

ПЕРСОНАЛЬНЫЙ АППАРАТНЫЙ КРИПТОПРОВАЙДЕР

ПАСПОРТ

**на USB-токен «iBank 2 Key»
(исполнение корпуса «М»)**



Оглавление

1. Обозначения и сокращения
2. Общие сведения о USB-токене «iBank 2 Key» (исполнение корпуса «М»)
3. Назначение и область применения
4. Основные характеристики, внешний вид, размеры
5. Подготовка токена к работе
6. Эксплуатация, хранение и транспортировка токена
7. Гарантийные обязательства
8. Адрес изготовителя ООО «БИФИТ»

1. Обозначения и сокращения

ЭЦП – электронно-цифровая подпись.

«iBank 2» – система электронного банкинга. Разработчик – компания «БИФИТ».

СКЗИ – средство криптографической защиты информации.

Имитовставка – последовательность данных фиксированной длины, получаемая по определенному правилу из открытых данных и секретного ключа и добавляемая к данным для обеспечения имитозащиты.

2. Общие сведения о USB-токене (исполнение корпуса «М»)

USB-токен «iBank 2 Key» (исполнение корпуса «М») – это аппаратное USB-устройство, состоящее из PC/SC-совместимого USB-картридера и криптографического микроконтроллера смарт-карт.

USB-токен «iBank 2 Key» (исполнение корпуса «А», в дальнейшем также USB-токен, токен) обеспечивает:

- . • аппаратную генерацию случайных чисел;
- . • генерацию ключей ЭЦП;
- . • формирование и проверку ЭЦП по ГОСТ Р34.10-2001;
- . • генерацию ключей шифрования;
- . • шифрование информации по ГОСТ 28147-89;
- . • формирование и проверку имитовставки по ГОСТ 28147-89;
- . • вычисление хеш-функции по ГОСТ Р34.11-94.

В токене может храниться до 64-х секретных ключей ЭЦП.

3. Назначение и область применения USB-токена

USB-токен «iBank 2 Key» подключается к компьютеру через порт USB и не требует для работы дополнительного оборудования.

Использование USB-токена «iBank 2 Key» делает принципиально невозможным хищение секретных ключей ЭЦП, используемых при работе в системе электронного банкинга «iBank 2». В том числе при работе в «недоверенной» программной среде.

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

Формирование ЭЦП клиента происходит в соответствии с ГОСТ Р34.10-2001 непосредственно внутри SIM-карты токена: на вход токен принимает электронный документ, на выходе выдает ЭЦП под данным документом.

Доступ ко всем криптографическим функциям USB-токена предоставляется только после ввода пользователем корректного PIN-кода. Для каждого секретного ключа ЭЦП – свой PIN-

код.

В одном токене допускается одновременно хранить секретные ключи:

- нескольких ответственных сотрудников одного корпоративного клиента;
- нескольких корпоративных клиентов;
- нескольких корпоративных клиентов, обслуживаемых в разных банках с помощью системы «iBank 2».

4. Основные характеристики USB-токена

(исполнение корпуса «А»)



Интерфейс:	USB 1.1 / USB2.0 Type A
Энергопотребление:	менее 50 мА
Рабочая температура окружающей среды:	+10 ... +70 градусов по Цельсию
Температура хранения и транспортировки:	-30 ... +85 градусов по Цельсию
Относительная влажность:	от 0 до 90% без образования конденсата
Габаритные размеры:	65 x 20 x 10 мм
Вес:	13 грамм

USB-токен объединяет в компактном пластиковом корпусе PC/SC-совместимый USB-картридер и криптографического микроконтроллера ST19NR66 производства компании STMicroelectronics. Микроконтроллер сертифицирован на соответствие стандарту ISO/IEC 15408 (common criteria) с уровнем доверия EAL5+.

В микроконтроллере при производстве масочным методом «прошита» карточная операционная система российского разработчика «Терна СИС». В составе карточной операционной системы содержится СКЗИ «Криптомодуль-С» (разработчик – ЗАО «Терна СБ»), сертифицированное ФСБ РФ по классу КС2. Сертификат ФСБ РФ рег. № СФ/114-1009 от 14.05.2007 г.

Для использования функций токена «iBank 2 Key» в систему электронного банкинга «iBank 2» встроена поддержка криптобиблиотеки СКЗИ «Криптомодуль С» компании «Терна СБ», сертифицированной ФСБ (сертификат соответствия рег. № СФ/1141009 от 14 мая 2007 года, действителен до 9 марта 2010 года).

Работа USB-токена обеспечена для следующих платформ :

- . • Microsoft Windows XP/2000/Vista/2003
- . • Apple Macintosh Mac OS X 10.4.8 или старше
- . • Linux 2.6.x

Поддержка USB-токена встроена в следующие клиентские модули системы «iBank 2»:

- Internet-Банкинг
- PC-Банкинг
- Центр финансового контроля Онлайн
- Центр финансового контроля Офлайн
- Корпоративный автоклиент

5. Подготовка USB-токена к работе

USB-токен «iBank 2 Key» проходит предпродажную подготовку, гарантирующую правильную работоспособность токена в системе электронного банкинга «iBank 2». Перед началом работы с токеном пользователю необходимо предварительно установить драйвер USB-токена.

Внимание!

Драйвер USB-токена «iBank 2 Key» необходимо установить до подключения устройства. Во время установки драйвера все приложения должны быть закрыты во избежание ошибки разделения файлов. Для установки драйвера пользователь должен иметь права администратора системы.

Для установки драйвера USB-токена «iBank 2 Key» запустите файл *iBank2KeySetup.exe*, который можно загрузить с сайта банка или с сайта компании БИФИТ по адресу: <https://www.bifit.com/distrib/ru/iBank2KeySetup.exe>. Подробное описание установки драйвера токена описано в «Руководстве по работе с USB-токенами «iBank 2 Key», которое предоставляет банк или которое можно получить с сайта компании БИФИТ по адресу: <http://www.bifit.com/download/docs/clients>.

6. Эксплуатация, хранение и транспортировка USB-токена

USB-токен «iBank 2 Key» является чувствительным электронным прибором. Следование данным правилам эксплуатации и хранения обеспечат длительный срок службы USB-токена «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.).
- . • Необходимо оберегать USB-токен от воздействия высоких и низких температур. При резкой смене температур (вносе охлажденного USB-токена 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, от воздействия влаги и агрессивных средств.

- . •Необходимо не допускать скачков напряжения питания компьютера и USB-шины при подключенном токене к USB-порту компьютера.
- . •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 для избежания механических повреждений разъема токена.
- . •В нерабочее время USB-токен необходимо всегда держать закрытым во избежание попадания на разъем 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 приведет к потере его работоспособности.
- . •Не извлекайте токен из USB-порта компьютера во время записи и считывания.
- . •В случае обнаружения неисправности или неправильного функционирования USB-токена обратитесь в Банк.

Важно!

Не передавайте USB-токен третьим лицам! Не сообщайте третьим лицам PIN-код доступа к секретному ключу ЭЦП! В случае утери (хищения) USB-токена немедленно свяжитесь с банком.

Перевозка упакованных токенов может осуществляться всеми видами транспорта, кроме негерметизированных отсеков самолетов и открытых палуб кораблей и судов, в соответствии с правилами перевозки грузов, действующими на данном виде транспорта. В качестве транспортной тары используют тару, обеспечивающую сохранность груза при транспортировании.

Транспортировка токенов осуществляется в технологической упаковке по 30 штук USB-токенов в упаковке.

Хранение токенов осуществляется в закрытом помещении комнатной температуры при отсутствии в окружающем воздухе кислотных, щелочных и других агрессивных примесей.

7. Гарантийные обязательства

Гарантийный срок эксплуатации USB-токена «iBank 2 Key» составляет двенадцать месяцев со дня продажи.

8. Адрес изготовителя ООО «БИФИТ»

Россия, 105203, г. Москва, ул. Нижняя Первомайская, д. 46, стр. 1
Телефон: (495) 797-8889
Email: token@bifit.com, ksn@bifit.com