социальные системы
www.socialsystems.ru

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

Эксплуатация программного обеспечения

Листов 17

Москва, 2023

Оглавление

Список сокращений

Сокращение	Расшифровка
AID	Application Identifier - номер платёжного приложения
CVM	Cardholder Verification Method – метод идентификации владельца карты
DDA	Dynamic Data Authentication – метод проверки легитимности EMV-карты, основанный на динамических данных
EMV	Europay + MasterCard + VISA – международный стандарт для операций по банковским картам с чипами
fDDA	fast Dynamic Data Authentication - быстрый динамический метод аутентификации
MCC	Merchant Category Code
SDA	Static Data Authentication – метод проверки легитимности EMV-карты, основанный на статических данных
TEI	Test Environment Interface - интерфейс тестового окружение - короткое название приложения "L2 Test Environment"
TTQ	Terminal Transaction Qualifier

Аннотация

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

1. Общие сведения

Программное обеспечение устройства для работы с бесконтактными картами платёжной системы "Visa" (далее ядро "Visa") соответствует документу "Visa Contactless Payment Specification (VCPS)", версии 2.2.

Для работы с ядром "Visa" 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 "Visa".

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 МС 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 "Visa", 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 "Visa", версии не ниже 1.0.0; устройство должно быть подключено к ПЭВМ по USB-кабелю;

- банковская карты, выпущенная с приложением Visa, 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).

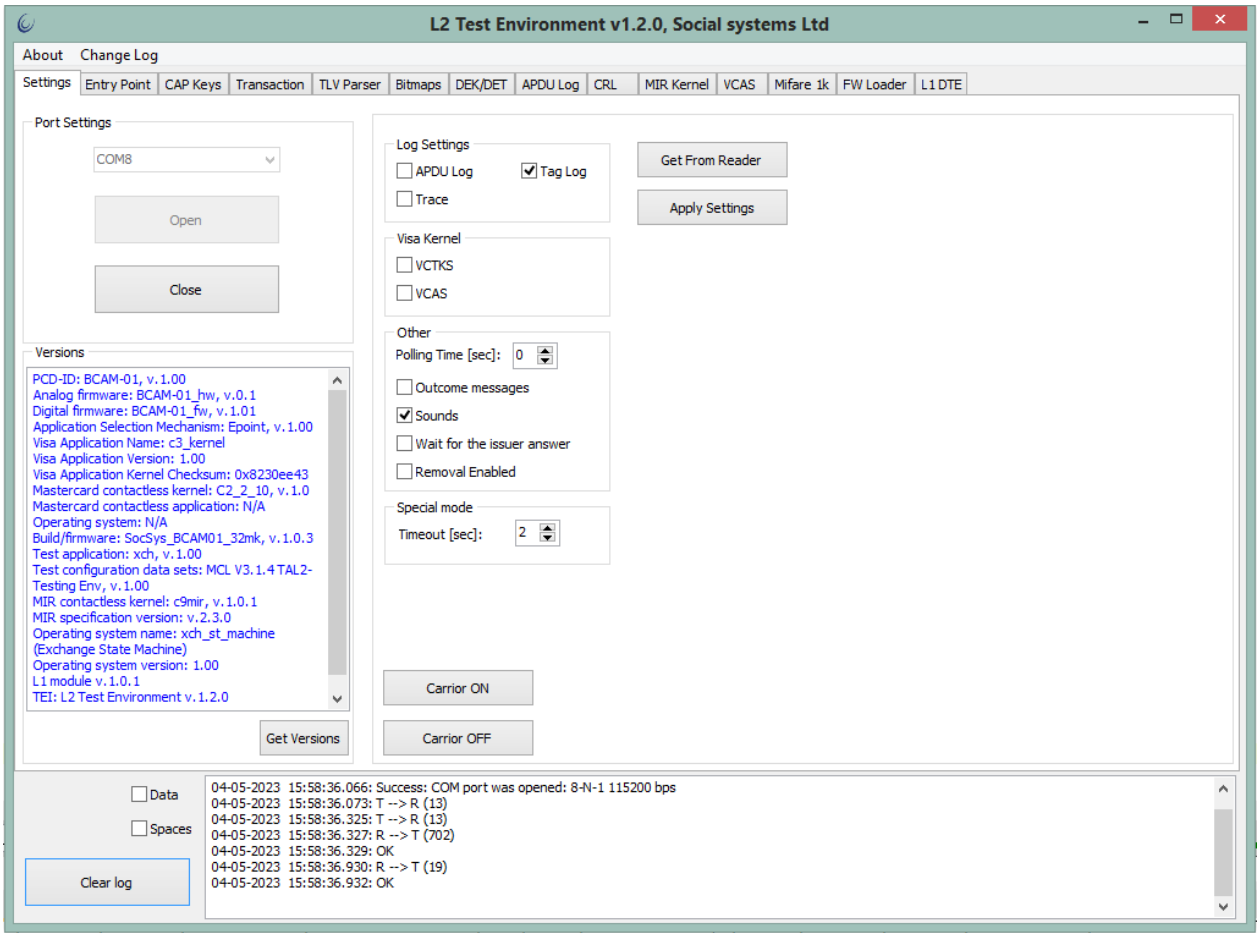

Рисунок 1 - Начало работы, открытие порта.

2. Функциональные характеристики ядра "Visa"

2.1. Настройки ядра "Visa"

Архитектура программного обеспечения ядра "Visa" позволяет:

- вводить настройки как для отдельных платёжных приложений (AID), так и для группы платёжных приложений;
- вводить настройки для каждого типа поддерживаемых операций;
- для операций "Purchase", "Manual cash" предусмотрены настройки лимитов и безопасности для вариантов операции с "Cashback" и без него.

Поддерживаются следующие настройки ядра:

- тип терминала (Terminal Type);
- код страны терминала (Terminal Country Code);
- настройки возможностей терминала (Terminal Capabilities);
- дополнительные настройки возможностей терминала (Additional Terminal Capabilities);
- настройки ограничений (Processing Restrictions Options);
- наименование категории точки продаж (Merchant Category Code - MCC);
- поддерживаемая версия платёжного приложения карты (Application Version Number);
- сумма транзакции, при превышении которой (и при отсутствии Reader Contactless Floor Limit) требуется онлайн-авторизация (Floor Limit), указывается для операций с "Cashback" и без него;
- сумма транзакции, при превышении которой требуется онлайн-авторизация (Reader Contactless Floor Limit), указывается для операций с "Cashback" и без него;
- сумма транзакции, при достижении или превышении которой транзакция отклоняется или предлагается использовать другой интерфейс ридера (Reader Contactless Transaction Limit), указывается для операций с "Cashback" и без него;
- сумма транзакции, при достижении или превышении которой требуется проверка держателя карты (Reader CVM Required Limit), указывается для операций с "Cashback" и без него;
- настройки управления рисками (Reader Risk Parameters), указывается для операций с "Cashback" и без него;
- квалификатор терминала (Terminal Transaction Qualifier - TTQ), указывается для операций с "Cashback" и без него;
- выбор поведения терминала при проверке статуса с нулевой суммой (Amount, Authorized of Zero Check: Option 1/Option 2).

Для реализации данного функционала в приложении TEI предусмотрены элементы управления. Для задания настроек ядра "Visa" следует открыть вкладку

'Entry Point'. В левой части окна, в секции 'Processing Configuration', добавить AIP (номер приложения) 'A000000003', 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-3 VISA', 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'.

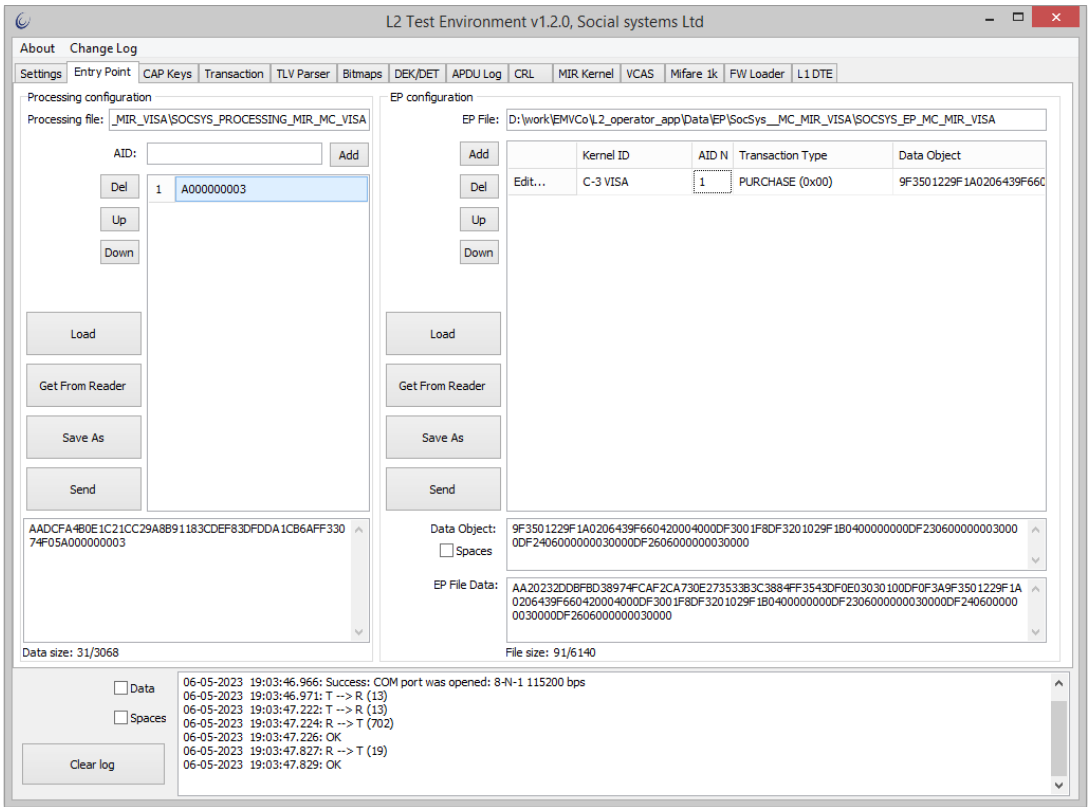

Рисунок 2 - Добавление поддерживаемых AID и настроек для AID.

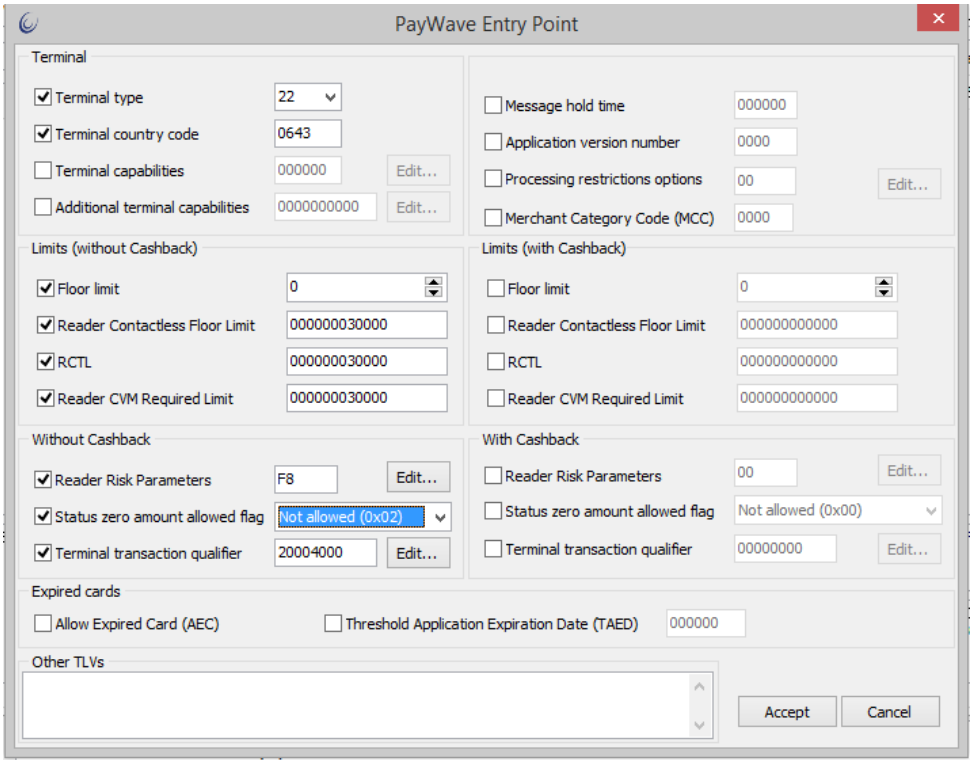

Рисунок 3 - Настройки бесконтактного ядра "Visa".

2.2. Поддерживаемые операции

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

Тип операции задаётся при конфигурировании ядра "Visa" (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 "Visa" поддерживается административная операция отмены транзакции. Для исполнения этой команды ядром "Visa" 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).

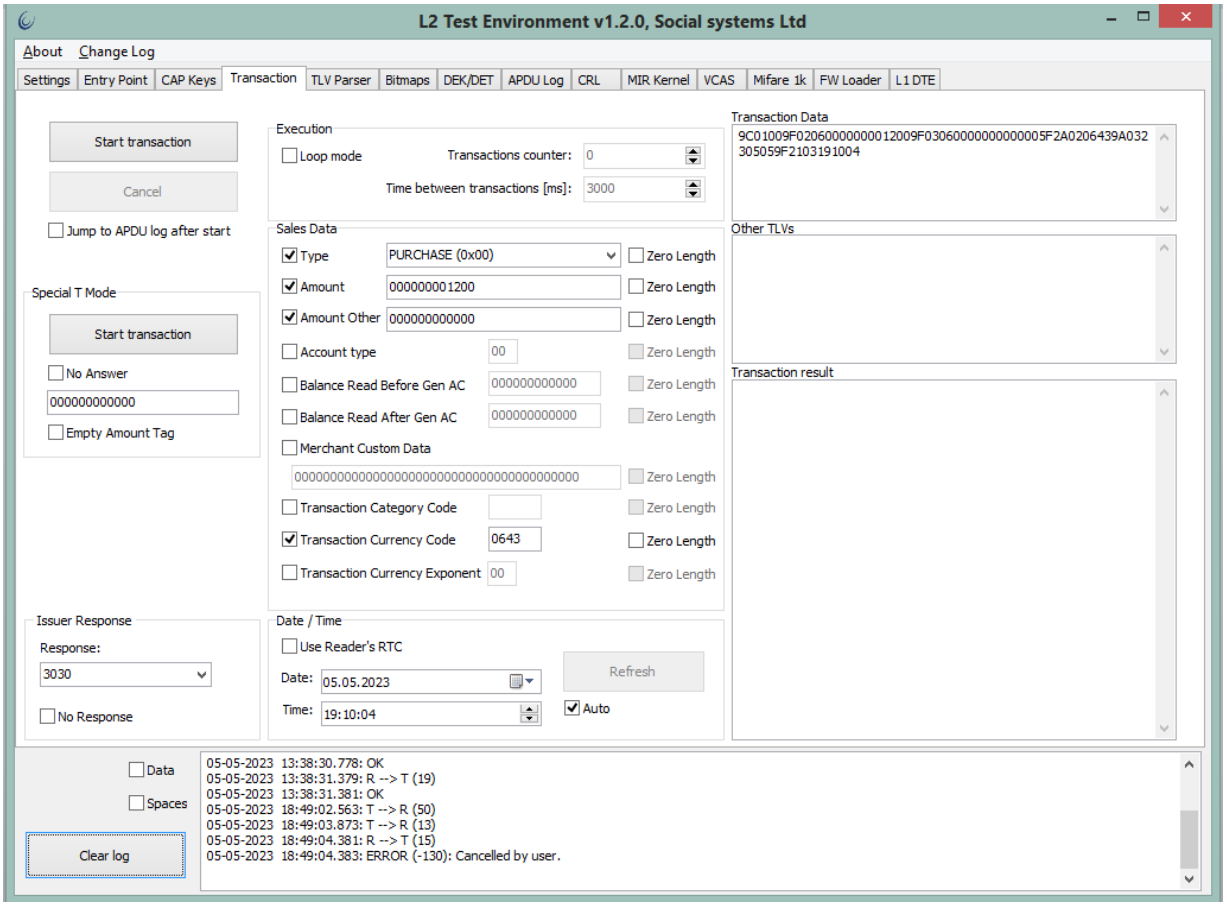

Рисунок 4 - Результат команды отмены транзакции. В нижней части формы, в консоли.

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

Ядро "Visa" 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 "Visa" 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).

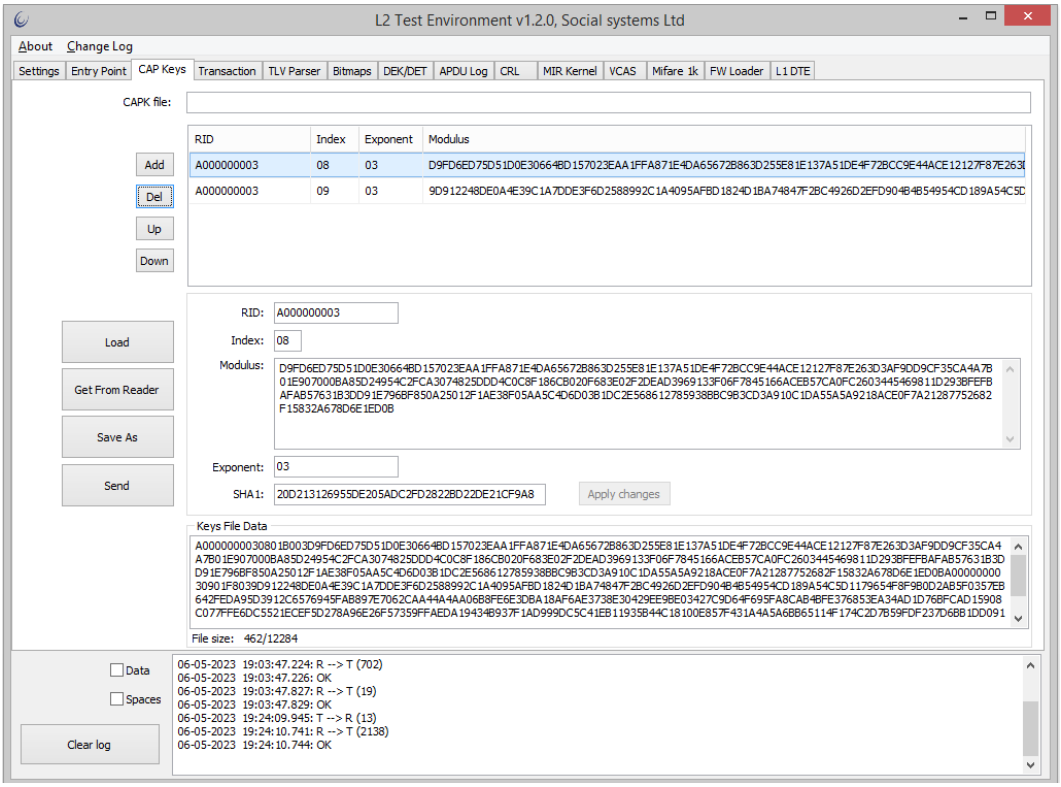

Рисунок 5 - Формирование списка CAPK

2.4. Поддержка сообщений в процессе транзакции (Outcome)

Ядро "Visa" 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 Visa 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:                   1502000000000000000000000000000000000000000000
      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:                   1E040000007275656E00000000000000000000000000
      Message:                CLEAR DISPLAY
      Status:                 CARD READ SUCCESSFULLY
      Hold Time:              000000
      Language Preference:    7275656E00000000
      Value Qualifier:        NONE
      Value:                  000000000000
      Currency Code:          0000


OUT - OUTCOME PARAMETR SET
      Data:                   30F0F800B0F0FF00
      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:                N/A
      DR:                     1
      DD:                     1
      Alternate Interface:    N/A
      Field Off:              N/A
      Removal Timeout:        0


OUT - DISCRETIONARY DATA
      Data:                   DF81150600000000000FF
      Error Indication        0000000000FF
      L1 error:               OK
      L2 error:               OK
      L3 error:               OK
      SW1SW2:                 0000
      Message on error:       N/A


OUT - DATA RECORD
      Data:
      9F390107DF17010857134817760259711616D22012011441390500001F5A0848177602597116165
F2002202F5F24032201315F2A0206435F340101820220009505000000000009A032305069C01009F020600
00000011009F03060000000000009F100706011103A020009F1A0206439F26082EF5BF84AF1655C19F270
1809F34033F00009F360206439F3704AF1A78759F6E04207000009F33030000409F21031934249F0607A0
0000000310109F660420004000
      9F39              07
      DF17              08
      57                4817760259711616D22012011441390500001F
      5A                4817760259711616
      5F20              202F
      5F24              220131
      5F2A              0643
      5F34              01
      82                2000
      95                0000000000
      9A                230506
      9C                00
```

```
9F02                000000001100
9F03                000000000000
9F10                06011103A02000
9F1A                0643
9F26                2EF5BF84AF1655C1
```

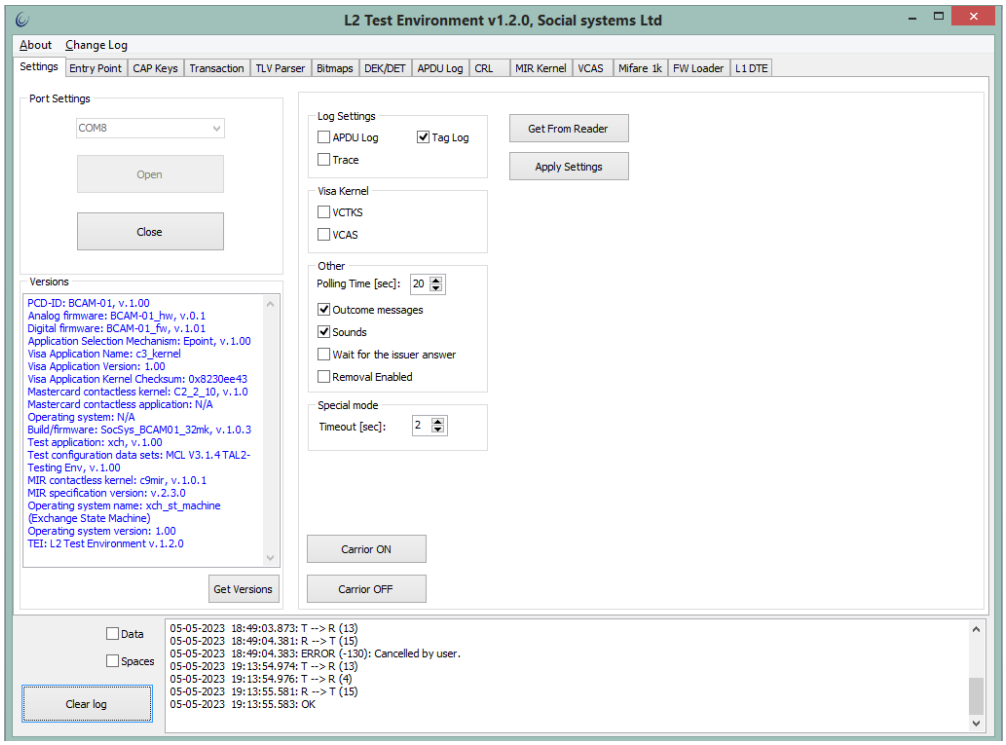

Рисунок 6 - Включение Outcome-сообщений

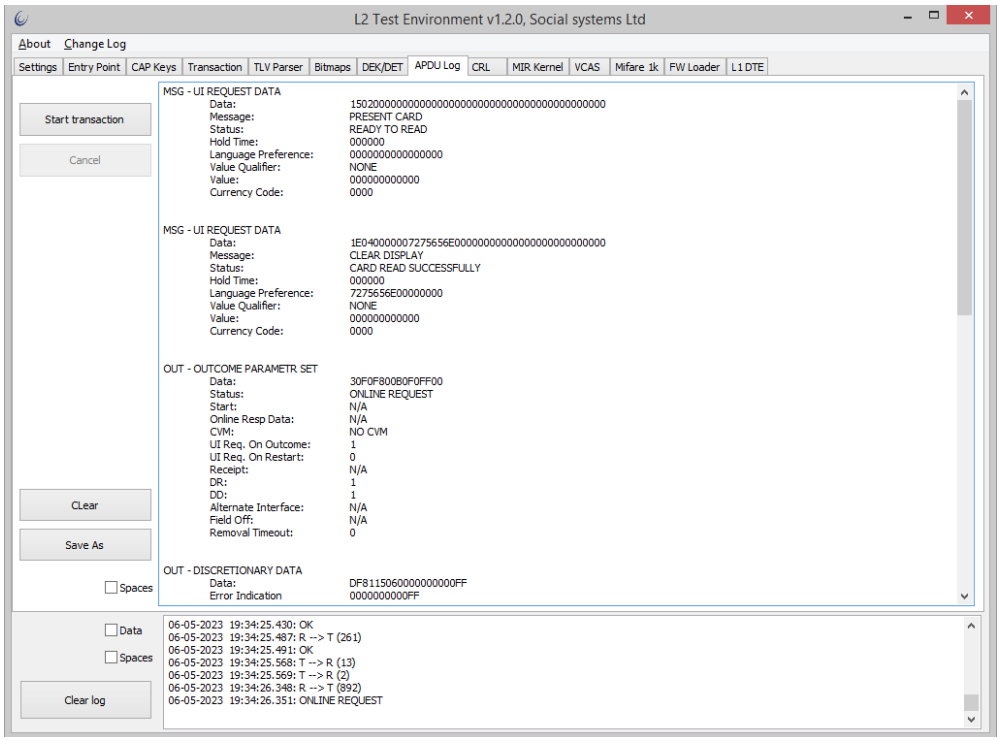

Рисунок 7 - Вывод Outcome-сообщений в приложении TEI в процессе транзакции.

2.5. Поддержка препроцессинга (Preliminary Transaction Processing - Pre-Processing)

Ядро "Visa" для минимизации времени работы с картой проводит препроцессинг в начале транзакции до включения поля антенны ридера. В рамках препроцессинга ядро осуществляет управление рисками на основе полученной суммы операции и настроек ядра. Если, например, превысить лимит ‘Reader Contactless Transaction Limit (RCTL)’ = 300, указав сумму транзакции, равной 301, то ридер вернёт ошибку ‘-127’ (“Contactless VISA transactions are not allowed” – бесконтактные транзакции Visa не разрешены), при этом ридер даже не включит поле антенны (рисунок 8).

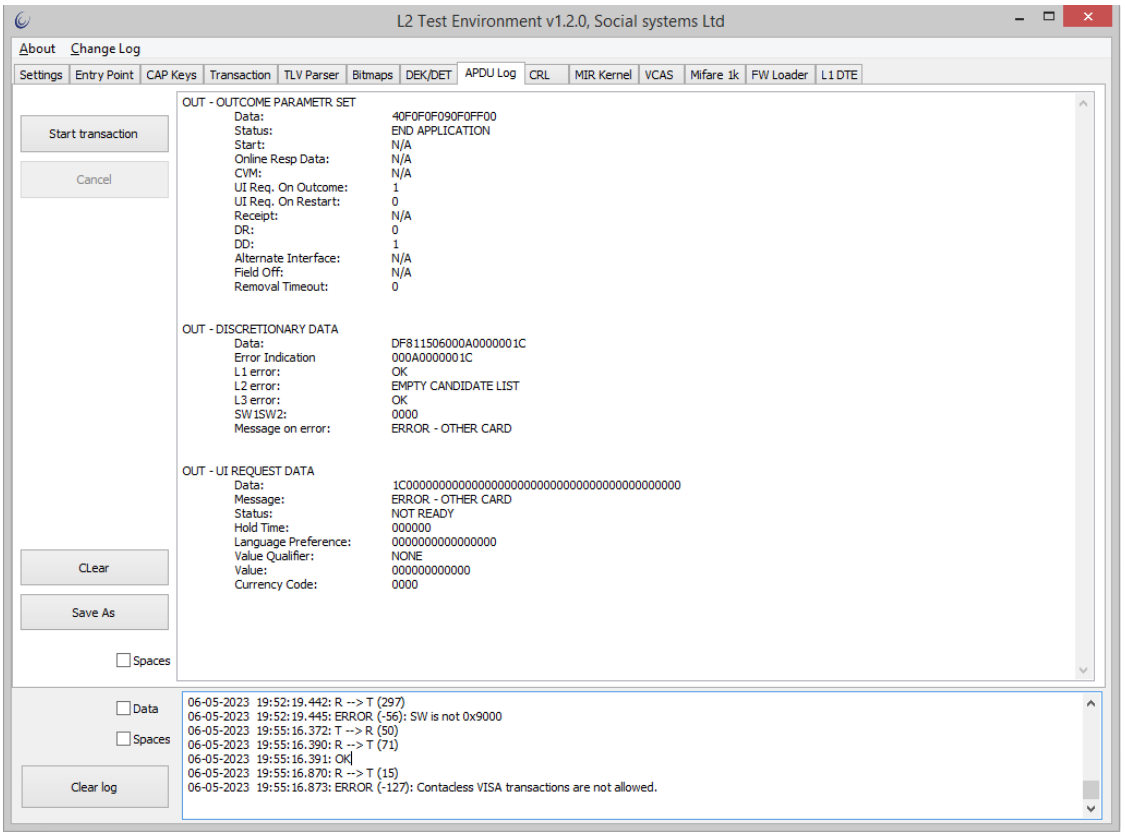

Рисунок 8 – Результат работы препроцессинга Visa, в нижней части формы, в консоли, можно видеть ошибку “ Contactless VISA transactions are not allowed ”.

2.6. Поддержка режимов работы ядра

В зависимости от типа терминала ядро "Visa" 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 "Visa", в частности "Terminal type". Значение "Terminal type" выставляется на форме настроек Visa - форма 'PayWave Entry Point' (рисунок 3).

2.7. Работа с отозванными сертификатами (CRL)

Ядро "Visa" поддерживает работу со списком отозванных сертификатов.

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 9). Отправить список в ридер можно, нажав кнопку 'Send'.

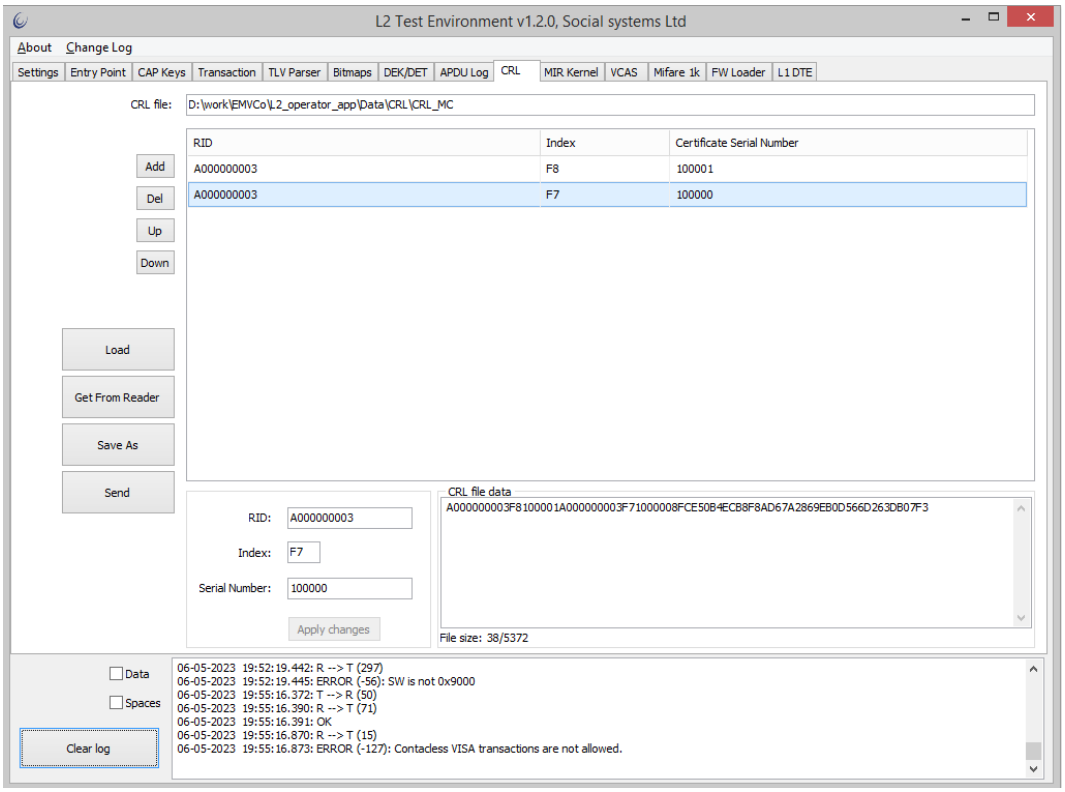

Рисунок 9 - Формирование и отправка ридеру списка отозванных сертификатов.

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

Ядро "Visa" 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).

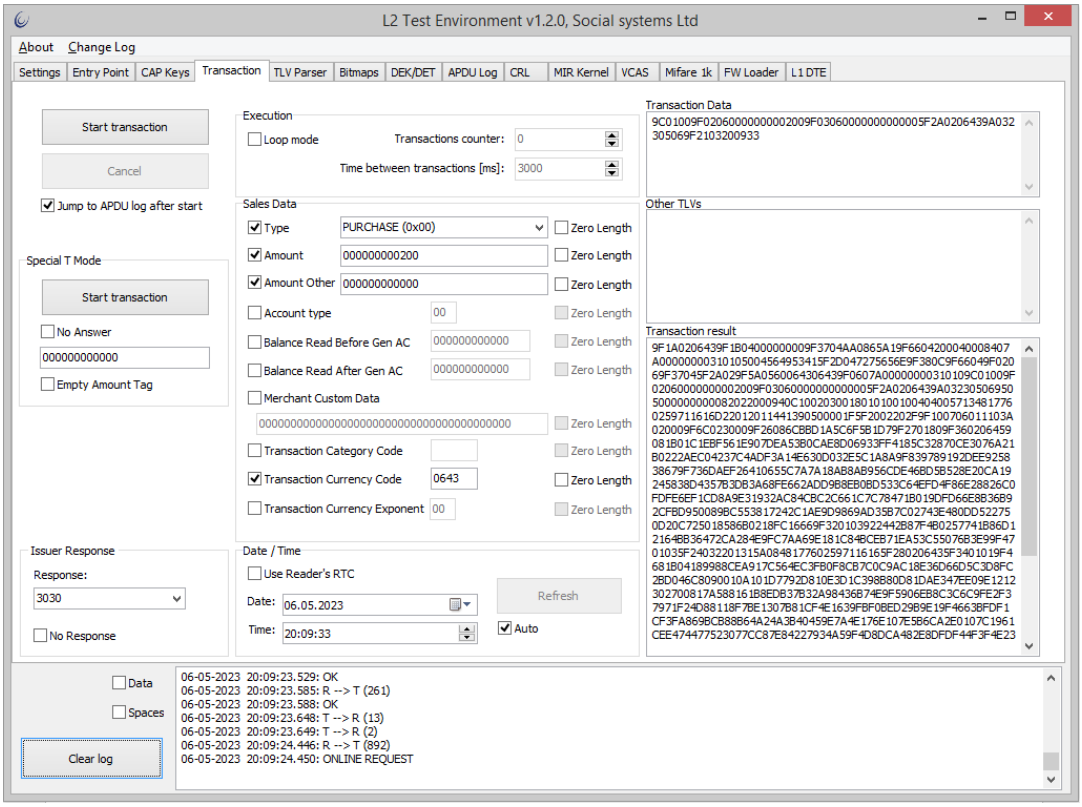

Рисунок 10 - Результат проведения транзакции (Online Request)

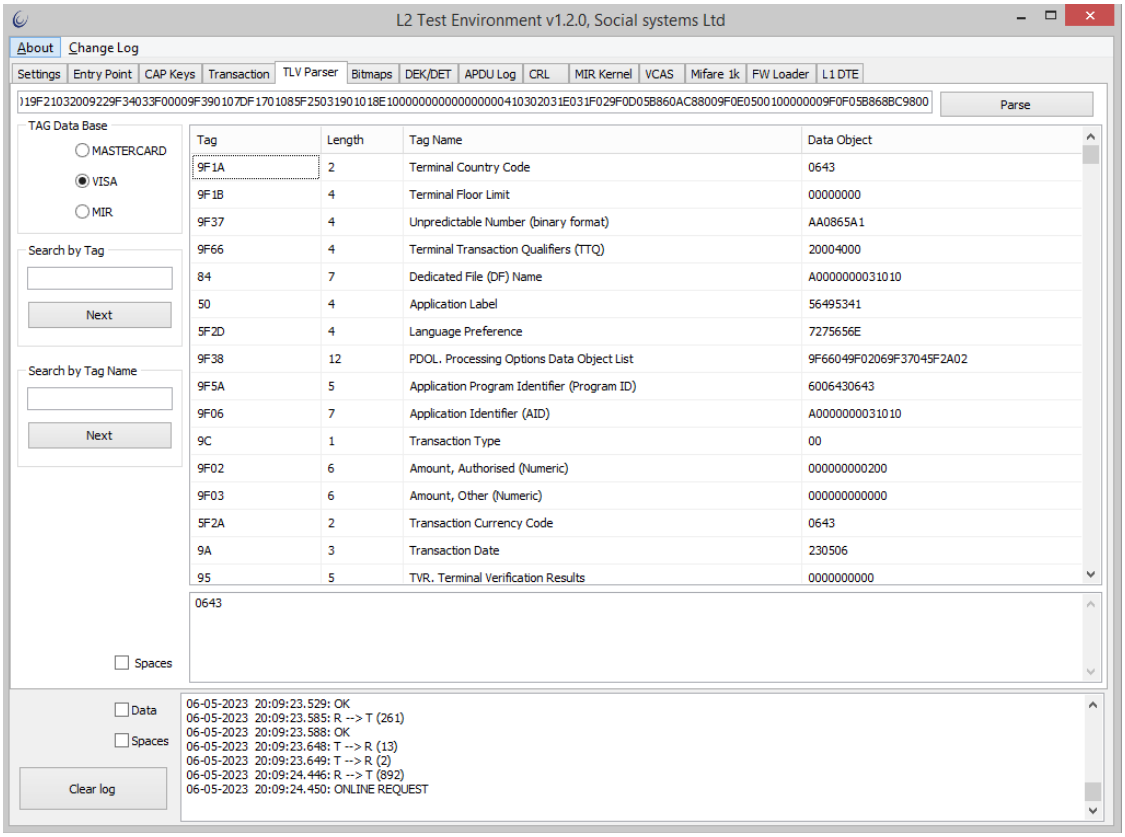

Рисунок 11 - Расшифровка тегов транзакции.

2.9. Аутентификация платёжного приложения

Ядро "Visa" поддерживает единственный метод аутентификации платёжного приложения: fDDA - Fast Dynamic Data Authentication - быстрый динамический метод аутентификации. По требованиям ПС "Visa" другие методы, такие как SDA и DDA, не поддерживаются.

Для аутентификации необходим лист CAPK, работа с которым рассмотрена в пункте 2.3 настоящего документа.