ПРИМЕНЕНИЕ ОТЕЧЕСТВЕННОЙ МИКРОСХЕМЫ С RF-ИНТЕРФЕЙСОМ ДЛЯ ЗАЩИЩЕННЫХ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

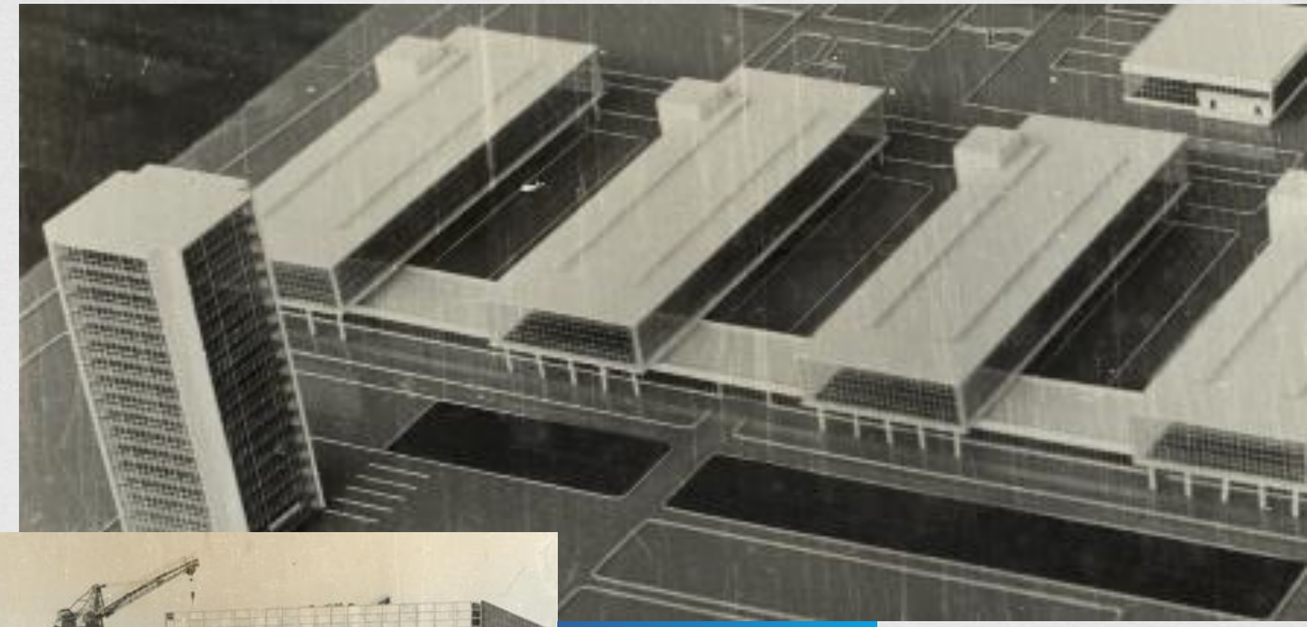
Предложения АО «НИИМЭ» и ПАО «Микрон» по современной идентификации граждан на базе интегральной микросхемы первого уровня MIK51AD144D

Конференция «РусКрипто-2020», Солнечногорский район, 19 марта 2020 г.

АО «НИИМЭ» И ПАО «МИКРОН»

Основаны в 1964 году как Научно-исследовательский институт молекулярной электроники и опытный завод «Микрон»

Расположены в Зеленограде (г. Москва)



Ведется строительство корпусов завода, 1964 год

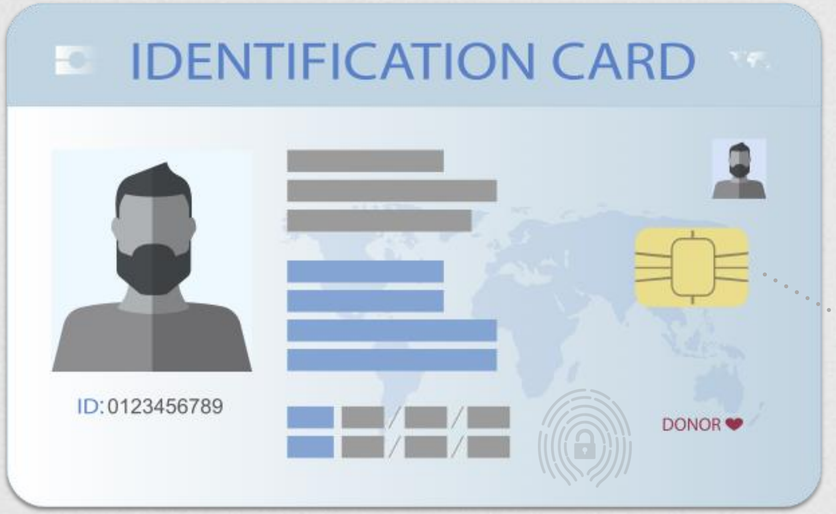
НИИМЭ и Микрон сегодня

Ведущие российские организации по разработке и производству интегральных микросхем и решений на их основе, технологических процессов микроэлектроники, встроенного программного обеспечения

СМАРТ-КАРТА С ЧИПОМ ДЛЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Электронный биометрический документ нового поколения

хранит персональные данные гражданина (включая биометрические данные) и уникальный идентификатор, использующийся для доступа к информационной системе и сервисам, применяемый на территории региона, страны или группы стран, содержит усиленную квалифицированную электронную подпись для осуществления юридически значимых действий

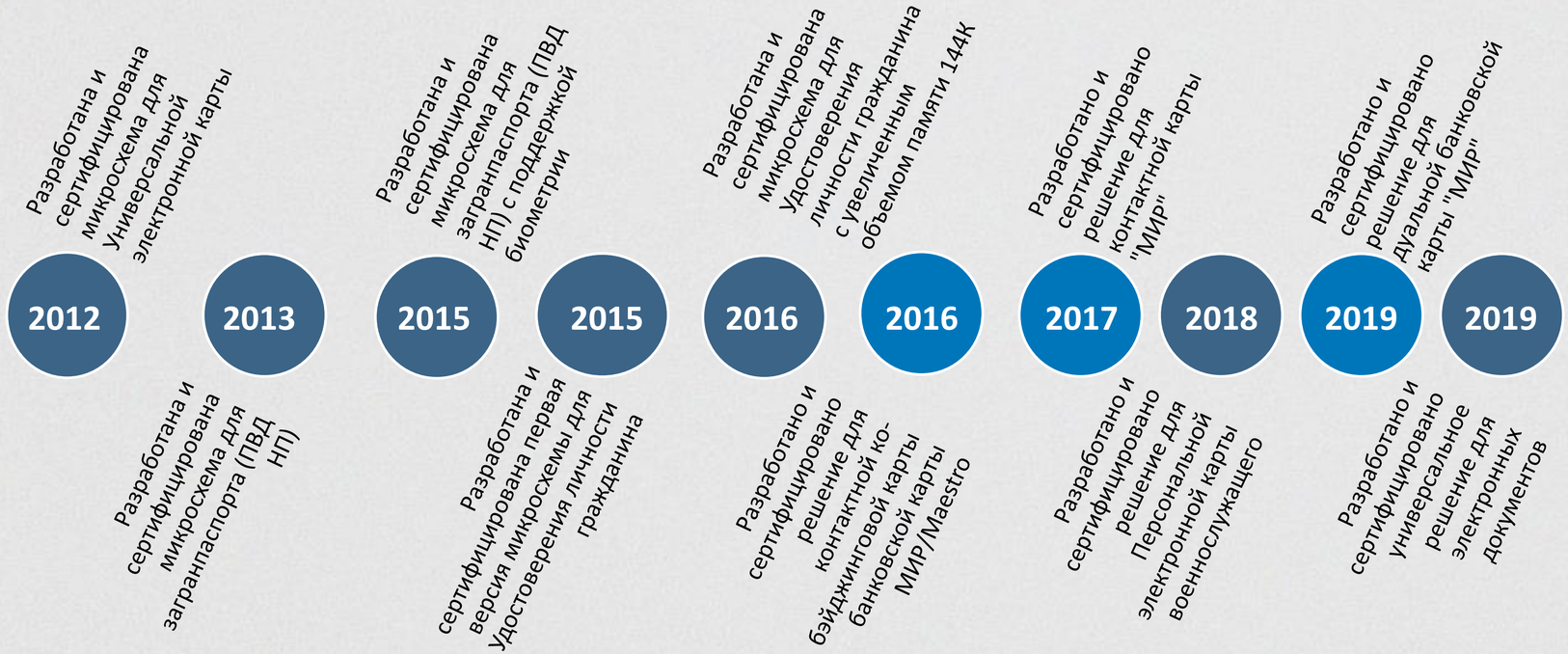


Графическое представление данных держателя с использованием технологий защищенной полиграфии (класс защиты не ниже В1)

Чип с персональными данными (включая биометрические) и уникальным идентификатором

Документ с персональными данными хранится на чипе - это международный стандарт для документов с высокой степенью защиты (в том числе криптографической), исключение возможности подделки

ИСТОРИЯ РАЗРАБОТКИ РЕШЕНИЙ ДЛЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ АО «НИИМЭ» И ПАО «МИКРОН»



Электронные документы
нового поколения

ОДНА КАРТА -
МНОГО ВОЗМОЖНОСТЕЙ

Медицинские услуги

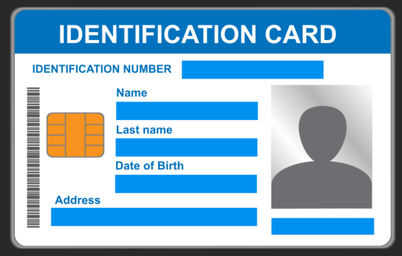
Идентификатор в системе медицинского страхования, доступ к медицинской карте

Карта туриста, карта гостя

Миграционный контроль и разграничение доступа

Платежная карта

Visa, MasterCard или другая платежная система



Карта студента

Идентификация студента и школьника, доступ в кампус, библиотеку и проч.

Электронная подпись

Электронный документооборот и осуществление юридически значимых действий

Пропуск на работу

Контроль доступа и авторизация

Социальные программы & программы лояльности

Идентификатор социального статуса и/или участника программы лояльности

Общественный транспорт

Транспортная карта для оплаты проезда

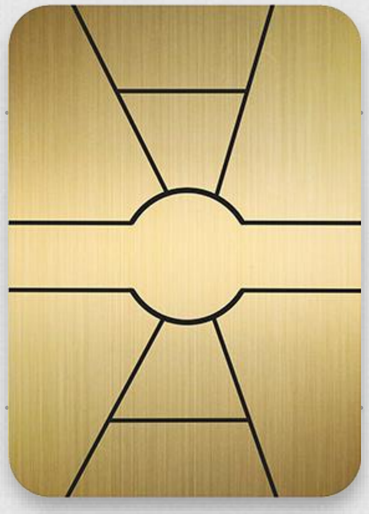
РЕШЕНИЕ НИИМЭ И МИКРОНА

АО «НИИМЭ» и ПАО «Микрон» разработано семейство микроконтроллеров MIK51, различающихся объемом памяти программ (от 160 до 384КБ) и энергонезависимой перезаписываемой памяти данных NVM (от 16 до 144КБ) под производство на ПАО «Микрон»

Микроконтроллер для биометрических документов

MIK51AD144D

Однокристальный микроконтроллер с дуальным (контактным и бесконтактным) интерфейсом и аппаратной поддержкой криптографии



01 Дуальный интерфейс: контактный ISO 7816, бесконтактный ISO 14443 A/B

02 Аппаратная поддержка и ускорение российской и международной криптографии (DES, 3DES, RSA, EC-DSA, ГОСТ 28147-89, ГОСТ Р34.10-2012, ГОСТ 34.11-2012, ГОСТ Р34.12-2015 МАГМА); программная реализация AES-128, AES-256, SHA-1, SHA-256

03 Память: 256 КБ ROM (память программ), 6 КБ RAM, 144 КБ EEPROM (память данных)

04 Сертифицировано Центром защиты информации (8-й центр ФСБ России)

РЕШЕНИЕ НИИМЭ И МИКРОНА

Программное обеспечение позволяет осуществлять либо нативную реализацию приложений электронных документов (операционные системы **Trust** разработки АО «НИИМЭ»), либо в виде апплета для виртуальной Java-машины (на базе операционных систем **Just** разработки АО «НИИМЭ»)

Предоставляются SDK для разработки ОС и Java-апплетов на стороне заказчика, либо разработка осуществляется ПАО «Микрон» и АО «НИИМЭ»

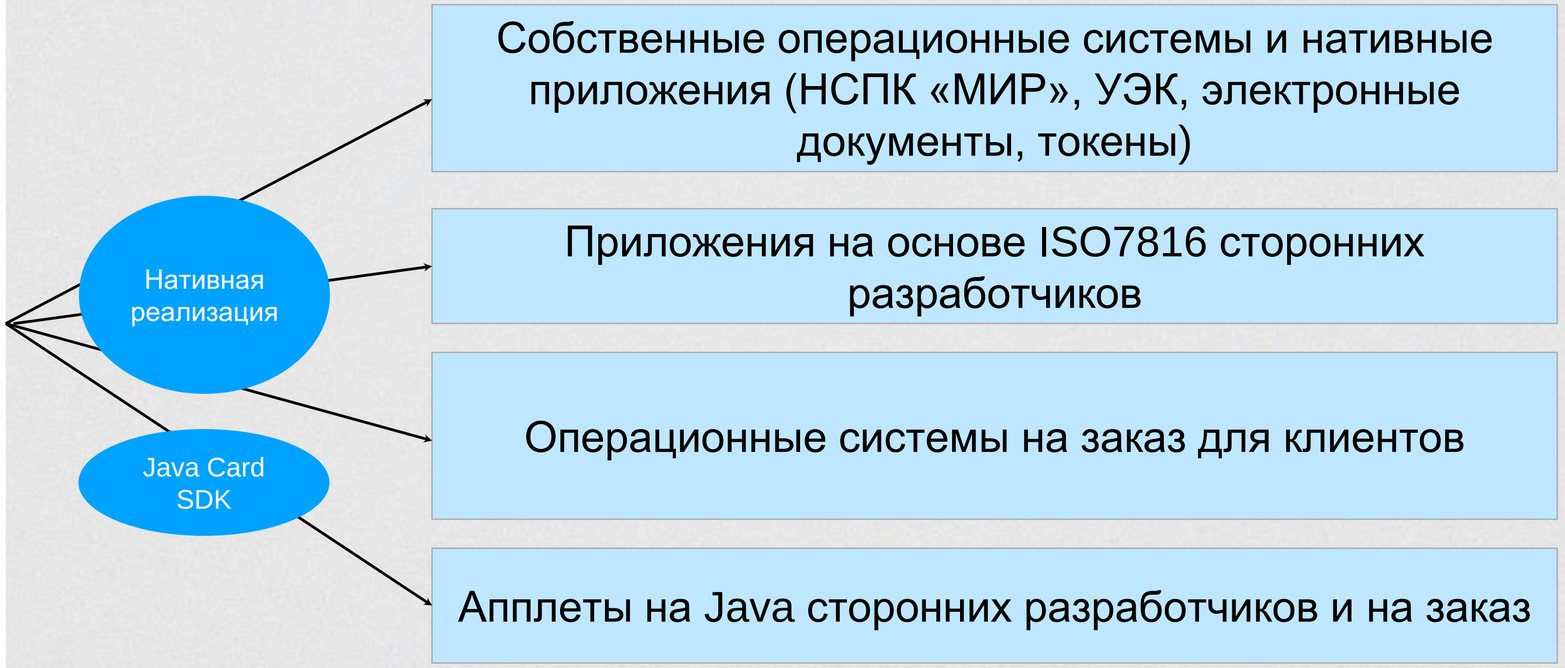
Программные продукты для семейства микроконтроллеров

Семейство чипов (память программ/память данных, КБ)

- К5016ХС2 (160 / 72КБ)
- К5016ВГ1 (384 / 72КБ)
- К5016ТС01 (160 / 144КБ)
- К5016ВК1 (160 / 72КБ)
- К5016ВК2 (160 / 72КБ)

Дуальный интерфейс, ГОСТ

Программное обеспечение



ВАРИАНТЫ РЕАЛИЗАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Операционная система Trust 3.0 с нативной реализацией приложения – имеется сертификат соответствия Центра защиты информации ФСБ РФ

- **ПОДДЕРЖКА ЭП, ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ ИНФРАСТРУКТУРЫ** УЛГ ДЛЯ СОБСТВЕННОГО РЕШЕНИЯ ЗАКАЗЧИКА (ИНФРАСТРУКТУРА СОЗДАЕТСЯ ГОСУДАРСТВОМ)
- **РАЗРАБОТКА ПРИЛОЖЕНИЯ СИЛАМИ ПАО «МИКРОН» И АО «НИИМЭ»** ПО СПЕЦИФИКАЦИИ ЗАКАЗЧИКА
- РАЗРАБОТКА ПОЛНОСТЬЮ ПРОИЗВОДИТСЯ **ИЗГОТОВИТЕЛЕМ МИКРОСХЕМЫ**
- БУДЕТ ИСПОЛЬЗОВАН **ОПЫТ СОЗДАНИЯ АНАЛОГИЧНЫХ ПРОДУКТОВ В РФ**
- ПРЕДОСТАВЛЕНИЕ **ПРОГРАММНОГО СИМУЛЯТОРА И КАРТ-ПРОТОТИПОВ ДЛЯ РАЗРАБОТКИ ОТВЕТНОЙ ЧАСТИ**
- В РАСПОРЯЖЕНИИ ПРИЛОЖЕНИЯ **БУДЕТ ПОРЯДКА 140 КБ СВОБОДНОЙ ПАМЯТИ ДАННЫХ EEPROM**

Операционная система Just 2.0 с виртуальной машиной Java

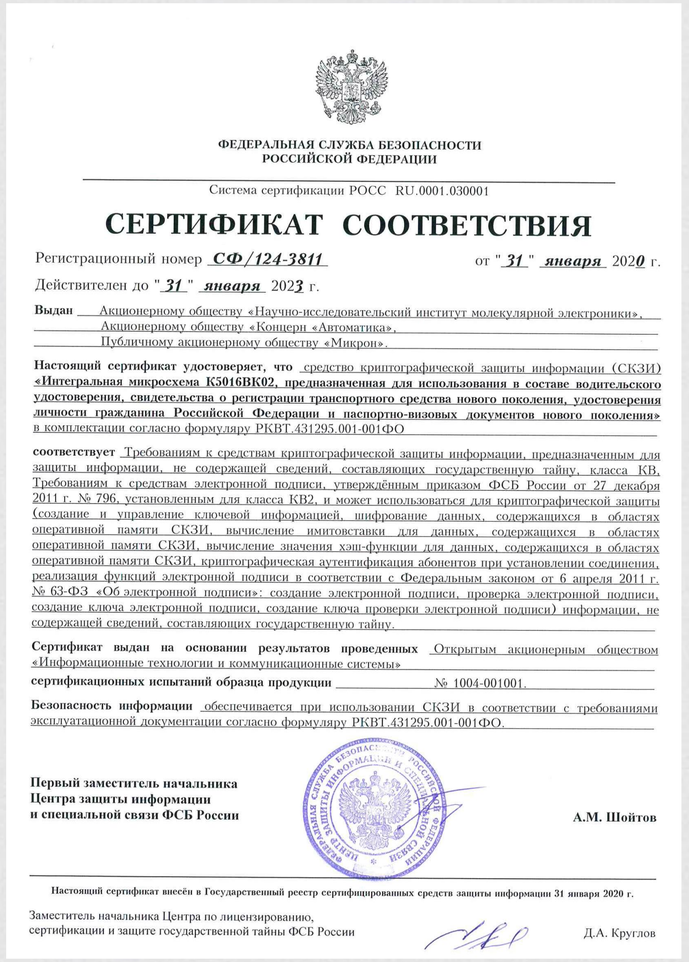
- ВОЗМОЖНОСТЬ **РАЗРАБОТКИ АППЛЕТА КАК НА СТОРОНЕ ЗАКАЗЧИКА** С ПОМОЩЬЮ SDK JEDI**, ТАК И НА СТОРОНЕ ПАО «МИКРОН» И АО «НИИМЭ»** (ПО ЖЕЛАНИЮ ЗАКАЗЧИКА)
- ВОЗМОЖЕН ВАРИАНТ ПРЕДОСТАВЛЕНИЯ **БАЗОВОГО ПРИЛОЖЕНИЯ ICAO,** КОТОРОЕ МОЖЕТ БЫТЬ ДОРАБОТАНО ЗАКАЗЧИКОМ
- ПРЕДУСМОТРЕНЫ **РАСШИРЕНИЯ СТАНДАРТНЫХ БИБЛИОТЕК JAVA CARD, ВКЛЮЧАЮЩИЕ РОССИЙСКИЕ КРИПТОАЛГОРИТМЫ И КРИПТОГРАФИЧЕСКИЕ ПРИМИТИВЫ**
- МОЖЕТ БЫТЬ ПРЕДОСТАВЛЕН **SDK JEDI ДЛЯ РАЗРАБОТКИ АППЛЕТОВ НА JAVACARD** С ПОДДЕРЖКОЙ РАСШИРЕНИЯ JC API
- ОЦЕНКА **СВОБОДНОГО МЕСТА** В ПАМЯТИ ДАННЫХ EEPROM ПОСЛЕ ЗАГРУЗКИ АППЛЕТА **- 100 КБ**
- **ПОДДЕРЖКА ВСЕХ СОВРЕМЕННЫХ КРИПТОАЛГОРИТМОВ – ГОСТ 34.10-2012, ГОСТ 34.11-2012, ГОСТ 34.12-2015 (МАГМА И КУЗНЕЧИК), ГОСТ 34.13-2015**

ЗАКАЗЧИКАМ ПРЕДОСТАВЛЯЮТСЯ БИБЛИОТЕКИ ДЛЯ НАПИСАНИЕ ТЕРМИНАЛЬНОГО ПО ПОД LINUX И ПОД WINDOWS

СЕРТИФИКАЦИЯ ЦЕНТРОМ ЗАЩИТЫ ИНФОРМАЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ И ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТАМОЖЕННОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Проводится сертификация программно-аппаратных средств криптозащиты информации на базе чипов НИИМЭ/Микрон на соответствие требованиям ФСТЭК России к **4 уровню** контроля отсутствия недекларированных возможностей (НДВ)

Средства криптозащиты информации на базе продуктов Микрона соответствуют ГОСТ 28147-89, ГОСТ Р34.10-2012, ГОСТ Р34.11-2012, ГОСТ Р34.12-2015 (Магма) , требованиям класса криптографической защиты до **КБ1 для применения в ПВД НП, водительском удостоверении и свидетельства о регистрации транспортного средства нового поколения, удостоверении личности гражданина**



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-3811* от "*31*" *января* 202*0* г.

Действителен до "*31*" *января* 202*3* г.

Выдан Акционерному обществу «Научно-исследовательский институт молекулярной электроники»,
Акционерному обществу «Концерн «Автоматика»,
Публичному акционерному обществу «Микрон».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) **«Интегральная микросхема К5016ВК02, предназначенная для использования в составе водительского удостоверения, свидетельства о регистрации транспортного средства нового поколения, удостоверения личности гражданина Российской Федерации и паспортно-визовых документов нового поколения»** в комплектации согласно формуляру РКВТ.431295.001-001ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КВ, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КВ2, 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, криптографическая аутентификация абонентов при установлении соединения, 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 Открытым акционерным обществом «Информационные технологии и коммуникационные системы»
сертификационных испытаний образца продукции № 1004-001001.

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру РКВТ.431295.001-001ФО.

Первый заместитель начальника
Центра защиты информации
и специальной связи ФСБ России **А.М. Шойтов**

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации 31 января 2020 г.

Заместитель начальника Центра по лицензированию,
сертификации и защите государственной тайны ФСБ России Д.А. Круглов

РЕАЛИЗОВАННЫЕ (ДЕЙСТВУЮЩИЕ) ПРОЕКТЫ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ НА ЧИПАХ ПАО «МИКРОН» И АО «НИИМЭ»

						
Микросхема	MIK51AB72D (K5016XC2)	MIK51AB144D (K5016TC01-04)	MIK51AB72R	MIK51SC72D (K5016ВГ1)	MIK51BC16D (K5016ВК1)	MIK51SC72D (K5016ВГ1)
Память (ROM/RAM/EEPROM)	160 / 6 / 72 КБ	160 / 6 / 144 КБ	160 / 6 / 72 КБ	384 / 8 / 72 КБ	256 / 6 / 16 КБ	384 / 8 / 72 КБ
Биометрия	Да	Да	Нет	Да	Нет	Нет
Интерфейс	Бесконтактный	Дуальный	Контактный	Дуальный	Дуальный	USB/контактный
Реализация ОС	Нативная	Нативная	Нативная	Нативная / Java	Нативная	Нативная / Java
Транспортное приложение	Нет	Нет	Нет	Да	Нет	Нет
Платежное приложение	Нет	Нет	Нет	Да	Да	Нет

ПЕРСПЕКТИВНЫЕ ПРОЕКТЫ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ НА БАЗЕ ГОТОВЫХ РЕШЕНИЙ ПАО «МИКРОН» И АО «НИИМЭ»

				
Микросхема	MIK51AD144D (K5016BK2)	MIK51AD144D (K5016BK2)	MIK51AD144D (K5016BK2)	MIK51AD144D (K5016BK2)
Память (ROM/RAM/EEPROM)	256 / 6 / 144 КБ	256 / 6 / 144 КБ	256 / 6 / 144 КБ	256 / 6 / 144 КБ
Биометрия	Да	Да	Да	Да
Интерфейс	Бесконтактный	Бесконтактный	Бесконтактный	Бесконтактный
Реализация ОС	Нативная	Нативная	Нативная	Нативная
Транспортное приложение	Опция	Нет	Нет	Опция
Платежное приложение	Опция	Нет	Нет	Опция

БЛАГОДАРИМ ЗА ВНИМАНИЕ!

www.mikron.ru
www.niime.ru

Вараксин Денис Владимирович
Директор по специальным проектам
ПАО «Микрон»

12, стр.1, 1ый Западный проезд, г. Зеленоград,
Москва, Российская Федерация
Тел. +7 495 7223720
dvaraksin@mikron.ru