УДК 004.428.4

ИСПОЛНЕНИЕ И АВТОРИЗАЦИЯ EMV-ТРАНЗАКЦИЙ

Ермаков К.С., Сидякин И.М.

ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)», Москва,
e-mail: cosmozz@yandex.ru, ivan.sidyakin@bmstu.ru

В статье рассматривается практическая реализация стандарта EMV, разработанного для микропроцессорных карт, которые являются важной частью современной инфраструктуры электронных платежей. Приводятся основные положения стандарта EMV, определяющие информационное взаимодействие между банковской картой и платежным терминалом, необходимое для исполнения финансовых операций. Представлена общая архитектура системы электронных платежей. В статье подробно описан цикл EMV-транзакции, исполняемый при совершении платежной операции. Рассмотрены отдельные этапы обработки транзакции, включая выбор приложения, верификацию владельца карты, проверку подлинности данных карты, онлайн- и офлайн-авторизацию. Приведены некоторые особенности обработки операций приложениями разных платежных систем, описан процесс аутентификации EMV-карт, приведено сравнение способов авторизации транзакций оплаты картой с магнитной полосой и смарт-чипом. Рассмотрены элементы интерфейса EMV-приложения, установленного на карте. Приведены форматы команд и ответов, пересылаемых между картой и терминалом в процессе исполнения транзакций. Практическим результатом работы является разработанное и протестированное на соответствие требованиям стандарта EMV-приложение для платежного терминала. Проведенное функциональное тестирование включает более 1,5 тыс. тестов, собранных в плане тестирования контактного интерфейса EMV.

Ключевые слова: EMV, смарт-карты, платежные карты, платежное приложение, транзакция

EMV-TRANSACTION PROCESSING AND AUTHORIZATION

Ermakov K.S., Sidyakin I.M.

Bauman Moscow State Technical University (National Research University), Москва,
e-mail: cosmozz@yandex.ru, ivan.sidyakin@bmstu.ru

The article discusses the practical implementation of the EMV-standard developed for microprocessor cards, which are an important part of the modern electronic payment infrastructure. Basic statements of the EMV-standard are given, which determine the information interaction between a bank card and a Point-of-Sale terminal required for the execution of financial transactions. The general architecture of the electronic payment system is presented. The article describes in detail the EMV-transaction process. The individual steps of transaction processing are considered, including application selection, cardholder verification, card data authentication, online and offline authorization. Some proprietary features of the transaction processing introduced by different payment systems are discussed. The process of authentication of EMV-cards is described and comparison of methods for authorizing payment transactions with a magnetic stripe data and a smart chip data is given as well. The interface of the smart-card EMV-application are depicted. The data formats of application data unit and corresponding response used for data exchange between the card and the terminal applications are given. The practical result of the work is the software application designed for the payment terminal developed and tested for compliance with the requirements of the EMV-standard. The functional testing carried out includes more than one and a half thousand tests declared in the EMV-contact interface test plan.

Keywords: EMV, smart-card, payment cards, payment applications, transaction

За последнее десятилетие платежные карты прошли два важных этапа развития. Контактные карты, разработанные по стандартам EMV, сменили карты с магнитной полосой. В настоящее время идет процесс замены контактных карт на бесконтактные средства оплаты, к которым кроме карт относятся мобильные телефоны и другие электронные устройства. По состоянию на начало 2022 г. большинство дебетовых и кредитных карт используют стандарт EMV [1], но при этом имеют магнитную полосу для совместимости со старым терминальным оборудованием.

Требования безопасности являются ключевым фактором смены технологий. Контактная карта EMV имеет существенно более высокую степень защищенности, чем карта с магнитной полосой. Стандарты EMV включают надежные способы аутентификации данных карты и защиты от копирования.

Стандарт EMV – это совместная разработка международных платежных систем VISA Inc и MasterCard Worldwide. Контактные карты EMV разных платежных систем в целом соответствуют этому стандарту, но могут иметь некоторые особенности реализации, не входящие в противоречие с требованиями спецификации.

Целью исследования является разработка и подготовка к сертификационному тестированию программного модуля ядра EMV Level 2, входящего в состав программного обеспечения платежного терминала.

Материалы и методы исследования

Для достижения поставленной цели использовались различные методы исследования, включая теоретический анализ спецификаций EMV и сравнительный анализ реализаций EMV-приложений различных платежных систем. Материалом исследования является опубликованная в открытом доступе документация EMVCO [1], а также несколько стандартов, применяемых в области электронных платежей.

Авторизация EMV-транзакции

Авторизация транзакции по карте – это процесс проверки данных карты и принятия решения об отказе или одобрении транзакции, которое принимается совместно несколькими участниками системы электронных платежей. В процессе исполнения банковской транзакции задействованы:

− платежная система;

− банк-эмитент – банк, который выпустил платежную карту и обслуживает связанный с ней счет;

− банк-эквайер – банк, который управляет платежным терминалом торговой точки или транспортным терминалом;

− платежный терминал – устройство, которое обеспечивает работу с платежной картой.

Архитектура системы электронных платежей показана на рис. 1.

Рис. 1. Архитектура системы электронных платежей

Микропроцессорная карта стандарта EMV – это программно-аппаратный комплекс, в состав которого входят:

− процессор;

− оперативная память;

− подсистема хранения данных;

− операционная система.

В смарт-карте должно быть установлено платежное EMV-приложение. Требования к этому приложению указаны в серии стандартов EMV Level 2. Общие требования к интерфейсу между терминалом и EMV-приложением карты приводятся в [2]. Вопросы безопасности, включая проверку подлинности данных карты, рассмотрены в [3]. Требования к алгоритму исполнения транзакции указаны в [4]. Требования к интерфейсам с держателем карты, продавцом и эквайером перечислены в [5].

Интерфейс EMV-приложения

Интерфейс приложения включает набор APDU (Application Protocol Data Unit) команд, используемых для проведения транзакций и управления EMV-приложением.

Последовательность команд и APDU определяет протокол обмена между картой и устройствами чтения карт в составе Point-of-Sale (POS) терминалов, банкоматов и пр. Устройство передает карте команду APDU-C, а карта возвращает ответ APDU-R. Инициатором обмена всегда является устройство чтения. Структура команды APDU-C [6] приведена в табл. 1.

Таблица 1

Формат APDU-C

Элемент	Размер (байт)	Описание
Заголовок		
CLA	1	Класс команды
INS	1	Код инструкции
P1	1	Параметр № 1
P2	1	Параметр № 2
Тело команды		
Lc	1	Длина отправляемых данных
Data	Lc	Данные
Le	1	Длина ожидаемого ответа

Ответ APDU-R состоит из заголовка, тела сообщения и трейлера с байтами статуса Status Word 1 (SW1) и Status Word 2 (SW2). Байты статуса составляют код, по которому определяется результат обмена. Структура команды APDU-R [6] приведена в табл. 2.

Байт SW1 содержит основную информацию, а SW2 дополнительную. В табл. 3 приведены примеры кодов статуса.

Для исполнения операции «оплата» по карте платежный терминал запускает цикл EMV-транзакции, который включает обмен APDU командами и ответами на них в заданной последовательности, а также

проверку подлинности данных карты и некоторые другие действия, описание которых приводится ниже.

Таблица 2

Формат APDU-R

Элемент	Размер (байт)	Описание
Заголовок		
Data	Le	Данные
Трейлер		
SW1	1	Слово статуса 1
SW2	1	Слово статуса 2

Таблица 3

Примеры комбинаций SW1SW2

SW1SW2	Значение
9000	Ок
66XX	Команда не была исполнена по причинам безопасности
6700	Неправильная длина команды
6E00	Неизвестный CLA

EMV-транзакция выполняется в несколько этапов. Транзакция начинается с того, что карта возвращает двоичный блок данных Answer to reset, ATR, подтверждая готовность к дальнейшему обмену данными.

Затем производится выбор платежного приложения. Карта и терминал совместно выбирают приложение, которое будет использовано для проведения операции. В настройках терминала указывается список поддерживаемых EMV-приложений. Кроме приложений EMV, включая приложения НСПК МИР, Visa International VSDC, MasterCard International M/Chip, на карте могут присутствовать программы лояльности, бонусные или идентификационные приложения, которые используют собственные, отличные от EMV, стандарты. В специально выделенной области памяти карты размещен список всех установленных в карте приложений.

Существует два метода построения списка приложений: Payment System Environment, PSE и Payment System Application, PSA [2]. Большинство современных смарт-карт поддерживают оба этих метода.

Метод PSE основан на данных каталога приложений, который считывается с карты первой командой APDU-C SELECT. Заданное в спецификации имя каталога передается в параметрах этой команды. В случае, если каталог PSE присутствует, карта возвращает статус SW1/SW2 = 9000 (OK) и параметры, необходимые для выбора приложения. Терминал выбирает одно из приложений каталога и запускает его с помощью команды SELECT.

Метод PSA для поиска приложения использует идентификатор Application Identifier, AID. Идентификатор AID состоит из двух частей:

− Registered Application Provider Identifier, RID – зарегистрированный идентификатор провайдера приложения. RID – это уникальный идентификатор платежной системы или другого эмитента, выпустившего данный карточный продукт.

− Proprietary Application Identifier Extension, PIX – частный идентификатор приложения или бизнес-код карточного продукта.

Данные карты хранятся в формате DER [7]. Номера тегов всех параметров карты указаны в спецификациях EMV Level 2.

Идентификатор AID в карте хранится в теге 4F или 84. В конфигурации терминала имеется список идентификаторов AID всех поддерживаемых терминалом приложений. Терминал последовательно отправляет карте команды SELECT с разными идентификаторами AID из своего списка. Если приложение с указанным в команде AID имеется в карте, карта возвращает код статуса SW12 = 9000 и переходит к исполнению приложения. Иначе карта возвращает ошибку «файл не найден» в поле статуса SW12 = 6A82 и терминал переходит к следующему идентификатору. Если в конфигурации устройства отсутствует AID приложения карты, транзакция завершается с ошибкой.

Команда выбора приложения SELECT запускает приложение карты и возвращает информацию об этом приложении. Различные платежные системы используют для передачи информации о приложении как общие теги, так и собственные частные теги и форматы. Например, Mastercard указывает региональную принадлежность карты в теге Third Party Data, а Visa – в теге Application Program. Эти теги несут сходную информацию, но имеют разный формат.

Карты многих платежных систем в ответе на команду SELECT возвращают тег Processing Options Data Object List, PDOL, содержащий список параметров, которые терминал должен передать карте для продолжения обработки транзакции. В списке указывается номер тега каждого параметра и ожидаемая длина данных. Например:

− PDOL Amex 9F3501 запрашивает тип терминала.

− PDOL Visa 9F66049F02069F37045F2A-029F1A02 запрашивает сумму операции, валюту, код страны терминала и некоторые другие элементы.

– PDOL. МИР 9F7A015F2A029F02069F 35019F40059F1A029F3303, запрашивает подробную информацию о терминале, его возможностях и местонахождении.

Терминал в параметрах команды Get Processing Options, GPO, должен передать всю запрошенную картой информацию, иначе транзакция будет прервана.

На следующем шаге цикла транзакции терминал выполняет проверку держателя карты. Если сумма транзакции не превышает заданный в настройках терминала предел, то разрешается провести операцию без проверки. Если сумма превышает предел, то также, в зависимости от настроек карты, выбирается один из методов проверки держателя карты. Для пластиковых карт обычно проверка держателя карты производится с помощью онлайн- или офлайн-проверки ПИН-кода.

Эмитент карты может делегировать проверку ПИН-кода платежному приложению карты. Значение ПИН-кода, введенное пользователем на терминальном устройстве, сравнивается с образцом, безопасно хранящимся в карте. Этот метод называется офлайн-проверкой ПИН-кода.

Для онлайн-проверки ПИН-код шифруется в терминале и передается на проверку к эмитенту.

После окончания проверки держателя карты выполняется проверка ограничений, накладываемых на использование карты, например:

– проверка срока действия карты,

– проверка лимитов по списаниям,

– проверка совместимости приложения и терминала,

– проверка кода банка-эмитента.

По результатам этих проверок принимается одно из трех возможных решений о завершении операции:

– отклонение операции в режиме офлайн;

– отправка запроса на онлайн-авторизацию;

– одобрение операции в режиме офлайн.

Режим офлайн означает принятие решения терминалом без участия банка. Режим онлайн означает принятие решения терминалом совместно с банком.

Аутентификация карты – это обязательный шаг цикла транзакции. Аутентификация подтверждает достоверность данных, считанных с карты, а также то, что банк – эмитент карты авторизирован платежной системой, выпустившей приложение карты.

Для аутентификации карты с магнитной полосой используются статические данные. Данные магнитной полосы каждый раз при авторизации карты передаются в банк-эмитент. Платежный терминал не имеет возможности проверить достоверность данных магнитной полосы самостоятельно, без участия банка. Банк-эмитент не может отличить карту от ее полной копии, поэтому имеется высокая вероятность проведения мошеннических операций копиями таких карт. Схема авторизации транзакции картой с магнитной полосой показана на рис. 2.

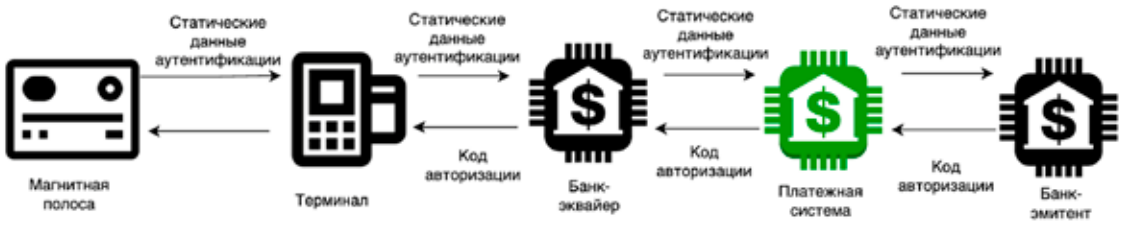

Рис. 2. Схема авторизации транзакции картой с магнитной полосой

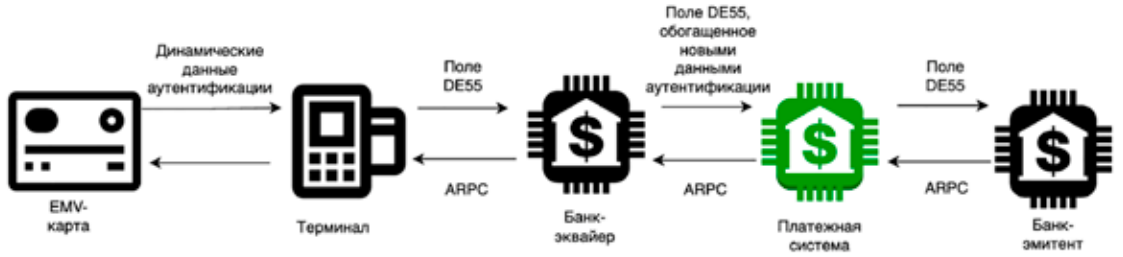

Рис. 3. Схема авторизации EMV-транзакции

EMV-карты для повышения уровня безопасности используют динамически вычисляемую цифровую подпись статических данных карты и динамических данных транзакции, которые передаются банку-эмитенту и подтверждают достоверность данных. Значение цифровой подписи уникально для каждой EMV-транзакции, поэтому транзакцию нельзя повторить, отправив банку копию перехваченной транзакции. Карта хранит в зашифрованном виде криптографический ключ, использующийся для вычисления цифровой подписи. Этот ключ недоступен для чтения. Изготовление копии карты без информации о ключе невозможно.

На рис. 3 показана процедура авторизации EMV-транзакции.

Транзакция начинается, когда контактная карта вставляется в слот устройства чтения или бесконтактная карта обнаруживается в поле терминала. Терминал передает карте данные транзакции, включая сумму, код валюты, код страны и прочее. Затем карта и терминал производят проверку рисков транзакции. Если проверка завершается успешно, карта возвращает терминалу данные транзакции и их цифровую подпись, которая называется криптограмма, а терминал, используя полученные от карты данные, создает и отправляет банку-эквайеру сообщение авторизации. Банк-эквайер передает сообщение банку-эмитенту.

Банк-эмитент проверяет подлинность криптограммы, которая вычисляется по динамическим данным текущей транзакции. Одновременно эта проверка позволяет удостовериться в подлинности карты.

Приведенное выше упрощенное описание цикла EMV-транзакции раскрывает главный аспект, обеспечивающий безопасность финансовых операций по карте – использование для аутентификации карты динамических данных.

EMV-карты добавляют важный функционал, который может использовать банк-эмитент, включая:

− проверку достоверности данных карты;

− идентификацию каждой транзакции;

− взаимную аутентификацию банка и карты. Банк возвращает собственную криптограмму терминалу в ответе на запрос авторизации;

− изменение данных карты после авторизации. Банк, например, может заблокировать карту или изменить предельные суммы операций.

Заключение

В статье приводится описание основных функций приложения, разработанного авторами в соответствии с требованиями стандарта EMV и предназначенного для использования в составе программного обеспечения платежного терминала. Рассмотрены основные этапы цикла исполнения платежной транзакции. Приведена схема авторизации платежной транзакции, а также интерфейс с EMV-приложением, установленным на смарт-карте. Выполнено функциональное тестирование приложения в соответствии с планом тестирования EMV [8], который содержит более 1,5 тыс. тестов.

Список литературы

1. EMVCO. [Электронный ресурс]. URL: https://www.emvco.com/ (дата обращения: 24.10. 2022).

2. EMVCO. EMV Integrated Circuit Card Specifications for Payment Systems Book 1 Application Independent ICC to Terminal Interface Requirements. Version 4.4. 2022. 81 с.

3. EMVCO. EMV Integrated Circuit Card Specifications for Payment Systems Book 2. Security and Key Management. Version 4.4. 2022. 192 с.

4. EMVCO. EMV Integrated Circuit Card Specifications for Payment Systems. Book 3. Version 4.4. 2022. 230 с.

5. EMVCO. EMV Integrated Circuit Card Specifications for Payment Systems Book 4 Cardholder, Attendant, and Acquirer Interface Requirements. Version 4.4. 2022. 133 с.

6. ISO/IEC 7816-4:2020. Identification cards — Integrated circuit cards, 2020. 176 с.

7. ISO X.690 Series X: Data networks and open system communications OSI networking and system aspects – abstract syntax notation one (ASN.1). Information technology – ASN.1 encoding rules: specification of basic encoding rules (BER), canonical encoding rules (CER) and distinguished encoding rules (DER). 2003. 39 с.

8. EMVCO. Terminal Type Approval Level 2 Test Cases. Version 43k. 2021. 1808 с.