Новый качественный уровень отечественных СКЗИ как результат импортозамещения в сфере информационной безопасности и защиты данных

Никита Кожемякин, директор по развитию бизнеса ISBC

Виталий Благодатов, инженер ОАО «НИИМЭ и Микрон»

Методы реализации существующих аппаратных СКЗИ в России

в форм-факторе USB-токенов и смарт-карт

- Сертифицированный апплет для Java-карты (Athena, Gemalto и др.)
- Использование микроконтроллеров общего назначения (Atmel, NXP и др.)
- Решение на базе специализированного смарт карточного чипа зарубежного производства (NXP, ST Microelectronics и др.)
- Решение на базе специализированного смарт карточного чипа отечественного производства (Микрон)

ESMART®

mikron

ESMART Token ГОСТ — СКЗИ с аппаратной реализацией алгоритмов ГОСТ на базе отечественного микроконтроллера MIK51

Назначения изделия ESMART Token ГОСТ

- средство электронной подписи (ГОСТ Р 34.10, ГОСТ Р 34.11);
- средство многофакторной аутентификации (в том числе, биометрической).

Сферы применения изделия

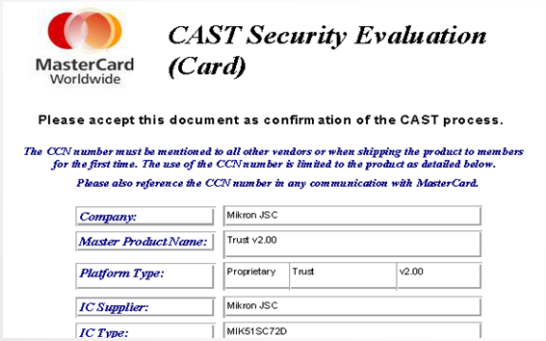
- юридически значимая электронная подпись в системах электронного документооборота;
- аутентификация в информационных системах;
- защита персональных данных;

ESMART Token ГОСТ

Совместный продукт компаний ОАО «НИИМЭ и завод Микрон» и ISBC Group (Россия, Зеленоград):

Роль ОАО «НИИМЭ и завод Микрон»

- разработка и производство микросхемы MIK51;
- разработка ОС для MIK51;
- сертификация устройства ФСБ, EMVCo, MasterCard.



MasterCard Worldwide

CAST Security Evaluation (Card)

Please accept this document as confirmation of the CAST process.

The CCN number must be mentioned to all other vendors or when shipping the product to members for the first time. The use of the CCN number is limited to the product as detailed below.

Please also reference the CCN number in any communication with MasterCard.

Company:	Mikron JSC		
Master Product Name:	Trust v2.00		
Platform Type:	Proprietary	Trust	v2.00
IC Supplier:	Mikron JSC		
IC Type:	MIK51SC72D		

EMVCo

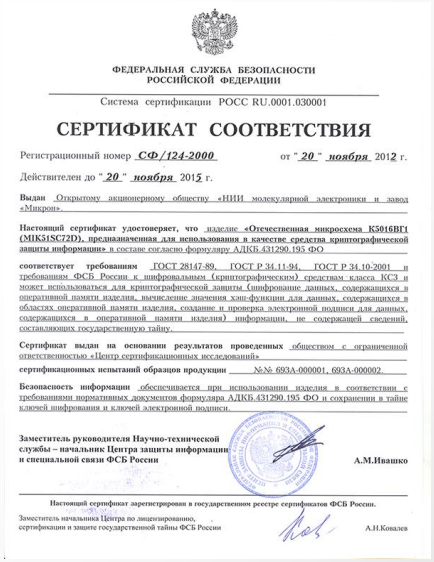
EMVCo Product Approval (IC)

Please accept this document as confirmation of the EMVCo Security Evaluation process

The ICCN number must be mentioned to all vendors or when shipping the product for the first time. The use of the ICCN number is limited to the product as detailed below.

Please also reference the ICCN number in any communication with EMVCo.

Company:	Mikron JSC
Master Component:	MIK51SC72D v 5.1



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-2000* от "*20*" *ноября* 2012 г.

Действителен до "*20*" *ноября* 2015 г.

Выдан Открытому акционерному обществу «НИИ молекулярной электроники и завод «Микрон».

Настоящий сертификат удостоверяет, что изделие **«Отечественная микросхема К5016ВГ1 (MIK51SC72D), предназначенная для использования в качестве средства криптографической защиты информации»** в составе согласно формуляру АДКБ.431290.195 ФО

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3 и может использоваться для криптографической защиты (шифрование данных, содержащихся в оперативной памяти изделия, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти изделия, создание и проверка электронной подписи для данных, содержащихся в оперативной памяти изделия) информации, не содержащей сведений, составляющих государственную тайну.

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

сертификационных испытаний образцов продукции №№ 693А-000001, 693А-000002

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями нормативных документов формуляра АДКБ.431290.195 ФО и сохранении в тайне ключей шифрования и ключей электронной подписи.

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

ESMART Token ГОСТ

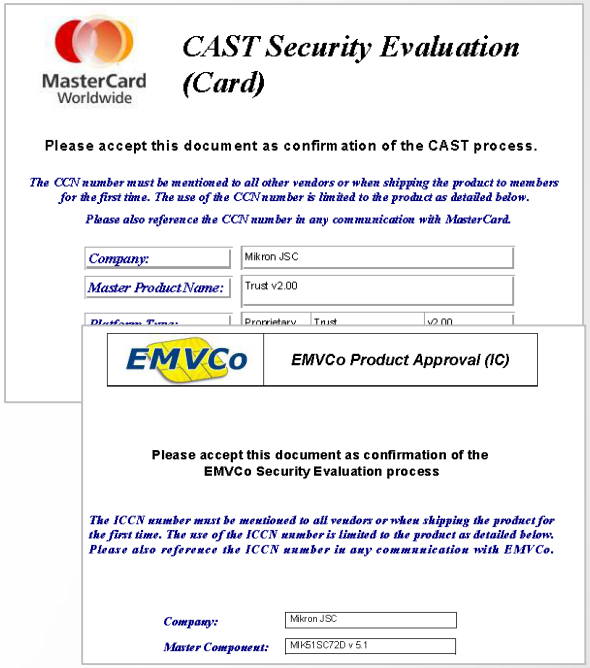
Совместный продукт компаний ОАО «НИИМЭ и завод Микрон» и ISBC Group (Россия, Зеленоград):

Роль Группы компаний ISBC

- разработка и производство изделий на основе микросхемы MIK51 в формате смарт-карты и SIM-карты (мощность производства – 2 млн. карт в месяц);
- разработка топологии печатных плат USB-токена и организация производства изделия в г. Зеленоград. Планируемая мощность – 200 тыс. токенов в месяц;
- разработка программного обеспечения для интеграции с СКЗИ и СЗИ (PKCS#11, minidriver, модули поддержки КриптоПро);
- продвижение и реализация изделия на территории России.

Опыт реализации проектов на базе микроконтроллера MIK51 с 2008 года

- Банковские карты
- Заграничный паспорт гражданина РФ
- Универсальная электронная карта
- ESMART Token ГОСТ


MasterCard Worldwide

CAST Security Evaluation (Card)

Please accept this document as confirmation of the CAST process.

The CCN number must be mentioned to all other vendors or when shipping the product to members for the first time. The use of the CCN number is limited to the product as detailed below.

Please also reference the CCN number in any communication with MasterCard.

Company: Mikron JSC

Master Product Name: Trust v2.00

EMVCo

EMVCo Product Approval (IC)

Please accept this document as confirmation of the EMVCo Security Evaluation process

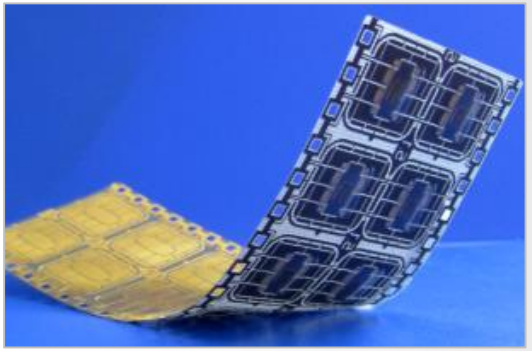
The ICCN number must be mentioned to all vendors or when shipping the product for the first time. The use of the ICCN number is limited to the product as detailed below. Please also reference the ICCN number in any communication with EMVCo.

Company: Mikron JSC

Master Component: MIK51SC72D v 5.1

Основные технические характеристики микроконтроллера MIK51

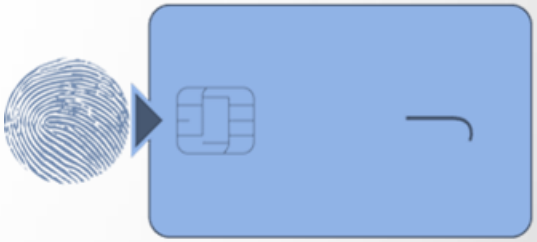
- Объем RAM: 8,75 Кбайт
- Объем EEPROM: 72 Кбайт
- Аппаратная поддержка симметричного шифрования: ГОСТ 28147-89, DES/3DES, AES-128/192/256
- Аппаратная поддержка алгоритмов вычисления / проверки ЭП: ГОСТ Р34.10-2001/2012, ECDSA-256, RSA до 2048 бит
- Аппаратная поддержка хеширования: ГОСТ Р34.11-94/2012, SHA-1, SHA-256
- Аппаратный модулярный сопроцессор 1024 бит



MIK51SC72D в форм-факторе чип-модульной ленты

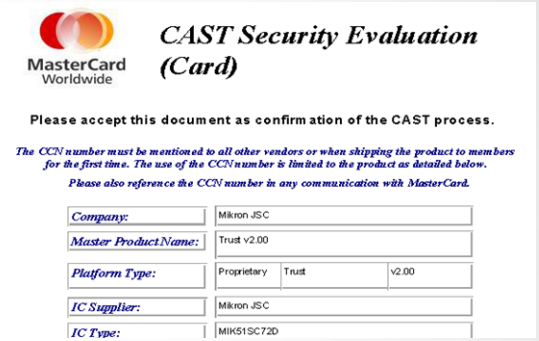
Операционная система TRUST

- Соответствие международному стандарту ISO 7816
- Файловая система: без ограничений на уровень вложенности файлов, все виды бинарных файлов и файлов записей
- Разграничение доступа: соответствует ISO 7816-4, правила разграничения доступа произвольной сложности
- Биометрическая верификация пользователя по отпечатку пальца, технология MatchOnCard. Поддержка Biometric Data Interchange Formats ISO 19794-2 fingerprint
- Виртуальная машина Java Card Classic 3.0.4 с расширениями JC API в т.ч. для поддержки российской криптографии
- Чип имеет сертификат MasterCard подтверждающий отсутствие влияния Java Card на интегрированные приложения
- Соответствие стандарту управления приложениями Global Platform 2.2 с поддержкой российского протокола SCP F2



Средства защиты от взлома MIK51

- Датчики инженерной защиты: вскрытия, напряжения, импульсной помехи, света
- Активный экран. Предотвращает анализ шин контактным методом и является источником шума для защиты от EMA
- Генератор шума на шине питания
- Маскирование данных на шинах
- Динамические Sbox для ГОСТ 28147-89
- Программные средства защиты от неразрушающих атак вида SPA, DPA, DFA
- Собственная лаборатория оценки качества мер защиты с применение различного инженерного оборудования FIB, Laser, DPA и др.



MasterCard Worldwide

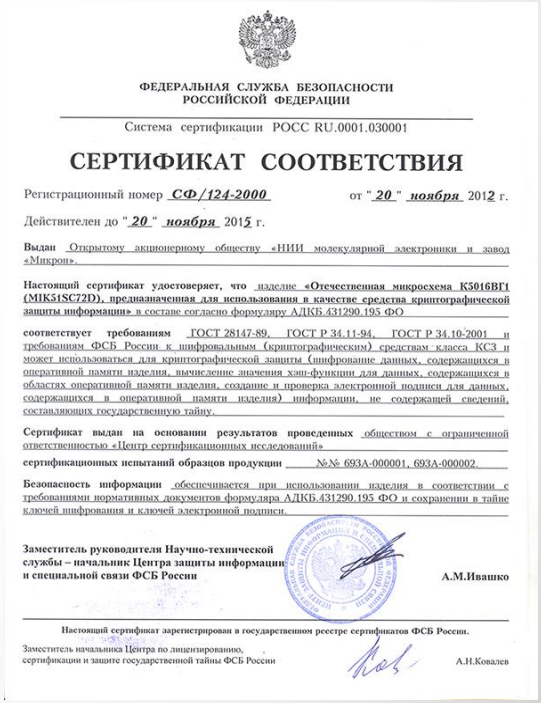
CAST Security Evaluation (Card)

Please accept this document as confirmation of the CAST process.

The CCN number must be mentioned to all other vendors or when shipping the product to members for the first time. The use of the CCN number is limited to the product as detailed below.

Please also reference the CCN number in any communication with MasterCard.

Company:	Mikron JSC		
Master Product Name:	Trust v2.00		
Platform Type:	Proprietary	Trust	v2.00
IC Supplier:	Mikron JSC		
IC Type:	MIK51SC72D		



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-2000* от "*20*" *ноября* 2012 г.

Действителен до "*20*" *ноября* 2015 г.

Выдан Открытому акционерному обществу «НИИ молекулярной электроники и завод «Микрон».

Настоящий сертификат удостоверяет, что изделие **«Отечественная микросхема К5016ВГ1 (MIK51SC72D), предназначенная для использования в качестве средства криптографической защиты информации»** в составе согласно формуляру АДКБ.431290.195 ФО

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3 и может использоваться для криптографической защиты (шифрование данных, содержащихся в оперативной памяти изделия, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти изделия, создание и проверка электронной подписи для данных, содержащихся в оперативной памяти изделия) информации, не содержащей сведений, составляющих государственную тайну.

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

сертификационных испытаний образцов продукции №№ 693А-000001, 693А-000002.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями нормативных документов формуляра АДКБ.431290.195 ФО и сохранении в тайне ключей шифрования и ключей электронной подписи.

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

Интеграция ESMART Token ГОСТ в решениях партнеров

Модуль поддержки для КриптоПро CSP 3.6 и выше

Поддержка в VipNet CSP 4.2

Бикрипт

Приглашаем к сотрудничеству!

Дополнительные возможности: поддержка биометрии

- *Аппаратная поддержка биометрической аутентификации Match-on-Card на уровне СКЗИ*

- *Поддержка как прокатных, так и оптических сканеров отпечатков для аутентификации через PKCS#11 и Minidriver*

Дополнительные возможности: использования в качестве банковской карты или электронного кошелька

- *Аппаратная поддержка спецификации MChip (MasterCard) и ПРО-100 позволяет использовать смарт-карту одновременно как средство ЭП/аутентификации так и как банковскую карту.*
- *Поддержка технологии* ESMART® Wallet для построения безопасных электронных кошельков (eWallet)

Основные преимущества и особенности ESMART Token ГОСТ

Российский продукт:

- *100% российская разработка и изготовление микросхемы СКЗИ на территории России*
- *100% российское производство конечного продукта в формате смарт-карты и USB-токена*
- *Российская разработка ПО для интеграции в продукты ИБ (PKCS#11 и др)*
- *Реализация ГОСТ алгоритмов в ОС смарт-чипа на уровне маски (в кремнии)*
- *Сертификация ФСБ по уровню КС3, EMVCo, MasterCard (CAST)*
- *72 КБ памяти EEPROM (весь объем доступен для пользовательских данных)*
- *Максимальная интеграция российской криптографии: Gost JC API, Global Platform SCP F2*
- *Протестировано в «Лаборатории по анализу защиты от инвазивных и неинвазивных атак (Микрон)»*

Спасибо за внимание!