РУТОКЕН

КОМПАНИЯ АКТИВ

Новое поколение токенов с аутентификацией по отпечатку пальца

Содержание

Введение

В современном цифровом мире пароли или фактор знаний остаются основным, но все более уязвимым способом защиты доступа к данным и сервисам.

По данным отчета Verizon Data Breach Investigations Report (DBIR), за 2023 год большинство утечек безопасности связаны с плохой практикой управления паролями: их повторное использование, простота, хранение в незашифрованных файлах и т.д. Пользователи вынуждены запоминать сотни уникальных комбинаций, что приводит к привычке выбирать легкие, предсказуемые пароли или записывать их в открытом виде. В результате — повышенный риск компрометации, дорогостоящие инциденты и падение доверия к бренду.

Биометрическая аутентификация предлагает фундаментально иной подход: вместо того чтобы полагаться на «что-то, что вы знаете», она использует «что-то, что вы есть» — уникальные физические характеристики человека.

Технологии распознавания отпечатков пальцев демонстрируют высокую точность, удобство и устойчивость к фишинг-атакам. Перейдя от паролей к биометрии, организации могут существенно снизить уровень угроз, упростить пользовательский опыт и построить более надежную основу для будущих сервисов.

Дальнейшие разделы White Paper подробно рассмотрят текущие вызовы традиционных паролей, технологический прогресс в биометрической аутентификации и практические рекомендации по ее внедрению.

Проблемы и угрозы
использования традиционных средств защиты

Традиционные средства защиты обладают уязвимостями, которые ставят под угрозу безопасность данных и бизнес-процессов.

Фактор знаний

- Использование простых PIN-кодов
- Использование PIN-кодов по умолчанию
- Хранение PIN-кодов в легко доступных местах
- Использование одних и тех же PIN-кодов от разных устройств
- ПИН-коды редко меняются
- Возможность передачи третьему лицу

Получение доступа к токену третьими лицами

- Случайная утеря токена с компрометацией PIN-кода
- Несанкционированная передача токена в пользование третьим лицам

Вредоносное ПО

- Скрытный для пользователя ввод PIN-кода вредоносным ПО для совершения несанкционированных операций, например, ЭП или аутентификации в ИС злоумышленником. Присутствие легитимного пользователя при этом не требуется

Отличным решением этих проблем можно предложить использование технологии биометрической идентификации, верификации и аутентификации.

Использование биометрических технологий

Выбор типа биометрии

Ключевые биометрические технологии современного рынка: сканирование отпечатков пальцев, распознавание лица, голосовая аутентификация, идентификация по радужной оболочке глаза, венозный паттерн ладони и динамика поведения (подпись, походка, способ ввода текста). Каждая из них обладает своими преимуществами — бесконтактность у распознавания лица, простота интеграции у голосовых систем, высокий уровень защиты у сканирования радужки — но одновременно имеет и ограничения, такие как чувствительность к освещению, шуму, необходимость дорогостоящего оборудования или меньшую устойчивость к подделкам.

Пальчиковая биометрия занимает лидирующее положение на рынке:

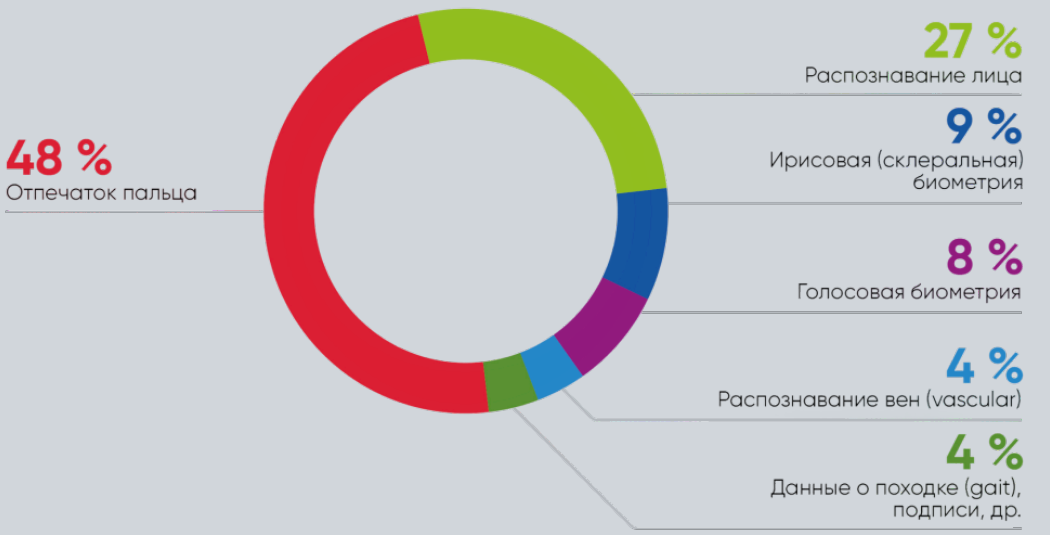


Рисунок 1. Доли рынка биометрических устройств по типу биометрии (2023-2024гг.)

Основные причины, по которым распознавание отпечатков пальцев является доминирующим биометрическим методом, используемым в коммерческих приложениях сегодня:

- Исключение для Единой биометрической системы (ЕБС, 572-ФЗ). Отпечатки пальцев не подпадают под нормативное регулирование и не требуют от Операторов ИС выстраивания взаимодействия с ЕБС
- Каждый отпечаток пальца обладает очень высоким уровнем уникальности, т.е. аутентификация является однозначной с высокой долей вероятности
- Отпечаток пальца обычно сохраняется на протяжении всей жизни человека
- Существующие технологии позволяют экономически эффективно считывать и измерять отпечаток пальца
- Считываемые параметры отпечатка пальца легко количественно оценить, что позволяет создавать эффективные алгоритмы сравнения отпечатков
- Ряд стандартов, касающихся распознавания отпечатков пальцев, уже действуют и создали основу для экономии за счет масштаба, т.е. снизили стоимость аппаратного и программного обеспечения

Преимущества этой технологии уже привели к широкому использованию сканеров отпечатков пальцев в мобильных устройствах, а также в платежных системах, системах доступа, в автомобильной индустрии, носимой и бытовой технике.

Как работает идентификация

Возможность идентификации по отпечатку пальца появляется благодаря его физиологическому строению. Бороздки на коже кончиков наших пальцев образуют уникальные узоры, которые отображаются на наших отпечатках пальцев. В биометрии узоры, образованные этими бороздками, называются минуциями.

Minutiae — латинское слово, обозначающее мелочи и незначительные детали

Примерами минуций являются окончания, пересечения, сердцевины и бифуркации гребней, как показано на рисунке:

Рисунок 2. Строение узора отпечатка пальца

Для получения отпечатков пальцев доступно несколько различных технологий — от ручных методов, традиционно используемых в криминалистике, до передовой активно-емкостной технологии. Уникальные характеристики отпечатка пальца могут быть считаны, например, оптическими, емкостными, ультразвуковыми, тепловыми или пьезоэлектрическими датчиками.

Биометрическая идентификация, верификация и аутентификация

Идентификация — процесс определения принадлежности предъявленных биометрических признаков (отпечатков пальцев) конкретному субъекту из базы данных информационной системы. При этом от системы ожидается один из ответов:

- Предъявленные признаки принадлежат такому-то субъекту
- Субъект не найден в базе данных

Биометрическая идентификация часто применяется в системах контроля и управления доступом (СКУД).

В идентификации существенную роль играет ошибка первого рода или вероятность принятия неавторизованного пользователя за легитимного (False Acceptance Rate, FAR). При сравнении с одним человеком вероятность 1 из 1000 нас устраивает, но, когда людей в базе данных много, большая вероятность, что эта ошибка может возникнуть для каждого из них.

Верификация — процесс сравнения предъявленных биометрических признаков с эталонными, заранее сохраненными на устройстве. При этом от устройства ожидается один из ответов:

- Верификация пройдена (успех) — предъявленный образец с достаточной степенью совпадения считается подлинным
- Верификация не пройдена (неуспех) — образец является подделкой

Верификация может использоваться сторонними приложениями или системами для принятия решения о дальнейших действиях с пользователем, например, для аутентификации и предоставлении доступа в приложение.

Аутентификация — процесс проверки личности по уникальным биологическим признакам человека с целью подтверждения его права доступа к ключевой информации на токене. При этом от токена ожидается один из ответов:

- Аутентификация пройдена — пользователь может получить доступ к ключевой информации
- Аутентификация не пройдена — личность не подтверждена, в доступе должно быть отказано

Факторы аутентификации

Способы аутентификации пользователя можно разделить на три основные категории, основанные на факторах аутентификации:

Не путать с многоэтапной аутентификацией, когда один и тот же фактор предъявляется несколько раз. Например, для входа на сайт пользователь вводит сначала пароль, потом код из СМС.
В данном случае это однофакторная (фактор знания) двухэтапная (пароль и код из СМС) аутентификация.

Фактор владения

Защищенное сертифицированное устройство для хранения ключевой информации

Фактор знания

Персональный ПИН-код для доступа к устройству с политикой качества

Фактор свойства

Отпечаток пальца — уникальное свойство владельца устройства

Каждый фактор аутентификации охватывает ряд элементов, используемых для аутентификации или проверки личности пользователя перед предоставлением доступа, одобрением запроса на транзакцию, подписанием документа, предоставлением полномочий другим лицам и т.д.

Безопасность или удобство (FAR или FRR)

Безопасность — ключевой критерий, который следует учитывать при сравнении систем биометрической аутентификации.

Но, как всегда, необходимо учитывать компромисс между высокой безопасностью и удобством пользователя.

Ни одна система не может быть абсолютно безопасной — имея неограниченные ресурсы (время и деньги), злоумышленник можете взломать и подделать что угодно.

Однако обнаружение активности и другие передовые биометрические методы делают такие вредоносные атаки дорогостоящими.

Ошибка первого рода или False Acceptance Rate (FAR)

Метрикой, часто используемой при оценке безопасности биометрических систем, является коэффициент ложного срабатывания FAR (иногда называемый FMR, False Match Rate).

Значение FAR показывает, как часто датчик статистически выдает положительное совпадение без правильных биометрических данных.

Коэффициент FAR зависит как от аппаратного, так и от программного обеспечения (алгоритма) биометрической системы.

Типичный коэффициент FAR сканеров отпечатков пальцев, используемых в современных смартфонах, составляет около 1/100 000, что, по сути, означает, что, если вы позволите случайно выбранным людям попытаться войти в ваш телефон с помощью сканера отпечатков пальцев, в среднем одному из 100 000 это удастся.

Значение FAR может варьироваться в зависимости от алгоритма и условий работы системы.

В режиме верификации — FAR 0,001% (один шанс из 100 000).

В режиме идентификации FAR увеличивается пропорционально количеству человек в базе данных системы при той же чувствительности (FRR). Например, если при FRR 1,3% лучший пальцевой сканер в режиме верификации обеспечивает FAR 0,001%, то в режиме идентификации при том же FRR и базе данных в 10 000 человек FAR составляет 10% (один шанс из 10), что уже недопустимо для большинства приложений.

Ошибка второго рода или False Rejection Rate (FRR)

Метрикой, часто используемой для оценки удобства биометрических систем, является коэффициент ложного отклонения (FRR) (также FNMR, False Non-Match Rate).

FRR показывает, как часто система ошибочно отклоняет легитимный биометрический признак в алгоритме сопоставления. Удобство также связано с другими характеристиками системы, такими как: насколько интуитивно понятно ее использование, скорость активации или какие действия требуются для активации датчика, а также как датчик интегрирован в конечный продукт, хотя это скорее следствие размера и гибкости конструкции датчика.

График зависимости коэффициента FRR от коэффициента FAR для различных типов биометрических систем аутентификации дает представление о компромиссах между безопасностью и удобством.

Идеальный датчик имеет минимальные FAR и FRR, но в реальности системы биометрической аутентификации находятся где-то на кривой, где либо высокое удобство (низкий FRR), но более низкая безопасность (высокий FAR), либо наоборот, см. рисунок 3.

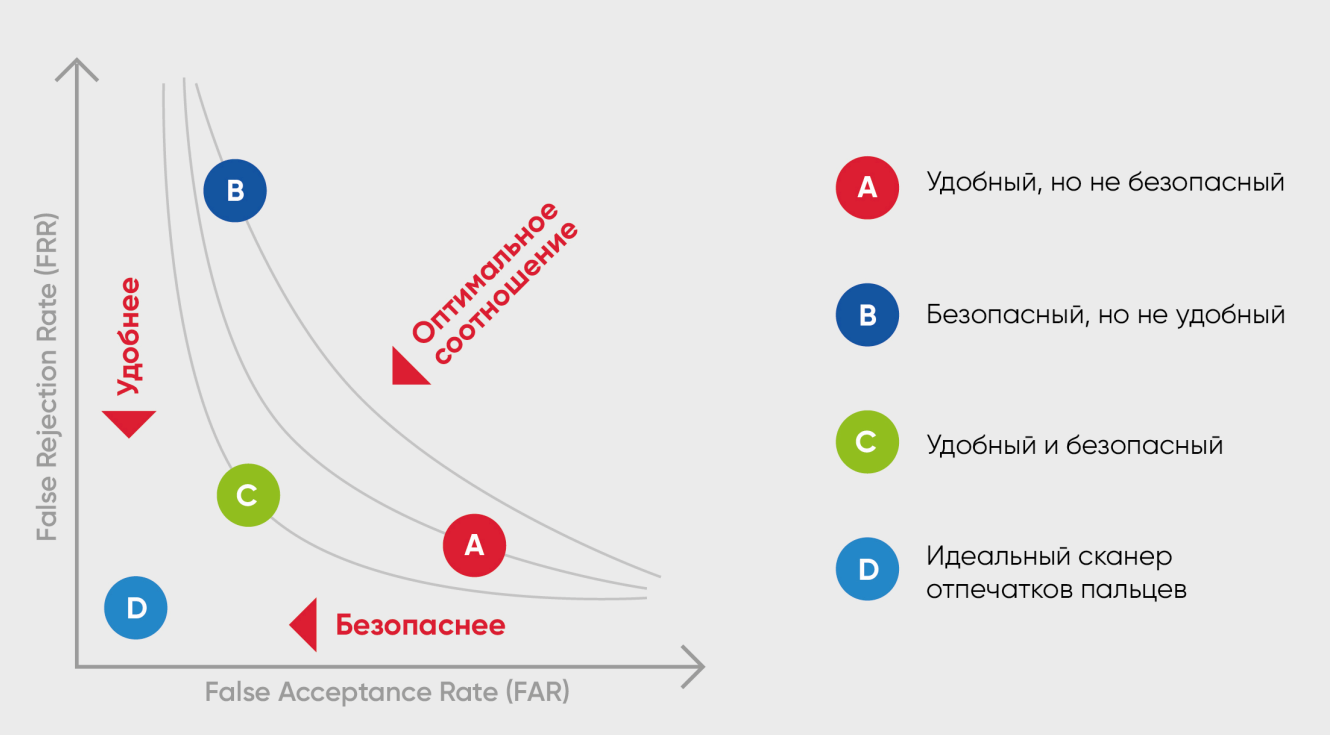


Рисунок 3. Иллюстрация компромисса между безопасностью и удобством

Рутокен ЭЦП 3.0
3250 (БИО)

Рутокен ЭЦП 3.0 3250 (БИО) — это устройство линейки Рутокен ЭЦП 3.0 с средством биометрической верификации пользователя для совершения операций с электронной подписью или аутентификации в ИС с помощью отпечатка пальца.

Является отдельным исполнением (несколько моделей USB-токенов) в рамках сертифицированного СКЗИ Рутокен ЭЦП 3.0.

Преимущества

Поддержка сканеров отпечатков пальцев, соответствующих высоким требованиям безопасности:

- Высокое разрешение изображения — от 500 dpi
- Размер изображения — не менее 260×300 pixels
- Соответствие требованиям к изображениям отпечатка пальца по **ГОСТ Р 58298–2018** (ISO/IEC 19794–4:2011)
- Использование технологий «Распознавание живого пальца» для предотвращения попыток несанкционированного доступа при помощи использования муляжа отпечатка пальца, сделанного из силикона, резины и т. д

Практически все встраиваемые сканеры отпечатков пальцев не соответствуют данным требованиям безопасности

Регистрация отпечатков пальцев пользователя возможна только администратором с использованием специального ПО.

Эталонные биометрические шаблоны хранятся внутри устройства Рутокен БИО в формате ГОСТ Р ИСО/МЭК 19794–2-2013.

Сравнение предъявляемого шаблона с эталонным также происходит на сертифицированном устройстве.

Привязка эталонного биометрического шаблона к конкретной ключевой паре происходит в момент ее создания и является опциональной, что позволяет реализовать разные способы аутентификации для разных сценариев использования устройства. Изменить параметры аутентификации для ключевой пары невозможно.

Для каждой операции с использованием ключей, привязанных к биометрии, требуется биометрическая аутентификация пользователя. Исключает возможность выполнения скрытых операций вредоносным ПО после однократной аутентификации на устройстве.

После регистрации отпечатков пальцев на устройстве их невозможно изменить или извлечь.

Логика работы с биометрическими шаблонами отпечатков пальцев реализована на уровне Рутокен ОС.

Архитектура решения

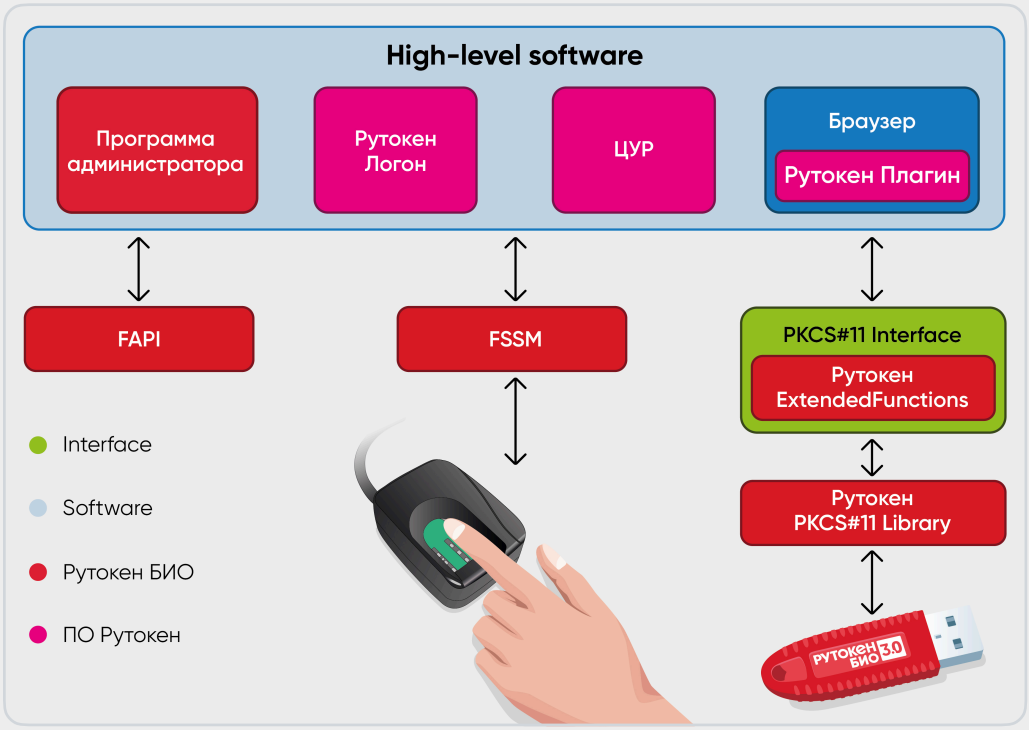


Схема 1. Взаимодействие и использование биометрических функций через BioSDK

Состав продукта

Устройство Рутокен ЭЦП 3.0 3250 (БИО) предназначено для защищенного хранения эталонного биометрического шаблона и сравнения с предъявляемым (биометрическая верификация).

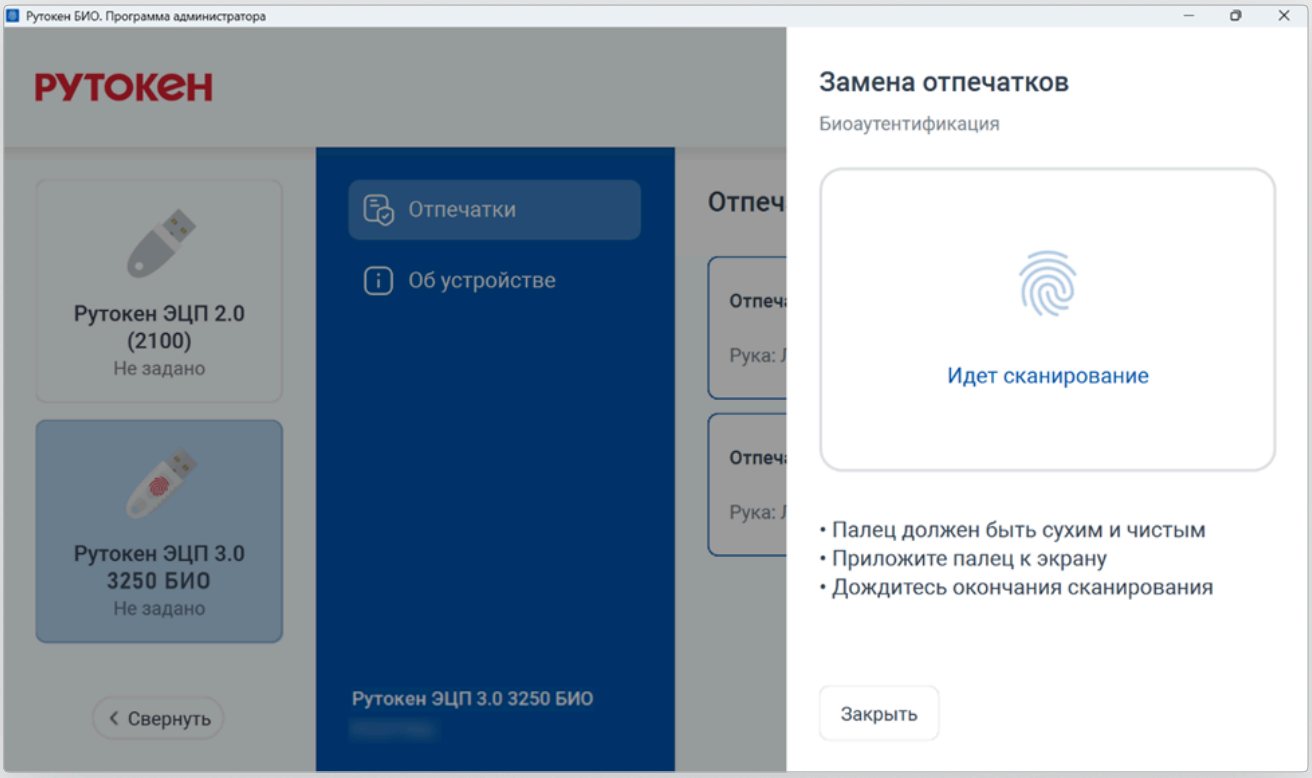
Возможные форм-факторы:

Классический

Миниатюрный USB-C

Micro

Программа администратора (ПО Admin) – это программное обеспечение с графическим интерфейсом, предназначенное для администрирования устройств Рутокен, поддерживающих биометрическую аутентификацию.



Основные функции программы:

- Регистрация (до 3-х), обновление отпечатков пальцев
- Разблокировка биометрической аутентификации
- Просмотр информации о зарегистрированных отпечатках пальцев
- Просмотр информации о подключенных устройствах
- Просмотр поддерживаемых и подключенных сканеров отпечатков пальцев
- Выгрузка логов работы программы

Программа поддерживается в системах:

- Windows 10/11 (x86-64)
- семейства Linux:
  - Astra Linux Special Edition (все сертифицированные и поддерживаемые версии) x86–64
  - Альт Рабочая станция 1×6–64
  - Альт 8 СП x86-64
  - РЕД ОС (сертифицированная редакция) x86–64
  - РЕД ОС 8 (рабочая станция) x86–64

BioSDK — это программный инструментарий, который позволяет разработчикам программного обеспечения интегрировать биометрические функции для работы с устройством Рутокен БИО в различные приложения.

Состав BioSDK:

- SDK PKCS#11 в части биометрии
- библиотеки FAPI, FSSM и BioLib
- Документация (описание библиотек и инструкции по их использованию)

- Тестовые утилиты
- Примеры кода

BioSDK использует библиотеки FAPI и FSSM для взаимодействия с интегрированным приложением. Ссылаясь на эти библиотеки, разработчики программного обеспечения могут использовать функциональность отпечатков пальцев в нужном приложении.

FAPI (Fingerpritn API) — библиотека, предназначенная для работы с биометрией. Назначение:

- Создание биометрических шаблонов из изображений пальца, полученных со сканера
- Поддержка шаблона ISO/IEC 19794–1-2013
- Определение подлинности отпечатков (антифейк)
- Контроль качества отпечатков

FSSM (Fingerprint Scanner Support Module) — модуль поддержки сканеров отпечатков пальцев.

Это динамически подключаемая библиотека, предоставляющая унифицированный интерфейс для взаимодействия с различными сканерами отпечатков пальцев от разных производителей для получения изображения необходимого качества.

BioLib — библиотека высокоуровневых команд, вызывающая низкоуровневые FSSM и FAPI.

Поддерживаемые сканеры

Для получения изображения отпечатка пальца высокого качества необходим сканер, отвечающий требованиям безопасности и **ГОСТ Р 58298–2018**:

- ZKTeco SLK20R

- ZKTeco ZK9500
- Futronic FS-80H
- Futronic FS26
- Futronic FS10 1 "x1"
- Anviz U Bio Reader
- И другие

Перечень неокончательный и будет расширяться.

В перечне представлены оптические или емкостные сканеры с подключением к рабочему месту пользователя или администратора через USB-порт.

Подробная информация по поддерживаемым сканерам доступна в Приложении Б.

Если нужного сканера на текущий момент нет в перечне поддерживаемых, то есть два варианта:

- Обратиться в Компанию «Актив». Компания подготовит необходимое обновление и обеспечит поддержку нового сканера
- Разработать плагин поддержки нового сканера самостоятельно и подключить его к FSSM по инструкции из комплекта документации разработчика BioSDK

Сертификаты

Сертификат ФСБ России № СФ/124–5011 от 30 октября 2024 г.

Сертификат ФСТЭК — в процессе. Включен в Реестр российской промышленной продукции (ПП РФ 719 от 17.07.2015):

- **Продукция российского происхождения**, номер реестровой записи — **10633367**
- Включен в Единый реестр российской радиоэлектронной продукции (ПП РФ 878)

Рекомендуемое ПО

- **Рутокен Логон для Linux** — средство для входа в операционную системы при помощи безопасной биометрической аутентификации
- **Рутокен Плагин** — модуль для связи устройств Рутокен БИО с браузером, он позволяет опознавать устройства и работать с ними
- **Центр управления Рутокен (ЦУР)** — инструмент администрирования и управления устройствами из линеек Рутокен ЭЦП и Рутокен Lite
- **Рутокен KeyBox** — централизованная система управления инфраструктурой открытых ключей
- **КриптоПро CSP** — ГОСТ-криптопровайдер с поддержкой биометрических операций
- **Secret Net Studio** — комплексная система защиты с возможностью использования токенов для биометрической аутентификации

Принципы работы биометрической системы

Особенности регистрации отпечатков пальцев

Процесс регистрации состоит из последовательных этапов:

- **Сбор биометрических данных** — для записи в токен собираются данные трех разных пальцев, по четыре отпечатка в каждом

- **Формирование биометрических шаблонов** — при занесении отпечатков происходит их анализ и математическая обработка
- **Сохранение шаблонов** — на финальном этапе в устройство записываются шаблоны пальцев в формате **ГОСТ Р ИСО/МЭК 19794-2-2013**

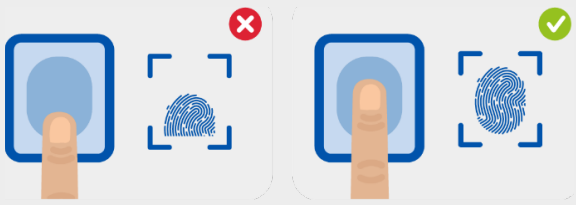
Механизмы, заложенные в архитектуру ОС Рутокен

- Ключевая пара привязывается к отпечаткам в момент ее создания
- Доступ к закрытому ключу предоставляется только при предъявлении отпечатка зарегистрированного пальца и PIN-кода
- После регистрации не допускается извлечение, изменение или удаление отпечатков из устройства
- Верификация биометрических данных происходит полностью на борту устройства

Механизмы устойчивости к атакам и улучшения пользовательского опыта

В состав Fingerprint API устройств Рутокен ЭЦП 3.0 с биометрическими механизмами входят две предобученные нейросети:

- **Нейросеть «КПП»**



Контроль качества прикладывания пальца.

Нейросеть распознает качество прикладывания пальца, отсекает случаи, когда предъявлен частичный отпечаток или палец приложен недостаточно плотно — в таком случае требуется повторить прикладывание.

- **Нейросеть «Антифейк»**

Реальный отпечаток

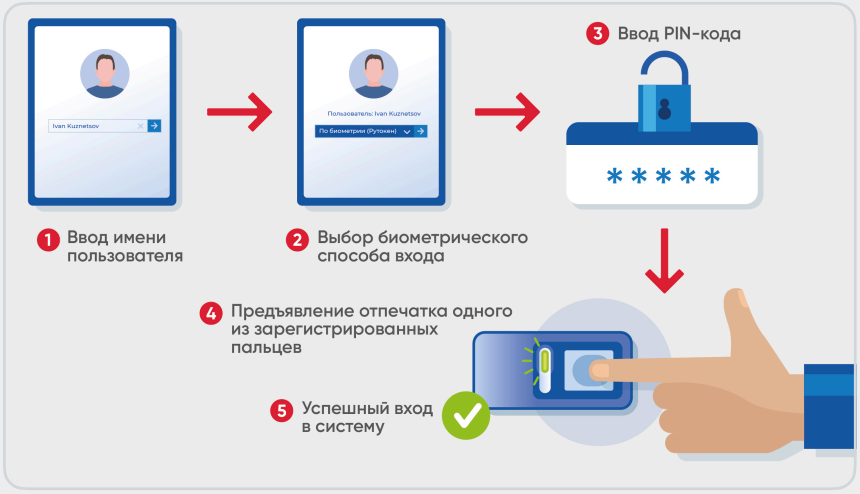
Силиконовая накладка

Выявление недостоверных отпечатков пальца.

Нейросеть отличает реальные отпечатки пальцев от некоторых разновидностей подделок: силиконовые накладки, слепки из эмульсии алифатической смолы, копии пальца из пластилина типа «play-doh», желатиновые слепки и другие.

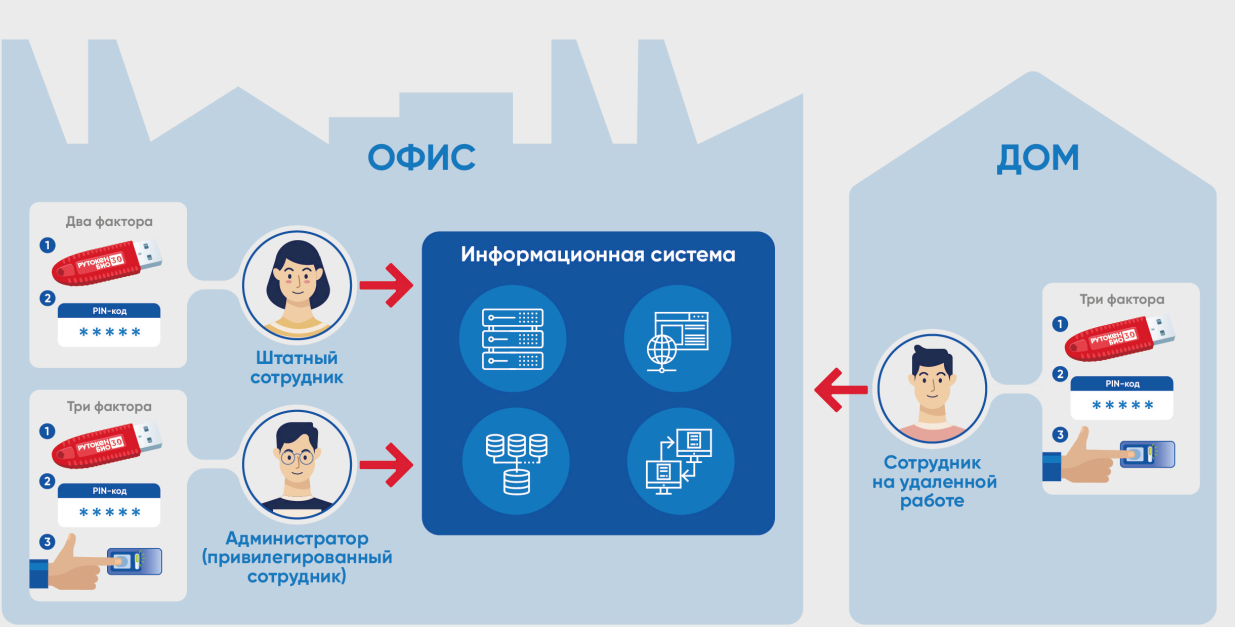
Сценарии использования

Трехфакторная аутентификация в ИС



Электронная подпись по пальцу

Способ аутентификации в зависимости от рисков



Рутокен БИО позволяет реализовать адаптивную аутентификацию на основе рисков. Как пример, администратор ИС может сгенерировать на ключевом носителе пользователя Рутокен ЭЦП 3.0 3250 (БИО) несколько ключевых пар с разными параметрами аутентификации для каждой пары в зависимости от сценария их использования.

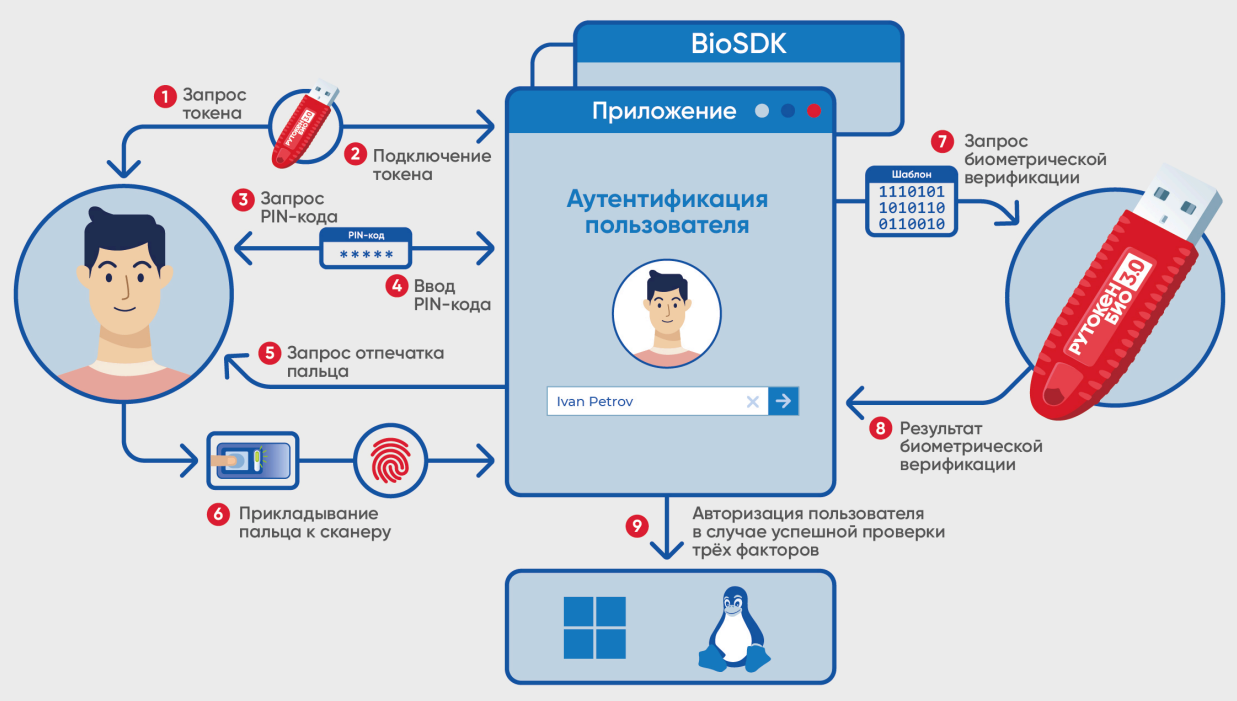
Подключение пользователя к корпоративной ИС:

- из дома по VPN — ключевая пара № 1 с привязкой к биометрических данным пользователя
- из офиса — ключевая пара № 2 без привязки к биометрических данным пользователя

В данном случае пользователю для аутентификации в ИС из офиса достаточно будет предъявить токен и ввести PIN-код, а для доступа к ИС из дома нужно будет дополнительно пройти биометрическую аутентификацию, но устройство в обоих случаях будет одно — Рутокен БИО.

Таким образом можно регулировать требования к аутентификации пользователя в зависимости от критичности данных и точки входа в информационную систему, обеспечивая принципы концепции Zero-Trust.

Биометрическая верификация для внешнего приложения



Устройство Рутокен БИО и BioSDK позволяет разработчику программного обеспечения проводить биометрическую верификацию внутри токена и передавать результат своему приложению для реализации аутентификации или подписи документа по биометрическому признаку.

1. Приложение запрашивает подключения токена к компьютеру
2. Пользователь подключает Рутокен БИО
3. Приложение запрашивает ПИН-код от Рутокен БИО
4. Пользователь вводит ПИН-код
5. Приложение запрашивает у пользователя отпечаток пальца
6. Пользователь предъявляет свой отпечаток
7. Приложение, используя BioSDK, получает изображение со сканера, формирует из него шаблон и передает его в устройство Рутокен БИО
8. Рутокен БИО проводит биометрическую верификацию и возвращает результат приложению

9. Приложение обрабатывает результат, полученный от устройства, и например, принимает решение об авторизации пользователя в приложение в зависимости от результата верификации

Приложение А.

Техническая спецификация Рутокен ЭЦП 3.0 3250

Биометрическая система

- Количество пальцев: до 3 пальцев
- Количество отпечатков одного пальца: 4 отпечатка
- Среднее время биометрической верификации: < 1 с
- Роли: администратор и пользователь
- Стандарт хранения биометрического шаблона: ГОСТ Р ИСО/МЭК 19794–2-2013

Аппаратные криптографические возможности

- ГОСТ Р 34.10–2001 генерация ключевых пар с проверкой качества, формирование и проверка электронной подписи, срок действия закрытых ключей до 3-х лет
- ГОСТ Р 34.10–2012/ГОСТ 34.10–2018 (256 и 512 бит): генерация ключевых пар с проверкой качества, формирование и проверка электронной подписи, срок действия закрытых ключей до 3-х лет
- ГОСТ Р 34.11–94: вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования ЭП
- ГОСТ Р 34.11–2012/ГОСТ 34.11–2018 (256 и 512 бит): вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования ЭП
- ГОСТ 28147–89: генерация ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ)

- ГОСТ Р 34.12-2015/ГОСТ 34.12-2018, ГОСТ Р 34.13-2015/ГОСТ 34.13-2018 (Кузнечик): генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ)
- ГОСТ Р 34.12-2015/ГОСТ 34.12-2018, ГОСТ Р 34.13-2015/ГОСТ 34.13-2018 (Магма): генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ)
- Выработка сессионных ключей (ключей парной связи):
  - по схеме VKO GOST R 34.10-2001 (RFC 4357)
  - по схеме VKO GOST R 34.10-2012 (RFC 7836)
  - расшифрование по схеме EC El-Gamal
- RSA: поддержка ключей размером 1024, 2048, 4096 бит, генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи
- ECDSA с кривыми secp256k1, secp256r1 и secp384r1 , secp521r1 : генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи
- Генерация последовательности случайных чисел требуемой длины

Возможности аутентификации владельца

- Двухфакторная аутентификация: по предъявлению самого идентификатора и по предъявлению уникального PIN-кода
- Поддержка 3 категорий владельцев: Администратор, Пользователь, Гость
- Поддержка 2-х глобальных PIN-кодов: Администратора и Пользователя
- Поддержка локальных PIN-кодов для защиты конкретных объектов (например, контейнеров сертификатов) в памяти устройства

- Настраиваемые аппаратные политики качества PIN-кодов, обрабатываются микропрограммой при соответствующих операциях. Устанавливаются при форматировании, опционально могут изменяться позднее по PIN-коду Администратора
- Варианты политик:
  - ограничение минимальной длины PIN-кода
  - ограничение использования PIN-кода по умолчанию
  - запрет PIN-кода, состоящего из одного повторяющегося символа
  - независимые требования по наличию в PIN-коде: прописных, строчных букв латинского и русского алфавитов; цифр; специальных символов
  - запоминание до 10 устанавливаемых значений PIN-кода, и возможность запрета установки ранее использованного PIN-кода
- Поддержка комбинированной аутентификации: по схеме «Администратор или Пользователь» и аутентификация по глобальным PIN-кодам в сочетании с аутентификацией по локальным PIN-кодам
- Создание локальных PIN-кодов для дополнительной защиты части ключевой информации, хранящейся на USB-токене. Возможность одновременной работы с несколькими локальными PIN-кодами (до 7 шт)
- Ограничение числа попыток ввода PIN-кода
- Индикация факта смены глобальных PIN-кодов с PIN кодов по умолчанию на оригинальные

Файловая система

- Встроенная файловая структура по ISO/IEC 7816-4
- Число файловых объектов внутри папки — до 255 включительно
- Использование File Allocation Table (FAT) для оптимального размещения файловых объектов в памяти
- Уровень вложенности папок ограничен объемом свободной памяти для файловой системы
- Хранение закрытых и симметричных ключей без возможности их экспорта из устройства

- Использование Security Environment для удобной настройки параметров криптографических операций
- Использование файлов Rutoken Special File (RSF-файлов) для хранения ключевой информации: ключей шифрования, сертификатов и т.п.
- Использование предопределенных папок для хранения разных видов ключевой информации с автоматическим выбором нужной папки при создании и использовании RSF-файлов
- Возможность изменения политики смены ПИН-кода пользователя. Смена может быть доступна Пользователю, Администратору или обеим ролям одновременно

Интерфейсы

- Стандартные протоколы обмена:
  - ISO/IEC 7816-12
  - ISO 14443 (NFC) для бесконтактной микросхемы
- Поддержка USB CCID: работа без установки драйверов устройства в современных версиях ОС
- Поддержка PC/SC
- Microsoft Crypto API
- Microsoft SmartCard API
- PKCS#11 (включая российский профиль)

Встроенный контроль и индикация

- Контроль целостности микропрограммы (прошивки) Рутокен ЭЦП
- Контроль целостности системных областей памяти
- Проверка целостности RSF-файлов перед любым их использованием
- Счетчики изменений в файловой структуре и изменений любых PIN-кодов для контроля несанкционированных изменений
- Проверка правильности функционирования криптографических алгоритмов

Общие характеристики

- Современный защищенный микроконтроллер
- Идентификация с помощью 32-битного уникального серийного номера
- Поддержка операционных систем:
  - Microsoft Windows 2022/11/10/8.1/2019/2016/2012R2/8/2012/7/2008R2
  - GNU/Linux, в том числе отечественные
  - Apple macOS 10.13 и новее
  - Android 7 и новее
  - iOS 13 и новее (iPhone XR, XS, XS Max и новее)
    Только для моделей с NFC
  - iOS/iPadOS 16.2 и новее
    При контактном подключении
  - Аврора 4+
- EEPROM память 128 КБ
- Интерфейс USB 1.1 и выше
- Размеры 58x16x8мм для USB-A и 52x16x8мм для USB-C
- Масса 6,3 г.

Специальные возможности

- Журналирование операций электронной подписи, сформированных по ГОСТ-алгоритмам, фиксация параметров электронной подписи и окружения
- Ведение неубывающего счетчика операций электронной подписи в рамках журнала
- Доверенное получение журнала, подтвержденное электронной подписью

Приложение Б.
Поддерживаемые сканеры

Модель	Фото	Отличительные признаки
Futronic FS-80H		FS-80H поддерживает технологию «Распознавание живого пальца»
Futronic FS26		Оптический сканер отпечатков пальцев, который имеет встроенный бесконтактный считыватель и запись карт MIFARE
Futronic FS10 1 "x1"		Профессиональный сканер отпечатков пальца от компании Futronic со сканирующей областью 25. × 5.4 мм
ZKTeco SLK20R		Защита от поддельных отпечатков пальцев. ТОП-3 по популярности в России

Модель	Фото	Отличительные признаки
ZKTeco ZK9500		Шифрование данных при передаче через USB-интерфейс. ТОП-3 по популярности в России
Папилон ДС-21С		Входит в реестр российской промышленной продукции Минпромторга (ПП РФ № 719)
Anviz U Bio Reader		Популярный сканер