



**РусКрипто**  
**XXVIII** НАУЧНО-ПРАКТИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

КОМПАНИЯ  
**ПРАКТИВ**

# Возможности и практическое применение доверенного компонента безопасности



**Максим Чукарев**

Ведущий инженер, Компания «Актив»

# Криптографические возможности

## 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)

## ГПСЧ

- Генерация случайных последовательностей

## CRISP

- ГОСТ Р 71252–2024

## Расширенные

- Криптографически стойкие протоколы для целевых систем



# Режим работы блочного шифра стойкий в Q2: критерии оценки ответов

1

**Неизвлекаемость  
криптографических  
ключей**



Подтверждено испытательной  
лабораторией



2

**Увеличенные  
сроки**



Увеличенные разрешенные  
сроки хранения ключевой  
информации до 5 лет

3

**Сертификация  
по классам СКЗИ:**

- КС1
- КС2
- КС3 (для целевых систем)

# Аппаратная универсальность



Поддержка наиболее востребованных физических интерфейсов подключения:

- USB
- UART
- SPI
- I2C



■ USB ■ UART ■ SPI ■ I2C



# Аппаратная универсальность

## Высокоуровневые программные интерфейсы

- Поддержка CCID на уровне операционной системы
- Кроссплатформенный драйвер уровня CCID
- Библиотека прикладного уровня PKCS#7 (CMS), PKCS#11

## Низкоуровневый APDU-интерфейс

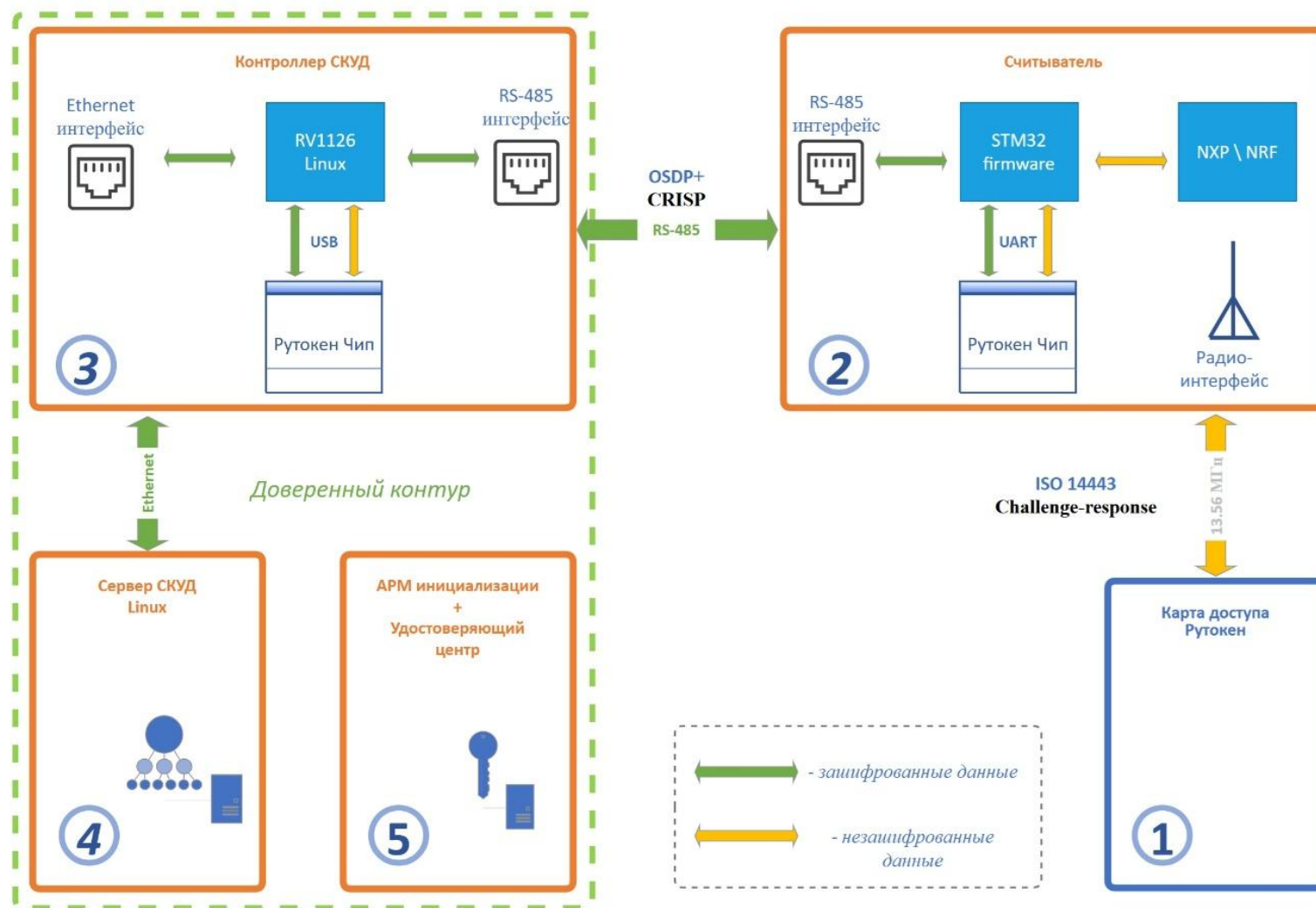
- USB-драйвер операционной системы
- Интерфейсы USB, SPI, I2C, UART
- Работа на аппаратном уровне (APDU, ISO/IEC 7816 ч.4)



# Пример применения



Возможность  
выступать  
связующим  
звеном в сложных  
комбинированных  
системах



# Спасибо за внимание!

КОМПАНИЯ  
РАКТИВ



info@rutoken.ru  
MChukarev@rutoken.ru



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



+7 495 925-77-90



## Максим Чукарев

Ведущий инженер, Компания «Актив»

 **РусКрипто**  
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ  
КОНФЕРЕНЦИЯ