sitronics
микроэлектроника

Операционная система смарт-карты проекта УЭК. Архитектура и криптографические возможности.

Константин Яковлевич Мытник
начальник отдела смарт-карт ОАО «НИИМЭ»

mkron

29 марта 2012

Смарт-технологии «Микрона»

- Собственный защищенный микроконтроллер MIK51
  - Разработан для смарт-карт с учетом высоких требований к безопасности
  - Производится по лицензированной у STM технологии 180нм.
- Собственная операционная система
  - Соответствует стандартам ISO и EMV
  - Содержит виртуальную машину JavaCard 3.0.2 Classic Edition
  - Интегрированные приложения: УЭК, EMV, Global Platform, ISO 7816-4
- Полный цикл изготовления карт
  - Производство микросхем
  - Корпусирование чип-модулей
  - Имплантация чип-модулей в пластик (дочерняя компания ССТ)
  - Персонализация карт (компания ССТ – имеет сертификаты МПС)

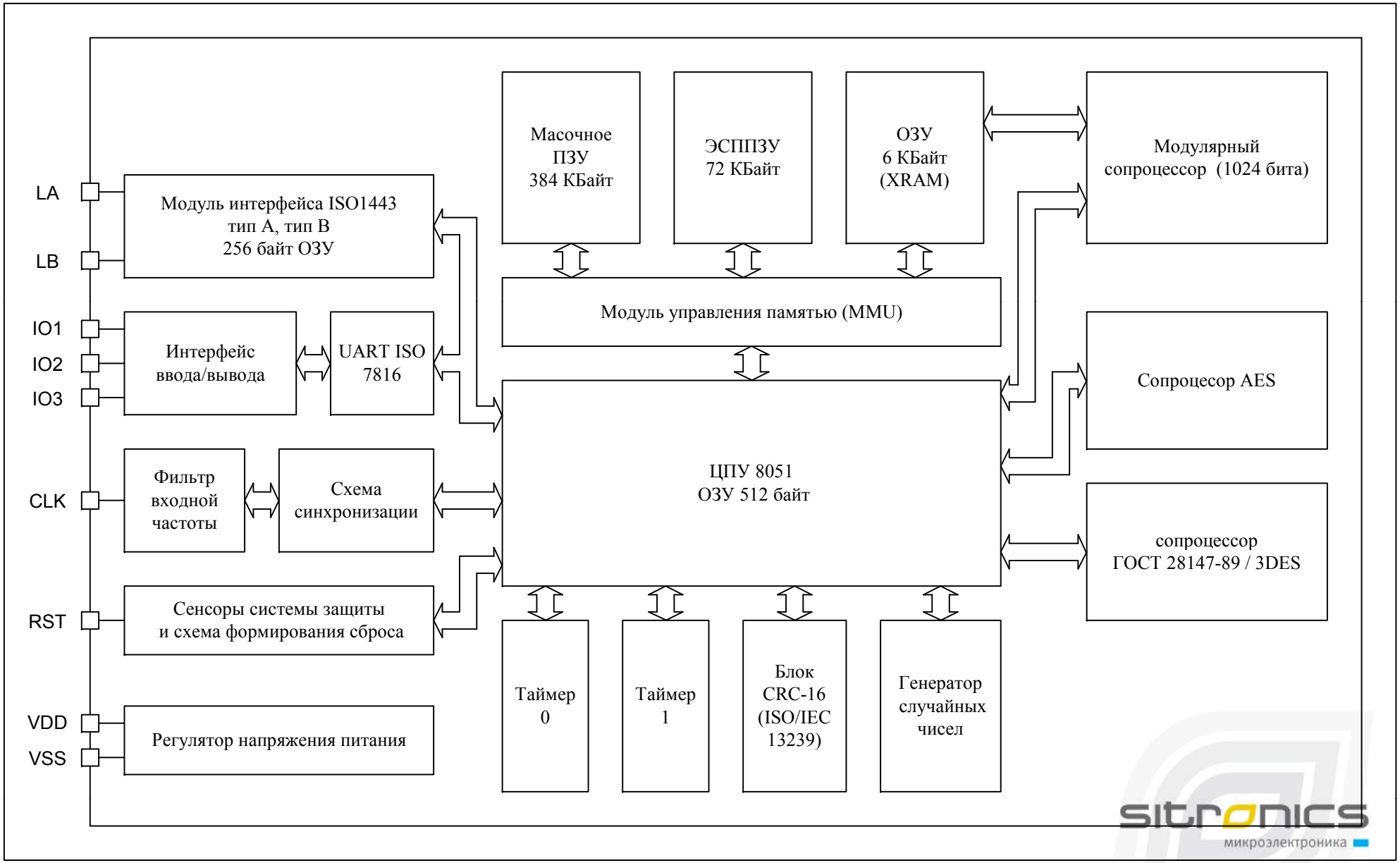
sitronics
микроэлектроника

Микроконтроллер MIK51

- 8-разрядный микроконтроллер с частотой до 30 МГц
- Объем EEPROM - 72K
- Двойной интерфейс
  - Контактный интерфейс T=0, T=1, скорость обмена до 200 Кбит/сек
  - Бесконтактный интерфейс Type A и Type B, скорость обмена до 424 Кбит/сек
- Криптографические сопроцессоры блочных алгоритмов:
  ГОСТ 28147-89, DES, 3DES, AES.
- Криптографический сопроцессор модулярной арифметики для вычисления и проверки ЭЦП по алгоритмам ГОСТ Р34.10-2001, ECDSA, RSA
- Поддержка протокола Mifare

sitronics
микроэлектроника

Структурная схема MIK51



Производительность криптографических операций

Алгоритм	Время операции @20MHz
ГОСТ 28147-89	0.3 мс/блок
3DES	0.3 мс/блок
AES-256	1.0 мс/блок
ГОСТ Р34.10-2001	95 мс – вычисление ЭЦП 173 мс – проверка ЭЦП
RSA-1024	98 мс – вычисление ЭЦП 3 мс – проверка ЭЦП
ECDSA-256	95 мс – вычисление ЭЦП 183 мс – проверка ЭЦП

Средства обеспечения безопасности

- Криптографические сопроцессоры
- Датчики высокой и низкой частоты, напряжения, температуры, света
- Аппаратные средства защиты от вскрытия
- Аппаратный контроль целостности EEPROM
- Аппаратный генератор случайных чисел
- Аппаратные средства активного противодействия инженерным атакам.
- Программные средства защиты в ОС
- Поддержка транзакций на уровне ОС.

Операционная система TRUST

- Модульная, переносимая, многоаппликационная ОС
- Поддержка дуального интерфейса (ISO 7816-3 и ISO 14443)
- Виртуальная машина JavaCard 3.0.2 Classic
- Поддержка жизненного цикла файлов и приложений (ISO 7816-9, Global Platform)
- Использование отечественных и основных международных криптографических алгоритмов.
- Технология проверки биометрических параметров на карте (MoC) (ISO 19794)
- Поддержка совместимости с картами Mifare Classic

Интегрированные приложения

- Идентификационное приложение УЭК ver. 1.0
- Платежное приложение ПРО100 / MasterCard M/Chip 4
  - Поддержка комбинированной аутентификации CDA
  - Поддержка динамической аутентификации DDA
  - Поддержка технологии шифрования ПИН-а.
- Домен безопасности Global Platform
- Приложение ISO 7816-4 (организация данных)
  - Файловая система любой конфигурации (ISO 7816-4)
  - Гибкая система разграничения доступа (ISO 7816-4)
- Приложение ISO 7816
- Загружаемые приложения для виртуальной машины JavaCard

Карта – защищенное хранилище данных

- Поддержка стандарта ISO 7816-4
- Файловая система произвольной глубины
- Файлы произвольного размера (более 64К)
- Механизм транзакций (гарантия атомарности записи)
- Аппаратный и программный контроль целостности данных
- Множество типов файлов:
  - Бинарные (transparent)
  - Файлы записей фиксированной и переменной длины
  - Циклические файлы записей
  - Файлы записей в формате Ber-TLV
- Гибкая система разграничения доступа
  - Задание атрибутов доступа в компактном или расширенном формате
  - Ядро безопасности, обеспечивающее разграничение доступа на основе дискреционной модели.

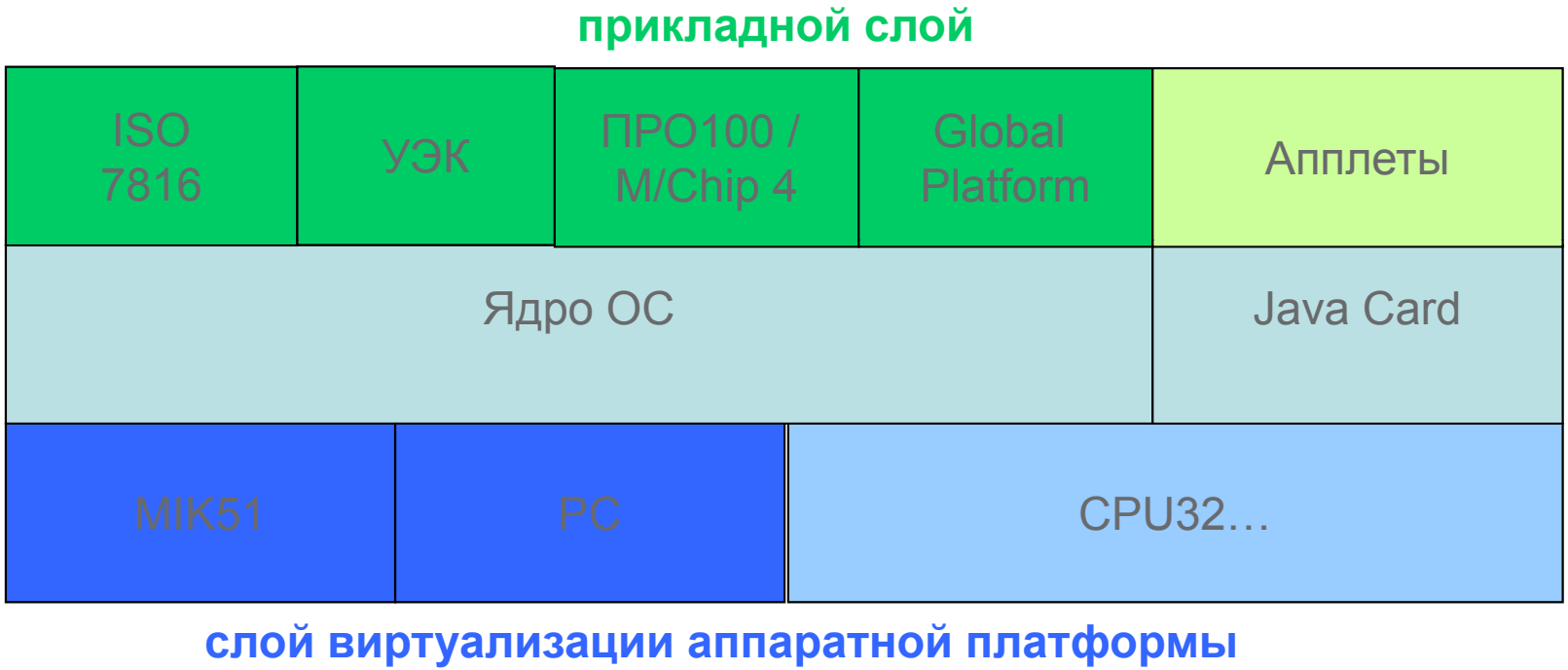
Карта - персональный модуль безопасности

- Поддержка стандарта ISO 7816-8
- Операции на симметричных криптографических алгоритмах (DES, 3DES, AES-128, AES-256, ГОСТ 28147-89)
  - Поддержка множества режимов шифрования ECB, CBC, OFB, CFB
  - Использование любого криптографического алгоритма (DES/3DES, AES, ГОСТ) для шифрования и контроля целостности и аутентичности данных
- Операции на алгоритмах с открытым ключом (RSA-1024/2048, ECDSA-256, ГОСТ Р34.10-2001):
  - Генерация ключей на карте
  - Вычисление и проверка ЭЦП
  - Проверка сертификата и загрузка открытого ключа
- Вычисление хеш-функций (SHA-1, SHA-256, ГОСТ Р34.11-94)
- Согласование ключей по алгоритму Диффи-Хелмана для эллиптических кривых

Виртуальная машина JavaCard

- Реализация спецификации Java Card 3.0.2 Classic
- Поддержка стандартных интерфейсов для использования основных международных криптографических алгоритмов
- Расширение Crypto API – встроенная поддержка отечественных алгоритмов:
  - ГОСТ 28147-89 (симметричный алгоритм)
  - ГОСТ Р34.10-2001 (ЭЦП)
  - ГОСТ Р34.11-94 (хеш-функция)
- Поддержка Bio API (проверка отпечатка пальца на карте)
- Обеспечение доступа к области данных Mifare через стандартный интерфейс

Структура операционной системы Trust



Архитектура криптографической подсистемы

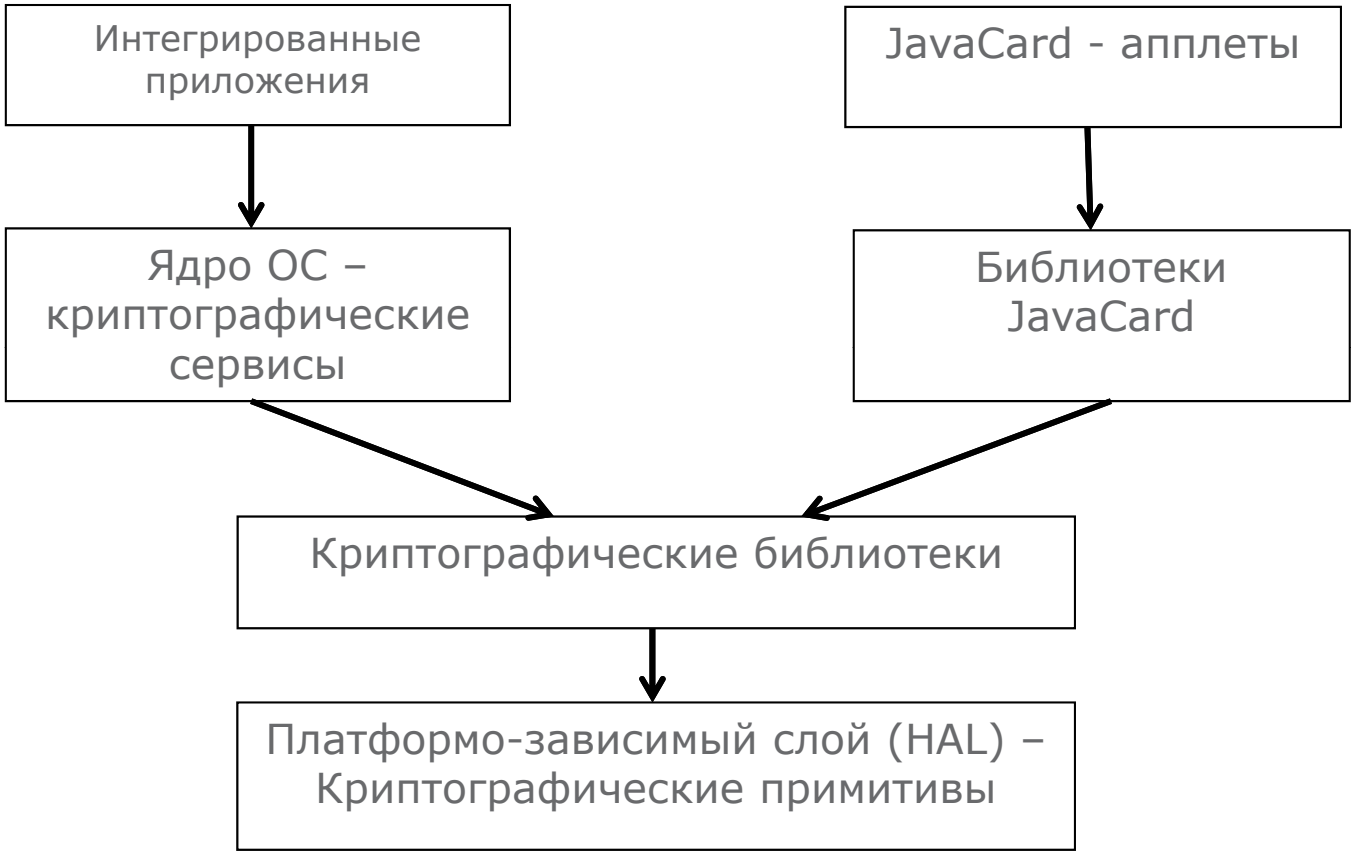


Схема защищенной сессии УЭК

Схема взаимной аутентификации по BSI 03110

Терминал	Карта
	Генерация случайного числа R_{ICC}
Генерация временной пары ключей (S'_{IFD}, P'_{IFD})	
Вычисление $R_{IFD} = Comp(P'_{IFD})$	
Вычисление проверочной криптограммы: $T_{IFD} = Sign[S_{IFD}](R_{ICC} \mid R_{IFD})$	
	Аутентификация терминала $Verify[P_{IFD}](T_{IFD})$, $Check(R_{ICC})$
Вычисление общего секрета: $K = KA(S'_{IFD}, P_{ICC})$	Вычисление общего секрета: $K = KA(S_{ICC}, P'_{IFD})$
Вывод сессионных ключей $K_{ENC} = KDF_{ENC}(K)$, $K_{CCS} = KDF_{CCS}(K)$	Вывод сессионных ключей: $K_{ENC} = KDF_{ENC}(K)$, $K_{CCS} = KDF_{CCS}(K)$
	Вычисление проверочной криптограммы: $T_{ICC} = CCS[K_{CCS}](R_{IFD})$
Аутентификация карты: $Check(T_{ICC})$	

sitronics
микроэлектроника

Спасибо за внимание

mkron