XXI международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи

12-14 сентября 2023, Санкт-Петербург

PKI ФОРУМ РОССИЯ 2023

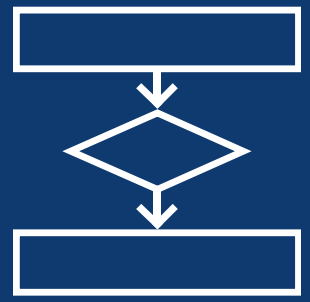
# Эволюция подходов к использованию ключевых носителей в отечественных PKI

**Владимир Иванов**
Директор по развитию
Компания «Актив»

# Решаемые задачи

**Целостность**

**Неизменность**

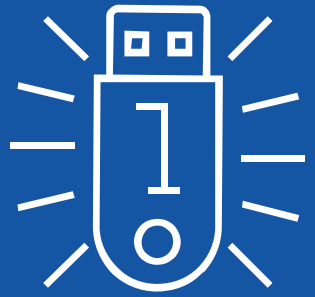


Доверие к алгоритмам подписи и хеширования

Доверие к реализациям алгоритмов

**Авторство**

**Неотрекаемость**



Существование ключа подписи в единственном экземпляре

Единоличное владение и доступ к ключу подписи

# Доисторические СКЗИ



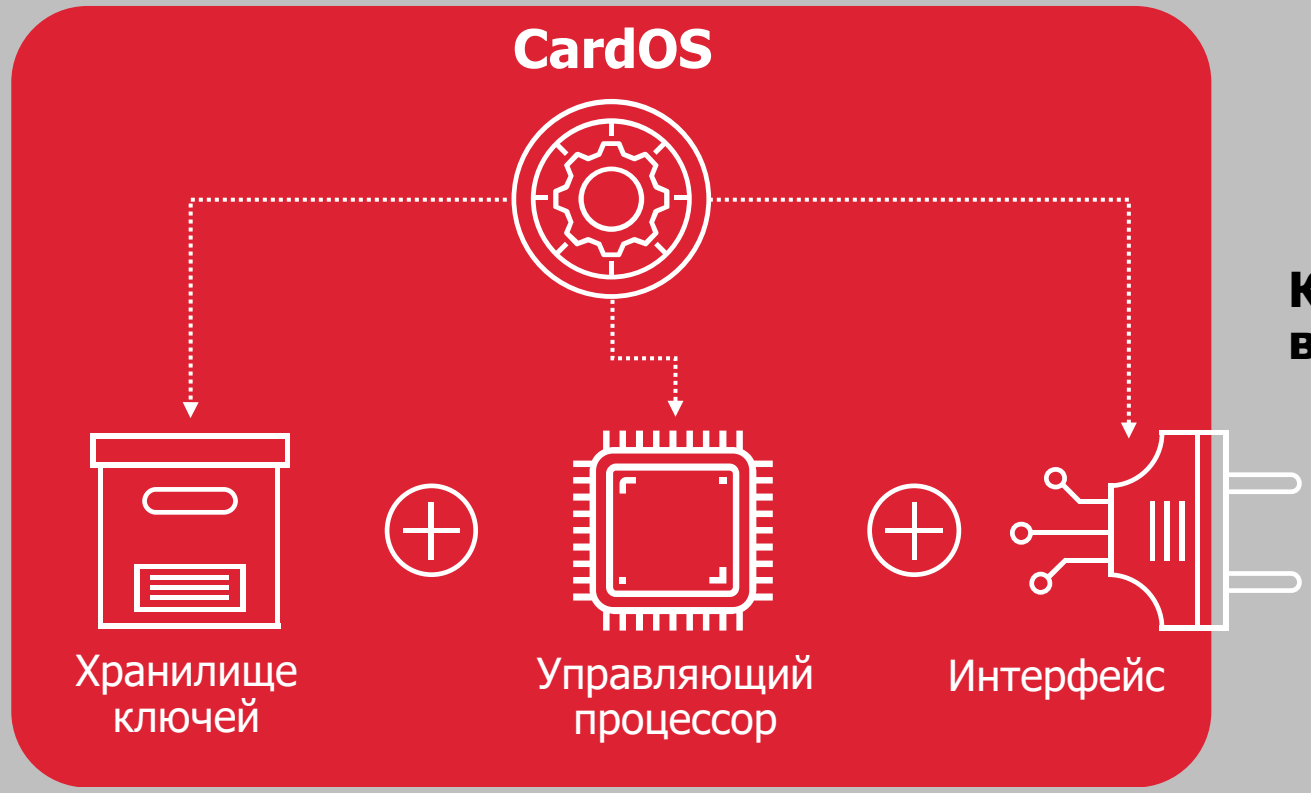
1. СКЗИ – само по себе доверенная среда исполнения
2. Эксплуатируется в заведомо безопасных условиях
3. Эксплуатируется заведомо квалифицированным персоналом
4. Программно-аппаратная платформа единственная

# Современные «гражданские» СКЗИ

1. Функционируют на множестве программно-аппаратных платформ
2. Эксплуатируются по большей части в недоверенной среде исполнения
3. Эксплуатируются в небезопасных условиях
4. Эксплуатируются неквалифицированными пользователями

# Как обеспечить безопасность ключей?

# Пассивный ключевой носитель




**Ключи извлекаются в память ПК**

**Доступ к хранилищу ключей защищен PIN-кодом**

**Доступ через смарт-карточные интерфейсы**
**Не является mass-storage**

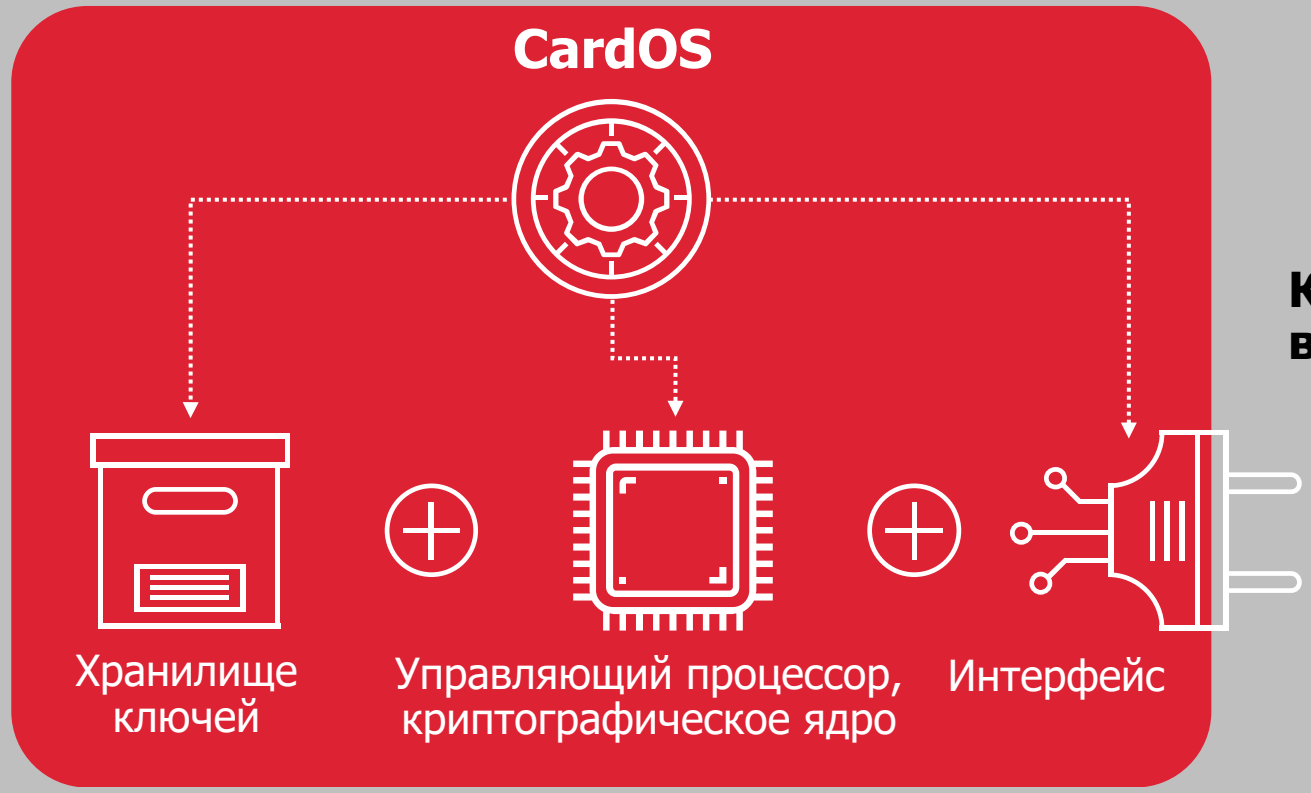
## Что получилось

- Повысили уровень защиты ключей
- Во многом упростили поддержку пользователй
- Сняли некоторые риски, связанные с бесконтрольным распространением ключей

## Что не получилось

- Не решили задачу  существования ключа в единственном экземпляре
- Не было подходящей аппаратной платформы
- Не решена задача работы СКЗИ в недоверенных средах

# Активный ключевой носитель

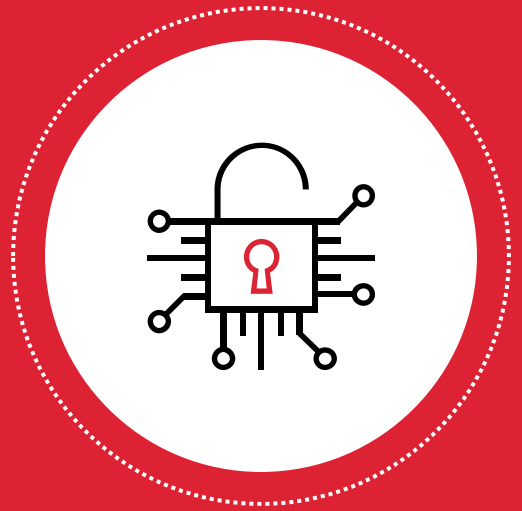



**Ключи НЕ извлекаются в память ПК**

**Доступ к использованию ключей защищен PIN-кодом**

**Доступ через смарт-карточные интерфейсы**
**Не является mass-storage**

# СКЗИ и ключи можно носить в кармане



# Первая ласточка

Универсальный браузерный плагин:

- Аутентификация и подпись через программные криптопровайдеры
- Аутентификация через устройства PKCS#11

# Переломный момент - ЕГАИС

Необходимость гарантировать единственность ключа подписи

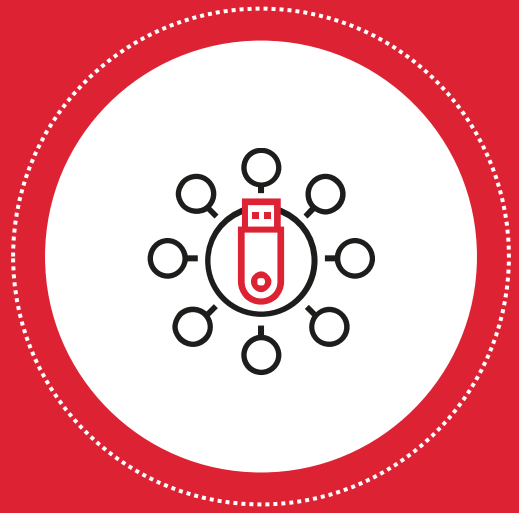
Обязательное применение активных ключевых носителей

# Федеральная налоговая служба

- Доступ к порталу через программные криптопровайдеры и при помощи активных ключевых носителей
- Единственный сертификат для руководителя, неэкспортируемый ключ подписи
- Обязательное применение ключевых носителей

# Активные ключевые носители момент можно и нужно применять ВЕЗДЕ!

**Поддержка в криптопровайдерах**



**Наделение полномочиями через МЧД**

**Поддержка стационарных и мобильных рабочих мест**

КОМПАНИЯ АКТИВ

# Владимир Иванов

Директор по развитию
Компания «Актив»


vov@rutoken.ru
info@rutoken.ru

+7 495 925-77-90

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