Спецификация СКЗИ «MS_KEY K». Исполнение 1.1.

- Исполнение 1.1 выпускается в форм-факторе USB-устройства, строится на чипе ST19NR66 производства STMicroelectronics.
- СКЗИ «MS_KEY K» Исполнения 1.1 имеет сертификат ФСБ на соответствие ГОСТ Р 34.10-2001 (электронная подпись, алгоритм на основе эллиптических кривых), ГОСТ Р 34.11-94 (хеш-функция), ГОСТ28147-89 (симметричный криптографический алгоритм) и требованиям к СКЗИ класса КС2. СКЗИ «MS_KEY K» Исполнения 1.1 может использоваться для генерации и управления ключевой информацией, формирования и проверки электронной подписи для информации, не содержащей государственную тайну (сертификат ФСБ СФ/124-2391 от 01 июля 2014 года). СКЗИ «MS_KEY K» Исполнение 1.1 включает сертифицированный ДСЧ.
- Объем электрически-перезаписываемой памяти (EEPROM) составляет 64 килобайта.
- Помимо указанных криптоалгоритмов устройство содержит дополнительные сервисы.
- Гарантийный срок составляет 1 (один) год.

Особенности СКЗИ «MS_KEY K» Исполнение 1.1:

- сертификат ФСБ (СФ/124-1695) подтверждает соответствие СКЗИ требованиям к СКЗИ класса КС2, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94; ГОСТ 28147-89;
- применяется технология неизвлекаемого ключа электронной подписи;
- время вычисления электронной подписи по ГОСТ Р 34.10-2001 составляет около 0,5 секунды;
- СКЗИ «MS_KEY K» Исполнение 1.1 содержит сертифицированный ДСЧ, что позволяет ему генерировать и управлять ключевой информацией;
- готово для работы в качестве ключевого носителя в системах, использующих Крипто-Про CSP 3.6.

Технические характеристики элементной базы СКЗИ «MS_KEY K» Исполнение 1.1

Микроконтроллер

- 8-ми разрядное процессорное ядро.
- Внутренний тактовый генератор ~20MHz.
- RAM – 6 Кбайт.
- ROM – 224 Кбайт.
- EEPROM – 66 Кбайт.
- 1088-битовый криптографический сопроцессор для криптографии с открытым ключом.
- Аппаратные средства защиты от динамического исследования методами SPA, DPA, DFA.
- Аппаратные средства защиты от статического исследования.
- Контактный интерфейс: поддержка протокола PPS.
- Микроконтроллер сертифицирован на соответствие стандарту ISO/IEC 15408. (Common criteria) с уровнем доверия EAL 5+.

Российские криптоалгоритмы

- симметричный криптоалгоритм в соответствии с ГОСТ. 28147-89. Таблицы подстановок CryptoPro A, CryptoPro B, CryptoPro C, CryptoPro D(по RFC4357);
- криптоалгоритм электронной подписи в соответствии с ГОСТ Р34.10-2001. Блоки параметров криптоалгоритма CryptoPro A, CryptoPro B, CryptoPro C (по RFC4357);
- хеш-алгоритм в соответствии с ГОСТ Р34.11-94. Таблица подстановок CryptoPro H (по RFC4357).

Дополнительные сервисы

- DES / 3DES;
- RSA;
- хеш-функция SHA-1.

Набор команд ОС в соответствии с ISO 7816:

- ISO 7816-4 (работа с данными),
- ISO 7816-8 (криптографические команды),
- ISO 7816-9 (команды управления жизненным циклом карты и файлов).

Спецификация аппаратной базы

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
Гарантируемый технический ресурс энергонезависимой памяти	500 000 циклов стирания/записи
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
Вес	12 гр.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер ***СФ/124-2391*** от "***01***" ***июля*** 201***4*** г.

Действителен до "***01***" ***июня*** 201***6*** г.

Выдан обществу с ограниченной ответственностью «МультиСофт Системз».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) **«MS_KEY_K»** (варианты исполнения 1.1, 2.1, 3.1, 4.1) в комплектации согласно формуляру 46448059.4012402.001.30.01.1

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС2 и может использоваться для криптографической защиты (создание и управление ключевой информацией, вычисление имитовставки для данных, содержащихся в областях оперативной памяти СКЗИ, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти СКЗИ, создание и проверка электронной подписи для данных, содержащихся в областях оперативной памяти СКЗИ) информации, не содержащей сведений, составляющих государственную тайну.

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

сертификационных испытаний образцов продукции №№ 650А-001001, 650Б-001001, 650В-001001, 650Г-001001.

Безопасность информации обеспечивается при использовании СКЗИ, изготовленного в соответствии с техническими условиями ТУ-4012-011-46448059-2010 и выполнении требований эксплуатационной документации формуляра 46448059.4012402.001.30.01.1

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