

**Чип-модуль Контактной-Бесконтактной Смарт Карты (ISO 7816/ISO 14443)****Краткая информация****ОСНОВНЫЕ ХАРАКТЕРИСТИКИ**

Защищенное микроконтроллерное ядро КМх32 разработки ООО «КМ211», режимы работы SYSTEM/USER с возможностью разграничения прав доступа пользовательских программ аппаратным firewall-ом;

- аппаратные средства самоконтроля и фаз жизни;
- уникальный серийный номер;

**ВСТРОЕННЫЕ СРЕДСТВА ЗАЩИТЫ**

- сенсор пластина/модуль;
- сенсор выхода напряжения питания за допустимый диапазон;
- сенсор целостности защитного экрана;
- генератор случайной последовательности;
- комплекс средств по защите микроконтроллера от утечки информации через ПЭМИН и ток потребления;
- комплекс средств по защите микроконтроллера от инженерных атак, имеющих целью нарушение целостности хранимых и обрабатываемых данных;
- комплекс средств по защите микроконтроллера от вскрытия с целью изучения и подключения к внутренним шинам.

**ВНУТРЕННЯЯ ПАМЯТЬ**

Все блоки внутренней памяти имеют аппаратную защиту\* целостности данных и защиту от несанкционированного доступа;

Внутренняя память, Кбайт:

- 512 Разделяемой Flash;
- 32 Bootloader;
- 12 SRAM;

Интерфейс ISO 7816: протоколы T=0, T=1; до 20 МГц;

Интерфейс ISO 14443: тип А; скорость обмена в обоих направлениях до 848 Кбит/сек;

**КРИПТОГРАФИЧЕСКИЕ СОПРОЦЕССОРЫ И АППАРАТНЫЕ УСКОРИТЕЛИ**

- ГОСТ Р 34.12-2015;
- ГОСТ Р 34.13-2015;
- ГОСТ Р 34.10-2012;
- ГОСТ Р 34.11-2012
- RSA-1024/2048/3072/4096;
- DES/3DES;
- AES-128/AES-256.
- CRC 8/16/32;

Время выполнения криптографических операций, мс:

- шифрование 1 блока по DES/3DES: 0,1
- шифрование 1 блока AES-128/AES-256: 0,2
- шифрование 1 блока по ГОСТ 34.12-2015:0,1
- вычисление ЭП RSA-1024 без использования CRT: 100
- вычисление ЭП по ГОСТ Р34.10-2012: 100
- проверка ЭП по ГОСТ Р34.10-2012: 200

Рабочий диапазон частот: 3 ... 23 МГц;

Напряжение питания: 5.0/3.3/1.8 В;

ESD защита: не менее 4000 В;

Рабочий температурный диапазон: -25 ... + 85<sup>0</sup> С;

**Варианты поставки:** Dual Interface smart-card;  
Dual Interface chip-module; M2M (MFF2), Wafer;

**Соответствие стандартам и сертификатам**

EMVCo;

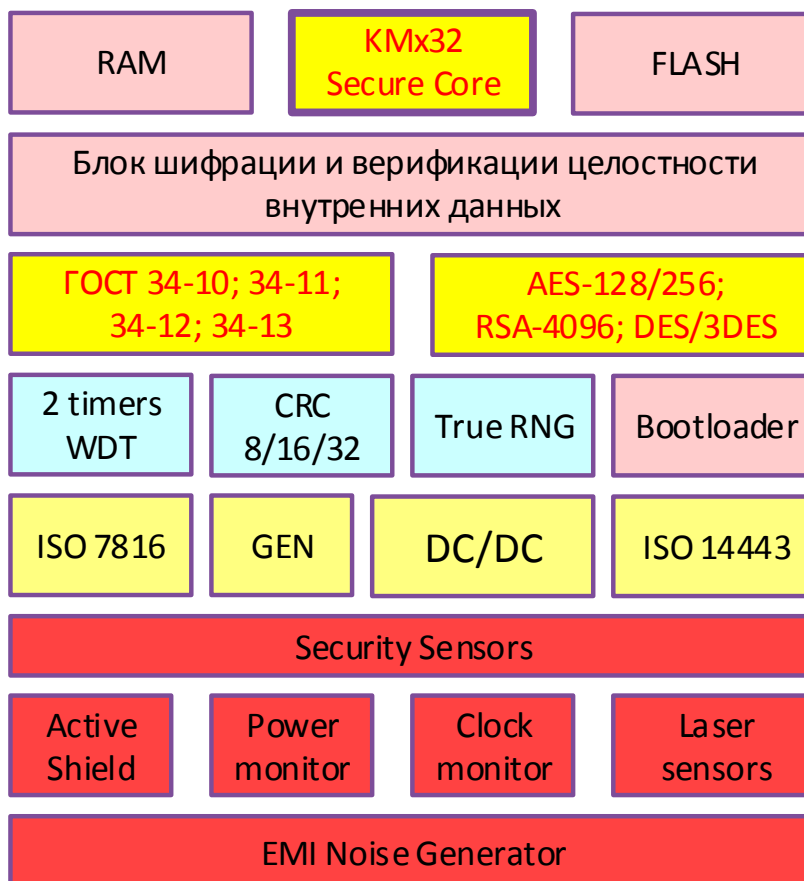
Уровни КБ/КС;

ГОСТ ИСО\МЭК 7816-3: 2006;

ГОСТ ИСО\МЭК 14443-1,2: 2013;

\*- **подробная информация доступна при подписании соглашения о неразглашении информации;**

## Функциональный состав



## ОТЛАДОЧНЫЕ СРЕДСТВА И КОМПЛЕКТ ПОСТАВКИ\*

- Отладочный комплект на основе FPGA;
- Отладочный комплект с тестовыми кристаллами;
- Микросхемы с отладочной прошивкой загрузчика;
- Среда разработки и отладки программ;
- Техническая поддержка online;
- Комплект документации в составе:
  - *Внутренняя архитектура*
  - *Руководство разработчика*
  - *Описание IDE*
  - *Система отладки*
  - *Компилятор, toolchain*
  - *Комплект тестового ПО*
  - *Описание Загрузчика*

\*- Опытные образцы и средства разработки будут доступны в мае 2018 г.