

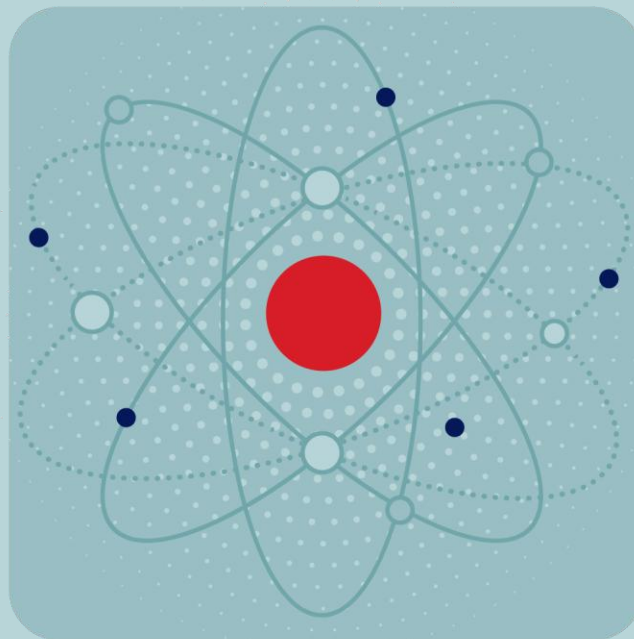
ТЕХНОЛОГИЧЕСКАЯ
ПАРТНЕРСКАЯ КОНФЕРЕНЦИЯ

РУТОКЕН

ОАЧ

ТЕХНОЛОГИИ

ДОВЕРИЯ



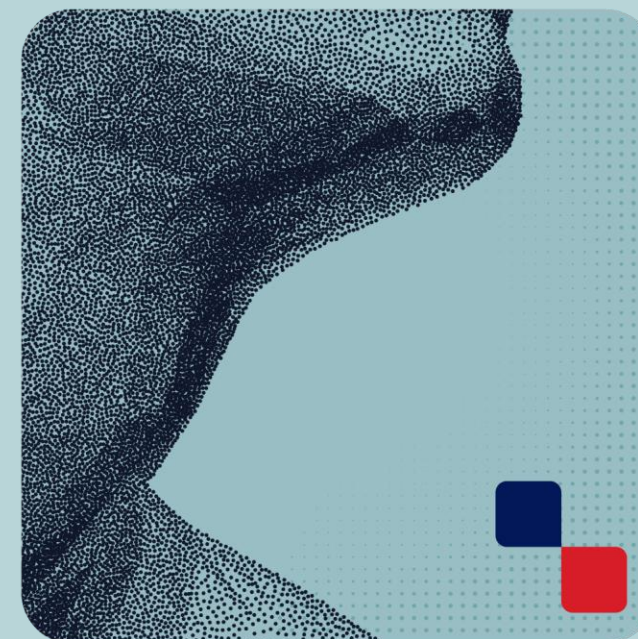
КОМПАНИЯ
ПРАКТИВ



Применение Рутокен БИО в классических сценариях ЭП

**Георгий
Крайнюков**

Программист,
отдел десктопной разработки,
Компания «Актив»



Преимущества и недостатки биометрии



Знание

- ✓ Пароль, ПИН-код, ответ на секретный вопрос
- ✓ Уязвимы к фишингу, кейлоггингу, AitM, подбору

Владение

- ✓ Смартфон, смарт-карта, токен
- ✓ Уязвимы к сниффингу, социальной инженерии

Свойство

- ✓ Отпечатки пальцев, проекция лица, электронный почерк
- ✓ Уязвим к утечке данных. Есть риск прохождения чужого отпечатка

Мультифакторная аутентификация = Фактор1 + Фактор2 + Фактор3 + ...



Что такое Рутокен БИО



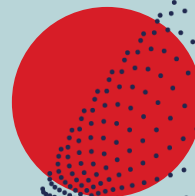
#1 Новые токены

#3 Новые функции PKCS#11

#5 BioSDK

#2 Новые библиотеки

#4 РтБиоАдмин



Токены Рутокен БИО



#1 Привычный Рутокен ЭЦП 3.0

#2 Защищенное хранение
эталонного
биометрического
шаблона



#3 Оптимизированное
сравнение отпечатков
пальцев

#4 Ограничение попыток
входа

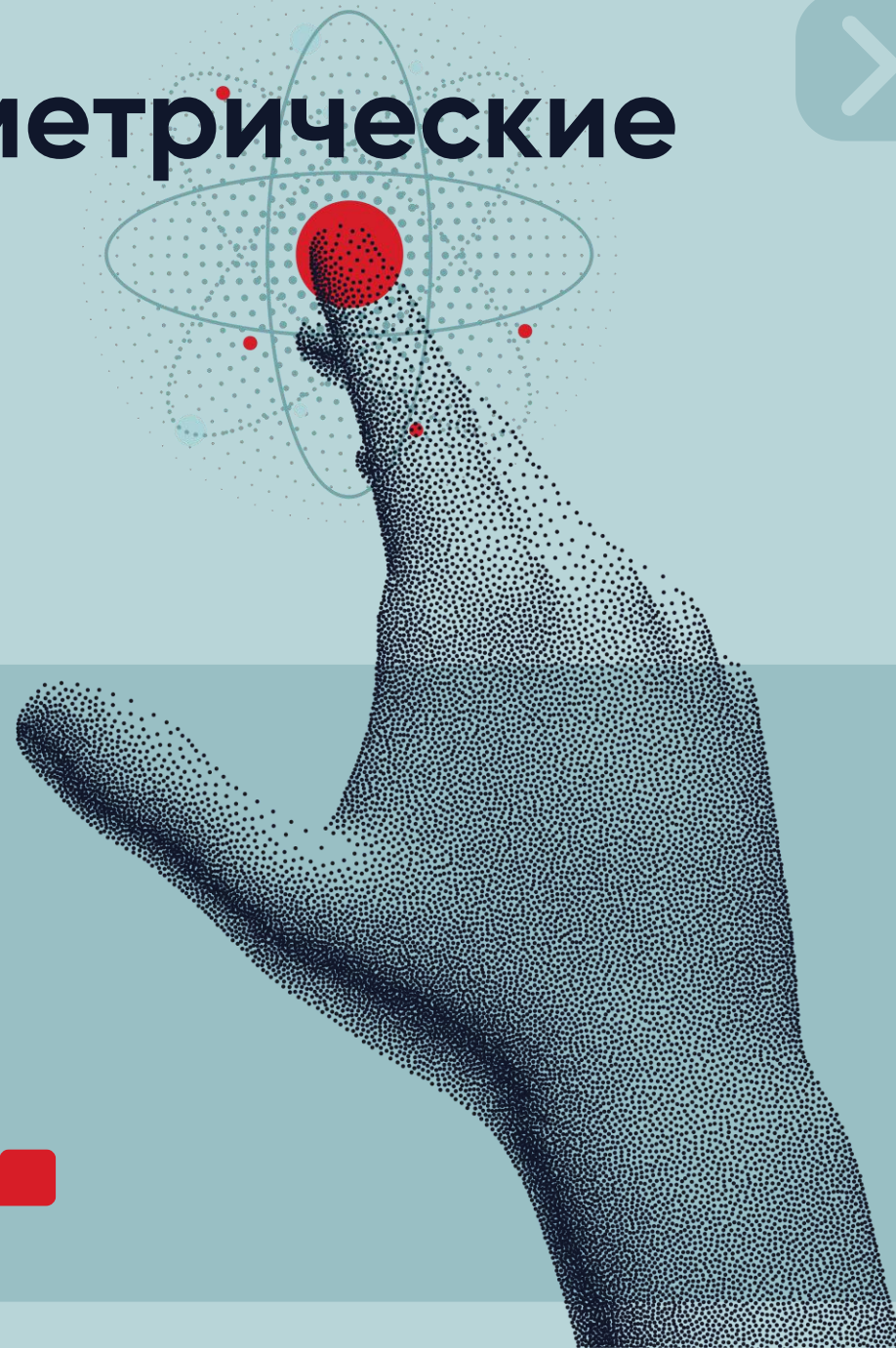


Программные биометрические КОМПОНЕНТЫ

FSSM

(Fingerprint Scanner
Support Module)

- ✓ Единый интерфейс для работы со сканерами отпечатков пальцев
- ✓ Изначальная поддержка популярных моделей
- ✓ Возможность реализации кастомных адаптеров для поддержки уже внедренных сканеров



Программные биометрические компоненты



FAPAPI
(Fingerprint API)

Создание комплексных
сверток из изображений
пальцев

Поддержка ISO/IEC
19794-2-2013

**Определение подлинности
отпечатков (антифейк):**

- слепки из эмульсии алифатической смолы
- кустарные копии пальца из пластилина типа «play-doh»

**Контроль качества
отпечатков:**

- отсеечение «плохих» отпечатков увеличивает скорость аутентификации и снижает количество отказов во входе
- вырабатывается привычка корректно прикладывать палец



Первоначальное внесение набора отпечатков пальцев

```
CK_VENDOR_BUFFER fingerprints[] = {
    { fingerprintByteArray1, sizeof(fingerprintByteArray1) },
    { fingerprintByteArray2, sizeof(fingerprintByteArray2) },
};
CK_ULONG fingerprintsCount = 2;
CK_ULONG maxRetryCount = 10;
```

```
const auto authObject = CKO_VENDOR_AUTHENTICATION_FACTOR;
const auto authType    = CKVAF_BIO_FP_CONVOLUTION;
CK_ATTRIBUTE fingerprintsTemplate[] = {
    { CKA_CLASS, &authObject, sizeof(authObject) },
    { CKA_VENDOR_AUTHENTICATION_FACTOR_TYPE, &authType, sizeof(authType) },
    { CKA_VENDOR_FP_CONVOLUTIONS_COUNT, &fingerprintsCount, sizeof(fingerprintsCount) },
    { CKA_VENDOR_FP_CONVOLUTIONS, &fingerprints, sizeof(fingerprints) },
    { CKA_VENDOR_MAX_RETRY_COUNT, &maxRetryCount, sizeof(maxRetryCount) },
};
```

```
rv = fList->C_CreateObject(..., fingerprintsTemplate, arraysize(fingerprintsTemplate),
                           &fingerprintsHandle);
```




Как отличается код для подписи

// Без биометрии

```
CK_RV rv;  
...  
rv = fList->C_OpenSession(...);  
...  
rv = fList->C_Login(...);  
...  
rv = functionList->C_Sign(...);
```



// С биометрией

```
CK_RV rv;  
...  
rv = fList->C_OpenSession(...);  
...  
rv = fList->C_Login(...);  
...  
// Найти объект отпечатков пальцев  
rv = fList->C_FindObjects(...);  
...  
// Аутентифицировать отпечатки пальцев  
rv = fListEx->C_EX_Authenticate(...);  
...  
rv = functionList->C_Sign(...);
```

BioSDK



- ✓ Инструкция по настройке сканеров
 - Futronic
 - ZKTeco
 - Papilon
 - Anviz
- ✓ Документация к модулям FSSM и FAPI
- ✓ Примеры кода PKCS#11, FSSM и FAPI

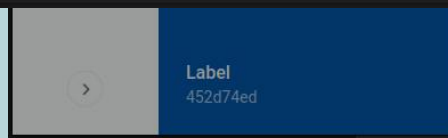
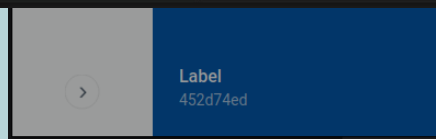
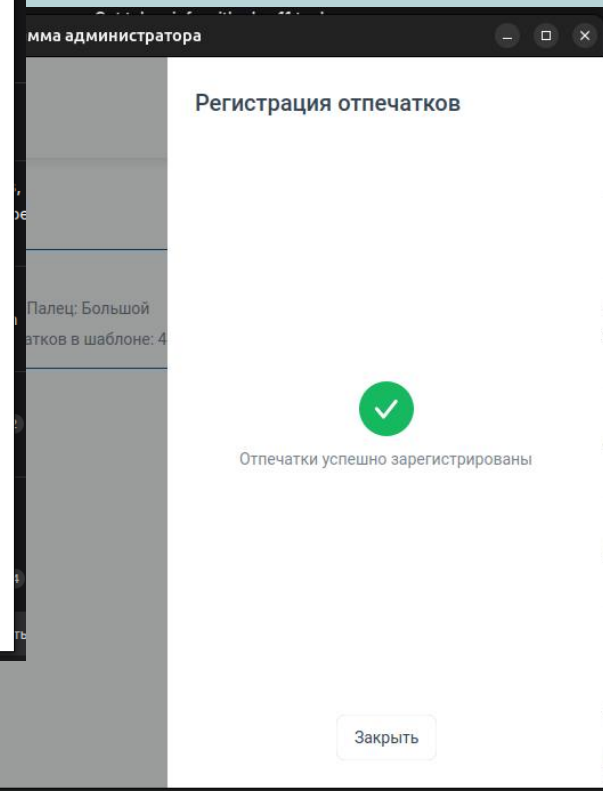
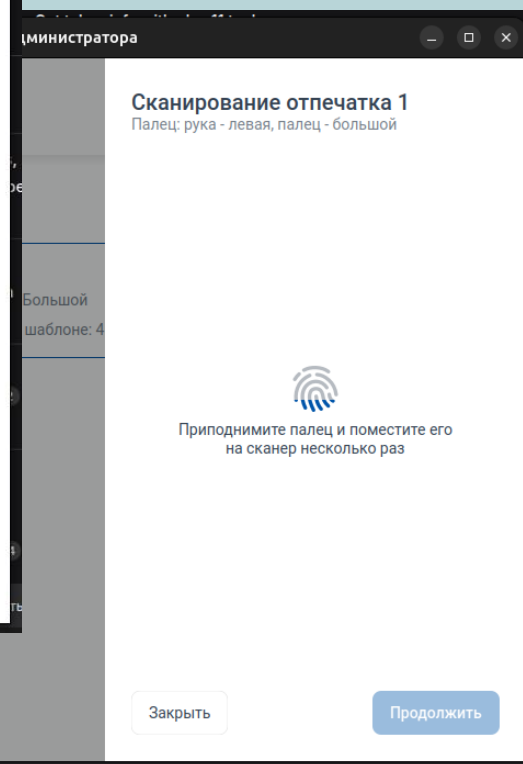
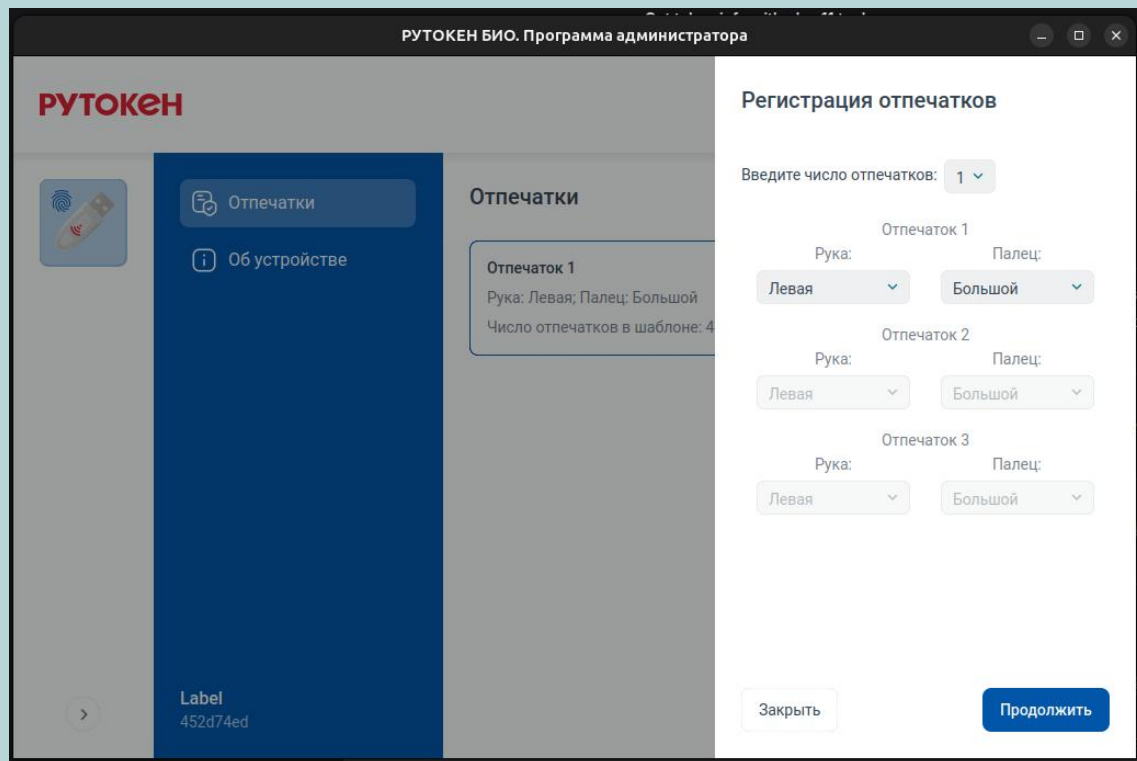


```

v docs
  Инструкция по настройк
  Описание утилиты FAPI.
  Описание утилиты FSSM.
  Примеры кода для BioSD
v fapi
  samples
    images
    include
      CMakeLists.txt
      Enroll.c
      EnrollUpdate.c
  fssm
  pkcs
    samples
      include
        BioCheckKeyPair.c
        BioCheckToken.c
        BioCreateKeyPair.c
        BioDeleteKeyPair.c
        BioGetInfo.c
        BioInitFingerprint.c
        BioResetAttempts.c
        BioUpdateFingerprint
        BioUseKeyPair.c
        CMakeLists.txt
NORMAL NvimTree_1
```



Приложение администратора



Перспективы



Рутокен Плагин



Рутокен Keybox



Центр управления Рутокен



Рутокен Логон для Linux



Прототип Рутокен БИО 2



**Контактная
информация**



**Георгий
Крайнюков**

Программист,
отдел десктопной разработки,
Компания «Актив»



Krajnyukov@rutoken.ru
info@rutoken.ru



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



+7 495 925-77-90