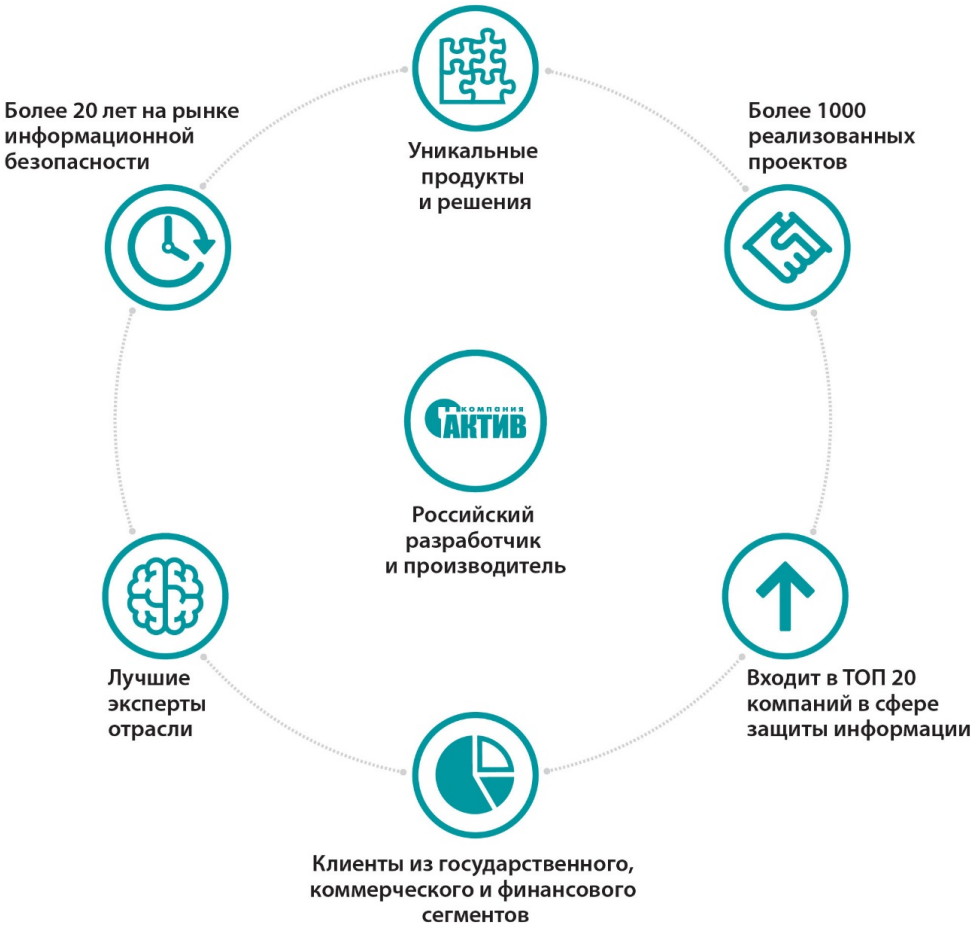
Конференция «Эволюция облаков и ЦОД в эпоху цифровой трансформации»

Варианты двухфакторной аутентификации при работе с облачными сервисами

Андрей Игнатов,
компания «Актив»

РУТОКЕН


Более 20 лет на рынке информационной безопасности
Уникальные продукты и решения
Более 1000 реализованных проектов
Компания Актив
Российский разработчик и производитель
Лучшие эксперты отрасли
Входит в ТОП 20 компаний в сфере защиты информации
Клиенты из государственного, коммерческого и финансового сегментов

РУТОКЕН

Зачем нам двухфакторная аутентификация в облаке

- Данные находятся за пределами организации
- Есть множество способов перехвата логина и пароля для доступа к облаку
- Злоумышленник может работать в облаке без ведома легального пользователя
- Есть положительные примеры эффективности защиты
- Google выдал аппаратные токены сотрудникам и в течении года не было ни одного взлома

РУТОКЕН

Что такое двухфакторная аутентификация

- **Фактор 1. «Я знаю».** Ввод пароля
- **Фактор 2. «Я имею».** Обладание физическим устройством
- **Фактор 3. «Я есть».** Биометрия — отпечатки, лицо, радужка
- Выбираем два фактора — вот и двухфакторная аутентифкация

Что не так с биометрикой

- Медленно
- Дорого
- Не надежно
- Количество глаз и пальцев конечно

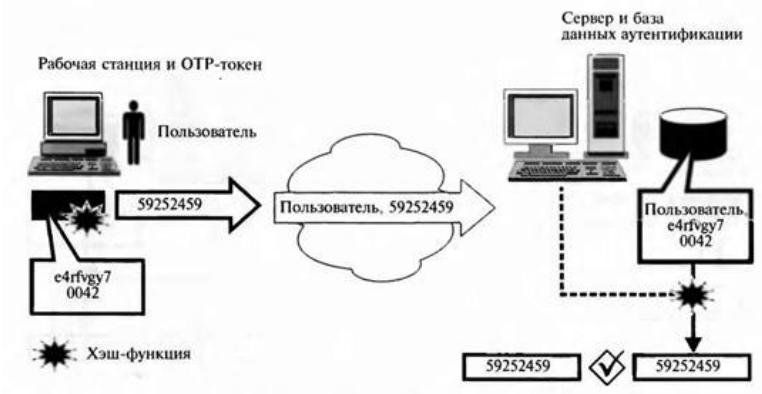
Варианты реализации фактора «Я имею»

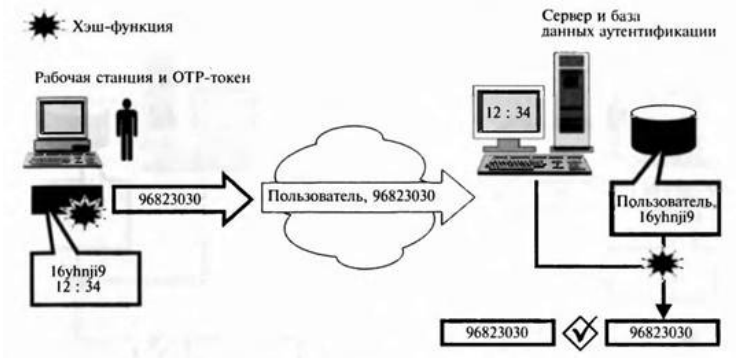
- OTP (One Time Password)
  - HOTP
  - TOTP
- USB-токены и смарт-карты + PKI
- FIDO U2F

РУТОКЕН

Аутентификация с помощью OTP

- Одноразовые пароли, используемые только в одной попытке аутентификации
- Токен зашифровывает либо счетчик количества подключений (HOTP), либо текущее время (TOTP) и выдает в виде числа (одноразового пароля), который отправляется на сервер
- Сервер также вычисляет одноразовый пароль, если они совпадают, то производится аутентификация





Способы генерации паролей OTP

- Программа для смартфона (Google Authenticator, Microsoft Authenticator)
- SMS-сервис
- Аппаратный токен с дисплеем
- Аппаратный токен с интерфейсом USB-HID

Плюсы OTP

- Дешево. А в случае программы для смартфона вообще бесплатно
- Удобно, но только в случае USB-HID
- Психологически понятно для пользователя

Минусы OTP

- Одноразовый пароль каждый раз необходимо вводить вручную
- При использовании SMS или программы для смартфона уровень защиты сильно снижается
- Устройство нельзя использовать для других целей
- В случае несовпадения часов токена и сервера, либо количество генераций ключа и попыток аутентификации, возможны ошибки
- Клиентскую и серверную часть для каждого сервера необходимо реализовывать отдельно
- Второй фактор аутентификации (пароль) нужно

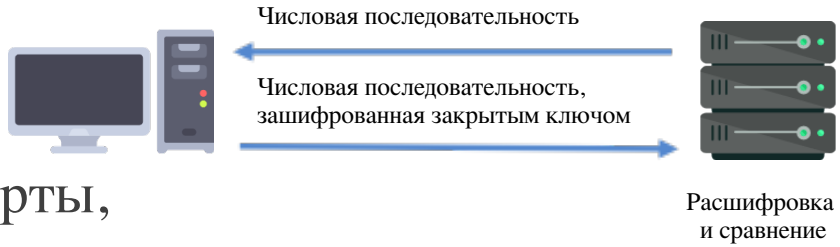
РУТОКЕН

Аутентификация с помощью USB-токенов / смарт-карт

- Уже реализовано в инфраструктуре Windows (сервер и клиент) и в облачной Azure
- У каждого пользователя есть USB-токен или смарт-карта
- На них хранятся неизвлекаемые личные ключи и сертификаты открытых ключей
- Существует Центр сертификации, который подписывает сертификаты ключей, удостоверяя их подлинность

Схема аутентификации

- Пользователь подключает свой USB-токен к порту USB,
а смарт-карту к считывателю.
- Пользователь вводит PIN-код токена или карты, чтобы разблокировать доступ к устройству.
- Используются асимметричные алгоритмы шифрования
RSA и отлично опробованные механизмы инфраструктуры
открытых ключей (PKI)
- Сервер аутентификации генерирует случайную числовую последовательность (challenge) и отправляет её на клиенту.



Плюсы токенов / смарт-карт

- Фактор знания пароля уже встроен в функционал токена — ничего на сервере реализовывать не нужно.
- Достаточно просто добавить аутентификацию к любому облачному сервису или приложению.
- В Microsoft Windows и Azure этот механизм уже реализован.
- Токены и смарт-карты можно использовать для хранения других ключей, предназначенных для ЭП, и прочей критической информации.
- Существуют токены, которые дополнительно защищены
с помощью кнопки на корпусе.

Минусы токенов / смарт-карт

- Стоит дороже, чем программные OTP-токены или SMS.
- Нет встроенной поддержки на уровне браузера (но есть от производителя токенов).
- Для интеграции с каждым конкретным сервисом, необходимо использовать либо библиотеки производителя токена, либо устанавливать криптопровайдер.

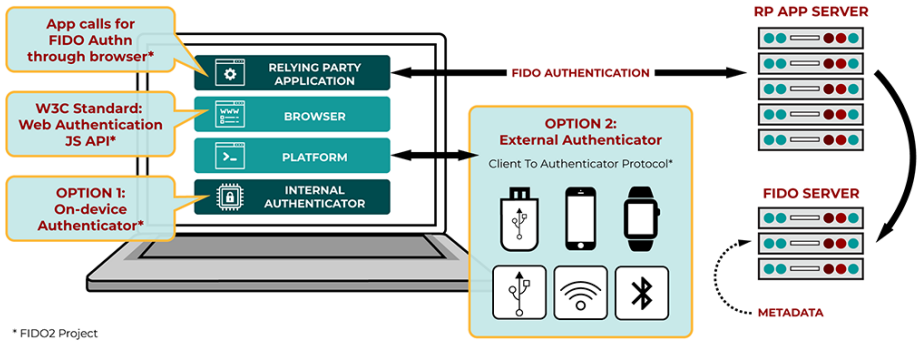
РУТОКЕН

Аутентификация с помощью токенов FIDO

- Стандарты разрабатывает FIDO Alliance, в него входят производители браузеров, смартфонов, провайдеры и пр.
- Ставилась цель создать недорогой способ надежной аутентификации с максимально широкой поддержкой.
- Текущий стандарт FIDO2
- Состоит из протокола CTAP (взаимодействие браузера с токеном) и WebAuthn (реализация аутентификации в web-сервисе).
- Производят, например, Google (Titan) и Yubico (Yubikey)

Схема аутентификации

- Каждый сервис имеет собственную базу для хранения ключей, либо обращается к серверу FIDO.
- При регистрации пользователя ключи генерируются
на токене и передаются в сервис.
- Использование пароля для FIDO2 не предусмотрено стандартом.
- Для аутентификации необходимо вставить токен в USB-порт, ввести свое имя и прикоснуться к определенному месту на корпусе токена.
- Сервис отправляет на клиенту



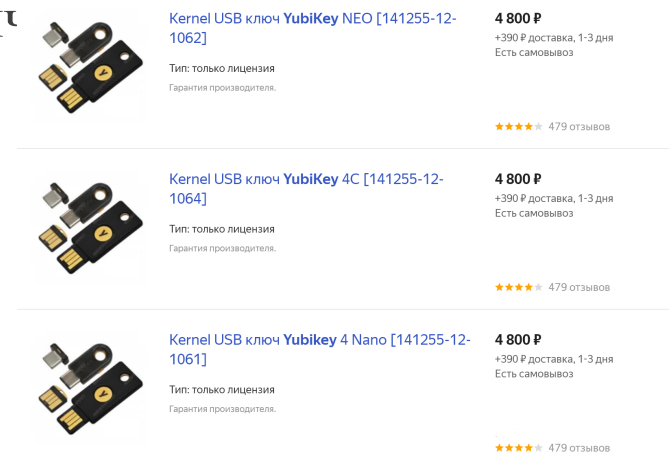
Плюсы токенов FIDO

- Поддержка FIDO2 встроена в ряд популярных облачных сервисов: Google Cloud, Dropbox, Salesforce и др.
- Не нужно реализовывать код поддержки FIDO2 на стороне клиента, в т.ч. мобильного
- Если в ключ встроен NFC, то будет работать почти на любом устройстве не для Китая

РУТОКЕН

Минусы токенов FIDO

- Несмотря на желание сделать дешевый токен, стоимость устройств YubiKey в России около 4 тысяч
- Стандарты есть далеко не на все аспекты аутентификации,
например обращение к серверу FIDO не стандартизировано
- В базовом варианте токены никак не защищены, то есть ими может пользоваться любой, достаточно только знать имя пользователя,
то есть фактически это однофакторная аутентификация
- Есть варианты токенов с биометрической защитой и клавиатурой



Перспективы использования различных вариантов двухфакторной аутентификации

- **SMS и программные OTP:** будут активно внедряться в первую очередь в бесплатных сервисах
- **Аппаратные OTP без HID:** будут использоваться в унаследованных сервисах и постепенно отмирать
- **Аппаратные OTP с HID:** займут свою нишу (например, платный сервис и низковалифицированные пользователи)
- **USB-токены и смарт-карты:** будут использоваться в сервисах, где безопасность критична. То есть в большинстве корпоративных сервисов.
- **Токены FIDO2:** будут продвигаться в первую очередь международными корпорациями, такими как Facebook, Google и Amazon. То есть будет актуально для сервисах размещенных в данных облаках. Внедрение на сторонних сервисах в ближайшее время маловероятно. В России надолго останется уделом энтузиастов.

РУТОКЕН

Вопросы

РУТОКЕН

Контактная информация

Андрей Игнатов

Электронная почта:
aignatov@rutoken.ru

Сайты:
www.rutoken.ru
www.aktiv-company.ru

Телефон:
+7 495 925-77-90
+7 968 813-49-28