

**Средство криптографической
защиты информации «MS_KEY K» –
«АНГАРА» (вариант исполнения 8.1.1)**

Руководство пользователя

Версия 1.2

Содержание

| | |
|---|----|
| Предисловие | 3 |
| Общие сведения | 4 |
| Подготовка «MS_KEY К» – «АНГАРА» Исп 8.1.1 к работе | 6 |
| Работа с «MS_KEY К» – «АНГАРА» Исп 8.1.1 | 7 |
| Эксплуатация и хранение | 7 |
| Использование USB-токенов при регистрации в системе «iBank» | 7 |
| Использование USB-токенов при входе в систему | 10 |
| Администрирование USB-токенов | 12 |
| Устранение неисправностей | 15 |
| USB-токен недоступен | 15 |
| Плагин BIFIT Signer не обнаруживает USB-токен | 16 |
| Нестабильная работа USB-токена | 19 |

Предисловие

Настоящий документ является руководством по использованию средства криптографической защиты информации «MS_KEY К» – «АНГАРА» (вариант исполнения 8.1.1) (далее «MS_KEY К» – «АНГАРА» Исп 8.1.1, USB-токен «MS_KEY К» – «АНГАРА» Исп.8.1.1) в системе «iBank».

В разделе [Общие сведения](#) подробно рассмотрено назначение USB-токенов «MS_KEY К» – «АНГАРА» Исп 8.1.1.

В разделе [Подготовка «MS_KEY К» – «АНГАРА» Исп 8.1.1 к работе](#) представлена информация о совместимости изделия с различными операционными системами и действиях, необходимых для обеспечения корректной работы устройства.

В разделе [Эксплуатация и хранение](#) описаны меры по обеспечению сохранности и надежности «MS_KEY К» – «АНГАРА» Исп 8.1.1.

Применение изделия при работе с системой «iBank» подробно рассмотрено в разделах:

- [Использование USB-токенов при регистрации в системе «iBank»](#)
- [Использование USB-токенов при входе в систему корпоративных клиентов](#)
- [Администрирование USB-токенов](#)

В разделе [Устранение неисправностей](#) описаны типовые неисправности и способы их устранения, которые могут возникнуть при эксплуатации «MS_KEY К» – «АНГАРА» Исп 8.1.1.

Общие сведения

USB-токен «MS_KEY К» – «АНГАРА» Исп.8.1.1 представляет собой компактное USB-устройство (см. [рис. 1](#)) с аппаратной реализацией российского стандарта электронной подписи (ЭП), шифрования и хеширования. Разработчиком устройства является компания ООО «НТЦ Альфа-Проект».



Рис. 1. USB-токен «MS_KEY К» – «АНГАРА» Исп.8.1.1

USB-токены «MS_KEY К» – «АНГАРА» Исп.8.1.1 генерируют ключи ЭП внутри себя, обеспечивают их защищенное неизвлекаемое хранение и формируют ЭП под электронными документами внутри устройства.

Аппаратная реализация стандарта ЭП, шифрования и хеширования внутри устройства обеспечивает:

- конфиденциальность обрабатываемой информации при передаче и хранении;
- целостность обрабатываемой информации;
- подтверждение авторства посредством электронной подписи.

Формирование ЭП в соответствии с ГОСТ Р34.10-2012 происходит непосредственно внутри устройства: на вход «MS_KEY К» – «АНГАРА» Исп.8.1.1 принимает электронный документ, на выходе выдает ЭП под данным документом.

В «MS_KEY К» – «АНГАРА» Исп.8.1.1 имеется защищенная область памяти, позволяющая хранить до 75 ключей ЭП ответственных сотрудников одного или нескольких клиентов.

Поддержка «MS_KEY К» – «АНГАРА» Исп.8.1.1 обеспечена в системе «iBank», начиная с версии 2.0.24.492

Использование «MS_KEY К» – «АНГАРА» Исп.8.1.1 возможно в следующих АРМ:

- Интернет-Банк для корпоративных клиентов (Web);
- ЦФК (Web);
- Офлайн-Банк;
- Корпоративный автоклиент;
- Автоклиент;
- Интернет-Банк для частных клиентов;
- Администратор банка/филиала;
- Операционист корпоративных клиентов;
- Операционист частных клиентов;
- Система управления контентом (CMS);
- Оператор сервиса «Чат».

Возможна одновременная работа сразу с несколькими подключенными к компьютеру устройствами (актуально при работе с ЦФК).

Примечание:

Иллюстрации в документе приведены для стандартных версий Web-АРМов системы «iBank».

В «MS_KEY К» – «АНГАРА» Исп 8.1.1 реализованы следующие криптографические функции:

- ГОСТ Р 34.10-2012 (генерация ключевых пар, формирование и проверка ЭП);
- ГОСТ Р 34.11-2012 (функция хеширования);
- ГОСТ 28147-89 (симметричное шифрование);
- ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 (блочные шифры и режимы работы блочных шифров);
- аппаратный криптографически стойкий генератор случайных чисел.

Средство криптографической защиты информации (СКЗИ) «MS_KEY К» – «АНГАРА» (вариант исполнения 8.1.1) имеет сертификат ФСБ РФ № СФ/124-3806 от 05.02.2020 – действителен до 15.02.2022.

Примечание:

В системе «iBank» поддерживается работа USB-токенов «MS_KEY К» – «АНГАРА» Исп 8.1.1 в специальной конфигурации, предназначенной для использования исключительно в системе «iBank».

Компания «БИФИТ» согласовала данную конфигурацию с производителем USB-токенов ООО «НТЦ Альфа-Проект», встроила поддержку конфигурации в систему «iBank», протестировала систему «iBank» на предмет совместимости с USB-токенами «MS_KEY К» – «АНГАРА» Исп 8.1.1 в данной конфигурации и осуществляет их поддержку в системе «iBank» только в специальной конфигурации.

В настоящее время в системе «iBank» реализована поддержка USB-токенов «MS_KEY К» – «АНГАРА» Исп 8.1.1 со специальной конфигурацией, приобретенных через авторизованных поставщиков ООО «БИФИТ Дата Секьюрити» и/или ООО «БИФИТ ЭДО» с ограничением области применения данных USB-токенов только в составе системы «iBank».

Использование USB-токенов «MS_KEY К» – «АНГАРА» Исп 8.1.1 с иными конфигурациями и/или приобретенных через не авторизованных поставщиков невозможно ввиду отсутствия поддержки работы таких устройств в системе «iBank».

Подготовка «MS_KEY К» – «АНГАРА» Исп 8.1.1 к работе

Работа с «MS_KEY К» – «АНГАРА» Исп 8.1.1 возможна на следующих платформах:

- Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;
- Apple Mac OS X: 10.10 (Yosemite) и выше;
- Linux: AltLinux 7 (x86/x64), Debian 7 (x86/x64), Mint 13 (x86/x64), SUSE Linux Enterprise Desktop 12 (x64), openSUSE 13 (x86/x64), Ubuntu 12.04 (x86/x64) и более современные версии указанных дистрибутивов.

«MS_KEY К» – «АНГАРА» Исп 8.1.1 поддерживает CCID-драйвер, который входит в состав современных ОС Microsoft Windows, Linux, Mac OS X, и не требует установки дополнительного программного обеспечения.

Для работы «MS_KEY К» – «АНГАРА» Исп 8.1.1 в WEB-версиях АРМ системы «iBank» необходим плагин **BIFIT Signer** версии 5.0 и выше.

Для работы «MS_KEY К» – «АНГАРА» Исп 8.1.1 в java-апплетах системы «iBank» необходимо дополнительно установить библиотеку **pkcs11-angara**.

Для получения библиотеки для используемой ОС обратитесь в ваш банк.

Разрядность используемой Java и библиотеки **pkcs11-angara** должны совпадать.

Разместите файл библиотеки в среде пользовательской ОС:

Для ОС Windows:

Файл библиотеки соответствующей разрядности (**pkcs11-angara.dll**) необходимо поместить в каталог, по которому java-апплет осуществляет поиск библиотек для подключенного устройства, например: **C:\Windows\System32**.

Для ос Linux:

Файл библиотеки соответствующей разрядности (**libpkcs11-angara.so**) необходимо поместить в каталог, по которому java-апплет осуществляет поиск библиотек для подключенного устройства, например: **/usr/lib**.

Для MAC OS X:

Файл библиотеки соответствующей разрядности (**libpkcs11-angara.dylib**) необходимо поместить в каталог, по которому java-апплет осуществляет поиск библиотек подключенного устройства, например: **/Users/имя_пользователя/Library/Java/Extensions/** (если его нет, необходимо создать каталог **/Java/Extensions/**).

Работа с «MS_KEY К» – «АНГАРА» Исп 8.1.1

Эксплуатация и хранение

USB-токены являются чувствительными электронными устройствами. При их хранении и эксплуатации пользователю необходимо соблюдать ряд правил и требований.

Следующие правила эксплуатации и хранения обеспечат длительный срок службы USB-токенов, а также сохранность конфиденциальной информации пользователя.

- Необходимо оберегать USB-токены от сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т.п.).
- USB-токены необходимо оберегать от воздействия высоких и низких температур. При резкой смене температур не рекомендуется использовать USB-токен в течение 3 часов во избежание повреждений из-за сконденсированной на электронной схеме влаги. Необходимо оберегать устройства от попадания на них прямых солнечных лучей.
- Необходимо оберегать USB-токены от воздействия влаги и агрессивных сред.
- Недопустимо воздействие на USB-токены сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества.
- При подключении USB-токена 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 допускается непрерывное функционирование USB-токена более суток (24 часов).
- Не разбирайте USB-токены, так как это ведет к потере гарантии!
- Необходимо избегать скачков напряжения питания компьютера и USB-шины при подключенном USB-порте, а также не извлекать USB-токен из USB-порта во время записи и считывания.
- В случае неисправности или неправильного функционирования USB-токенов обращайтесь в ваш банк.

Внимание!

1. Не передавайте USB-токены третьим лицам! Не сообщайте третьим лицам пароли от ключей ЭП!
2. Подключайте USB-токен к компьютеру только на время работы с системой «iBank».
3. В случае утери (хищения) или повреждения USB-токена немедленно свяжитесь с вашим банком.

Использование USB-токенов при регистрации в системе «iBank»

Процесс предварительной регистрации корпоративных клиентов осуществляется в АРМ «**Регистратор для корпоративных клиентов**», банковских сотрудников — в АРМ «**Регистратор для банковских сотрудников**»:

1. Подключите USB-токен «MS_KEY К» – «АНГАРА» Исп 8.1.1 к USB-порту компьютера.
2. Подключитесь к Интернету, запустите Web-браузер и перейдите на страницу входа для клиентов или для сотрудников банка системы «iBank» вашего банка.
3. На странице входа клиентов выберите пункт: **Регистрация** → **Подключение к системе**, на странице входа сотрудников банка — **Регистрация** или **Операционист** → **Новый сотрудник**.

В результате загрузится соответствующий АРМ.

4. Пройдите все этапы регистрации. На восьмом шаге (корпоративный клиент) или на третьем шаге (банковский сотрудник) в качестве хранилища ключей выберите из списка пункт **Аппаратное устройство** (см. [рис. 2](#), [рис. 3](#)).

iBank для Бизнеса

Подключение к системе

Шаг 8 из 12.

Новый ключ ЭП должен быть добавлен в хранилище ключей.
В одном хранилище может содержаться несколько ключей ЭП.

Укажите полный путь к файлу или серийный номер аппаратного устройства, которое будет использоваться для генерации ключей ЭП.

Если хранилище не существует, будет создано новое.

Аппаратное устройство

"MS_Key К" - "АНГАРА" Исп.8.1.1 (001524) **Выбрать...**

Назад **Вперед**

Рис. 2. АРМ «Регистратор для корпоративных клиентов (Web)». Предварительная регистрация. Шаг 8 из 12

iBank для Бизнеса

Регистрация нового сотрудника

Шаг 3 из 7.

Новый ключ ЭП должен быть добавлен в хранилище ключей.
В одном хранилище может содержаться несколько ключей ЭП.

Укажите полный путь к файлу или серийный номер аппаратного устройства, которое будет использоваться для генерации ключей ЭП.

Если хранилище не существует, будет создано новое.

Аппаратное устройство

"MS_Key К" - "АНГАРА" Исп.8.1.1 (001524) **Выбрать...**

Назад **Вперед**

Рис. 3. АРМ «Регистратор для банковских сотрудников (Web)». Предварительная регистрация. Шаг 3 из 7

5. Если к «MS_KEY К» – «АНГАРА» Исп 8.1.1 задан PIN-код, то появится окно для ввода PIN-кода (см. [рис. 4](#)). Укажите значение PIN-кода пользователя.

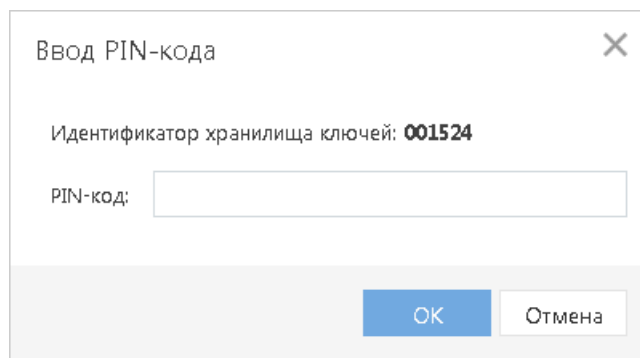


Рис. 4. Ввод PIN-кода пользователя

Внимание!

После 10 последовательных попыток ввода неверного PIN-кода пользователя устройство блокируется.

На следующих шагах регистрации вам необходимо ввести наименование и пароль к создаваемому ключу ЭП. Для повышения уровня безопасности пароля воспользуйтесь следующими рекомендациями:

- 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, девичья фамилия жены и т.д.), которое можно легко подобрать или угадать.

Если при вводе наименования ключа в хранилище ключей уже существует ключ с таким наименованием, то в этом случае перезаписи ключа не произойдет, о чем будет выдано соответствующее предупреждение (см. [рис. 5](#)). В этом случае необходимо либо присвоить другое наименование ключу, либо предварительно удалить ненужный ключ из хранилища (см. раздел [Администрирование USB-токенов](#)).

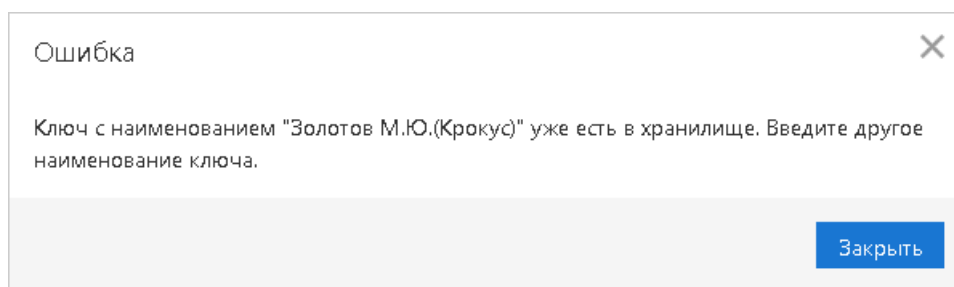


Рис. 5. Сообщение об ошибке

Примечание:

В памяти USB-токена «MS_KEY К» – «АНГАРА» Исп 8.1.1 может храниться не более 75 ключей ЭП, включая удаленные. Предупреждение о переполнении памяти токена выдается при создании последнего возможного ключа. При исчерпании памяти токена необходимо обратиться в банк для повторной инициализации токена. При этом все существующие на токене ключи ЭП будут удалены.

Внимание!

Неправильно ввести пароль к ключу ЭП, который находится на USB-токене «MS_KEY К» – «АНГАРА» Исп 8.1.1, можно не более 15 раз подряд. После этого ключ ЭП блокируется навсегда.

Использование USB-токенов при входе в систему

Для загрузки поддерживаемых АРМ (список поддерживаемых АРМ см. в разделе [Общие сведения](#)) подключитесь к Интернету, запустите Web-браузер и перейдите на страницу для клиентов или для сотрудников банка системы «iBank» вашего банка.

Подключите USB-токен «MS_KEY К» – «АНГАРА» Исп 8.1.1 к USB-порту компьютера.

На странице входа корпоративных клиентов банка выберите необходимый пункт:

- Вход в Интернет-Банк → Выбрать электронную подпись;
- Вход в Центр Финансового Контроля;
- Запустите приложение Офлайн-Банк и выполните синхронизацию.

Или на странице входа банковских сотрудников выберите необходимый пункт:

- Операционист;
- Администратор;
- Система управления контентом.

Для входа в АРМ «Оператор» сервиса «Чат» перейдите на страницу входа в сервис.

Список ключей ЭП корпоративного клиента представлен на [рис. 6](#).

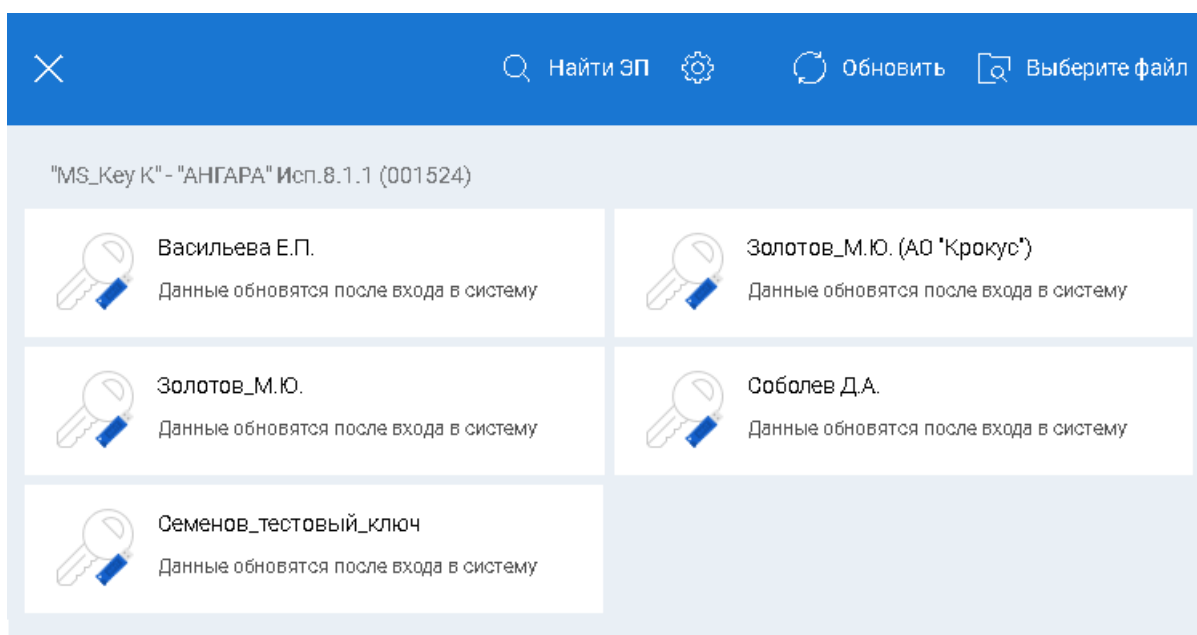



Рис. 6. Список ключей ЭП

Выберите необходимый ключ ЭП, укажите пароль к нему и нажмите кнопку 

При использовании аппаратного устройства, к которому задан PIN-код, появляется поле для его ввода (см. [рис. 7](#)).

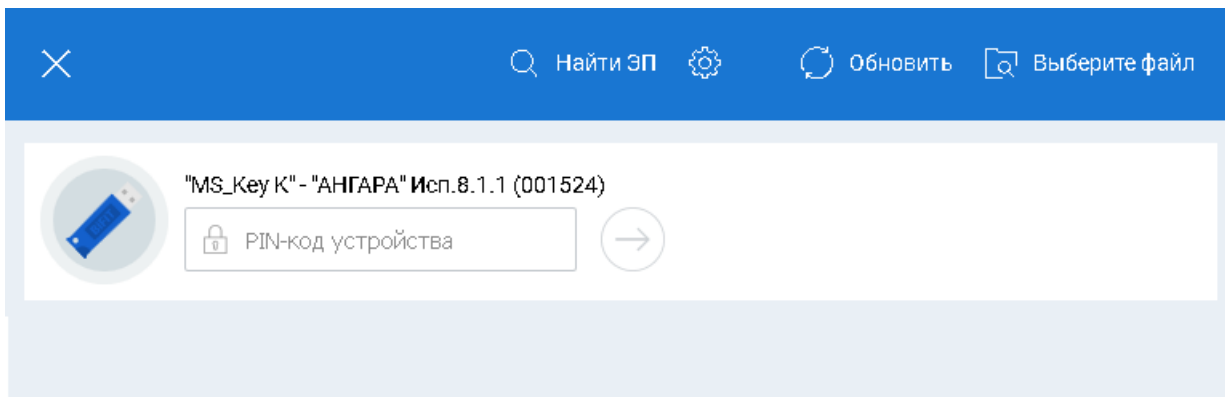


Рис. 7. Список ключей ЭП. Ввод PIN-кода

Окно **Вход в систему** для ЦФК, сотрудников банка и оператора сервиса «Чат» представлено на рис. 8.

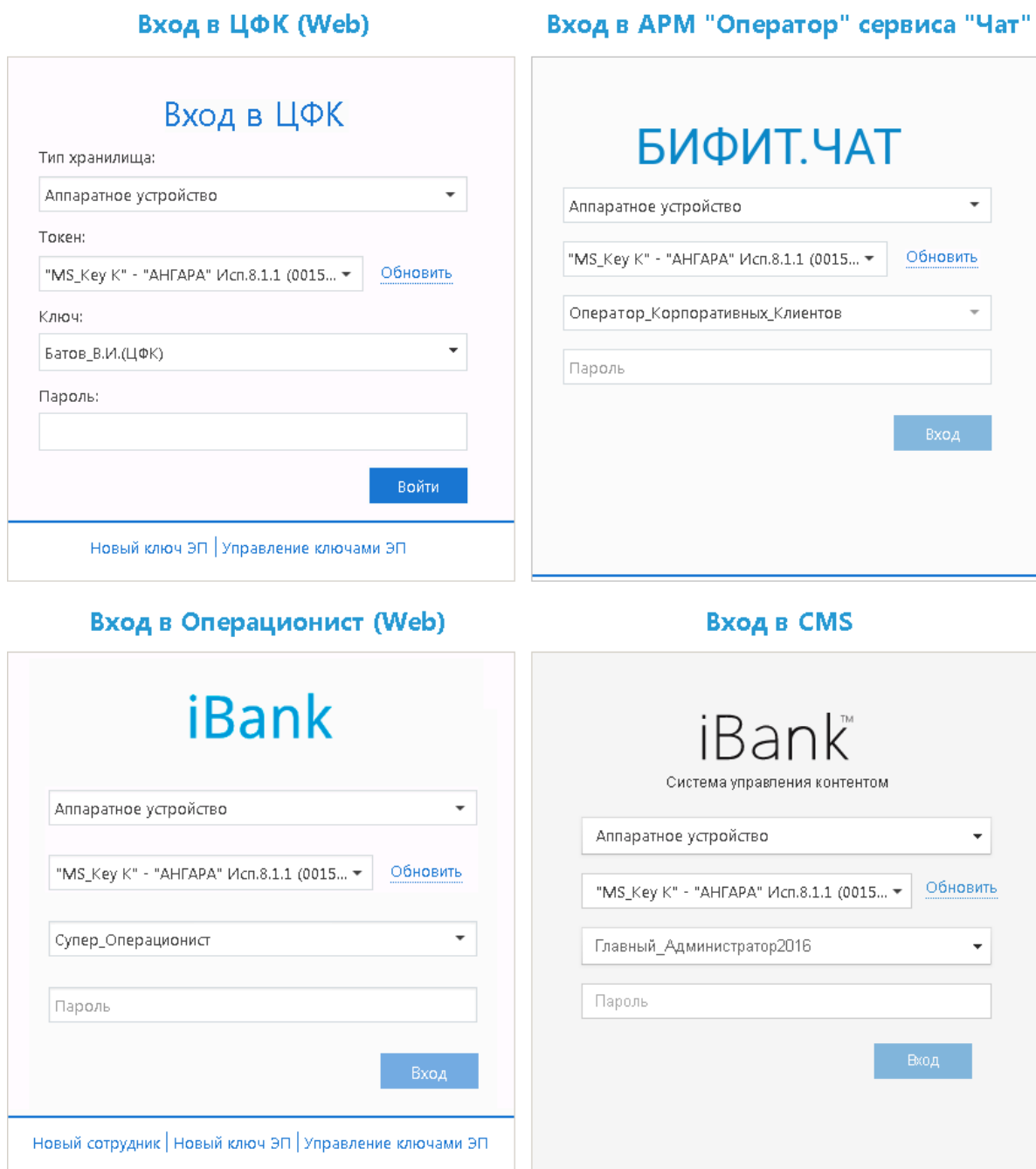


Рис. 8. Окно «Вход в систему. Аутентификация в iBank»

В этом окне необходимо выполнить следующие действия:

- В поле **Тип хранилища** выберите **Аппаратное устройство**. В поле **Идентификатор** отобразится серийный номер выбранного USB-токена.
- При использовании USB-токена, к которому задан PIN-код, после выбора устройства на предыдущем шаге появляется окно для ввода PIN-кода (см. [рис. 9](#)).

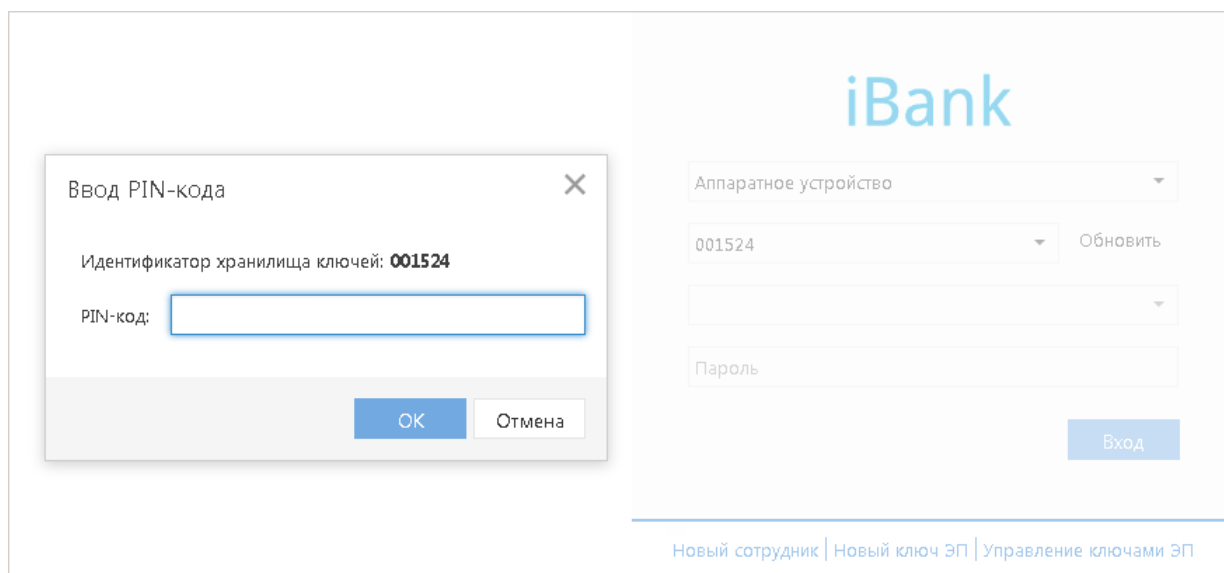


Рис. 9. Окно «Вход в систему. Ввод PIN-кода»

- Из списка поля **Ключ** выберите наименование ключа ЭП. Укажите **Пароль** для доступа к выбранному ключу. При вводе пароля учитываются язык (русский/английский) и регистр (заглавные/прописные буквы).
- Для входа в систему нажмите кнопку **Вход**.

Администрирование USB-токенов

Возможны следующие действия с «MS_KEY К» – «АНГАРА» Исп 8.1.1 и ключами ЭП:

1. [Задание PIN-кода доступа](#)
2. [Печать сертификата ключа проверки ЭП](#)
3. [Смена пароля для доступа к ключу ЭП](#)
4. [Смена наименования ключа ЭП](#)
5. [Удаление ключа ЭП](#)

Администрирование ключей ЭП, хранящихся в памяти «MS_KEY К» – «АНГАРА» Исп 8.1.1, осуществляется:

- корпоративными клиентами и сотрудниками центра финансового контроля в АРМ «**Регистратор для корпоративных клиентов (Web)**». Для перехода в АРМ выполните:
 - Интернет-Банк — на странице входа клиентов банка перейдите **Регистрация** → **Администрирование ключей ЭП**;
 - Офлайн-Банк — перейдите в раздел **Ключи ЭП** → **Администрирование ключей ЭП**;
 - ЦФК — на странице входа клиентов банка перейдите **Вход в Центр Финансового Контроля** → **Управление ключами ЭП**.

- сотрудниками банка в АРМ «**Регистратор для банковских сотрудников (Web)**». Для перехода в АРМ на странице входа сотрудников банка перейдите **Операционист** → **Управление ключами ЭП**.

Выполните следующие действия:

1. Запустите соответствующий АРМ.
2. Укажите тип хранилища ключей ЭП — **Аппаратное устройство**.
3. В поле ниже отобразится серийный номер подключенного к компьютеру устройства. При необходимости вы можете выбрать другое подключенное устройство, нажав кнопку **Выбрать**. Под серийным номером отобразится список ключей ЭП (см. [рис. 10](#)).

iBank для Бизнеса

Администрирование ключей ЭП

Укажите тип хранилища ключей ЭП

Ключ на диске

Аппаратное устройство

"MS_Key К" - "АНГАРА" Исп.8.1.1 (001524) Выбрать

| Наименование ключа |
|-----------------------------------|
| Васильева Е.П. |
| Золотов_М.Ю. (АО "Крокус") |
| Золотов_М.Ю. |
| Соболев Д.А. |
| Васильева Е.П. (Крокус) |

Количество ключей на аппаратном устройстве: 5

Сменить PIN Печать Сменить пароль Переименовать Удалить

Рис. 10. Администрирование ключей ЭП

4. Выберите ключ ЭП и для выполнения необходимого действия нажмите соответствующую кнопку.

Задание PIN-кода доступа

Примечание:

Задание и смена PIN-кода доступа осуществляется только в WEB-АРМах системы «iBank».

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся в памяти «MS_KEY К» – «АНГАРА» Исп 8.1.1, реализована возможность задавать PIN-код доступа к устройству.

При обращении к «MS_KEY К» – «АНГАРА» Исп 8.1.1 с заданным PIN-кодом отсутствует возможность получения списка ключей устройства и каких-либо действий с ними, до момента ввода корректного PIN-кода.

PIN-код к «MS_KEY К» – «АНГАРА» Исп 8.1.1, если он установлен, запрашивается у пользователя при выполнении следующих действий:

- аутентификация в клиентском АРМ;
- обращение к «MS_KEY К» – «АНГАРА» Исп 8.1.1 в случае его отключения и последующего подключения;
- обращение к «MS_KEY К» – «АНГАРА» Исп 8.1.1 в ходе администрирования ключей ЭП;
- подпись документов и синхронизация данных с банком во время работы в Офлайн-Банке.

Для назначения PIN-кода нажмите кнопку **Сменить PIN**, дважды введите новое значение PIN-кода и нажмите кнопку **Принять**.

Назначенный PIN-код к «MS_KEY К» – «АНГАРА» Исп 8.1.1 удалить нельзя, его можно лишь сменить.

Внимание!

После 10 последовательных попыток ввода неверного PIN-кода устройство блокируется.

Печать сертификата ключа проверки ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Печать**. Укажите пароль для доступа к ключу ЭП. Нажмите кнопку **Принять**.

Смена пароля для доступа к ключу ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Сменить пароль**. Укажите текущий пароль ключа ЭП и дважды — новый пароль. Нажмите кнопку **Принять**. Новый пароль к ключу ЭП будет установлен.

Смена наименования ключа ЭП

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Переименовать**. Укажите пароль для доступа к ключу ЭП и новое наименование ключа ЭП в хранилище ключей. Нажмите кнопку **Принять**. Новое наименование ключа ЭП в хранилище будет установлено.

Удаление ключа ЭП

Внимание!

Если ключ ЭП удалить из хранилища ключей, восстановить его будет невозможно. Поэтому удалять можно ключи, которые в дальнейшем не будут использоваться при работе с системой (ключи с истекшим сроком действия, скомпрометированные ключи и т.д.).

Выберите в списке требуемый ключ ЭП и нажмите кнопку **Удалить**. Укажите пароль для доступа к ключу ЭП. После нажатия кнопки **Принять** ключ будет безвозвратно удален из хранилища ключей.

Устранение неисправностей

Наиболее часто встречающиеся неисправности:

- USB-токен недоступен для выбора
- Плагин BIFIT Signer не обнаруживает USB-токен
- Нестабильная работа USB-токена

USB-токен недоступен

Неисправность проявляется в недоступности USB-токен для выбора в WEB-АРМах системы «iBank».

Причиной неисправности может быть установленное в современных версиях ОС семейства Windows ограничение на общее количество устройств чтения смарт-карт в Диспетчере устройств — **не более 10 устройств**.

При превышении установленного ограничения некоторые токены или смарт-карты могут быть недоступны для использования.

Решение неисправности заключается в сокращении до допустимого количества подключенных считывателей в **Диспетчере устройств**.

Для устранения неисправности выполните действия:

1. Проверьте текущее количество устройств в системе: **Диспетчер устройств** → список **Устройства чтения смарт-карт** (см. [рис. 11](#)).

Устройства в данном разделе могут быть как реальными (смарт-карты и токены, подключенные в текущий момент к компьютеру), так и виртуальными (создаются при установке драйверов).

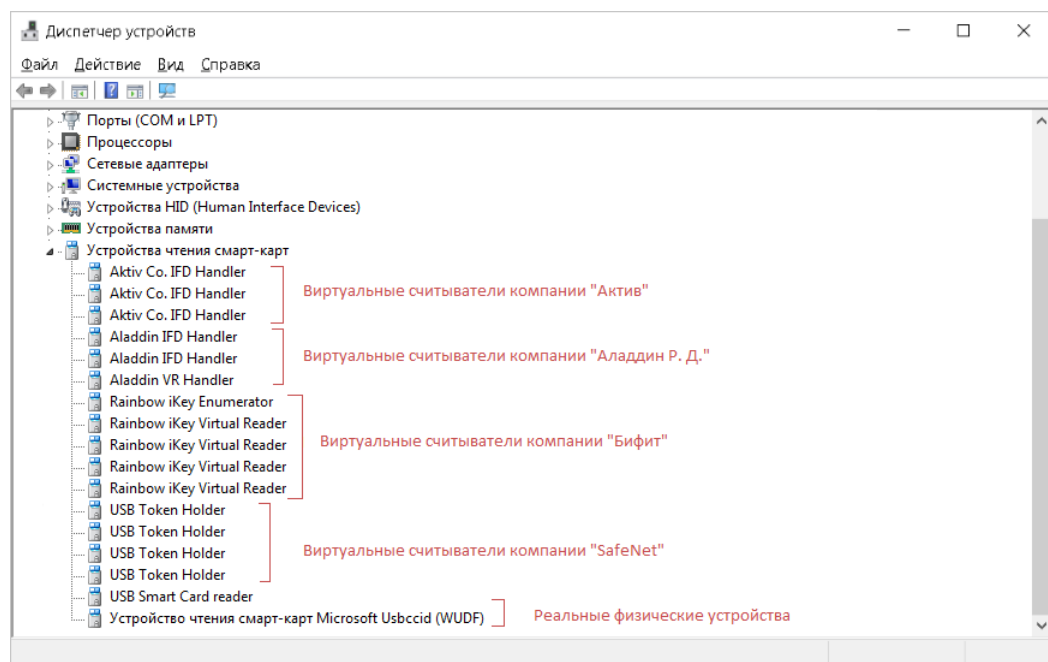


Рис. 11. Диспетчер устройств. Устройства чтения смарт-карт

2. Определите устройства по производителю и модели подключенных токенов и смарт-карт, которые можно удалить.
3. Удалите считыватели из списка **Устройства чтения смарт-карт**:
 - **Реальные считыватели** — отключите устройство от компьютера;
 - **Виртуальные считыватели** — используйте контекстное меню в **Диспетчере устройств** (см. [рис. 12](#)) или выполните деинсталляцию установленного для устройства ПО.

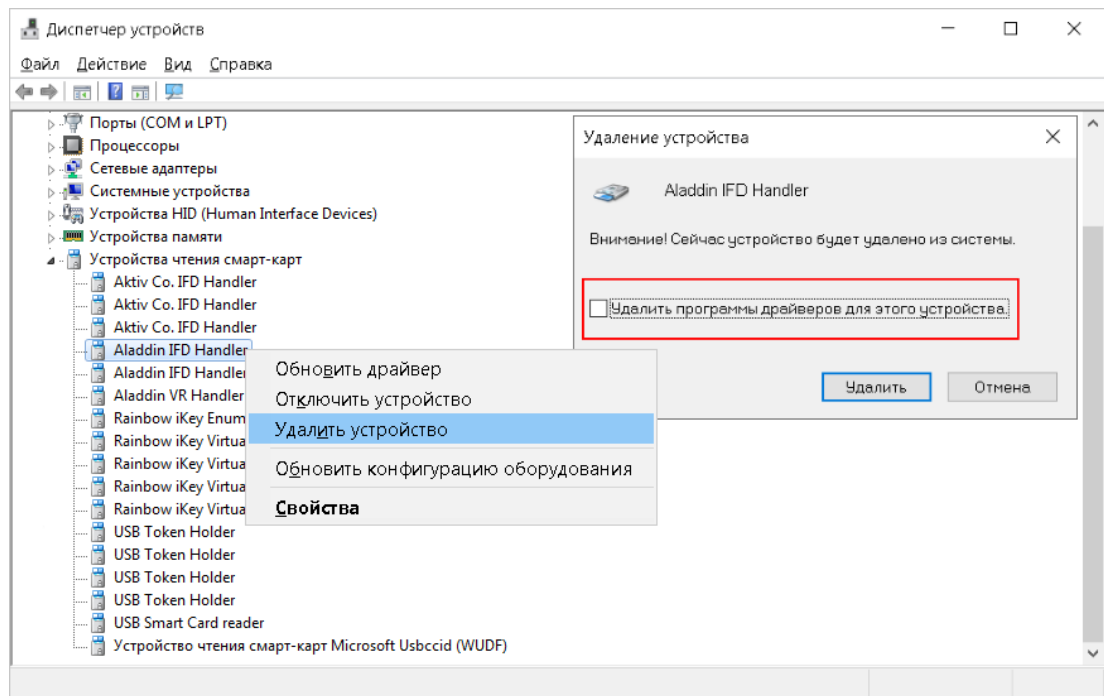


Рис. 12. Диспетчер Устройств. Удаление виртуального считывателя

Плагин BIFIT Signer не обнаруживает USB-токен

Решение неисправности приведено отдельно для каждой операционной системы:

- [ОС семейства Windows](#)
- [ОС семейства Linux](#)
- [ОС Apple OS X](#)

Неисправность может проявляться следующим образом:

- USB-токен не отображается:
 - при входе в систему в списке ключей ЭП;
 - при входе в систему для ЦФК, сотрудников банка и оператора сервиса «Чат»;
 - при администрировании ключей ЭП;
 - при выборе аппаратного устройства для генерации ключа ЭП;
 - в иных случаях.
- Отображается сообщение об ошибке – *Не установлены драйвера или не запущена служба 'Smart Card'*:
 - при входе в систему для ЦФК и сотрудников банка;
 - при выборе аппаратного устройства для генерации ключа ЭП;
 - при переходе в раздел **Электронные подписи** в Интернет-Банке для корпоративных клиентов;
 - при подписании документов в ЦФК;
 - в иных случаях.

Решение для операционных систем семейства Windows

USB-токен может отображаться в диспетчере устройств, но не определяться плагином BIFIT Signer.

Варианты устранения неисправности:

- Перезапустите службу **Смарт-карта**, например, указанным способом:
 1. Откройте окно настроек служб Windows: **Панель управления** → **Система и безопасность** → **Администрирование** → **Службы**
 2. Выберите пункт контекстного меню **Перезапустить** для службы **Смарт-карта** (см. [рис. 13](#)).

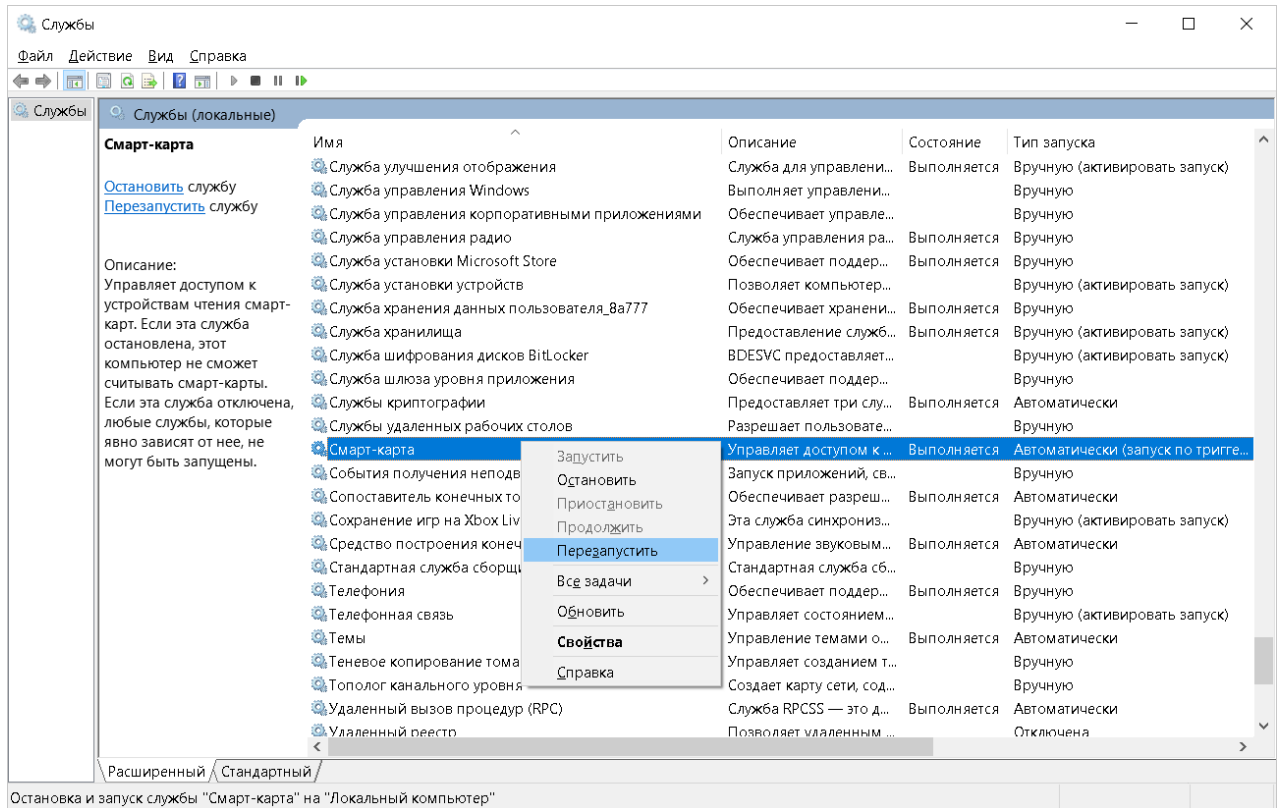


Рис. 13. Окно настроек служб Windows. Перезапуск службы Смарт-карта

- Проверьте, что установленное на компьютере антивирусное программное обеспечение не блокирует работу плагина BIFIT Signer. Отключите антивирусное ПО на время проверки и настройки плагина BIFIT Signer;
- Переустановите плагин BIFIT Signer, запустив инсталлятор от имени администратора.

Решение для операционных систем семейства Linux

Возможные причины неисправности и их решение:

- Не установлен драйвер iBank2Key
 - Скачайте и установите драйвер iBank2Key
- Отсутствуют позиционно-зависимые записи о USB-токене в конфигурационном файле Info.plist
 1. Проверьте наличие записей и при необходимости добавьте их в конфигурационный файл: `/usr/lib/pcsc/drivers/ifd-bundle/Contents/Info.plist`
 2. При отсутствии записей добавьте их в конец каждого массива:
 - в массив `ifdVendorID` добавить `<string>0x23a0</string>`
 - в массив `ifdProductID` добавить `<string>0x0008</string>`
 - в массив `ifdFriendlyName` добавить `<string>Angara</string>`

3. Проверьте работоспособность USB-токена:

— остановите сервис `pcscd`, если он запущен – `sudo killall pcscd`

— запустите сервис `pcscd` с ключами `adf` для получения расширенного отладочного лога – `sudo pcscd -adf`

Если в логе терминала есть упоминание нужного устройства, значит оно работает корректно (см. [рис. 14](#)).

```
00000045 hotplug_libudev.c:296: get_driver() Looking for a driver for VID: 0x0424, PID: 0x2514, path: /dev/bus/usb/003/002
00000048 hotplug_libudev.c:296: get_driver() Looking for a driver for VID: 0x23A0, PID: 0x0008, path: /dev/bus/usb/003/013
00000005 hotplug_libudev.c:435: HPAddDevice() Adding USB device: BIFIT ANGARA
00000022 readerfactory.c:1012: RFInitializeReader() Attempting startup of BIFIT ANGARA 00 00 using /usr/lib/pcsc/drivers/itd-bifit
00000094 readerfactory.c:897: RFBindFunctions() Loading IFD Handler 3.0
00000013 ifdhandler.c:1750: init_driver() Driver version: 1.4.4
00000005 ifdhandler.c:79: IFDHCCreateChannelByName() lun: 0, device: usb:23a0/0008:libudev:0:/dev/bus/usb/003/013
00000005 cccd_usb.c:180: OpenUSBBYName() Reader index: 0, Device: usb:23a0/0008:libudev:0:/dev/bus/usb/003/013
00000007 cccd_usb.c:212: OpenUSBBYName() interface number: 0
00001726 cccd_usb.c:303: OpenUSBBYName() Checking device: 3/13
00000004 cccd_usb.c:358: OpenUSBBYName() Trying to open USB bus/device: 3/13
00000034 cccd_usb.c:448: openUSBBYName() Using USB bus/device: 3/13
00000003 cccd_usb.c:932: ControlUSB() request: 0x03
00000084 cccd_usb.c:876: get_data_rates() IFD does not support GET_DATA_RATES request: -9
00055352 NotifySlotChange: 50 03
00000017 -> 000000 65 00 00 00 00 00 00 00 00 00
00000133 <- 000000 81 00 00 00 00 00 00 00 01 00 00
00000012 ifdhandler.c:401: IFDHGetCapabilities() tag: 0xFB3, usb:23a0/0008:libudev:0:/dev/bus/usb/003/013 (lun: 0)
00000004 readerfactory.c:355: RFAddReader() Using the reader polling thread
00000152 ifdhandler.c:401: IFDHGetCapabilities() tag: 0xFAE, usb:23a0/0008:libudev:0:/dev/bus/usb/003/013 (lun: 0)
00000008 ifdhandler.c:489: IFDHGetCapabilities() Reader supports 1 slot(s)
00000123 hotplug_libudev.c:296: get_driver() Looking for a driver for VID: 0x0424, PID: 0x2514, path: /dev/bus/usb/003/002
00000083 ifdhandler.c:1151: IFDHPowerICC() action: PowerUp, usb:23a0/0008:libudev:0:/dev/bus/usb/003/013 (lun: 0)
00000009 -> 000000 62 00 00 00 00 00 04 00 00 00
```

Рис. 14. Отладочный лог терминала

После выполнения всех действий, запустите фоновую службу `pcscd`. Если служба запускается корректно, перезагрузите компьютер.

Решение для операционной системы Apple OS X

Возможные причины неисправности и их решение:

- Не установлен драйвер `iBank2Key`
Скачайте и установите драйвер `iBank2Key`
- Отсутствуют записи о USB-токене в конфигурационном файле `libccid`
 1. Проверьте наличие записей и при необходимости добавьте их в конфигурационный файл (см. [рис. 15](#)): `/usr/libexec/SmartCardServices/drivers/ifd-ccid.bundle/Contents/Info.plist`

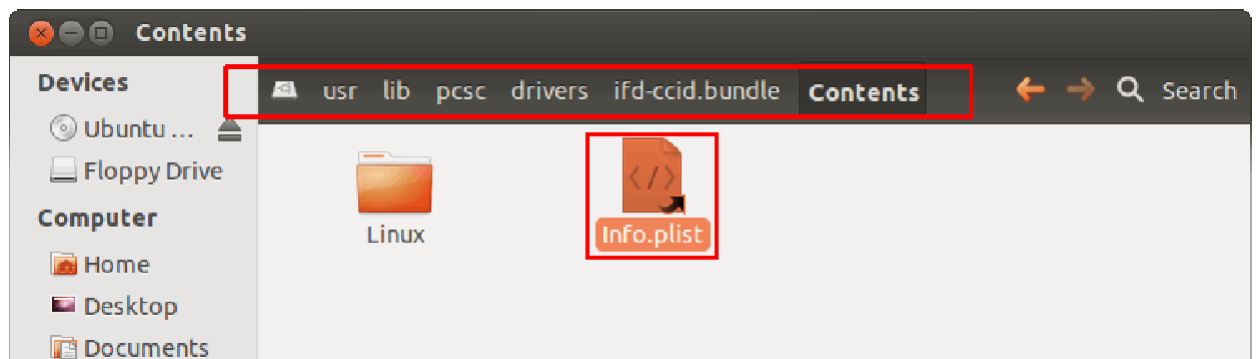


Рис. 15. Конфигурационный файл `Info.plist`

Конфигурационный файл `Info.plist` представляет собой обычный файл, который открывается любым текстовым редактором с правами суперпользователя.

Для работы электронных идентификаторов добавьте в файл в конец каждого массива записи:

- в массив `ifdVendorID` добавить `<string>0x23a0</string>`
- в массив `ifdProductID` добавить `<string>0x0008</string>`
- в массив `ifdFriendlyName` добавить `<string>Angara</string>`

2. Проверьте работоспособность USB-токена одним из способов:

— запустите `Terminal` и введите команду `pcstest`, после чего два раза введите единицу;

— запустите вручную сервис `pcscd` в отладочном режиме: `sudo arch -x86_64 /usr/sbin/pcscd -adffffff`

Результаты проверки отобразятся в соответствующих логах.

Нестабильная работа USB-токена

Неисправность проявляется следующим образом:

- Нестабильная работа USB-токена;
- Ошибки при выполнении операций в АРМах системы.

Возможные причины неисправности:

- Наличие USB-удлинителей или USB хабов;
- Ненадлежащее состояние USB-порта на компьютере или на USB-токене.