

«iBank 2 Key»™ электронный ключ



Электронный ключ «iBank 2 Key» - это аппаратно-программная реализация украинских криптографических стандартов в виде миниатюрного USB-брелока.

Основным назначением «iBank 2 Key» является генерация и защищенное **неизвлекаемое** хранение секретных ключей ЭЦП, а также формирование электронно-цифровой подписи непосредственно внутри устройства.

«iBank 2 Key» имеет широкий спектр применения

«iBank 2 Key» может выступать как единое устройство для аутентификации в компьютерных системах, для получения доступа к ресурсам корпоративной сети, защищенного хранения пользовательских данных (таких как ключи, пароли, сертификаты), для обеспечения конфиденциальности и целостности данных при передаче их по сети и т.д.

«iBank 2 Key» разработан для широкого применения в системах электронного банкинга и в полной мере учитывает особенности этой сферы.

Поддержка промышленных стандартов PC/SC, PKCS#11, MS CryptoAPI, X.509 позволяет без труда встраивать «iBank 2 Key» в уже существующие системы безопасности.

«iBank 2 Key» удобен и практичен

«iBank 2 Key» выполнен в форм-факторе USB-брелока, он легкий и прочный. «iBank 2 Key» поддерживает работу для всего спектра популярных ОС, и не требует установки дополнительного программного обеспечения. При работе с «iBank 2 Key» пользователю не требуется наличие дополнительных сертифицированных криптографических библиотек, все необходимые криптографические операции уже реализованы в «iBank 2 Key».

«iBank 2 Key» гарантирует неизвлекаемость секретных ключей ЭЦП

«iBank 2 Key» генерирует секретные ключи ЭЦП внутри себя и хранит их в защищенной памяти. Все операции с секретными ключами ЭЦП осуществляются непосредственно внутри устройства. Секретные ключи ЭЦП не могут быть считаны из устройства никем, включая разработчика и производителя.

«iBank 2 Key» позволяет генерировать и хранить до 64-х секретных ключей ЭЦП

Для большинства пользователей, использующих несколько ключей ЭЦП неудобно, и более того, невыгодно носить связку USB-токенов для всех своих ключей ЭЦП. Вместо этого клиент может использовать всего одно устройство для хранения нескольких ключей различного назначения.

«iBank 2 Key» имеет рекордную скорость формирования ЭЦП

При разработке «iBank 2 Key» большое внимание было уделено скорости выполнения криптографических операций. Время формирования ЭЦП - 54 мс (для 257 битных ключей), а скорость шифрования, выработки имитовставки и вычисления хеш-вектора - 1 Мбит/с.

«iBank 2 Key» поддерживается в ОС: Windows, Linux, MacOS

Для работы «iBank 2 Key» в Windows (начиная с Windows Vista), Linux и MacOS не требуется установки дополнительного программного обеспечения. Для более ранних версий Windows необходимо установить стандартный драйвер для работы с CCID классом USB устройств.

«iBank 2 Key» может взаимодействовать с произвольной ОС, которая поддерживает работу с CCID классом USB устройств и оборудована USB версии 1.1 или выше.

«iBank 2 Key» имеет экспертное заключение № 05/1-1147 ГСССЗИ Украины

Согласно экспертному заключению, криптографические алгоритмы, реализованные в электронном ключе «iBank 2 Key», соответствуют требованиям стандартов ДСТУ ГОСТ 28147:2009, ДСТУ 4145-2002, ДСТУ ISO/IEC 15946-3:2006, ГОСТ 34.311-95.

«iBank 2 Key» -

разработка компании «БИФИТ»

Украинская компания «БИФИТ» основана в 2002 году. Основное направление деятельности компании – разработка, внедрение и сопровождение программных решений для электронного банкинга – системы «iBank 2 UA» и средств криптографической защиты информации. В настоящее время система «iBank 2 UA» внедрена и успешно эксплуатируется во многих украинских и российских банках.

Для осуществления деятельности, связанной с разработкой, производством, распространением и техническим обслуживанием средств криптографической защиты информации, украинская компания «БИФИТ» имеет Лицензию ГСССЗИ Украины.

«iBank 2 Key»™ электронный ключ

Основные характеристики

- Габаритные размеры: 53x16x8 мм
- Масса: 6,1 г
- Интерфейс: USB тип A (USB 1.1/USB 2.0)
- Потребляемая мощность: 300 мВт
- Корпус: цельнолитой, из высокопрочного пластика
- Поддерживаемые ОС: Windows, Linux, MacOS
- Не требует установки дополнительного ПО
- Поддерживаемые стандарты:
 - ✓ ISO/IEC 7816
 - ✓ PC/SC
 - ✓ Microsoft CryptoAPI
 - ✓ PKCS#11

Поддерживаемые криптографические алгоритмы

- Шифрование по ДСТУ ГОСТ 28147:2009
- Вычисление имитовставки по ДСТУ ГОСТ 28147:2009
- Вычисление хеш-функции по ГОСТ 34.311-95
- Генерация псевдослучайных последовательностей по ДСТУ 4145-2002
- Генерация ключей по ДСТУ 4145-2002
- Формирование/проверка ЭЦП по ДСТУ 4145-2002
- Выработка общего секрета по ДСТУ ISO/IEC 15946-3

Операционная система

- позволяет сохранять произвольные данные во внутренней памяти и обеспечивает их защиту от несанкционированного доступа
- предоставляет 48 Кб памяти общего назначения с возможностью разграничения доступа
- позволяет генерировать и сохранять вплоть до 64-х секретных ключей ЭЦП во внутренней защищенной памяти
- имеет высокую скорость формирования ЭЦП
- позволяет использовать произвольные криптографические параметры
- поддерживает работу устройства одновременно в нескольких приложениях
- имеет механизм проверки подлинности устройства
- имеет контроль целостности и работоспособности

Основные характеристики микроконтроллера

- Ядро: ARM 32-bit Cortex-M3 CPU
- Тактовая частота микроконтроллера: 72 MHz
- Система команд, режим адресации: ARMv7-M
- Объем Flash: 128 Кб
- Объем оперативной памяти: 20 Кб

Дополнительные особенности

- Аппаратный двухканальный генератор случайных чисел
- Световая индикация



Производительность криптографических алгоритмов

Алгоритм	Режим	Значение	Метрика
ДСТУ ГОСТ 28147	Режим простой замены	119	КБ/с
ДСТУ ГОСТ 28147	Режим гаммирования	119	КБ/с
ДСТУ ГОСТ 28147	Режим гаммирования с обратной связью	119	КБ/с
ДСТУ ГОСТ 28147	Вычисление имитовставки	119	КБ/с
ГОСТ 34.311	Вычисление хэш-вектора	112	КБ/с
ДСТУ 4145	Генератор псевдослучайных чисел	5	КБ/с
ДСТУ 4145	Генерация ключевой пары (257 бит)	57	мс
ДСТУ 4145	Формирование ЭЦП (257 бит)	54	мс
ДСТУ 4145	Проверка ЭЦП (257 бит)	174	мс
ДСТУ ISO/IEC 15946-3	Выработка общего секрета (без кофактора)	168	мс
ДСТУ ISO/IEC 15946-3	Выработка общего секрета (с кофактором)	191	мс