СКЗИ «MS_KEY K» Исполнение 5.1.1.

СПЕЦИФИКАЦИЯ

1. Общее описание СКЗИ "MS_KEY K" Исполнение 5.1.1.

СКЗИ «MS_KEY K» Исп. 5.1.1. (далее СКЗИ «MS_KEY K») – высокотехнологичный продукт, сочетающий в себе удобства смарт-ключа и защищенность средства криптографической защиты информации, построенного на безопасной технологии интеллектуальных карт.

СКЗИ «MS_KEY K» строится базе смарт-карточного микроконтроллера NXP P5CC081 с операционной системой «Вигрид» (VIGRID – Verification Interoperability GRID) версии 1.0, которая является продуктом российского производства и сочетает в себе весь потенциал российских разработок в данной области.

В основу принципов функционирования карты и операционной системы положены стандарты серии ISO 7816-4,8,9 (ГОСТ Р ИСО/МЭК 7816-4,8,9).

2. Функции СКЗИ «MS_KEY K»

- генерация случайных последовательностей произвольной длины с помощью программного датчика случайных чисел (ПДСЧ);
- аутентификация пользователей СКЗИ;
- криптографическая аутентификация между картой и терминальной системой;
- вычисление значения хеш-функции в соответствии с ГОСТ Р 34.11-94;
- шифрование (расшифрование) данных, поступающих из Терминальной системы по алгоритму ГОСТ 28147-89 в режимах гаммирования и гаммирования с обратной связью;
- выработка ключа парной связи на основе закрытого/открытого ключа шифрования по схеме Диффи-Хеллмана (в соответствии с RFC4357);
- формирование имитовставки для данных, поступающих из терминальной системы в соответствии с ГОСТ 28147-89/проверка имитовставки;
- выработка пар закрытый/открытый ключи ЭП, в соответствии с ГОСТ Р 34.10-2001;
- выработка симметричных (сессионных) ключей шифрования;
- загрузка пары закрытый/открытый ключ ЭП и симметричных ключей ГОСТ 28147-89 внутрь микроконтроллера в его энергонезависимую память;
- хранение закрытых ключей ЭП и симметричных ключей для вычисления имитовставки в соответствии с ГОСТ 28147-89 внутри микроконтроллера в его энергонезависимой памяти в открытом виде без возможности экспорта;
- вычисление/верификация электронной подписи (ЭП) в соответствии с ГОСТ Р 34.10-2001;
- установление криптографически-защищенного соединения между СКЗИ и терминальной системой.

3. Особенности СКЗИ «MS_KEY K»

СКЗИ «MS_KEY K» соответствует закону №63-ФЗ «Об электронной подписи», может применяться для вычисления квалифицированной электронной подписи.

СКЗИ «MS_KEY K» соответствует закону №152-ФЗ «О персональных данных», и может применяться в качестве элемента защиты ИСПДн согласно общей (или частной) модели угроз и технического задания на подсистему защиты персональных данных в ИСПДн.

СКЗИ «MS_KEY K» выпускается в нескольких исполнениях, включающих портативное USB-устройство и смарт-карту (ISO7816).

4. Технические характеристики СКЗИ «MS_KEY K»

4.1 Криптопротоколы и российские криптоалгоритмы

№	Компонент	Криптоалгоритмы и криптопротоколы
1	Смарт-ключ	ГОСТ Р 34.10-2001. Аппаратная реализация вычисления подписи и проверки подписи. Сертификат №СФ/124-2211, для исполнения 5.1.1. ГОСТ Р 34.11-94. Аппаратная реализация вычисления хеш-функции. Сертификат №СФ/124-2211, для исполнения 5.1.1. ГОСТ 28147-89. Аппаратная реализация шифрования и вычисления имитовставки. Сертификат №СФ/124-2211, для исполнения 5.1.1. Выработка ключевой информации, в том числе ключевых пар по ГОСТ Р 34.10-2001, ключей шифрования и имитовставки по ГОСТ 28147-89. Сертификат №СФ/124-2211, для исполнения 5.1.1. Выработка ключевой информации по алгоритму Диффи-Хеллмана в соответствии с RFC4357 (VKO GOST). Сертификат №СФ/124-2211, для исполнения 5.1.1. Выработка случайных последовательностей произвольной длины. Сертификат №СФ/124-2211, для исполнения 5.1.1. Криптографическая аутентификация. Сертификат №СФ/124-2211, для исполнения 5.1.1.

4.2 Дополнительные сервисы

Доступны следующие зарубежные криптографические алгоритмы:

- DES/3DES (блочное шифрование);
- AES (блочное шифрование);
- RSA (вычисление/проверка подписи);
- SHA-1 (хеш-функция).

4.3 Спецификация аппаратной базы для исполнения 5.1.1.

Параметр	**Описание**
Интерфейс	Спецификация CCID более совершенная, чем классический PC/SC. Характеризуется большей универсальностью, скоростью обмена с ПК и упрощенной поддержкой в большинстве современных операционных систем.
Питание	USB-порт
Интерфейс, тип разъема	USB 1.1/USB2.0/USB3.0 Type A
Допустимый уровень влажности	от 0 до 100% без конденсата
Диапазон приемлемой температуры окружающей среды (во время работы)	от 0 до 70 градусов С
Диапазон приемлемой температуры окружающей среды (при хранении)	от -20 до 85 градусов С

4.4 Характеристики микроконтроллера

№	**Параметр**	**Значение**
2	Сертификат микроконтроллера	ISO15408 Common Criteria по уровню EAL5+
3	Объем масочного ПЗУ	264 килобайта
4	Объем ОЗУ	7,5 килобайта
5	Объем EEPROM	80 килобайт
6	Напряжение питания контактного интерфейса	от 1,62 В до 5,5 В
7	Рабочее энергопотребление	1.0 до 12.5 ма
8	Энергопотребление в режиме энергосбережения	40 - 80 мка
9	Допустимый уровень напряжения статического электричества	4000 В
10	Гарантируемое время хранения данных в энергонезависимой памяти	25 лет
11	Гарантируемый технический ресурс энергонезависимой памяти	500 000 циклов стирания/записи
12	Тактовая частота внутреннего генератора процессора	до 62 MHz
13	Контактный интерфейс	в соответствии с ISO7816 (T=0)
14	внешний CLOCK	до 10 МГц
15	Генератор случайных чисел	• Штатный: аттестован по FIPS 140-2 и AIS31; • Для СКЗИ «MS_KEY K»: усиленный, ДСЧ СКЗИ может вырабатывать ключевую информацию.

5. Приложение 1. Сертификат ФСБ России на СКЗИ «MS_KEY K»

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер ***СФ/124-2673*** от "***30***" ***июля*** 201***5*** г.

Действителен до "***01***" ***августа*** 201***8*** г.

Выдан обществу с ограниченной ответственностью «МультиСофт Системз».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) **«MS_KEY K»** (варианты исполнения 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.2.4) в комплектации согласно формуляру 46448059.4012402.002.30.01.1

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1 (для вариантов исполнения 5.1.2, 5.2.2), класса КС2 (для вариантов исполнения 5.1.1, 5.1.3, 5.2.1, 5.2.3, 5.2.4). Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для вариантов исполнения 5.1.2, 5.2.2), класса КС2 (для вариантов исполнения 5.1.1, 5.1.3, 5.2.1, 5.2.3, 5.2.4), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование данных, содержащихся в областях оперативной памяти СКЗИ, вычисление имитовставки для данных, содержащихся в областях оперативной памяти СКЗИ, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти СКЗИ, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «Центр сертификационных исследований»

сертификационных испытаний образцов продукции №№ 650Д1-001001, 650Д2-001001.

Безопасность информации обеспечивается при использовании СКЗИ, изготовленного в соответствии с техническими условиями ТУ-4012-002-46448059-2013, и выполнении требований эксплуатационной документации согласно формуляру 46448059.4012402.002.30.01.1.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **А.М.Ивашко**

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.Н.Ковалев