социальные системы
www.socialsystems.ru

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

Руководство по эксплуатации

Листов 19

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
TEI	Test Environment Interface - интерфейс тестового окружение - короткое название приложения "L2 Test Environment"
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".

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.

Для работы с ядром MC необходимо предварительно скомпилировать, собрать его под определённую аппаратную платформу и установить. Процесс сборки и установки ПО лежит за рамками этого документа. Подразумевается, что аппаратная платформа, на которое производится установка, обладает необходимым функционалом реализации физического уровня протокола ISO/IEC 14443(A/B), другими словами, должна иметь в своём составе микросхему NFC. Для упрощения здесь и далее предлагается называть такую аппаратную платформу ридером или устройством.

Для управления ридером и обмена данными с ридером должен быть разработан протокол, реализующий набор необходимых команд для эксплуатации функций программных модулей, установленных на ридер, в частности одним из таких модулей должно быть ядро MC.

Для управления ридером по разработанному протоколу необходима реализация так называемой терминальной программы или терминального ПО, которое может быть установлено на другое устройство и осуществлять взаимодействие с ридером в автоматическом режиме, либо такое ПО может быть выполнено в виде программы как с графическим интерфейсом, так и без него, установленной на ПЭВМ и работающей по командам или манипуляциям человека-оператора.

В данном документе предлагается описание эксплуатации ядра MC по второму варианту, где в качестве терминального ПО выступает приложение с графическим интерфейсом, которое устанавливается на ПЭВМ. Приложение было разработано для сертификации в одной из лабораторий компании EMVCo, по требованиям к этому ПО интерфейс приложения - английский. В качестве примера аппаратной платформы в данном документе будет рассмотрен ридер "BCAM-01", разработанный российской компанией ООО "Социальные системы". Протокол обмена и управления "BCAM-01" - PB3P, разработанный также ООО "Социальные системы".

1.1. Требования к программным и техническим средствам

Для работы с ядром MC, где терминальной программой является приложение, установленное на ПЭВМ, и с выбранной аппаратной платформой "BCAM-01" требуется:

- инструментальная ПЭВМ под управлением ОС Windows, версии не ниже 8, с установленной на ПЭВМ программой "L2 Test Environment" (далее TEI), версии не ниже 1.2.0;

- устройство "BCAM-01" с загруженной на него рабочей программой, версии не ниже 2.5.1, с модулем ядра MC, версии не ниже 1.0; устройство должно быть подключено к ПЭВМ по USB-кабелю;

- банковская карты, выпущенная с приложением Mastercard, с бесконтактным интерфейсом.

1.2. Начало работы

Для начала работы требуется запустить приложение TEI, открыть вкладку 'Settings', выбрать порт, который назначен для ридера, нажать на форме кнопку 'Open'. Приложение TEI откроет порт, автоматически опросит версии ПО ридера и выведет их в поле 'Versions' (рисунок 1).

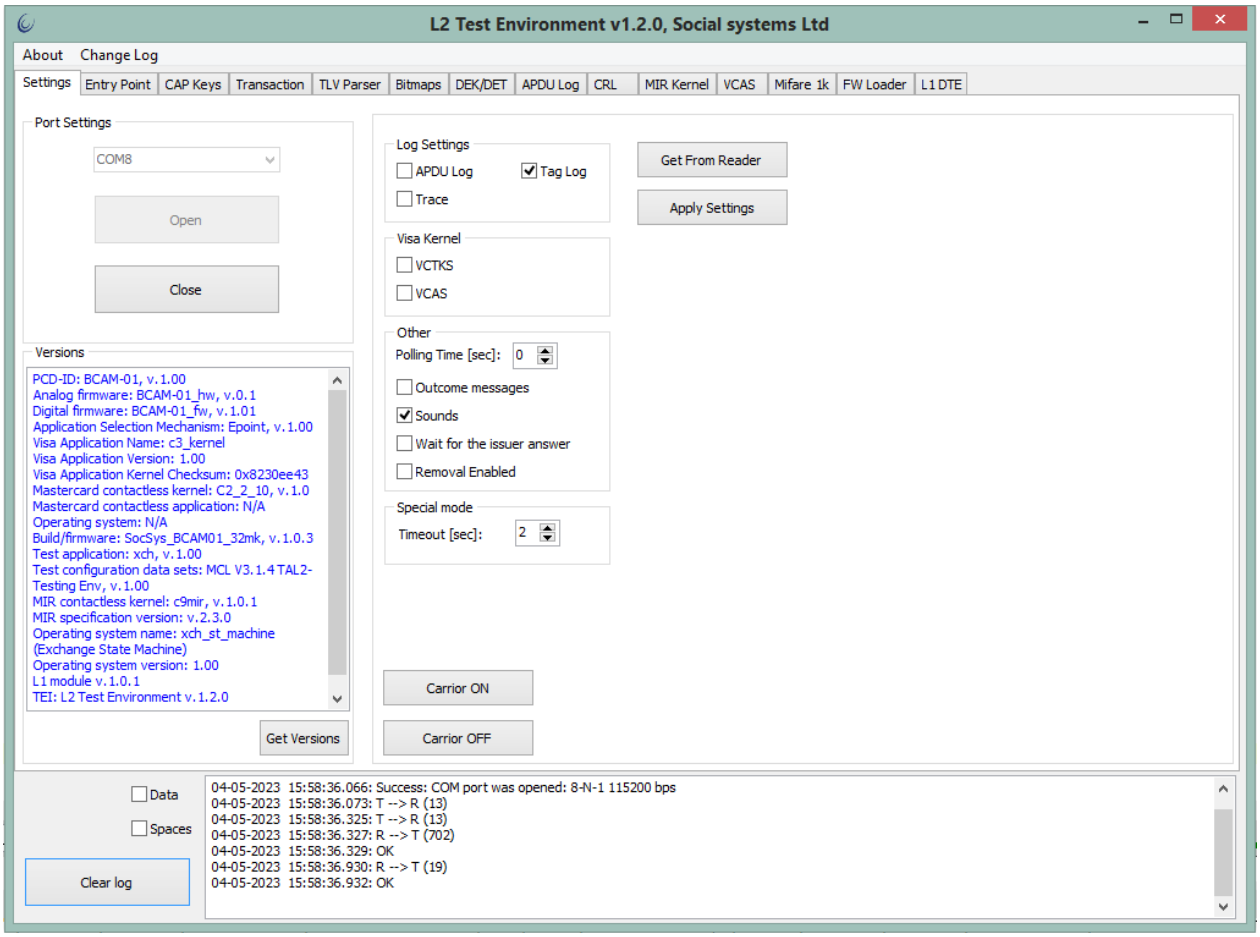

Рисунок 1 - Начало работы, открытие порта.

2. Эксплуатация ядра МС

2.1. Настройки ядра МС

Архитектура программного обеспечения ядра МС 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 МС уточняет решение согласно настройкам проверки держателя карты (Reader CVM Required Limit).

Для реализации данного функционала в приложении TEI предусмотрены элементы управления. Для задания настроек ядра МС следует открыть вкладку 'Entry Point'. В левой части окна, в секции 'Processing Configuration', добавить AIP (номер приложения) 'A000000004', нажав на кнопку 'Add'. В правой части, в секции 'EP configuration', добавить запись с настройками (кнопка 'Add'), изменить поле 'Kernel ID', кликнув на поле и выбрав из списка элемент 'C-2 MASTERCARD', слева от созданной записи нажать на 'Edit...' (рисунок 2). Откроется форма, в которой можно

вводить обозначенные в данном пункте настройки (рисунок 3), в конце изменений следует нажать кнопку 'Accept'.

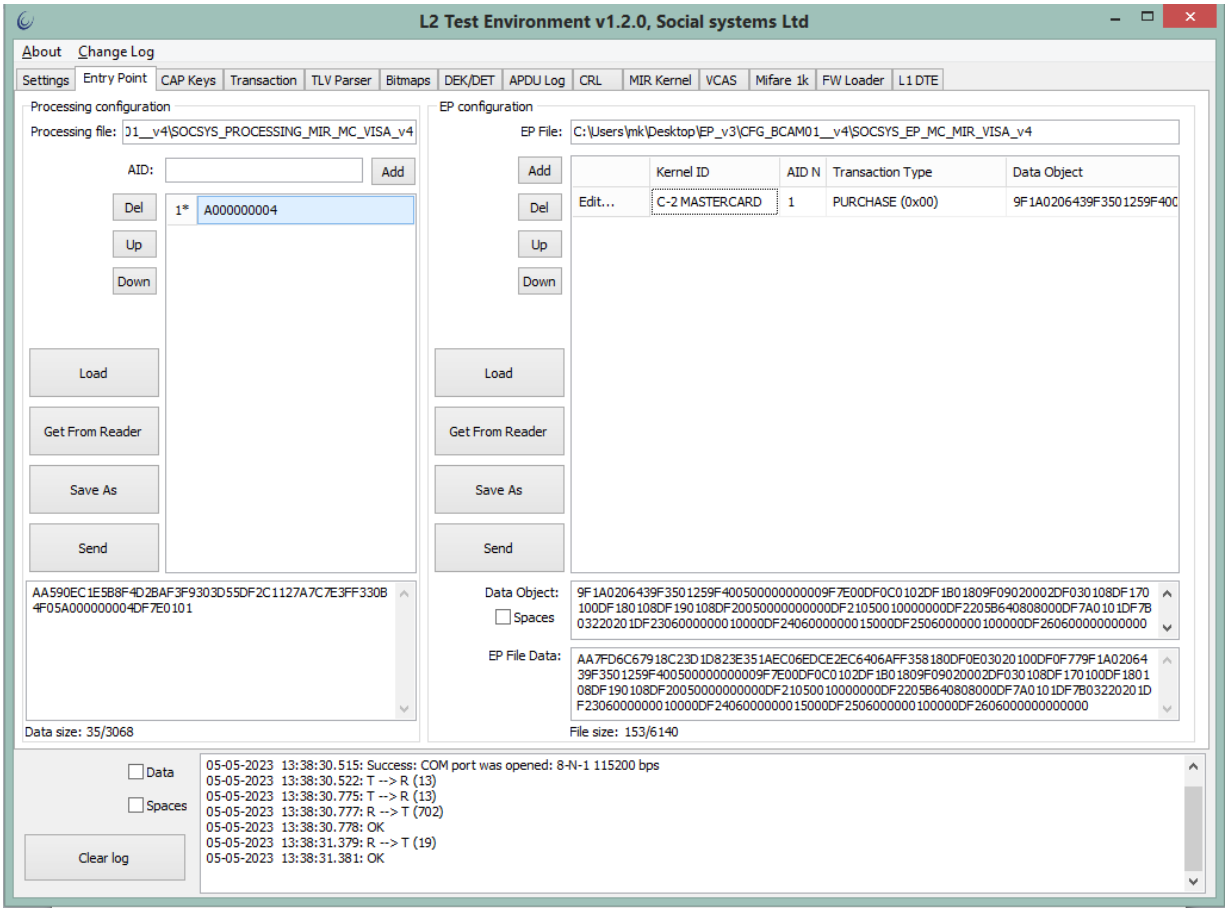

Рисунок 2 - Добавление поддерживаемых AID и настроек для AID.

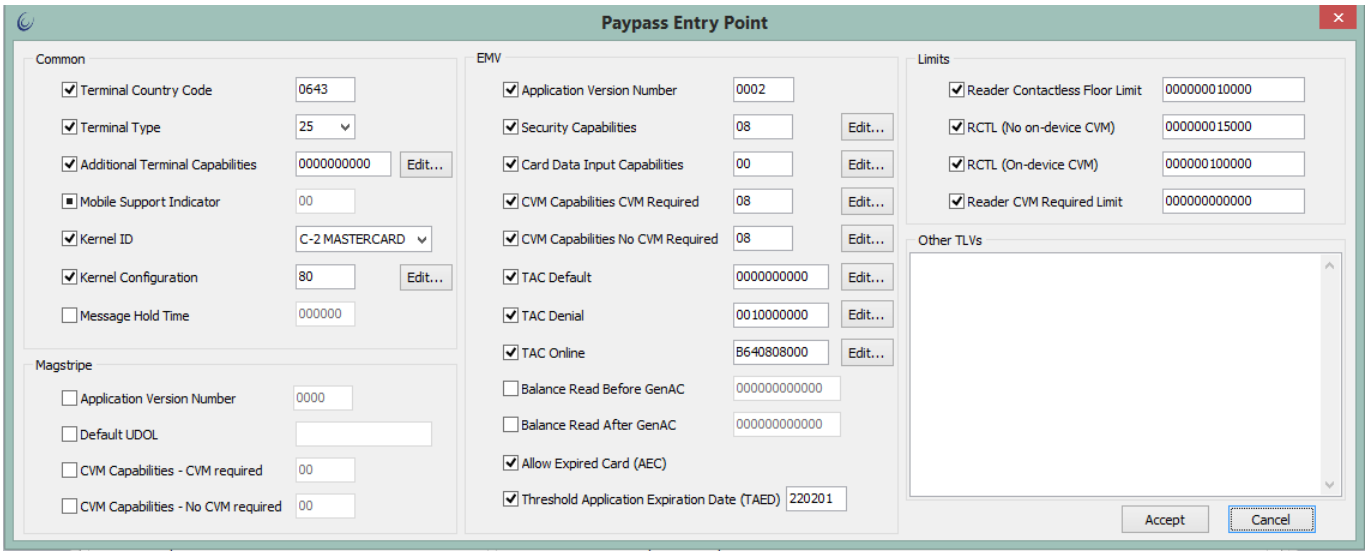

Рисунок 3 - Настройки бесконтактного ядра Mastercard

После внесения изменений настройки следует отправить в ридер, для этого необходимо в секциях 'Processing Configuration' и 'EP configuration' нажать кнопку 'Send'.

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.

Тип операции задаётся при конфигурировании ядра МС (пункт 2.1 настоящего документа). Для задания поддерживаемой операции на вкладке 'Entry Point', в секции 'EP configuration' необходимо кликнуть на сформированной записи в поле 'Transaction Type' и выбрать из списка необходимую операцию (Рисунок 2). Для каждой тройки 'Kernel ID - AID N - Transaction Type' требуется своя конфигурационная запись.

Ядром МС поддерживается административная операция отмены транзакции. Для исполнения этой команды ядром МС необходима предварительная команда начала транзакции. Чтобы начать транзакцию, необходимо на вкладке 'Settings' полю 'Polling Time' присвоить значение 20 [секунд], нажать кнопку на форме 'Apply Settings'. Далее требуется перейти на вкладку 'Transaction' и нажать кнопку 'Start transaction', приложение пошлёт команду ридеру и будет в течение 20 секунд ожидать результата транзакции. Отменить транзакцию можно, нажав на кнопку 'Cancel' на той же вкладке 'Transaction', ридер ответит на команду результатом '-130' ("Cancelled by user") (рисунок 4).

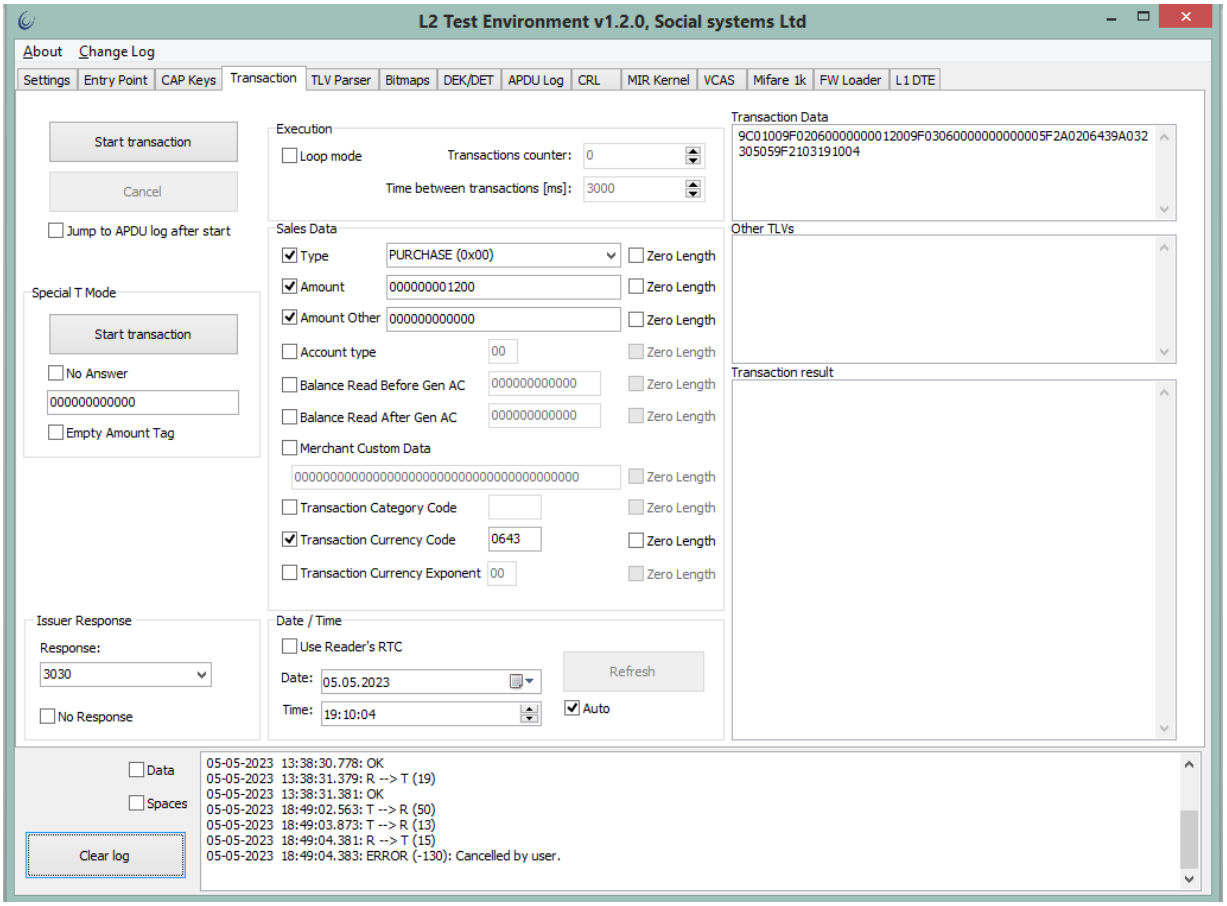

Рисунок 4 - Результат команды отмены транзакции. В нижней части формы, в консоли.

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

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

Для составления списка в приложении TEI предусмотрены элементы управления на вкладке 'CAPK'. Перед началом работы с ядром МС необходимо передать ридеру список CAPK, для этого следует перейти на указанную вкладку в приложении TEI нажать кнопку 'Add' и заполнить поля: RID, Index, Modulus, Exponent. При необходимости повторить по количеству ключей. Сформированный таким образом список CAPK требуется передать ридеру, это можно сделать, нажав кнопку 'Send' на вкладке 'CAPK' (рисунок 5).

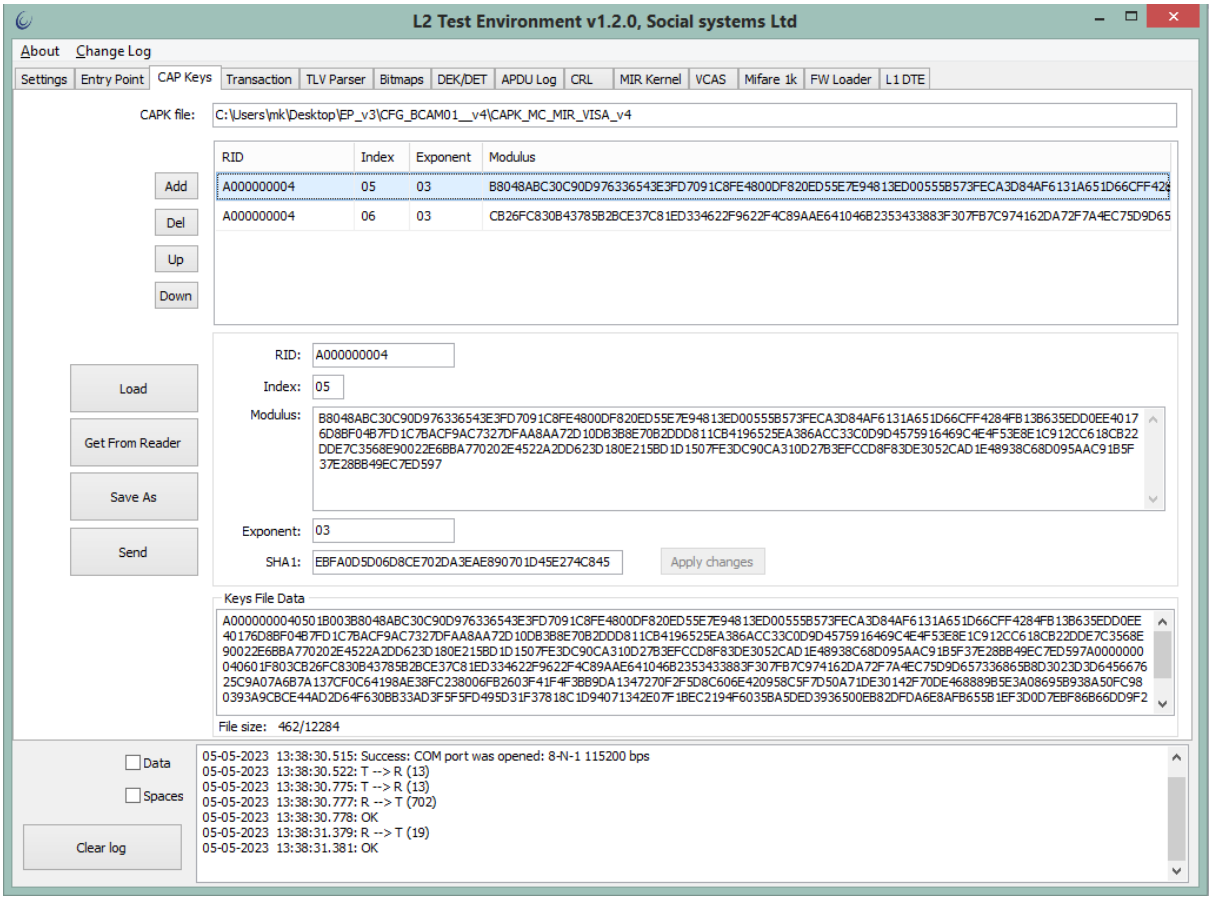

Рисунок 5 - Формирование списка CAPK

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. Чтобы включить Outcome-сообщения необходимо перейти на вкладку 'Settings' приложения TEI и отметить поле 'Outcome messages' и нажать кнопку 'Apply Settings' (рисунок 6). В процессе транзакции от ридера будут приходить формализованные сообщения в виде посылок PB3P от ридера, их интерпретация - ответственность терминальной программы - в данном случае TEI. Для начала транзакции требуется перейти на вкладку 'Transaction' и нажать кнопку 'Start transaction', внести карту Mastercard в поле действия антенны. После того, как ридер вернёт результат, перейти на вкладку 'APDU Log'. В консоли выполнения транзакции будут видны сообщения ядра с результатом (рисунок 7). Содержимое консоли в зависимости от результата будет следующее:

```
MSG - UI REQUEST DATA
      Data:                  15020000000000000000000000000000000000000000000000
      Message:               PRESENT CARD
      Status:                READY TO READ
```

```
      Hold Time:              000000
      Language Preference:    0000000000000000
      Value Qualifier:        NONE
      Value:                  000000000000
      Currency Code:          0000


MSG - UI REQUEST DATA
      Data:                   1E040000007275656E66726465000000000000000000
      Message:                CLEAR DISPLAY
      Status:                 CARD READ SUCCESSFULLY
      Hold Time:              000000
      Language Preference:    7275656E66726465
      Value Qualifier:        NONE
      Value:                  000000000000
      Currency Code:          0000


OUT - OUTCOME PARAMETR SET
      Data:                   30F0F000B8F0FF00
      Status:                 ONLINE REQUEST
      Start:                  N/A
      Online Resp Data:       N/A
      CVM:                    NO CVM
      UI Req. On Outcome:     1
      UI Req. On Restart:     0
      Receipt:                YES
      DR:                     1
      DD:                     1
      Alternate Interface:    N/A
      Field Off:              N/A
      Removal Timeout:        0


OUT - DISCRETIONARY DATA
      Data:
      9F42020643DF810E0100DF810F01009F6E07064300003030000DF8115060000000000FF
      Error Indication        0000000000FF
      L1 error:               OK
      L2 error:               OK
      L3 error:               OK
      SW1SW2:                 0000
      Message on error:       N/A
      9F42                    0643
      DF810E                  00
      DF810F                  00
      9F6E                    06430000303000


OUT - DATA RECORD
      Data:
      9F02060000000012009F03060000000000009F2608D8A36A5CE0C8C4585F2403220531820219805
00A4D617374657243617264 5A0855369137500000000F3401019F120A4D617374657243617264 9F3602065
C9F0702FF009F090200029F2701809F34031F03028407A00000000410109F10120110A040032200000000
00000000930001FF9F1101019F33030008089F1A0206439F3501229505004000000157135536913750858
918D22052011236557900000F5F2A0206439A032305059C01009F3704039DDF25
      9F02              000000001200
      9F03              000000000000
      9F26              D8A36A5CE0C8C458
      5F24              220531
```

```
82                  1980
50                  4D617374657243617264
5A                  5536913750000000
5F34                01
9F12                4D617374657243617264
9F36                065C
9F07                FF00
9F09                0002
9F27                80
9F34                1F0302
84                  A0000000041010
9F10                0110A040032200000000000000000930001FF
9F11                01
9F33                000808
9F1A                0643
9F35                22
95                  0040000001
57                  5536913750858918D22052011236557900000F
5F2A                0643
9A                  230505
9C                  00
9F37                039DDF25
```

```
OUT - UI REQUEST DATA
      Data:                     1B0000000072756 56E6672646500000000000000000
      Message:                  AUTHORISING, PLEASE WAIT
      Status:                   NOT READY
      Hold Time:                000000
      Language Preference:      7275656E66726465
      Value Qualifier:          NONE
      Value:                    000000000000
      Currency Code:            0000
```

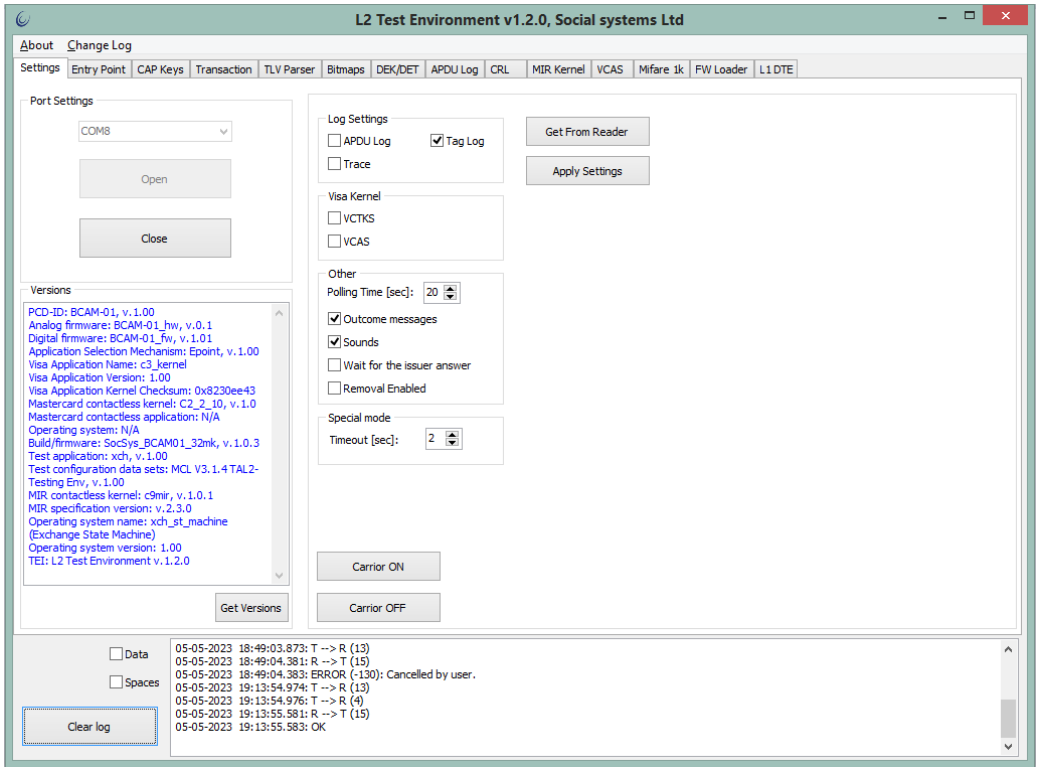

Рисунок 6 - Включение Outcome-сообщений

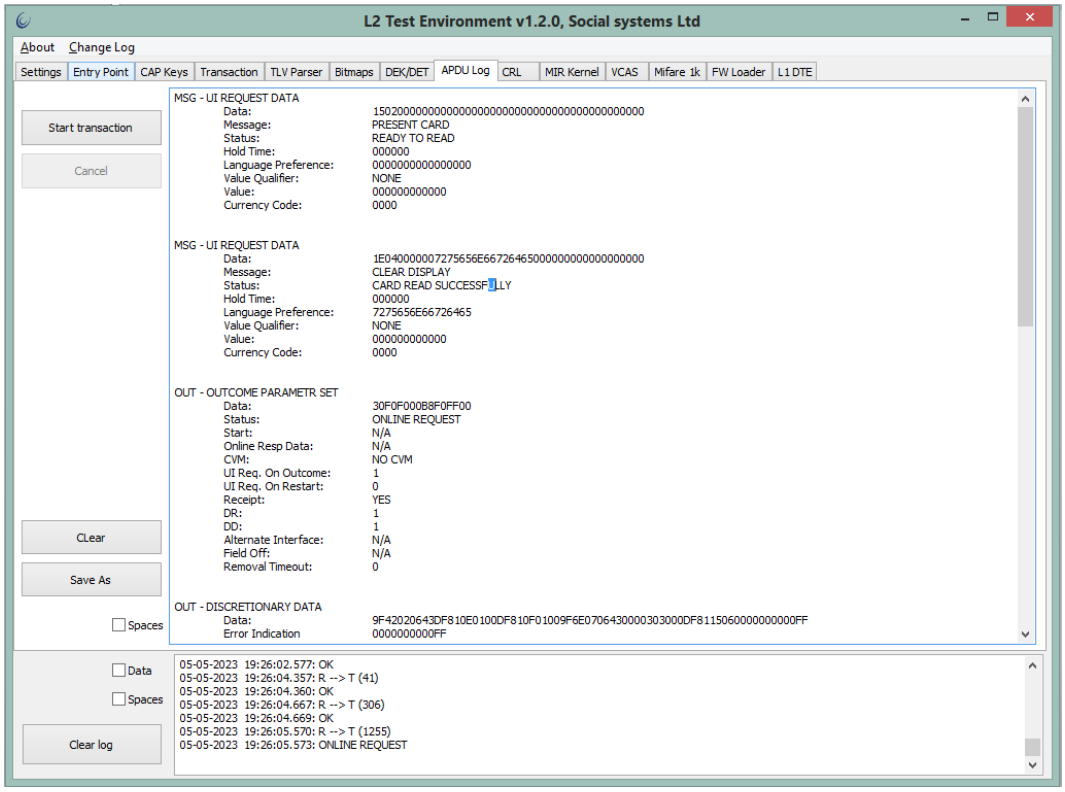

Рисунок 7 - Вывод Outcome-сообщений в приложении TEI в процессе транзакции.

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

Ядро MC 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.

Начало процесса обмена программируется через теги конфигурации согласно спецификации бесконтактного ядра Mastercard. В приложении TEI для DEK/DET обмена предусмотрен механизм xml-скриптов. Скрипт обмена может быть открыт в приложении TEI на вкладке 'DEK/DET' (рисунок 8).

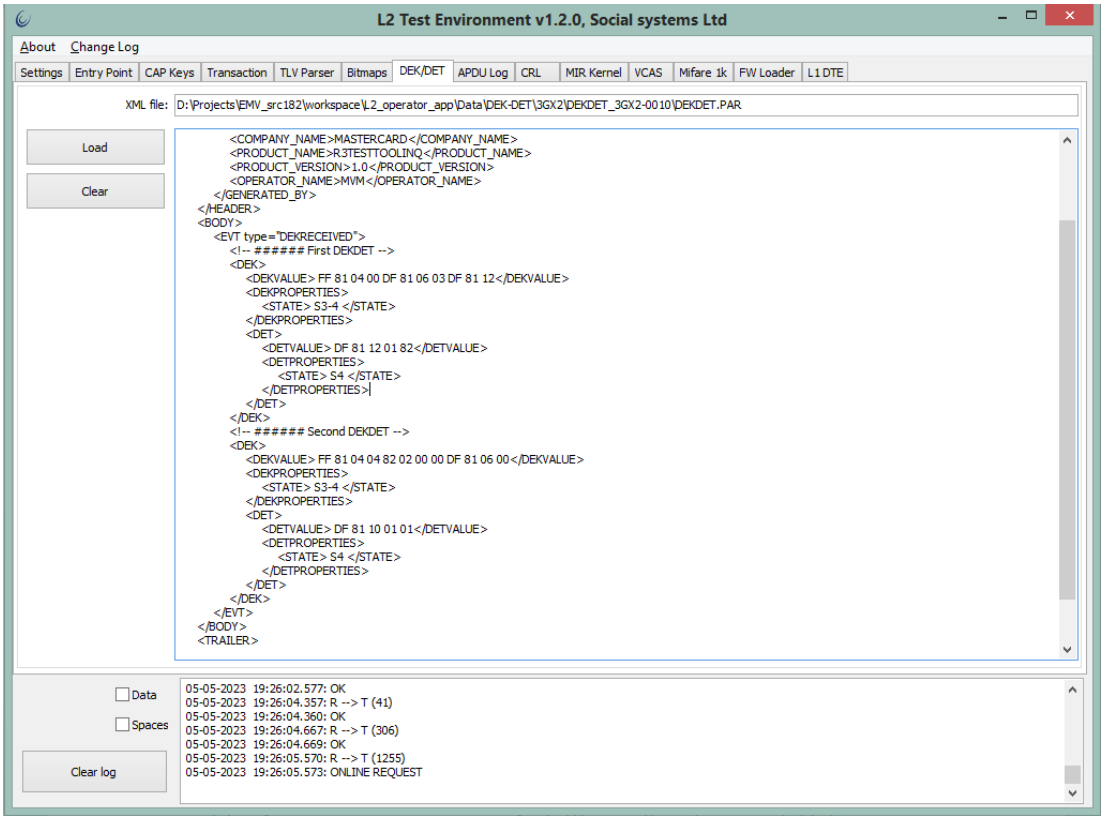

Рисунок 8 - Загрузка скрипта DEK/DET

2.6. Поддержка режимов работы ядра

В зависимости от типа терминала ядро MC 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". Значение "Terminal Type" выставляется на форме настроек Mastercard - форма 'Paypass Entry Point' (рисунок 3).

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.

Баланс передаётся приложению от ридера в виде тегов в соответствии со спецификацией Mastercard.

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

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

Поддержка инфраструктуры настраивается на форме 'Paypass Entry Point', в секции 'Magstripe' (рисунок 3), включается возможность проведения транзакции в этом режиме в поле 'Kernel Configuration' на той же форме (рисунок 9).

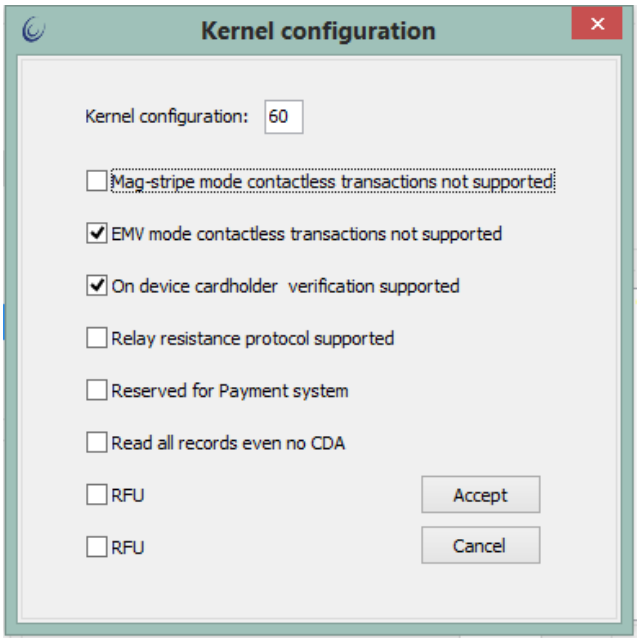

Рисунок 9 - Настройка параметра 'Kernel configuration'

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

Ядро МС 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).

Ридер в конце транзакции присылает результат и данные транзакции. В приложении TEI теги транзакции помещаются в поле 'Transaction result' на вкладке 'Transaction' (рисунок 10). В нижней части окна приложения - в консоли - выводится результат: ERROR в случае ошибки, Online Request в случае, когда необходим ответ эмитента, Approved в случае, когда транзакция одобрена в offline, и Decline в случае отклонения транзакции. Данные транзакции представляют собой набор тегов, записанных в формате BER-TLV, просмотреть которые можно дважды щёлкнув мышкой на поле 'Transaction result', в этом случае приложение переключится на вкладку 'TLV Parser' (рисунок 11).

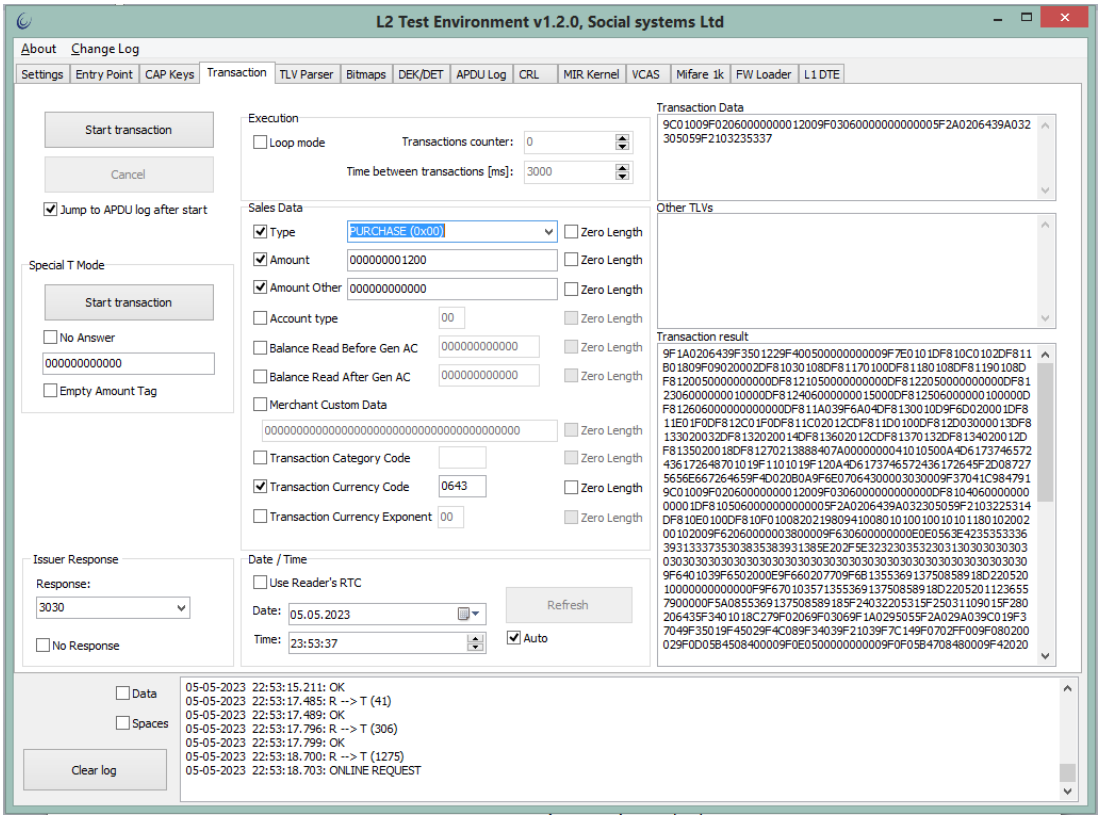

Рисунок 10 - Результат проведения транзакции (Online Request)

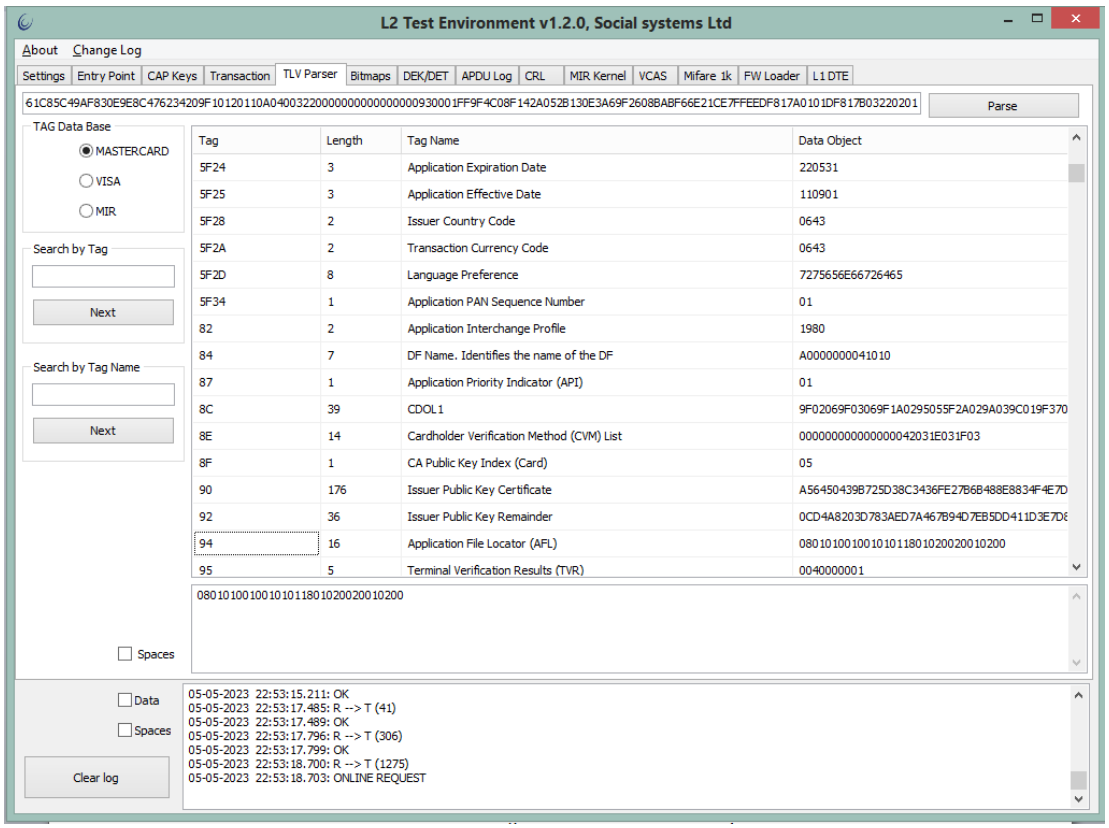

Рисунок 11 - Расшифровка тегов транзакции.

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.

Включение поддержки в ядре CDA осуществляется через форму 'Paypass Entry Point' в поле 'Security Capability' (рисунок 12).

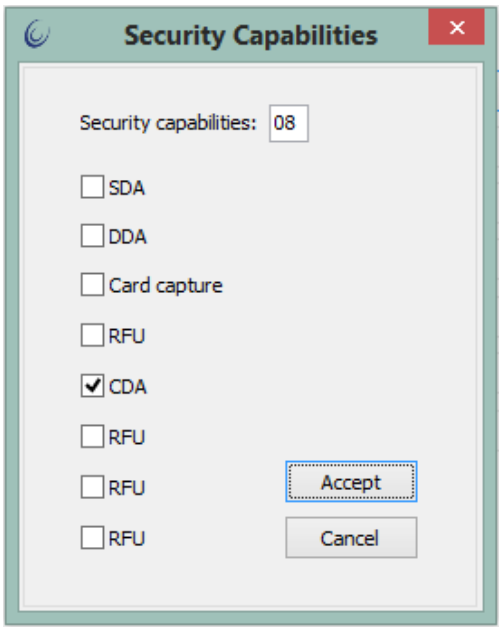

Рисунок 12 - Включение поддержки CDA

2.11. Работа с мобильными устройствами (Mobile Transactions)

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

Включение поддержки проведения транзакции с методом проверки держателя карты "On-device CVM" производится в настройках ядра MC, изменение этого параметра включения можно произвести в приложении TEI на форме 'Paypass Entry Point', в поле 'Mobile Support Indicator' (рисунок 3).

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

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

Поддержка этого протокола настраивается через конфигурацию ядра. В приложении TEI сделать это можно через форму 'Paypass Entry Point', в поле 'Kernel Configuration' (рисунок 9).

2.13. Работа с отозванными сертификатами

Ядро МС поддерживает работу со списком отозванных сертификатов: чтение, поиск по списку.

Список отозванных сертификатов загружается в ридер наряду с настройками ядра. Создать и загрузить в ридер список отозванных сертификатов (CRL) можно в приложении TEI на вкладке 'CRL' (рисунок 13). Отправить список в ридер можно, нажав кнопку 'Send'.

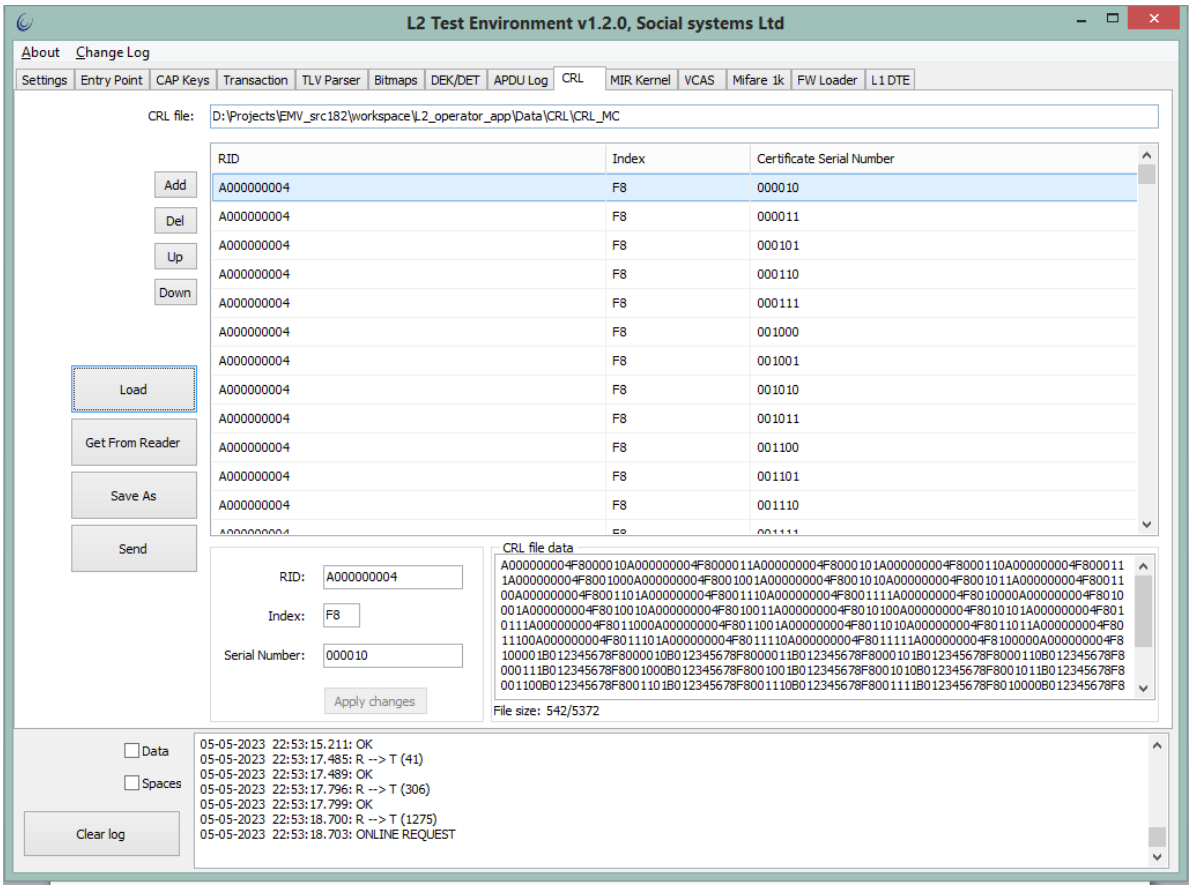

Рисунок 13 - Формирование и отправка ридеру списка отозванных сертификатов.