социальные системы
www.socialsystems.ru

Программное обеспечение устройства работы с бесконтактными картами платёжной системы "Mastercard"

Функциональные характеристики программного обеспечения

Листов 8

Москва, 2023

Оглавление

Список сокращений

Сокращение	Расшифровка
AID	Application Identifier - номер платёжного приложения
CDA	Combined Data Authentication – метод проверки легитимности EMV-карты, основанный как на динамических данных, так и статических
CVM	Cardholder Verification Method – метод идентификации владельца карты
DDA	Dynamic Data Authentication – метод проверки легитимности EMV-карты, основанный на динамических данных
DEK	Data Exchange Kernel – передача данных от ядра в рамках протокола прямого обмена данными с ядром
DET	Data Exchange Terminal – передача данных от терминала в рамках протокола прямого обмена данными с ядром
EMV	Europay + MasterCard + VISA – международный стандарт для операций по банковским картам с чипами
Mag-stripe	Magnetic stripe – в данном документе режим эмуляции работы с магнитной полосой через бесконтактный интерфейс
MC	Mastercard – платёжная система
RRP	Relay Resistance Protocol
SDA	Static Data Authentication – метод проверки легитимности EMV-карты, основанный на статических данных
TAC	Terminal Action Code
TVR	Terminal Verification Result
UDOL	Unpredictable number Data Object List

Аннотация

Данный документ содержит описание функциональных характеристик программного обеспечения согласно спецификации бесконтактного платёжного ядра платёжной системы "Mastercard".

Документ предназначен для ознакомления с функциональными возможностями программного обеспечения устройства работы с бесконтактными картами платёжной системы "Mastercard".

1. Общие сведения

Программное обеспечение устройства для работы с бесконтактными картами платёжной системы "Mastercard" (далее "ядро MC") соответствует спецификации "Mastercard Contactless Reader Specification", версии 3.1.4.

2. Функциональные характеристики ядра MC

2.1. Настройки ядра MC

Архитектура программного обеспечения ядра MC позволяет:

- вводить настройки как для отдельных платёжных приложений (AID), так и для группы платёжных приложений;
- вводить настройки для каждого типа поддерживаемых операций.

Поддерживаются следующие настройки ядра:

- код страны терминала (Terminal Country Code);
- тип терминала (Terminal Type);
- дополнительный возможности терминала (Additional Terminal Capabilities);
- поддержка мобильных устройств (Mobile Support Indicator);
- конфигурация ядра (Kernel Configuration);
- поддерживаемая версия платёжного приложения карты (Application Version Number);
- настройки безопасности (Security Capabilities);
- настройка поддержки интерфейсов терминала (Card Data Input Capabilities);
- настройки проверки держателя карты (CVM Capabilities);
- спецификаторы для принятия решений ядром на основании результатов проведения транзакции (TVR) - (TAC Denial, TAC offline, TAC online);
- настройки чтения оффлайн-баланса (Balance Read);
- значение по умолчанию UDOL (Default UDOL);
- настройки проверки держателя карты в режиме работы с магнитной полосой (далее MSM - Magnetic Stripe Mode) - (CVM Capabilities);
- значение лимита, при котором принимается решение авторизации транзакции в онлайн-режиме (Reader Contactless Floor Limit);
- значение лимита, при превышении которого принимается решение отмены транзакции (Reader Contactless Transaction Limit (On-Device CVM/No On-Device CVM));
- значение лимита, при котором ядро MC уточняет решение согласно настройкам проверки держателя карты (Reader CVM Required Limit).

2.2. Поддерживаемые операции

Поддерживаются следующие типы финансовых операций:
- оплата товара/услуги с использованием карты - Purchase;
- выдача наличных - Cash;
- покупка с выдачей наличных - Purchase with Cashback;
- возврат денежных средств - Refund;
- внесение наличных - Cash Deposit;
- выдача наличных с участием оператора - Manual Cash;
- и другие.

Поддерживается административная операция отмены транзакции.

2.3. Поддержка работы со списком открытых ключей аутентификации (CAPK)

Ядро МС поддерживает работу со списком открытых ключей аутентификации: чтение поиск по индексу.

2.4. Поддержка сообщений в процессе транзакции (Outcome)

Ядро МС в полном объёме поддерживает выдачу стандартизованных сообщений Outcome. Кроме того, архитектура программного обеспечения позволяет включать и отключать выдачу Outcome-сообщений с помощью административных настроек.

2.5. Поддержка протокола прямого обмена данными с ядром во время транзакции (DEK/DET)

Ядро МС в полном объёме поддерживает протокол прямого обмена данными с ядром согласно спецификации "Mastercard Contactless Reader Specification". Для поддержки протокола архитектурой программного обеспечения предусмотрена передача необходимой информации ядру вместе с настройками.

2.6. Поддержка режимов работы ядра

В зависимости от типа терминала ядро МС поддерживает работу в следующих режимах:
- только онлайн (online-only);

- только оффлайн (offline-only);
- оффлайн с возможностью онлайн (offline with online capability).

Режим работы регулируется настройками ядра MC, в частности "Terminal Type".

2.7. Чтение баланса (Balance Read)

Некоторые карты платёжной системы Mastercard поддерживают хранение оффлайн-баланса, ядро MC поддерживает чтение этого баланса и передачу его в Outcome-сообщении и/или тегах транзакции.

2.8. Режим работы с магнитной полосой (Mag-stripe Mode)

Ядро MC поддерживает инфраструктуру магнитной полосы - проведение транзакции на основании данных "дорожки 1" (track1) и "дорожки 2" (track2), полученных с карты.

2.9. Режим работы с инфраструктурой чипа карты (EMV Mode)

Ядро MC в полном объёме поддерживает работу в режиме EMV с выдачей минимального требуемого объёма данных транзакции, кроме того, ядро предоставляет возможность выдачи всего объёма данных (всех тегов, полученных во время транзакции).

2.10. Поддерживаемые методы аутентификации платёжного приложения

Ядро MC поддерживает следующие методы аутентификации платёжного приложения:

- SDA - Static Data Authentication - аутентификация, основанная на статических данных;
- DDA - Dynamic Data Authentication - аутентификация, основанная на динамических данных;
- CDA - Combined Data Authentication - комбинированная аутентификация.

Современные карты платёжной системы Mastercard используют только один тип аутентификации платёжного приложения - CDA.

2.11. Работа с мобильными устройствами (Mobile Transactions)

Ядро МС поддерживает работу с мобильными устройствами при проведении транзакций, также ядро поддерживает проведение транзакции с методом проверки держателя карты "On-device CVM".

2.12. Защита от атак с использованием стороннего терминала, протокол RRP

Ядро МС поддерживает в полном объёме протокол RRP (Relay Resistance Protocol).

2.13. Работа с отозванными сертификатами

Ядро МС поддерживает работу со списком отозванных сертификатов.