KEYNECTIS® OPE

Почему PKI?

Почему PKI?

KEYNECTIS OPE

Потому что преграды…

…очень легко обойти!

Почему PKI?

KEYNECTIS OPE

Потому что защищая только что-то одно...

...Вы можете потерять все остальное!

Почему PKI?

KEYNECTIS OPE

Потому что личные данные…

…можно легко подделать!

KEYNECTIS OPE

PKI позволяет делать следующее:

- **Укрепить и дополнить преграды**

  Строгая аутентификация

- **Обеспечить идентификацию пользователя**

  Цифровая подпись, строгая аутентификация

- **Защитить данные**

  Шифрование данных

Что можно сделать с помощью PKI

KEYNECTIS OPE

С PKI доступны следующие технологии:

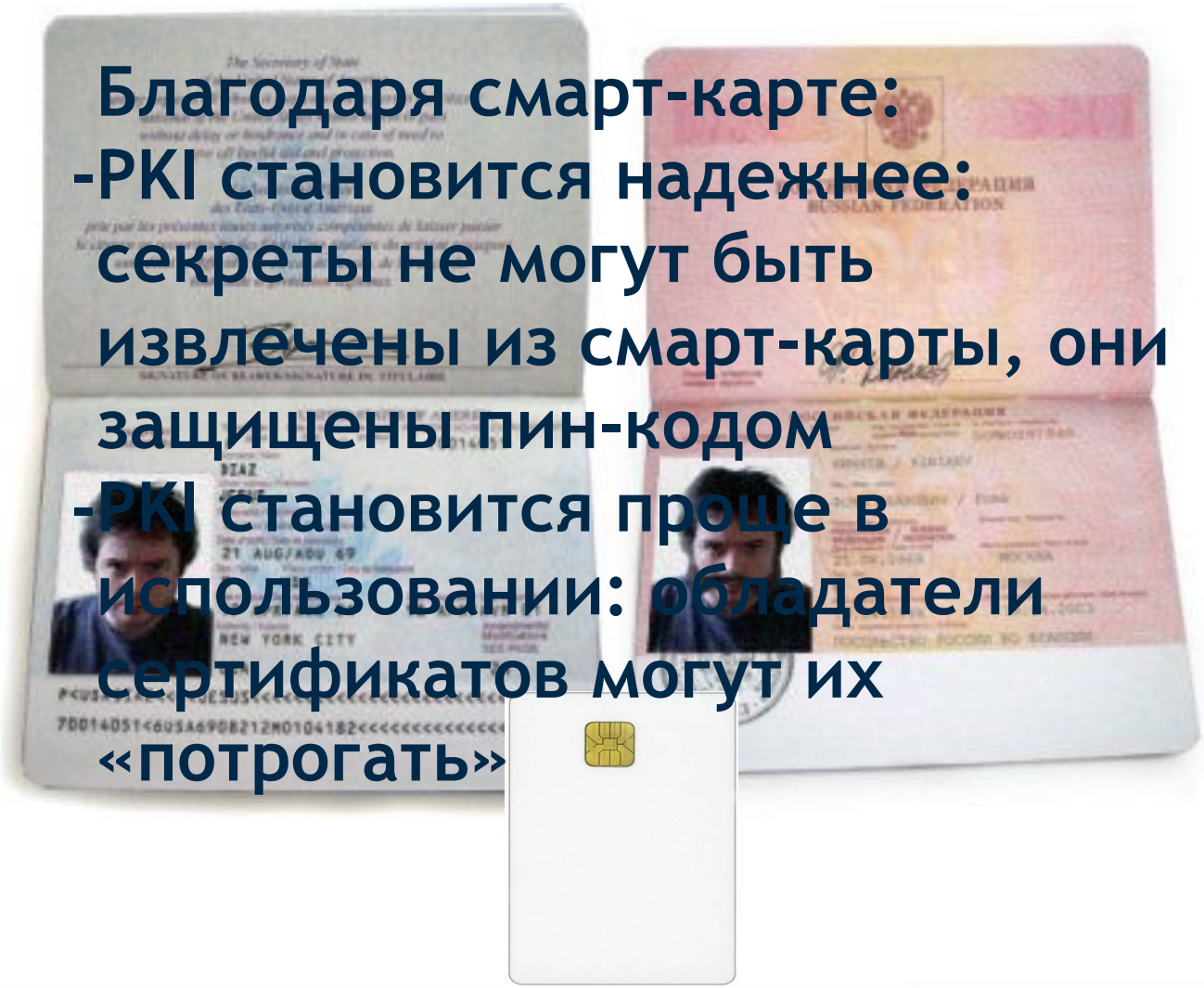
- **Строгая аутентификация для вех пользователей**
  HTTPS, End User VPN, E-Mail,…
- **Строгая аутентификация для всех компьютеров**
  WiFi, 802.1X, Branch Office VPN,…
- **Цифровая подпись**
  S/MIME E-Mail Signature, PDF/A Signature, XAdES,…
- **Шифрование данных**
  S/MIME E-Mail Encryption, Disk Encryption,…

Некоторые из этих функций сразу готовы к использованию с привычным ПО Microsoft, Mozilla Foundation, Apache Foundation, итд.: все что необходимо, это конфигурация и управление сертификатами

PKI и паспорт

- **Вам это уже знакомо!**
- **В реальной жизни, в любом месте на планете, ID=Паспорт**
- **В цифровом мире, ID=Сертификат**
- **PKI - инструмент управления сертификатами. Включает в себя следующие модули:**
  - **Регистрационный центр (EE)**
    - Аналог для обычного паспорта : Acceptance Facility (Почта, Администрация, …)
  - **Удостоверяющий центр (RA)**
    - Аналог: Паспортный стол
  - **Центр сертификации (CA)**
    - Аналог: завод по изготовлению паспортов

Why Smart cards?



Благодаря смарт-карте:

-PKI становится надежнее: секреты не могут быть извлечены из смарт-карты, они защищены пин-кодом

-PKI становится проще в использовании: обладатели сертификатов могут их «потрогать»

КЛЮЧЕВЫЕ ОСОБЕННОСТИ

KEYNECTIS OPE

Поддержка ГОСТ на базе сертифицированных СКЗИ

- Разработано совместно с ведущим Российским разработчиком СКЗИ «КриптоКом»
  - На базе сертифицированных СКЗИ
  - Полная поддержка:
    - ГОСТ Р 34.10-2001
    - ГОСТ Р 34.11-94
    - ГОСТ 28147-89

OpenTrust PKI - примеры внедрений

ОАО «КАМАЗ» выбрал решение OpenTrust PKI для решения следующих задач информационной безопасности:

- ✔Защита корпоративной электронной переписки (e-mail) электронно-цифровой подписью (ЭЦП), гарантирующей подлинность отправителя и целостность сообщения,
- ✔Безопасная аутентификация пользователей и устройств для доступа к корпоративным серверам по защищенному каналу,
- ✔
- ✔Надежное шифрование важных данных, в том числе отправляемых по e-mail сообщений, в целях обеспечения эксклюзивного доступа к ним соответствующих лиц.

OpenTrust PKI - примеры внедрений в крупнейших европейских организациях

более 80 000 пользователей - корпоративные бэйджи, для физического доступа в помещение и доступа к сети и приложениям

OpenTrust PKI + OpenTrust SCM

более 60 000 пользователей - корпоративные бэйджи, шифрование, безопасный WiFi

Интеграция с SSO (Evidian) и IAM (SUN)

OpenTrust PKI + OpenTrust SCM + Opentrust MFT

более 7 000 пользователей в 130 странах - защищенная электронная почта

OpenTrust PKI

Q&A