DIGITAL DESIGN
мы делаем мир разумнее!

ГОСТ-овая ЭЦП на платформе Apple iOS

Константин Гильберг
Менеджер продукта «Планшет Руководителя»
Центр разработки планшетных решений Digital Design

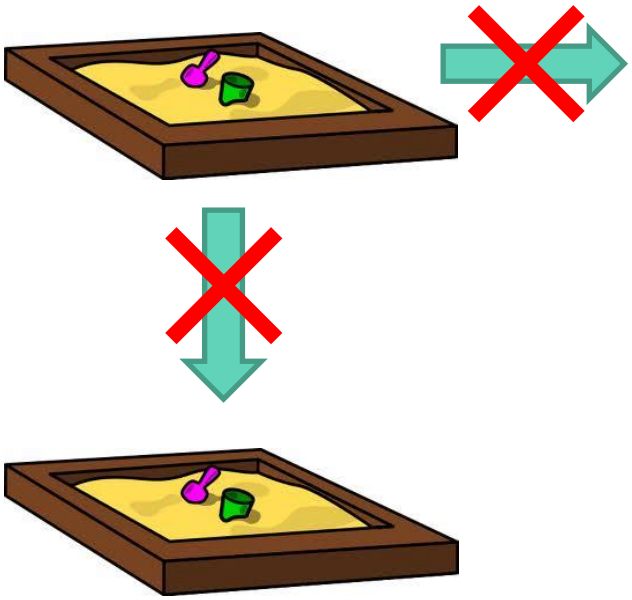
План презентации

DIGITAL DESIGN
мы делаем мир разумнее!

1. Схема интеграции СКЗИ в среду iOS приложения
2. Варианты хранения ключа ЭП на iOS устройстве
3. Сертификация СКЗИ и программных продуктов iOS

Схема интеграции СКЗИ с iOS приложением

DIGITAL DESIGN
мы делаем мир разумнее!



- Каждое iOS приложение исполняется в своей «песочнице»
- Пресекаются попытки попасть в «песочницу» другого iOS приложения
- Пресекаются попытки прямого обращения к ОС

Схема интеграции СКЗИ с iOS приложением

DIGITAL DESIGN
мы делаем мир разумнее!

- Библиотека СКЗИ, реализующая альтернативные крипто-алгоритмы, должна исполняться внутри «песочницы» iOS приложения

- Данный подход НЕ требует jailbreak (взлома устройства)

- С точки зрения Apple, подход считается корректным и рекомендуется Разработчикам

Отечественные СКЗИ

DIGITAL DESIGN
мы делаем мир разумнее!

КРИПТО ПРО

infotecs

- Электронно-цифровая подпись
- Аутентификация
- Шифрование данных
- SSL/TLS
- Взаимодействие с УЦ

Варианты хранения ключа ЭП

DIGITAL DESIGN
мы делаем мир разумнее!

Ключ ЭП хранится на iOS устройстве

- Ключ ЭП генерируется, хранится и не покидает iOS устройство
- Для защиты контейнера используется парольная фраза
- Apple (в лице Дмитрия Вишнякова) считает, что iOS устройство защищено не хуже, чем смарт-карта

Альтернативные варианты хранения ключа ЭП

DIGITAL DESIGN
мы делаем мир разумнее!

Bluetooth считыватель смарт-карт

Ключ ЭП находится на отчуждаемом носителе

Защита bluetooth соединения опирается на зарубежные алгоритмы

Альтернативные варианты хранения ключа ЭП

DIGITAL DESIGN
мы делаем мир разумнее!

Слухи:

Вероятно появление на рынке электронного USB-ключа с 30-пиновым разъемом для Apple iPad/iPhone

С точки зрения iOS приложения устройство «выглядит» видео-камерой

Ключ ЭП передается в формате псевдо-графического изображения

Сертификация СКЗИ

DIGITAL DESIGN
мы делаем мир разумнее!

КРИПТО ПРО

Добро пожаловать! Поиск | Активные темы | Участники | Вход | Регистрация

Форум Крипто-Про » Средства криптографической защиты информации » Apple »
Сертифицированная версия Крипто-Про CSP для iOS

Сертифицированная версия Крипто-Про CSP для iOS Options

Предыдущая тема · Следующая тема

DimonSV	**От:** 7 июня 2011 г. 11:35:45
Ранг: Новичок Группа: Участники Регистрация: 17.12.2009 Сообщений: 2 [Points]: -135 Откуда: Москва	Добрый день. Сообщите, пожалуйста, примерные сроки выхода официальной сертифицированной версии Крипто-Про CSP для iOS.
В начало	
Татьяна	**От:** 7 июня 2011 г. 19:33:41
Ранг: Эксперт Группа: Администраторы , Участники Регистрация: 06.02.2008 Сообщений: 1 101 [Points]: 2 216 Откуда: Крипто-Про	Здравствуйте. Платформа iOS в ТЗ на разработку новой версии КриптоПро CSP с ФСБ согласована. Сроки сертификации зависят не только от нас но и от того, как будет проходить проверка в сертифицирующих органах, поэтому прогнозы очень примерные. Мы ожидаем, что продукт сертифицируется к концу года. Текущая информация о статусе сертификации публикуется в ReleaseNotes в разделе с вопросами и ответами. Татьяна ООО Крипто-Про
В начало	

Пользователи, просматривающие тему

Guest

КриптоПро, 07.06.2011:
«Платформа iOS в ТЗ на разработку новой версии КриптоПро CSP с ФСБ согласована… ожидаем, что продукт сертифицируется к концу года»

Сертификация iOS приложений

Наличие на рынке СКЗИ, сертифицированных ФСБ, станет катализатором появления сертифицированных прикладных систем, поддерживающих ЭП, аутентификацию, защиту трафика, шифрование данных на основе алгоритмов ГОСТ.

Пример:

В январе 2012 года Digital Design планирует подать заявку в ФСТЭК на сертификацию программного продукта «Планшет Руководителя», использующего библиотеку КриптоПро CSP iOS для целей аутентификации пользователей, операции ЭЦП, шифрование данных

Планшет Руководителя

DIGITAL DESIGN
мы делаем мир разумнее!

- ✓ Автономность
- ✓ Простота
- ✓ Эстетика

Планшет Руководителя – мобильное рабочее место топ-менеджера компании, интегрирующее функции ключевых бизнес-инструментов в среде планшета: Документооборот, Электронная почта, Органайзер, Электронная почта, Аналитика, Связь с секретарем.

Наши заказчики

DIGITAL DESIGN
мы делаем мир разумнее!

ГАЗПРОМ

МИНПРОМТОРГ РОССИИ

Аппарат правительства Мурманской области

Российские железные дороги

СБЕРБАНК

ССК

КИРОВСКИЙ ЗАВОД

РУСГИДРО

ВТОРАЯ ГРУЗОВАЯ КОМПАНИЯ

DIGITAL DESIGN
мы делаем мир разумнее!

Спасибо за внимание

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