

Аутентификация на шлюзе КриптоПро NGate с помощью устройств Рутокен: многофакторность и комбинирование



Аутентификация на шлюзе КriptoПро NGate с помощью устройств Рутокен: многофакторность и комбинирование



Александр Никитков
КriptoПро



Сегодня в программе:

- Расскажем о типах клиентской аутентификации на шлюзе КriptoПро NGate
- Проиллюстрируем интеграцию с решениями Рутокен
- Покажем сценарии использования на реальных клиентских устройствах



Что умеет наш продукт?



Универсальный шлюз удаленного доступа КриптоПро NGate, объединяет в себе следующий функционал:

WEB TLS

TLS-сервера доступа к веб-сайтам

WEB Portal TLS

Сервера портального доступа

Point-to-Site TLS VPN

VPN-сервера удаленного доступа

Site-to-Site IPsec VPN

VPN-сервера доступа между площадками

Что умеет наш продукт?



Универсальный шлюз удаленного доступа КриптоПро NGate, объединяет в себе следующий функционал:

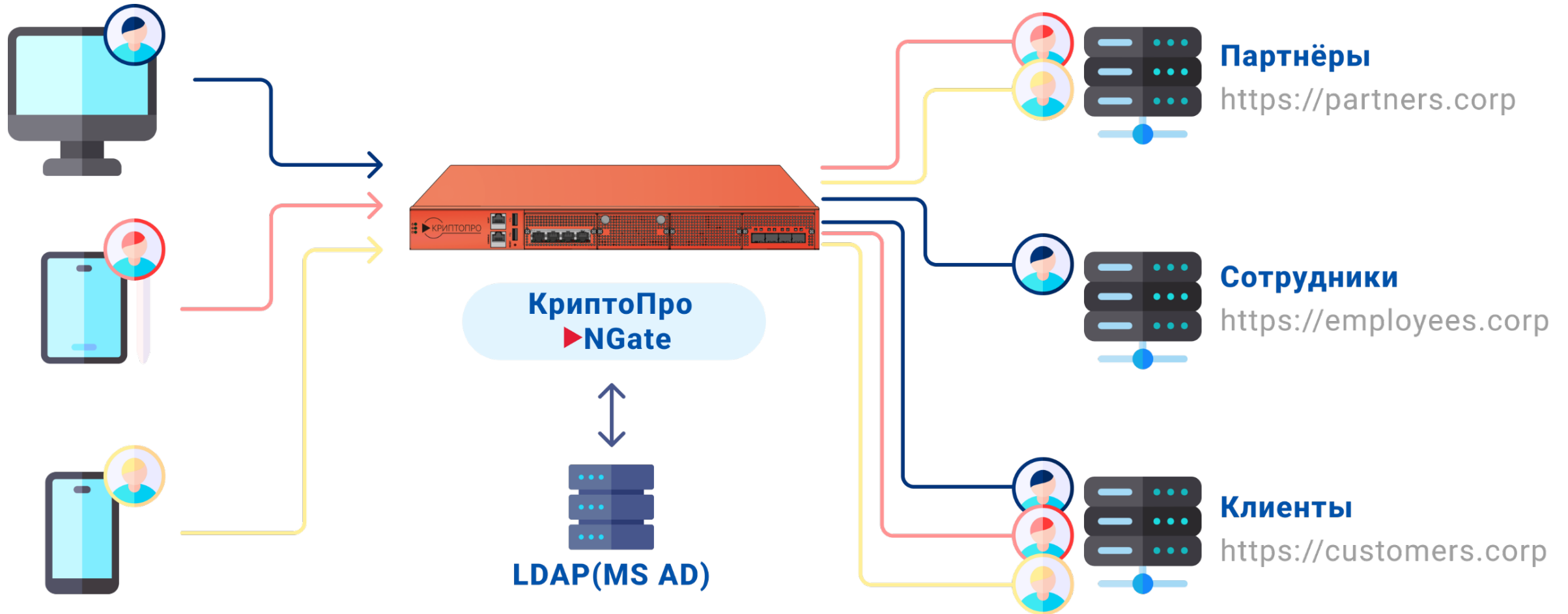
WEB Portal TLS

Сервера портального доступа

Point-to-Site TLS VPN

VPN-сервера удаленного доступа

Сервер порталного доступа (WEB Portal TLS)



Преимущества NGate при доступе к опубликованным ресурсам



Безопасный доступ к внутренним ресурсам через веб-браузер

Независимые виртуальные порталы на одном шлюзе

Отдельная политика доступа для каждого портала

Комбинация правил на одном портале для ГОСТ и не ГОСТ

Поддержка различных видов аутентификации и их комбинация

VPN-сервер удаленного доступа (Point-to-Site TLS VPN)



VPN-доступ по
протоколу TLS

Возможность интеграции с
отечественными FW

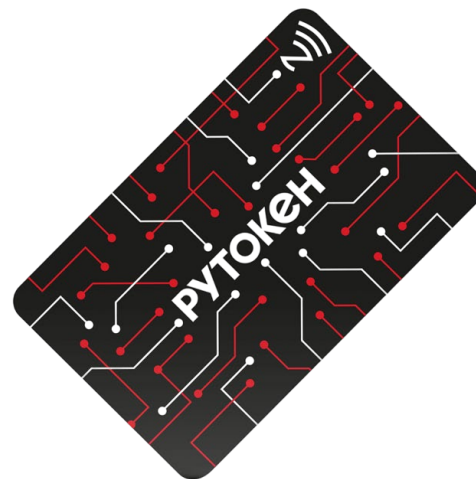
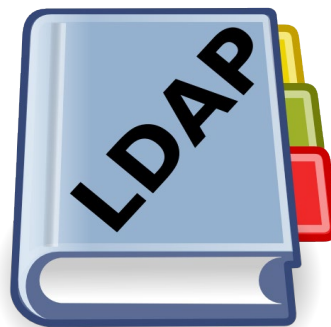
Клиент под все
платформы

Возможность замены Cisco
AnyConnect на NGate

Внутренние
корпоративные сервисы



Широчайшие возможности клиентской аутентификации



- **Логин\пароль**
- **Сертификаты**
- **Сертификат в LDAP**
- **Сертификат в LDAP (+ UPN)**
- **MFA (HOTP/TOTP и тд)**
- **RADIUS (VSA и все-все-все..)**
- **+ Ключевые носители**
- **+ Дата, время, день недели..**



**Возможность комбинировать
различные типы!**

РУТОКЕН

КОМПАНИЯ
ПРАКТИВ

Продукты Рутокен, как средство двухфакторной аутентификации в информационные системы

Кирилл Аверченко

Руководитель отдела
технического пресейла,
Компания «Актив»



Методы аутентификации в информационные системы



Методы:	Классы по ГОСТ Р 58833-2020:
Статические пароли	Простая аутентификация
Биометрия (палец\лицо)	Доп. фактор аутентификации
Одноразовые пароли HOTP/TOTP, в т.ч. через push, email и т.д.	Усиленная аутентификация
PKI (Инфраструктура открытых ключей)	Строгая
Веб-аутентификация на основе технологий U2F/FIDO	Строгая



Более качественная аутентификация обеспечивает более высокий уровень доверия

Основные кейсы **Рутокен** по MFA



- Защищенный **удаленный доступ**/VPN
- Вход на **рабочие станции** — Windows, Linux, Домены
- Защита **рабочих станций**

- Вход в веб-приложения
- Единая карта сотрудника — вход в помещения и рабочие станции

Три продукта, три технологии



Рутокен OTP
Технология TOTP



Рутокен ЭЦП 3.0
Технология PKI



Рутокен MFA
Технология FIDO2



Пользовательские аутентификаторы **Рутокен**

Рутокен OTP

- Вычисляет одноразовый пароль **по времени** (алгоритм OATH TOTP)
- Персональное устройство **с экраном**
- **Аппаратный таймер** подсчета времени
- Не требует **связи** с ПК для работы
- Настройка через **NFC** (Android/Windows)
- Возможность поставки преднастроенных устройств



Инициализация Рутокен OTP

Секретный ключ (HEX):

Информация об аккаунте:

Шаг времени: Алгоритм:

Время до отключения: Количество попыток ввода:

Устанавливаемое время:

Токен подключен

Сценарии: дополнительная аутентификация через OTP для Remote-Access VPN/802.1X

Решение

Примеры RADIUS-серверов с поддержкой OTP

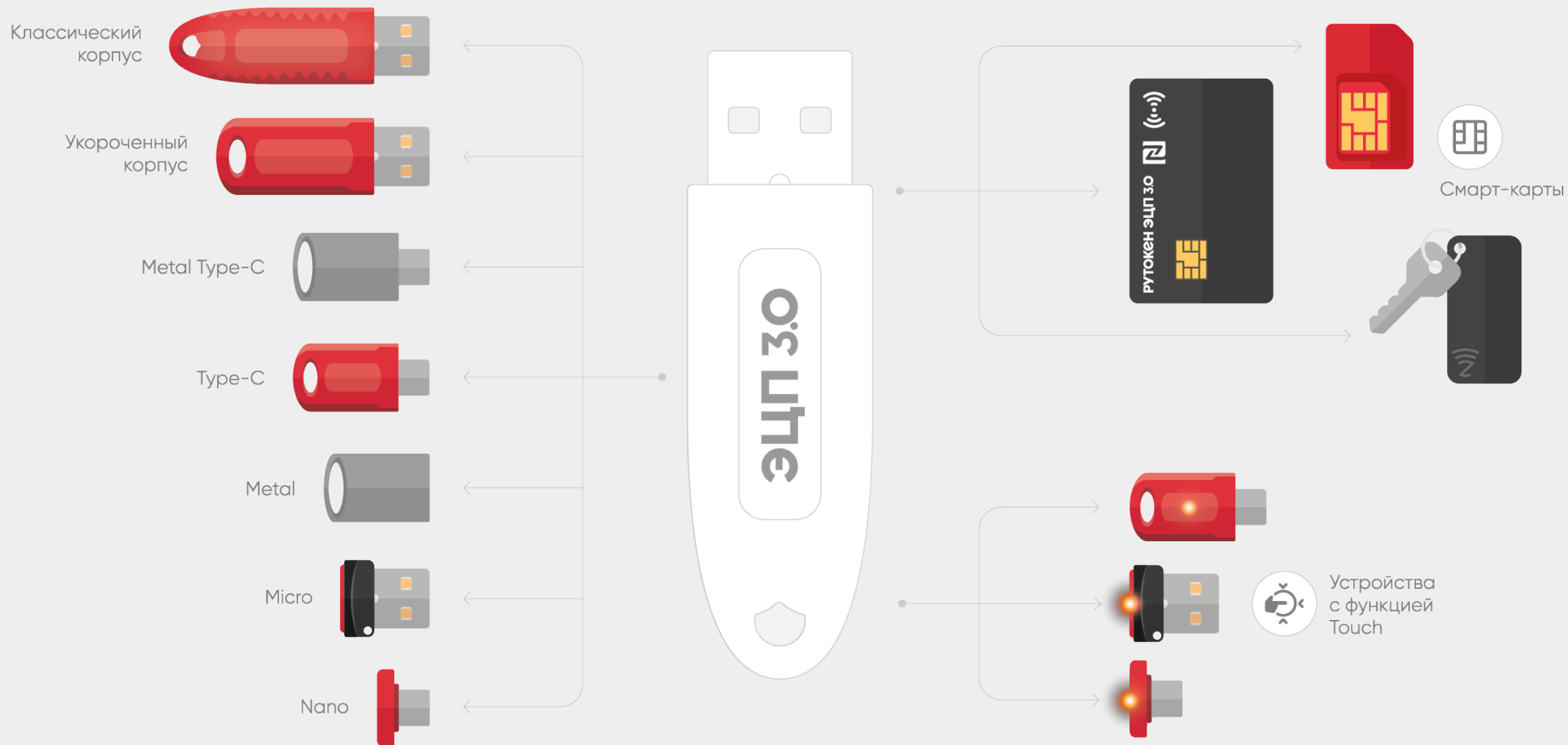
- ✓ **Клиенты VPN:** Cisco AnyConnect\
Checkpoint Endpoint Security\
КриптоПро NGate 1.0R2
- ✓ Сетевые устройства с поддержкой **802.1X**
- ✓ RADIUS-сервер с поддержкой **Access-Challenge**
- ✓ На сервере: **Генератор TOTP**
У пользователя: **Рутокен OTP**

- ✓ **Коммерческие:**
SAS от mfasoft, AvanPost, Multifactor, Сакура и др.
- ✓ **Open-source:**
FreeRadius + LinOTP



Рутокен ЭЦП 3.0

> Криптографические ключевые носители
для аутентификации и электронной подписи



Сценарии: защита удаленного доступа



Доступ
к ИТ-ресурсам
(VPN, VDI)

Хранение ключей для VPN/TLS-клиента:

1-й этап:

Подключение с помощью
КриптоПро NGate Client

2-й этап:

Доступ к внутренним ресурсам компании
через RDP или WEB

Преимущества

#1

Честный 2FA:

нет токена — нет
VPN-соединения

#2

Рекомендуемый
сценарий у всех
производителей
(**best practice**)

#3

Выполнение **Compliance**:

- ИБ — готовит токены,
- ИТ — дистрибутивы





Сценарии: вход на рабочие станции



Рутокен ЭЦП вместо логина-пароля в ОС

- ✓ Есть во **всех ОС** – Windows, Linux, MacOS
- ✓ Полная поддержка **российских ОС** – Astra Linux, ОС Альт, РЕД ОС, Роса, Аврора
- ✓ **Сертификат** или **сложный пароль** средствами доп. ПО

Требования к инфраструктуре

#1 ОС и домен

#2 Удостоверяющий
Центр для
сертификатов

#3 Рутокен Логон
или IAM-система
для сложного
пароля

Универсальная карта доступа сотрудника



Одно устройство —
много возможностей!



Преимущества:

- Функциональность нескольких карт
- Удобство в использовании и управлении картами с Рутокен KeyBox
- Повышение общей безопасности системы и снижение стоимости
- Дизайн под ваши предпочтения

Мобильные рабочие места



Быстрый и удобный способ подписывать документы
с помощью смартфона или планшета, 2фа

Рутокен ЭЦП 3.0, Рутокен TAG,
Рутокен ЭЦП 3.0 NFC



Решение для Веб-аутентификации



Рутокен MFA

Линейка устройств в формате USB-C, USB-C Nano и USB-A micro

- Стандарт **FIDO2**
 - **Не требует** драйверов
 - **Строгая** аутентификация
 - **Просто** для пользователя
- **Беспарольная** защита ("passkey") на 15 аккаунтов
- Поддержка в **отечественных ОС** и **браузерах**
- **Возможность обновления** прошивки

Планы:

- Поддержка NFC
- Сертификация во ФСТЭК по УД4



Сценарии: защита входа в веб-приложения

Решение — использовать Рутокен MFA на основе FIDO2

- ✓ Интегрируем FIDO2/Webauthn средствами IAM-системы или библиотек на портал
- ✓ Выдаем пользователю **токен**
- ✓ Пользователь привязывает токен к своей учетной записи

Преимущества для заказчика:

#1

Беспарольная аутентификация

#2

Не требует драйверов или отдельного ПО

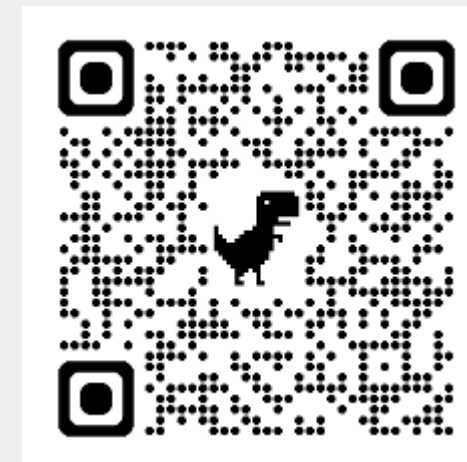
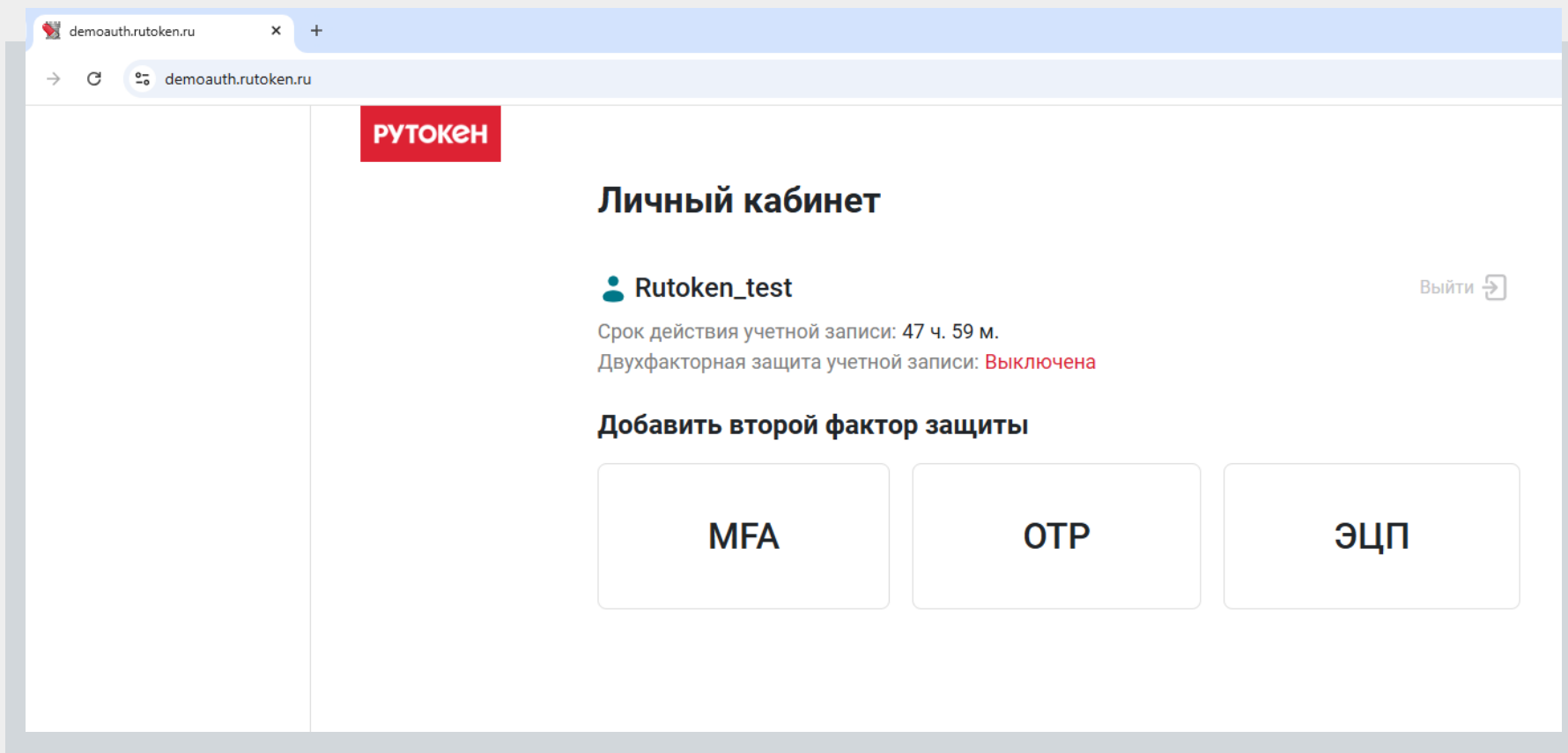
#3

Просто для пользователя



SERVICE

Демопортал для Веб-аутентификации



Преимущества аппаратных аутентификаторов



Безопасность

- Устойчивость к взлому
- Изоляция ключей



Независимость от устройства пользователя

- Кроссплатформенность
- Мобильность



Дополнительные проверки





Павел Луцик

Директор по продажам
и развитию бизнеса,
«КриптоПро»
plutsik@cryptopro.ru
+7 495 984-07-90



Александр Никитков

Эксперт отдела защиты сетей,
«КриптоПро»
alexandern@cryptopro.ru
+7 495 995-48-20



Кирилл Аверченко

Руководитель отдела
технического пресейла,
Компания «Актив»
Averchenko@rutoken.ru
+7 495 925-77-90

