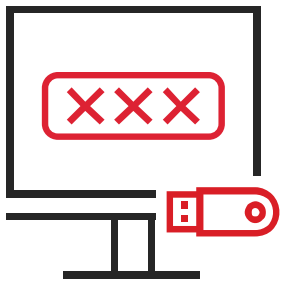
РУТОКЕН

Решения «Рутокен» для электронной подписи и двухфакторной аутентификации в информационные системы



Андрей Шпаков,
Руководитель проектов по информационной безопасности
Компания «Актив»

Компания «Актив»

На рынке информационной безопасности с 1994 года

Имеем все необходимые лицензии на разработку СКЗИ и СЗИ

Являемся членом АЗИ, РОСЭУ, ТК26, РусКрипто, ISDEF

Входим в 20 крупнейших ИБ-компаний в России

Участвуем в международных и российских криптографических конференциях

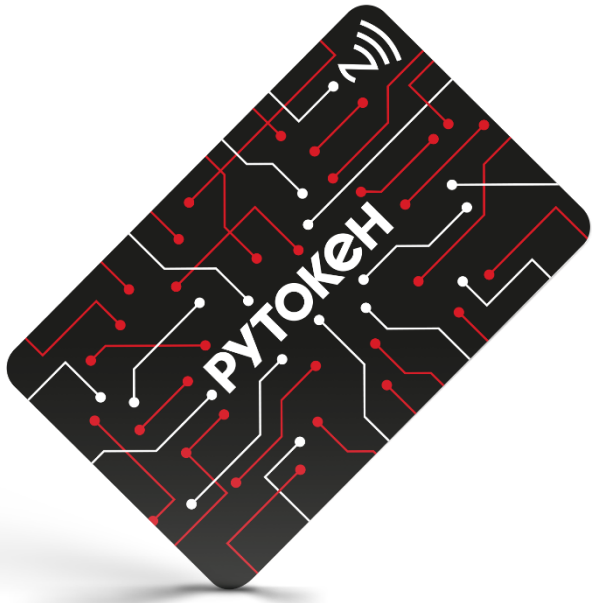
Приятные факты

- Производитель токенов и смарт-карт **#1 в России**
- ПО, драйверы и карточная система Рутокен ОС — **в едином реестре Минцифры**
- Все токены и смарт-карты — **в реестре РЭП Минпромторга**

Минцифры России

МИНПРОМТОРГ РОССИИ

Форм-факторы и назначение Рутокен



Смарт-карта

USB-токены

Хранение ключевой информации (PKI)

Расширенная пользовательская аутентификация

Электронная подпись

Виды токенов по типу выработки ключа

Пассивные –

используются для хранения ключа (а не генерации).

- **Рутокен Lite**

Активные –

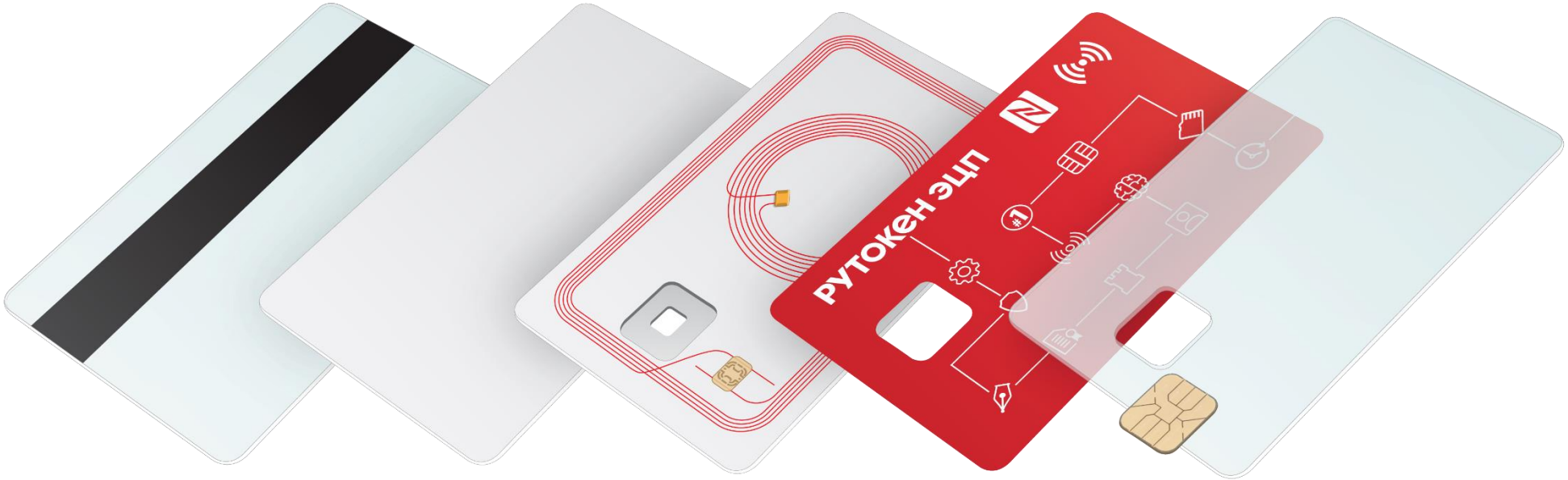
генерируют ключ средствами микроконтроллера. Ключи в таких токенах – неизвлекаемые.

- **Линейка Рутокен ЭЦП**

Активные токены позволяют использовать ключ подписи 3 года

Электронное удостоверение сотрудника

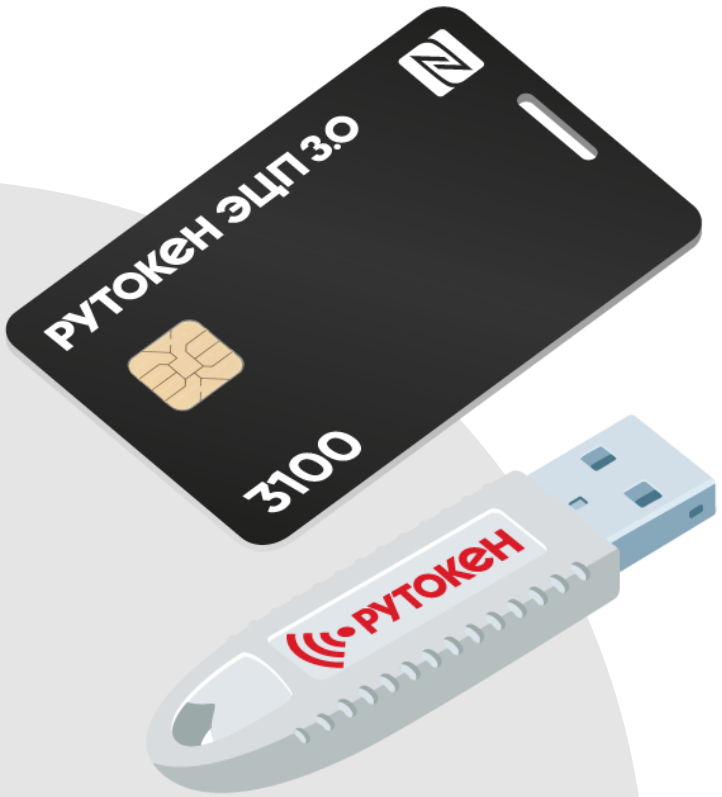
Одно устройство — много возможностей!



Преимущества

- Функциональность нескольких карт в одной Рутокен ЭЦП 3.0 3100 NFC MF (Mifare)
- Удобство в использовании и управлении картами с Рутокен KeyBox
- Повышение общей безопасности системы и снижение стоимости
- Дизайн под ваши предпочтения

Дуальные устройства
Рутокен ЭЦП 3.0 NFC



- Подпись касанием к мобильному устройству или считывателю
- Аппаратная криптография, неизвлекаемые ключи
- Использование на ПК бесконтактно и контактно
- Не требуются дополнительного питания при работе через NFC
- Работа на всех стационарных (Win, Linux, macOS) и мобильных (Android, iOS, Аврора) ОС с любой архитектурой (x86, ARM, MIPS, включая Эльбрус и Байкал)
- Сертификаты ФСБ России и ФСТЭК России
- Секреты хранятся отдельно от приложений и документов
- Интерфейсы: NFC, ISO 7816 (контактные карты), USB Type A, USB Type C

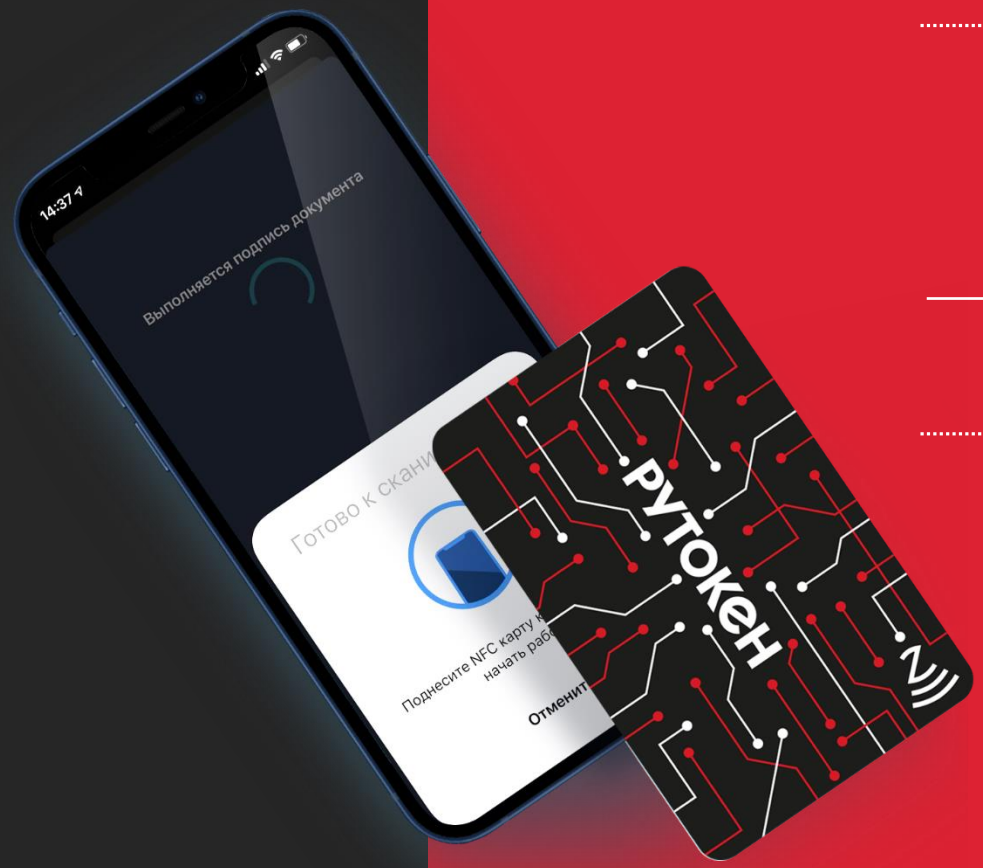
Электронное подписание документов

Электронная подпись и шифрование файлов на любых платформах (включая iOS и Android)

РУТОКЕН

Преимущества использования Рутокен ЭЦП 3.0 NFC:

- Простота интеграции
- Широкая поддержка разработчиками ПО
- Криптография на борту на неизвлекаемых ключах

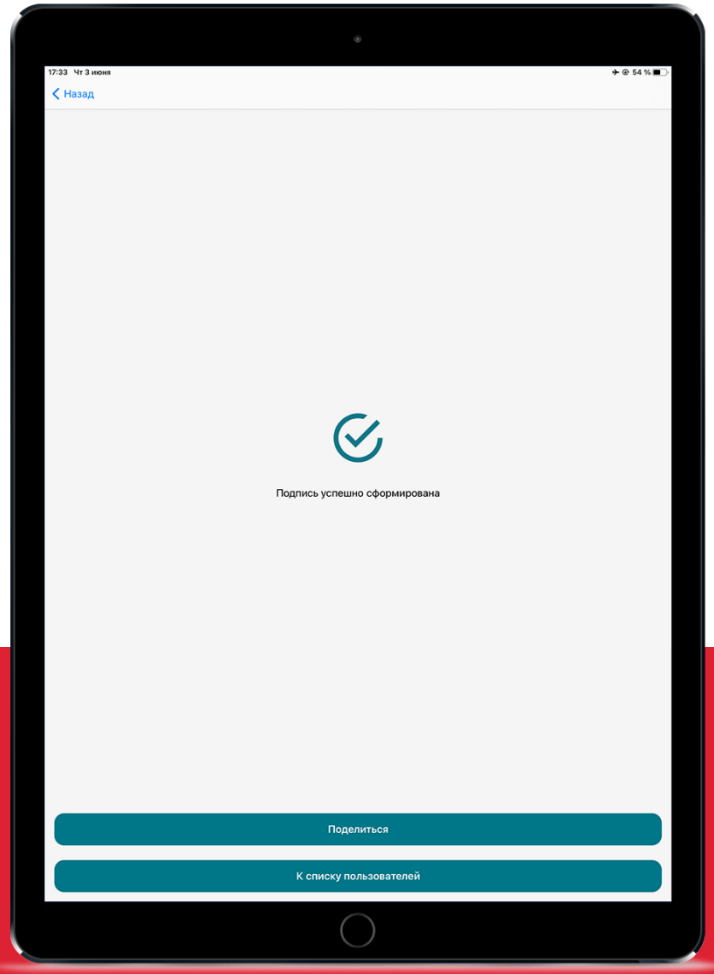


КриптоАРМ ГОСТ

infotecs

ViPNet PKI Client

Виртуальный считыватель смарт-карт Рутокен VCR



Поддерживаемые модели устройств:

- iPhone: Модели: XR+
  iOS: 13 +
- iPad: Модели: 2018 год +
  iPadOS: 13 +

Корпоративная мобильность в распределенных компаниях

Сложности таких компаний

- Сложный документооборот
- Персональная ответственность сотрудников
- Множество процедур (экзамены, регламенты, обучения, заявки, отчетность)

Мобильная электронная подпись заменяет ежедневный бумажный документооборот и увеличивает эффективность бизнеса

Применение:

- Энергетика
- Транспорт
- Системы здравоохранения
- Государственные органы
- Промышленность

Автоматизация горнодобывающих и промышленных предприятий

GRUPP

РУТОКЕН

АС Альтан — система информационной безопасности для горнодобывающих предприятий

Преимущества использования Рутокен ЭЦП 3.0 NFC:

- Работа в оффлайн и онлайн
- Универсальный пропуск на объекты
- Авторизация и электронная подпись одним устройством
- Оптимизация бизнес-процессов

Автоматизация энергосбытовых компаний

ЭНЕРГИЯ ЭФФЕКТИВНЫХ РЕШЕНИЙ

- АСУ «Мобильные Бригады» разработана с учетом специфики энергетических компаний и включает в себя:
  - мобильное приложение – АРМ мобильной бригады с возможностью полноценной работы офлайн
  - портал управления для централизованного планирования деятельности мобильных бригад
  - ЭДО с применением КЭП Рутокен ЭЦП 3.0 NFC
- Собственный УЦ

Защита внутрикорпоративного документооборота

Возможность заверения и передачи электронных документов внутри организации существенно ускоряет ход бизнес-процессов и избавляет от необходимости хранения значительных объемов бумажных документов.
При этом использование систем ЭДО предполагает соблюдение определенных правил защиты информации – организацию безопасной регистрации и аутентификации пользователей, предотвращение несанкционированного просмотра документов при передаче, обеспечение юридической значимости электронных документов.

Эффективно решить поставленные задачи способны аппаратные средства защиты информации, USB-токены и смарт-карты Рутокен, использующие криптографические алгоритмы для шифрования данных, строгой двухфакторной аутентификации пользователей и электронной подписи, в том числе на мобильных устройствах. Хранение ключей пользователя на идентификаторе Рутокен позволяет обеспечить их надежную защиту.

USB-токены и смарт-карты Рутокен ЭЦП 2.0 2100

USB-токены и смарт-карты Рутокен ЭЦП 3.0

Организация удаленной работы государственных экстренных служб

Бригады скорой помощи, пожарные, экологи, сотрудники органов правопорядка и другие службы, работающие на выезде, активно задействуют сегодня мобильные устройства для ведения электронного документооборота. Это позволяет сократить время и избежать сложностей при оформлении бумажных документов, предотвратив их потерю.

Использование сотрудниками выездных бригад USB-токенов и смарт-карт Рутокен позволяет им участвовать в электронном документообороте, одним касанием подписывая на мобильном устройстве юридически значимые документы усиленной квалифицированной электронной подписью.

USB-токены Рутокен ЭЦП 3.0 3100 NFC

Смарт-карты Рутокен ЭЦП 3.0 NFC

Защита взаимодействия с государственными информационными сервисами

Сегодня многие организации и частные лица почти ежедневно используют различные цифровые сервисы, предоставляющие доступ к государственным услугам. Среди них – сдача налоговых деклараций и получение выписок из ЕГРН, регистрация производителями товаров, участие в электронных торгах и прочие.

Сертифицированные ФСТЭК и ФСБ USB-токены и смарт-карты Рутокен помогают защищать от злоумышленников доступ в личный кабинет с помощью двухфакторной аутентификации, а также позволяют формировать усиленную квалифицированную электронную подпись для подписания юридически значимых документов.

Устройства Рутокен выступают в данном случае как более надежная альтернатива аутентификации в государственных информационных системах с помощью связки логин-пароль.

- **USB-токены и смарт-карты Рутокен ЭЦП 2.0 2100**
- **USB-токены Рутокен ЭЦП 2.0 Flash**
- **USB-токены Рутокен Lite**

Аутентификация и статические пароли

+

- **Привычно и просто** для пользователей
- **Широко распространены** у разработчиков ПО
- **Не требуют** дополнительных **технических средств**

40En5N8*6=goG4A26v

Хороший пароль — пользователь не использует

–

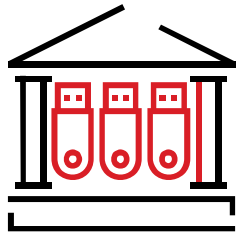
- **Трудно придумать (и запомнить)** хороший пароль
- **Невозможно** установить факт компрометации
- Пользователи используют **одинаковые** пароли в разные сервисы
- На пароли возможно **множество векторов атак**

Методы аутентификации в информационные системы

Классификация аутентификации по ГОСТ Р 58833-2020	Метод аутентификации	Продукт Рутокен
Простая	Статические пароли	Рутокен Логон
Дополнительный фактор	Биометрия (палец\лицо)	Ведем работу над добавлением в Рутокен ЭЦП 3.0
Усиленная	Одноразовые пароли (OATH HOTP, TOTP)	Рутокен OTP
Строгая	PKI (Инфраструктура открытых ключей)	Рутокен Lite Рутокен ЭЦП 3.0
Строгая	Веб-аутентификация на основе технологий U2F/FIDO	Рутокен MFA

Для достижения нужного уровня доверия к аутентификации нужно использовать комбинации разных методов!

МФЦ Нижнего Новгорода



70
Отделений по городу и области

2
системы ЭДО

5 000
пользователей

ЮЭДО
внедрение

2ФА
на основе PKI

Рутокен KeyBox
внедрена

Итоги:

- Повышена ответственность пользователей
- Решение парольной проблемы
- Соответствие нормативным требованиям

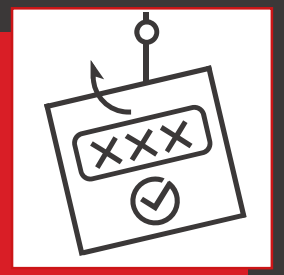
Одноразовые пароли (One Time Password – OTP)

+

- Криптографическая основа для **OATH HOTP\TOTP**
- Хорошая **интеграция** с сетевыми устройствами
- Компрометация одноразового **пароля** не компрометирует **аккаунт**
- **Разные** пароли для **разных** аккаунт
- Развитие стандартов **профильной инициативной группой** (OATH – Initiative for Open Athentication)

–

- **Вредоносы** могут считывать Push, SMS и OTP с мобильных устройств без уведомления пользователя
- Нужно **носить с собой** средство генерации OTP
- Аппаратные устройства **стоят денег**
- **Уязвимость** к фишинговым атакам

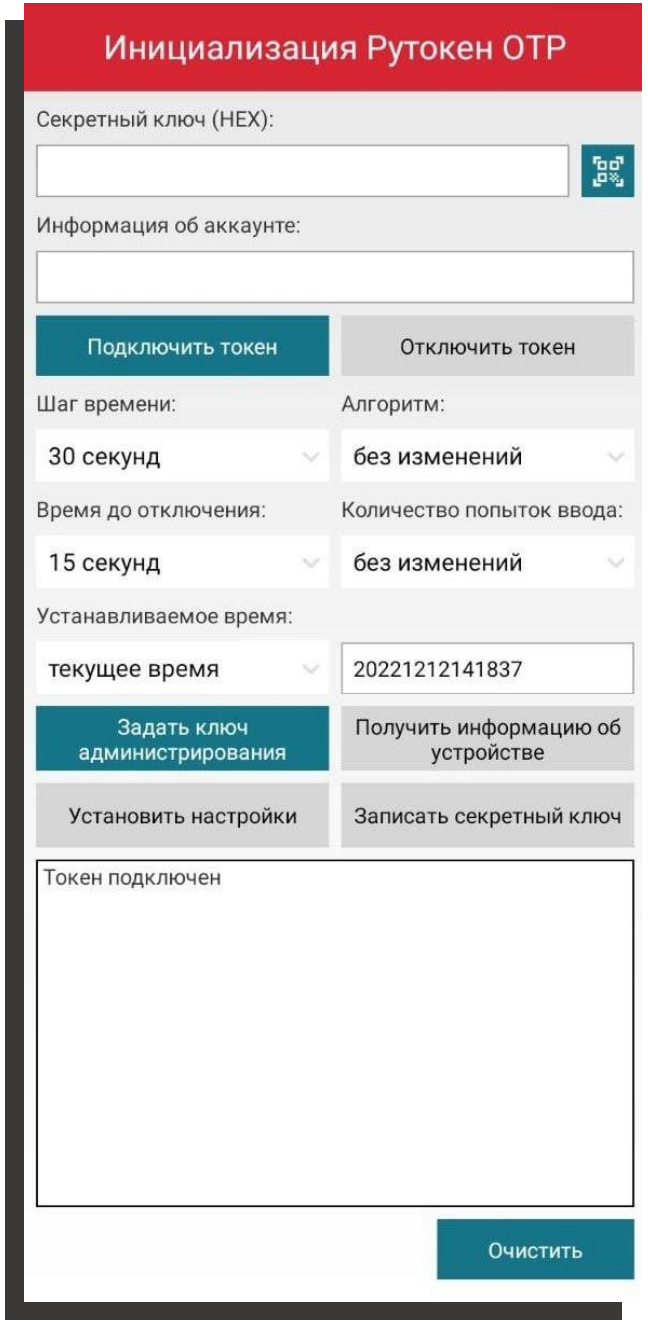


Криптографически вычисляемые OTP – крайне эффективны, но уязвимы к фишингу

Решение для OTP

Новое поколение Рутокен OTP:

- Алгоритм **OATH TOTP** (RFC6238)
- **Не требует связи** с ПК/мобильным устройством для **работы**
- **NFC** для импорта секретного ключа и настройки (есть ПО для мобильных и стационарных ОС)
- **Аппаратный таймер** для подсчета времени
- Возможность поставки **преднастроенных** устройств (удобно крупным корпоративным заказчикам)



Аутентификация FIDO в веб-приложениях

Набор стандартов FIDO2 – решение для беспарольной аутентификации пользователя в веб-приложениях

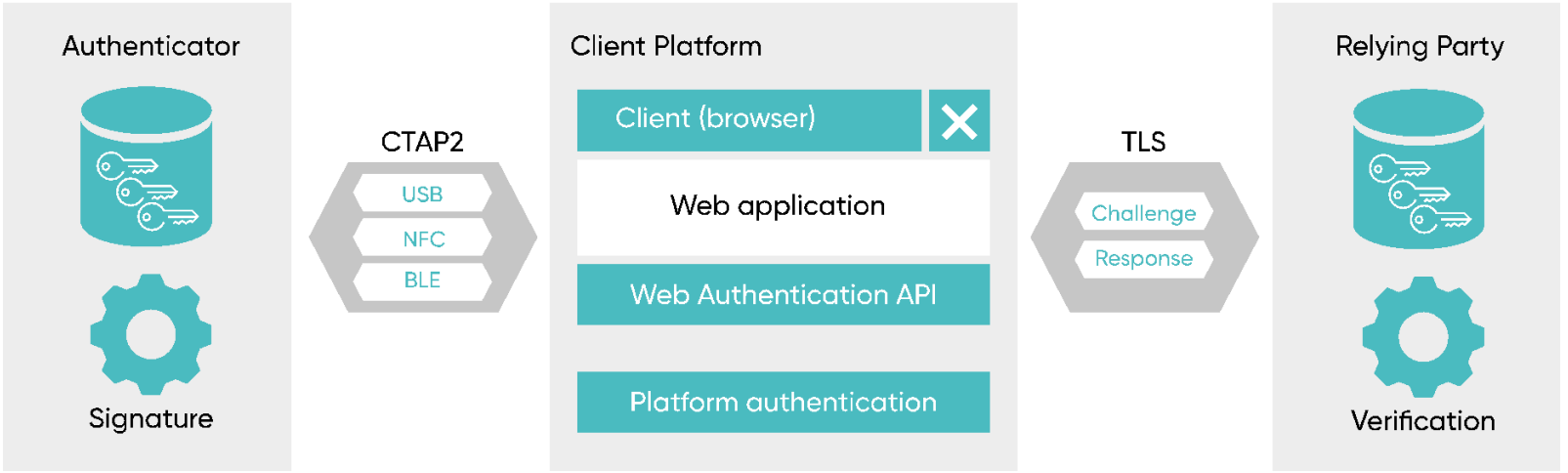
- **Открытый**, без драйверный протокол для двухфакторной аутентификации
- Поддерживается и развивается **консорциумом FIDO Alliance**
- В основе – **ассиметричная** криптография
- **Развитие** предыдущего стандарта U2F

Спецификация FIDO2 выпущена в 2019 году и включает в себя протоколы:

- К ключам безопасности (CTAP)
- К серверу и браузеру (W3C WebAuthn)

fido™ ALLIANCE

Компоненты FIDO2



1 Аутентификатор FIDO2

(ключ безопасности, подключается по USB\ BLE\NFC)

2 Клиент FIDO2

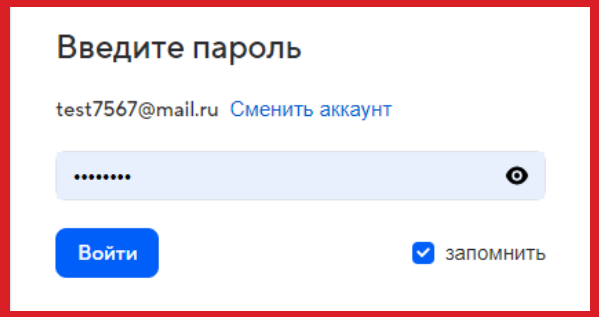
Браузер, который взаимодействует с аутентификатором

3 Сервер FIDO2

Веб-сервер, поддерживающий спецификацию WebAuthn, реализует операции регистрации и аутентификации пользователя

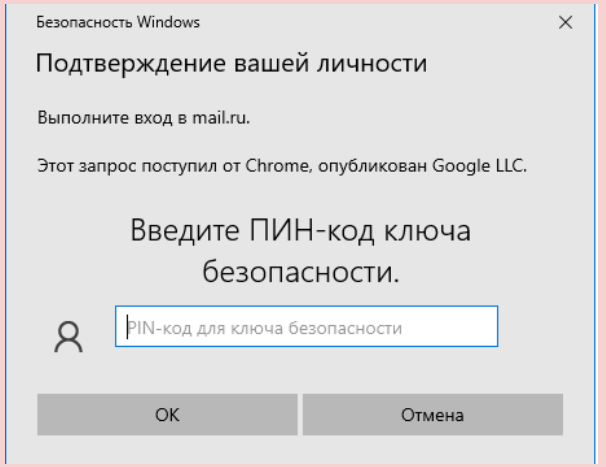
Как выглядит аутентификация по FIDO2 (на примере Mail.ru)

1 Вводим логин\пароль

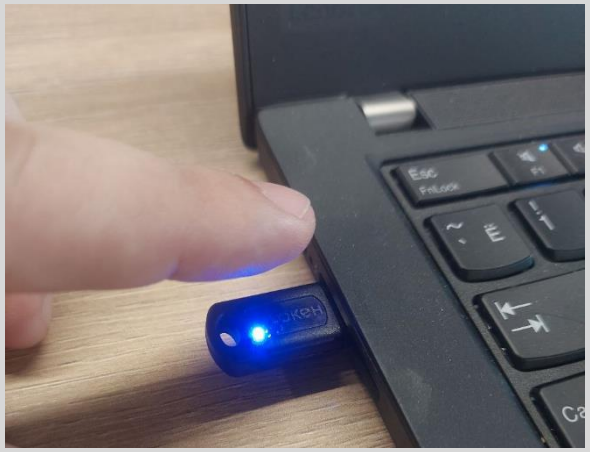


2 Вставляем/прикладывем ключ

3 Вводим PIN-токена



4 Касаемся устройства



В каких браузерах FIDO2 работает «из коробки»?





Windows/Linux/MacOS/Аврора

- Google Chrome 67+
- Mozilla Firefox 60+
- Microsoft Edge 18+
- Apple Safari 13+
- **Яндекс Браузер 16.7+**

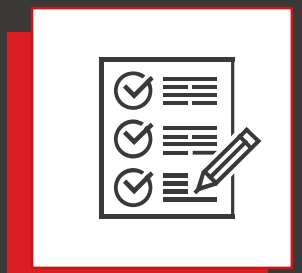
Android/IOS

- Google Chrome 105+
- Apple Safari 14.5+

Аутентификация FIDO в веб-приложениях

+

- **Не требуется** установка драйверов и дополнительного ПО
- **Простота** использования для пользователя
- **Один** аутентификатор используется для **множества** ресурсов
- **Высокий** уровень безопасности:
  - Использует ассиметричную криптографию
  - Защищает от фишинга и атак Man-in-the-middle (MITM)
  - Нет передаваемых по сети паролей



Соответствие AAL3 по NIST 800-63b

−

- **Узкий** спектр применения
- Использует **зарубежную** криптографию

Решение для Веб-аутентификации

Рутокен MFA:

Линейка устройств в формате USB-C и USB-A микро.

- Поддержка протоколов **U2F, FIDO2**
- Поддержка **беспарольной** аутентификации (passwordless) для 16-ти аккаунтов
- Возможность **обновления** прошивки

Устройство в полноразмерном формате USB-Type-A

- Поддержка **NFC** для мобильных устройств
- В будущем – **сертификация** ФСТЭК России по УД

Вопросы?

Андрей Шпаков

Руководитель проектов
по информационной безопасности
Компания «Актив»

shpakov@rutoken.ru
info@rutoken.ru

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

+7 495 925-77-90
+7 916 518-70-26