ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

СКАНТЕК

SCANTECH Mobile Card. Описание решения.

Версия 1.0

июнь 2017

СКАНТЕК

SCANTECH Mobile Card
Описание решения

История изменений

Дата	Автор	Версия	Примечание

Содержание

Введение

Решение SCANTECH Mobile Card предназначено для эмуляции в смартфоне в рамках Мобильного Приложения Заказчика топливных карт и/или карт лояльности.

В данном документе приводится описание основных модулей решения SCANTECH Mobile Card и схема их взаимодействия в рамках Системы Обработки Мобильных Карт Лояльности.

В Приложении №1 дано сравнение вариантов эмуляции карты лояльности.

В Приложении №2 предлагается обзор преимуществ решения SCANTECH Mobile Card которые обеспечивают корректную и безопасную работу Мобильного Приложения Заказчика, эмулирующего работу Карты Лояльности.

1

Основные модули

Эмуляция карты лояльности Мобильным Приложением Заказчика обеспечивается работой следующих модулей Системы Обработки Мобильных Карт Лояльности:

SCANTECH Mobile Card Emulation SDK / Приложение (Android)

Представляет собой набор библиотек для мобильного устройства Android, предназначенных для интеграции с Мобильным Приложением Заказчика.

Позволяет эмулировать работу карты лояльности с использованием NFC-модуля устройства (если он имеется) или посредством генерации штрих-кодов или QR-кодов.

Набор библиотек собран под ОС Android 4.4 KitKat в среде разработки Android Studio и может быть интегрирован в приложение для смартфона стандартными средствами.

SCANTECH Mobile Card Emulation SDK / Приложение (iOS)

Представляет собой набор библиотек для устройств, работающих под управлением iOS, , предназначенных для интеграции с Мобильным Приложением Заказчика. Позволяет эмулировать работу карты лояльности в виде штрих-кода или QR-кода.

Набор библиотек собран под iOS 7.0 в среде разработки XCode и может быть интегрирован в приложение для смартфона стандартными

средствами.

SCANTECH Mobile Card Perso Center

Центр Персонализации Мобильных Приложений обеспечивает подготовку данных персонализации и их загрузку в Мобильное Приложение Заказчика (регистрацию Мобильного Приложения Заказчика). Работает под управлением ОС Windows Server с использованием MS SQL БД.

Компоненты Центра Персонализации Мобильных Приложений:

SCANTECH Mobile Card Perso Server

Сервер персонализации, выполняющий:

- проверку корректности данных в запросе на персонализацию, поступившем от Мобильного Приложения Заказчика
- формирование крипто-данных по корректным запросам
- передачу крипто-данных Мобильному Приложению Заказчика

SCANTECH Light Security Module (LSM)

Крипто-модуль (смарт-карта, установленная в PC/SC ридер), использующийся для выполнения криптографических операций и хранения ключей.

SCANTECH Mobile Card Perso Administrator

Рабочее место Администратора Центра Персонализации Мобильных Приложений, с которого выполняется управление данными в LSM и в БД Персонализации.

2

Взаимодействие модулей

Взаимодействие модулей Системы Обработки Мобильных Карт Лояльности при выпуске и использовании Мобильной Карты представлено на рис.1.

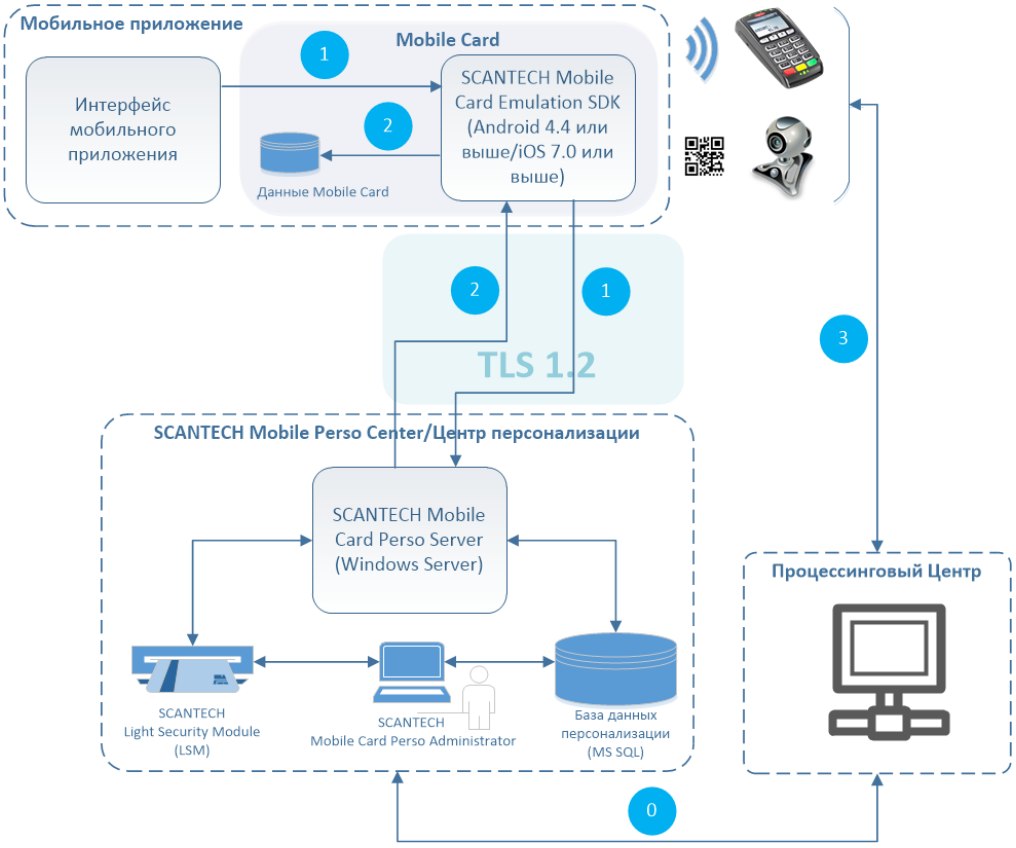

Рисунок 1. Взаимодействие модулей Системы Обработки Мобильных Карт Лояльности.

0 - Процессинговый Центр (ПЦ) передает в Центр Персонализации Мобильных Приложений диапазон номеров карт, для которых необходимо подготовить данные персонализации и ключи аутентификации.

1 – Мобильное Приложение Заказчика передает в Центр Персонализации Мобильных Приложений запрос на персонализацию, включающий последние 4 цифры номера карты и одноразовый пароль.

2 – Выпуск Мобильной Карты: после успешной проверки Центром Персонализации Мобильных Приложений корректности данных запроса на персонализацию[1] Мобильное Приложение Заказчика считается зарегистрированным в системе и Центр Персонализации отправляет Мобильному Приложению крипто-данные для эмуляции Мобильной Карты лояльности.

3 – Формирование транзакции по Мобильной Карте.

[1] Данные запроса на персонализацию (одноразовый пароль и номер карты) считаются корректными, если по базе данных Центра Персонализации Мобильных Приложений установлено соответствие одноразового пароля номеру карты.

Приложение 1. Сравнение вариантов эмуляции карты лояльности

Эмуляция «физической» карты лояльности средствами смартфона может быть выполнена с использованием различных технологий. В представленной ниже Таблице 1 дается сравнение различных технологий в аспекте обеспечения безопасности решения и необходимости проведения дополнительных интеграционных работ.

Таблица 1.

Технология	Оценка безопасности	Необходимость дополнительной интеграции
EMV-совместимая (ONLINE аутентификация)		
NFC[1]	Аналогично «физической» карте.	Модификации процессинга лояльности и АСУ АЗС не требуется.
EAN128 / QR code	Аналогично «физической» карте (при условии наличия контроля не уменьшения АТС на хосте).	Требуется модификация (считывание средствами АСУ АЗС). Необходим предварительный ввод суммы операции на телефоне
OFFLINE аутентификация в терминале		
NFC[1]	Аналогично OFFLINE аутентификации «физической» карты на несимметричных ключах.	Модификации процессинга лояльности и АСУ АЗС не требуется.
EAN13	Возможно «копирование» карты лояльности.	Модификации процессинга лояльности и АСУ АЗС не требуется.
EAN128 / QR	OFFLINE аутентификация на симметричных ключах с контролем времени использования.	Требуется модификация (считывание средствами АСУ АЗС).

[1] для iOS возможно после предоставления производителем доступа к NFC iOS.

Приложение 2. Преимущества решения SCANTECH Mobile Card

Использование поддержанных в решении SCANTECH Mobile Card технологий безопасности (см. Табл. 2) обеспечивает возможность запуска проекта в кратчайшие сроки и с минимальными затратами.

Применение NFC-интерфейса и EMV-криптографии позволяет осуществить внедрение проекта без модификации ПО АСУ АЗС и авторизационного центра с сохранением высокого уровня безопасности, обеспечиваемого использованием EMV-карт.

С «мобильной» картой лояльности возможно выполнение всех операций, доступных при использовании «физической» карты (начисление баллов, списание баллов, перенос баллов с одной карты на другую).

SCANTECH Mobile Card поставляется в виде библиотек (SDK), что дает возможность интегрировать требуемый функционал в существующее Мобильное Приложение Заказчика.

Работа мобильных карт лояльности с использованием SCANTECH Mobile Card была успешно протестирована на АЗС одной из ведущих нефтяных компании.

Таблица 2. Технологии безопасности, используемые в SCANTECH Mobile Card.

Технология	Поддержка в SCANTECH Mobile Card	Комментарий
NFC	Поддерживается в версии для Android.	Интерфейс доступа к NFC-модулю для реализации HCE проектов для iOS пока закрыт производителем.
EMV	Поддерживается ONLINE аутентификация как при использовании NFC, так и при использовании штрих-кодов достаточной размерности.	EMV-криптограмма для ONLINE аутентификации (ARQC) генерируется мобильным приложением.

Технология	Поддержка в SCANTECH Mobile Card	Комментарий
		В случае использования NFC данные транзакции получаются от терминала стандартным образом проведения бесконтактной транзакции, в случае использования штрих кода сумма операции должна быть введена в мобильном приложении.
Токенизация (подменный номер карты)	Поддерживается опционально.	Номер карты в проектах карт лояльности и топливных карт не является секретной информацией, поэтому нет необходимости подменять его фиктивным номером.
Session Unit Keys	Поддерживается опционально.	Загрузка диверсифицированных ключей в мобильное устройство является теоретически более безопасным способом хранения ключей, но требующим регулярного выхода на связь с сервером персонализации. С учетом низких рисков атаки приложения лояльности в мобильном устройстве допускается хранение в устройстве уникального ключа эмулируемой карты.
HSM	Поддерживается по запросу.	Стандартное решение включает в себя использование LSM (Light Security Module), представляющим собой смарт-карту со специализированным криптографическим апплетом. В случае использования технологии Session Unit Keys и достаточно большом (более 10 000) количестве активных пользователей программы рекомендуется переход на более производительное оборудование.
White Box Cryptography	Поддерживается.	Используемые средства и механизмы защиты ключей в памяти мобильного устройства могут быть переданы на внешний аудит.