DIGITAL DESIGN
мы делаем мир разумнее!

Практические аспекты организации защищенного подключения iOS- приложений к корпоративным ресурсам

Михаил Альперович,
Директор Лаборатории защищенной мобильности
www.digdes.ru/zm

Удаленный доступ к информационным ресурсам

DIGITAL DESIGN
мы делаем мир разумнее!

- Мобильные устройства работают из Интернета (= по открытым каналам)
- Защищать открытые каналы связи нужно по ГОСТу

Технологии удаленного доступа

DIGITAL DESIGN
мы делаем мир разумнее!

- В компаниях, как правило, существуют шлюзы удаленного доступа
- И они даже поддерживают ГОСТ
- Но подавляющее их большинство - это оборудование:
  - IPSec
  - PPTP
  - OpenVPN
  - И пр. технологии VPN

Классический VPN – не выход для iOS

DIGITAL DESIGN
мы делаем мир разумнее!

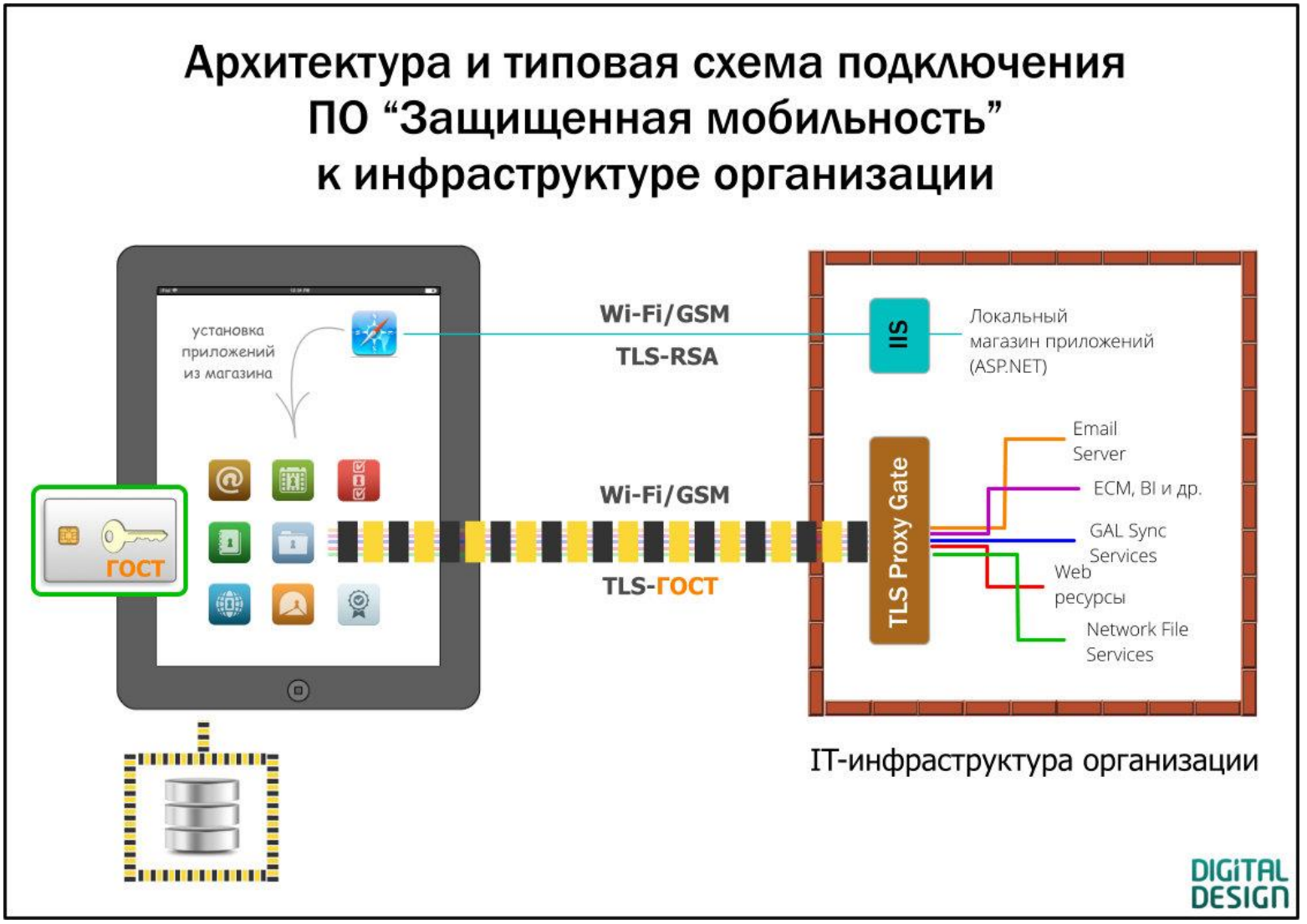
- Реализация VPN возможна только на уровне операционной системы
- Для этого нужно спец разрешение Apple или jailbreak
- На текущий момент нет решений VPN для iOS (без jailbreak) с реализацией ГОСТа
- А также:
  - VPN – влияет на эргономику (нужно включать, нужно дополнительно аутентифицироваться)
  - VPN – ведет к блокировке функциональности как штатных, так и сторонних приложений

Выбор технологии – SSL/TLS VPN

DIGITAL DESIGN
мы делаем мир разумнее!

- Может быть реализован на прикладном уровне
- Может быть реализован ГОСТ
  - 28147-89, 34.10-2001, 34.11-94
- Позволяет туннелировать траффик выборочно
- Содержит необходимые механизмы:
  - Шифрование
  - Контроль целостности
  - Аутентификацию

Схема решения

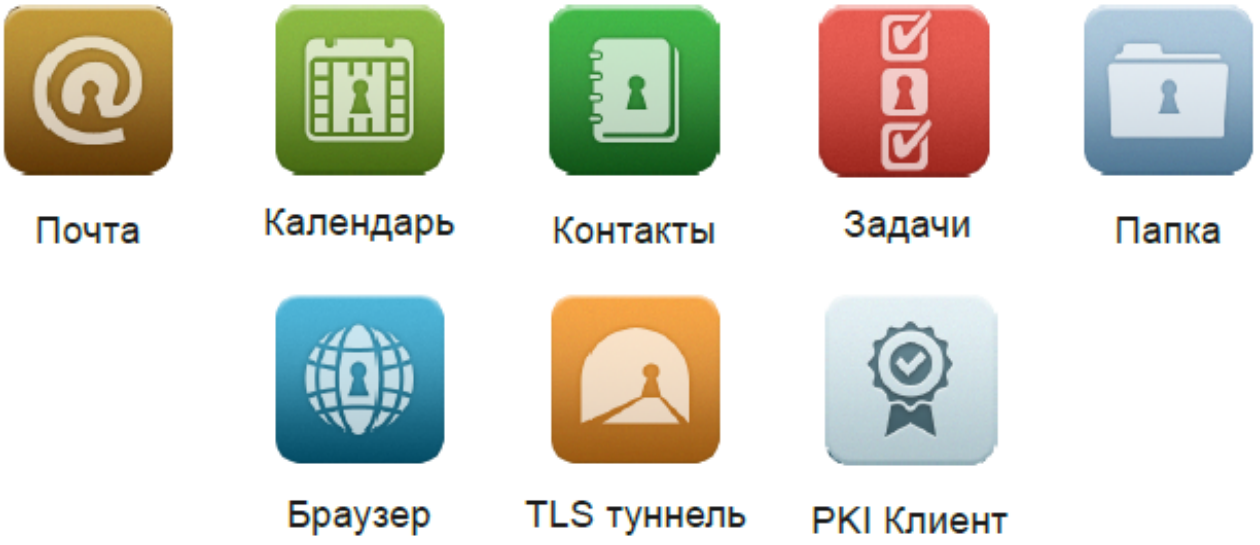


Клиентская часть

- Линейка продуктов «Защищенная мобильность»
- Встраивание в приложения сторонних разработчиков (в т.ч. на SAP Mobile Platform)
- Защита канала для готовых приложений 3-их фирм:
  - RoamBI
  - QlickView
  - системы СЭД
  - Терминальные решения – Microsoft RDP, Citrix

Digital Design “Защищенная мобильность”

Защищенная мобильность - программное обеспечение для организаций, позволяющее мобильной категории пользователей iOS-устройств получать доступ к корпоративным ресурсам, осуществлять хранение и обработку конфиденциальной информации с применением сертифицированных ФСБ России СКЗИ, средств защиты от утечек и НСД.

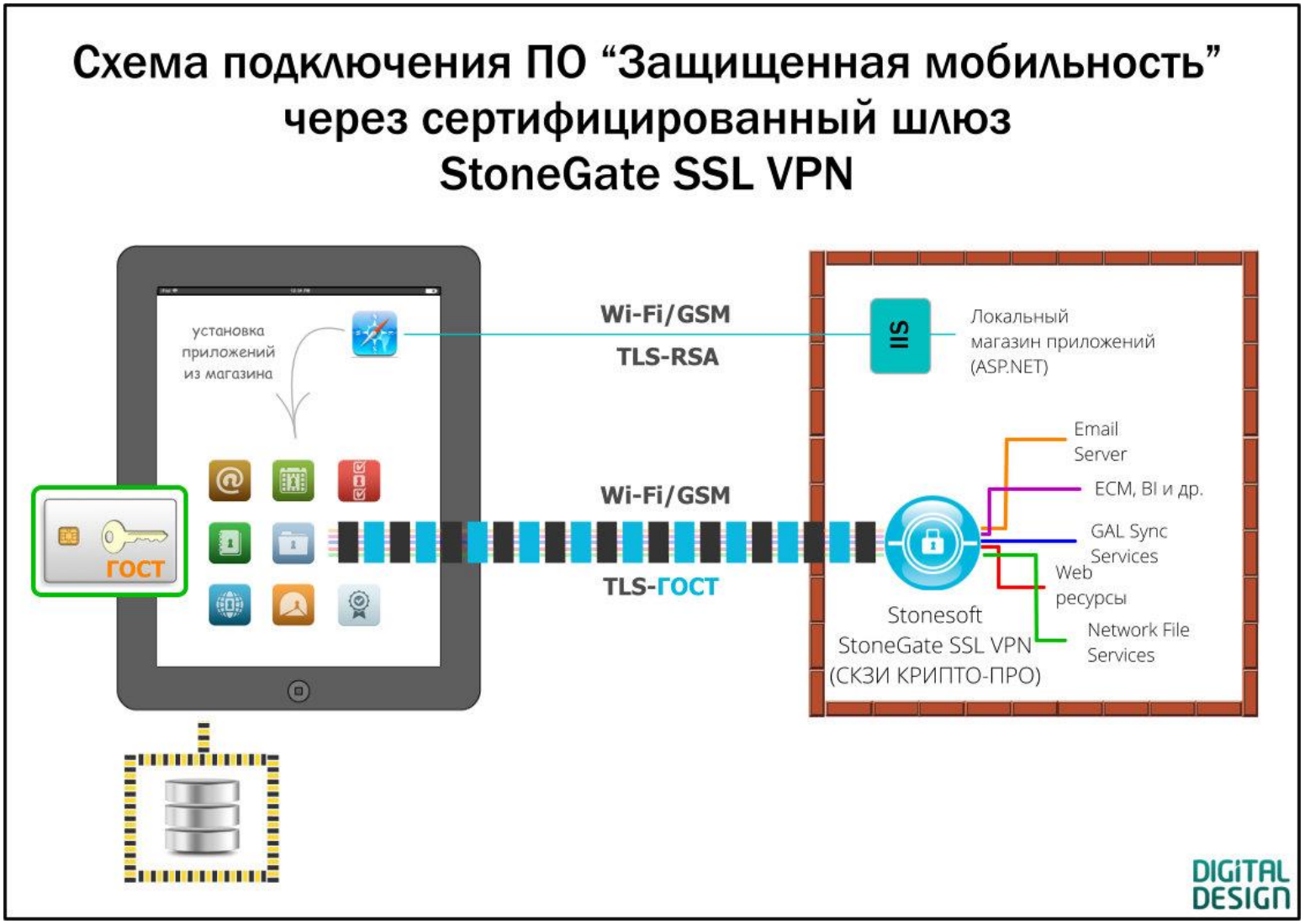


Серверная часть

DIGITAL DESIGN
мы делаем мир разумнее!

- В составе своих продуктов, ДД поставляет SSL/TLS шлюз собственной разработки
- Позволяет маршрутизировать входящий ГОСТированный траффик на соответствующий ресурс внутренней сети
- Основные преимущества:
  - Стоимость
  - Низкие требования к аппаратному и программному обеспечению
  - Поддержка ГОСТа

Пример сертифицированного решения



Выбор серверного решения

DIGITAL DESIGN
мы делаем мир разумнее!

- Примеры решений - TLS шлюзы:
  - Microsoft IIS (Reverse Proxy Mode)/ISA/TMG/UAG
  - Apache
  - КриптоПро Stunnel
  - StoneGate
  - CheckPoint

Во всех указанных случаях применяется КриптоПро CSP для реализации криптографии

Нюансы выбора решения

- Возможность «проброса» соединений с одного слушающего порта на множество узлов корпоративной сети
- Поддержка режима Forward Proxy – туннелирование по ГОСТированному TLS зашифрованного трафика по RSA SSL/TLS (критично, например, для Citrix)
- Средства аутентификации (элементы SSO, аутентификация цифровым сертификатом)

DIGITAL DESIGN
мы делаем мир разумнее!

Спасибо за внимание!

www.digdes.ru/zm

115230, **Москва**
Варшавское шоссе, д. 36
стр. 8, подъезд 5
тел. +7 (499) 788-74-94
тел./факс +7 (499) 788-74-95

199178, **Санкт-Петербург**
наб. реки Смоленки, д. 33
тел. +7 (812) 346-58-33
факс +7 (812) 346-58-34
info@digdes.com
www.digdes.ru