Как защитить информацию на iOS-устройствах при помощи российских СКЗИ

конференция
РусКрипто'2013

Центр Мобильных Решений Digital Design

Константин Гильберг

Руководитель направления мобильной безопасности

zapps@digdes.com

DIGITAL DESIGN

Группа компаний Digital Design

На рынке с 1992 года

Digital Design
Docsvision
RAIDIX

Центр Мобильных Решений DIGITAL DESIGN

Digital Design сегодня:

- Штат 500 сотрудников
- Санкт-Петербург
- Москва

Центр Мобильных Решений в России:

- Мобильность
- Безопасность
- ГОСТ-криптография
- Бизнес-приложения

Услуги:

- Тиражируемые продукты
- Заказные системы
- Комплексные внедрения
- Консалтинг

Устройства iPad и iPhone завоевали популярность в корпоративной среде

Топ-менеджеры

- Электронная почта
- СЭД клиент
- Аналитика

Руководители подразделений

- Электронная почта
- СЭД клиент
- Библиотеки, содержащие файлы и документы

Линейные сотрудники

- Электронная почта
- Web доступ к ресурсам организации
- Приложения, специфичные для предметной области

Рост популярности BYOD

Актуальные риски:

- Кража устройства
- Потеря устройства
- Перехват данных

Защита информации:

- Контейнеризация
- Шифрование
- Условия доступа
- Сложные пароли
- Количество попыток
- Очистка устройства

Управляемый BYOD:

- W&B-list устройств
- W&B-list приложений
- Enterprise App Store

Линейка продуктов Digital Design “Мобильная безопасность для iOS”

Защищенная Почта

Защищенный Браузер

Защищенный СЭД-клиент

Защищенная Папка

В основе продуктов лежат технологии:

Apple

КРИПТО ПРО

Аладдин РД

Microsoft

Уникальность линейки “Мобильная безопасность”

Приложения сохраняют данные в изолированных контейнерах, криптографически защищенных от утечек и изменений

Протоколы аутентификации, шифрования и электронной подписи отвечают российским криптографическим стандартам

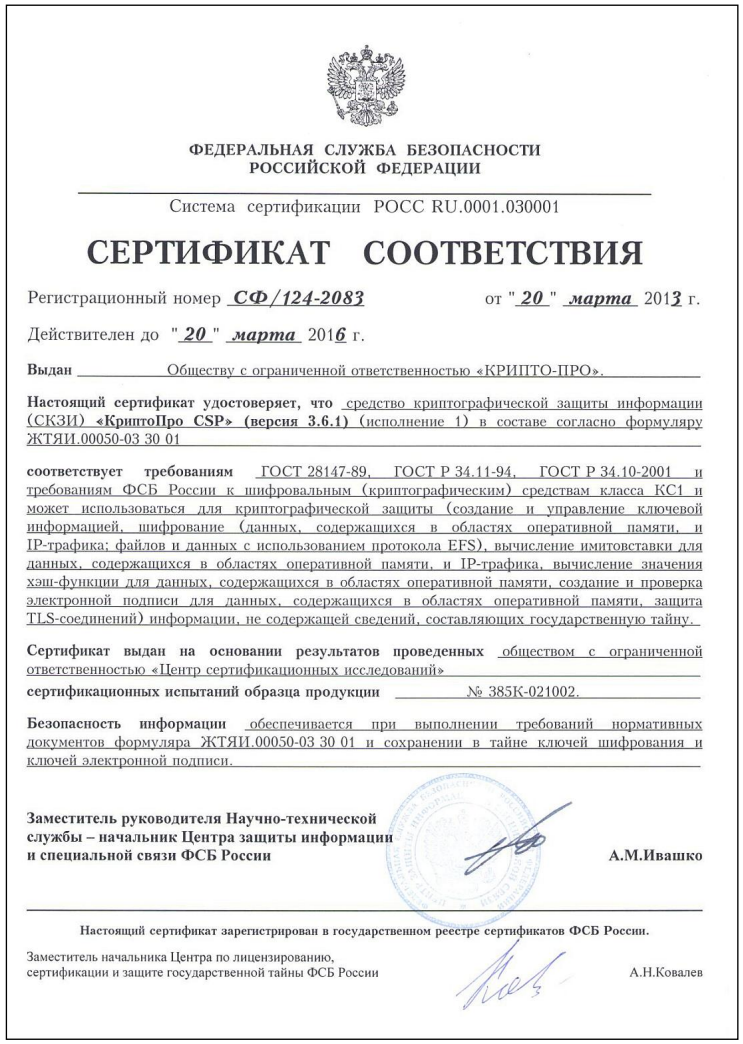
ГОСТ 28147-89 ГОСТ Р 34.11-94 ГОСТ Р 34.10-2001

Для защиты ключевого контейнера используется PIN-код и, как опция, отчуждаемый носитель: смарт-карта

Для работы приложения НЕ требуется взлом (jailbreak) iOS-устройства

DIGITAL DESIGN

Интеграция продуктов “Мобильная безопасность” с сертифицированным на территории РФ СКЗИ компании КРИПТО-ПРО



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-2083 от "20" марта 2013 г.

Действителен до "20" марта 2016 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) «КриптоПро CSP» (версия 3.6.1) (исполнение 1) в составе согласно формуляру ЖТЯИ.00050-03 30 01

соответствует требованиям ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 и требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1 и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование данных, содержащихся в областях оперативной памяти, и IP-трафика; файлов и данных с использованием протокола EFS), вычисление имитовставки для данных, содержащихся в областях оперативной памяти, и IP-трафика, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти, создание и проверка электронной подписи для данных, содержащихся в областях оперативной памяти, защита TLS-соединений) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных обществом с ограниченной ответственностью «Центр сертификационных исследований» сертификационных испытаний образца продукции № 385К-021002.

Безопасность информации обеспечивается при выполнении требований нормативных документов формуляра ЖТЯИ.00050-03 30 01 и сохранении в тайне ключей шифрования и ключей электронной подписи.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.М.Ивашко

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.Н.Ковалев

КриптоПро CSP 3.6.1 (R3) iOS

Используется:

- **Реализация ГОСТ алгоритмов**
- **Реализация TLS протокола**
- **Интеграция с УЦ, OCSP, TSP**

Не требуется выполнять jailbreak iOS устройства

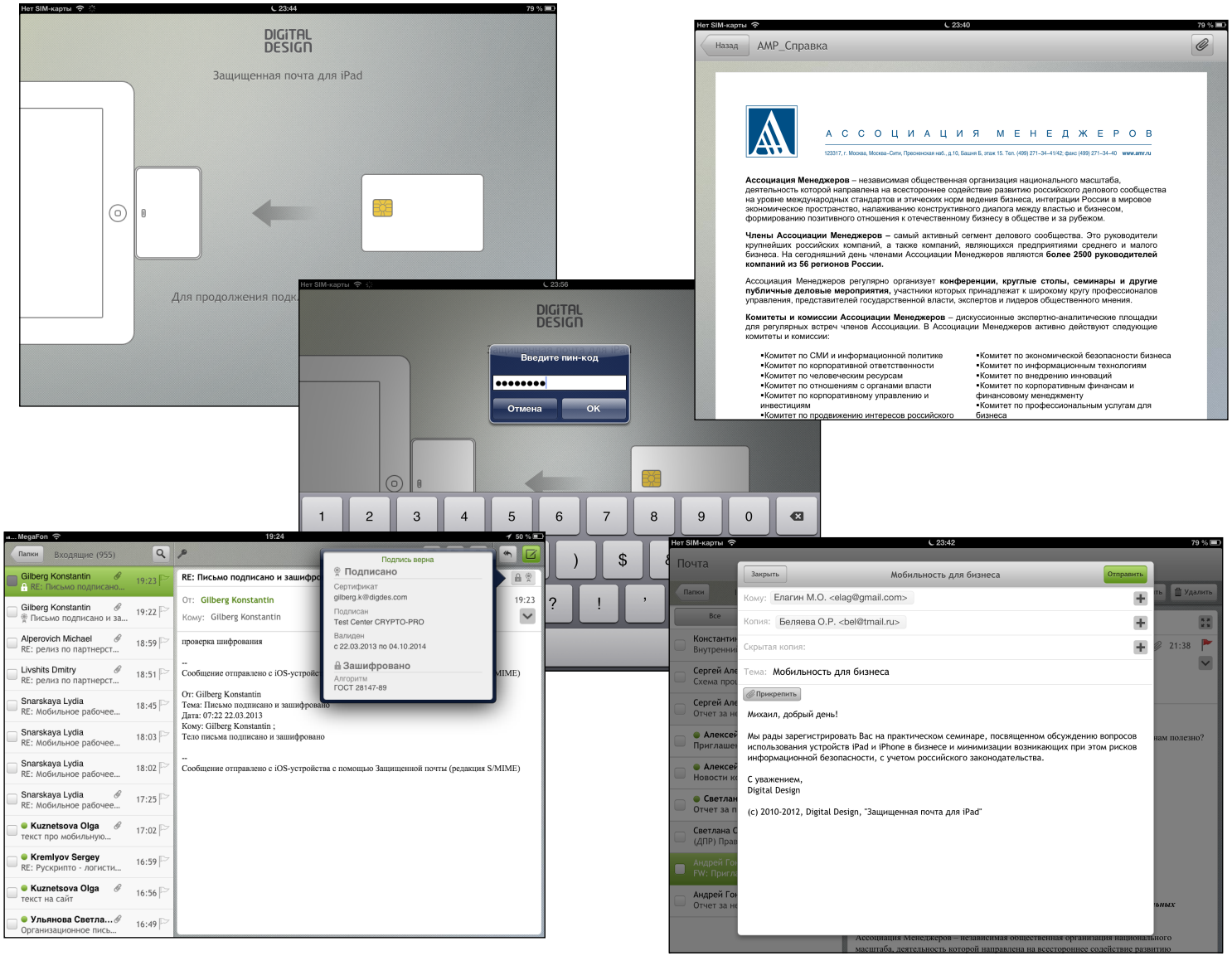
DIGITAL DESIGN

Защищенная почта

для пользователей iPad и iPhone

Microsoft® Exchange

IBM Lotus



Алгоритмы:

- ГОСТ 28147-89
- ГОСТ Р 34.10-94
- ГОСТ Р 34.11-2001

Объекты шифрования:

- БД приложения
- Канал передачи данных
- Письмо

S/MIME:

- Шифрование
- Электронная подпись
- CAdES

PKI службы:

- УЦ (КриптоПро, MS)
- Active Directory
- OCSP, TSP

Защищенный браузер

для пользователей iPad и iPhone

Функции безопасности:

- Двухсторонняя аутентификация с использованием сертификата X.509
- Конфиденциальность сеанса работы за счет шифрования сессии: URL, IN/OUT данные, протокол
- Шифрование содержимого локального кеша

Интеграция с продуктами анализа web-трафика

- Антивирусные системы
- DLP системы

Защищенный СЭД-клиент

для топ-менеджеров, руководителей и их помощников

Индивидуальный подход:

- Индивидуальный дизайн
- Специфика процессов

Безопасность:

- Защита данных
- Защита трафика
- ЭП документов
- ЭП по стандарту CAdES
- Смарт-карта

Сценарии работы:

- Рассмотрение документов
- Согласование документов
- Выдача поручений
- Утверждение проектов
- Исполнение поручений
- Контроль исполнения

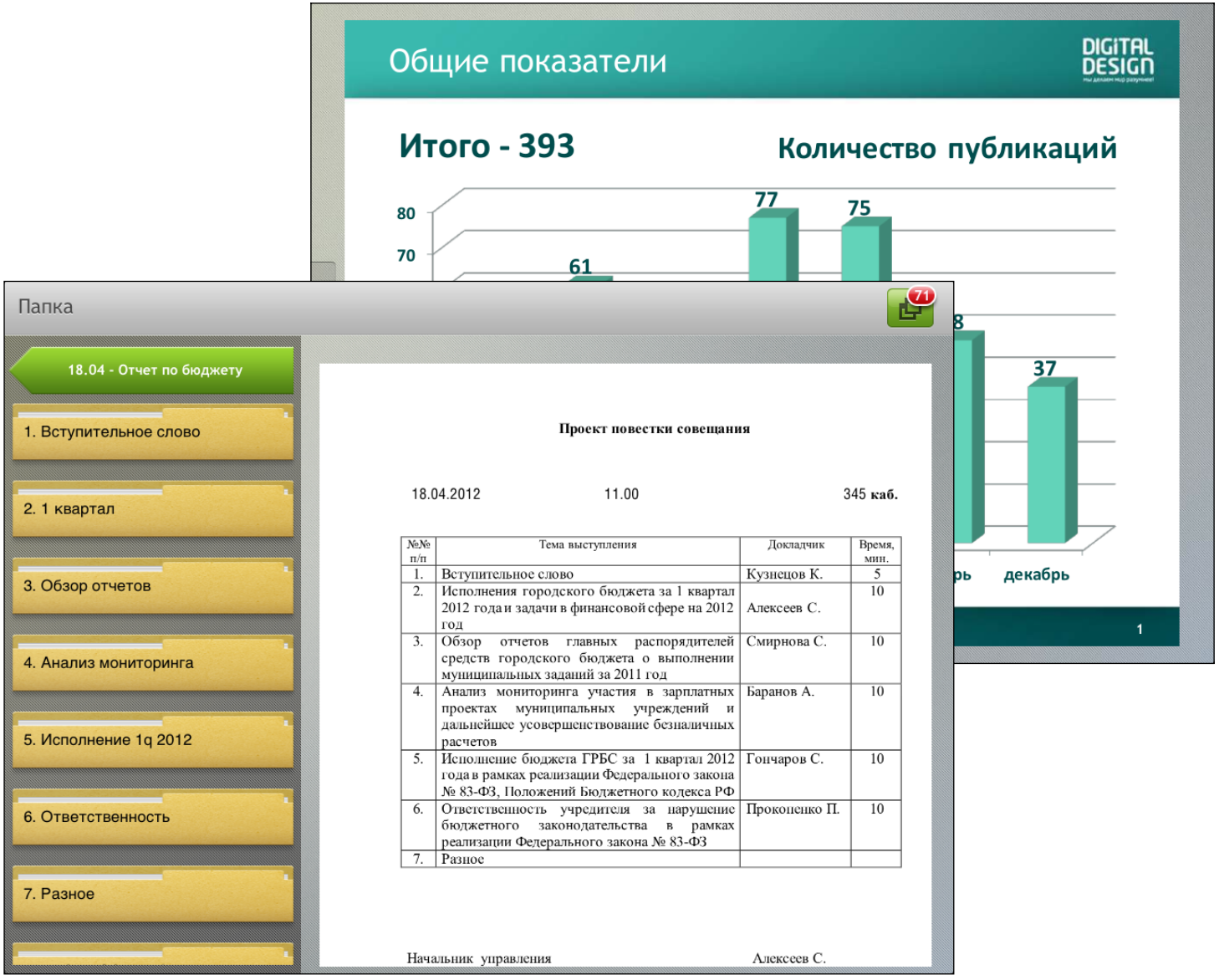
Дополнительно:

- Off-line работа
- SDK для интеграции с СЭД

beta

Защищенная Папка

для пользователей iPad и iPhone устройств



Алгоритмы

- ГОСТ 28147-89
- ГОСТ Р 34.10-94
- ГОСТ Р 34.11-2001

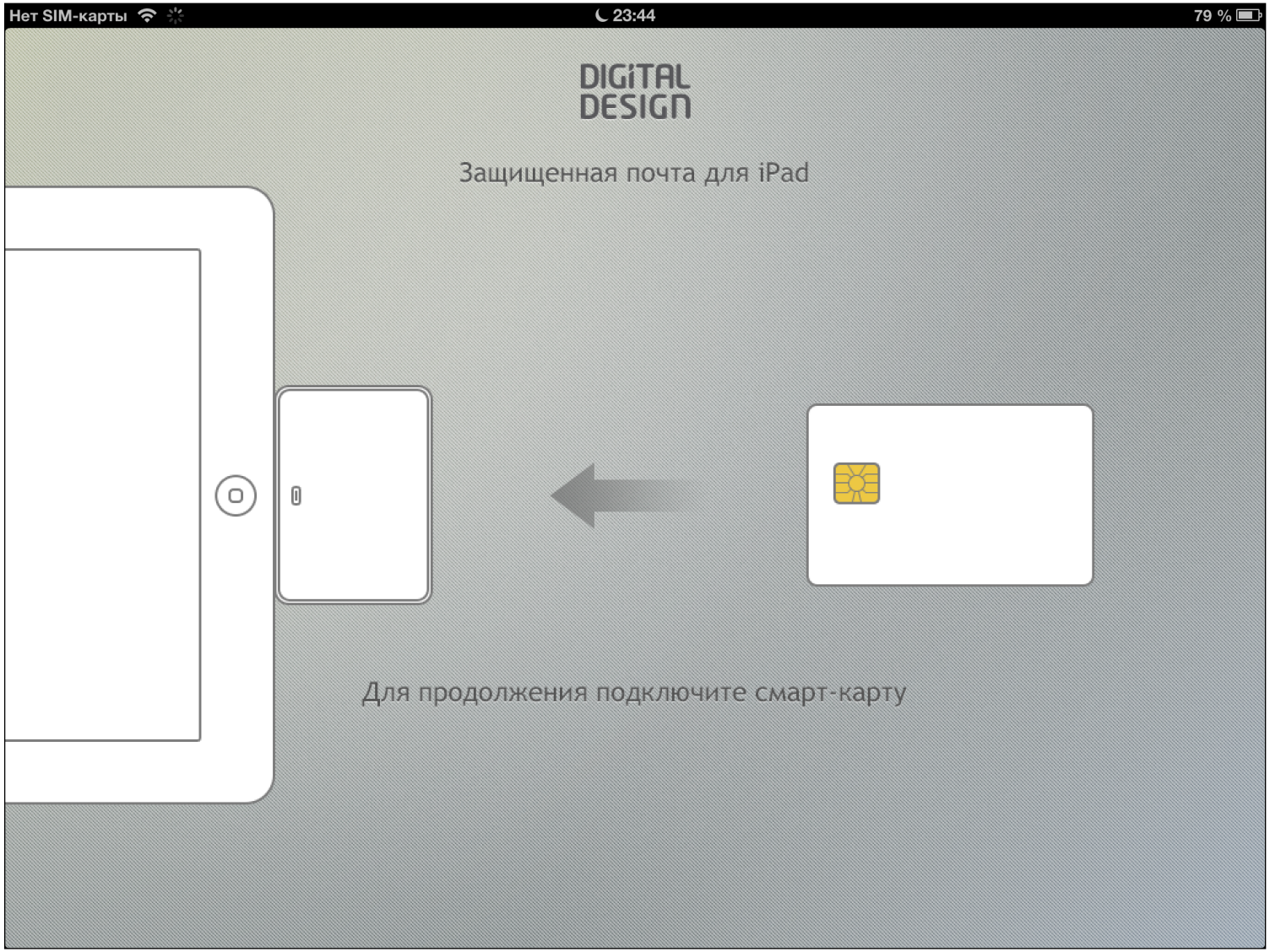
Функции защиты:

- Шифрования трафика
- Шифрование кеша
- Блокировка “Открыть в”
- Блокировка “Screenshot”

Источники данных:

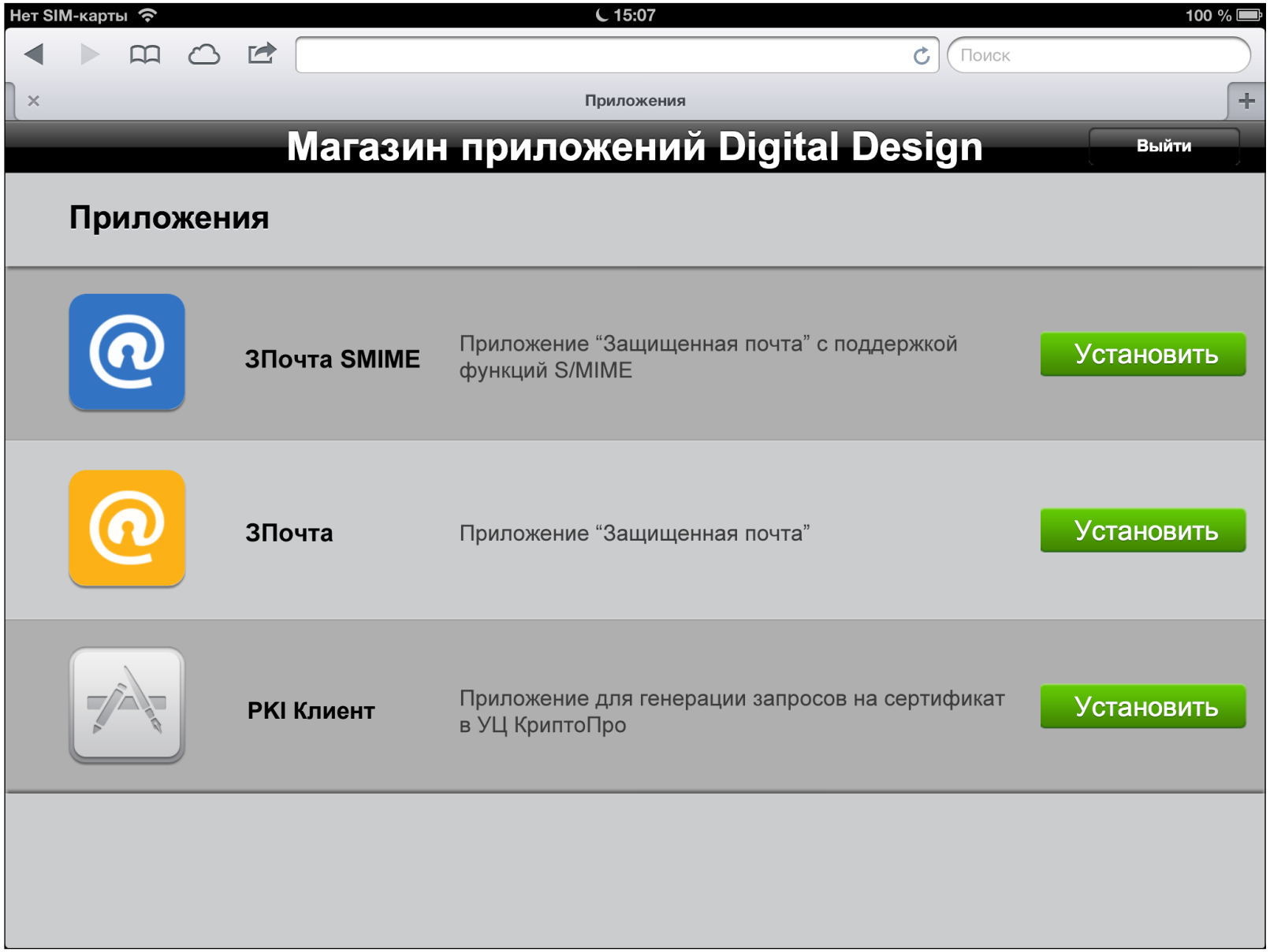
- ПК пользователя
- Sharepoint (MOSS)
- Сетевые папки Windows

Усиление уровня безопасности за счет хранения ключевого контейнера на смарт-карте



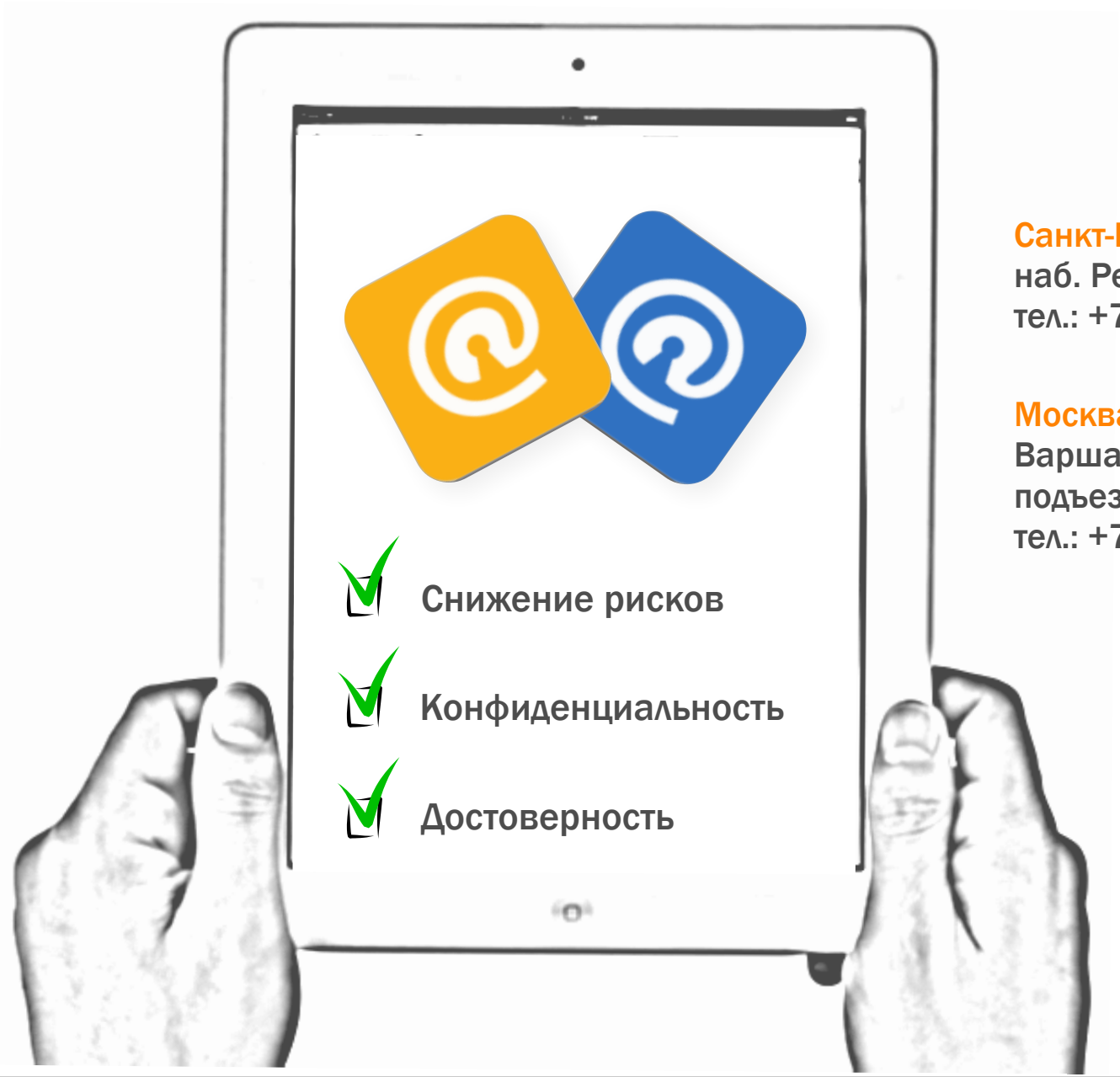
DIGITAL DESIGN

Распространение iOS-приложений, содержащих в своем составе СКЗИ модуль (DEP-лицензия)



DIGITAL DESIGN

Спасибо за внимание!



Санкт-Петербург,
наб. Реки Смоленки, 33
тел.: +7 (812) 346 5833

Москва,
Варшавское шоссе, 36 стр. 8,
подъезд 5, 1 этаж
тел.: +7 (499) 788 7494