конференция
РусКрипто'2013
http://www.ruscrypto.ru/conference/

inside SECURE

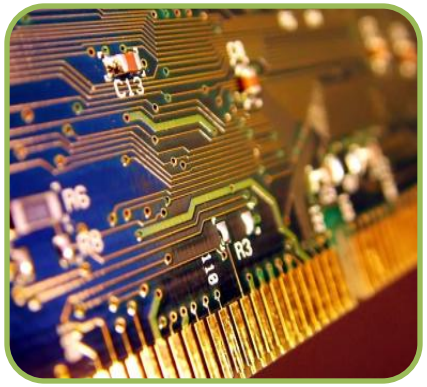
Аппаратная реализация криптографических алгоритмов в защищенных микроконтроллерах Inside Secure

Платонов В.В. к.т.н., профессор кафедры «Информационная безопасность компьютерных систем» ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет»

Компания Inside Secure

- Основана в 1995 году. 340 сотрудников.
- В 2010 году приобретено подразделение Atmel по разработке защищенных микроконтроллеров.
- Головной офис во Франции, представительства в Европе, Северной Америке и Азии.
- Совокупный среднегодовой темп роста доходов за 2005-2011 годы составил 54 процента.

- Fabless - компания - около 500 млн чипов производится ежегодно.
- Основное направление - решения для обеспечения цифровой безопасности.
- Разработки подкреплены 500 патентами.



Защищенная архитектура

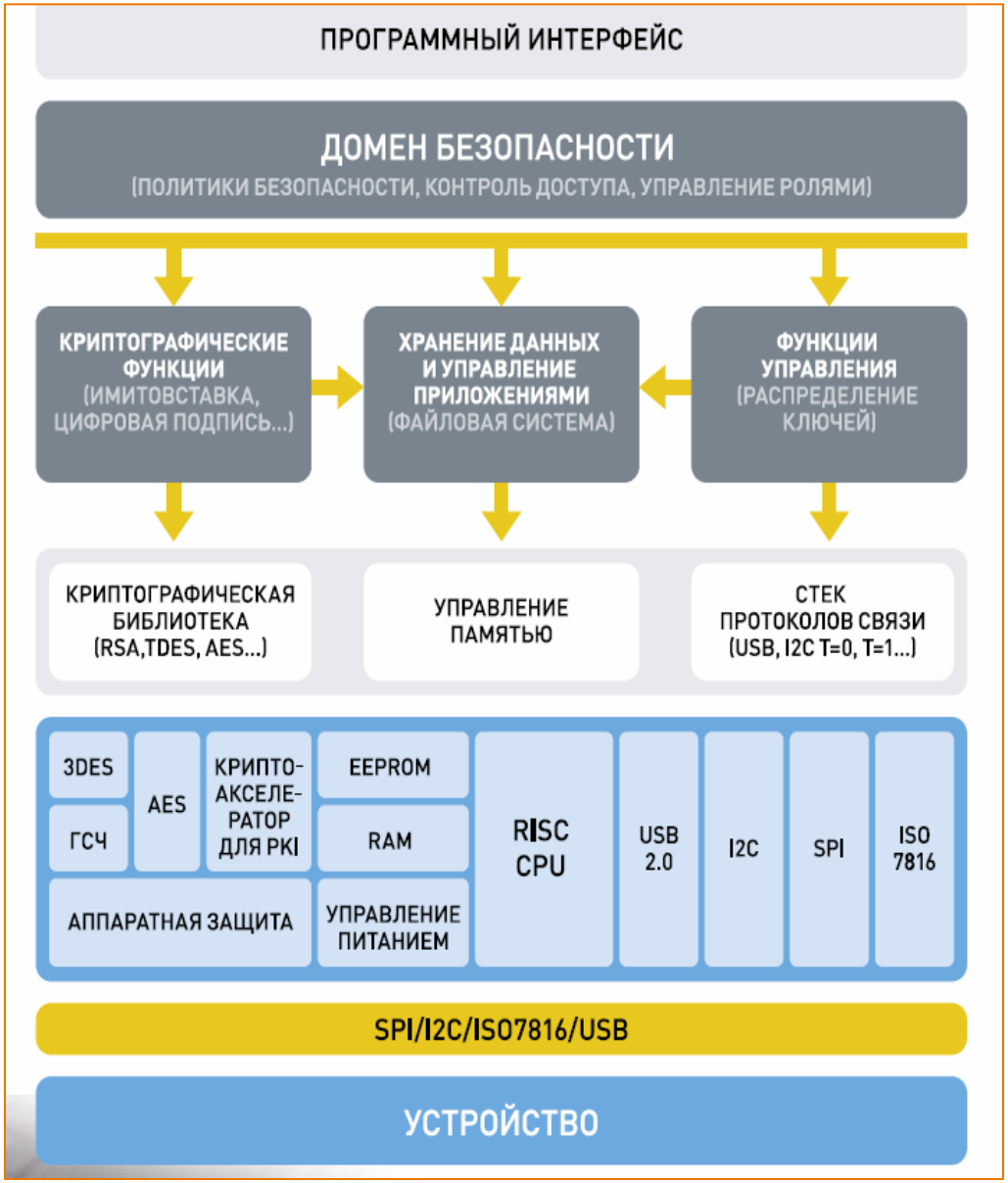
Линейка продуктов VaultIC

Защищенные модули **Vault*IC*™** являются инновационной разработкой **Inside Secure**, не имеющей аналогов.

Основная особенность - наличие встроенного программного обеспечения, включающего реализацию алгоритмов шифрования и цифровой подписи, генерацию ключей, сертификатов и одноразовых паролей, вызов которых осуществляется с помощью специальных библиотек.

Готовый продукт с их использованием может быть выпущен на рынок в максимально короткое время.

Принципы построения



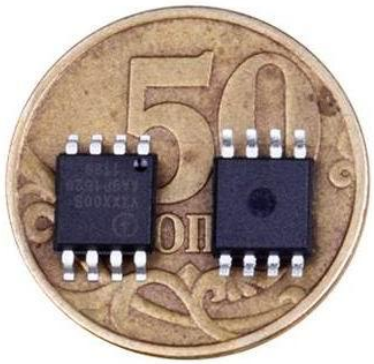
Линейка продуктов VaultIC

Марка	Файловая система	Алгоритмы	Конструкция
VaultIC 405	16K	TDES, RSA, AES, ECC	SOIC8, QFN20
VaultIC 420/421	32K	TDES, RSA, AES, ECC	SOIC8,QFN44/20
VaultIC 440/441	64K	TDES, RSA, AES, ECC	SOIC8,QFN44/20
VaultIC 460	112K	TDES, RSA, AES, ECC	SOIC8,QFN44

Аппаратная реализация

- 8/16 битовый RISC процессор;
- внутренняя файловая система;
- стандартные интерфейсы;
- аппаратный генератор случайных чисел;
- аппаратная реализация криптоалгоритмов.

8-SOIC

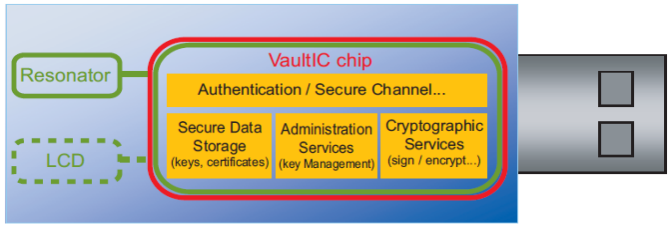


5мм x 5 мм

44-QFN

7мм x 7 мм

Реализация в виде токенов



Аппаратная реализация

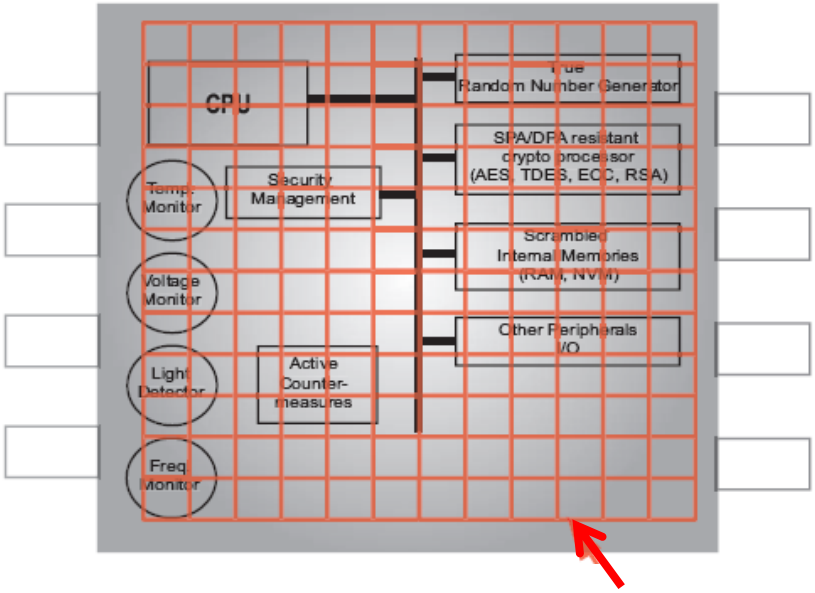
Реализованные криптоалгоритмы	Длина ключа (бит)
DES	**56**
TrippleDES	**112**
AES	**128,192,256**
RSA	**512, 1024, 1920, 2048, 4096**
ECC	**до 384**

- аппаратный ускоритель формирования 32 битных ключей (RSA - 512, 1024, 1920, 2048, 4096 бит, DSA - 512, 1024, 1920 и 2048 бит);
- вычисление хеш-функций HMAC: 160 (HMAC-SHA1), 256 (HMAC-SHA256), 384 (HMAC-SHA384), 512 (HMAC-SHA512) бит.

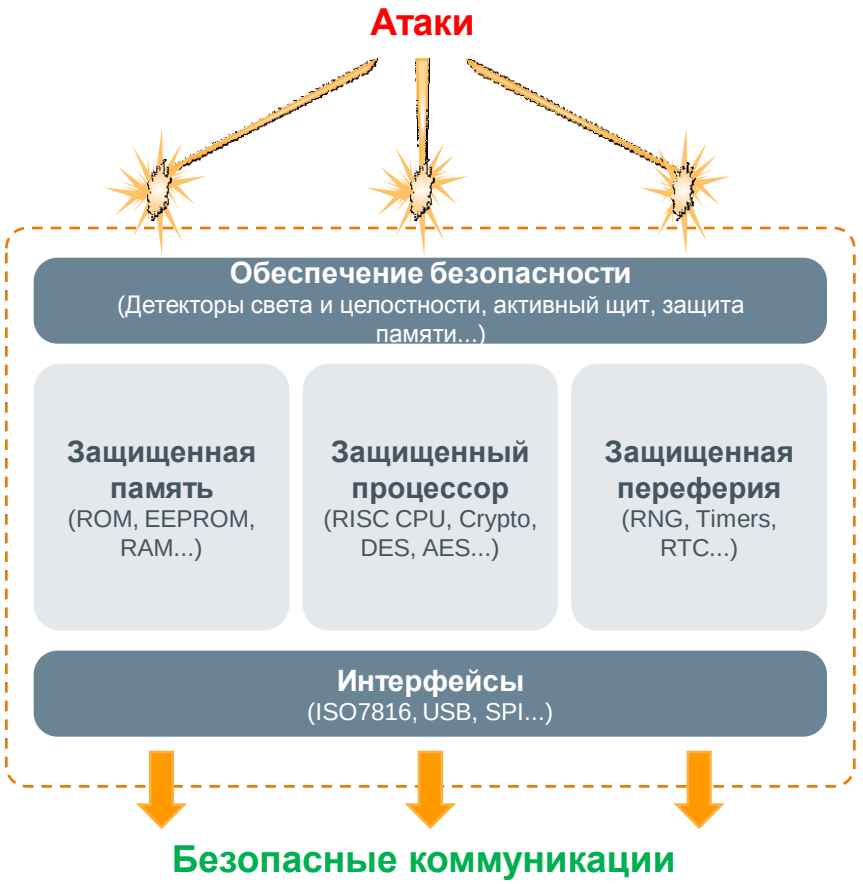
Особенности продуктов

Защищенность (защита от атак):

- детекторы света;
- детекторы напряжения;
- детекторы частоты;
- детекторы температуры;
- детекторы целостности.



Активное поле



Пример реализации

Защищенная передача данных со счетчиков

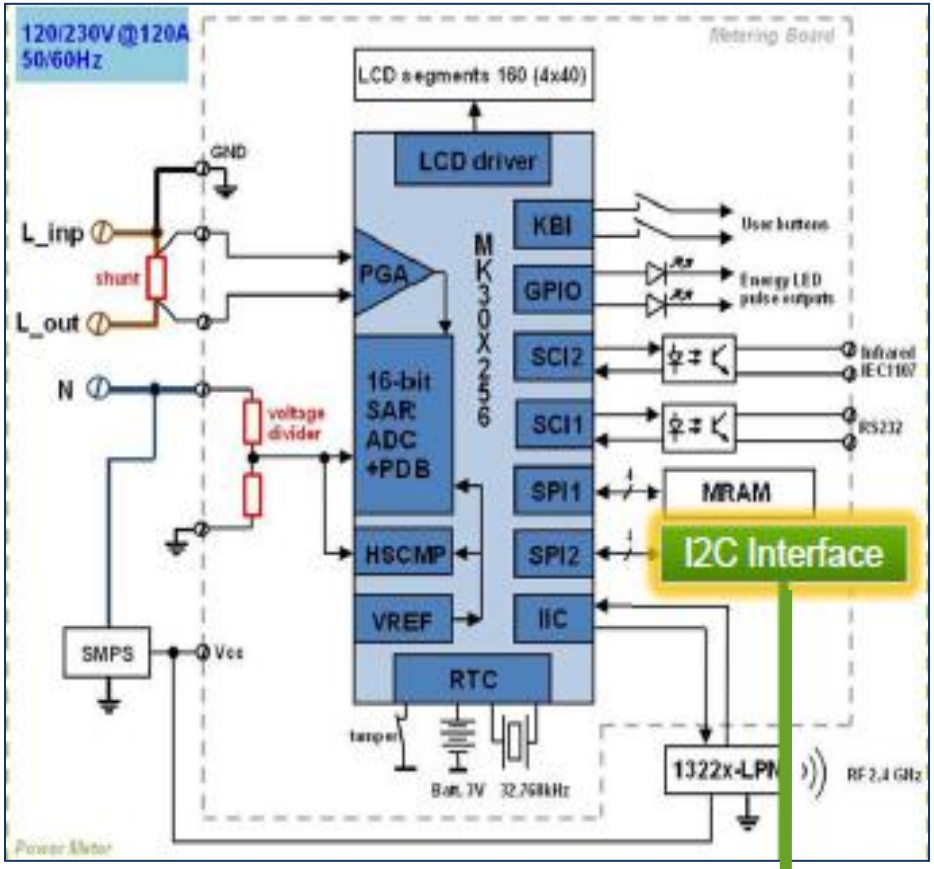
freescale™

inside SECURE

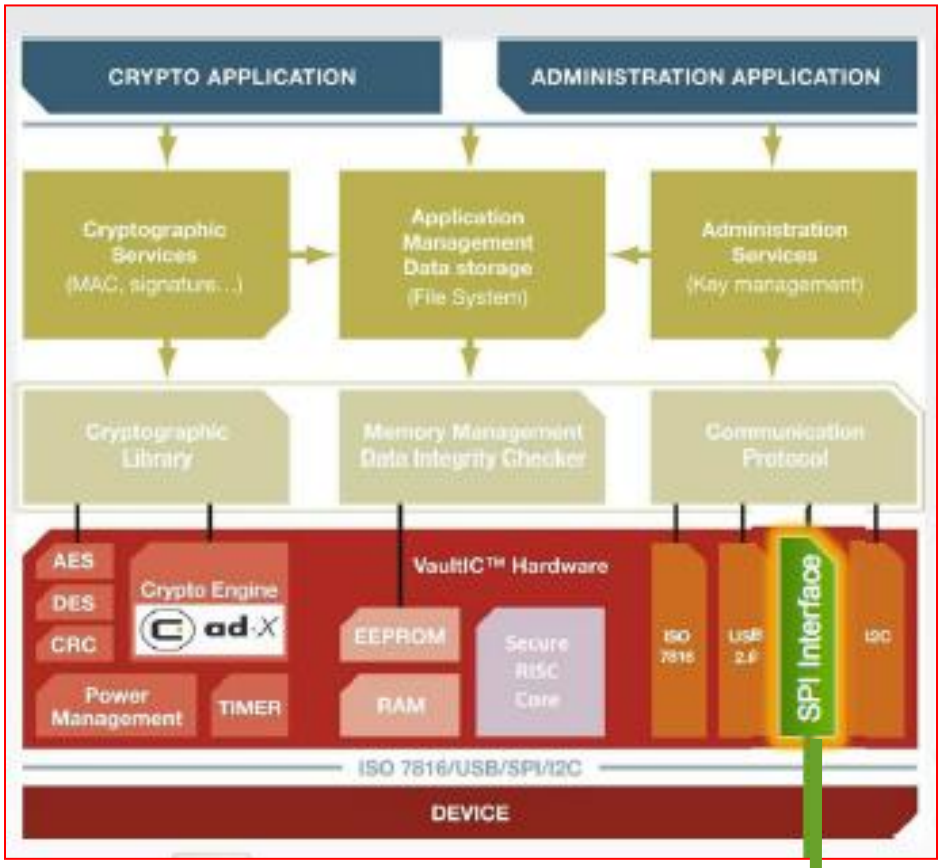
Счетчики позволяют пользователям безопасно считывать данные с помощью смартфонов или других устройств, оснащенных функцией NFC, или передавать зашифрованную информацию в энергетические компании для оплаты счетов.

Пример реализации

Freescale K30 ARM Cortex M4



Inside Secure VaultIC Security IC



Особенности технологии

- *Защищенное исполнение:*
  - Защита от различных атак.

- *Коммуникационные интерфейсы:*
  - SPI (Serial Protocol Interface);
  - I^2C (Twisted Wire Interface);
  - USB 2.0 (Universal Serial Bus);
  - ISO7816 Smart Card Interface.

- *Встроенные функции:*
  - безопасная память;
  - аутентификация идентичности: производитель, администратор, пользователи;
  - генератор псевдослучайных чисел;
  - аппаратно реализованные алгоритмы: DES, 3DES, AES, RSA PKCS#11, DSA, EC-DSA, MAC (с использованием DES, 3DES или AES).

Сертификаты

Все микроконтроллеры Inside Secure сертифицированы по стандарту FIPS 140-2 security Level 3. Микроконтроллеры Inside Secure готовы к сертификации по стандарту EAL4+ (Evaluation Assurance Level).

Данные стандарты приняты и введены в действие как
ГОСТ Р ИСО/МЭК 15408-1 – 2008 г.,
ГОСТ Р ИСО/МЭК 15408-2 – 2008 г. и
ГОСТ Р ИСО/МЭК 15408-3 – 2008 г.

ГОСТ ИСО/МЭК 15408-3 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования гарантированной безопасности».

EAL4 = УГО 4 ГОСТ

Аналоги

Компания	Продукты	Достоинства	Недостатки
RENESAS	Based on N-series (SC products)	- Популярность на рынке США - Поддержка симметричного шифрования AES, шифрования с открытым ключом RSA, хеширования SHA-256 - Наличие интерфейсов I2C, SPI и портов ввода-вывода общего назначения - Различные корпуса	- Плохой радиочастотный интерфейс - Неудачная стратегия безопасности
infineon	ORIGA™ SLE95050F1 SLE95050F2 SLE76 серия	- Используется криптография на эллиптических кривых - Высокий уровень технологий, безопасности и поддержки	- Единственный продукт - Интерфейс взаимодействия – только SWP
STMicroelectronics	AuKey	- Высокий уровень технологий, безопасности и поддержки - Поддержка алгоритмов AES, RSA и криптографии на эллиптических кривых	- Слабое развитие линейки - Только один протокол взаимодействия – I2C - Неясная ситуация с инвестициями в проект - Ориентация на использование в качестве TPM (Trusted Platform Module)
NXP founded by Philips	Au10tic A7001	- Высокий уровень технологий, безопасности и поддержки - Успешное использование в камерах Lumix в Китае - Наличие центра улучшения программного обеспечения - Поддержка алгоритмов AES, DES, RSA и криптографии на эллиптических кривых	- Слабое развитие линейки (единственный продукт) - Только один интерфейс взаимодействия – низкоскоростной I2C (100 кбит/с)
ATMEL	CryptoMemo CryptoRF	- Большая клиентская база - Известность на рынке	- Не является микроконтроллером - Нет поддержки инфраструктуры открытых ключей (PKI) - Поддержка только двух интерфейсов взаимодействия – ISO7816 и I2C

Защищенные микроконтроллеры с закрытой архитектурой

Достоинства:

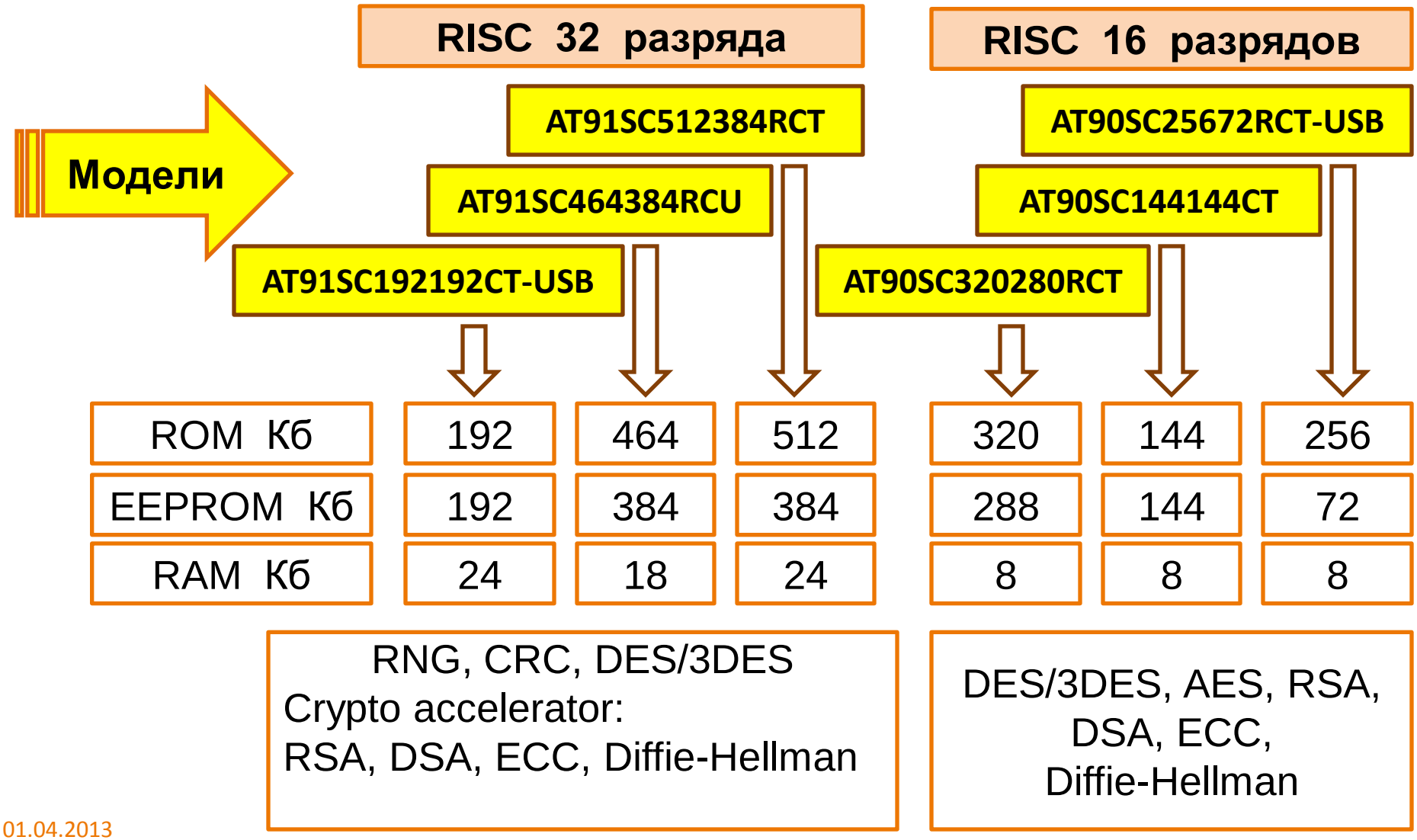
- законченное решение на базе 8/16-разрядных защищенных микроконтроллеров;
- поставляются с прошивкой и библиотеками;
- сертифицированы согласно FIPS, готовы к EAL4+;
- минимальные размеры.

Области применения:

- аппаратная защита систем (USB-ключи, фемтосоты, сети smart grid, игры, бытовая техника и т.д.);
- аутентификация и контроль доступа;
- интернет-банкинг;
- идентификационные карты/электронные паспорта;
- спутниковое телевидение;
- интеллектуальные системы измерений;
- системы защиты интеллектуальной собственности.

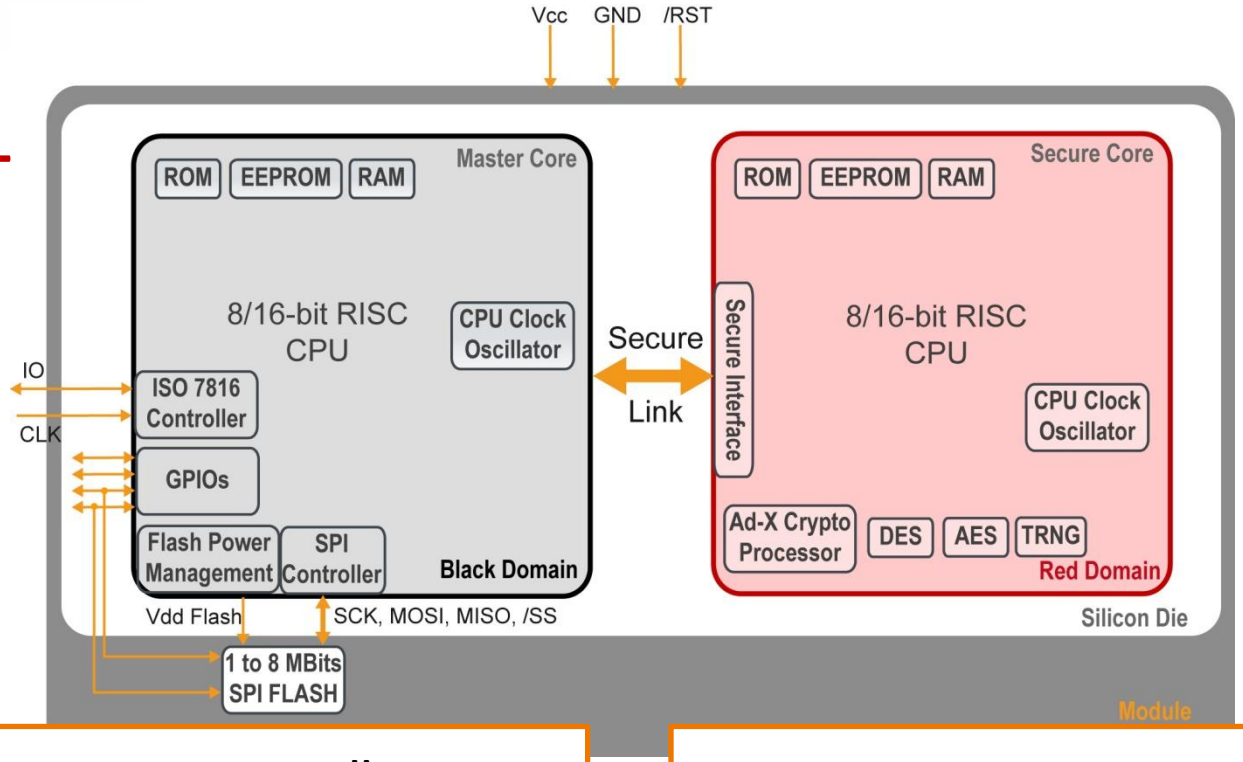
Открытая архитектура

Примеры линейки микроконтроллеров AT91SC и AT90SC



Dual Core процессор

TwinCore – AT90SDC



Основное ядро имеет прямой доступ к внешней среде через контроллер ISO. Ядро управляет интерфейсом SPI и питанием для внешней флэш-памяти, используемой для хранения данных. Интерфейс SPI может также служить дополнительным каналом связи.

Вспомогательное ядро является встроенным криптоакселлератором и не имеет связей с внешней средой. Включает безопасное хранение данных и реализации алгоритмов: AES, TDES, RSA и ECC.

Защищенные микроконтроллеры с открытой архитектурой

Достоинства:

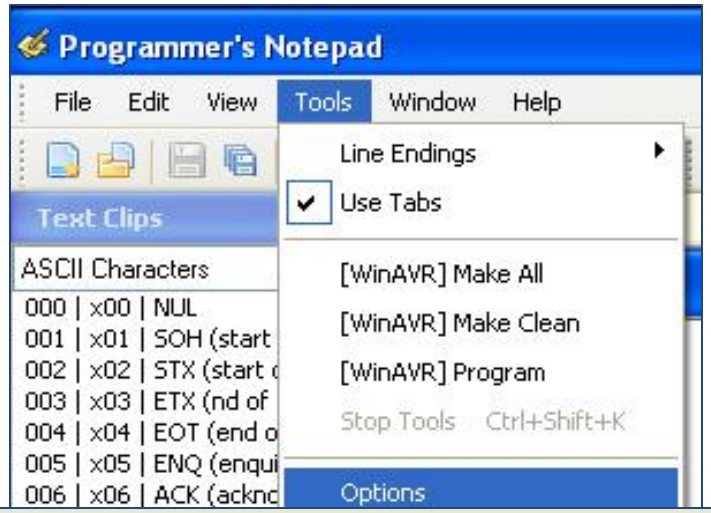
- 8-/16 и 32-разрядные защищенные микроконтроллеры
- Поставляются без прошивки
- Модули и бескорпусное исполнение
- Сертифицированы согласно EAL5+, EMVCo
- Возможность тонкой настройки для повышения уровня безопасности
- Удобная среда разработки приложений
- Большая номенклатура

Области применения:

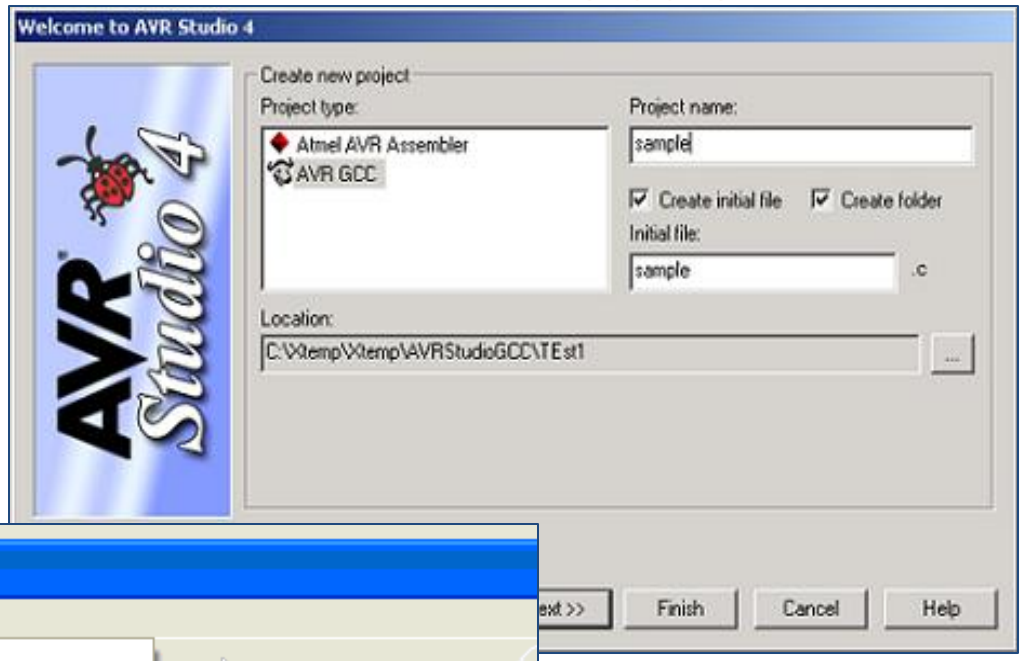
- Банковские карты
- Медицинские карты
- Платное ТВ
- Электронное правительство
- Электронные паспорта

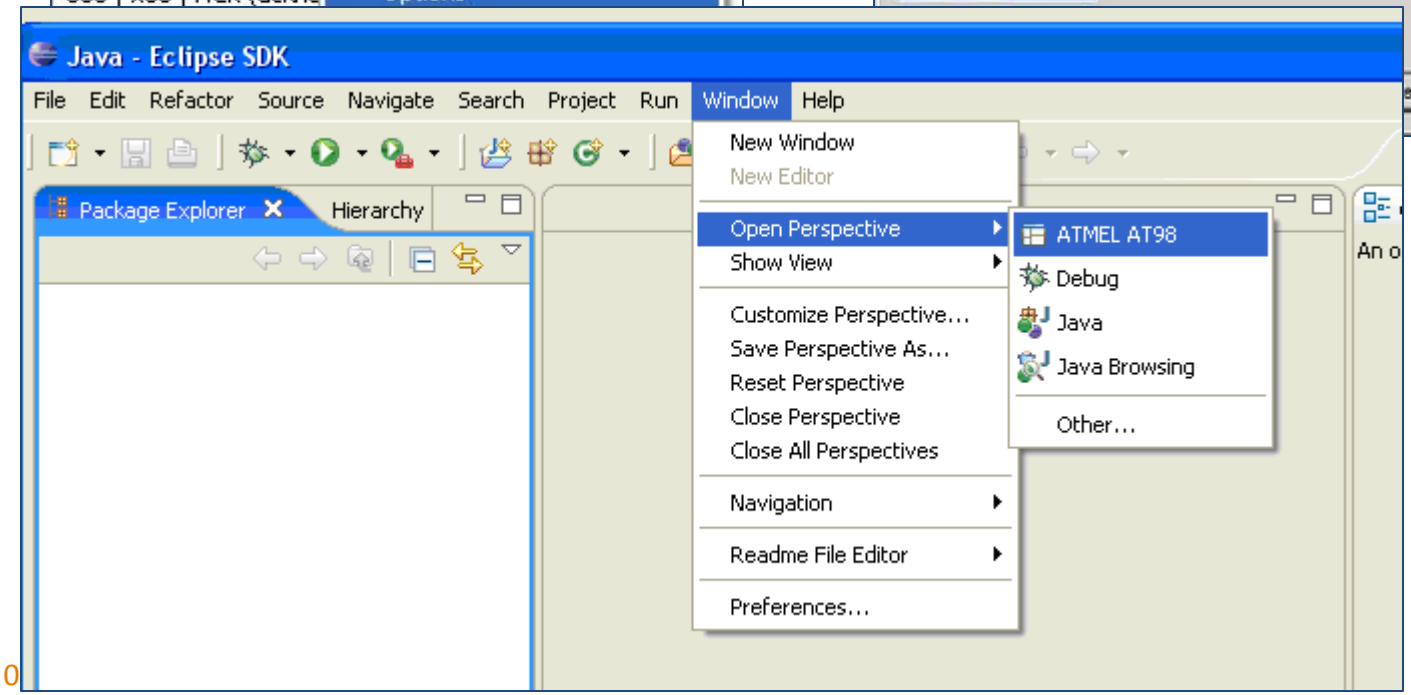
Средства разработки приложений

WinAVR™



AVRStudio





VaultIC STK

www.inside-rus.ru

e-mail: info@inside-rus.ru

тел.: (812)331-0967