РУТОКЕН

Токен + Российский VPN.
Нестандартные сценарии использования

Шпаков Андрей
Руководитель проектов
по информационной безопасности
Компания «Актив»

Традиционные сценарии «Токен+VPN»

Криптошлюз + токен

Хранение ключей?

Удаленный доступ

- Хранение ключей
- Дополнительные факторы аутентификации — владение токенов и PIN

И это все сценарии?

I. Виды токенов по типу выработки ключа

Пассивные —

используются для хранения ключа (а не выработки).

«Флешка с PIN-кодом» (с)

Активные —

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

«Настоящий токен» (с)

Разница для нас — в сроке хранения ключа (<15 месяцев vs 36 месяцев)

II. Программные интерфейсы токенов:

Низкоуровненый интерфейс — APDU

Универсальный интерфейсы — PKCS#11, Microsoft CryptoAPI

Высокоуровненый интерфейс: Рутокен Плагин на основе JavaScript

III. Программные интерфейсы: плюсы и минусы для VPN

Интерфейс\критерий	APDU	Crypto API
Плюсы	Прямой доступ к функциям токена	Глубокая интеграция с Windows
Минусы	• Большой объем кода • Сложность поддержки	• Требует наличия криптопровайдера • Костыли для non-Windows
Где используется?	АПМДЗ	КриптоПро CSP
		КРИПТОПРО

III. Программные интерфейсы: плюсы и минусы для VPN

Интерфейс\критерий	PKCS#11
Плюсы	• Общепризнанный стандарт • Кроссплатформенность • Поддержка всех типов объектов на токене
Минусы	Плохо поддерживается в Windows
Где используется?	Почти везде

Все криптошлюзы и VPN-клиенты используют PKCS#11

III. Файловая система токена

ОС токена работает с фиксированной файловой системой (как FAT)
К данным используется дискретное разграничение прав доступа.

Типы данных:

- Открытые ключи
- Закрытые ключи
- Журналы устройства
- **Другие данные**

Можно ли из токена сделать хранилище менеджера паролей? — Да!

Сценарий №1. Хранение политики безопасности VPN-клиента на токене

Задача:
обеспечить удаленный доступ сотрудников в банк, при этом:

- В компании — жесткое разделение ответственности — IT\ИБ
- Типовой ноутбук для каждого сотрудника — готовит IT
- Персональный токен для каждого сотрудника — готовит ИБ
- КриптоПро УЦ для выпуска сертификатов — рулит ИБ
- Управление ключами реализуется через систему PKI Management

Сценарий №1. Хранение политики безопасности VPN-клиента на токене

Решение:

- С-Терра Клиент для удаленного доступа\С-Терра Шлюз для терминации VPN
- Сценарий «Token Pattern» или «Политика на токене»
- Пользователь получает ноутбук с типовым «образом» (ОС, Софт, «пустой» VPN-клиент с демолицензией)
- Пользователь получает токен, который содержит ключи для ЭП (ЭДО), Ключи для аутентификации в VDI и политику безопасности VPN (файл LSP)
- Персонализация токенов — AvanPost PKI (PKCS №11-интерфейс)
- Лицензии на клиентов — меняются через С-Терра КП

Сценарий №1. Хранение политики безопасности VPN-клиента на токене

Какие плюшки по итогу?

Корпоративный Compliance

Баланс сил между IT и ИБ — соблюден.
Ноуты готовит IT, ИБ — готовит токены

Масштабируемость

Срок подготовки корпоративного ноутбука – сокращен

Унификация

VPN-клиент, по-сути, просто пустой дистрибутив.
Все остальное – на токене

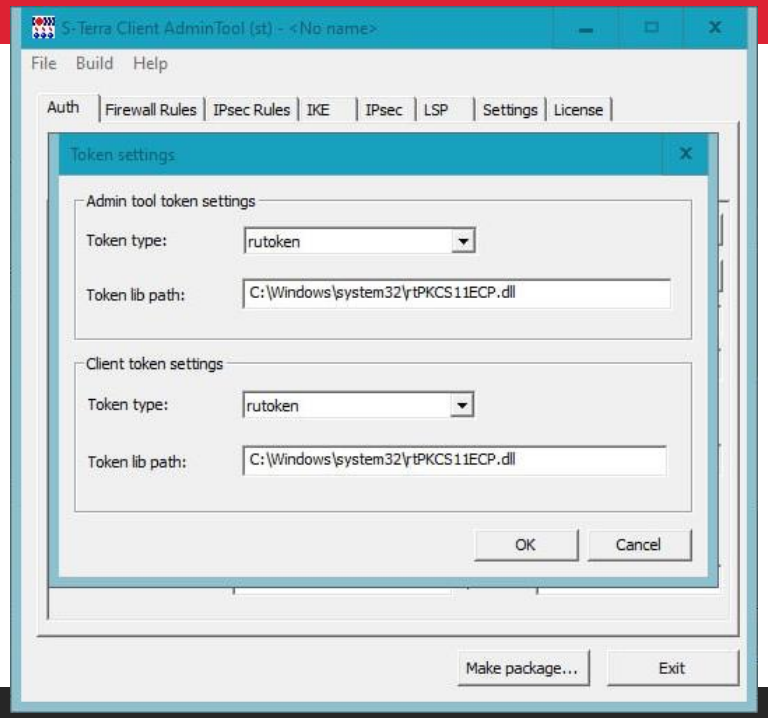
Оптимизация

За счет интерфейса PKCS#11 кастомизацией VPN занимается AvanPost PKI

Сценарий №1. Хранение политики безопасности VPN-клиента на токене

Что нужно от вендора VPN?

- **Иметь +- статический конфиг в виде файла (по аналогии с LSP S-Terra)**
- **Поддержать стандартный интерфейс PKCS#11.**
  Проверить работу с библиотека основных вендоров
- **Добавить инструменты в GUI для работы с токеном**



Ссылка на сценарий – линк. На токене можно хранить любые небольшие статические данные (например лицензии)

Сценарий №2. Дополнительная аутентификация через OTP для Remote-Access

Задача:

обеспечить удаленный доступ с дополнительной аутентификацией пользователя при подключении, обеспечив, при этом, более эффективный метод, чем логин\пароль.

Решение:

- Продукты — С-Терра VPN 4.3\ КриптоПро Ngate 1.0R2
- Сервер аутентификации (RADIUS-сервер) поддерживающий расширение Access-Challenge
- На сервере: генератор H-OTP или T-OTP согласно спецификации OATH
- Пользователю: программный или аппаратный токен для OTP
- (Опционально) — служба каталогов

Сценарий №2. Дополнительная аутентификация через OTP для Remote-Access

Немного теории:

- OATH- Initiative for Open Authentication, инициативная группа по придумываю протоколов
- H-OTP — HMAC-Based One-Time Password Algorithm, RFC4226
- T-OTP — Time-based One-Time Password Algorithm, RFC6238

oath
initiative for open authentication
CERTIFIED

Примеры «правильных» RADIUS-серверов:

- Коммерческие — Cisco ISE, Jacarta Authentication Server
- Open-source — FreeRadius + LinOTP — opensource

Не путайте OTP и одноразовые пароли по SMS!

Сценарий №2. Дополнительная аутентификация через OTP для Remote-Access

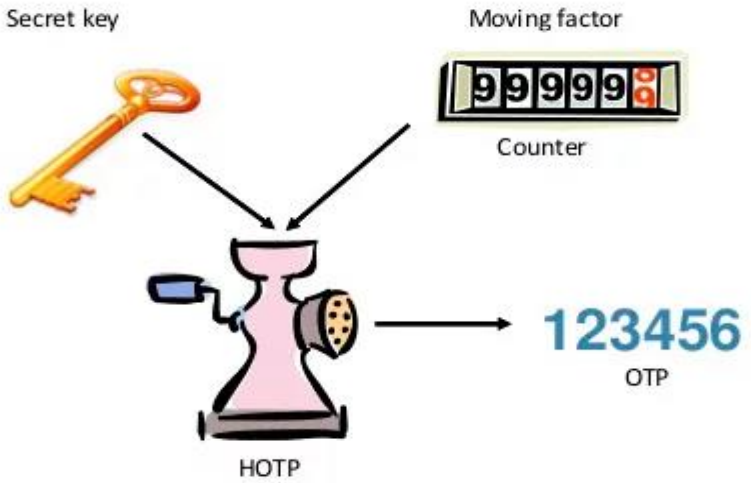
Принцип работы:

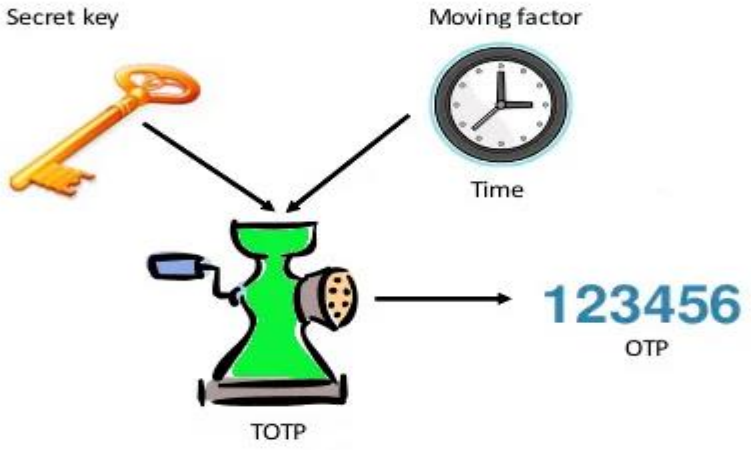
H-OTP

- Общий ключ
- Счетчик
- Хеширование (SHA1 или SHA2)

T-OTP

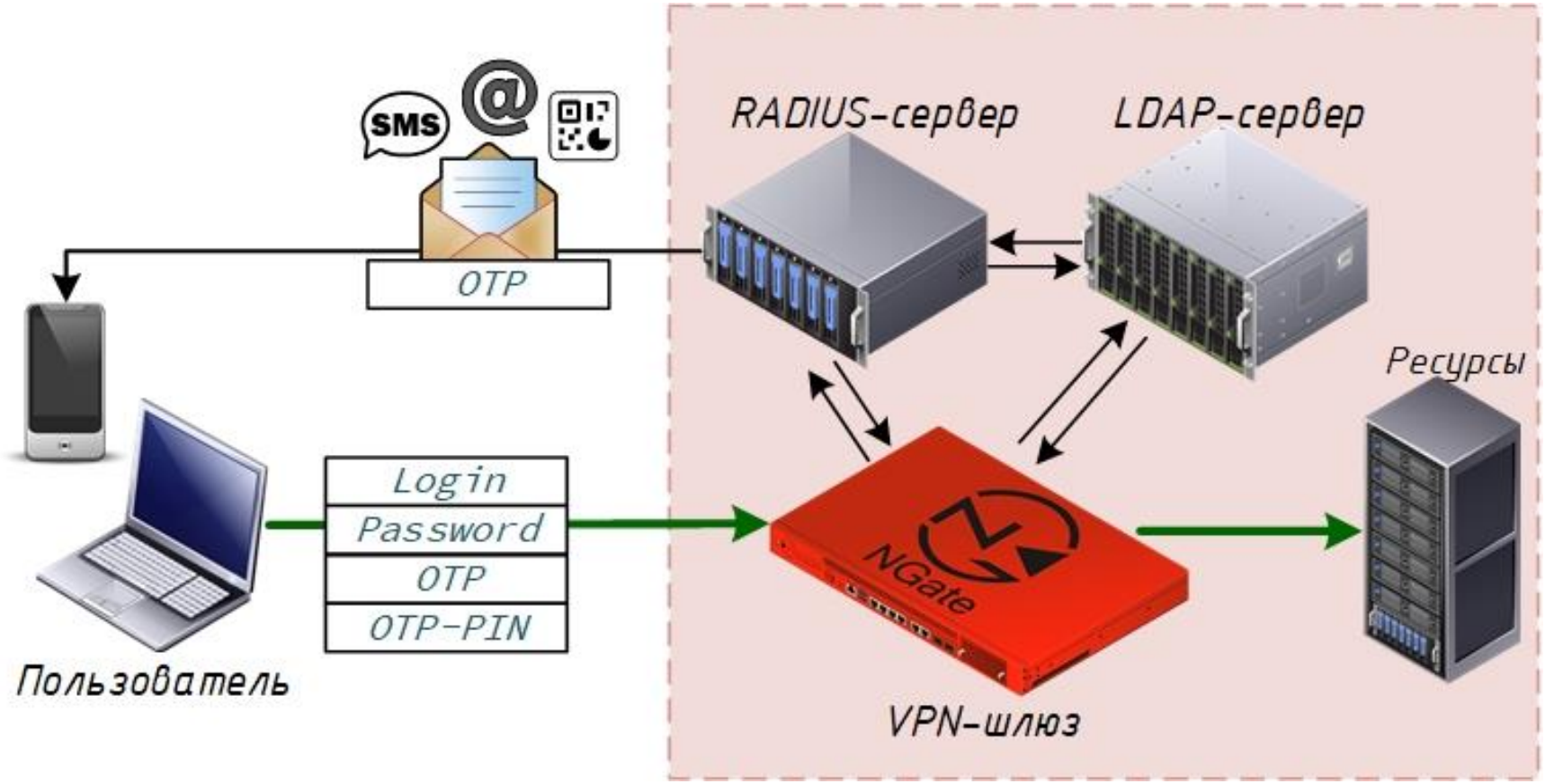
- Общий ключ
- Время
- Хеширование (SHA1 или SHA2)





Сценарий №2. Дополнительная аутентификация через OTP для Remote-Access

Схема в продакшене:



Сценарий №2. Дополнительная аутентификация через OTP для Remote-Access

Виды клиентских устройств:

Программные:

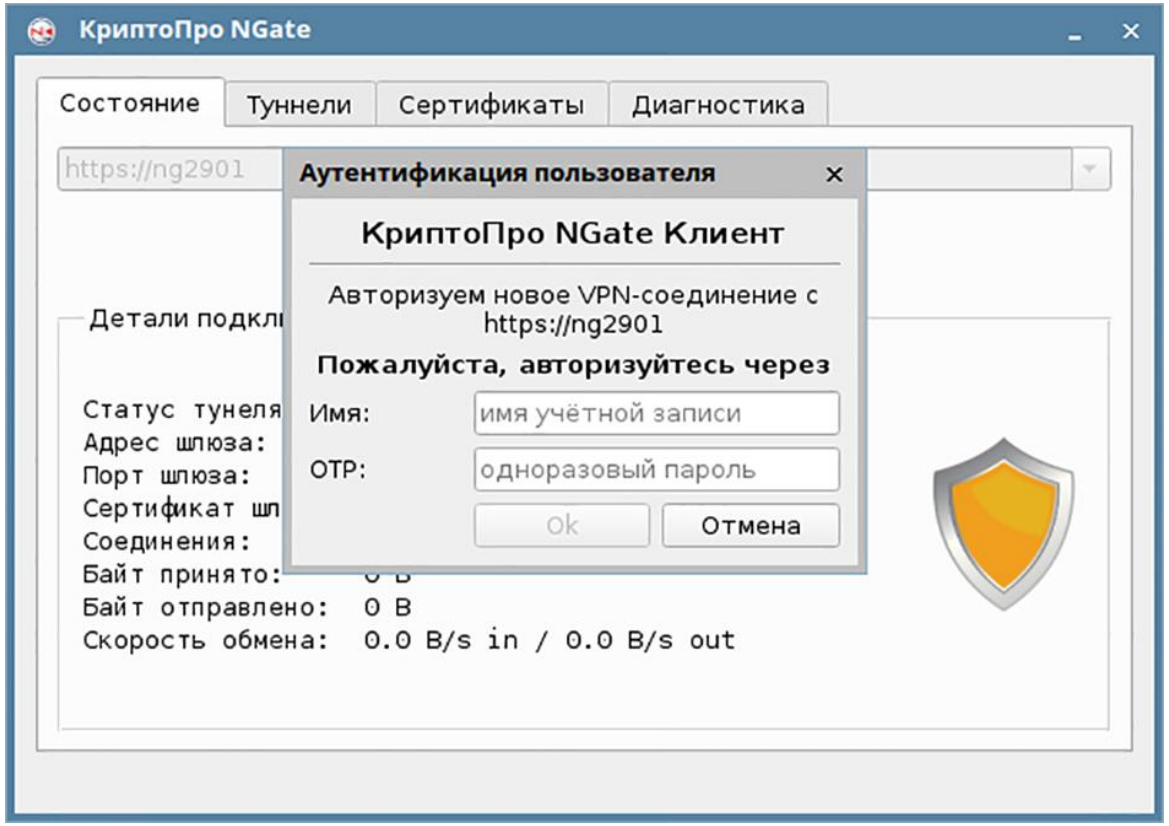
- Google Authenticator
- Яндекс Ключ
- Yubico Authenticator

Аппаратные:

- Рутокен OTP (old)
- Рутокен OTP (new)
- Yubikey

Сценарий №2. Дополнительная аутентификация через OTP для Remote-Access

Как это выглядит для пользователя?



Сценарий №2. Дополнительная аутентификация через OTP для Remote-Access

Какие плюшки по итогу?

Бесплатная безагентская интеграция с AD

За счет RADIUS-а

Многообразие выбора клиентских устройств

Программные и аппаратные токены

Качественный доп.фактор аутентификации

OTP — баланс между стоимостью внедрения и качеством аутентификации

Минусы: слабая поддержка OTP у российских RADIUS-серверов

Сценарий №3. 3-х летняя схема распределения ключей

Задача:
обновить ГК КШ в сети Континента «легально»

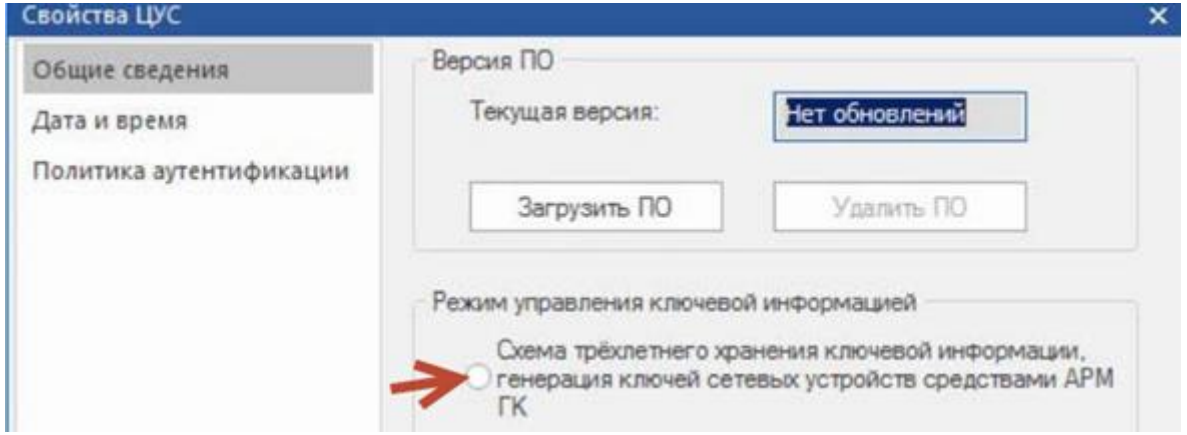
Фрагмент из ПП на Континент 3.9:

рассылка ключевых документов производится доверенным способом (уполномоченными людьми согласно установленной процедуре) на узлы сети (возможна передача ключевой информации по специальным шифрованным каналам связи, предназначенным для передачи ключей, аттестованным ФСБ России);

Сценарий №3. 3-х летняя схема распределения ключей

Решение:

- Сеть VPN на АКПШ Континент 3.7.7\3.9
- Трехлетняя схема распределения ключей
- АРМ ГК (на базе IPC-10), не имеющий сетевых соединений
- Рутокен ЭЦП на каждый КШ



Сценарий №3. 3-х летняя схема распределения ключей

Процесс разворачивания:

1. Генерируем на АРМ ГК 3 ключа (каждый по году) на каждый Рутокен ЭЦП
2. Рассылаем ключи вместе с КШ. Инициализируем КШ
3. Активируем ключи посредством ПУ ЦУС
4. Меняем ключи раз в год через ПУ ЦУС
5. По итогу 3-х лет повторяем процедуру заново

Сценарий №4. Проблемы удаленного обновления ключей

Предпосылки:

Класс АПМДЗ оказался под угрозой после начала СВО

СофтМДЗ сейчас использует БиоДСЧ или гамму с ЦУС

Класс СофтМДЗ получил резкий скачек (Инфотекс — 100% платформ, С-Терра — 60% платформ, КодБез — исследует почву)

ФДСЧ стоит достаточно дорого (~4500 ₽)

Пересылка гаммы может быть запрещена в обозримой перспективе. Как тогда удаленно обновлять ключи?

Сценарий №4. Проблемы удаленного обновления ключей

Гипотеза: использование активных токенов в составе КШ

Потенциальные плюшки:

- Смена ключей раз в 3 года, вместо 1 года
- Генерация ключей без пересылки гаммы по сети
- Уменьшение затрат на администрирование

Потенциальные риски:

- Зависимость сертификата соответствия КШ от сертификата токена
- Большая работа с регулятором по Формулярам, ПП и сценариям

Вопросы

Контактная информация

Шпаков Андрей

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

РУТОКЕН