РУТОКЕН

Примеры практического применения мобильной электронной подписи

Дмитрий Соколов
Руководитель отдела
по работе с заказчиками и партнерами Рутокен
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

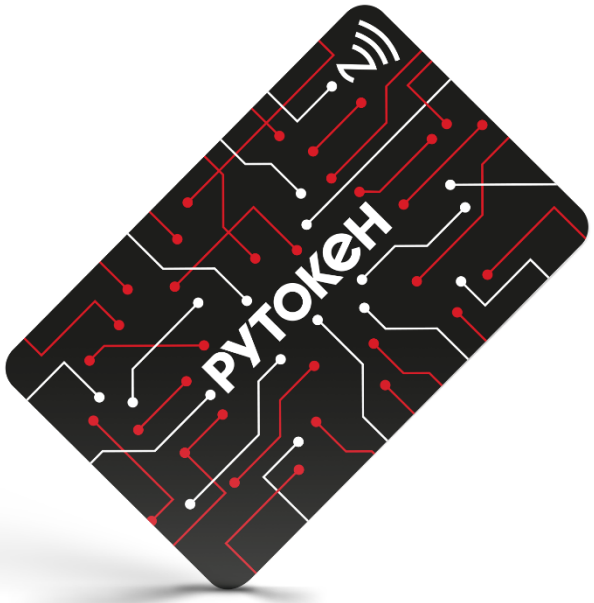
Приятные факты

- 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

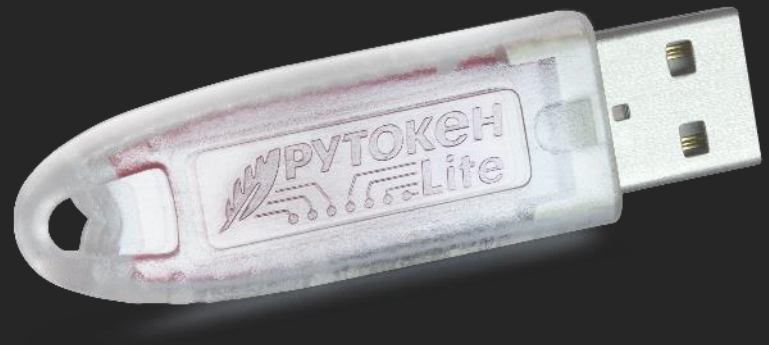
Электронная подпись

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

Аутентификация и стат ские пароли

\+

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

\–

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

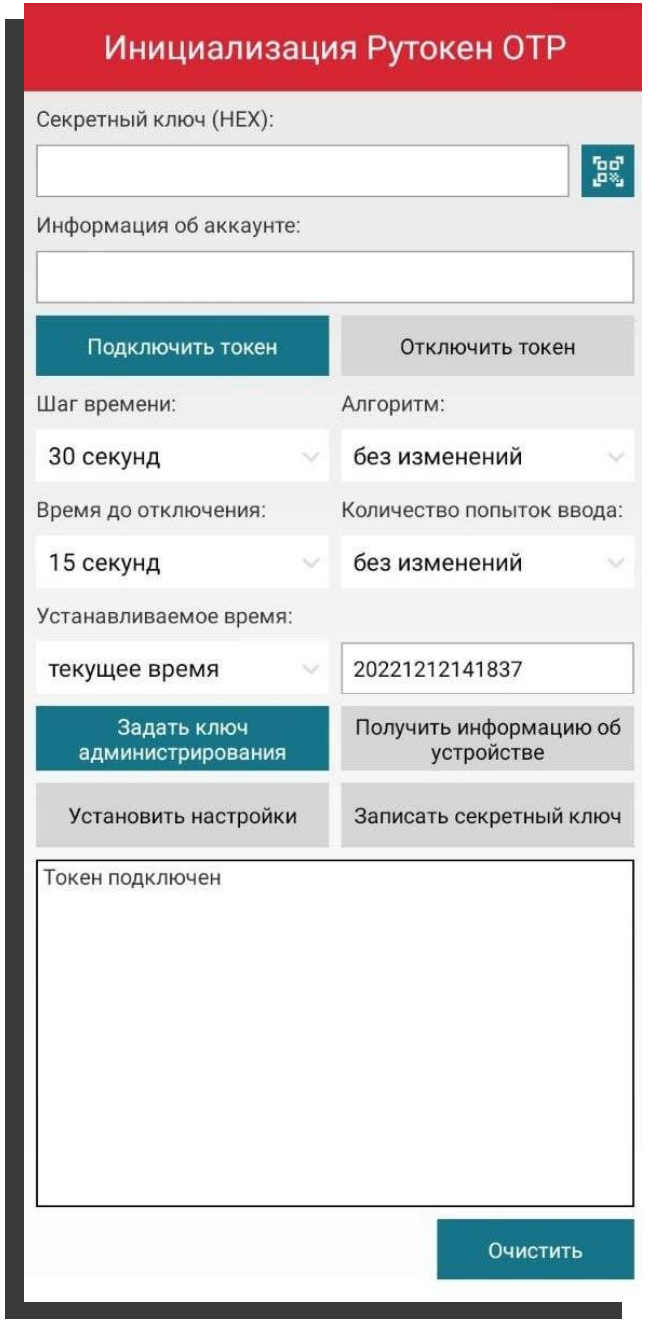
Реализация 2ФА на основе Рутокен

- Рутокен ЭЦП 3.0 – Windows / Linux
- Рутокен ОТП и MFA – Web-приложения

Решение для OTP

Новое поколение Рутокен OTP:

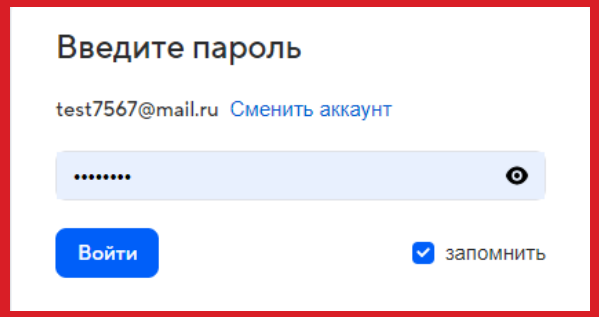
- Алгоритм **OATH TOTP** (RFC6238)
- **Не требует связи** с ПК/мобильным устройством для **работы**
- **NFC** для импорта секретного ключа и настройки (есть ПО для мобильных и стационарных ОС)
- **Аппаратный таймер** для подсчета времени
- Возможность поставки **преднастроенных** устройств (удобно крупным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



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

1

Вводим логин\ пароль

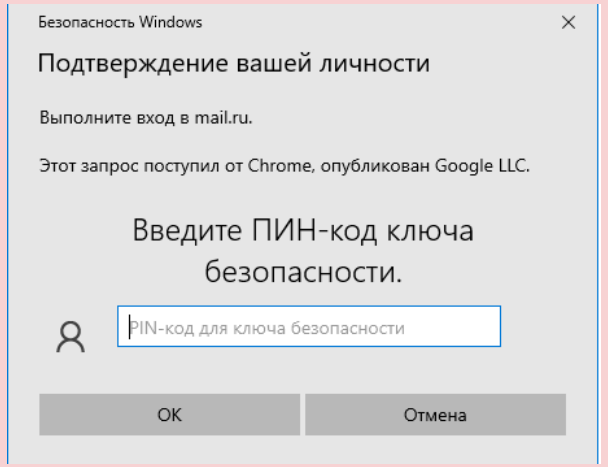


2

Вставляем/ прикладывем ключ

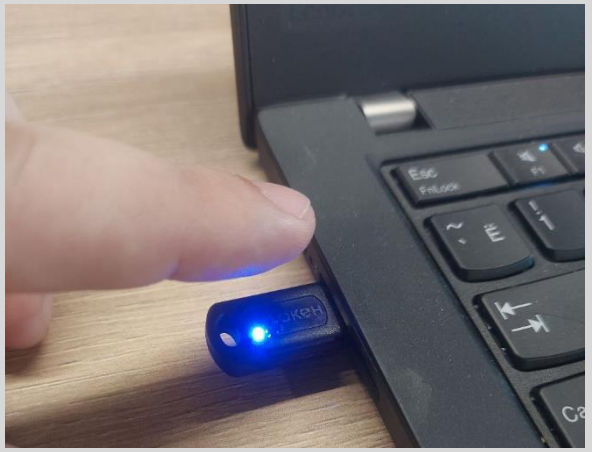
3

Вводим PIN-токена



4

Касаемся устройства



Реализация по-настоящему мобильной электронной подписи

Характеристики
Рутокен ЭЦП 3.0 NFC

Аппаратная реализация криптографии:

- ГОСТ 34.10-2012 (256/512 бит)
- ГОСТ 34.11-2012
- VKO GOST
- ГОСТ Р 34.12-2015 Магма
- ГОСТ Р 34.12-2015 Кузнечик
- RSA 1028, 2048, 4096 бит
- ECDSA с кривыми secp256k1 и secp256r1

- Совместимость с современными ОС, включая отечественные и мобильные
- Совместимость с криптопровайдерами
- Защита NFC-канала (SESPAKE)
- Высокая производительность
- SDK для встраивания

Электронное подписание документов

Электронная подпись и шифрование файлов на любых платформах

Преимущества использования Рутокен ЭЦП 3.0 NFC:

- Универсальная работа на мобильных устройствах и настольных ПК
- Ключи доступа хранятся отдельно от приложения
- Криптография на борту на неизвлекаемых ключах

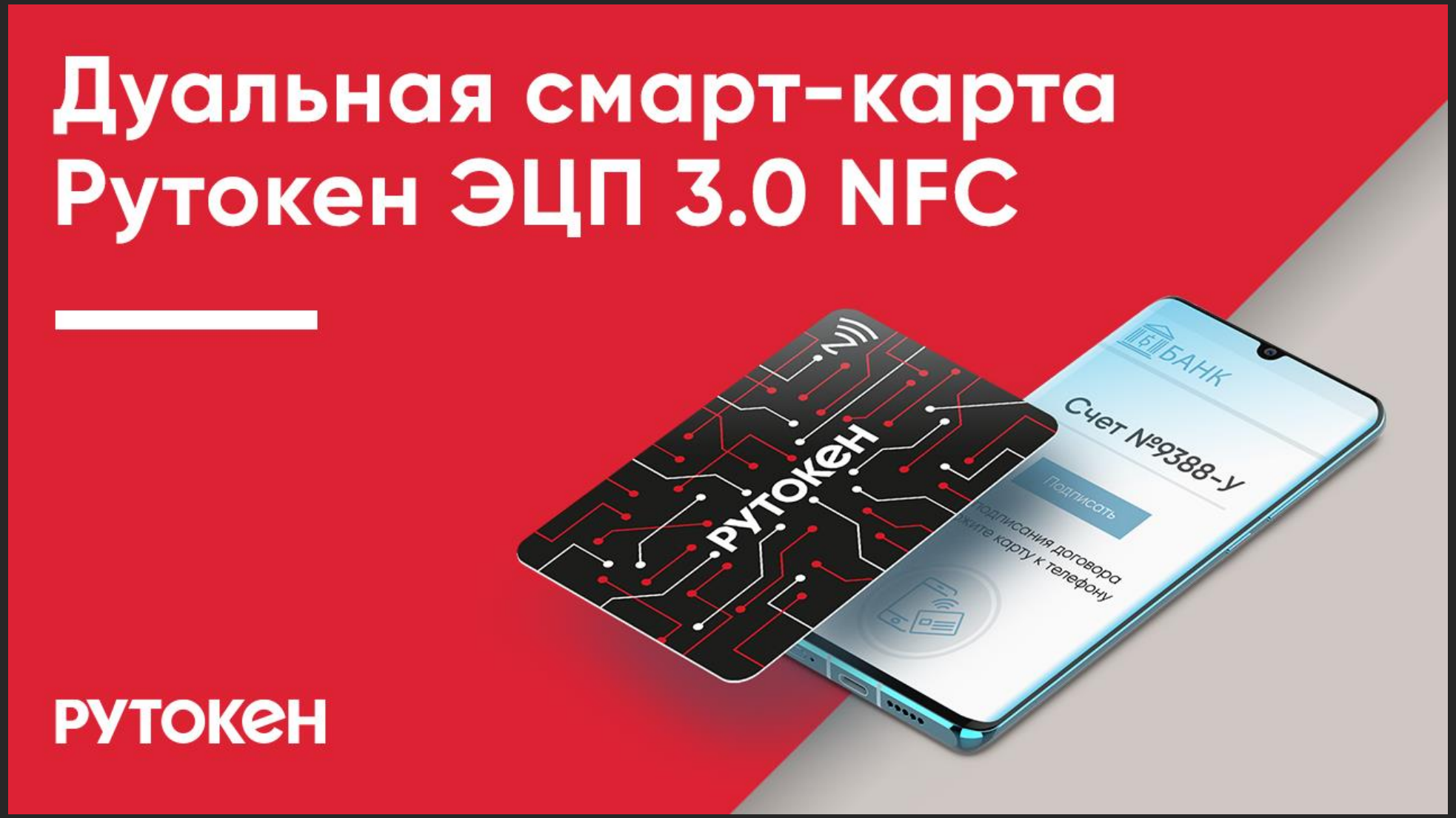
РУТОКЕН

КриптоАРМ ГОСТ

infotecs

ViPNet PKI Client

Просто и быстро



Корпоративная мобильность

РУТОКЕН

Мобильная электронная подпись заменяет ежедневный бумажный документооборот

Преимущества использования Рутокен ЭЦП 3.0 NFC:

- Смарт-карта - средство эл. подписи «в полях» и рабочий пропуск
- Избавляет офис от бумажной рутины
- Не требует физического подключения
- Надежность и производительность
- Секреты хранятся отдельно от приложения

Применение:

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

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 3100 NFC

Поддержка работы выездных бригад

Необходимость поиска и заполнения бумажных документов, как правило, создает массу трудностей для специалистов выездных бригад (нефтяников, горнодобытчиков, энергетиков, водители-экспедиторов), выполняющих работу в сложных условиях отдаленных районов. Использование электронного документооборота (ЭДО) на мобильных устройствах значительно упрощает получение и подтверждения нарядов, заполнение необходимых форм и отчетов, оформление множества других документов.

- Применение в ЭДО сертифицированных криптографических устройств Рутокен обеспечивает безопасность и удобство мобильной электронной подписи. Прилагая минимум усилий и сохраняя непрерывность бизнес-процессов, пользователь получает возможность лично подписывать электронной подписью по беспроводному каналу NFC необходимые документы.
- При этом ключ электронной подписи хранится отдельно от недоверенных мобильных устройств и приложения для документооборота.

Смарт-карты Рутокен ЭЦП 3.0 3100 NFC

Автоматизация горнодобывающих и промышленных предприятий

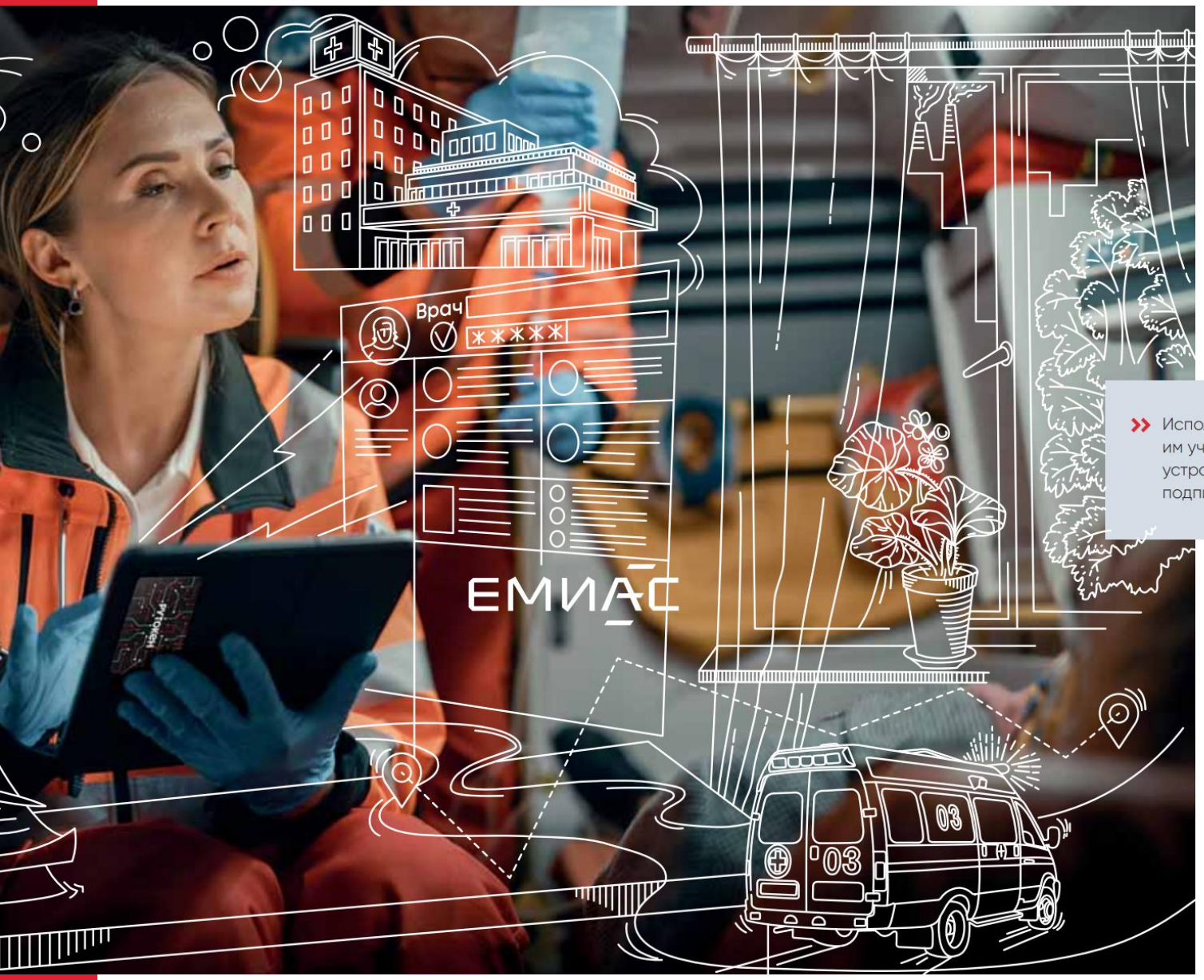
GRUPP

РУТОКЕН

Процесс согласования документов сложен
и имеет ряд этапов, в которых задействованы
сотрудники из разных городов

Преимущества использования Рутокен ЭЦП 3.0 NFC:

- Снижение количества ошибок и нарушений
- Ускорение и оптимизация бизнес-процессов
- Рост эффективности предприятия и снижение рисков травмирования
- Смарт-карта как средство эл. подписи



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 3100 NFC

Рутокен

База Используется для ведения учета и управления:

Защищенными ключевыми носителями (токенами, смарт-картами и HSM) различных производителей (Рутокен, JaCarta, и т. д.)

Прочими ключевыми носителями (реестр, файловая система, usb-flash и т. д.)

Программными криптопровайдерами, установленными на ПК сотрудников

Ключами и сертификатами электронной подписи

Прочими СКЗИ и СЗИ (только учет, без возможности управления)

Рутокен База. Возможности

- Вести журнал учета ключевых носителей, ключей и сертификатов
- Формировать журнал учета СКЗИ в соответствии с приказом ФАПСИ №152
- Формировать различные отчеты — по ключевым носителям, прочим СКЗИ, ключам и сертификатам ЭП и пр.
- Формировать запросы на выдачу квалифицированных сертификатов ЭП
- Фиксировать события, связанные с жизненным циклом ключевых носителей и сертификатов ЭП
- Уведомлять пользователей и ответственных
- Вести аналитику жизненного цикла ключевых носителей и сертификатов ЭП, на основании аналитики планировать закупки новых ключевых носителей в связи с выходом существующих из эксплуатации (плановой и внеплановой)
- С помощью интерфейса самообслуживания дать сотрудникам возможность осуществления сервисных операций с носителями (например, запрос сброса PIN-кода заблокированных ключевых носителей)
- Выполнять удаленное управление ключевыми носителями, такие как запись на носители контейнеров с ключами и сертификатами на носители, удаление ключей, дистанционная очистка носителей.

Каталог продукции Рутокен

Криптографические токены и смарт-карты

- **Хранение ключей электронной подписи**
  - Рутокен Lite
- **Двухфакторная аутентификация и электронная подпись**
  - Рутокен ЭЦП 3.0 3100 NFC
  - Рутокен ЭЦП 2.0 2100
  - Рутокен ЭЦП 2.0 3000
- **Бесконтактная электронная подпись для мобильных платформ**
  - Смарт-карта Рутокен ЭЦП 3.0 3100 NFC
- **Защита аккаунтов**
  - Рутокен FIDO2
  - Рутокен OTP

Интеллектуальные карты для СКУД

- Смарт-карта Рутокен ЭЦП 3.0 3100 NFC
- Смарт-карта Рутокен ЭЦП 2.0 2100 с RFID-меткой

Защищенные считыватели смарт-карт

- Рутокен SCR 3001
- Рутокен VCR 3001

Встраиваемые криптомодули для киберфизических систем (IoT, M2M)

- Рутокен Модуль

Специализированное ПО

- **Защита электронной почты и аутентификация в домене**
  - Рутокен для Windows
- **Двухфакторная аутентификация на рабочих местах вне домена**
  - Рутокен Логон
- **Двухфакторная аутентификация и электронная подпись из браузера**
  - Рутокен Плагин
- **Защита критически важных данных в памяти устройства**
  - Рутокен Диск

Комплексные системы

- **Управление жизненным циклом средств аутентификации и электронной подписи**
  - Рутокен KeyBox
- **Единая точка доступа к ИТ-системам для обеспечения двухфакторной аутентификации**
  - Рутокен MA
- **Управление доступом к привилегированным учетным записям**
  - Рутокен PAM
- **Безопасность удаленной работы**
  - Рутокен VPN

Контактная информация

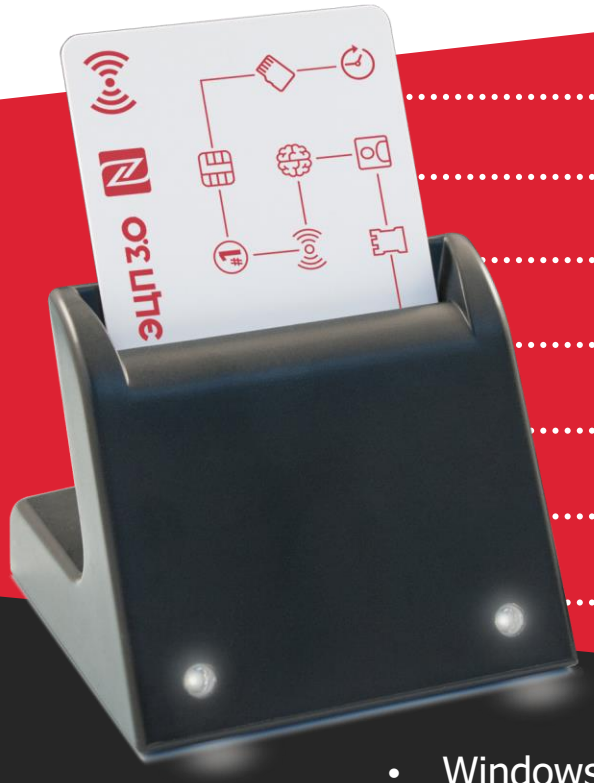
Дмитрий Соколов

Sokolovd@rutoken.ru
info@rutoken.ru

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

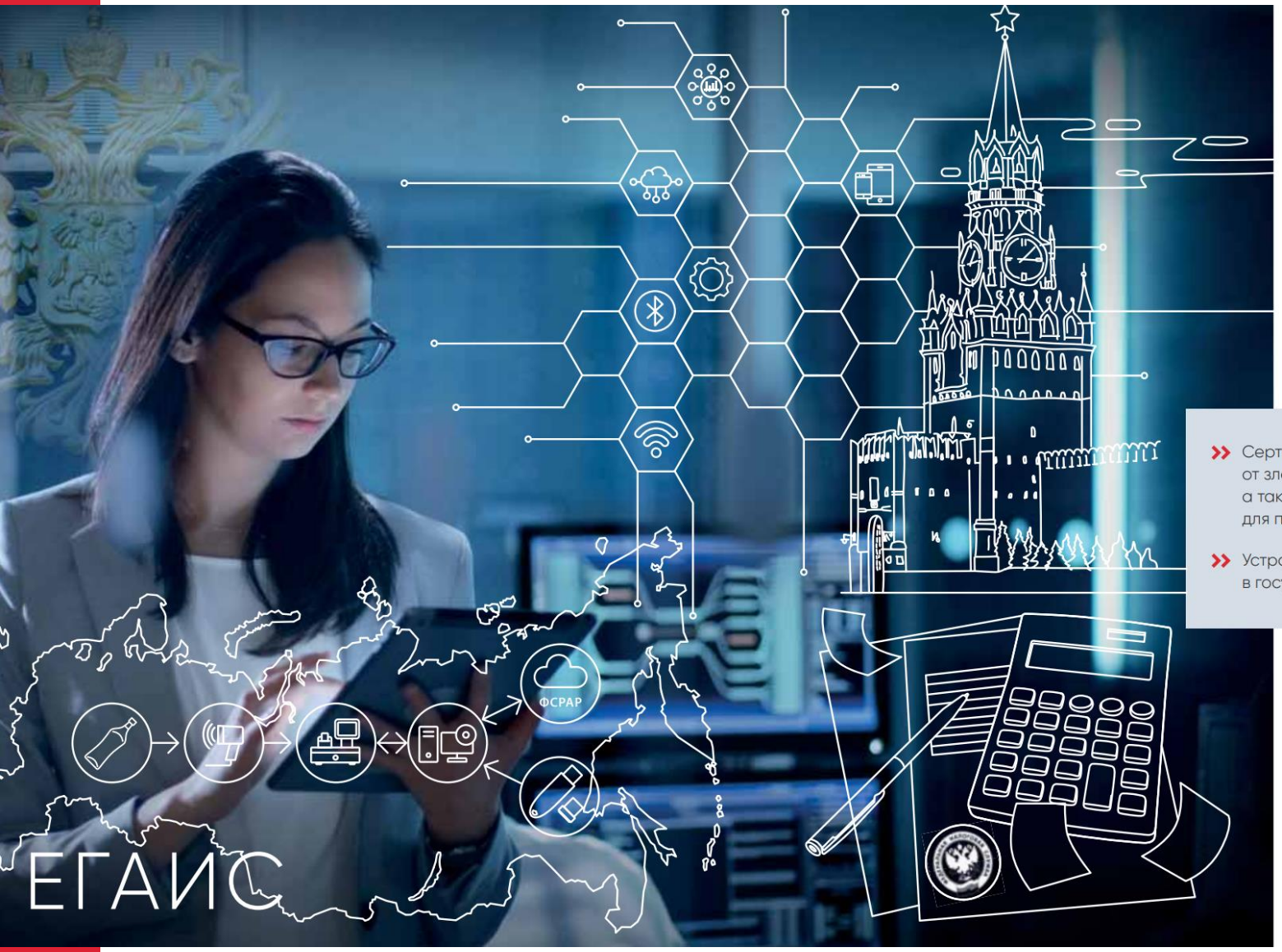
+7 495 925-77-90
+7 903 720-56-79

Считыватель смарт-карт
Рутокен SCR 3001



- Детектор движения карты с автоматическим отключением питания
- Автоматическое определение типа смарт-карты
- Защита от короткого замыкания и перегрева
- USB 2.0 CCID, USB Type-C (на заказ)
- До 480 Мбит/с (USB 2.0 High Speed)
- Срок службы: 200 000 операций ввода карты
- Индикатор состояния: два светодиода

- Windows 11/10/8.1/8/7/Vista/XP
- Windows Server 2019/2016/2012R2/2012/2008R2
- macOS 12/11.00/10.15/10.14/10.13/10.12/10.11/10.10/10.9
- GNU/Linux
- Android 5 и выше



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