РУТОКЕН

PKI-форум 2018
Санкт-Петербург, 24–27 сентября 2018

Куда движутся технологии аутентификации пользователей?

Аутентификация и электронная подпись, открытые информационные системы и корпоративные проекты.

Кирилл Мещеряков,
директор продуктового направления Рутокен,
Компания «Актив»

КРУПНЫЕ КОРПОРАЦИИ

Microsoft

- 2FA с использованием PKI реализована очень давно
- Слой работы со смарт-картами был придуман в Microsoft и был портирован на Linux и Mac
- Использует смарт-карты и токены более 18 лет для удаленного доступа
- Добавлена реализация 2FA с использованием Windows Hello for Business
  - Смарт-карта заменена на TPM
  - PIN-код может быть заменен на биометрические данные

Google

- Простая парольную защиту
- Двухэтапная аутентификация с помощью SMS
- Двухфакторную аутентификация с помощью Google Authenticator
- Ничего из этого корпорация сама не использует! Интересно, почему ;-)

А вот, например, почему

- Житель Ростова-на-Дону, используя незаконно приобретенную базу данных сим-карт абонентов с электронными ключами к ним, а также специальное программное обеспечение, изготавливал дубликаты сим-карт мобильных номеров, подключенных к банковским картам.
- С их помощью злоумышленник списывал денежные средства со счетов граждан и, проводя их через цепочку транзакций, обналичивал с помощью электронного кошелька. Он подозревается в хищении 27 млн рублей.

https://www.interfax.ru/russia/623902
https://blockchain.ru/posts/20-letnij-student-iz-bostona-ukral-putem-vzloma-sim-kart-bolee-5-mln-v-kriptovalyute

Токены в Google

- Корпорация Google в начале 2017 года перевела аутентификацию всех своих сотрудников (более 85 тысяч человек) на аппаратные токены.

- С тех пор не было зафиксировано ни одной успешной кражи аккаунтов сотрудников.

  https://meduza.io/feature/2018/07/24/samaya-nadezhnaya-zaschita-ot-fishinga

Токены от Google для людей

- Google Titan уже в продаже ~ $50 (производства Feitian)

  https://store.google.com/us/product/titan_security_key_kit

  https://www.ftsafe.com/Products/FIDO

- Поддерживают стандарты аутентификации FIDO
- Позволяет выполнять надежную и действительно двухфакторную аутентификацию в сервисах Google

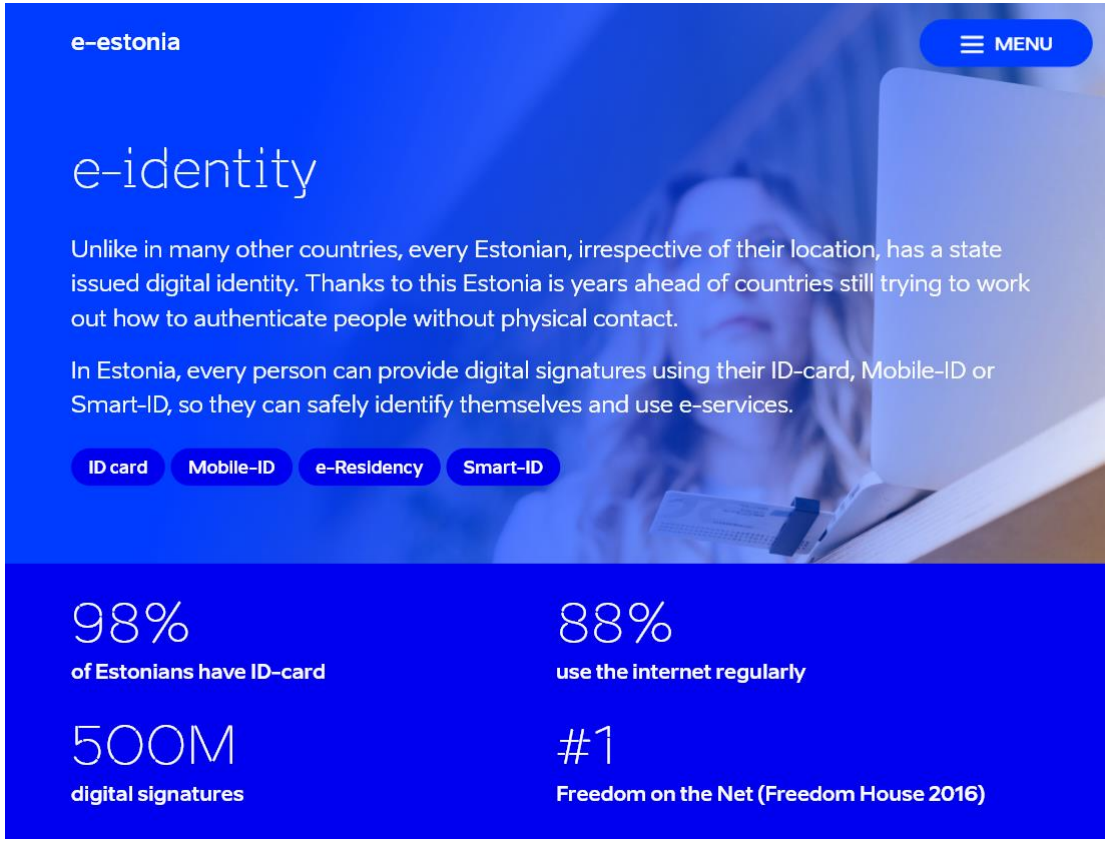
Вывод #1

- Корпорации, обладающие разнообразным набором технологий на любой вкус,
  SMS и OTP системами аутентификации,
  для себя выбирают **аппаратные устройства**
- Внедрение аппаратных токенов для 2FA показывает, что время старых методов уходит.
  Продвижение 2FA и гигиены информационной безопасности дает свои плоды.
  Новое поколение миллениалов гораздо активнее задумываются о безопасности.
  https://www.crn.ru/news/detail.php?ID=124375

ГОСУДАРСТВО

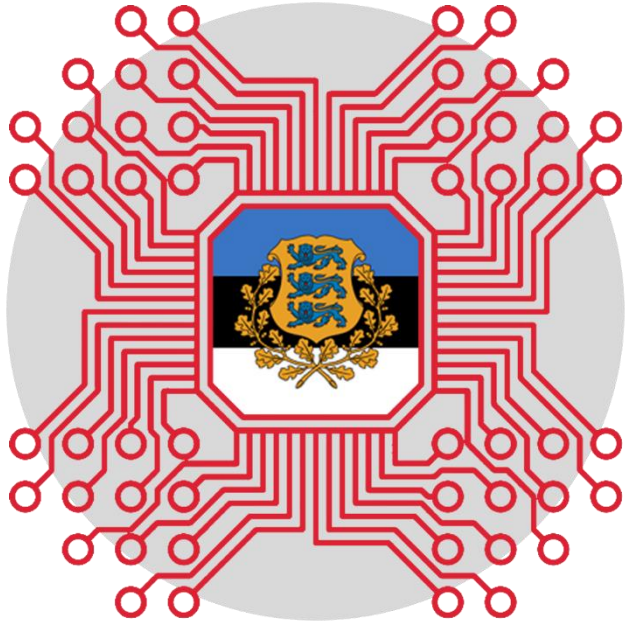
E-estonia

- Государство поставило себе задачу обеспечить граждан смарт-картами, а все сервисы — возможностью использования
- Когда государство ставит себе задачу обеспечить своих граждан надежным механизмом 2FA и ЭП, то цифра 98% обладателей ID-card становится реальностью



Единый инструмент для…

- legal travel ID for Estonian citizens travelling within the EU
- national health insurance card
- proof of identification when logging into bank accounts
- for digital signatures
- for i-Voting
- to check medical records, submit tax claims, etc.
- to use e-Prescriptions

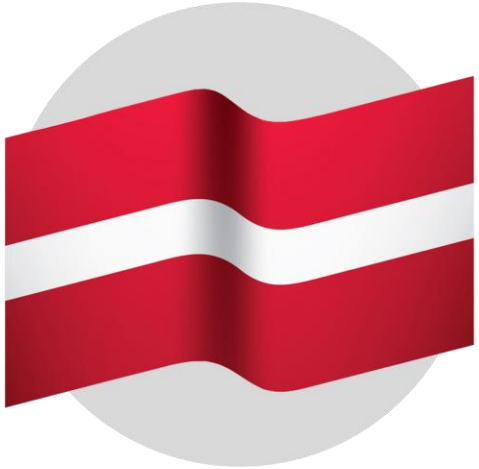


E-residency

- Ведение европейского бизнеса онлайн
- Одна смарт-карта = доступ ко многим сервисам
  - Бизнес
  - Финансы
  - Государства

А вот в Латвии…

- E-ID каждого гражданина позволяет хранить ключ ЭП
- Генерация ключа платная (около 8 евро),
  срок действия — год
- Если ключа нет, то для ЭП можно использовать
  государственный DSS (2-3 евро за подпись)
- Аутентификация в DSS осуществляется с помощью ДБО
  одного из латвийских банков
- Сложность аутентификации зависит от статуса клиента
  (суммы на счете) – от программного ОТП
  до аппаратного ОТП от Vasco с поддержкой
  с PIN-кода и challenge-response



Вывод #2

- Государства которые не на словах, а на деле становятся цифровыми государствами – своими силами развивают как инфраструктуру смарт-карт, так и сервисы, доступные с их помощью — 2FA и ЭП, а главное систему государственного доверия
- Вложения в инфраструктуру и аппаратное обеспечение для PKI многократно окупается через снижение нагрузки на чиновников и уменьшение их количества

ИНФРАСТРУКТУРА

Новые стандарты и протоколы 2FA

- FIDO опубликовал новый стандарт FIDO2 в дополнение к U2F
- В него входит:
  - протокол CTAP для связи между браузером/OS и токеном
  - Протокол WebAuthn для стандартной и одинаковой безопасной аутентификации web
- Реализуется поддержка всеми браузерами

Выходят новые устройства

- Gemalto, NXP, ACS, Yubico, Feitian, Актив выпускают новые устройства и новые классы устройств
- Новые «непривычные» способы:
  - U2F
  - FIDO/FIDO2
  - Bluetooth (BLE)
  - NFC
  - Устройства с экраном
- В разы повысилась скорость вывода устройств на рынок (пример – поддержка FIDO2), а значит увеличились суммы на R&D

Некоторые опасались падения, а по факту наблюдается рост

- Появляются новые модели и разновидности токенов, смарт-карт и считывателей
- Криптография в интернете уже никого не удивляет, интернет активно переходит на HTTPS
- Bluetooth и NFC больше не экзотика, а тренды
- Количество продаваемых и **используемых** устройств растет

Вывод #3

- Слухи о смерти персональных аппаратных технологий для безопасной аутентификации значительно преувеличены
- Создаются новые методы аутентификации, новые версии уже известных методов, стремительно появляется их поддержка в браузерах и ОС, выходят новые устройства
- В мире использование криптографических аппаратных носителей становится устойчивым трендом

И ЕЩЕ ОДНА ВЕЩЬ…

CAST OF “GAME OF THRONES” WAS REQUIRED TO SET UP TWO-FACTOR AUTHENTICATION ON THEIR EMAIL ACCOUNTS THIS YEAR

Контактная информация

Кирилл Мещеряков

Электронная почта:

mk@rutoken.ru

hotline@rutoken.ru

Сайты:

www.rutoken.ru

www.aktiv-company.ru

Телефон:

+7 495 925-77-90

+7 905 509-70-24