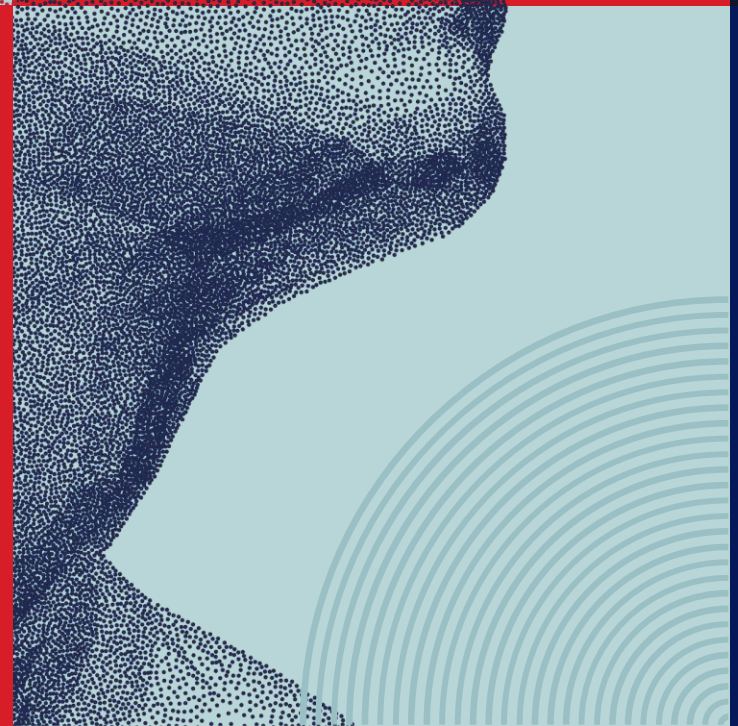
ТЕХНОЛОГИЧЕСКАЯ КОНФЕРЕНЦИЯ

РУТОКЕН DAY

ТЕХНОЛОГИИ ДОВЕРИЯ

КОМПАНИЯ АКТИВ

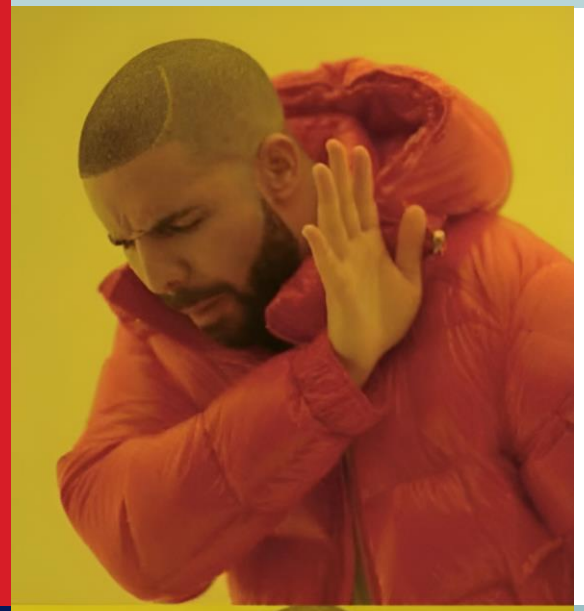


Особенности встраивания Рутокен с биометрическими технологиями

Дмитрий Мешков

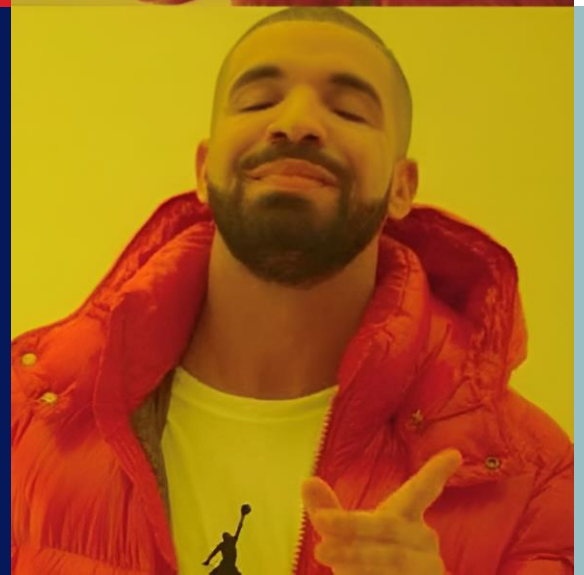
Руководитель отдела десктопной разработки, Компания «Актив»

Зачем использовать токены?

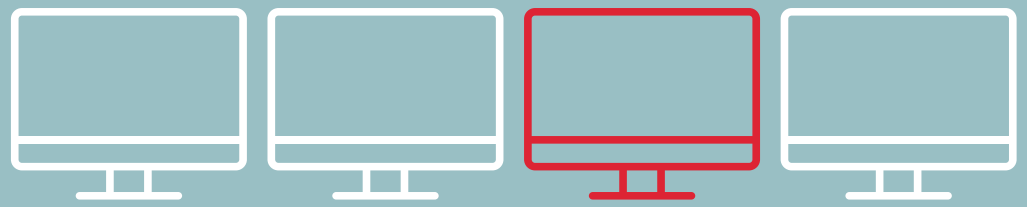


```
Meshkov@DESKTOP-OG24H4O MINGW64 ~/.ssh
$ file $(realpath *) | grep private
/c/Users/Meshkov/.ssh/id_ed25519:       OpenSSH private key
/c/Users/Meshkov/.ssh/id_rsa_d9:        OpenSSH private key
```

- Многофакторная аутентификация
- Безопасное хранение ключей



Дополнительный фактор



Привязка
к рабочему месту

Биометрическая
верификация

Постановка задачи

#1 Биометрическая верификация как дополнительный фактор доступа к закрытому ключу

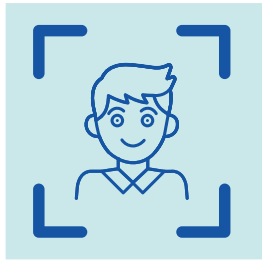
#2 Имеющаяся аппаратная база

#3 Новые задачи → новые программные компоненты

#4 Старые задачи → существующие программные компоненты

#5 Возможность близкого взаимодействия с интегратором

Распространенные виды биометрии



Изображение лица

Голос

Отпечаток пальца

Радужная оболочка глаза

Рисунок вен ладони

FSDK API: нейронные сети, интерфейс работы с отпечатками

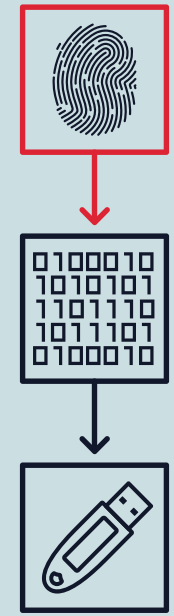
```
FSDK_API_ENTRY uint32_t FSDK_STDCALL PS_EnrollInit(FSDK_HANDLE* pHandle, fsdk_finger_position position,
                                                   size_t fingerprintsCountInTemplate);
FSDK_API_ENTRY uint32_t FSDK_STDCALL PS_EnrollUpdate(FSDK_HANDLE handle, const uint8_t* pImageBuf, size_t
imageWidth, size_t imageHeight);
FSDK_API_ENTRY uint32_t FSDK_STDCALL PS_EnrollFinal(FSDK_HANDLE handle, uint8_t* pTemplateBuf, size_t*
pTemplateSize);

FSDK_API_ENTRY uint32_t FSDK_STDCALL PS_EnrollGetCount(FSDK_HANDLE handle, size_t* pCount);
```

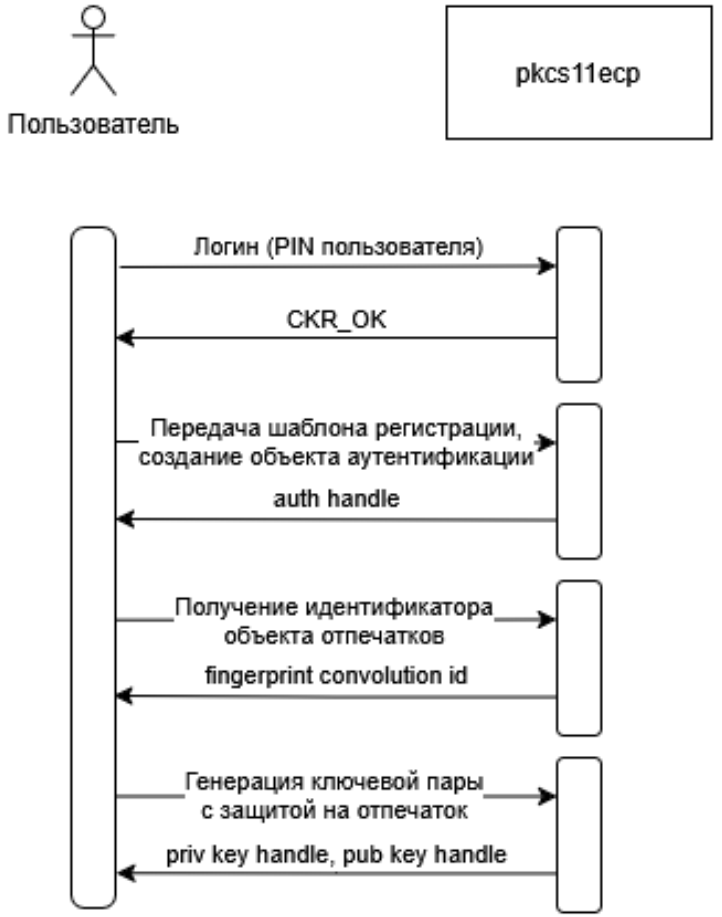
Регистрация

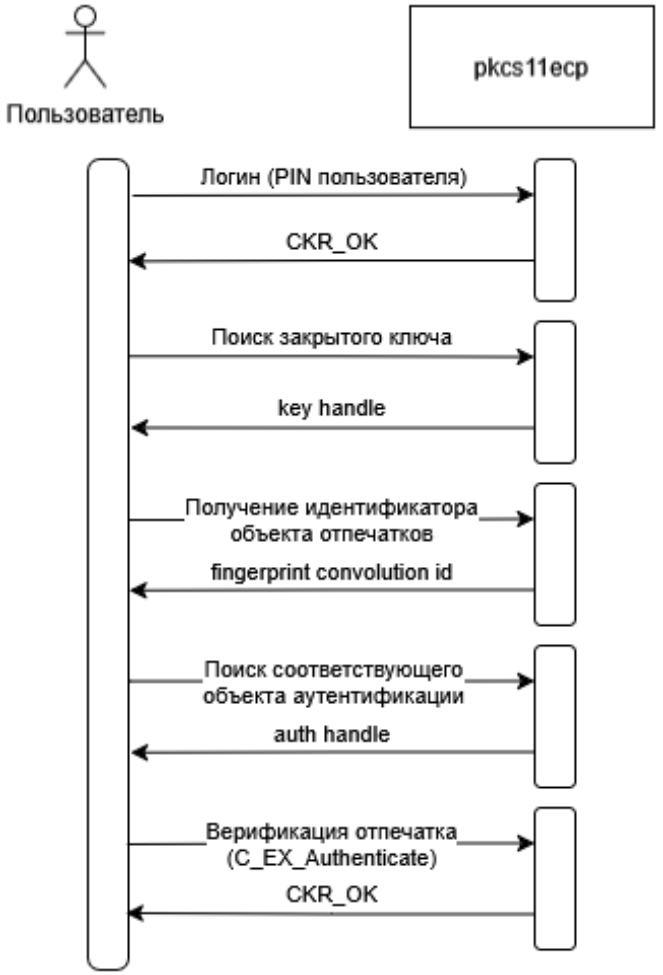
```
FSDK_API_ENTRY uint32_t FSDK_STDCALL PS_Enroll(const uint8_t* pImageBuf, size_t imageWidth, size_t imageHeight,
                                               uint8_t* pTemplateBuf, size_t* pTemplateSize);
```

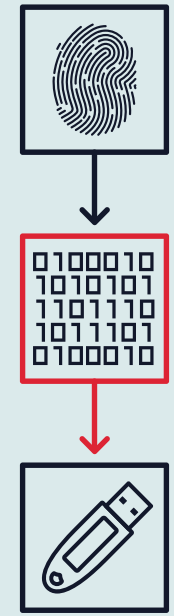
Верификация



Pkcs11ecp: транспорт, защита ключей





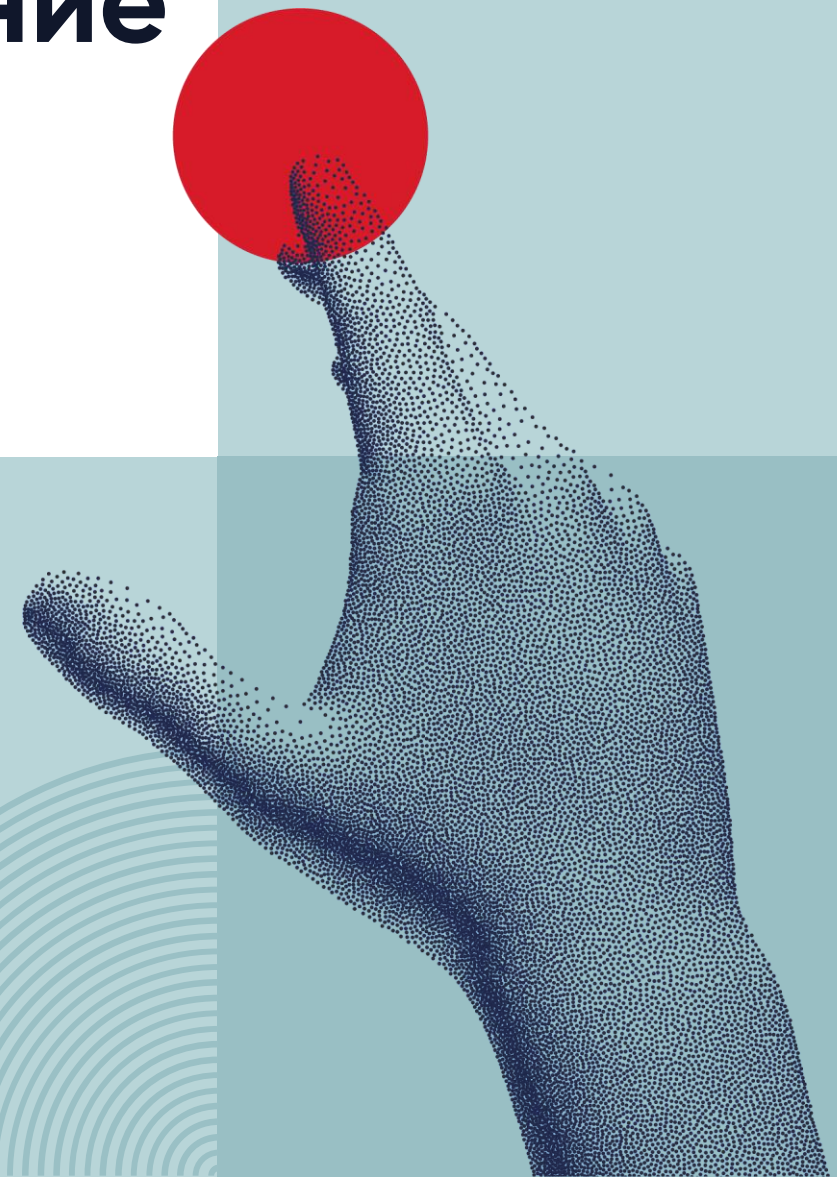


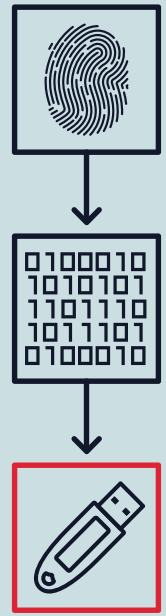
Генерация ключевой пары и создание отпечатка

Использование ключевой пары

Рутокен ЭЦП: хранение и сравнение отпечатков

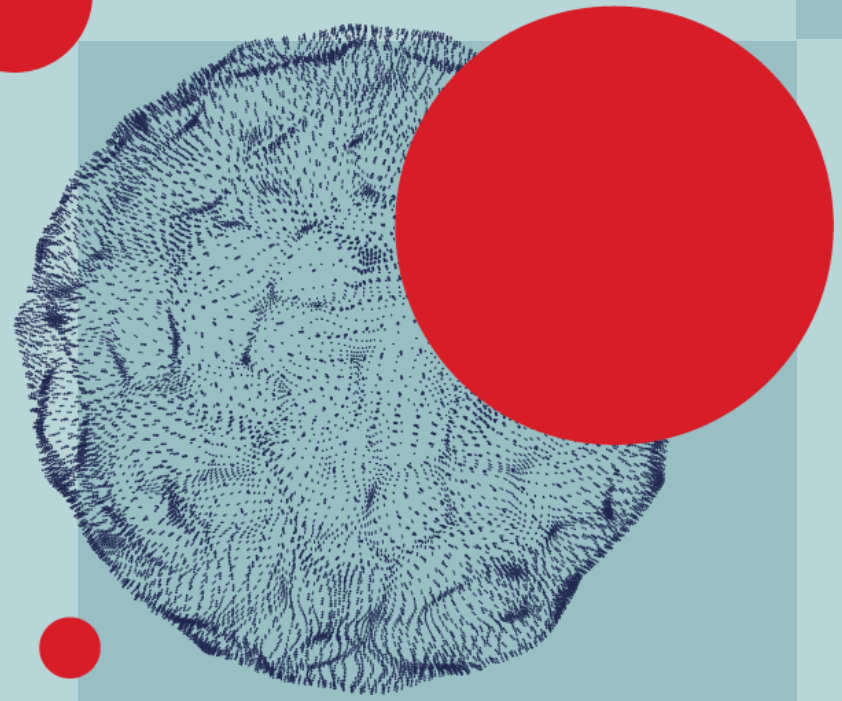
- Отпечатки пальцев неизвлекаемы
- Оптимизация проверок в условиях небольшого количества ресурсов
- Запоминание последней успешной верификации





Всё ли идеально?

- Необходимость отдельного нефиксированного считывателя отпечатков пальцев
- Невозможность использования сканеров смартфонов и лэптопов
- Vendor-defined расширение pkcs11ecp
- Pkcs11ecp – единственный доступный интерфейс для использования на данный момент



Развитие

Создание SDK

Добавление поддержки в продукты экосистемы

Лицевая биометрия

Рутокен со встроенным считывателем отпечатков

КОМПАНИЯ АКТИВ

РУТОКЕН DAY

Контактная информация

Дмитрий Мешков

Руководитель отдела десктопной разработки, Компания «Актив»

meshkov@rutoken.ru
info@rutoken.ru

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

+7 495 925-77-90