ПЕРСОНАЛЬНЫЙ АППАРАТНЫЙ КРИПТОПРОВАЙДЕР

ПАСПОРТ

на смарт-карту «iBank 2 Key»

http://www.bifit.com
e-mail: info@bifit.com
ph/fax +7 (495) 797-8889

Оглавление

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 смарт-карте.

Смарт-карта «iBank 2 Key» – это интеллектуальная пластиковая карта с встроенным криптографическим микроконтроллером смарт-карт, позволяющим осуществлять криптографические операции и вычисления.

Смарт-карта «iBank 2 Key» (в дальнейшем также смарт-карта, карта) 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 карте может одновременно храниться до 64-х секретных ключей ЭЦП.

3. Назначение и область применения смарт-карты.

Смарт-карта «iBank 2 Key» подключается к компьютеру через кардридер - внешнее или внутреннее устройство для осуществления операций чтения/записи с/на смарт-карту. Внешним устройством чаще всего используется недорогой портативный USB-считыватель смарт-карт. Также может использоваться настольная клавиатура с интегрированным считывателем смарт-карт. На многих моделях ноутбуков встроенный считыватель уже присутствует в базовой конфигурации.

Использование смарт-карты 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 карты, хранится в защищенной памяти карты и никогда, никем и ни при каких условиях не может быть из карты считан.

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

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

На одной карте 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 смарт-карты

Интерфейс:	ISO 7816-3 T=1 и T=0 протокол
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:	86 x 54 x 0.8 мм
Вес:	4 грамма

Смарт-карта включает в себе криптографический микроконтроллер 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 смарт-карты «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).

На обратной стороне карты нанесен внутренний идентификатор карты, состоящий из 14-символьной алфавитно-цифровой последовательности.

Работа смарт-карты обеспечена для следующих платформ :

- Microsoft Windows XP/2003/Vista
- Apple Macintosh Mac OS X 10.5.4 или старше
- Linux 2.6.x

Поддержка смарт-карты встроена в следующие клиентские модули системы «iBank 2»:

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

5. Подготовка смарт-карты к работе

Смарт-карта «iBank 2 Key» проходит предпродажную подготовку, гарантирующую правильную ее работоспособность в системе электронного банкинга «iBank 2».
Перед началом работы со смарт-картой пользователю необходимо предварительно установить драйвер считывателя смарт-карт (если он не установлен). При использовании CCID-совместимого считывателя смарт-карт установка драйвера для него не потребуется.

> *Внимание!*
> *Драйвер считывателя смарт-карт 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.*

6. Эксплуатация, хранение и транспортировка смарт-карты

Следование следующим правилам эксплуатации и хранения обеспечат длительный срок службы смарт-карты «iBank 2 Key» и сохранность конфиденциальной информации пользователя.

. •Необходимо оберегать смарт-карту от механических повреждений, от воздействия высоких и низких температур, влаги и агрессивных средств.
. •Недопустимо воздействие на смарт-карту сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества.
. •Не извлекайте смарт-карту из считывателя во время записи и считывания.
. •В случае обнаружения неисправности или неправильного функционирования смарт-карты обратитесь в Банк.
. •Храните смарт-карту так же, как денежные средства, в местах, недоступных посторонним лицам.
. •Предпринимайте все меры для предотвращения утраты смарт-карты или ее неправомерного использования.

Важно!
Не передавайте смарт-карту третьим лицам! Не сообщайте третьим лицам PIN-код доступа к секретному ключу ЭЦП! В случае утери (хищения) смарт-карты немедленно свяжитесь с банком.

Перевозка упакованных смарт-карт 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.

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

7. Гарантийные обязательства

Гарантийный срок эксплуатации смарт-карты «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