

Руководство по работе с устройством «MAC-токен VIFIT» в системе «iBank»

Руководство пользователя

Версия 1.1

Содержание

Общие сведения об устройстве	3
Работа с MAC-токеном BIFIT в системе «iBank»	6
Эксплуатация и хранение	6
Использование MAC-токена при регистрации в системе	6
Использование MAC-токена при входе в систему	8
Подтверждение данных	10
Администрирование MAC-токена	18
Устранение неисправностей	23
Устройство недоступно	23
BIFIT Signer не обнаруживает устройство	24
Нестабильная работа устройства	26

Общие сведения об устройстве

MAC-токен BIFIT – это аппаратное устройство в компактном пластиковом корпусе. Устройство подключается к компьютеру пользователя через USB-порт (см. [рис. 1](#)).




Рис. 1. MAC-токен BIFIT

Основное назначение MAC-токена BIFIT – подтверждение критичных данных электронных документов с предварительной визуализацией.

MAC-токен BIFIT может использоваться в системе «iBank» для подтверждения:

- Входа в систему;
- Платежного поручения;
- Доверенного получателя;
- Для группового подтверждения платежных поручений.

Процесс подтверждения на примере подтверждения платежного поручения:

1. Пользователь выбирает документ для подтверждения и выбирает пункт меню **Подтвердить**.
2. Поля документа, требующие проверки, передаются в MAC-токен BIFIT и отображаются на экране устройства.
3. Пользователь проверяет, совпадают ли отображаемые на устройстве данные с данными в платежном поручении.
4. Если данные верны, пользователь нажимает кнопку  на корпусе устройства.
5. MAC-токен BIFIT формирует код подтверждения с использованием подтверждаемых данных и секретного ключа, хранящегося в устройстве.
6. Код подтверждения передается на сервер системы «iBank» для дальнейшей проверки.
7. Если проверка завершилась успешно, документ считается подтвержденным и передается на исполнение банком.

Преимущества MAC-токена BIFIT:

- MAC-токен BIFIT является отдельным аппаратным устройством и не подвержен влиянию вредоносного ПО;
- Подтверждаемые данные отображаются на экране устройства. Пользователь сразу же сможет обнаружить несоответствие данных, если они были подменены;

- Формирование кода подтверждения производится по нажатию кнопки на корпусе устройства. Невозможна атака, при которой злоумышленник использует для формирования кодов подтверждения подключенное к USB-порту устройство без ведома владельца;
- Код подтверждения имеет длину 128 байт и формируется с использованием в том числе уникального идентификатора документа. Код подтверждения, сформированный для одного документа, не может быть использован для подтверждения другого документа.

Преимущество MAC-токена BIFIT перед кодами SMS-подтверждения — это отсутствие рисков, связанных с операторами мобильной связи и SMS-агрегаторами:

- Неработоспособность оператора мобильной связи или SMS-агрегатора;
- Задержка передачи SMS-сообщения;
- Дополнительные сложности и задержки при передаче SMS-сообщения за рубеж или в другие регионы;
- Сбор сторонними организациями данных из платежных поручений, передаваемых в SMS-сообщении, и последующее использование (BigData);
- Подмена SIM-карты;
- Перехват SMS-сообщения.

Аналогичные риски присутствуют при использовании банками мессенджеров для передачи корпоративным клиентам кодов подтверждений.

Преимущества MAC-токена BIFIT перед MAC-токенами других производителей:

- Удобство работы для пользователя — нет необходимости вводить критичные данные в MAC-токен вручную. Критичные данные передаются через USB-порт. Пользователь лишь контролирует данные на LCD-экране MAC-токена BIFIT;
- Удобство работы для пользователя — нет необходимости вручную вводить в клиентском АРМе сформированный код подтверждения. Код передается через USB-порт;
- Высокая криптографическая стойкость алгоритма формирования кода подтверждения — в MAC-токене BIFIT используется асимметричный криптоалгоритм на базе ГОСТ Р34.10-2012 с длиной модуля 512 бит. Секретный ключ для формирования кода подтверждения имеет длину 32 байта, является неизвлекаемым и уникальным для каждого MAC-токена BIFIT. Длина кода подтверждения — 128 байт;
- Отсутствие у банка возможности подделать код подтверждения, сформированный MAC-токеном BIFIT. Банк может лишь проверить корректность кода подтверждения под данными.

Дополнительно MAC-токен BIFIT предоставляет возможность защищенного хранения ключей ЭП.

В MAC-токене BIFIT могут сохраняться криптоконтейнеры с ключами ЭП и сертификаты ключей ЭП для СКЗИ «Крипто-КОМ 3.4».

Сертификаты ФСБ РФ на СКЗИ «Крипто-КОМ 3.4»: СФ/114-3268 (исп.40), СФ/124-3269 (исп.41), СФ/114-3270 (исп.42), СФ/124-3271 (исп.43) от 11.01.2018 г.

Сроки действия сертификатов для исп. 40-41 — 31.12.2019 г., исп. 42-43 — 11.01.2021 г.

При обращении к ключу ЭП, сохраненному в MAC-токене BIFIT, потребуется подтвердить доступ к ключу ЭП нажатием кнопки на устройстве. Для дополнительной защиты информации на MAC-токен BIFIT можно установить PIN-код.

В памяти MAC-токена BIFIT может храниться до 60 ключей ЭП.

Для работы в АРМах системы «iBank» с ключами ЭП, находящимся в памяти MAC-токена BIFIT, необходим **BIFIT Signer**. Его установка и дистрибутив для скачивания предлагаются при обращении к АРМ.

Внимание!

MAC-токен ВІFІТ обеспечивает только хранение ключей ЭП. Для формирования электронной подписи под документом криптоконтейнер с ключом ЭП извлекается из MAC-токена ВІFІТ и передается в СКЗИ, развернутое на компьютере пользователя. Расшифрование криптоконтейнера и формирование электронной подписи выполняет СКЗИ.

Хранение ключей ЭП в MAC-токене ВІFІТ является значительно более безопасным, чем хранение ключей ЭП в файле на жестком диске или флеш-носителях. Но менее безопасным, чем использование USB-токенов с неизвлекаемыми ключами ЭП (например, «MS_KEY К – АНГАРА»). Корпоративным клиентам настоятельно рекомендуется использовать USB-токены с неизвлекаемыми ключами ЭП для защищенного хранения ключей ЭП и формирования электронной подписи под документами.

Для работы с MAC-токеном ВІFІТ не требуется установки дополнительных драйверов.

MAC-токен ВІFІТ поддерживается на операционных системах:

- Windows версии 7 и выше¹;
- Linux (все версии с долговременной поддержкой);
- MacOS X версии 10.10 и выше².

Поддержка MAC-токена ВІFІТ реализована в системе «iBank», начиная с версии 2.0.24.416, в Интернет-Банке «iBank для Бизнеса».

¹Для работы с MAC-токеном ВІFІТ на операционной системе Windows 7 необходима установка официального Hotfix с сайта microsoft.com.

²При работе с MAC-токеном ВІFІТ действия, связанные с использованием ключей ЭП, недоступны в связи с ограничениями поддержки СКЗИ «Крипто-КОМ 3.4» на операционных системах MacOS.

Работа с MAC-токеном BIFIT в системе «iBank»

Эксплуатация и хранение

MAC-токен BIFIT является чувствительным электронным устройством. При его хранении и эксплуатации пользователю необходимо соблюдать ряд правил и требований, нарушение которых приводит к поломке устройства.

Следующие правила эксплуатации и хранения обеспечат длительный срок службы устройства, а также сохранность конфиденциальной информации пользователя:

- Необходимо оберегать устройство от сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т.п.);
- Устройство необходимо оберегать от воздействия высоких и низких температур. При резкой смене температур (при перемещении устройства с мороза в теплое помещение) не рекомендуется использовать устройство в течение 3 часов во избежание повреждений из-за сконденсированной на электронной схеме влаги. Необходимо оберегать устройство от воздействия прямых солнечных лучей;
- Необходимо оберегать устройство от воздействия влаги и агрессивных сред;
- Недопустимо воздействие на устройство сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества;
- При подключении устройства не прилагайте излишних усилий;
- При засорении USB-разъема устройства нужно принять меры для его очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо;
- Не разбирайте устройство — это ведет к потере гарантии;
- Необходимо избегать скачков напряжения питания компьютера и USB-шины при подключенном USB-порте, а также не извлекать устройство во время записи и считывания;
- В случае неисправности или неправильного функционирования устройства обращайтесь в ваш банк.

Внимание!

1. Не передавайте MAC-токен третьим лицам;
2. Подключайте MAC-токен к компьютеру только на время работы с системой «iBank»;
3. В случае утери (хищения) или повреждения MAC-токена немедленно свяжитесь с вашим банком.

Использование MAC-токена при регистрации в системе

Примечание:

Действие недоступно пользователям операционных систем семейства MacOS в связи с ограничениями поддержки СКЗИ «Крипто-КОМ 3.4» на данных системах.

Процесс предварительной регистрации корпоративных клиентов осуществляется в АРМ «Регистратор для корпоративных клиентов»:

1. Подключите MAC-токен к USB-порту компьютера.
2. Подключитесь к Интернету, запустите web-браузер и перейдите на страницу входа для клиентов системы «iBank» вашего банка.
3. На странице входа клиентов выберите пункт: **Регистрация** → **Подключение к системе**. В результате загрузится соответствующий АРМ.

Если на компьютере еще не установлен BIFIT Signer, появится соответствующее предупреждение со ссылкой на скачивание дистрибутива.

4. Пройдите все этапы регистрации. На восьмом шаге (см. [рис. 2](#)) в качестве хранилища ключей ЭП выберите из списка пункт **Аппаратное устройство**. В поле ниже отобразится серийный номер подключенного к компьютеру устройства.

iBank для Бизнеса

Подключение к системе

Шаг 8 из 11.

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

MAC-токен BIFIT (00-59-64-61) **Выбрать...**

Назад **Вперед**

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

5. Если к MAC-токену задан PIN-код, то появится диалог для ввода PIN-кода (см. [рис. 3](#)). Укажите значение PIN-кода пользователя.

BIFIT Signer

Введите PIN-код для хранилища ключей:
MAC-токен BIFIT (00-64-61)

PIN-код: [.....] [eye icon]

OK **Отмена**

Рис. 3. Ввод PIN-кода пользователя

Внимание!

Допускается не более 5 последовательных попыток ввода неверного PIN-кода к устройству. После этого доступ к ключам ЭП блокируется. Подробнее см. в разделе [задание PIN-кода доступа устройства](#).

6. На следующих шагах регистрации необходимо указать 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.

Примечание:

В одном MAC-токене может содержаться до 60 ключей ЭП ответственных сотрудников разных корпоративных клиентов, обслуживаемых в разных банках с разными экземплярами системы «iBank».

Использование MAC-токена при входе в систему

Примечание:

Действие недоступно пользователям операционных систем семейства MacOS в связи с ограничениями поддержки СКЗИ «Крипто-КОМ 3.4» на данных системах.

Для входа в систему:

1. Подключитесь к интернету, запустите web-браузер и перейдите на страницу для клиентов системы «iBank» вашего банка.
2. Подключите MAC-токен к USB-порту компьютера.
3. На странице входа клиентов выберите пункт: **Вход в Интернет-Банк → Выбрать электронную подпись**.
4. Выберите в списке MAC-токен (см. [рис. 4](#)), если к устройству задан PIN-код, то появится диалог для его ввода. Укажите значение PIN-кода.

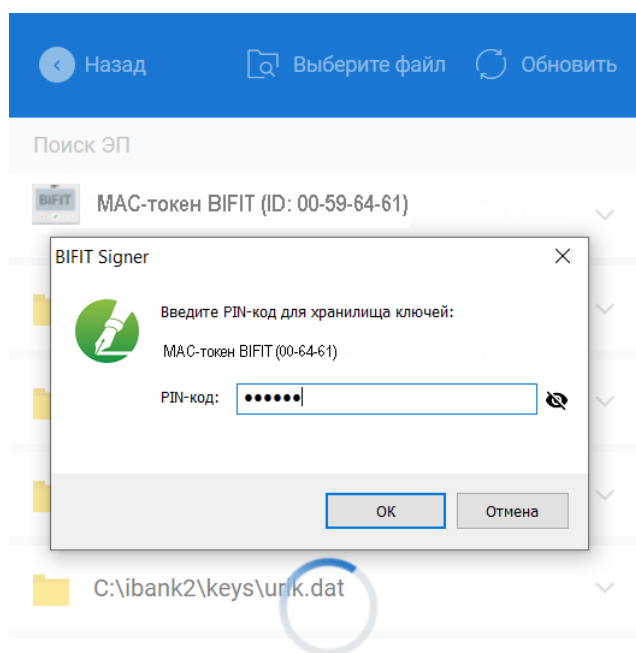


Рис. 4. Список ключей ЭП. Ввод PIN-кода

Внимание!

Допускается не более 5 последовательных попыток ввода неверного PIN-кода к устройству. После этого доступ к ключам ЭП блокируется. Подробнее см. в разделе [задание PIN-кода доступа устройства](#).

Если ввод PIN-кода не требуется выберите ключ ЭП ([рис. 5](#)) и укажите пароль к нему.

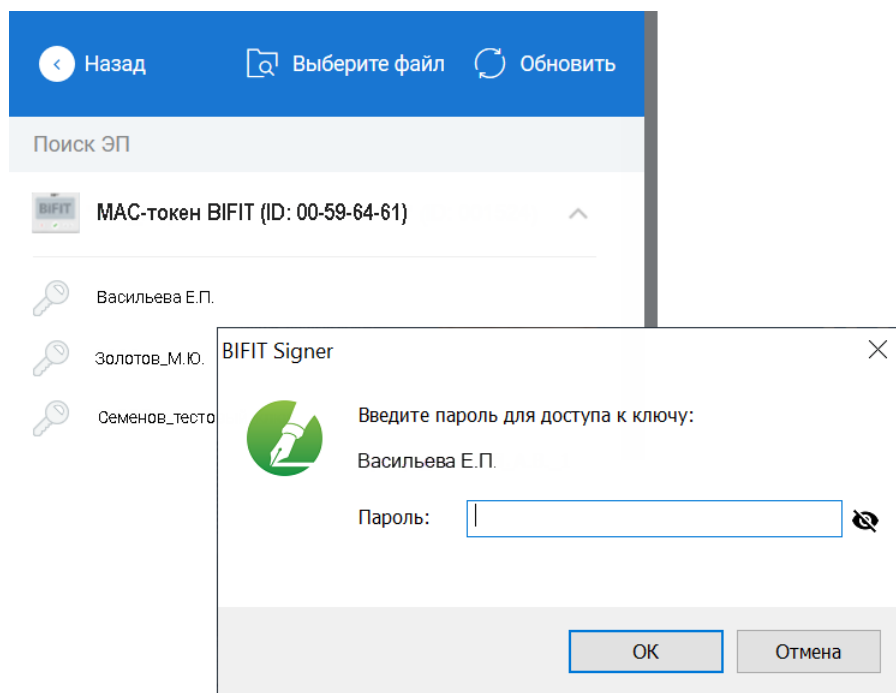


Рис. 5. Список ключей ЭП. Ввод PIN-кода

- На экране компьютера отобразится сообщение о необходимости подтверждения доступа к ключу на MAC-токене (см. [рис. 6](#)).

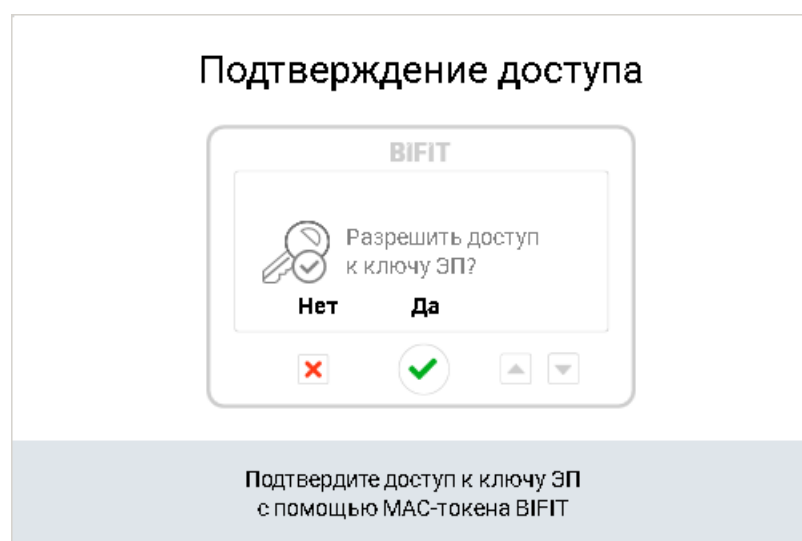


Рис. 6. Подтверждение доступа к ключу ЭП в MAC-токене


- На экране MAC-токена отобразится запрос на доступ к ключу ЭП (см. [рис. 7](#)). Для разрешения доступа к ключу нажмите кнопку  на корпусе устройства.



Рис. 7. MAC-токен. Запрос на доступ к ключу

Подтверждение данных

Настройка подтверждений

Для подтверждения документов MAC-тоном BIFIT необходимо выбрать его в качестве источника кодов подтверждения.

Настройка выполняется через меню клиентского АРМ **Настройки**, закладка **Подтверждение** (см. рис. 8).

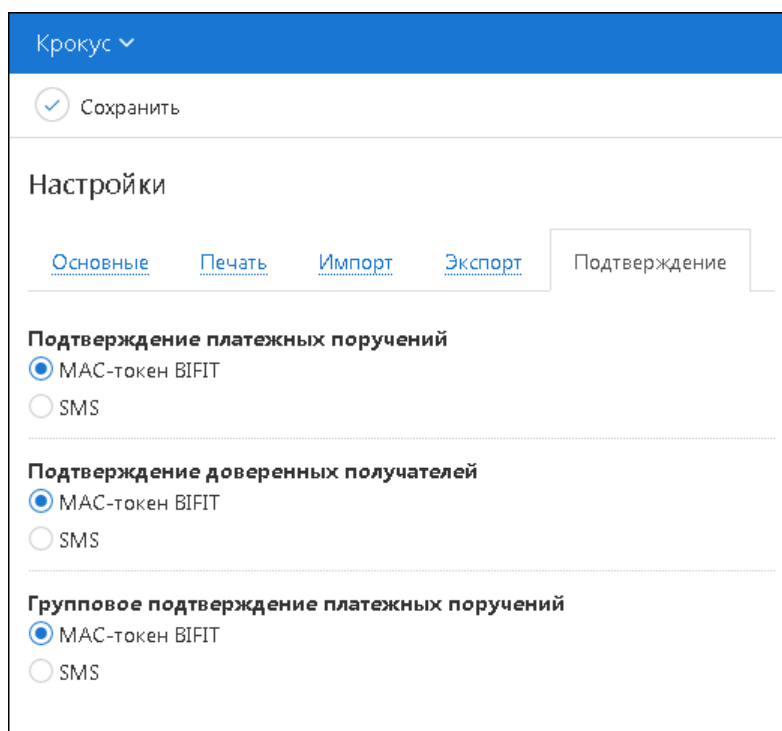


Рис. 8. Настройки подтверждения

Подтверждение входа в систему

Если для входа в систему «iBank» используется механизм многофакторной аутентификации, то после выбора ключа ЭП и ввода пароля:

1. На странице выбора способа подтверждения для входа в систему (см. [рис. 9](#)) выберите **MAC-токен BIFIT**.

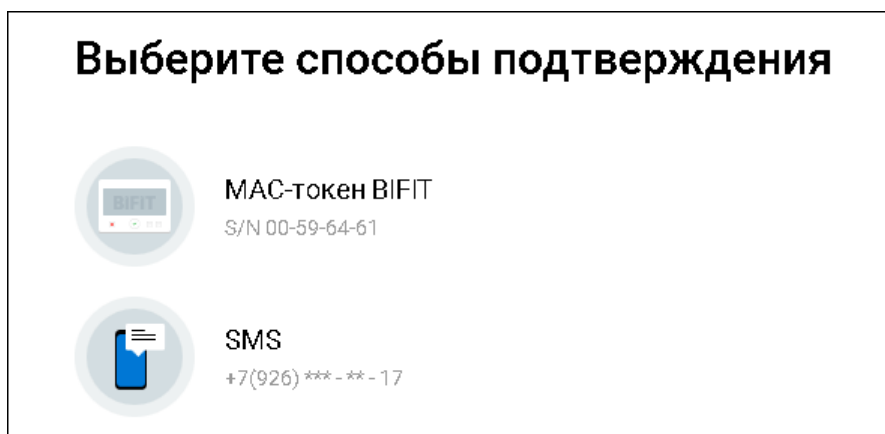


Рис. 9. Выбор способа подтверждения

2. На экране MAC-токена отобразится запрос на подтверждение входа в систему (см. [рис. 10](#)).

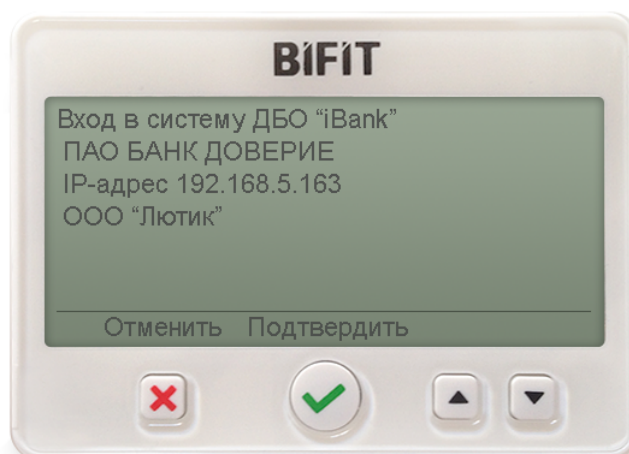


Рис. 10. MAC-токен. Запрос на подтверждение входа в систему

3. Для подтверждения входа в систему нажмите кнопку **✓** на корпусе MAC-токена. Для отмены нажмите кнопку **✗**

Подтверждение платежных поручений

Для подтверждения платежного поручения:

1. Отметьте в списке документ в статусе **Требует подтверждения** и выберите пункт **Подтвердить** контекстного меню или нажмите соответствующую кнопку на странице просмотра документа.
2. Отобразится диалог **Подтверждение платежного поручения** (см. [рис. 11](#)).

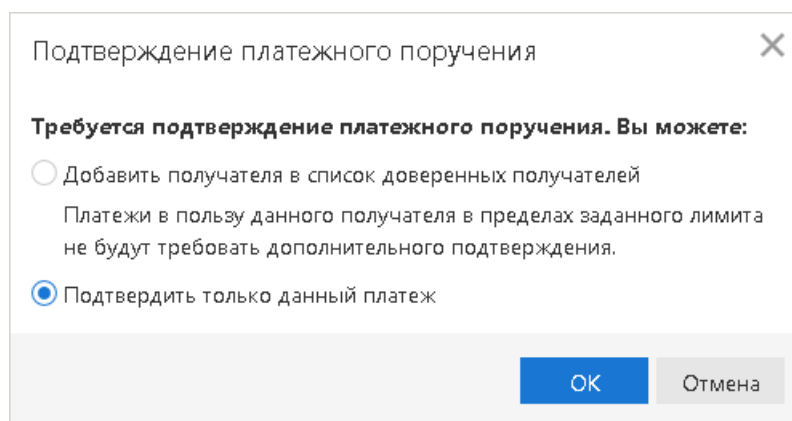


Рис. 11. Подтверждение платежного поручения. Шаг 1

3. Поставьте переключатель в положение **Подтвердить только данный платеж** и нажмите кнопку **ОК**.
4. **Примечание:**
Если подтверждение доверенных получателей недоступно, отобразится диалог как на [рис. 12](#).

В диалоге отображается серийный номер подключенного (выбранного в настройках) устройства (см. [рис. 12](#)).

Нажмите кнопку **Подтвердить** — диалог закрывается, на MAC-токен передаются критичные данные, необходимые для формирования кода подтверждения. Все элементы управления в интерфейсе Интернет-Банка блокируются.

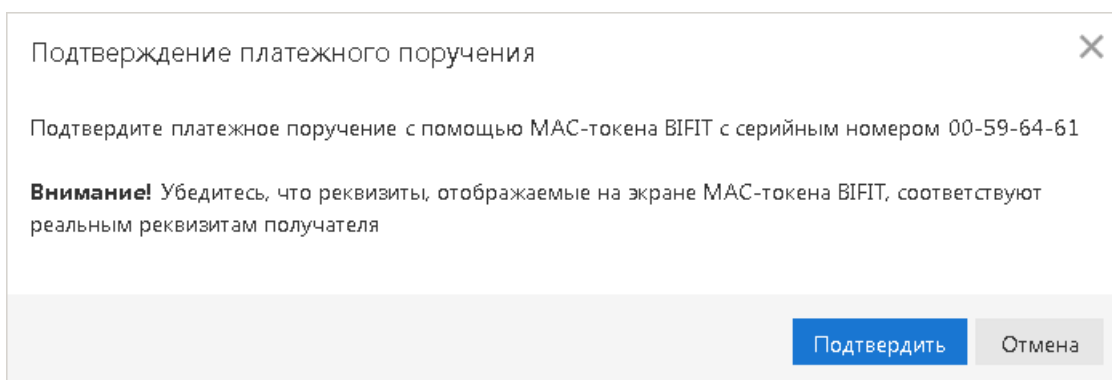


Рис. 12. Подтверждение платежного поручения. Шаг 2

5. На экране MAC-токена отображаются критичные данные (реквизиты получателя, сумма, дата и номер документа) подтверждаемого платежного поручения (см. [рис. 13](#)).

Обязательно убедитесь, что реквизиты на экране MAC-токена совпадают с фактическими реквизитами подтверждаемого документа.

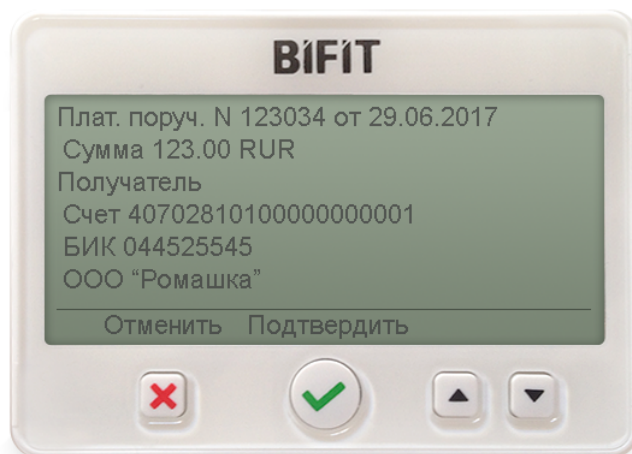








Рис. 13. MAC-токен. Запрос подтверждения платежного поручения

6. Для подтверждения документа нажмите кнопку  на корпусе MAC-токена. Для отмены нажмите кнопку .

Если кнопка  недоступна (нет подписи кнопки на экране MAC-токена), необходимо выполнить просмотр всех подтверждаемых данных на экране устройства. Для просмотра используйте кнопки  /  на корпусе устройства.

7. По итогам выполнения выбранного действия на экране MAC-токена отобразится одно из сообщений:

- *Успешно* — если была нажата кнопка , код подтверждения сформирован и прошел проверку системой «iBank» в банке;
- *Отмена* — если была нажата кнопка .
- *Ошибка* — если была нажата кнопка , но в процессе формирования кода подтверждения произошли ошибки или если код подтверждения не прошел проверку системой «iBank» в банке.

Элементы управления в интерфейсе Интернет-Банка будут разблокированы.

8. В случае успешного подтверждения документ приобретает статус **Доставлен** и направляется в банк на обработку.

Групповое подтверждение платежных поручений

Для подтверждения группы документов:

1. Отметьте в списке документы в статусе **Требует подтверждения** и выберите пункт **Подтвердить** контекстного меню.
2. Отобразится диалог **Подтверждение платежных поручений** (см. [рис. 14](#)).

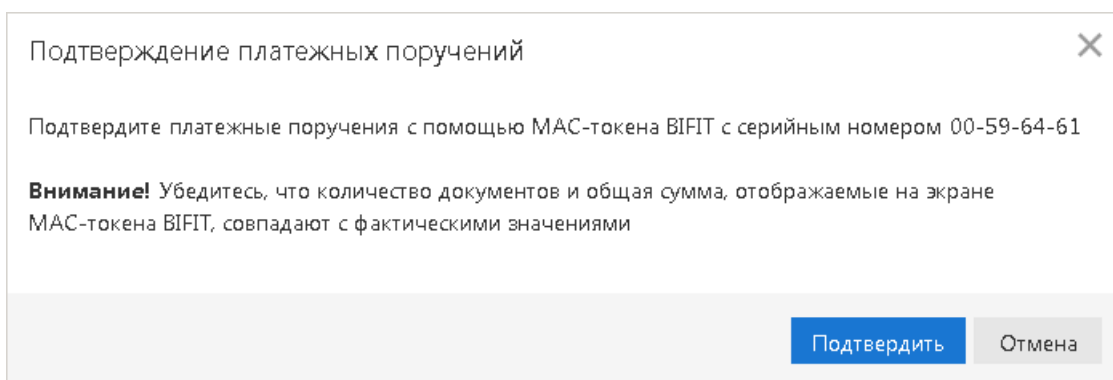


Рис. 14. Групповое подтверждение платежных поручений

3. Нажмите кнопку **Подтвердить** — диалог закрывается, на MAC-токен передаются данные, необходимые для формирования кода подтверждения. Все элементы управления в интерфейсе Интернет-Банка блокируются.
4. На экране MAC-токена отображаются параметры выбранной группы платежных поручений (см. рис. 15).

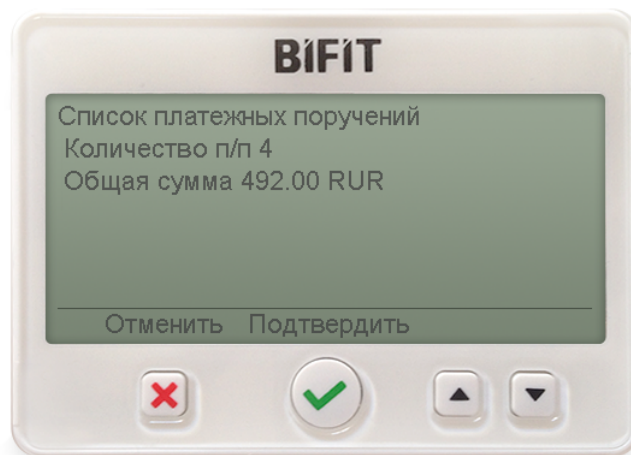


Рис. 15. MAC-токен. Запрос подтверждения группы платежных поручений

5. Обязательно убедитесь, что отображаемые на экране MAC-токена данные совпадают с параметрами подтверждаемых документов.
6. Для подтверждения операции нажмите кнопку **✓** на корпусе MAC-токена. Для отмены нажмите кнопку **✗**.
7. По итогам выполнения выбранного действия на экране MAC-токена отобразится одно из сообщений:
 - *Успешно* — если была нажата кнопка **✓**, код подтверждения сформирован и прошел проверку системой «iBank» в банке;
 - *Отмена* — если была нажата кнопка **✗**
 - *Ошибка* — если была нажата кнопка **✓**, но в процессе формирования кода подтверждения произошли ошибки или если код подтверждения не прошел проверку системой «iBank» в банке.
 Элементы управления в интерфейсе Интернет-Банка будут разблокированы.
8. В случае успешного подтверждения документы приобретают статус **Доставлен** и направляются в банк на обработку.

Подтверждение списка документов

Последовательное подтверждение выбранных документов доступно, если запрещено групповое подтверждение.

Для последовательного подтверждения документов из списка:

1. Отметьте в списке документы в статусе **Требует подтверждения** и выберите пункт **Подтвердить** контекстного меню.
2. Отобразится диалог **Подтверждение платежных поручений** (см. [рис. 16](#)).

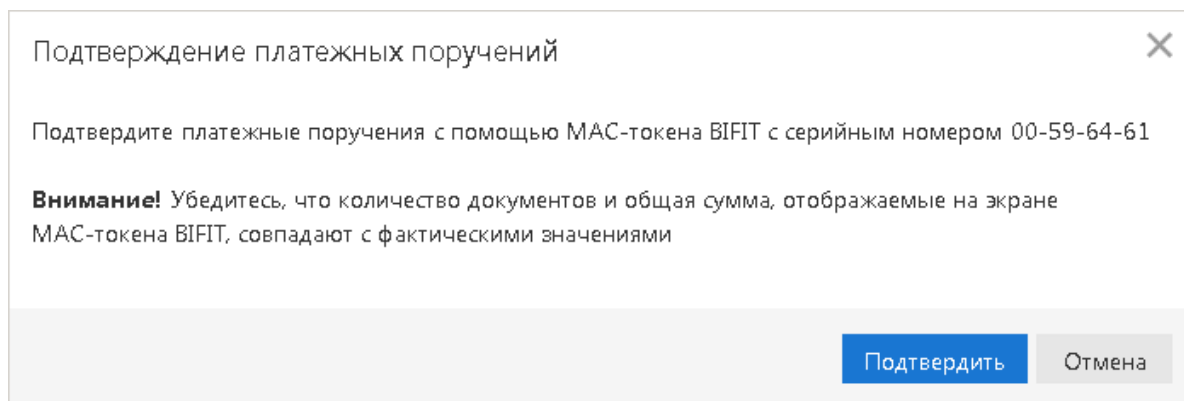


Рис. 16. Подтверждение платежных поручений

3. Нажмите кнопку **Подтвердить** — диалог закрывается. На экране компьютера отобразится диалог **Подтверждение документов** (см. [рис. 17](#)).

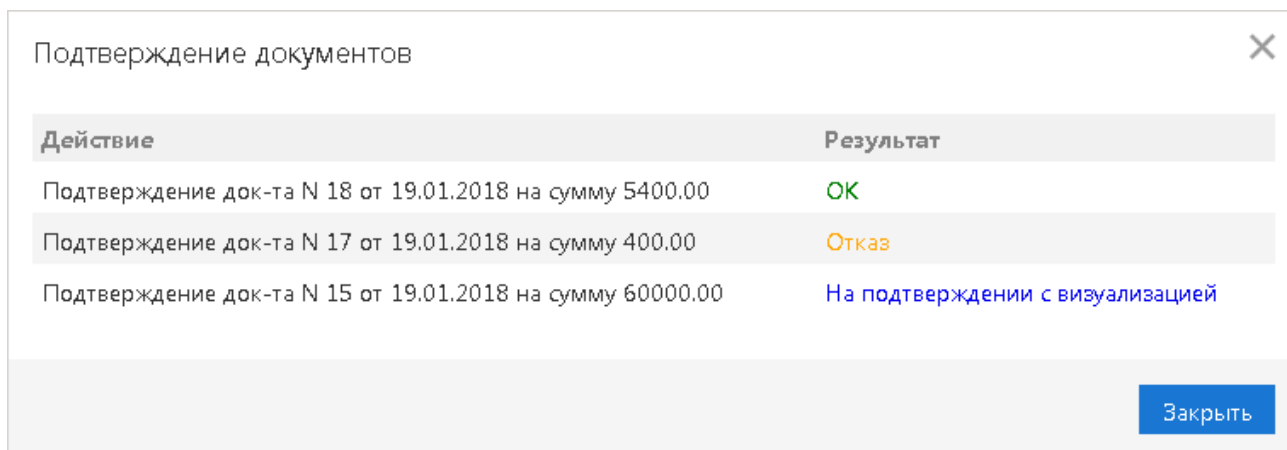




Рис. 17. Подтверждение документов

4. Далее выполняется последовательное подтверждение выбранных документов по одному, начиная с первого.

При подтверждении одного из группы документов на экране MAC-токена отображаются реквизиты подтверждаемого документа (см. [рис. 13](#)). Для подтверждения операции нажмите кнопку  на корпусе MAC-токена. Для отмены нажмите кнопку .

5. После завершения подтверждения очередного документа с любым вариантом завершения, в том числе отмены, происходит автоматический переход к подтверждению следующего документа.
6. В диалоге **Подтверждение документов** в столбце **Результат** могут отображаться следующие значения:

- «» (пусто) — документ ожидает своей очереди;
- **На подтверждении с визуализацией** — документ передан в MAC-токен и ожидается результат подтверждения;
- **ОК** — документ успешно подтвержден;
- **Отказ** — пользователь отменил подтверждение документа. Документ не подтвержден;
- **Ошибка** — при обработке документа возникла ошибка. Документ не подтвержден.

Подтверждение доверенного получателя

Справочник **Доверенные получатели** позволяет формировать список контрагентов, платежи в пользу которых не будут требовать дополнительного подтверждения. Как правило, такими получателями являются контрагенты, с которыми наиболее часто осуществляются взаиморасчеты. Для каждого доверенного получателя разрешено задавать индивидуальный лимит для суммы платежного поручения. Платежи в пользу таких получателей, совершаемые в рамках индивидуального лимита, не будут требовать дополнительного подтверждения, а сразу получают статус **Доставлен**.

Для управления доверенными получателями необходимо наличие соответствующих прав.

Для добавления доверенного получателя:

1. Начните добавление доверенного получателя одним из следующих способов:
 - Выберите опцию **Добавить получателя в список доверенных получателей** в диалоге **Подтверждение платежного поручения** (см. [рис. 11](#));
 - Нажмите ссылку **Сделать получателя доверенным** на форме просмотра платежного поручения;
 - Выберите пункт **Добавить в доверенные** контекстного меню в **Справочнике корреспондентов**;
 - Нажмите кнопку **Новый** в **Справочнике доверенных получателей**.
2. Откроется диалог **Добавление доверенного получателя** (см. [рис. 18](#)).

Добавление доверенного получателя

Счет 4070281062407879272 БИК 043207730

Получатель ОАО "Прогресс Парк"

Установить лимит на разовый платеж в размере 100000 руб.

Платеж на сумму, превышающую лимит, потребует подписи с визуализацией или дополнительного подтверждения

Подтвердить Отмена

Рис. 18. Добавление доверенного получателя. Шаг 1

3. Заполните или отредактируйте реквизиты доверенного получателя. При необходимости установите лимит на разовый платеж.
4. Нажмите кнопку **Подтвердить** — в диалоге отобразится серийный номер подключенного (выбранного) устройства (см. [рис. 19](#)). В MAC-токен направляются данные о доверенном получателе. Все элементы управления в интерфейсе Интернет-Банка блокируются.

Добавление доверенного получателя

Счет 4070281062407879272 БИК 043207730

Получатель ОАО "Прогресс Парк"

Установить лимит на разовый платеж в размере 100000 руб.

Платеж на сумму, превышающую лимит, потребует подписи с визуализацией или дополнительного подтверждения

Подтвердите реквизиты получателя с помощью MAC-токена BIFIT с серийным номером 00-59-64-61

Внимание! Убедитесь, что реквизиты, отображаемые на экране MAC-токена BIFIT, соответствуют реальным реквизитам получателя

Подтвердить Отмена

Рис. 19. Добавление доверенного получателя. Шаг 2

- На экране MAC-токена отображаются реквизиты доверенного получателя (см. рис. 20).

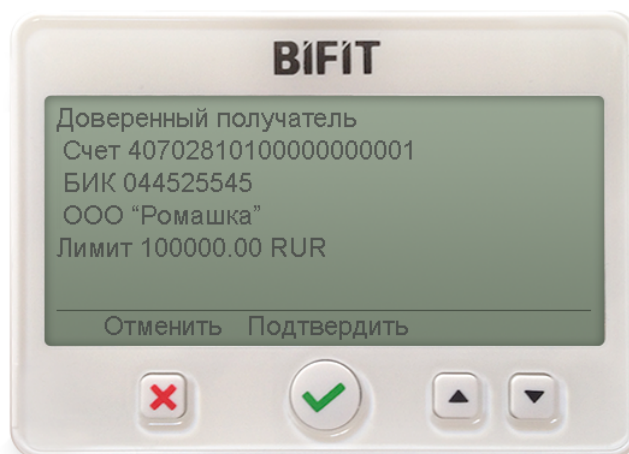



Рис. 20. MAC-токен. Запрос подтверждения доверенного получателя

- Обязательно убедитесь, что реквизиты на экране MAC-токена совпадают с реквизитами подтверждаемого доверенного получателя.
- Для подтверждения операции нажмите кнопку на корпусе MAC-токена. Для отмены нажмите кнопку .
- По итогам выполнения выбранного действия на экране MAC-токена отобразится одно из сообщений:
 - Успешно* — если была нажата кнопка , код подтверждения сформирован и прошел проверку системой «iBank» в банке;
 - Отмена* — если была нажата кнопка .

- *Ошибка* — если была нажата кнопка , но в процессе формирования кода подтверждения произошли ошибки или если код подтверждения не прошел проверку системой «iBank» в банке.

Элементы управления в интерфейсе Интернет-Банка будут разблокированы.

Администрирование MAC-токена

Примечание:

Действие недоступно пользователям операционных систем семейства MacOS в связи с ограничениями поддержки СКЗИ «Крипто-КОМ 3.4» на данных системах.

Для ключей ЭП хранящихся в памяти MAC-токена доступны следующие действия:

- Печать сертификата ключа ЭП;
- Смена пароля к ключу ЭП;
- Удаление ключа ЭП;
- Смена наименования ключа ЭП.

Для MAC-токена доступно [задание PIN-кода доступа устройства](#).

Администрирование ключей ЭП, хранящихся в памяти MAC-токена, выполняется:

- корпоративными клиентами и сотрудниками центра финансового контроля в АРМ **«Регистратор для корпоративных клиентов»**. Для перехода в АРМ выполните:
 - Интернет-Банк — на странице входа клиентов банка перейдите: **Регистрация** → **Администрирование ключей ЭП**;
 - Офлайн-Банк — перейдите в раздел **Электронные подписи** → **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»**. 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. Под серийным номером отобразится список ключей ЭП (см. [рис. 21](#)).

Администрирование ключей ЭП

Укажите тип хранилища ключей ЭП

Ключ на диске

Аппаратное устройство

MAC-токен BIFIT (00-59-64-61) Выбрать

Наименование ключа
Петров П.П.
Иванов С.И.
Сахаров Н.В.
Иванов И.И.

Количество ключей на аппаратном устройстве: 4

Сменить PIN Печать Сменить пароль Переименовать Удалить

Рис. 21. АРМ «Регистратор». Администрирование ключей ЭП

- Выберите ключ ЭП и нажмите кнопку, соответствующую операции, которую необходимо выполнить.
- Для получения доступа к ключу ЭП будет запрашиваться пароль к ключу и подтверждение доступа к ключу с помощью нажатия кнопки на корпусе устройства (см. [рис. 22](#)).

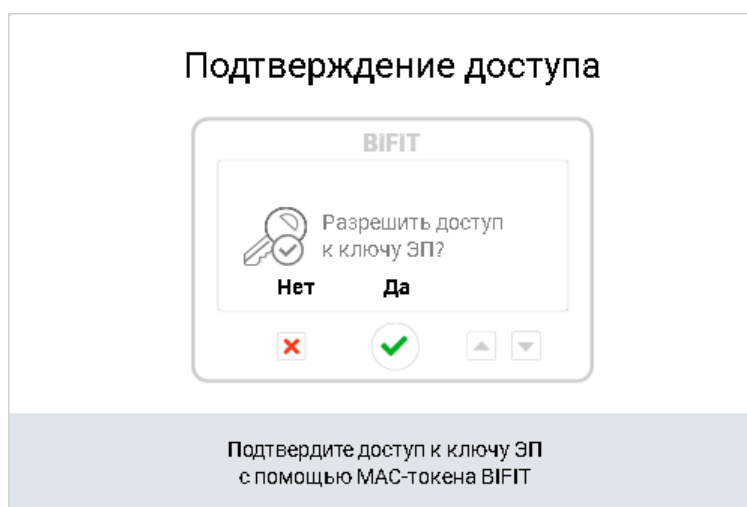


Рис. 22. Подтверждение доступа к ключу ЭП в MAC-токене

При смене пароля к ключу ЭП подтверждение доступа к ключу будет запрашиваться дважды. Сначала для проверки текущего пароля к ключу, потом для установки нового пароля.

При удалении ключа дополнительно будет запрашиваться подтверждение удаления ключа (см. [рис. 23](#)).

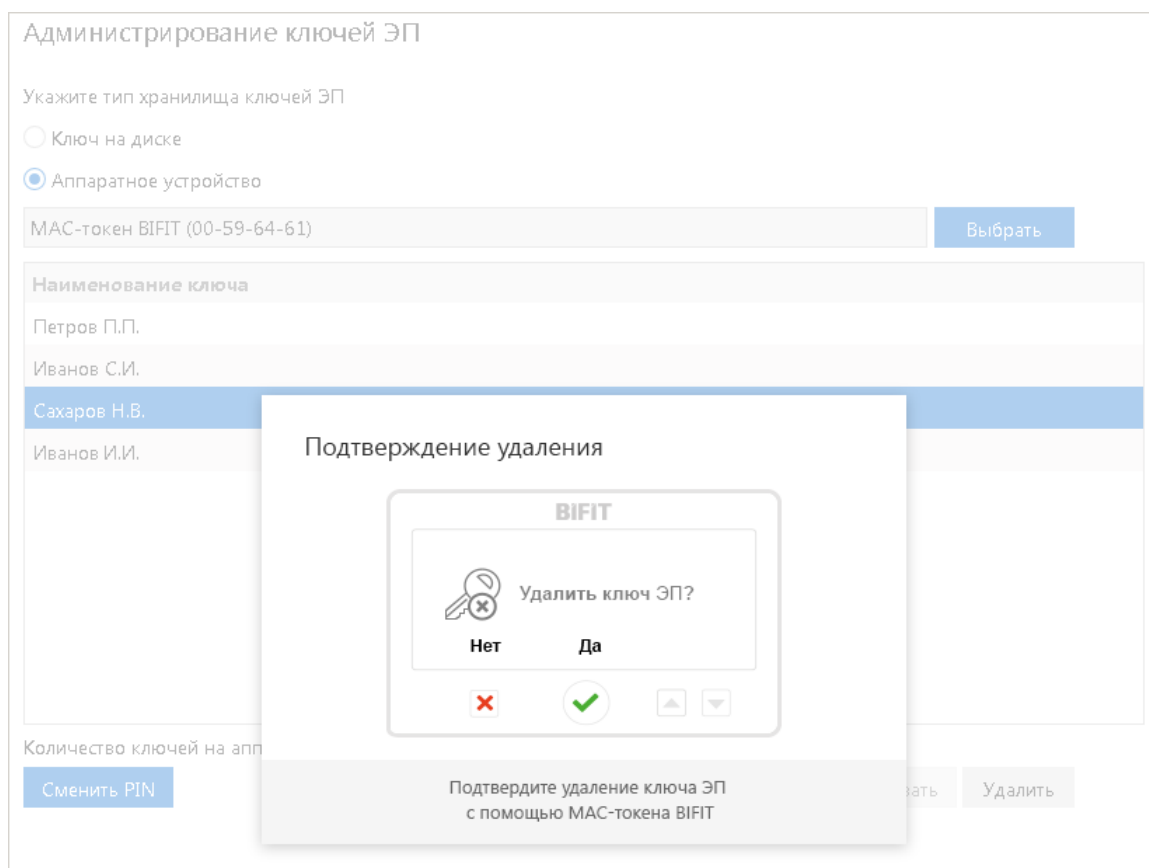


Рис. 23. Подтверждение удаления ключа в MAC-токене



На экране MAC-токена отобразится запрос на удаление ключа ЭП (см. рис. 24). Для подтверждения удаления ключа ЭП нажмите кнопку  на корпусе устройства. Для отмены удаления нажмите кнопку .



Рис. 24. MAC-токен. Запрос на удаление ключа ЭП

Внимание!

Ключи ЭП удаляются безвозвратно, восстановление удаленного ключа невозможно. Будьте внимательны при выборе ключа ЭП для удаления.

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 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.

Задание PIN-кода доступа устройства

Для обеспечения дополнительной защиты от несанкционированного доступа к ключам ЭП, хранящимся в памяти MAC-токена, реализована возможность задавать PIN-код доступа к устройству.

При обращении к MAC-токену с заданным PIN-кодом отсутствует возможность получения списка ключей устройства и каких-либо действий с ними, до момента ввода корректного PIN-кода.

Назначенный PIN-код к MAC-токену удалить нельзя, его можно лишь сменить.

PIN-код к MAC-токену, если он установлен, запрашивается у пользователя при выполнении следующих действий:

- аутентификация в клиентском АРМ;
- обращение к MAC-токену в случае его отключения и последующего подключения;
- обращение к MAC-токену 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** (см. [рис. 25](#), [рис. 26](#)), дважды введите новое значение PIN-кода и нажмите кнопку **Принять** (см. [рис. 27](#)).

Внимание!

Допускается не более 5 последовательных попыток ввода неверного PIN-кода к устройству. После этого доступ к ключам ЭП блокируется.

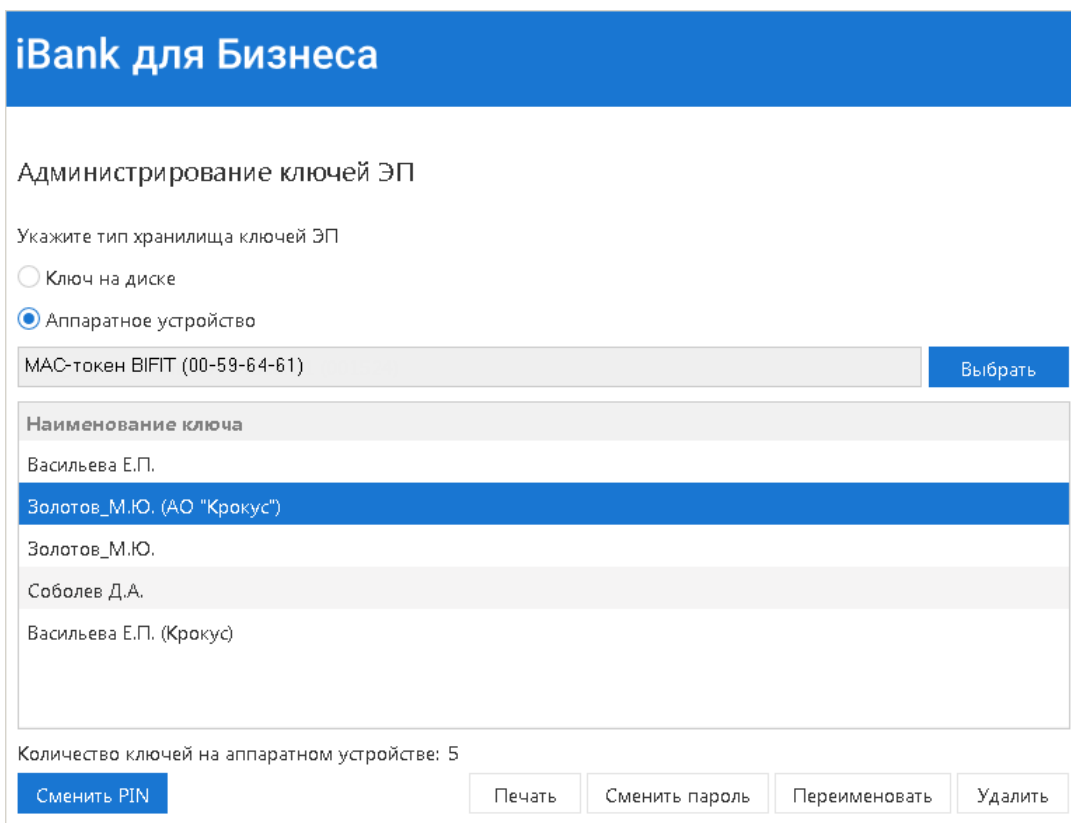


Рис. 25. АРМ "Регистратор для корпоративных клиентов". Администрирование ключей ЭП

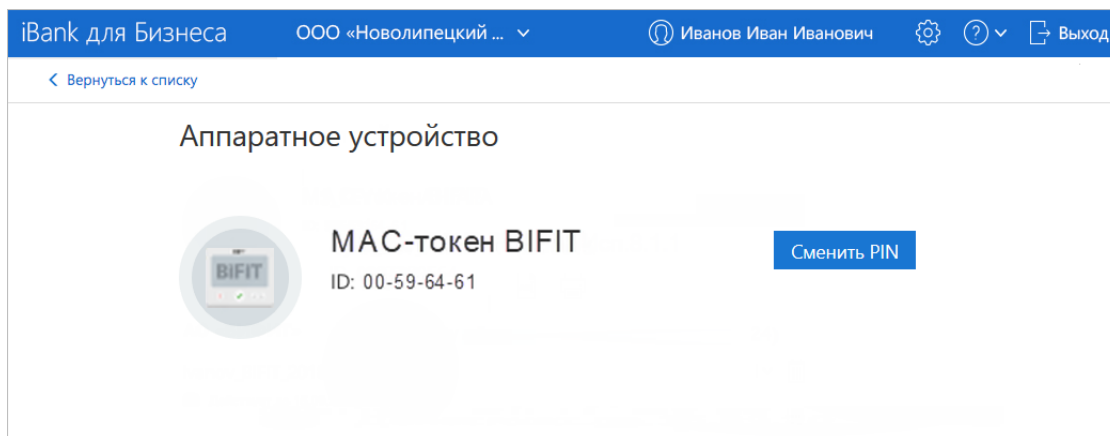


Рис. 26. АРМ "Интернет-Банк для корпоративных клиентов". Раздел "Электронные подписи", вкладка "Аппаратные устройства"

Рис. 27. Смена PIN-кода для хранилища ключей

Устранение неисправностей

Наиболее часто встречающиеся неисправности:

- Устройство недоступно для выбора
- BIFIT Signer не обнаруживает устройство
- Нестабильная работа USB-токена

Устройство недоступно

Неисправность проявляется в недоступности устройства для выбора в системе «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. 28](#)).

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).

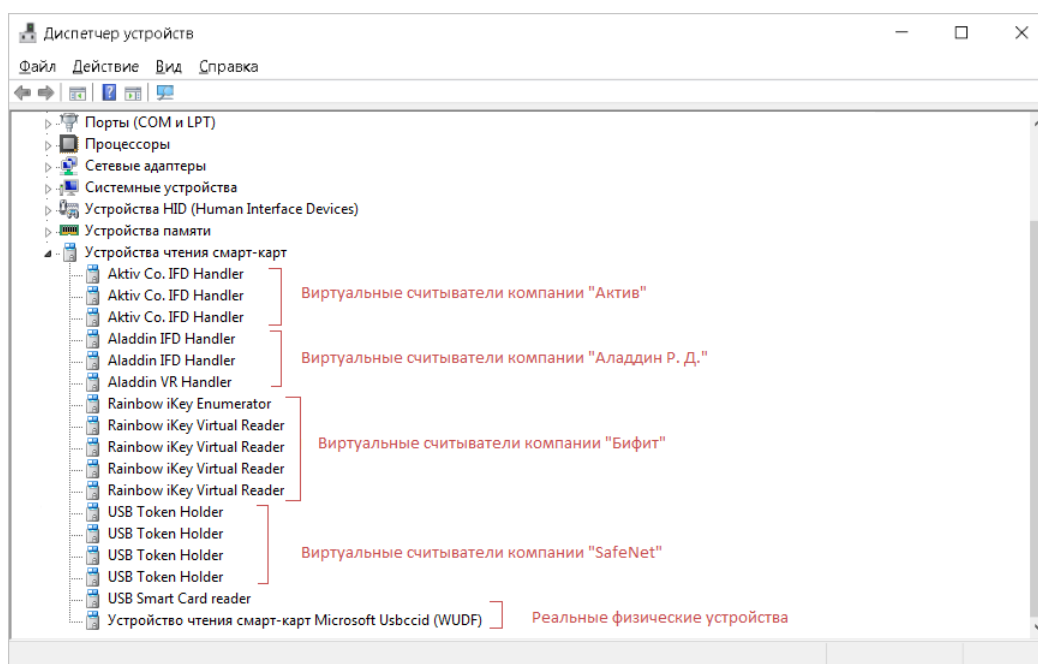


Рис. 28. Диспетчер устройств. Устройства чтения смарт-карт

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. 29](#)) или выполните деинсталляцию установленного для устройства ПО.

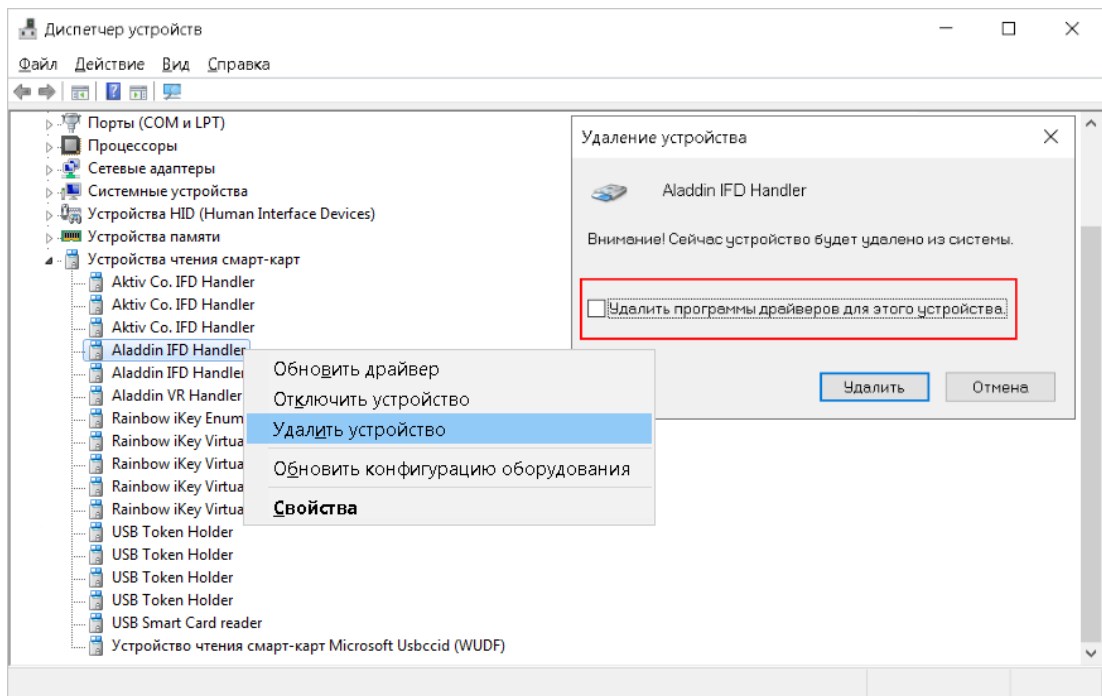


Рис. 29. Диспетчер Устройств. Удаление виртуального считывателя

BIFIT Signer не обнаруживает устройство

Решение неисправности приведено отдельно для операционных систем:

- [ОС семейства Windows](#)
- [ОС семейства Linux](#)

Неисправность может проявляться следующим образом:

- Устройство не отображается:
 - при входе в систему в списке ключей ЭП;
 - 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 выборе аппаратного устройства для генерации ключа ЭП;
 - при переходе в раздел **Электронные подписи** в Интернет-Банке для корпоративных клиентов;
 - при подписании документов;
 - в иных случаях.

Решение для операционных систем семейства Windows

Устройство может отображаться в диспетчере устройств, но не определяться BIFIT Signer.

Варианты устранения неисправности:

- Перезапустите службу **Смарт-карта**, например, указанным способом:

1. Откройте настройки служб Windows: **Панель управления** → **Система и безопасность** → **Администрирование** → **Службы**
2. Выберите пункт контекстного меню **Перезапустить** для службы **Смарт-карта** (см. [рис. 30](#)).

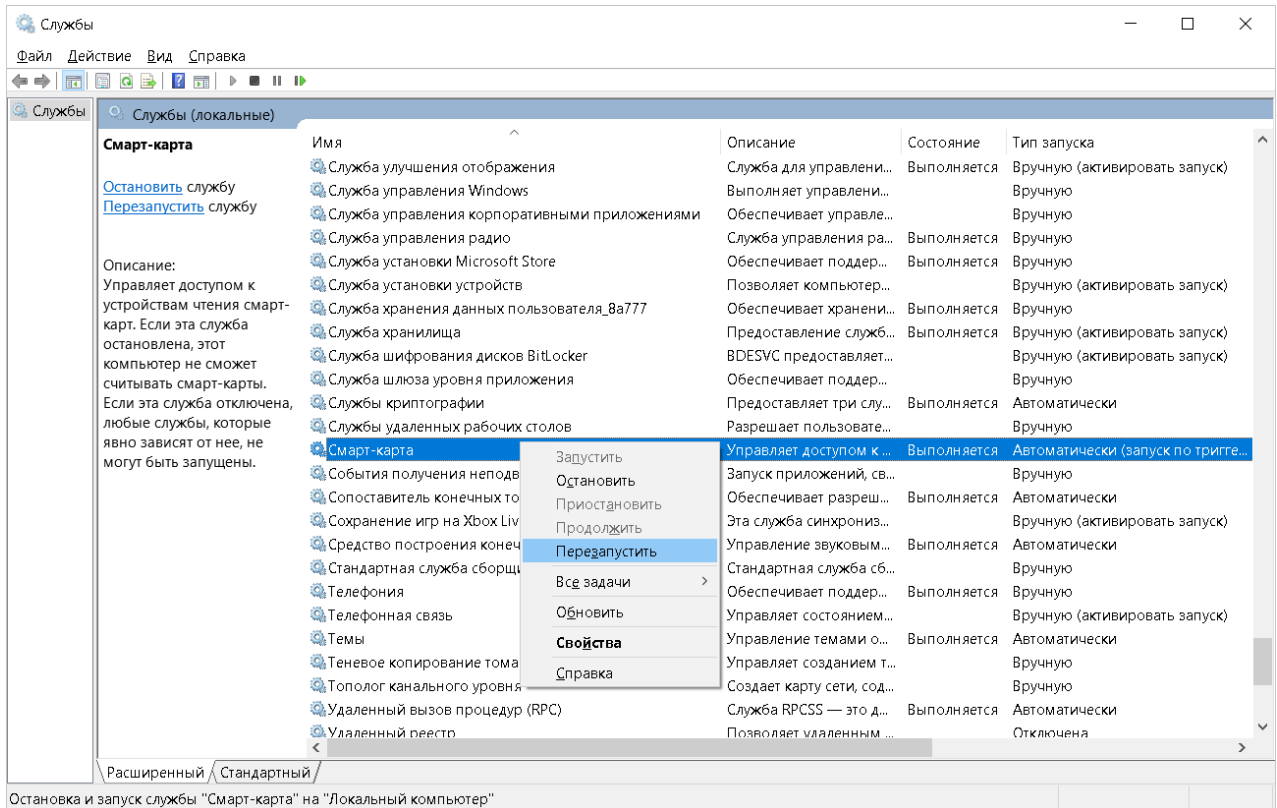


Рис. 30. Настройки служб Windows. Перезапуск службы "Смарт-карта"

- Проверьте, что установленное на компьютере антивирусное программное обеспечение не блокирует работу BIFIT Signer. Отключите антивирусное ПО на время проверки и настройки BIFIT Signer;
- Переустановите 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>0x0005</string>`
 - в массив `ifdFriendlyName` добавить `<string>MAC-token BIFIT</string>`
 3. Проверьте работоспособность устройства:

— 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. 31](#)).

```
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/ufd-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: IFDHCreateChannelByName() lun: 0, device: usb:23a0/0008:libudev:0:/dev/bus/usb/003/013
00000005 ccid_usb.c:180: OpenUSBByName() Reader index: 0, Device: usb:23a0/0008:libudev:0:/dev/bus/usb/003/013
00000007 ccid_usb.c:212: OpenUSBByName() interface number: 0
0001726 ccid_usb.c:303: OpenUSBByName() Checking device: 3/13
00000004 ccid_usb.c:358: OpenUSBByName() Trying to open USB bus/device: 3/13
00000034 ccid_usb.c:446: OpenUSBByName() using USB bus/device: 3/13
00000003 ccid_usb.c:932: ControlUSB() request: 0x03
00000084 ccid_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. 31. Отладочный лог терминала

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

Нестабильная работа устройства

Неисправность проявляется следующим образом:

- Нестабильная работа устройства;
- Ошибки при выполнении операций в APMax системы.

Возможные причины неисправности:

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