

**Паспорт на USB-токены
и смарт-карты «iBank 2 Key»**

Содержание

1. Общие сведения	3
2. Назначение и область применения	4
3. Основные характеристики, внешний вид, размеры	5
4. Требования к эксплуатации	8
5. Подготовка к работе	9
6. Гарантийные обязательства	10
7. Адрес поставщика	11

1. Общие сведения

Паспорт содержит сведения о USB-токенах и смарт-картах «iBank 2 Key».

«iBank 2 Key» является персональным средством аутентификации и предназначен для генерации ключей электронной подписи (ЭП) и их защищенного хранения.

В «iBank 2 Key» реализованы следующие криптографические функции:

- аппаратный криптографически стойкий генератор случайных чисел;
- генерация ключа ЭП;
- формирование и проверка ЭП 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

2. Назначение и область применения

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

Ключ ЭП генерируется самим «iBank 2 Key», хранится в защищенной памяти «iBank 2 Key» и никогда, никем и ни при каких условиях не может быть считан из «iBank 2 Key».

Формирование ЭП в соответствии с ГОСТ Р34.10-2001 происходит непосредственно внутри токена: на вход «iBank 2 Key» принимает электронный документ, на выходе выдает ЭП под данным документом. При этом время формирования ЭП менее 0,5 сек.

В «iBank 2 Key» имеется защищенная область памяти, позволяющая хранить до 64-х ключей ЭП:

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

Поддержка «iBank 2 Key» встроена в клиентские модули системы электронного банкинга «iBank 2»:

- Internet-Банкинг
- РС-Банкинг
- Центр финансового контроля (ЦФК)
- Корпоративный автоклиент

Возможна одновременная работа сразу с несколькими подключенными к компьютеру «iBank 2 Key» (актуально при работе с ЦФК).

Доступ ко всем криптографическим функциям «iBank 2 Key» предоставляется только после ввода пользователем корректного PIN-кода. Для каждого ключа ЭП, хранящегося в памяти «iBank 2 Key», задается свой пароль.

3. Основные характеристики, внешний вид, размеры

«iBank 2 Key» имеет два типа исполнения:

- USB-токен
- смарт-карта

USB-токен «iBank 2 Key» — это аппаратное USB-устройство в компактном пластиковом корпусе, состоящее из USB-картридера и защищенного карточного микроконтроллера ST19NR66 или ST23YL18 производства компании STMicroelectronics

Тип микроконтроллера зависит от модели исполнения корпуса «iBank 2 Key» (см. [Таблица 1](#)).

Микроконтроллеры сертифицированы на соответствие стандарту ISO/IEC 15408 (common criteria) с уровнем доверия EAL5+.

В микроконтроллере при производстве масочным методом «прошита» карточная операционная система «Магистра» (разработчик ООО «Смарт-Парк»). В составе операционной системы содержится СКЗИ, сертифицированное ФСБ РФ по классу КС2.

USB-токен подключается к компьютеру через порт USB

Смарт-карта «iBank 2 Key» представляет собой карточный криптографический микроконтроллер, имплантированный на пластиковую карту и полностью соответствующий спецификациям ISO 7816

Функционально смарт-карта полностью аналогична USB-токену за исключением электрического интерфейса.

Смарт-карта подключается к компьютеру через CCID-совместимый картридер (см. [рис. 1](#)) — внешнее USB-устройство для осуществления операций чтения/записи с/на смарт-карту. Также может использоваться настольная клавиатура с интегрированным считывателем смарт-карт. На многих моделях ноутбуков встроенный считыватель уже присутствует в базовой конфигурации.

Информация о разных типах исполнения корпуса и сертификатах, выданных на содержащееся в «iBank 2 Key» СКЗИ представлена в таблице ниже.

Работа «iBank 2 Key» поддерживается в следующих ОС

USB-токены «iBank 2 Key» предназначены для работы на следующих платформах:

- исполнение «А», исполнение «М», исполнение «В2», смарт-карты (ST19NR66): Windows XP Professional/ XP Home/ Server 2000/ Server 2003/ Professional 2000/ Vista; Mac OS X 10.5.4 или старше, Linux 2.6.x
- исполнение «М2», исполнение «В», смарт-карты (ST23YL18): Windows XP/ 2000/ 2003/ Vista/ 7; Mac OS X 10.4.8 или старше, Linux 2.6.x

Считыватель смарт-карт соответствует стандартам: ISO 7816-1/2/3, EMV, Microsoft PC/SC и совместим с большинством компьютерных платформ. Он является CCID-совместимым устройством и не требует для своей работы установки драйверов в операционных системах Windows Vista, Linux, MacOS.

В других операционных системах семейства Windows требуется установить стандартный драйвер CCID-устройства от Microsoft или скопировать драйвер устройства с сайта банка.





							
Исполнение корпуса	смарт-карта		A	M	M2	B	B2
Криптографический микроконтроллер, производитель STMicroelectronics	ST19NR66	ST23YL18	ST19NR66	ST19NR66	ST23YL18	ST23YL18	ST19NR66
USB-интерфейс подключения	Через CCID-совместимый картридер		CCID	PC/SC	PC/SC	ICCD, CCID	
СКЗИ, сертификат ФСБ РФ на СКЗИ							
Криптомодуль-С	СФ/114-1009 с 14.05.2007 по 09.03.2010	+		+	+		
	СФ/114-1436 с 09.03.2010 по 30.06.2010	+		+	+		
	СФ/114-1510 с 01.07.2010 по 01.05.2013	+		+	+		
Криптомодуль С23	СФ/114-1511 с 08.07.2010 по 01.05.2013		+			+	+
	СФ/114-2176 с 20.06.2013 по 31.12.2013		+			+	+
	СФ/114-2312 с 31.12.2013 по 06.11.2014		+			+	+
ФОРОС. Исполнение №1	СФ/124-2151 с 03.06.2013 по 01.02.2016	+		+	+		+

Таблица 1. Основные характеристики «iBank 2 Key»



Рис. 1. Картридер EZ100PU

Физические характеристики USB-токена «iBank 2 Key» для исполнений корпуса «А», «В» и «М» представлены в таблице ниже.




	Исполнение «А»	Исполнение «В»	Исполнение «М», «М2»
			
Интерфейс:	USB 1.1/ USB 2.0 Type A		
Габаритные размеры (мм)	57×16×8	53×16×9	65×20×10
Вес (грамм)	6	5,3	13
Энергопотребление (мА)	менее 50 мА		
Рабочая температура окружающей среды (°C)	+10... +70		
Температура хранения и транспортировки (°C)	-30... +85		

Таблица 2. Физические характеристики USB-токена «iBank 2 Key»

Физические характеристики смарт-карты «iBank 2 Key» представлены в таблице ниже.


	
Интерфейс:	ISO 7816-3 T=1 и T=0 протокол
Габаритные размеры (мм)	86×54×0.8
Вес (грамм)	4
Рабочая температура окружающей среды (°C)	+10... +70
Температура хранения и транспортировки (°C)	-30... +85

Таблица 3. Физические характеристики смарт-карты «iBank 2 Key»

4. Требования к эксплуатации

USB-токены, смарт-карты и картридеры являются чувствительными электронными устройствами. При их хранении и эксплуатации пользователю необходимо соблюдать ряд правил и требований, при нарушении которых указанные устройства могут выйти из строя.

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

- Необходимо оберегать устройство от сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т. п.).
- Необходимо оберегать устройство от воздействия высоких и низких температур.

При резкой смене температур (вносе охлажденного устройства с мороза в теплое помещение) не рекомендуется использовать устройство в течение 3 часов во избежание повреждения устройства из-за сконденсированной на его электронной схеме влаги.

- Необходимо оберегать устройство от попадания на него 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 к компьютеру не прилагайте излишних усилий для избежания механических повреждений разъема устройства.
- Не извлекайте устройство во время записи и считывания.
- В нерабочее время устройство необходимо всегда держать закрытым во избежание попадания на разъем пыли, грязи, влаги и т. п.

При засорении разъема 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 работоспособности и гарантии.
- В случае неисправности или неправильного функционирования «iBank 2 Key» необходимо обратиться в банк.

Перевозка упакованных «iBank 2 Key» 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.

Хранение «iBank 2 Key» осуществляется в закрытом помещении комнатной температуры при отсутствии в окружающем воздухе кислотных, щелочных и других агрессивных примесей.

Важно!

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

5. Подготовка к работе

«iBank 2 Key» проходит предпродажную подготовку, гарантирующую правильную работоспособность устройства в системе электронного банкинга «iBank 2».

Перед началом работы с «iBank 2 Key» пользователю необходимо предварительно установить драйвер устройства.

Важно!

- Драйвер для «iBank 2 Key» устанавливается до подключения устройства.
- Во время установки драйвера все приложения должны быть закрыты во избежание ошибки разделения файлов.
- Для установки драйвера пользователю необходимы права администратора системы. Во избежание ошибок при установке драйвера не производите установку через Remote Desktop Protocol

Дистрибутив драйвера, соответствующий Вашей операционной системе, можно скачать с сайта <https://ibank2.ru>

6. Гарантийные обязательства

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

7. Адрес поставщика

Поставщик: ООО «БИФИТ Дата Секьюрители»
Адрес: ул. Нижняя Первомайская, д. 46, г. Москва, Россия, 105203
Тел.: +7 (495) 532-15-02, (499) 705-01-01
E-mail: token@bifit.com, info@bifit.com