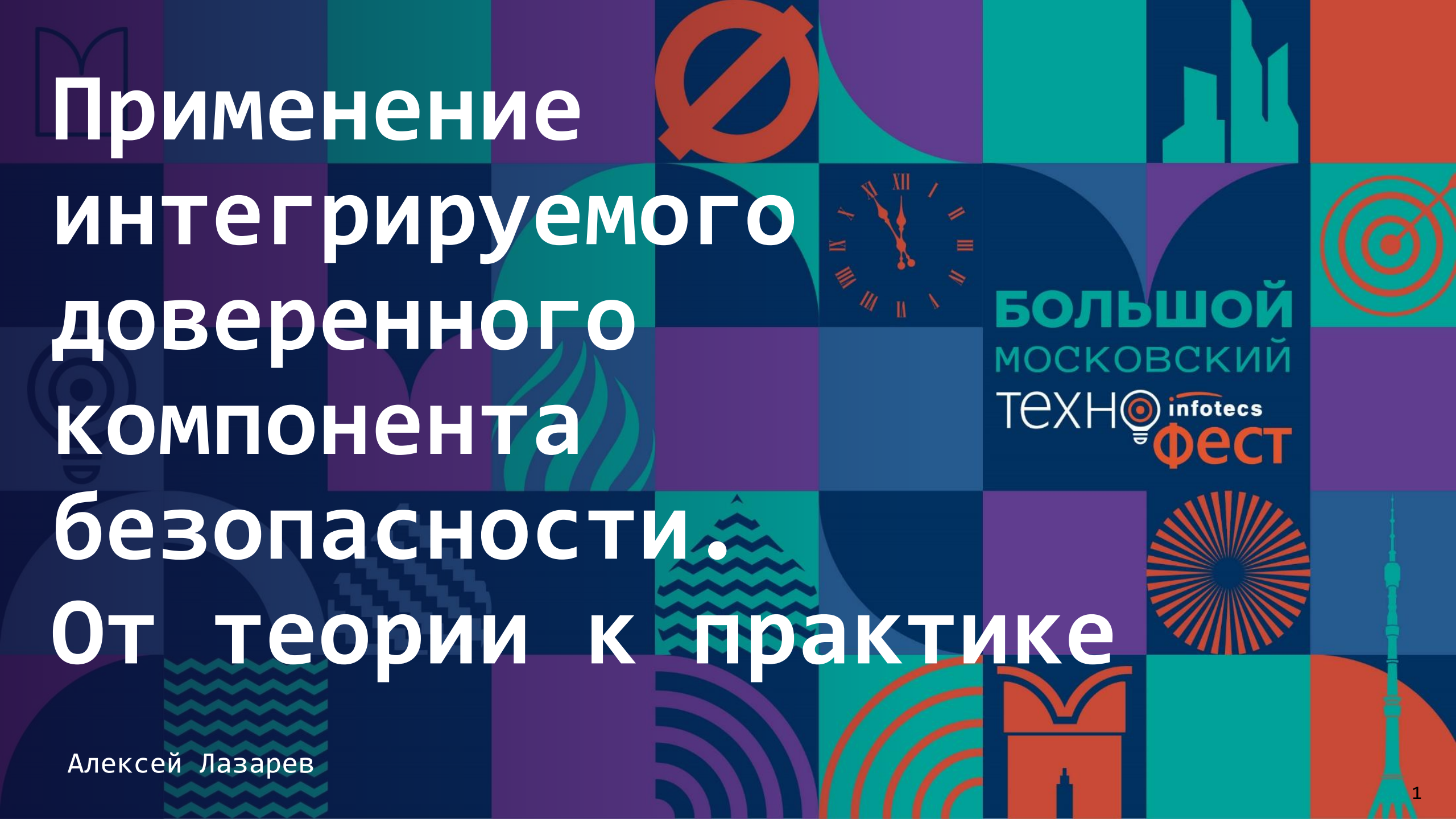
Применение интегрируемого доверенного компонента безопасности. От теории к практике



Алексей Лазарев

КОМПАНИЯ АКТИВ

Применение интегрируемого аппаратного компонента безопасности. От теории к практике.

Алексей Лазарев
Руководитель департамента защиты киберфизических систем, Компания «Актив»

Сергей Панасенко
Директор по научной работе, Компания «Актив»

Что такое доверенный компонент безопасности?

Модуль, на котором основывается обеспечение безопасности функционирования устройства или вычислительной системы.

Должен содержать:

- Основные/корневые секретные криптографические ключи
- Реализации криптографических преобразований, критичных для безопасности устройств/систем

Должен обеспечивать:

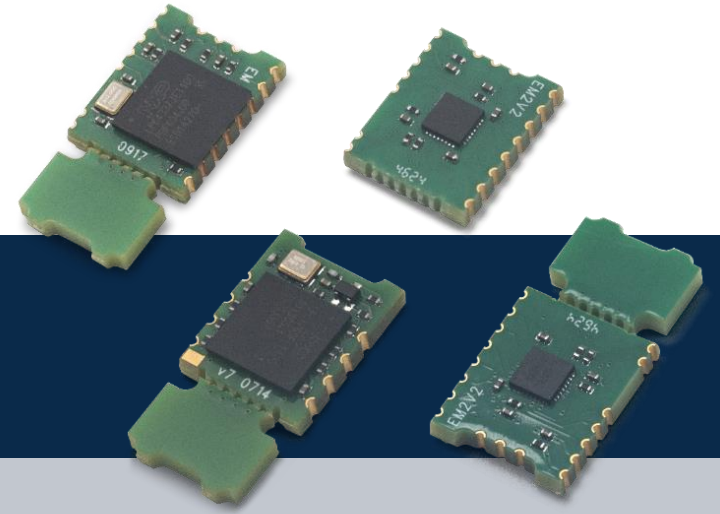
- Высокий уровень надежности
- Защищенность модуля от НСД
- Неизвлекаемость криптографических ключей
- Невозможность воздействия на выполняемые операции извне

Концепция
и сферы применения

Сферы применения:

- Банки
- Телеком
- АСУ (включая АСУ ТП) и их компоненты
- IoT

Сценарии применения



Интегрируемый доверенный компонент безопасности, используемый в реализации сценариев защиты

В средствах вычислительной техники

- Функциональность TPM
- Электронная подпись документов
- Проверка электронной подписи
- Аутентификация пользователей
- Защищенный сетевой обмен (TLS, VPN)
- Шифрование данных на носителях

В кибер-физических системах

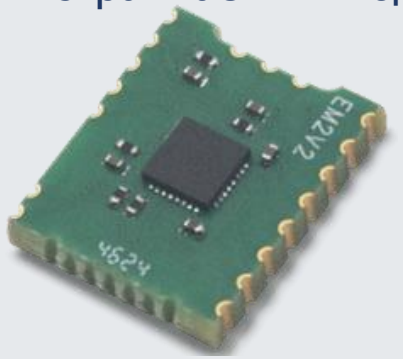
- Защита от атак повтора пакета
- Контроль целостности и аутентичности данных на носителях и данных, передаваемых по каналам связи
- Обеспечение конфиденциальности данных
- Контроль аппаратной целостности устройства
- Генерация случайных последовательностей

Общие сценарии

- Контроль целостности ПО
- Доверенное обновление ПО
- Аутентификация запускаемых процессов
- Организация цепочки доверия для загрузки и исполнения программного кода
- Сценарии защиты на неподменяемых корневых сертификатах

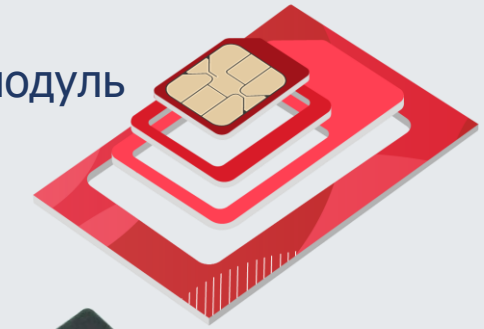
Форм-факторы

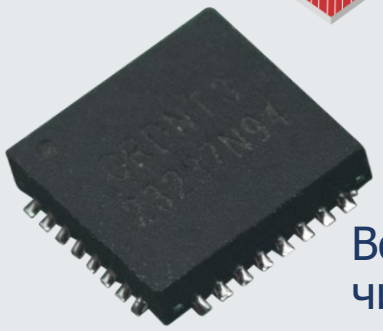
Встраиваемый модуль



USB-устройства

SAM-модуль





Встраиваемый чип

Хеширование

- ГОСТ Р 34.11-2012/2018

Электронная подпись

- ГОСТ Р 34.10-2012/2018

Шифрование, имитовставка

- ГОСТ Р 34.12-2015/2018, ГОСТ Р 34.13-2015/2018 (Кузнечик, Магма)

CRISP (ГОСТ Р 71252–2024)

Способы интеграции

Поддержка стандартов ISO/IEC 7816, PKCS#7, PKCS#11

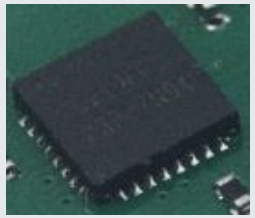
В уже разработанных системах

USB-устройство

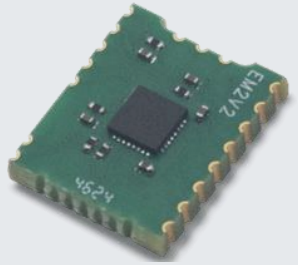
SAM-модуль

Во вновь создаваемых системах

Микросхема



Многоинтерфейсный интегрируемый модуль



Прикладное ПО, Плагины для браузеров

Библиотека прикладного уровня PKCS#7 (CMS), PKCS#11

Поддержка CCID на уровне операционной системы

Кроссплатформенный драйвер уровня CCID

Работа на аппаратном уровне (APDU, ISO/IEC 7816 ч.4)

USB-драйвер операционной системы

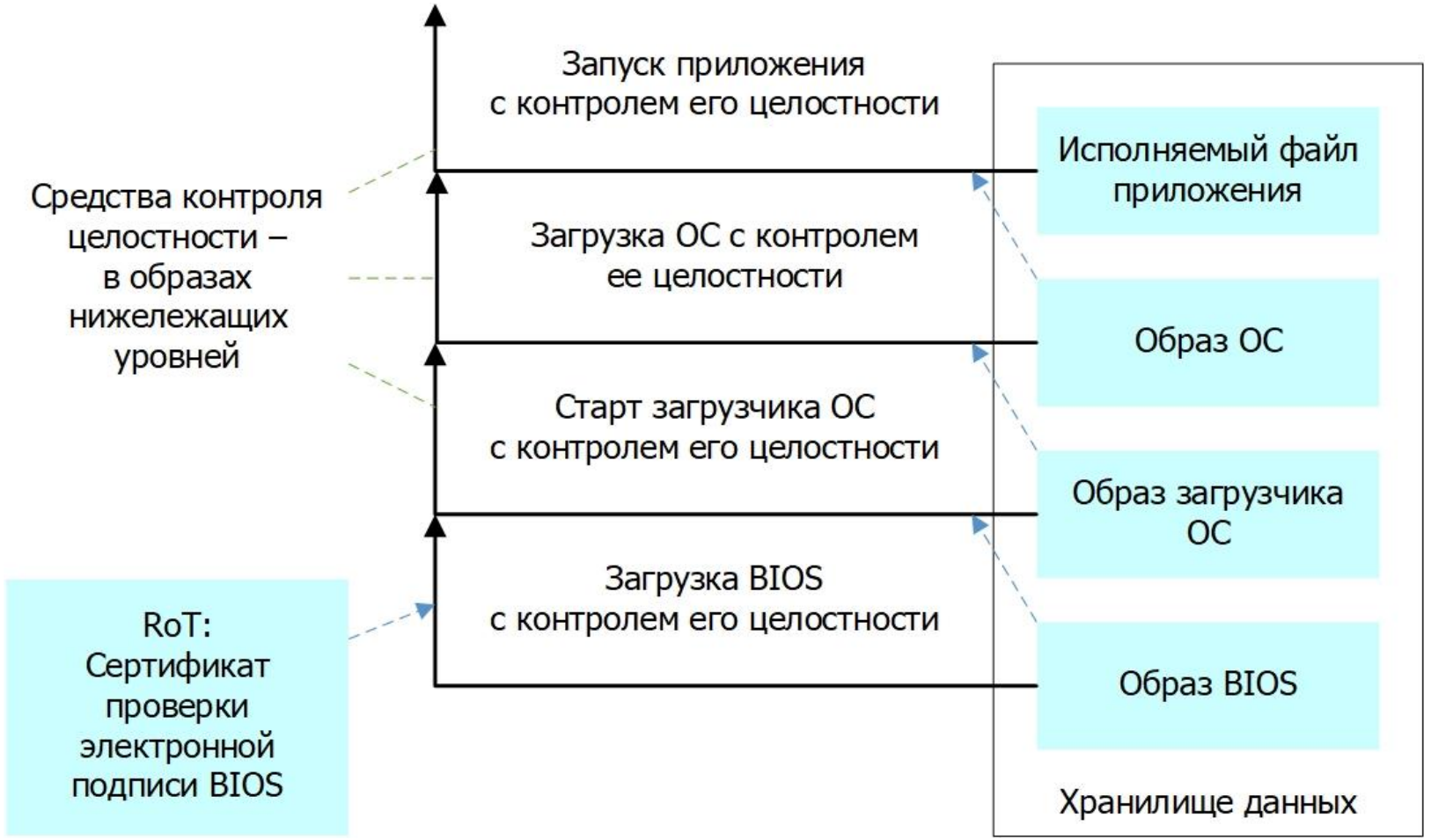
Интерфейсы USB, SPI, I2C, UART

Примеры использования: доверенная загрузка

Цепочка доверенной загрузки программных компонентов с поочередным контролем целостности на всех этапах.

На нижнем уровне контроль выполняется средствами RoT.

Предотвращение загрузки недоверенных программных компонентов.



Примеры использования: строгая взаимная аутентификация

Взаимная аутентификация устройства и сервера на основе электронной подписи.

Может сопровождаться вычислением общего симметричного ключа для защиты канала связи.

Пример применения:

- клиент – сенсор IoT;
- сервер – пограничный узел.

Примеры использования:
Контроль

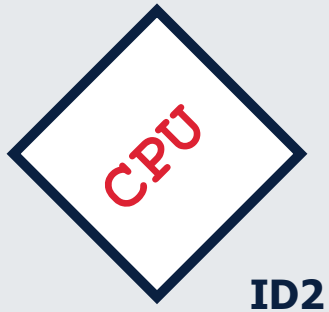
Функциональный модуль

- ID и S/N носителей
- ID и S/N CPU
- Mac-адреса сетевых устройств
- Динамические параметры (ДП)

Доверенный компонент безопасности

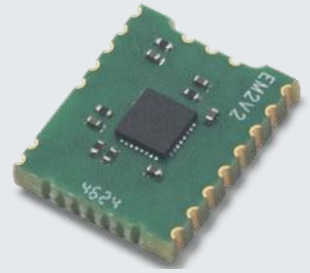
- ID микросхемы
- Хеш последовательности ID’s
- Границы допустимых значений ДП

Функциональный модуль (ID 1)



ID2

ID3

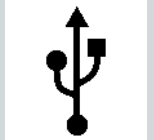


ДКБ ID4

RAM

Внешние интерфейсы

MAC1



MAC2

CRISP

Пример защищенной SCADA-системы

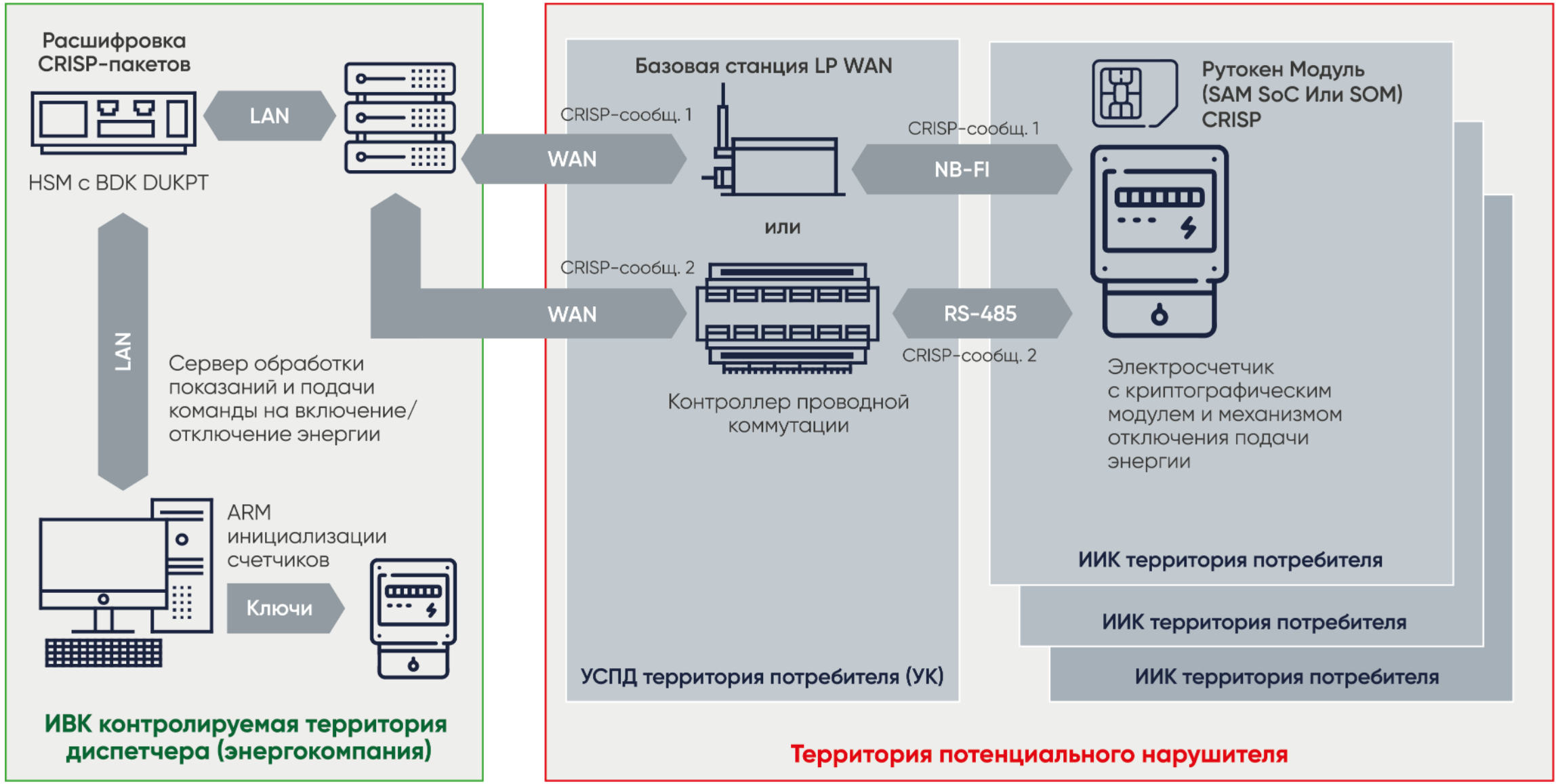


Схема DUKPT

DUPKT: Derive Unique Key Per Transaction.

Алгоритм используется в банковской сфере для шифрования PIN-кода и защиты данных в платежных системах VISA, MasterCard, МИР.

BDK: Base Derivation Key (базовый ключ алгоритма, суперсекрет).

Известен только производителю (поставщику) конечных устройств. Генерируется и хранится, как правило, в HSM на принимающей стороне, не покидая его.

IK (IPEK): Initial Key (исходный ключ диверсификации).

Вырабатывается из BDK методом криптографической диверсификации. Загружается на устройство производителем в контролируемой зоне. Используется для генерации будущих ключей.

DK: промежуточный ключ диверсификации.

DK вырабатываются из IPEK на инициирующей стороне и хранится до времени использования. Отработанные ключи DK удаляются из памяти конечного устройства на инициирующей стороне.

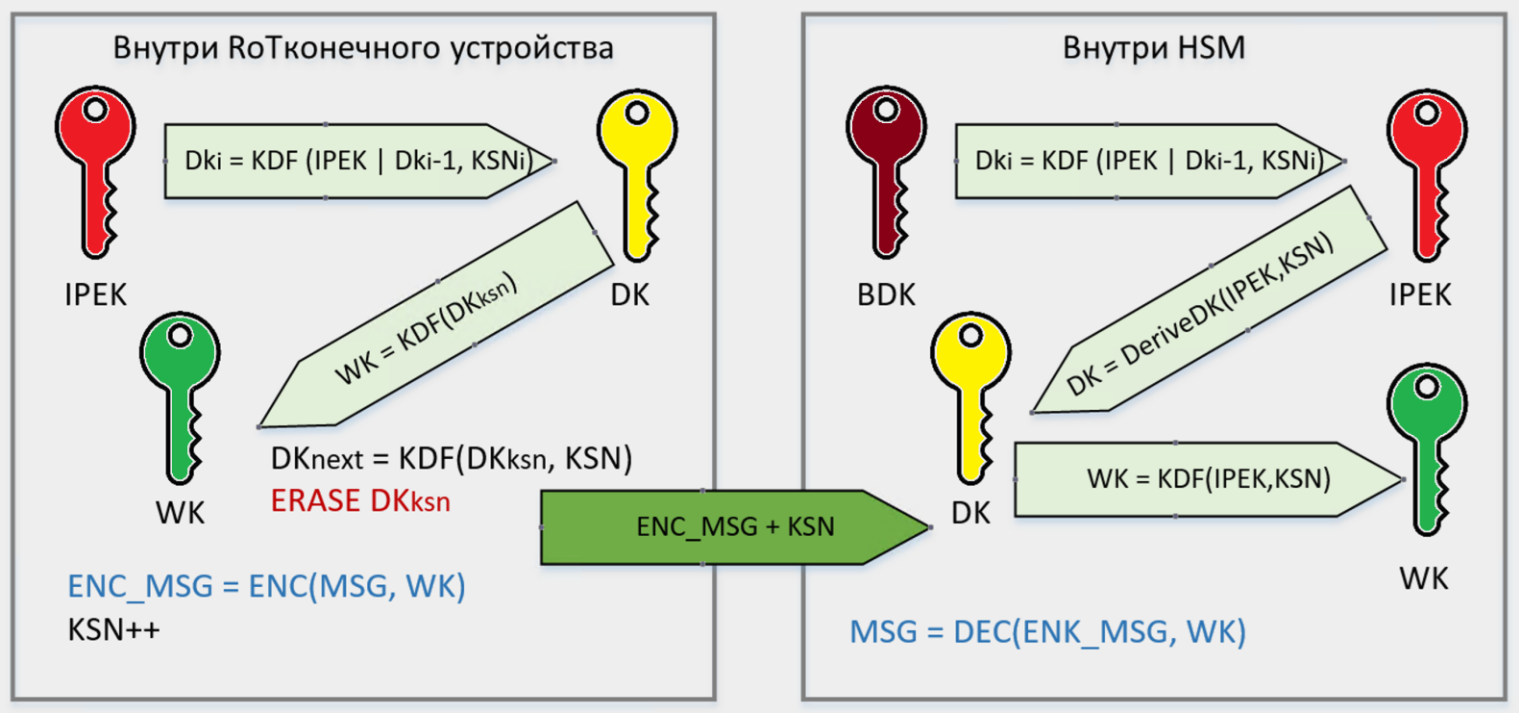
WK: Working key (рабочий ключ).

Вырабатывается из DKi на инициирующей стороне. Ключ, используемый для — защиты данных в текущей транзакции.

KSN: Key Serial Number (серийный номер ключа).

Комбинация серийного номера конченого устройства и счетчика количества транзакций которое было выполнена на устройстве. Счетчик инкрементируется с каждой выработкой ключа DK.

Схема DUKPT.
Принципы работы



Преимущества

Компрометация IPEK одного устройства не компрометирует систему

Уникальный ключ для каждой новой транзакции.При компрометации одного ключа другие ключи не компрометируются

Низкоресурсная схема за счет применения симметричной криптографии

Недостатки

Получив доступ к BDK, злоумышленник контролирует систему

Смена BDK приводит к необходимости переинициализации всех устройств

Пакет CRISP как контейнер информации для DUKPT

```
//CS=8 DUKPT-MAGMA-CMAC
struct crisp_dukpt_header {//128 bits (16 bytes)
    struct _init_info {             //32 bits (4 bytes)
        unsigned ExternalKeyIdFlag : 1; // 1
        unsigned Version : 15;// 0
        unsigned CS : 8; // Crypto set
        // Key ID
        unsigned KeyIDUse : 1; // = 1 Use key ID
        unsigned KeyIDLen : 7; // = 6 (First 6 bytes of KSN info)
    } init_info;

    union { // 96 bits (12 bytes)
        struct _crisp_keyid_secnum {// SecNum
            uint8_t KeyIData[6];        // CRISP KeyID  6 bytes
            uint8_t SeqNum[6];          // CRISP SecNum 6 bytes
        }crisp_keyid_secnum;
        struct _dukpt_ksn {         // DUKPT KSN
            uint8_t BDK_ID[sizeof(uint32_t)];           // DUKPT BDK ID
            uint8_t DerivationID[sizeof(uint32_t)];     // DUKPT Derivation ID
            uint8_t TransactionCounter[sizeof(uint32_t)];// DUKPT TransactionCounter
        }dukpt_ksn;
        struct _crisp_iv {          // InitVector for CS=1 (8?)
            uint8_t align[8];           // Not used for IV
            uint8_t IV[4];              // CRISP init vector
        }crisp_iv;
    };
    // PayLoadData Message data 00..800
    // ICV bytes
};
```

Применение в системах СКУД

Случайное число

CRISP-пакет

Подпись ОК
Сигнал
на открытие

IP-канал

Карта приложена

Случайное число

CRISP-пакет (ID, СЧ) CS3

Применяя наши решения, и, взаимодействуя с нашими специалистами, вы сможете:

1. Делать ваши IT-продукты по-настоящему защищенными при умеренных затратах
2. Соблюсти требования регуляторов при выводе на рынок новых решений
3. Быть на шаг впереди конкурентов, создавая продукты с прицелом на текущую и перспективную нормативную базу
4. Осваивать новые рыночные ниши там, где нужны специальные знания и навыки

Компания Актив оказывает содействие:

- В техническом сопровождении встраивания устройств Рутокен в продукты заказчика
- В проведении тематических исследований и сертификации

Спасибо за внимание!

КОМПАНИЯ АКТИВ

info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 495 925-77-90

Сергей Панасенко

panasenko@aktiv-company.ru

Алексей Лазарев

lazarev@aktiv-company.ru

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA

NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ

GLOBAL DIGITAL SPACE

CISOCLUB

РУТОКЕН КОМПАНИЯ АКТИВ

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

АВАНГАРД

PRinteg

АТБ ЭЛЕКТРОНИКА

infotecs {/-cademy}

merlion

УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС