Программное обеспечение устройства работы с бесконтактными картами по спецификации EMV, Level 1 (L1)

Руководство по эксплуатации

Листов 16

Москва, 2023

Оглавление

Список сокращений

Сокращение	Расшифровка
ATTRIB	Attribute - команда активации 4-ой части протокола ISO/IEC 14443 (B)
ATQA	Answer to request - Ответ на команду WUPA
DTE	Device Test Environment - тестовое программное окружение для работы с командами L1
EMV	Europay + MasterCard + VISA – международный стандарт для операций по банковским картам с чипами
HLTA	Halt, Type A - команда перевода карты в состояние HALT
IEC	International Electrotechnical Commission - международная некоммерческая организация по стандартизации в области электрических, электронных и смежных технологий
ISO	International Organization for Standartization - международная организация по стандартизации
L1	Level 1 - абстрактный уровень разделения программного обеспечения по спецификации EMV - уровень управления модулем NFC и поддержка ISO/IEC 14443
L2	Level 2 - абстрактный уровень разделения программного обеспечения по спецификации EMV - уровень поддержки спецификаций различных платёжных систем
NFC	Near Field Communications - технология ближней бесконтактной связи
PB3P	Название протокола обмена с ридером BCAM-01
RATS	Request for Answer To Select - команда активации 4-ой части протокола ISO/IEC 14443 (A)
SELx	Select - команда выбора карты в цикле антиколлизии
TEI	Test Environment Interface - интерфейс тестового окружение - короткое название приложения "L2 Test Environment"
UID	Unique identifier - универсальный идентификатор карты
WUPA	Wake Up, Type A - команда начала работы с картой ISO/IEC 14443 (A) в поле антенны

WUPB	Wake Up, Type B - команда начала работы с картой ISO/IEC 14443 (B) в поле антенны
ПО	Программное обеспечение

Аннотация

Данный документ содержит описание эксплуатации функциональных возможностей программного обеспечения устройства работы с бесконтактными картами по спецификации EMV.

1. Общие сведения

Программное обеспечение устройства для работы с бесконтактными картами в стандарте EMV (далее ПО L1) соответствует спецификации бесконтактной оплаты в платёжных системах - "EMV Contactless Specification for Payment Systems", версии 2.6.

Для работы с ПО L1 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 ПО L1.

Для управления ридером по разработанному протоколу необходима реализация так называемого 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 ПО L1 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 ПО L1, 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 ПО L1, версии не ниже 1.0.0; устройство должно быть подключено к ПЭВМ по USB-кабелю;

- две банковские карты с бесконтактным интерфейсом (одна карта типа А и одна карта типа Б).

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).

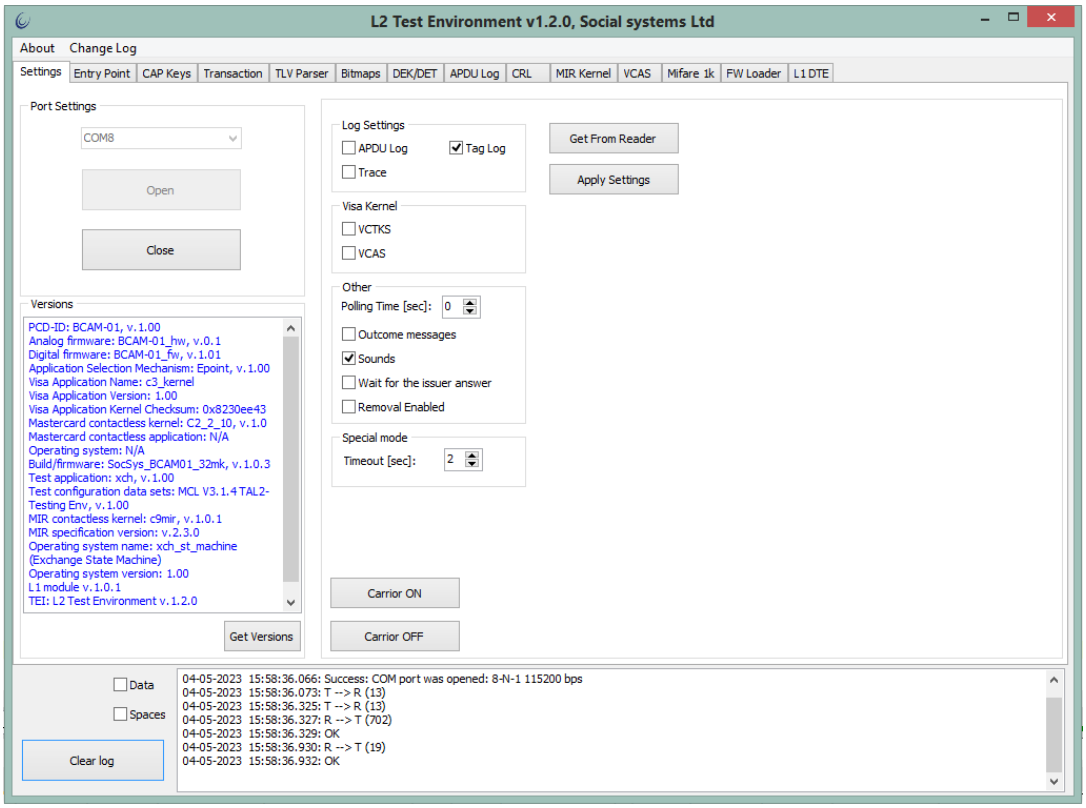

Рисунок 1 - Начало работы, открытие порта.

2. Эксплуатация функционала ПО L1

2.1. Управление модулем NFC

Для включения и отключения поля ридера в приложении TEI предусмотрены кнопки управления 'Carrior ON' и 'Carrior OFF' расположенные на вкладке 'L1 DTE' (рисунок 2). Для дальнейшей работы с ридером следует включить поле, нажав кнопку 'Carrior ON'.

Настройка NFC на работу по протоколу ISO14443A или ISO14443B происходит внутри модуля L1 автоматически при выборе команды обнаружения карты в поле: WUPA или WUPB, дополнительных манипуляций не требуется.

Для передачи карте команды WUPA следует внести карту типа A в поле действия антенны ридера, перейти на вкладку 'L1 DTE' приложения TEI и нажать кнопку 'WUPA'. При этом ридер вернёт приложению ответ карты ATQA (рисунок 2). Следует также отметить, что при отправке команды WUPA (или WUPB) при выключенном поле или с картой вне поля действия антенны, ридер вернёт ошибку '-3' (Timeout).

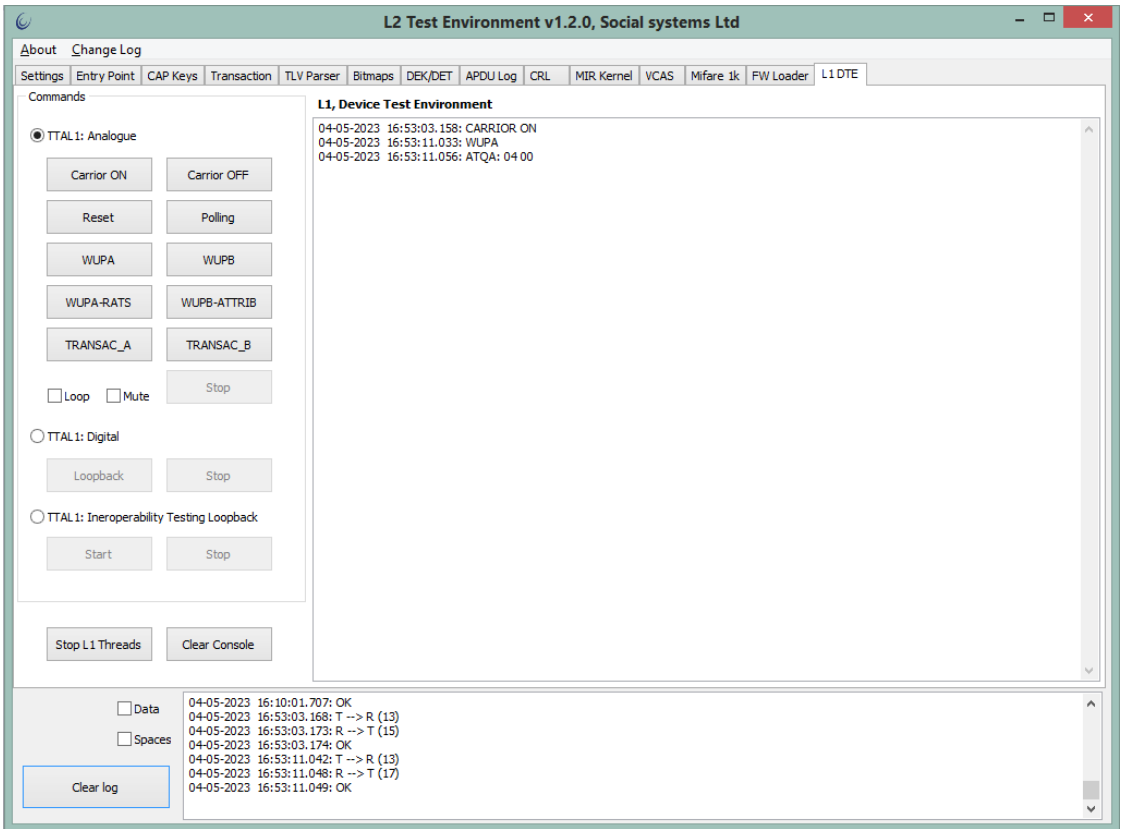

Рисунок 2 - Команды L1. Выполнение команды WUPA.

Для передачи карте команды WUPB следует внести карту типа B в поле действия антенны ридера, перейти на вкладку 'L1 DTE' приложения TEI и нажать кнопку 'WUPB'. При этом ридер вернёт приложению ответ карты ATQB (рисунок 3).

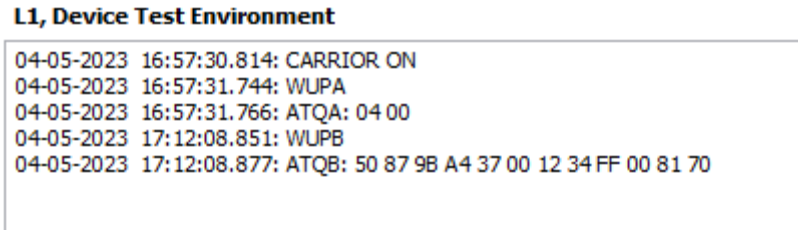

Рисунок 3 - Отображение результатов команд L1.

Активация четвёртой части стандарта ISO14443 для карт типа A обеспечивается командой RATS. После активации четвёртой части стандарта карта готова к обмену командами APDU с ядрами платёжных систем, логика такого обмена относится уже к уровню L2 и выходит за рамки ответственности модуля L1 ПО, однако технический уровень передачи данных (формирование I-block, R-block, S-block - в соответствии со стандартом, настройка скорости, деление команд на части в соответствии с возможностями карты и чипа NFC и так далее) лежит в зоне ответственности ПО L1.

Команды селекции карты SEL1, SEL2, SEL3, HLTA используются при работе с картами типа A для перемещения по графу состояний конечного автомата карты, описанного в стандарте ISO14443. Команды служат для выбора карты при выполнении процедуры антиколлизии.

Команда RATS - команда активации четвертой части стандарта ISO14443 - возможна только после успешного выполнения команд WUPA-SEL1-[SEL2-SEL3]. Для выполнения цепочки этих команд следует на вкладке 'L1 DTE' приложения TEI нажать на кнопку 'WUPA-RATS', при этом карта типа A должна находится в поле действия антенны ридера. Устройство в ответ на команду должно вернуть ATS как результат выполнения команды RATS, а также UID карты, ATQA, SAK, и контрольные суммы частей UID в зависимости от длины UID: BCC0, BCC1, BCC2 (рисунок 4).

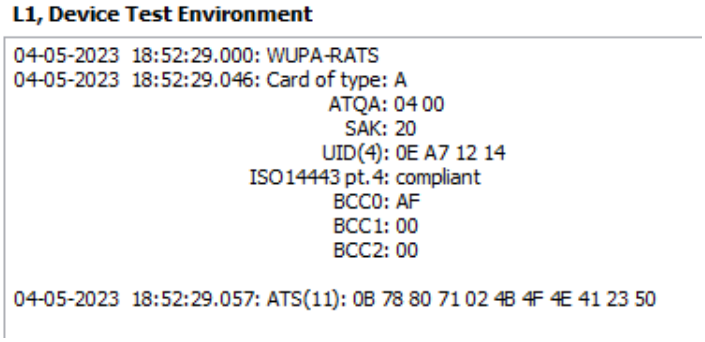

Рисунок 4 - Результат выполнения команды WUPA-RATS

Активация четвёртой части стандарта ISO14443 для карт типа Б осуществляется с помощью команды ATTRIB. Команды может выполняться только после успешного завершения команды WUPB. Чтобы выполнить последовательную цепочку этих

команд следует на вкладке 'L1 DTE' приложения TEI нажать на кнопку 'WUPB-ATTRIB', при этом карта типа Б должна находится в поле действия антенны ридера. В ответ на команду устройство должно вернуть ATQB - ответ карты (рисунок 5). В случае неудачного выполнения команды, например, карта не поддерживает ISO14443-4, ридер должен вернуть ошибку '-3' (Timeout).

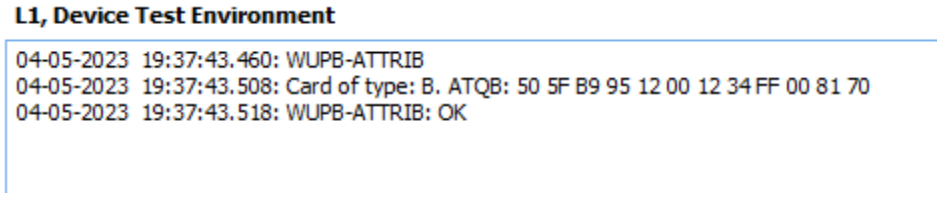

Рисунок 5 - Результат выполнения команды 'WUPB-ATTRIB'

2.2. Обмен данными с картой по стандарту ISO/IEC 14443

2.2.1 Обнаружение карты в поле действия антенны устройства (Polling)

ПО L1 осуществляет обнаружение в поле действия антенны устройства карт стандарта ISO/IEC 14443 типа А и типа Б по требованиям спецификации EMV. Для осуществления обнаружения карты в поле антенны с последующим циклом антиколлизии следует на вкладке 'L1 DTE' приложения TEI, отметить поле 'Loop' и нажать на кнопку 'Polling'. При отсутствии карты в поле действия антенны ридер постоянно будет выдавать ошибку таймаута (-3), при внесении в поле устройства карты типа А - ATQ, SAK, UID, BCC0, BCC1, BCC2, а при внесении карты В - ATQB (рисунок 6).

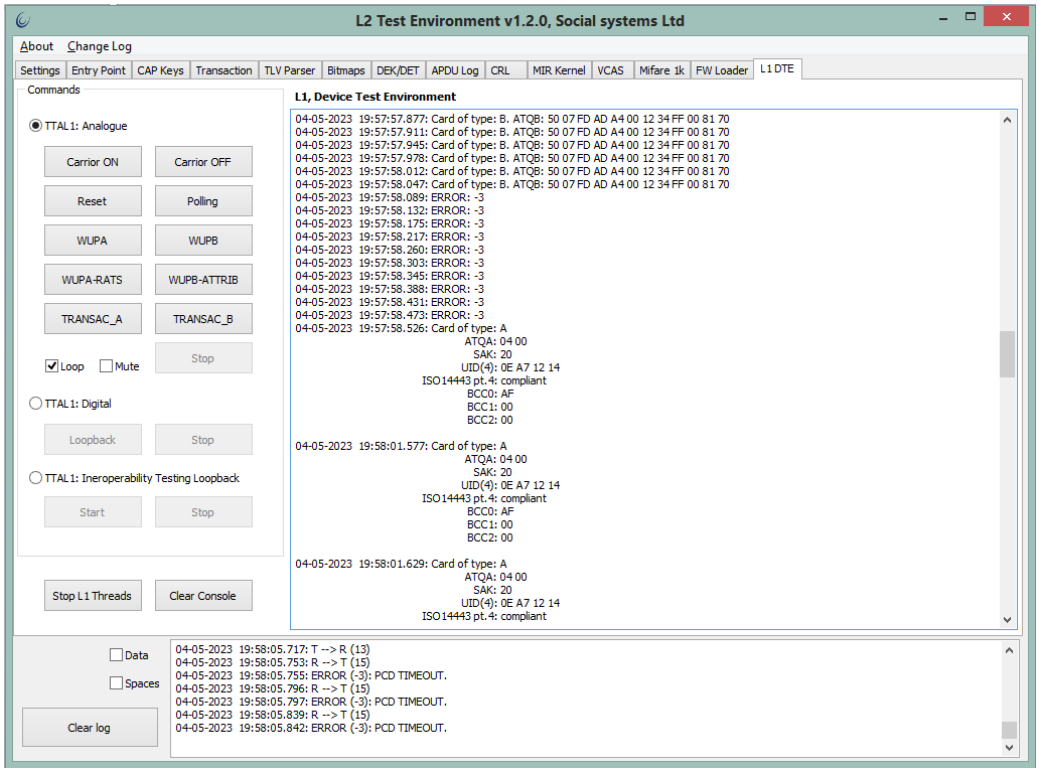

Рисунок 6 - Результат выполнения команды 'Polling' при поочерёдном внесении карты типа Б и карты типа А в поле действия антенны ридера.

2.2.2 Антиколлизия (Anticollision)

Реализованный в ПО L1 по спецификации EMV метод антиколлизии позволяет обнаруживать коллизию в следующих случаях:

- при нахождении в поле действия антенны двух и более карт одного типа (либо А, либо Б);

- при нахождении в поле действия антенны двух и более карт разных типов (и тип А, и тип Б).

При обнаружении коллизии ридер возвращает ошибку '-5' (Collision). Чтобы проверить, как это происходит на практике достаточно при выполнении команды 'Polling' внести в поле действия антенны обе карты: типа А и типа Б (рисунок 7).

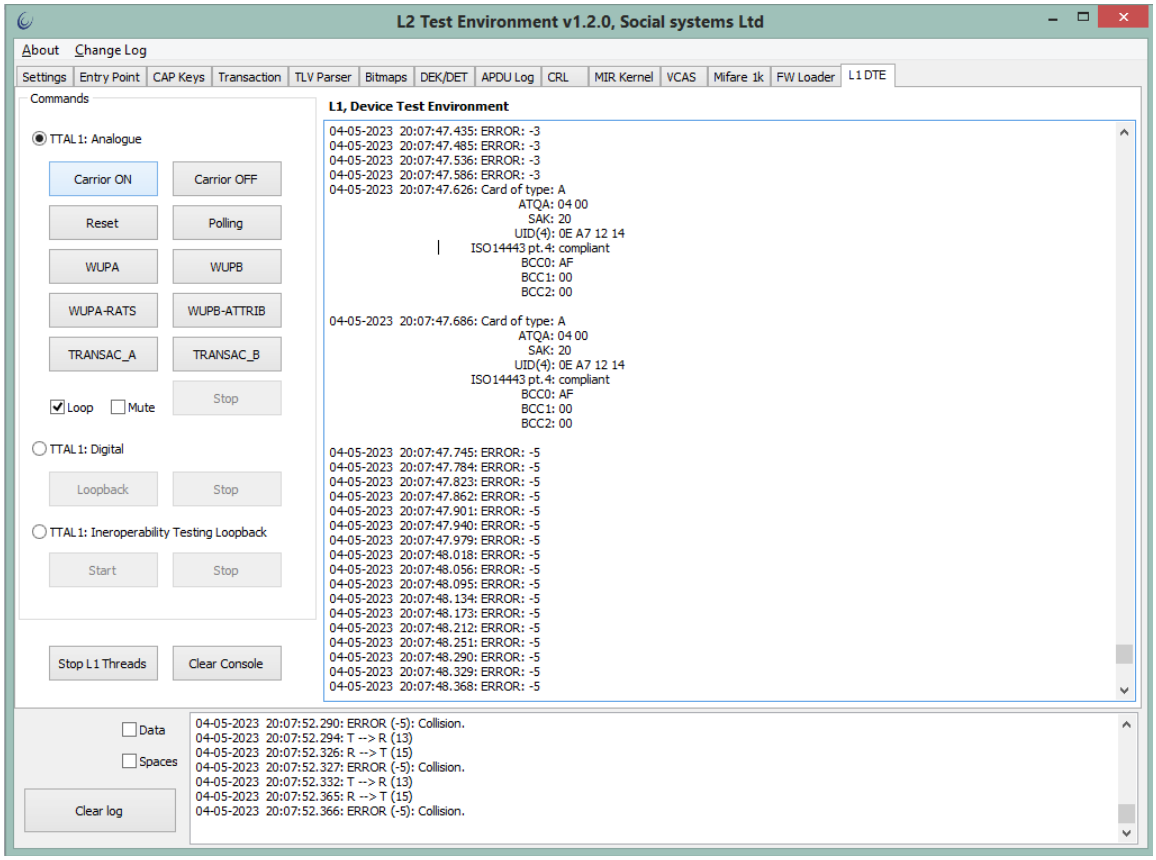

Рисунок 7 - Результат выполнения операции 'Polling' с одновременном нахождением в поле действия антенны двух карт: типа А и типа Б, при этом в консоли видно, что в начальный момент в поле антенны не было карт (-3), потом при внесении в поле двух карт первой успела определиться и начать отвечать карта типа А, а когда это сделала и карта типа Б, ридер распознал коллизию и вернул ошибку (-5).

2.2.3 Передача данных

ПО L1 в рамках стандарта ISO/IEC 14443 и по требованиям спецификации EMV поддерживает блочный протокол передачи данных - T1, также поддерживается "сцепление" (chaining) блоков одной передачи внутри протокола T1.

Полученные данные от карты сохраняются до следующей сессии обмена с картой.

Косвенно работы ПО L1 можно увидеть, выполнив ряд операций в TEI. На вкладке 'Settings' отметить поле 'APDU Log', значение 'Polling Time' установить 10 секунд, нажать на кнопку 'Apply Settings' (рисунок 8). Перейти на вкладку 'Transaction', установить значение 'Amount' равным 100, отметить поле 'Jump to APDU log after start', нажать кнопку 'Start transaction' (рисунок 9). Внести банковскую карту в поле действия антенны. После нажатия на 'Start transaction' приложение 12

переключится на вкладку 'APDU Log' в которой можно пронаблюдать обмен APDU-командами между ридером и картой. Каждая пара команд CAPDU-RAPDU - есть результат работы ПО L1 (рисунок 10). При этом в логе не отображается разбиение команд на части (chaining) и также не отображаются служебные блоки данных S-block и R-block по стандарту ISO14443-4.

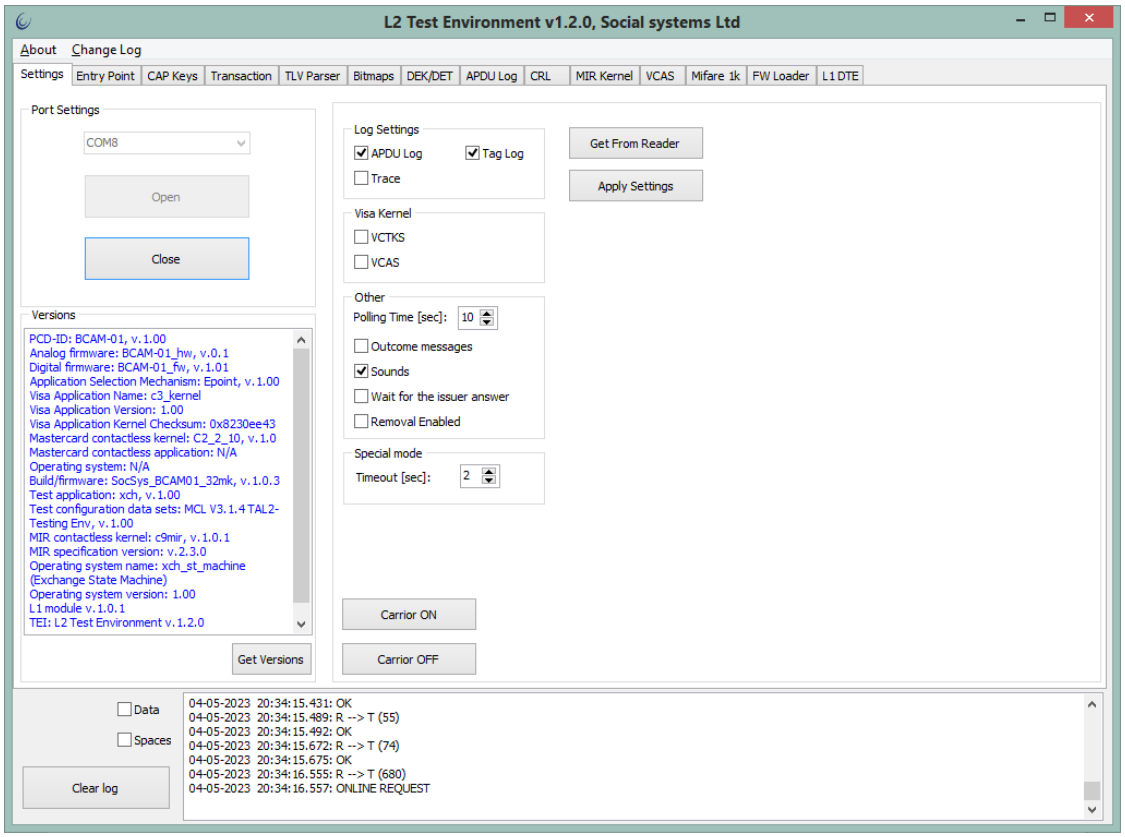

Рисунок 8 - Включение отображения лога обмена и установка времени поиска карты в поле ридера.

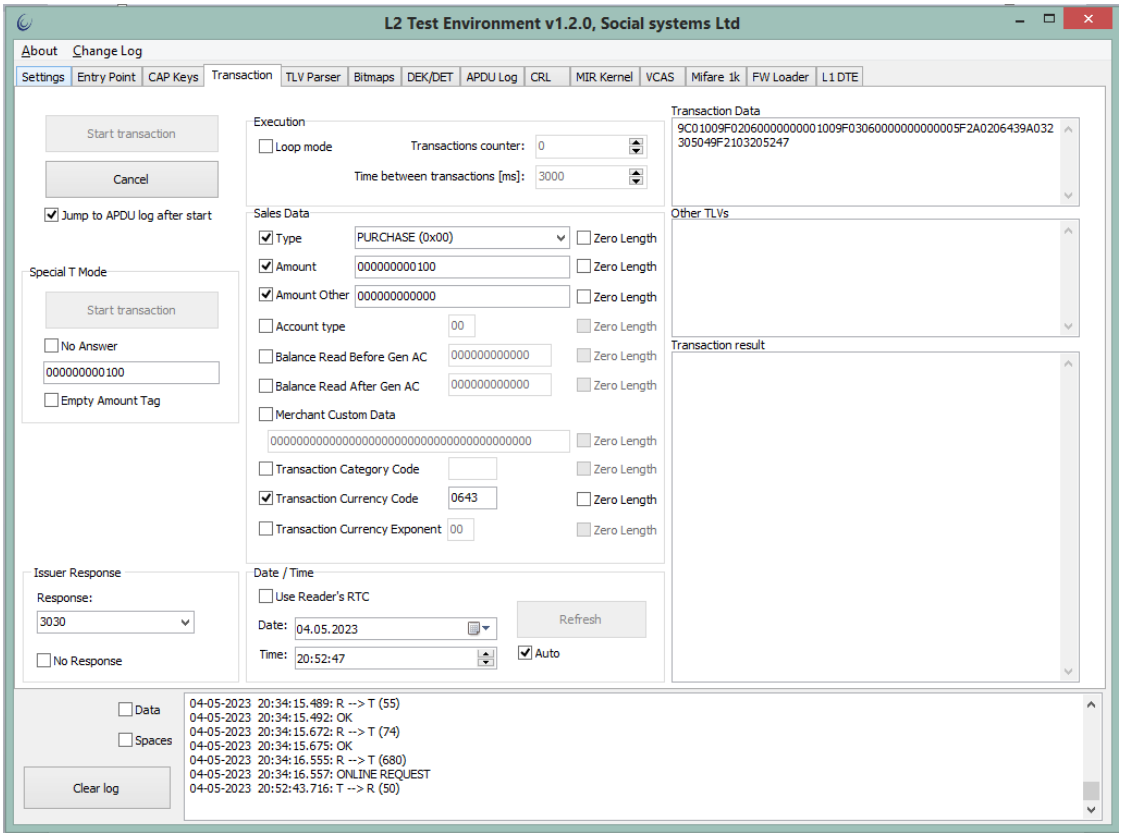

Рисунок 9 - Установка параметров транзакции

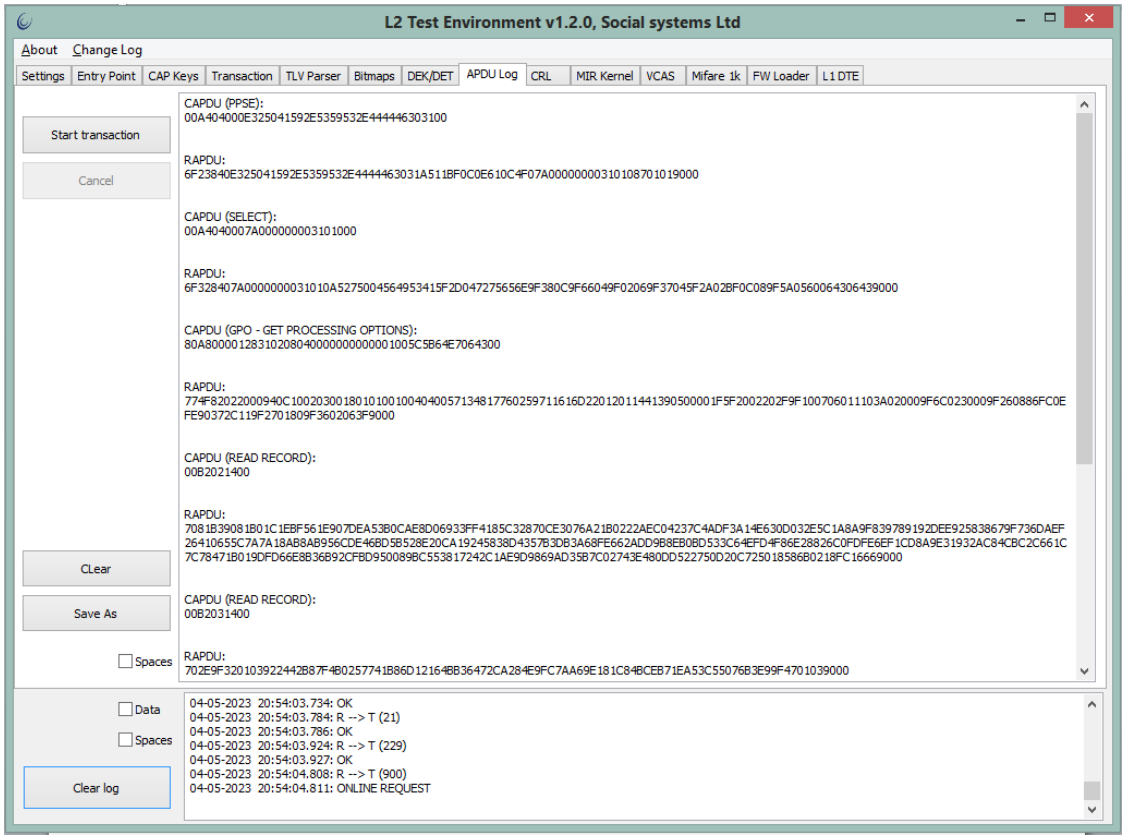

Рисунок 10 - Результат обмена данными между ридером и картой

2.2.4 Процедура сброса (Reset)

По требованию спецификации EMV в конце работы с картой необходима процедура сброса. Процедура заключается в отключении поля антенны и включения его через указанный интервал времени, который может варьироваться от пяти до десяти миллисекунд. В ПО L1 реализована процедура сброса, интервал отключения поля составляет семь миллисекунд.

Продемонстрировать работу Reset можно следующим образом. После активации карты в четвёртой части протокола карта игнорирует команды WUPA, если это карта типа А, и WUPB, если это карта типа Б. На вкладке 'L1 DTE' приложения TEI следует нажать кнопку 'WUPA-RATS' при этом карта типа А должна находиться в поле действия антенны, ридер вернёт данные, как это описано в пункте 2.1. настоящего документа, после чего, не извлекая карту из поля действия антенны, выполнить команду 'WUPA', в этот раз ридер вернёт ошибку '-3' (Timeout): карта игнорирует команду. Нажать кнопку 'Reset' на той же вкладке 'L1 DTE', дождаться ответа ридера и снова попробовать выполнить либо команду 'WUPA', либо команду 'WUPA-RATS', в этом случае ридер вернёт ответ карты на команду (рисунок 11).

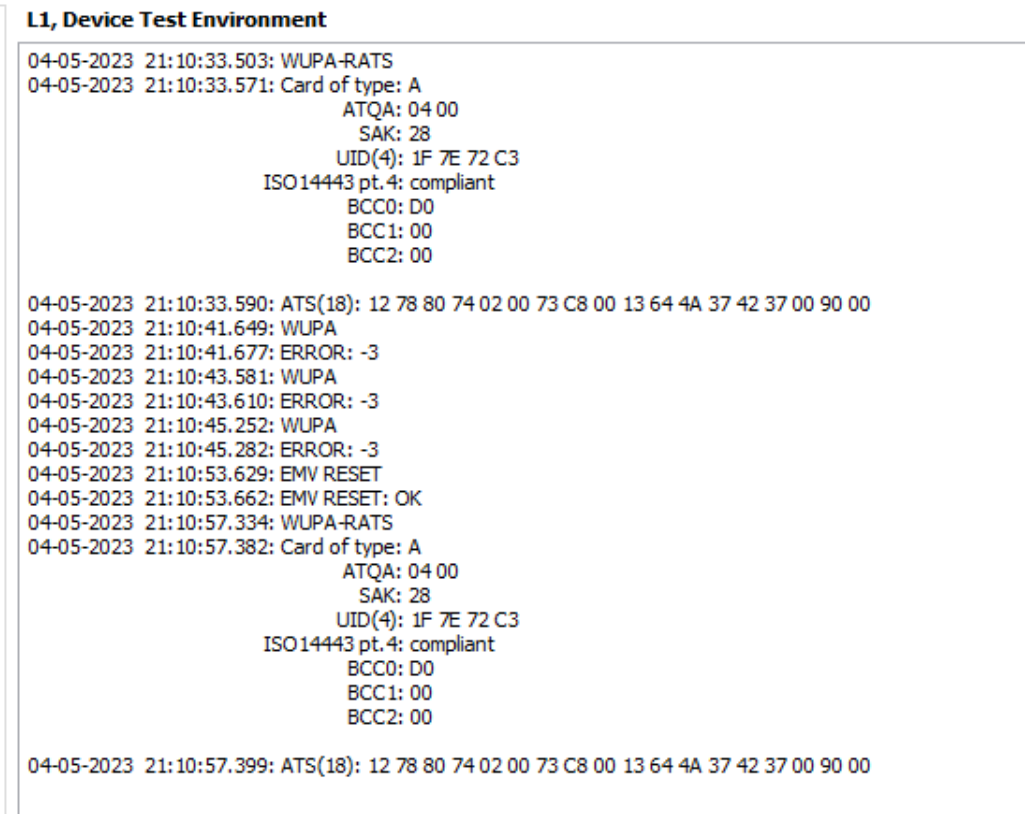

Рисунок 11 - Результат работы команды RESET.

2.2.5 Процедура удаления карты (Removal)

В ряде случаев ядру платёжной системы необходимо убедиться в процессе работы, что карта покинула поле антенны.

В ПО L1 реализована процедура удаления карты из поля действия антенны. Процедура выполняет сброс (п.2.2.4), затем, в цикле осуществляет обнаружение карты в поле. Пока карта в поле, процедура не завершается.

Для включения этого функционала на вкладке 'Settings' приложения TEI предусмотрено поле 'Removal Enabled', требуется отметить его и нажать кнопку 'Apply Settings' на той же вкладке. Далее повторить действия из пункта 2.2.3. При таких настройках транзакция не завершится пока карта будет находиться в поле действия антенны. Завершить транзакцию можно, убрав карту из поля ридера.