ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

СКАНТЕК

Жизненный цикл платежного аплета PayCORN

Версия 18.10

Сентябрь 2015

СКАНТЕК

Приложения на Java-карте

© СКАНТЕК, 2016

Россия, 119049, г. Москва, Донская ул., д. 15

Телефон: (499) 271-9661 • e-mail: 2b@scantech.ru

Содержание

1

Основные понятия

Жизненный цикл аплетов, загружаемых на карту, значительно отличается от привычного жизненного цикла приложений для компьютеров. При установке аплета создаются все его объекты и аплет регистрируется операционной системой карты как одно из приложений карты (на карте может быть несколько приложений). Каждый зарегистрированный аплет имеет собственный AID (Application Identifier), который используется для дальнейшего общения с приложением. Все объекты аплета создаются в постоянной памяти. Есть несколько особенностей применения аплетов, загружаемых на карту, на которые стоит обратить внимание.

Во-первых, в отличие от традиционных компьютерных программ, состояние приложений на карте является постоянным и не теряется даже при выключении карты. Это не означает, что на карте совсем нет памяти, которая изменяет своё состояние при выключении питания (удалении карты из устройства чтения). Такая память есть, но она очень ограничена по объему и используется для хранения промежуточных данных сеанса работы с картой (например, сессионных ключей, входных данных и т. п.).

Во-вторых, после загрузки и персонализации аплета дальнейшие технологические действия с ним невозможны. Можно сказать, что аплет – это такой объект, который не поддается никаким воздействиям ни со стороны других приложений на карте, ни со стороны операционной системы карты. Прежде всего, это связано с безопасностью и определяется спецификациями Java Card (например, см. документы серии *Java Card Platform, Version 2.2.2*). В соответствии с этими спецификациями аплеты являются полностью независимыми элементами обработки данных, которые инкапсулируют все данные и методы их обработки, и не подвержены никаким воздействиям за счет использования брандмауэров между аплетами, а также брандмауэра между операционной системой и аплетами. Справедливости ради нужно сказать, что существует механизм разделяемых интерфейсов, когда какое-то приложение предоставляет другим возможность использования своих объектов и методов работы с ними, но эта специфическая возможность используется только в том

случае, когда какие-то данные разделяются между несколькими приложениями (что в большинстве практических случаев не требуется).

В третьих, получение каких-то отладочных данных или протоколов функционирования аплета обычно никогда не применяется. Это напрямую не связано с безопасностью и может быть реализовано, но включение данных процедур в аплет требует большого количества памяти, о она на картах ограничена. Стоимость карт очень сильно зависит от объема памяти на карте, поэтому процесс отладки и сопровождения аплетов никогда не переносится на этап их эмиссии (слишком это будет дорого стоить для эмитента).

В связи с вышеизложенным, наверное лучше говорить не о жизненном цикле аплета, а о жизненном цикле карты, а также методах разработки и тестирования аплета. Хотя эмитент может заблокировать и платежное приложение, а не всю карту. Этот процесс также описан ниже.

2

Жизненный цикл аплета и карты

Индустрия производства карт – это сложный, многоэтапный процесс, в который вовлечено большое количество организаций. Этот процесс сложен ещё и потому, что на различных этапах организации, вовлеченные в процесс, обмениваются между собой секретными ключами обеспечения безопасности эмиссии карт.

Далее объясняются некоторые общие положения из индустрии производства карт. Жизненный цикл карты принято делить на пять основных фаз:

- фаза производства микросхемы
- фаза пред-персонализации карты и загрузки на неё аплета PayCORN
- фаза персонализации карты
- фаза использования карты
- фаза блокировки карты

Деление на фазы позволяет контролировать безопасность карты на разных этапах её существования и обеспечивает распределение ответственности между всеми участниками процессов производства, персонализации и использования карт.

Хотя первые две фазы и выпадают из рассмотрения (они к аплету не имеют никакого отношения), но следует обратить внимание на несколько основных положений, без которых дальнейшее изложение не будет понятным.

На первых двух фазах жизненного цикла на карту загружаются два элемента, уникальные для каждой карты:

- серийный номер карты
- секретный ключ, который используется операционной системой карты для контроля доступа к карте

Хотя секретный ключ и уникален для каждой карты, но он может быть получен путем диверсификации мастер-ключа всего лота (партии) карт, поставленных производителем, на уникальном серийном номере карты.[1]

С помощью секретного ключа операционная система карты устанавливает защищенное соединение с внешним источником[2]. Для этого сначала выполняется взаимная аутентификация карты и внешнего источника, а затем организуется защищенное соединение для передачи карте данных персонализации от внешнего источника.

Процесс подготовки данных персонализации выполняется в бэк-офисной системе эмитента платежных карт. Этот процесс может использовать данные, хранящиеся на разных хостах эмитента. Его цель – подготовить данные, которые должны быть загружены на карту. Часть этих данных может быть общей для всего набора эмитируемых карт. Некоторые данные меняются от карты к карте. Часть данных может передаваться карте в открытом виде. В то же время имеются данные (ключи, PIN-коды), которые во время всего процесса персонализации должны храниться и передаваться в зашифрованном виде.

Подробно весь процесс персонализации описан в документе *EMV Card Personalization Specification. Version 1.1. July 2007*. Особенности персонализации аплета PayCORN описаны в документе *Платежный аплет PayCORN. Версия 19.14. Сентябрь 2015*.

Фаза использования карты интересна в связи с предоставленной возможностью менять параметры платежного приложения в процессе сопровождения аплета на карте. Для этого используется скрипт-процессинг.

[1] На самом деле для контроля доступа к карте используется не один ключ, а три, но все они получаются путем диверсификации мастер-ключа. Кроме того, следует сказать, что ряд производителей карт использует другую схему дистрибуции ключей, когда с лотом карт поставляется не один ключ, а три.

[2] Терминологически не совсем верно, поскольку за установку защищенного соединения отвечает специальный аплет карты, который называется Issuer Security Domain.

Скрипт-процессинг

В ответе эмитента на онлайновую обработку могут присутствовать команды скрипт-процессинга, предназначенные для платежного аплета. С помощью этих команд эмитент имеет возможность менять параметры платежного приложения, разблокировать или изменить PIN-код, заблокировать приложение карты. Эмитент может присвоить каждой команде скрипт-процессинга статус критичной (команда направляется карте сразу после получения её терминалом до выполнения второй команды GENERATE AC) или некритичной (команда передается карте после выполнения второй команды GENERATE AC). Более подробно команды скрипт-процессинга описаны в документе *Платежный аплет PayCORN. Версия 19.14. Сентябрь 2015*.

Эмитент может заблокировать платежное приложение, прислав в ответе на запрос авторизации элемент данных Card Status Update (CSU) с установленным признаком того, что приложение должно быть заблокировано.

Если выполнена успешная аутентификация эмитента (ответ эмитента признан достоверным), то приложение блокируется по требованию эмитента – переводится в состояние APPLICATION BLOCK. В этом состоянии текущая транзакция может быть завершена любым образом и после второй команды GENERATE AC могут быть выполнены команды некритичного скрипт-процессинга. Но любая следующая транзакция может быть обработана только с определенными ограничениями:

- команда SELECT для выбора платежного приложения всегда завершается с кодом, информирующим о том, что платежное приложение заблокировано и работа с ним возможна только в ограниченных пределах (но в ответе предоставляется объект FCI)
- после выбора платежного приложения без ограничения могут использоваться команды GET PROCESSING OPTIONS, GET DATA, READ RECORD, GET CHALLENGE и VERIFY
- на команду GENERATE AC платежное приложение всегда возвращает криптограмму AAC (отвергает транзакцию)
- не допускаются никакие команды скрипт-процессинга, кроме команды APPLICATION UNBLOCK, использующейся для разблокирования платежного приложения.

Разблокирование платежного приложения, осуществляемое с помощью команды APPLICATION UNBLOCK, может быть выполнено только на специальном терминале, поскольку процедура разблокирования отличается от стандартного алгоритма выполнения транзакции и скрипт-процессинга.

Более подробная информация о разблокировании платежного приложения приведена в документе *Платежный аплет PayCORN. Версия 19.14. Сентябрь 2015*.

Заблокированная карта

Эмитент может заблокировать не только платежное приложение, как это описано в предыдущем разделе, но и карту. Если выполнена успешная аутентификация эмитента (ответ эмитента признан достоверным), то карта блокируется по требованию эмитента. После этого работа ни с одним из приложений на карте становится невозможной.

В платежном приложении обработка требования эмитента по блокированию карты выполняется следующим образом:

- платежное приложение переводится в состояние CARD BLOCK
- с помощью средств GlobalPlatform среде GlobalPlatform Environment, отвечающей за управление состоянием карты, сообщается, что карта должна быть заблокирована

Для того, чтобы платежное приложение могло заблокировать карту, должны выполняться следующие условия:

- платежное приложение должно иметь привилегию Card Lock
- текущее состояние карты должно быть SECURED

Если карта успешно заблокирована, то текущая транзакция может быть завершена любым образом и после второй команды GENERATE AC могут быть выполнены команды некритичного скрипт-процессинга. Но в дальнейшем при попытке выбора любого приложения на карте (а не только приложения, заблокировавшего карту), среда GlobalPlatform Environment будет сообщать, что карта заблокирована и работа с ней невозможна (команда SELECT для выбора любого аплета, кроме аплета с привилегий Final Application[1], возвращает байты состояния 6A81).

Разблокирование карты хотя и возможно, но не имеет никакого отношения к спецификациям EMV и платежному аплету. Более подробная информация о блокировании и разблокировании карты приведена в документе *GlobalPlatform. Card Specification. Version 2.2. March 2006*.

[1] Обычно, аплет с привилегий Final Application – это Issuer Security Domain.

3

Методы разработки и тестирования

Для разработки аплета PayCORN применялись средства создания cap-файла, которые были предоставлены NXP Semiconductors по соглашению NDA (Non-Disclosure Agreement). Инструменты NXP Semiconductors использует большинство разработчиков аплетов для карт на платформе Java Card (история вопроса, почему именно эти средства используются, достаточна интересна, но не относится к сфере вопросов, рассматриваемых в документе). Поскольку NDA запрещают все обсуждения о средствах разработки, можно сказать только одно – средства разработки отвечают всем современным требованиям, предъявляемым к среде разработки приложений.

Хотя инструментальные средства NXP Semiconductors и включают систему скриптов для загрузки аплета на карту, обмена командами с картой, а также эмулятор среды карты для отладки аплетов, но они не использовались при разработке аплета PayCORN. Для этих целей использовались только проприетарные средства СКАНТЕК, разработанные специально и не являющиеся собственностью NXP Semiconductors.

Кроме того, платежный аплет PayCORN успешно прошел полную систему тестов совместимости со спецификациями Common Core Definitions (CCD) для платежных аплетов (Level 2 Evaluation Tests для контактных карт, удовлетворяющих спецификациям EMV, компании UL, сертифицированной для этих целей EMVCo).

ДЛЯ ЗАМЕТОК