

Драйвер USB-токена необходим для работы с USB-токеном «iBank 2 Key» в системе электронного банкинга «iBank 2».

Внимание!

Драйверы USB-токена «iBank 2 Key» устанавливаются до подключения устройства. Во время установки драйверов все приложения должны быть закрыты во избежание ошибки разделения файлов. Для установки драйверов пользователю необходимы права администратора системы.

Для установки драйвера USB-токена «iBank 2 Key» с сайта банка http://www.nmbank.ru/ibank2/ibank2key-driver-x86-1.04.exe. На экране появится окно выбора языка установки (см. рис. 2).

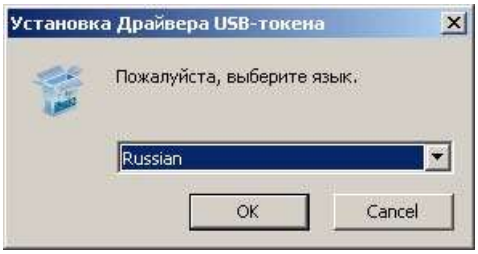

Рис. 2. Выбор языка установки

Выберите требуемый язык и нажмите кнопку **ОК** для перехода к стартовому окну мастера установки драйвера (см. рис. 3).

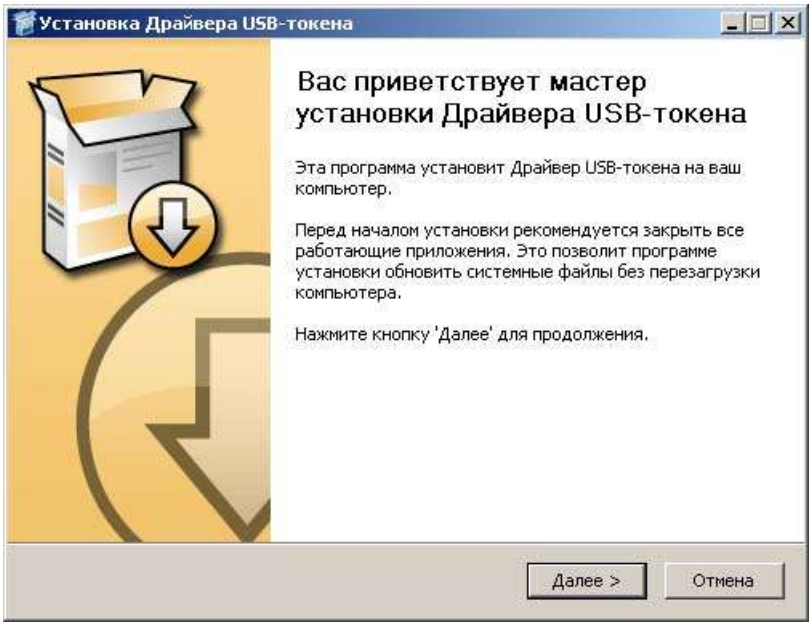

Рис. 3. Стартовое окно мастера установки Драйвера

В этом окне нажмите кнопку **Далее** для перехода к окну выбора каталога установки (см. рис. 4).

Введите адрес каталога, в который будет установлен Драйвер USB-токена «iBank 2 Key», в соответствующее поле или выберите его с помощью кнопки **Выбор** (адрес по умолчанию C:\Program Files\BIFIT\iBank 2 USB Token Driver). Нажмите кнопку **Установить**.

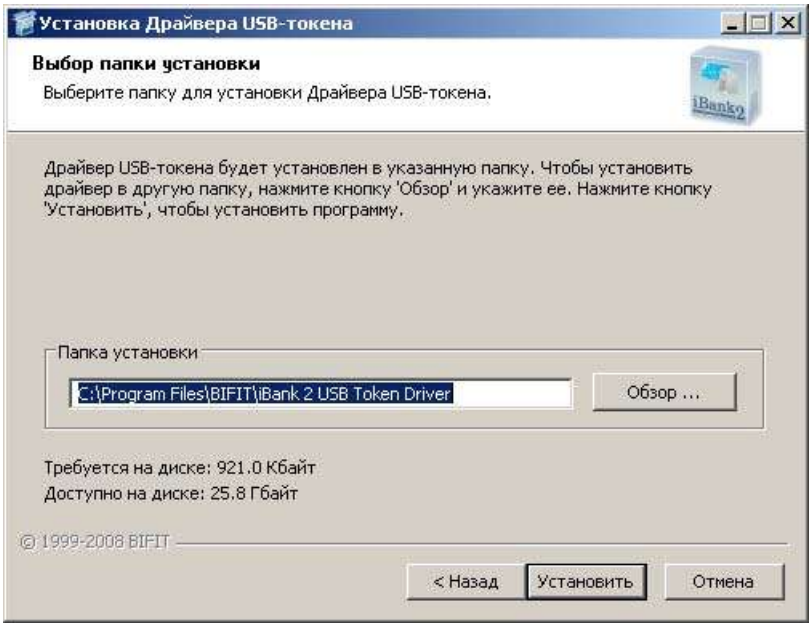

Рис. 4. Выбор каталога установки Драйвера

После завершения процесса установки в финальном окне диалога установки нажмите кнопку **Далее** (см. рис. 5).

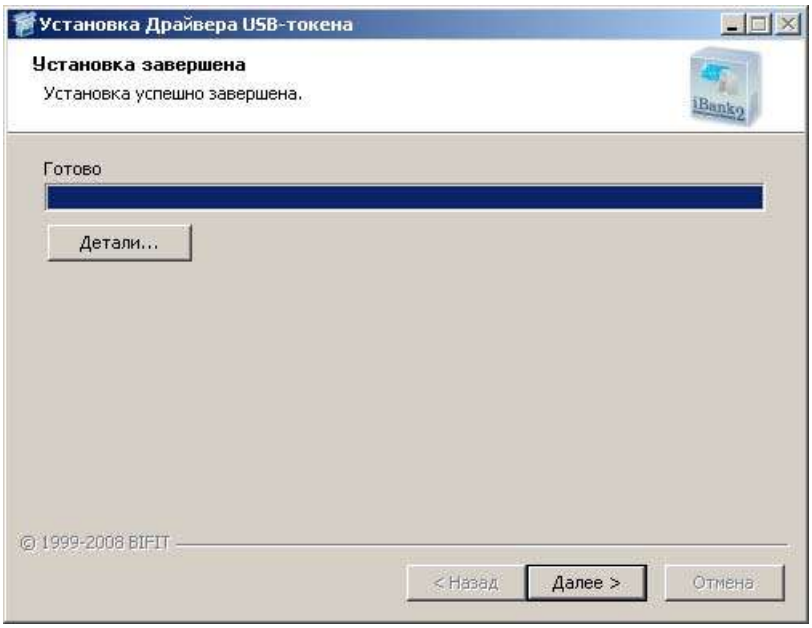

Рис. 5. Финальное окно диалога установки Драйвера

В окне **Завершение работы мастера установки Драйвера USB-токена** отметьте поле **Показать файл ReadMe** и нажмите кнопку **Готово** (см. рис. 6).

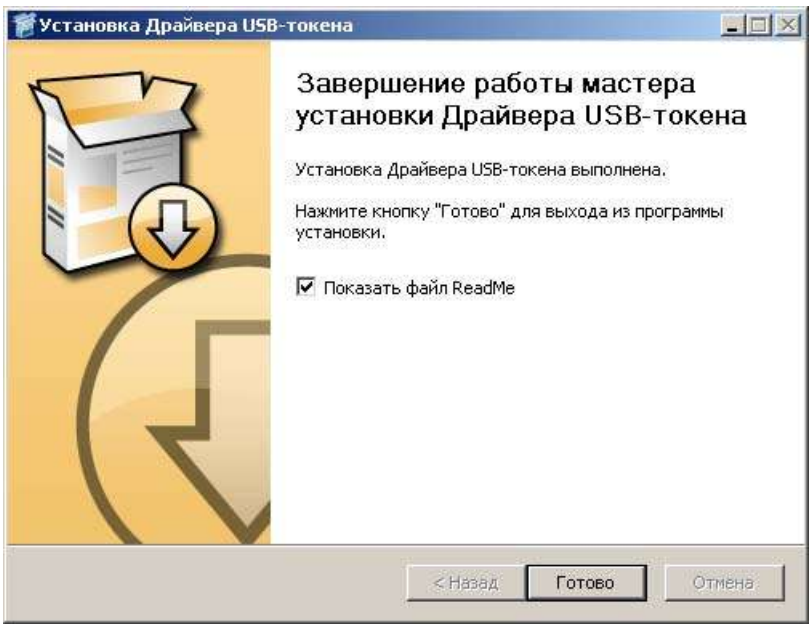

Рис. 6. Окно Завершение работы мастера установки USB-токена

Работа с USB-токеном «iBank 2 Key»

Использование USB-токена «iBank 2 Key» при регистрации и управлении ключами

Процесс предварительной регистрации осуществляется в АРМ «Регистратор», который представляет собой Java-апплет. Для загрузки Java-апплета «Регистратор» подключитесь к Интернет, запустите Web-браузер и перейдите на сайт банка на страницу «Клиент-Банк».

На странице «Интернет-Банк» выберите пункт **Предварительная регистрация**, в результате чего сначала загрузится html-страница, содержащая краткое описание процедуры регистрации нового клиента, а через 15 — 30 секунд (в зависимости от скорости доступа в Интернет) загрузится АРМ «Регистратор», оформленный в виде Мастера.

Подключите USB-токен «iBank 2 Key» к USB-порту компьютера. В системной области панели задач (system tray) появится сообщение, свидетельствующие об успешной установке «iBank 2 Key».

Пройдите все этапы регистрации. На шаге, требующем указать путь к файлу с Хранилищем ключей, в качестве Хранилища ключей выберите из списка USB-токен (пример для корпоративных клиентов приведен на рис.7).

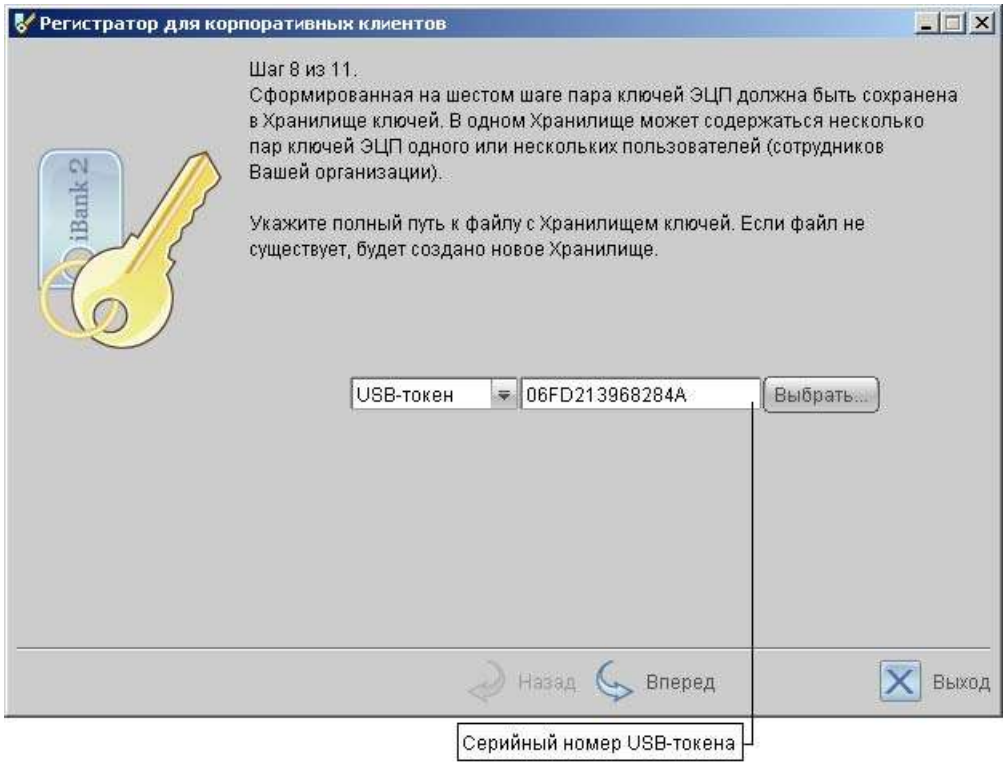

Рис. 7. Предварительная регистрация.

Примечания:
В одном Хранилище ключей USB-токена может содержаться несколько секретных ключей ЭЦП одного или нескольких клиентов.

Важно!

Для того чтобы Ваш пароль был безопасным:

- пароль не должен состоять из одних цифр (так его легче подсмотреть из-за спины);
- 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, девичья фамилия жены и т.д.), которое можно легко подобрать или угадать.

Важно!

Неправильно ввести пароль к ключу можно не более 15 раз подряд.

После этого ключ блокируется навсегда. Для дальнейшей работы потребуется генерация нового ключа на токен с последующей его регистрацией в Банке.

Администрирование USB-токенов клиента осуществляется в АРМ «Регистратор».

Загрузите Java-апплет «Регистратор», при этом в окне выбора варианта действия выберите поле **Администрирование ключей ЭЦП** и нажмите кнопку **Вперед** для перехода к основному окну, в котором возможно произвести следующие действия над USB-токенами:

- печать Сертификата открытого ключа ЭЦП клиента;
- смена пароля для доступа к секретному ключу ЭЦП в Хранилище ключей;
- смена наименования секретного ключа ЭЦП в Хранилище ключей;
- копирование секретного ключа ЭЦП в другое Хранилище ключей;
- удаление секретного ключа ЭЦП из Хранилища ключей.

Вход в систему

Для загрузки Java-апплета «Internet-Банкинг» подключитесь к Интернет, запустите Web-браузер и перейдите на сайт банка на страницу «Интернет-Банк».

Подключите USB-токен «iBank 2 Key» к USB-порту компьютера. В системной области панели задач (system tray) появится сообщение, свидетельствующие об успешной установке «iBank 2 Key».

На странице «Интернет-Банк» выберите пункт **Обслуживание**, в результате чего сначала загрузится стартовая html-страница, а через 15 – 30 секунд (в зависимости от скорости доступа в Интернет) загрузится АРМ «Internet-Банкинг», первое окно которого, Вход в систему, предназначенное для аутентификации клиента, на примере корпоративных клиентов представлено на рис. 8. В этом окне необходимо выполнить следующие действия:

Рис. 8. Окно Вход в систему. Аутентификация клиента

- В поле **Тип хранилища**: выберите **USB-токен**. В поле **Путь**: отобразится серийный номер USB-токена. Для выбора другого USB-токена воспользуйтесь кнопкой **Обзор**.

- Из списка поля **Ключ**: выберите наименование секретного ключа ЭЦП. Укажите пароль для доступа к выбранному ключу. При вводе пароля учитываются язык (русский/латиница) и регистр (заглавные/прописные буквы).

- Из списка поля **Профиль** выберите необходимый профиль работы. При выборе профиля **Текущий** загружаются настройки пользователя, сделанные в предыдущем сеансе работы. При выборе профиля **По умолчанию** загружаются настройки апплета, принятые системой по умолчанию.

- Если для подключения к Интернет используется Proxy-сервер введите в поля **адрес** и **порт**, соответственно, адрес и порт Proxy-сервера. Если для подключения Proxy-сервер не используется, снимите метку в поле **Использовать прокси**.

- Для входа в АРМ «Internet-Банкинг» нажмите кнопку **Вход**.

Эксплуатация и хранение USB-токенов «iBank 2 Key»

USB-токены «iBank 2 Key» являются чувствительным электронным прибором. При хранении и эксплуатации пользователю необходимо соблюдать ряд правил и требований, при нарушении которых USB-токен легко может выйти из строя. Следующие правила эксплуатации и хранения обеспечат длительный срок службы USB-токенов «iBank 2 Key» и сохранность конфиденциальной информации пользователя.

- Необходимо оберегать USB-токен от сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т. п.).

- USB-токен необходимо оберегать от воздействия высоких и низких температур. При резкой смене температур (вносе охлажденного USB-токен с мороза в теплое помещение) не рекомендуется использовать USB-токен в течение 3 часов во избежание повреждения USB-токена из-за сконденсированной на его электронной схеме влаги. Необходимо оберегать USB-токен от попадания на него прямых солнечных лучей.

- Необходимо оберегать USB-токен от воздействия влаги и агрессивных сред.

- Недопустимо воздействие на USB-токен сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества.

- При подключении USB-токена к компьютеру не прилагайте излишних усилий.

- USB-токен в нерабочее время необходимо всегда держать закрытым во избежание попадания на разъем USB-токена пыли, грязи, влаги и т. п. При засорении разъема токена нужно принять меры для его очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо.

- Не разбирайте USB-токен, это ведет к потере гарантии!

- Необходимо избегать скачков напряжения питания компьютера и USB-шины при подключенном USB-порте, а также не извлекать токен из USB-порта во время записи и считывания.

- В случае неисправности или неправильного функционирования USB-токена обращайтесь в Банк.

Важно!

Не передавайте USB-токен третьим лицам! Не сообщайте третьим лицам пароль от ключей ЭЦП! В случае утери (хищения) или повреждения USB-токена немедленно свяжитесь с банком.