Технология Bluetooth как способ расширения PKI на мобильные платформы

Кузнецов Сергей Борисович, Региональный Директор в России и СНГ

Сентябрь 17, 2015

Слияние двух лидеров

Security at the CORE

№1 в мире

Мировой лидер в PKI USB технологии токенов

Security at the EDGE

№1 в мире

Мировой лидер в PKI Смарт Кард технологиях

Мировой лидер в цифровой безопасности

Уникальность. Глобальность. Инновационность

IDCore семейство продуктов

Java Card 2.2.2

Полное соответствие стандартам
GP 2.1.1.A
(включая SCP01, SCP02, SD-извлечение & Delegated Management)

3DES (ECB, CBC)
AES (128,192,256)
SHA-1, SHA-256,384,512,
RSA 2048,
ECC P-224 - 521

Высокая производительность (до 460 kbps)

T=0, T=1, T=CL
Протоколы обмена

ISO14443 type A&B
Compliant
(106, 212, 424, 848 Kbps)

Поддержка RSA & Генерация ключа на Чипе до 2048 bits

Сохранность данных до 25 лет

Апплеты в ROM:
MPCOS, OATH

GOST 28147-89,
R 34.10-2001,
R 34.10-2012
доступна
(опция)

Варианты памяти EEPROM:
80 - 128 Kbytes

ГОСТ совместимое (смарт карта и токен)

JavaCard 2.2.2
Global Platform 2.1.1

CryptoPro PKI апплет на борту

122 KB память для данных и апплетов

ECC на чипе
Генерация ключа по GOST R 34.10-2001

ЕЦП по GOST R 34.10-2012

T=0 протокол обмена

Минимум 500,000 циклов запись/удаление

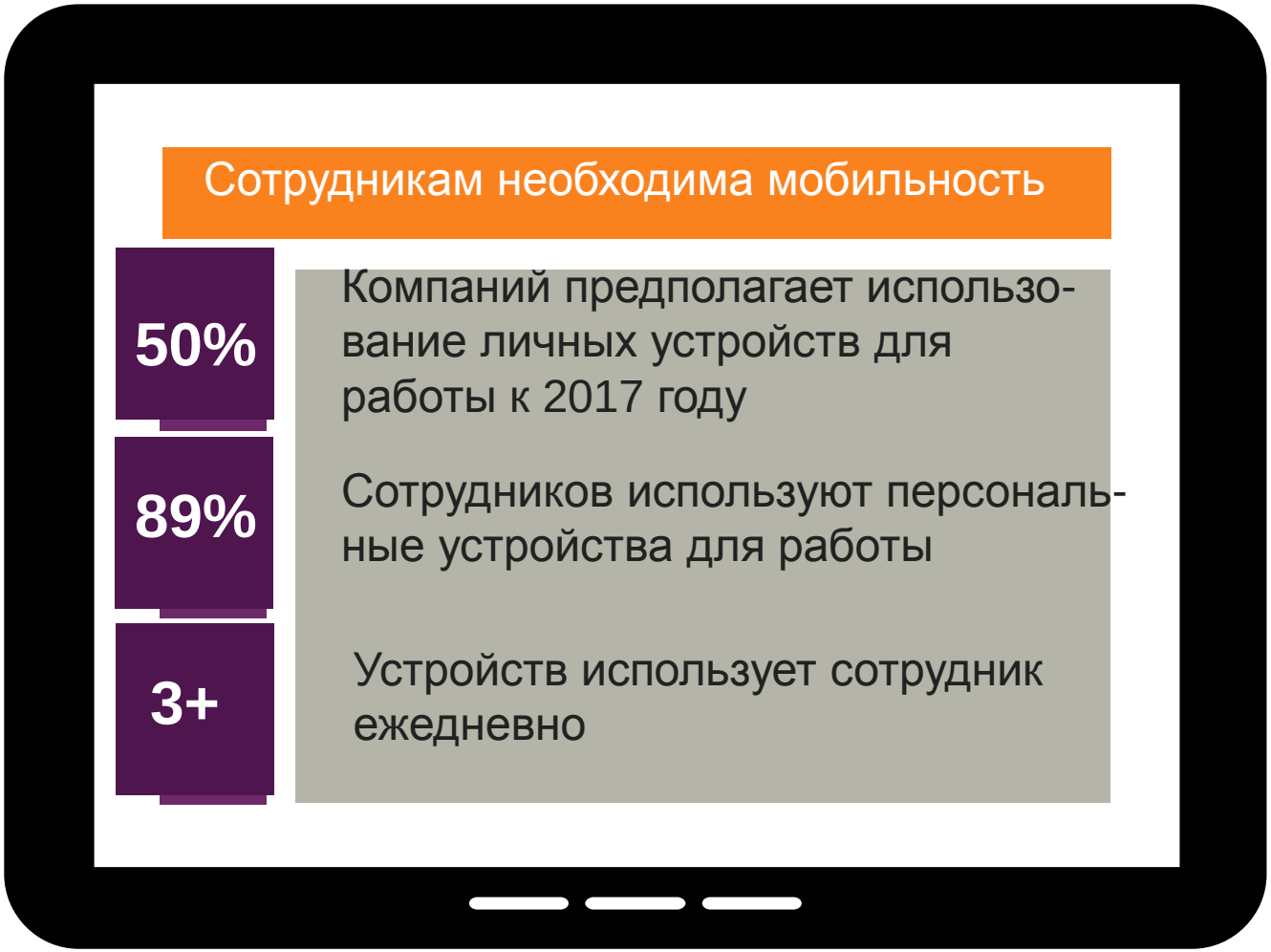
Сохранение данных до 25 лет

GOST Сертификация в процессе
(КриптоПро ФКН 4.0)

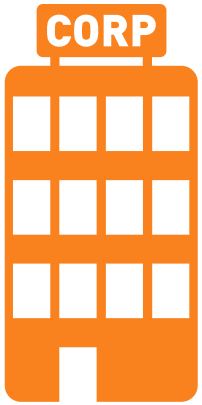
ГОСТ поддержка

- **CryptoPro CSP 4.0 ФКН**
  - генерация ключей для использования в криптографических алгоритмах по стандартам ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 в микроконтроллере
  - шифрование/расшифрование данных по ГОСТ 28147-89
  - контроль целостности данных посредством вычисления имитовставки по стандарту ГОСТ 28147-89
  - вычисление хэш-функции по ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012
  - формирование и проверка ЭЦП по ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012;
- ФКН 4.0 находится в процессе сертификации по требованиям ФСБ России
- Организация производства в России в 2015 году (в процессе согласования)

Взрывной рост мобильных технологий для работы и персональных нужд



Тренд



Мобильные стройства кардинально меняют подход сложившийся уклад. Помимо традиционных компьютеров, лэптопов, добавляются планшеты, смартфоны, используемые для бизнеса задач.

Проблема

- Большинство мобильных устройств не имеют встроенных ридеров или USB слотов для исользования PKI
- Предприятия с внедренными PKI решениями должны найти пути для расширения PKI на мобильные устройства.

Решение:

мобильный офис с Bluetooth

Gemalto предлагает MobilePKI Bluetooth, предлагает решение позволяющее распространить PKI на любое мобильное устройство

Gemalto’s Bluetooth мобильный PKI позволяет расширить применение PKI на мобильные устройства (iOS, Android and Windows)

Умный Bluetooth

Новый расширенный функционал Bluetooth Smart

Время работы батареи — Поддержка стандарта BT 4.0 с ноу-хау по управлению питанием (smart power management protocol), Bluetooth Smart работает примерно в 10 дОльше между требуемыми зарядками устройств по сравнению с предыдущими версиями протоколов BT.

Безопасность установления соединения (Secure pairing)— Gemalto предложила новый технологический подход к установлению соединения BT устройств: быстрее и безопаснее.

- Поддержка соединения по ГОСТ - в разработке

Безопасный канал — Преодолены известные недостатки протокола передачи данных Bluetooth

gemalto
security to be free

Вопросы?

Спасибо!

sergey.kuznetsov@gemalto.com
sergey.kuznetsov@safenet-inc.com