ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

СКАНТЕК

# Усовершенствованный аплет лояльности

Версия 3.0

Август 2016

СКАНТЕК

# Приложения на Java-карте



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

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

**Список изменений.**

**19.04.2016**

1. Изменен формат сертификата публичного ключа эмитента. Теперь сертификат включает полный идентификатор карты лояльности.

2. Описаны требования, которым должен удовлетворять формат данных лояльности.

**17.08.2016**

1. Новая версия приложения лояльности, в котором реализованы следующие основные возможности:
   - онлайновая аутентификация данных
   - верификация владельца карты для транзакции оплаты бонусами

2. Поскольку онлайновая аутентификация данных не отменяет, а дополняет офлайновую аутентификацию, полностью изменен формат данных, которыми обмениваются терминал и приложение лояльности. В результате можно констатировать, что приложения лояльности версии 2 и 3 с точки зрения терминала не совместимы – это разные приложения. С точки зрения эмитента карт лояльности – это дальнейшее развитие приложения лояльности, так как в приложении лояльности может использоваться только офлайновая аутентификация. В этом случае для эмитента карт лояльности персонализация карт и обработка транзакций не претерпевают никаких изменений.

3. В связи с реализацией верификации владельца карты и поддержкой метода верификации «Проверка незашифрованного PIN-кода путем предъявления его карте (offline PIN)» добавлены команды VERIFY и PIN CHANGE / UNBLOCK для сопровождения PIN-кода на карте.

4. В свою очередь реализация команды PIN CHANGE/UNBLOCK привела к необходимости поддержки терминалом обработки команд скрипт-процессинга, поступивших от процессингового центра лояльности.

5. Значительно переработана структура документа. Не удивительно, что появились новые разделы, описывающие формат данных, которые используются для онлайновой аутентификации данных и верификации владельца карты. Но автор попытался создать документ, после прочтения которого *все всё поймут*. Может быть ему это и не удалось, но документ значительно растолстел (с 20-ти страниц до 100).

**18.08.2016**

1. Добавлен новый раздел «Общая схема инициализации», который отвечает на множество FAQ, поступивших от организаций, занимающихся персонализацией. Общая тональность вопросов сводится к следующему: «А что такое *инициализация* и кому это нужно»? Автор попытался объяснить, хотя и сам это до конца не понимает.
2. Модифицирован алгоритм вычисления криптограммы приложения. Теперь из состава подписываемых данных эмитент может исключить проприетарный объект TTQ, который с одной стороны является обязательным, а с другой – не совсем понятен эмитенту.
3. Описаны объекты персонализации, значения которых определены по умолчанию. Попытка избавиться от таких объектов ни к чему хорошему не привела – значения по умолчанию по прежнему нужны (по разным причинам).
4. В результате вычитки документа исправлены ошибки в определениях, формулах, и просто ошибки в синтаксисе и семантике.

**22.08.2016**

1. Добавлены новые разделы «Легкий вариант персонализации» и «Вариант полной персонализации». Первый из этих разделов поясняет процесс персонализации аплета лояльности в случае, когда используется только офлайновая аутентификация (эмитенту не требуется хранить секретную информацию и обрабатывать её в процессинговом центре). Во втором разделе приводится описание персонализации аплета лояльности в том случае, когда используются все возможности аплета.
2. Описаны привилегии, которые в определенных ситуациях должны быть установлены для аплета лояльности при его загрузке на карту.
3. Исправлены ошибки при описании элементов данных, использующихся при выполнении транзакции лояльности.

# Содержание

1

# Основные понятия

Аплет лояльности – это специализированное приложение, которое предназначено для обеспечения программы лояльности с использованием бонусов (за покупку товара продавец начисляет покупателю бонусы – внутреннюю валюту, которая используется для оплаты товаров наряду с обычными деньгами). В аплете лояльности предусмотрены средства для инициализации (начальной настройки аплета), персонализации (создания ключей и данных), и получения данных лояльности (идентификатора пользователя системы лояльности) с возможностью их офлайновой аутентификации терминалом или онлайновой аутентификации эмитентом.

Основные компоненты аплета лояльности показаны на рис. 1. Не все компоненты обязательно присутствуют в аплете. Во время персонализации аплета эмитент определяет опции его использования, в соответствии с которыми выполняется настройка аплета и формирование необходимых компонентов.

Любому аплету сопоставляется 8-ми байтный уникальный серийный номер аплета, который может использоваться в качестве уникального идентификатора карты с аплетом лояльности. Уникальный серийный номер формируется в процессе инициализации аплета.

Для обеспечения офлайновой аутентификации данных лояльности, которая выполняется с использованием несимметричной криптографии, в аплет должны быть загружены следующие данные об инфраструктуре открытых ключей (PKI):

- сертификат публичного ключа эмитента, полученный на секретном ключе центра сертификации, и экспонента публичного ключа эмитента
- индекс ключа центра сертификации, который использовался для генерации сертификата публичного ключа эмитента
- секретный ключ эмитента, применяемый для получения сертификата предоставляемых данных лояльности

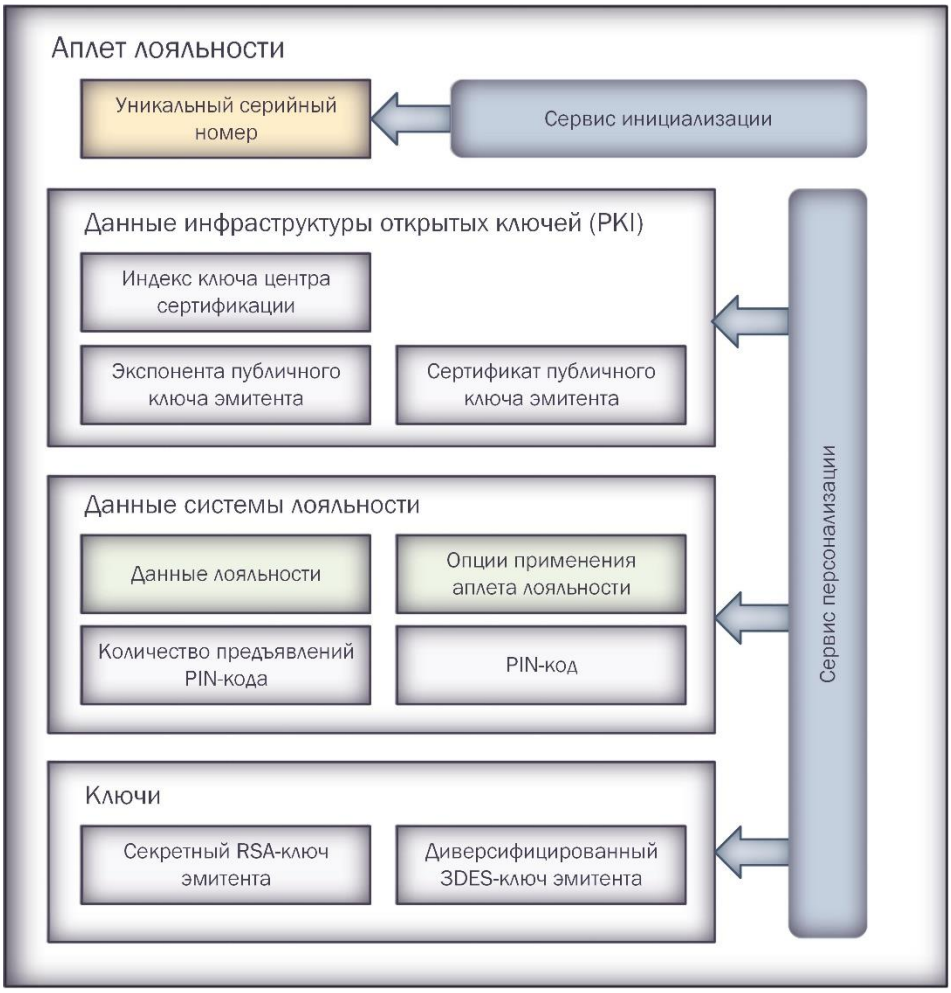


Рис. 1. Основные компоненты аплета лояльности.

Если офлайновая аутентификации данных не должна использоваться, то все перечисленные выше элементы данных не загружаются в аплет в процессе персонализации. Для онлайновой аутентификации данных лояльности используется симметричный 3DES-ключ, который отсутствует в аплете, если эмитент не использует онлайновую аутентификацию. Эмитент может также определить необходимость использования офлайнового PIN-кода[1] для верификации владельца карты. В этом случае при персонализации вводится значение PIN-кода и максимальное количество его предъявлений.

Единственными обязательными элементами являются данные лояльности и опции применения аплета лояльности.[2]

[1] Офлайновый PIN-код проверяется картой. Для проверки PIN-кода терминал должен использовать команду VERIFY (аналогично тому, как это делается для платежных карт).

[2] Опции применения аплета лояльности также не являются обязательным элементом, т. к. существует значение по умолчанию для опций применения (см. раздел «Персонализация»). Но для дальнейшего изложения пока будет удобнее считать, что опции применения должны быть определены.

## Формат данных лояльности

Формат данных лояльности определяется эмитентом, но в общем виде данные лояльности должны удовлетворять следующим требованиям:

- первый байт определяет идентификатор формата в шестнадцатеричном виде (в текущей версии – значение 0x01)
- последующие байты (от 8 до 19) задаются в текстовом виде и должны определять идентификатор карты лояльности[1] в виде последовательности десятичных цифр
- за идентификатором карты лояльности следует разделитель – символ '=' (шестнадцатеричное значение 0x3D)
- после разделителя могут быть определены любые символы или не определено ни одного символа

Таким образом, длина данных лояльности не может быть меньше 10 байт. Максимальная длина данных лояльности определяется ограничениями на длину данных, получаемых от карты, и равна 48 байтам.

## Возможности эмитента

Ещё один обязательный элемент данных в аплете лояльности (кроме данных лояльности) – это опции применения аплета лояльности, которые устанавливает эмитент карт лояльности. Эти опции определяют, каким образом должен обрабатывать транзакцию лояльности терминал в зависимости от типа транзакции и его возможностей.[2]

Аплет лояльности обрабатывает два типа транзакций: начисление бонусов и оплата бонусами. Начисление бонусов – это операция, которая не требует особых мер безопасности, поскольку она всегда связана с оплатой покупки (эта операция не может заинтересовать злоумышленника). А вот процесс оплаты бонусами злоумышленнику интересен, поэтому он может предпринять различные атаки на схему безопасности системы лояльности.

Ещё одно отличие между начислением бонусов и оплатой бонусами заключается в том, что начисление может быть выполнено в офлайновом режиме, а оплата – нет. В случае начисления бонусов терминал может сохранять данные о транзакции в файле транзакций, который пересылается процессинговому центру лояльности в результате клиринговой операции (например, при закрытии смены). Это актуально не только для терминалов, у

[1] Аналогично PAN на платежной карте.

[2] Опции применения аплета лояльности используются также самим аплетом при персонализации. Они определяют состав данных персонализации и используются при проверке корректности данных в процессе персонализации.

которых нет возможности онлайновой обработки, но также и в случае, когда терминалу не удалось связаться с процессинговым центром (ситуация Unable to go Online). Оплата бонусами возможна только в случае онлайновой обработки, так как сумма накопленных бонусов хранится в процессинговом центре лояльности, и только процессинговый центр может авторизовать транзакцию оплаты.

В зависимости от типа транзакций эмитент определяет различные методы их обработки. Обработка любой транзакции всегда связана с аутентификацией данных лояльности, методом верификации владельца карты и авторизацией запроса на оплату бонусами, выполняемой процессинговым центром лояльности.

Аплет лояльности предоставляет две возможности по аутентификации данных лояльности: офлайновую и онлайновую аутентификацию. Офлайновую аутентификацию всегда выполняет терминал, а онлайновую – процессинговый центр лояльности. Для офлайновой аутентификации используется несимметричная криптография, а для онлайновой – симметричные ключи, которые хранятся в процессинговом центре лояльности.

Эмитент также определяет и метод верификации владельца карты (CVM) при оплате бонусами.[1] Для этого может использоваться PIN-код, который хранится только в процессинговом центре лояльности, или в процессинговом центре и на карте лояльности, или только на карте. Поэтому можно говорить о вводе PIN-кода в онлайновом режиме (PIN-код проверяет эмитент) или в офлайновом режиме (PIN-код проверяет карта лояльности). Если PIN-код не используется, то единственные методы CVM – это подпись владельца или «No CVM» (верификация не требуется).

В приведенной ниже таблице показано, какие опции применения аплета лояльности могут быть установлены эмитентом.

[1] Для начисления бонусов верификация владельца карты не требуется, так как абсолютно бесполезна.

| | Обработка | | Аутентификация | | CVM | | | |
|---|---|---|---|---|---|---|---|---|
| | Offline | Online | Offline | Online | Offline PIN | Online PIN | Подпись | No CVM |
| Начисление | C | C | C[1] | C[1] | NA | NA | NA | M[2] |
| Оплата | NA | M | C[1] | C[1] | C[3,4] | C[4] | C[4] | C |

В таблице используются следующие сокращения:

- C (Conditional). Данная возможность не является обязательной, но может использоваться в зависимости от других используемых возможностей и требований эмитента.
- M (Mandatory). Эта возможность является обязательной или единственной, которая может быть выбрана.
- NA (Not Applicable). Не применимо для данного типа транзакции.

Более подробная информация об опциях применения аплета лояльности, которые может использовать эмитент для настройки аплета лояльности, приведена в разделе «Формат опций применения».

## Списки объектов данных

Для выполнения некоторых команд требуются данные о транзакции и терминале. В реализации аплета лояльности такие данные требуются для команды READ – команды чтения данных лояльности (см. раздел «Команда READ»). Список объектов данных, необходимых для выполнения команды, в общем случае называется Data Object List (DOL). В применении для команды READ список называется Read DOL (RDOL).

Список объектов данных представляет собой перечень тэгов и длин объектов данных, которые должны быть переданы карте. Список RDOL записывается на карту в процессе её персонализации и предоставляется терминалу в ответ на команду SELECT. Терминал использует список RDOL для формирования данных, которые должны быть переданы команде READ. Карте передаются только значения объектов в порядке их определения в списке. Предполагается, что объекты из списка известны терминалу (в качестве значения неизвестного объекта терминал предоставляет нулевое значение).

---

[1] Должен использоваться хотя бы один метод аутентификации данных лояльности.

[2] Поскольку для начисления бонусов верификация владельца карты не требуется, единственный используемый метод верификации «No CVM».

[3] Предъявление PIN-кода в офлайновом режиме (PIN-код проверяет карта лояльности) доступно только для контактного режима.

[4] Любой метод верификации владельца карты доступен только в том случае, если терминал поддерживает этот метод.

Значения объектов, определенных в RDOL, используются командой READ для формирования данных офлайновой и онлайновой аутентификации, а также для определения метода верификации владельца карты. Перечень объектов и их порядок в списке определяет эмитент. Три объекта являются обязательными для определения в RDOL. Они приведены в следующей таблице.

| Тэг | Длина | Значение |
|---|---|---|
| C7 | 1 | Terminal Transaction Qualifiers (TTQ) |
| 9C | 1 | Transaction Type |
| 9F37 | 4 | Unpredictable Number |

Объект Terminal Transaction Qualifiers (TTQ) является проприетарным и описан в разделе «Кодирование элементов данных». Значения других обязательных объектов Transaction Type[1] и Unpredictable Number являются стандартными для терминала (описаны в спецификациях EMV).

В RDOL могут быть определены и другие объекты, известные терминалу, но они не являются обязательными. Например, объекты, которые приведены в следующей таблице.

| Тэг | Длина | Значение |
|---|---|---|
| 9F02 | 6 | Amount, Authorized (Numeric) |
| 9F1A | 2 | Terminal Country Code |
| 5F2A | 2 | Transaction Currency Code |
| 9A | 3 | Transaction Date |

Таким образом, длина RDOL не может быть меньше 7 байт. Максимальная длина RDOL определяется ограничениями на длину данных, принимаемых от карты, и равна 24 байтам.

Существует ограничение на суммарную длину значений всех объектов, перечисленных в списке RDOL. Максимальная длина значений всех объектов не должна быть больше 64-х байт.

[1] Значение объекта Transaction Type для системы лояльности определено в разделе «Кодирование элементов данных».

## Транзакция лояльности

В выполнении транзакции лояльности принимают участие терминал, карта с аплетом лояльности и процессинговый центр лояльности. Терминал подготавливает данные для выполнения транзакции и предоставляет их карте. Важнейшая роль в процессе обработки транзакции отводится карте, которой эмитентом делегируются функции, связанные с принятием решения о способе завершения транзакции. Карта сообщает о принятом решении терминалу. Терминал выполняет офлайновую аутентификацию данных лояльности и верификацию владельца карты, когда это требуется. Кроме того, терминал выполняет онлайновую обработку (запрашивает авторизацию транзакции у процессингового центра лояльности), если это необходимо.

Рассмотрим, каким образом в выполнении транзакции лояльности принимают участие терминал и карта.

### Терминал

Обработка транзакции лояльности терминалом начинается с выбора аплета лояльности на карте (см. рис. 2). Предположим, что терминал знает, какое приложение лояльности используется для обработки транзакции.[1]

Для выбора аплета используется команда SELECT, которая передает терминалу данные для дальнейшей обработки транзакции. Терминал проверяет результат выполнения команды SELECT, и отклоняет транзакцию, если обнаруживает ошибки (неожиданное поведение аплета лояльности). Транзакция немедленно завершается в следующих случаях:

- команда SELECT завершена с ошибкой (вернула байты состояния, отличающиеся от 0x9000, или не предоставила никаких данных)
- обнаружена ошибка в данных, возвращенных командой SELECT

Формат данных, возвращаемых командой SELECT, зависит от того, может ли использоваться офлайновая аутентификация данных лояльности (см. раздел «Команда SELECT»). В связи с этим проверка корректности формата данных команды SELECT включает следующие шаги.

1. Если длина данных, возвращенных командой (Ls), меньше 11, то данные считаются некорректными.

[1] В документе не рассматривается, каким образом терминал определяет, какое приложение лояльности должно быть выбрано на карте. Методы выбора обрабатываемого приложения на карте общеизвестны и определены в спецификациях EMV.

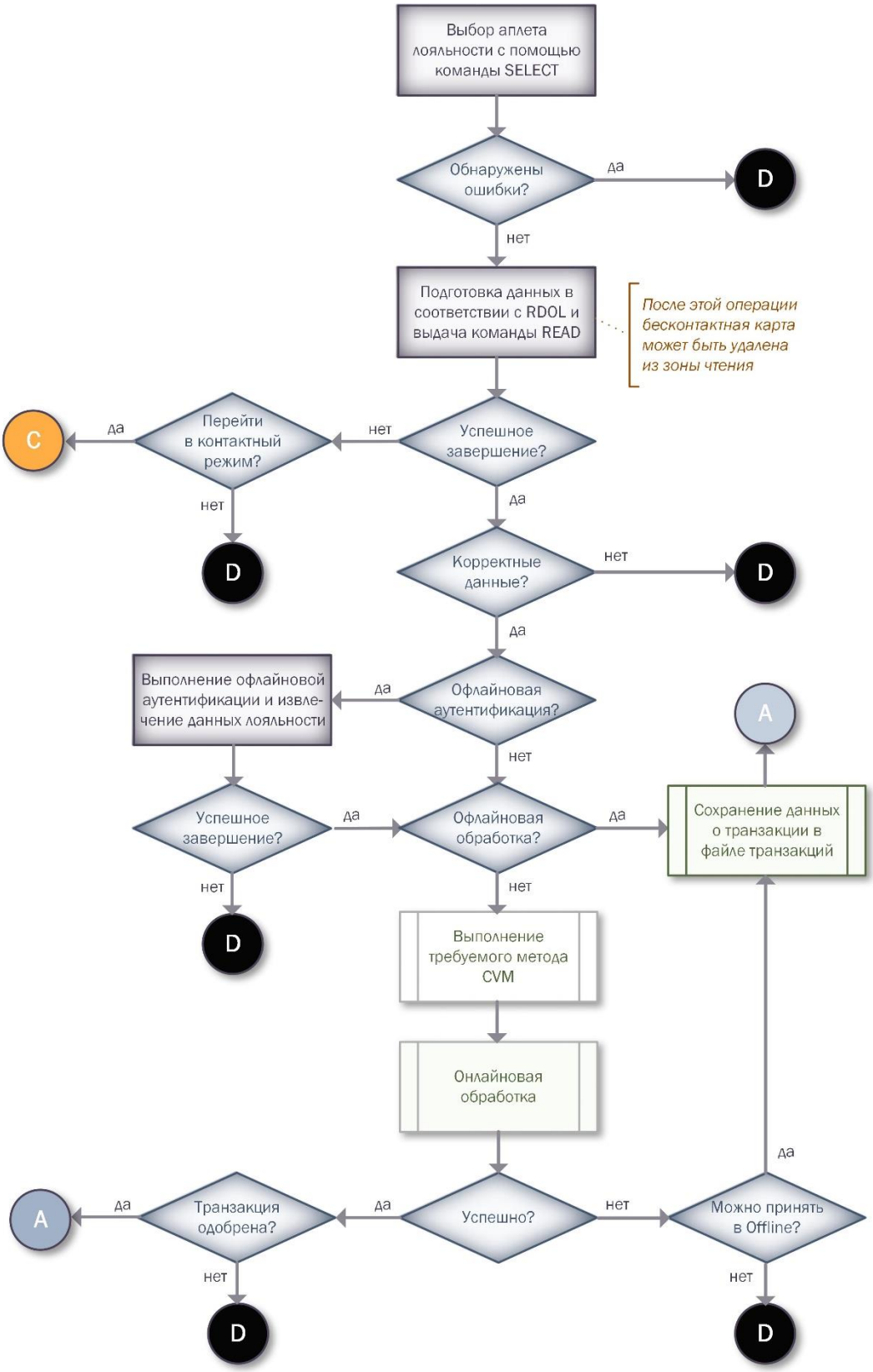


Рис. 2. Обработка транзакции лояльности терминалом.

2. Длина экспоненты публичного ключа эмитента Npx может быть равна 0, 1 или 3. При любом другом значении фиксируется ошибка в данных.

   Если значение Npx равно 0, то информация для офлайновой аутентификации не предоставлена. Первые три байта данных команды SELECT должны быть равны 0 (иначе фиксируется ошибка в данных). Длина сертификата публичного ключа эмитента Nca принимается равной 0.

   Когда значение Npx больше 0, длина сертификата публичного ключа эмитента Nca должна быть определена в интервале от 132 до 224 (ограничения на длины RSA-ключей описаны в разделе «Объекты персонализации»). Также должно выполняться условие Npx+Nca+3 < Ls, где Ls – длина ответа команды SELECT. В противном случае фиксируется ошибка в данных. Для дальнейшей обработки сохраняются индекс ключа центра сертификации, экспонента публичного ключа эмитента и сертификат публичного ключа эмитента, после чего устанавливается внутренний признак «*Предоставлена информация для офлайновой аутентификации*».

3. Длина RDOL, обозначаемая через Ld, должна быть задана в интервале от 7 до 24 (см. раздел «Списки объектов данных»). Кроме того, длина данных, возвращенных командой SELECT, должна равняться Npx+Nca+Ld+4. Если эти условия не выполняется, данные команды SELECT считаются некорректными. Когда всё хорошо, RDOL сохраняется для дальнейшей обработки.

Следующий этап обработки транзакции – подготовка данных в соответствии со списком RDOL и выдача команды READ. Формирование входных данных для команды READ в соответствии с RDOL – это стандартный процесс, описанный в спецификациях EMV (см. документ «EMV. ICC Specifications for Payment Systems. Book 3. Application Specification. Version 4.2. June 2008»). Следует учесть, что длина данных для команды READ должна быть больше 0 и не превышать 64. Если это условие не выполняется, то список RDOL считается некорректным и транзакция завершается.

Терминал проверяет результат выполнения команды READ и отклоняет транзакцию, если обнаружены ошибки, или обеспечивает обработку транзакции в контактном режиме, когда этого требует карта. После выполнения команды READ должны быть выполнены следующие шаги.

1. Если команда READ завершена с ошибкой (вернула байты состояния, отличающиеся от 0x9000 или не предоставила никаких данных), то проверяется, требуется ли переход в контактный режим обработки. Когда байты состояния указывают, что обработка транзакции должна быть выполнена в контактном режиме, выполняется процедура перевода транзакции в контактный режим. В любом случае транзакция завершается.

2. Проверяется корректность данных, возвращенных командой READ. Вначале выполняются общие проверки:

   - длина данных, возвращенных командой READ, должна находиться в интервале от 28 до 205
   - должен быть предоставлен корректный объект «Решение карты» (первые два байта данных, предоставленных командой READ); терминалу должны быть известны индикатор обработки, которую он должен выполнить, и применяемый метод верификации владельца карты
   - длина сертификата данных лояльности Ni может быть равна 0 или должна находиться в интервале от 96 до 188
   - длина данных онлайновой аутентификации Lo может быть равна 0 или 13
   - длина данных лояльности Li может быть равна 0 или должна находиться в интервале от 10 до 48
   - в данных, возвращенных командой READ, должен присутствовать или сертификат данных лояльности, или данные онлайновой аутентификации (Ni и Lo не могут быть одновременно равны 0)
   - в данных команды не могут одновременно присутствовать сертификат данных лояльности и данные лояльности; если сертификат отсутствует, то должны быть представлены данные лояльности
   - длина данных, возвращенных командой READ, должна равняться Ni+Lo+Li+4

   Если не выполняется хотя бы одно из перечисленных условий, данные команды READ считаются некорректными и транзакция отклоняется.

3. Если длина сертификата Ni не равна 0, то для дальнейшей обработки сохраняется предоставленный сертификат данных лояльности и устанавливается внутренний признак «*Предоставлен сертификат*».

4. Когда длина данных онлайновой аутентификации Lo равна 0, данные команды READ считаются корректными и проверка на этом завершается. Иначе, устанавливается внутренний признак «*Требуется онлайновая аутентификация*» и сохраняются данные онлайновой аутентификации.

5. Если длина данных лояльности Li равна 0, данные команды READ считаются корректными и проверка на этом завершается. Иначе, проверяется корректность предоставленных данных лояльности. Формат данных лояльности должен удовлетворять требованиям, описанным в разделе «Формат данных лояльности». Если это не так, данные команды READ считаются некорректными и транзакция отклоняется. Иначе, данные лояльности сохраняются (при этом устанавливается внутренний признак «*Предоставлены данные лояльности*»).

Терминал получил все данные от карты и проверил их корректность. Осталось только проанализировать полученные данные и проверить их на противоречивость. Для этого выполняются следующие действия.

1. Если внутренний признак «*Предоставлен сертификат*» не установлен, выполняется переход к шагу 2. Когда сертификат данных лояльности предоставлен, проверяется установлен ли внутренний признак «*Предоставлена информация для офлайновой аутентификации*». Если нет, то полученные данные противоречивы и транзакция отклоняется. Иначе, устанавливается внутренний признак «*Требуется офлайновая аутентификация*».

2. Для транзакция начисления бонусов в предоставленном решении карты проверяется применяемый метод CVM. Если он отличается от «Верификация владельца карты не требуется», то транзакция отклоняется.

Следующий этап обработки транзакции, который должен выполнить терминал, состоит в выполнении офлайновой аутентификации данных, когда это требуется (установлен внутренний признак «*Требуется офлайновая аутентификация*»). Офлайновая аутентификация данных лояльности не может быть пропущена терминалом, поскольку только в процессе офлайновой аутентификации можно получить данные лояльности (другого пути получения данных лояльности просто нет). Для этого терминал должен выполнить несколько процедур.

Сначала нужно восстановить публичный ключ эмитента из сертификата публичного ключа эмитента, подписанного на секретном ключе центра сертификации.[1] Эта процедура подробно описана в разделе «Восстановление ключа эмитента». Если восстановление публичного ключа эмитента не выполнено, то считается, что аутентификация провалилась.

После восстановления публичного ключа эмитента требуется проверить сертификат данных лояльности, который сформирован на секретном ключе эмитента (см. раздел «Проверка сертификата лояльности»). При неуспешном завершении проверки сертификата лояльности считается, что аутентификация провалилась. Если сертификат лояльности признан достоверным, из него извлекаются данные лояльности. На этом процесс офлайновой аутентификации считается завершенным.

Дальнейшая обработка в терминале определяется индикатором обработки в решении карты. Если требуется принять транзакцию в офлайновом режиме,

[1] Для этого используются данные, полученные по команде SELECT при выборе аплета – индекс ключа центра сертификации и экспонента публичного ключа эмитента.

то данные о транзакции сохраняются в файле транзакций, который пересылается процессинговому центру лояльности в результате клиринговой операции (например, при закрытии смены), и обработка транзакции завершается.

Когда транзакция должна быть обработана в онлайновом режиме (передана на авторизацию эмитенту), то терминал сначала выполняет требуемый картой метод верификации владельца карты. Только после этого формируется запрос в процессинговый центр лояльности, который содержит данные авторизуемой транзакции. Обратите внимание на следующие нюансы онлайновой обработки:

- запрос в процессинговый центр лояльности не обязательно содержит данные онлайновой аутентификации (онлайновая аутентификация может не выполняться процессинговым центром, если эмитент считает, что достаточно офлайновой аутентификации данных), но в нем обязательно должны присутствовать данные лояльности (тем самым гарантируется, что офлайновая аутентификация была выполнена терминалом)
- если используется онлайновая аутентификация, то в запросе авторизации транзакции должны быть предоставлены все данные, которые используются при вычислении криптограммы приложения (см. раздел «Данные онлайновой аутентификации»)
- если требуемый картой метод верификации владельца карты провалился, то это не является поводом для отклонения транзакции; об этой ситуации извещается процессинговый центр (через CVM Results), который и должен принять решение об одобрении или отклонении транзакции

Когда онлайновая авторизация транзакции невозможна (например, в случае ситуаций «Unable to go Online» или «Ответ эмитента не получен»), действия терминала зависят от индикатора обработки в решении карты. Если транзакция может быть принята в офлайновом режиме (индикатор обработки равен 1), то данные о транзакции сохраняются в файле транзакций и пересылаются процессинговому центру в результате клиринговой операции. В противном случае транзакция отклоняется.

При получении авторизационного ответа процессингового центра терминал отклоняет или одобряет транзакцию в соответствии с его решением. Если в авторизационном ответе присутствуют команды скрипт-процессинга, то они должны быть выполнены при завершении транзакции[1] (этот процесс на рис. 2 не показан).

[1] Эмитент определяет в опциях применения (см. раздел «Формат опций применения»), возможна ли обработка команд скрипт-процессинга в бесконтактном режиме. Если скрипт-процессинг возможен только в контактном режиме, а карта считает, что он необходим, терминалу будет сообщено, что требуется переход в контактный режим.

## Карта

Обработка транзакции лояльности картой начинается с команды SELECT (см. рис. 3). При обработке команды SELECT карта еще не знает типа выполняемой транзакции. Поэтому проверяется, запланировал ли эмитент офлайновую аутентификацию данных для транзакции начисления бонусов или транзакции оплаты бонусами (см. опции применения аплета лояльности в разделе «Формат опций применения»). Если да, то формируется ответ команды с данными для офлайновой аутентификации, сформированными в процессе персонализации аплета. Т. е. в ответ команды заносится индекс ключа центра сертификации, экспонента публичного ключа эмитента и сертификат публичного ключа эмитента. Когда офлайновая аутентификация не запланирована, никакие данные для офлайновой аутентификации в ответ не заносятся (они отсутствуют в аплете).

В любом случае в ответ команды заносится список RDOL (см. раздел «Списки объектов данных»). Сформированные данные передаются терминалу и выполнение команды SELECT завершается.

Выполнение команды READ всегда начинается с проверки входных данных. Входные данные должны быть подготовлены терминалом в соответствии со списком RDOL, поэтому карта знает, где находятся интересующие её элементы данных в массиве входных данных. Карту проверяет только два объекта: Terminal Transaction Qualifiers (TTQ) и Transaction Type (тип транзакции).[1]

Входные данные для команды READ считаются корректными, если выполняются все из перечисленных условий:

- длина данных, переданных вместе с командой READ, равна суммарной длине объектов данных, определенных в списке RDOL
- тип транзакции известен карте
- в TTQ не установлены противоречащие друг другу признаки[2]

Если в данных обнаружены ошибки, то команда READ завершается, информируя терминал о некорректных входных данных (возвращаются байты состояния 0x6A80).

---

[1] TTQ определяет возможности терминала (см. раздел «Terminal Transaction Qualifiers (TTQ)»), а Transaction Type – тип транзакции лояльности, обрабатываемой терминалом (см. раздел «Transaction Type»).

[2] В TTQ не должны быть одновременно установлены признаки «Терминал не поддерживает онлайновую обработку (offline only)» и «Терминал не поддерживает офлайновую обработку (online only)», а также признаки «Терминал не поддерживает онлайновую обработку (offline only)» и «Терминал поддерживает онлайновый ввод PIN-кода».

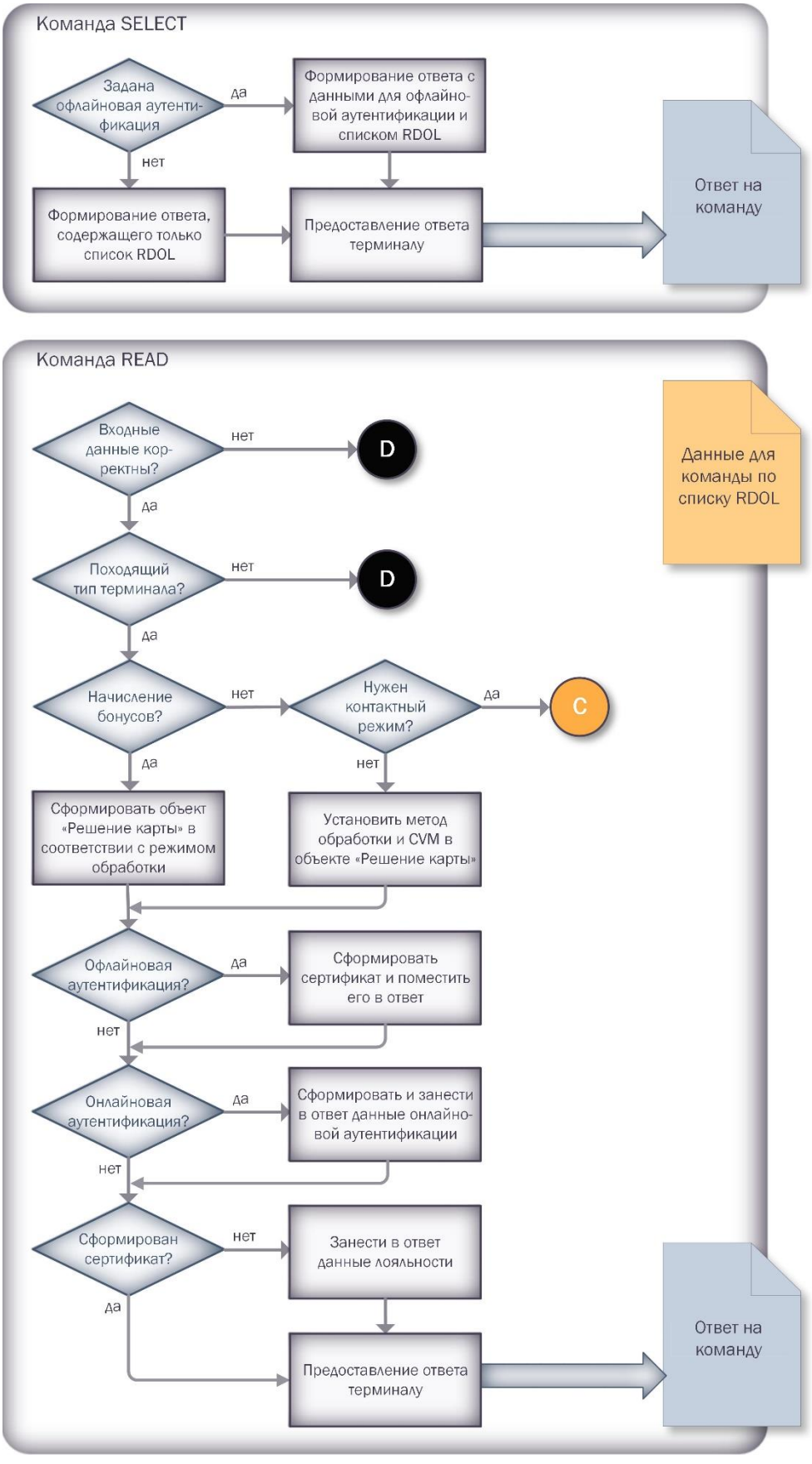


Рис. 3. Обработка транзакции лояльности картой.

Далее анализируются возможности терминала, определенные в TTQ, и определяется, возможно ли выполнение транзакции терминалом. Для транзакции начисления бонусов выполняются следующие проверки:

- если транзакция должна быть обработана в офлайновом режиме, то терминал должен поддерживать офлайновую обработку (в TTQ не должен быть установлен признак «Терминал не поддерживает офлайновую обработку (online only)»)
- если транзакция должна быть обработана в онлайновом режиме, то терминал должен поддерживать онлайновую обработку (в TTQ не должен быть установлен признак «Терминал не поддерживает онлайновую обработку (offline only)»)

Для транзакции оплаты бонусами, которая может быть выполнена только в онлайновом режиме, проверяется, поддерживает ли терминал онлайновую обработку (в TTQ не должен быть установлен признак «Терминал не поддерживает онлайновую обработку (offline only)»).

Если выполнение транзакции невозможно из-за особенностей терминала, выполнение команды READ завершается и возвращаются байты состояния 0x6482 (транзакция должна быть отклонена терминалом).

После этого начинается обработка транзакции. В случае транзакции «Начисление бонусов» формируется объект «Решение карты», который содержит индикатор обработки 0, 1 или 2 в зависимости от выбора эмитента (см. раздел «Формат опций применения») и метод CVM «Верификация владельца карты не требуется». Затем осуществляется переход к шагу 2.

Для транзакции «Оплата бонусами» всё немного сложнее. Во-первых, карта проверяет, требуется ли установка PIN-кода на карте при выполнении транзакции. Установка PIN-кода на карте требуется и возможна, если в соответствии с политикой эмитента выполняются следующие условия:

- применяется верификация владельца карты (определен список CVM)
- применяется метод верификации «Проверка PIN-кода на карте»
- PIN-код на карте не установлен
- терминал поддерживает онлайновый ввод PIN-кода

Когда все эти условия выполняются, установка PIN-кода необходима и может быть осуществлена в любом случае для контактной транзакции через скрипт-процессинг. Если транзакция выполняется в бесконтактном режиме, то должно быть учтено решение эмитента о возможности обработки команд скрипт-процессинга в бесконтактном режиме (см. «Формат опций применения»). Когда эмитент разрешает обработку команд скрипт-процессинга только в контактном режиме, команда READ завершается и возвращаются байты состояния 0x6481 (требуется переход в контактный режим обработки). В случае, когда скрипт-процессинг возможен при выполнении текущей

транзакции, устанавливается внутренний признак «*Требуется установка PIN-кода*» и осуществляется переход к шагу 1.

Разблокирование PIN-кода на карте требуется при выполнении следующих условия:

- применяется верификация владельца карты (определен список CVM)
- применяется метод верификации «Проверка PIN-кода на карте»
- PIN-код на карте заблокирован (счетчик предъявлений PIN-кода равен 0)

Когда все условия выполняются, разблокирование PIN-кода может быть осуществлено для контактной транзакции через скрипт-процессинг. Для бесконтактного режима обработки транзакции должно быть учтено решение эмитента о возможности обработки команд скрипт-процессинга в бесконтактном режиме (аналогично тому, как это делается при установке PIN-кода). Поэтому команда READ может быть завершена с кодом 0x6481 (требуется переход в контактный режим обработки). В случае, когда скрипт-процессинг возможен при выполнении текущей транзакции, устанавливается внутренний признак «*Требуется разблокирование PIN-кода*».

**1** Далее карта формирует в объекте «Решение карты» индикатор обработки (всегда равен 2) и метод CVM. Если верификация владельца карты не применяется (список CVM не определен), то в качестве метода CVM используется метод «Верификация владельца карты не требуется». В противном случае последовательно анализируются все методы CVM, определенные в списке, и определяется, возможно ли применение очередного метода для верификации владельца в соответствии с возможностями терминала. Если нет, то выполняется анализ возможности применения следующего метода в списке. Когда будет найден метод CVM, который может быть применен, он выбирается в качестве используемого метода CVM. Если ни один метод CVM из списка не может быть применен, то в качестве метода CVM в объекте «Решение карты» формируется значение 0 (ни один из методов CVM не может быть применен и решение об одобрении транзакции с учетом этого факта должен принять эмитент). Если в конце списка CVM определен метод «Верификация владельца карты не требуется», то в качестве используемого метода CVM будет выбран этот метод (считается, что терминал всегда поддерживает этот метод).

**2** После формирования решения карты проверяется, требуется ли для транзакции офлайновая аутентификация данных. Если эмитент не запланировал офлайновую аутентификацию данных для транзакции данного типа (см. опции применения аплета лояльности в разделе «Формат опций применения»), то осуществляется переход к шагу 3. Когда офлайновая аутентификация данных требуется, выполняется генерация сертификата данных лояльности, как это описано в разделе «Генерация сертификата лояльности», и устанавливается внутренний признак «*Сгенерирован сертификат лояльности*».

**3** Далее проверяется, требуется ли для транзакции онлайновая аутентификация данных. Если эмитент не запланировал онлайновую аутентификацию данных для транзакции данного типа (см. опции применения аплета лояльности в разделе «Формат опций применения»), то осуществляется переход к шагу 4. Когда онлайновая аутентификация применяется, увеличивается Application Transaction Counter (ATC), генерируется сессионный ключ и на этом ключе вычисляется криптограмма приложения. Затем формируются данные онлайновой аутентификации, как это описано в соответствующем разделе,[1] и устанавливается внутренний признак «*Сгенерированы данные онлайновой аутентификации*».

**4** Наконец проверяется, установлен ли внутренний признак «*Сгенерирован сертификат лояльности*». Если нет, то в ответ команды READ должны быть занесены данные лояльности, поскольку они нужны для онлайновой аутентификации. В связи с этим устанавливается внутренний признак «*В ответ должны быть занесены данные лояльности*».

Команда READ завершается формированием ответа, который должен содержать следующие элементы данных:

- значение объекта «Решение карты»
- сертификат данных лояльности, если установлен внутренний признак «*Сгенерирован сертификат лояльности*»
- данные онлайновой аутентификации, если установлен внутренний признак «*Сгенерированы данные онлайновой аутентификации*»
- данные лояльности, если установлен внутренний признак «*В ответ должны быть занесены данные лояльности*»

Сформированные данные передаются терминалу и выполнение транзакции картой завершается. Если процессинговый центр лояльности пришлет команды скрипт-процессинга, то они будут выполнены картой как продолжение текущей транзакции (в контактном режиме) или при следующем выборе аплета лояльности (в бесконтактном режиме).

[1] Следует учесть, что признаки в поле данных онлайновой аутентификации «Особые случаи, зафиксированные для приложения лояльности» (байт со смещением 12) устанавливаются в соответствии со значением внутренних признаков «*Требуется установка PIN-кода*» и «*Требуется разблокирование PIN-кода*».

## Этапы жизненного цикла аплета

Можно говорить о нескольких этапах жизненного цикла (состояниях) аплета лояльности. Далее перечислены все состояния аплета.

1. После загрузки аплета лояльности на карту он имеет состояние LOADED. Аплет готов к выполнению процесса инициализации.

2. При выполнении инициализации аплета формируются уникальный серийный номер аплета. Инициализация аплета всегда выполняется на внутреннем секретном ключе аплета, который известен только разработчику аплета. После завершения инициализации аплет переходит в состояние INITIALIZED.[1]

3. В состоянии INITIALIZED аплет может быть персонализирован. Для персонализации аплета всегда используется канал безопасности, по которому данные передаются карте (см. раздел «Безопасный обмен данными с картой»). При завершении персонализации аплет переходит в состояние PERSONALIZED.[2]

4. После выполнения персонализации аплет готов к работе. Только на этом этапе данные лояльности могут быть считаны.

[1] Переход из состояния INITIALIZED в состояние LOADED невозможен (т. е. повторная инициализация аплета невозможна).

[2] Переход из состояния PERSONALIZED в состояние INITIALIZED невозможен.

## Соглашения

В документе используются следующие соглашения по кодированию и обозначению информации.

1. Все числовые значения определяются в виде десятичных чисел (например, 12) или в виде шестнадцатеричных значений с префиксом 0x (например, 0x38).

2. Тэги объектов данных задаются в виде шестнадцатеричных значений без префикса 0x (например, 9F37).

3. Если поле или бит зарезервированы (для использования в дальнейшем), то в них могут быть установлены нулевое значение или любое другое (зарезервированные поля и биты не проверяются).

4. Байты в поле нумеруются слева направо, начиная с 0 (например, байт 0 – это самый первый байт поля). Биты в байте нумеруются справа налево, начиная с 0 (например, бит 0 – это самый младший бит байта).

# 2

## Выбор аплета

Для выбора аплета лояльности на карте используется команда SELECT, с которой карте всегда передается идентификатор аплета (AID – Application Identifier), установленный эмитентом. Если аплет лояльности не персонализирован (находится в состоянии LOADED или INITIALIZED), то в ответ на команду SELECT никакие данные не возвращаются. Когда аплет персонализирован и готов к работе, с командой SELECT возвращается информация о том, каким образом следует обрабатывать предоставляемые данные лояльности.

Но главное в другом – только после успешного выбора аплета с помощью команды SELECT последующие команды будут направляться операционной системой карты аплету. Поскольку на карте может быть несколько аплетов, операционной системе карты нужно знать, какому именно из них адресованы команды и данные, подаваемые на карту. Вот это и определяется с помощью команды SELECT.

В связи с этим, с команды SELECT должна начинаться любая процедура работы с аплетом лояльности – инициализация, персонализация или получение данных лояльности.

## Особенности бесконтактного режима

Механизм выбора приложения в бесконтактном режиме достаточно гибок и основывается на том, что на карте присутствует PPSE (Proximity Payment System Environment).[1]

За выбор аплета в бесконтактном режиме отвечает компонент программного обеспечения терминала, который называется Entry Point (см. документ «EMV. Contactless Specifications for Payment Systems. Book B. Entry Point Specification. Version 2.5. March 2015»). Entry Point должен не только определить AID приложения на карте, но и сопоставить ему Kernel ID – идентификатор одного из Kernel, который входит в состав программного обеспечения терминала и отвечает за обработку приложения. Сочетание AID и Kernel ID называется комбинацией. Entry Point формирует список комбинаций, взаимно поддерживаемых картой и терминалом. Для этой цели и служит PPSE, который содержит список приложений, которые могут быть выбраны на карте через бесконтактный интерфейс.

В дальнейшем изложении присутствуют некоторые термины, которые следует пояснить. Исторически сложилось, что файловая структура на карте всегда описывается в терминах стандартf ISO 7816-4. В соответствии со стандартом ISO 7816-4 на карте существуют файлы DF (Dedicated File), или каталоги, которые могут содержать другие DF–файлы или EF-файлы (Elementary File). Являясь каталогом, DF (или ADF – Application DF) не содержит данных, а является так называемой точкой доступа к другим файлам. Информация о DF–файле содержится в заголовке файла, который называется File Control Information (FCI)

Реально, на современных картах нет физических объектов файловой структуры (DF и EF) – это только логические понятия. Можно утверждать, что DF – это приложение на карте. Именем DF является идентификатор приложения, который называется AID (Application Identifier). Для выбора приложения на карте используется команда SELECT. В ответе на команду SELECT приложение возвращает FCI.

[1] В спецификациях EMV не запрещаются и другие подходы к выбору приложения, но они не рассматриваются (вне сферы спецификаций).

PPSE – это аплет на карте, AID которого равен 2PAY.SYS.DDF01. При выборе этого аплета с помощью команды SELECT, он возвращает ответ, который содержит список бесконтактных приложений следующего вида.

| | | | | |
|---|---|---|---|---|
| 6F | FCI Template | | | |
| | 84 | DF Name (2PAY.SYS.DDF01) | | O[1] |
| | A5 | FCI Proprietary Template | | M |
| | | BF0C | FCI Issuer Discretionary Data | M |
| | | | 61 Directory Entry | M |
| | | | 4F ADF Name (AID) | M |
| | | | 50 Application Label | O |
| | | | 87 Application Priority Indicator | C[2] |
| | | | 9F2A Kernel Identifier | C[3] |
| | | | 9F29 Extended Selection | C |
| | | | 61 Directory Entry | O |
| | | | 4F ADF Name (AID) | M |
| | | | 50 Application Label | O |
| | | | 87 Application Priority Indicator | C |
| | | | 9F2A Kernel Identifier | C |
| | | | 9F29 Extended Selection | C |

Может быть определено только одно приложение или несколько приложений. Дополнительные объекты данных могут быть включены в FCI Issuer Discretionary Data (тэг BF0C) and Directory Entry (тэг 61), но Entry Point игнорирует такие объекты. Назначение почти всех объектов данных в ответе на выбор PPSE интуитивно понятно и не требует дополнительных разъяснений (см. также раздел «Объекты данных»). Остановимся на тех объектах, которые используются для построения списка комбинаций и выбора обрабатываемой комбинации.

**Application Priority Indicator**. Имеет следующий формат.

| | |
|---|---|
| XXXX .... | Резерв |
| .... XXXX | Приоритет от 1 до 15 (1 – наивысший приоритет). Если задано значение 0, то принимается 15 |

[1] Этот объект опционален с точки зрения терминала, но с точки зрения карты – это обязательный объект для персонализации PPSE.

[2] Если на карте присутствует несколько бесконтактных приложений, то каждое приложение должно иметь свой приоритет. Если приоритет не определен, то по умолчанию принимается самый низкий приоритет.

[3] Если используемый Kernel определяется явно.

**Kernel Identifier**. Имеет переменную длину. Длина Kernel Identifier может быть равна одному, трем или более байтам (но не двум). Kernel Identifier имеет следующий формат.

| *Байт* | *Биты* | *Объяснение* |
|---|---|---|
| 1 | XX.. .... | Тип Kernel:<br>• 00 – международный Kernel с идентификатором, назначенным EMVCo, который кодируется в Short Kernel ID<br>• 01 – RFU<br>• 10 – внутренний Kernel с идентификатором в формате EMVCo (в виде конкатенации Short Kernel ID и Extended Kernel ID)<br>• 11 - внутренний Kernel с идентификатором в проприетарном формате (в виде конкатенации Short Kernel ID и Extended Kernel ID) |
| | ..XX XXXX | Short Kernel ID:<br>• 0 – Kernel выбирается по AID приложения<br>• 1-63 – номер Kernel |
| 2-3 | | Extended Kernel ID:<br>• для международного Kernel: RFU<br>• для внутреннего Kernel с идентификатором в формате EMVCo: код валюты (ISO 4217)<br>• для внутреннего Kernel с идентификатором в проприетарном формате: проприетарное значение |
| 4-8 | | RFU |

Если объект Kernel Identifier отсутствует, то Entry Point опирается в выборе Kernel ID на значение объекта ADF Name (AID приложения).[1]

**Extended Selection**. Если этот элемент данных представлен, то Entry Point использует значение объекта Extended Selection в качестве постфикса AID (ADF Name) выбираемого аплета в команде SELECT.

Поскольку аплет лояльности не является стандартным бесконтактным приложением и для него должен быть разработан Kernel с уникальным идентификатором, рекомендуется определять для аплета лояльности в PPSE объект Kernel Identifier (тэг 9F2A). Для придания гибкости программному обеспечению терминала может также использоваться объект Extended Selection (тэг 9F29).[2]

[1] Другими словами, если объект Kernel Identifier отсутствует, то считается что значение этого объекта – нулевой байт (см. формат Kernel Identifier).

[2] Этот объект позволяет использовать для обработки приложений в различными AID один и тот же Kernel.

## Команда SELECT

Команда SELECT кодируется следующим образом.

| Поле | Код | Описание |
|---|---|---|
| CLA | 0x00 | Команда общего назначения |
| INS | 0xA4 | SELECT |
| P1 | 0x04 | Индикатор выбора аплета по AID |
| P2 | 0x00 | Индикатор выбора первого или единственного приложения на карте[1] |
| Lc | XX | Длина AID аплета (от 5 до 16) |
| Данные | | AID аплета, установленный эмитентом при его загрузке на карту |
| Le | XX | Длина ответа на команду SELECT (равна 0, если аплет находится в состоянии LOADED или INITIALIZED) |

Данные, возвращаемые в ответ на команду SELECT, когда аплет лояльности персонализирован (находится в состоянии PERSONALIZED), имеют следующий вид.

| Смещение | Длина | Содержимое |
|---|---|---|
| 0 | X | Данные для аутентификации |
| X | 1 | Длина RDOL (Ld) |
| X+1 | Ld | RDOL |

[1] Параметр P2 команды указывает, определен полный или частичный AID выбираемого аплета. Для выбора аплета лояльности рекомендуется использовать только полный AID, поэтому параметр P2 должен быть равен 0. В ISO 7816-4 определены и другие значения параметра P2, когда выбор файла (в терминологии ISO 7816-4) осуществляется по частичному AID.

Формат возвращаемых данных зависит от того, может ли использоваться офлайновая аутентификация данных лояльности (независимо от типа транзакции и возможностей терминала). Если аплет лояльности был персонализирован с возможностью офлайновой аутентификации данных лояльности, то ответ на команду имеет следующий вид.

| Смещение | Длина | Содержимое |
|---|---|---|
| 0 | X | Данные для офлайновой аутентификации, которые определяются эмитентов в процессе персонализации |
| X | 1 | Длина RDOL (Ld) |
| X+1 | Ld | RDOL |

Когда в аплете лояльности не предусмотрена возможность офлайновой аутентификации данных лояльности, ответ на команду SELECT выглядит следующим образом.

| Смещение | Длина | Содержимое |
|---|---|---|
| 0 | 3 | Нули |
| 3 | 1 | Длина RDOL (Ld) |
| 4 | Ld | RDOL |

В ответ на команду SELECT могут быть возвращены следующие байты состояния:

| SW1 | SW2 | Описание |
|---|---|---|
| 0x90 | 0x00 | Аплет выбран и готов к обработке команд |
| 0x6A | 0x82 | Аплету передана команда для выбора другого аплета, которого нет на карте |
| XX | XX | Общие коды ошибок (см. приложение) |

# 3

## Инициализация

Для того чтобы начать работу с аплетом лояльности, необходимо выполнить его инициализацию. Инициализация аплета лояльности включает формирование уникального серийного номера аплета и всегда выполняется на внутреннем секретном ключе аплета. После завершения инициализации аплет переходит в состояние INITIALIZED. Повторная инициализация аплета в этом состоянии невозможна.

Таким образом, инициализация аплета лояльности выполняется однократно и не может быть повторена. Уникальный серийный номер аплета после завершения инициализации не может быть изменён в течение всего цикла жизни аплета.

Рассмотрим основные принципы инициализации.

## Общая схема инициализации

Для инициализации аплета лояльности требуется мастер-карта. Владелец аплета лояльности загружает на мастер-карту аплет, обеспечивающий настройку лота карт с аплетами лояльности. В дальнейшем будем называть аплет, загружаемый на мастер-карту, мастер-аплетом. Все данные для настройки лота карт с аплетами лояльности заносятся в мастер-аплет во время его загрузки и установки на карту. Поэтому после изготовления мастер-карты она полностью готова к работе и никакие другие параметры функционирования не устанавливаются.

Инициализация аплета лояльности выполняется в автоматическом режиме. Мастер-аплет по запросу терминала предоставляет команды для инициализации аплета лояльности. При этом терминал выступает только в качестве звена передачи данных между мастер-картой и инициализируемой картой.[1] Этот процесс показан на рис. 4.

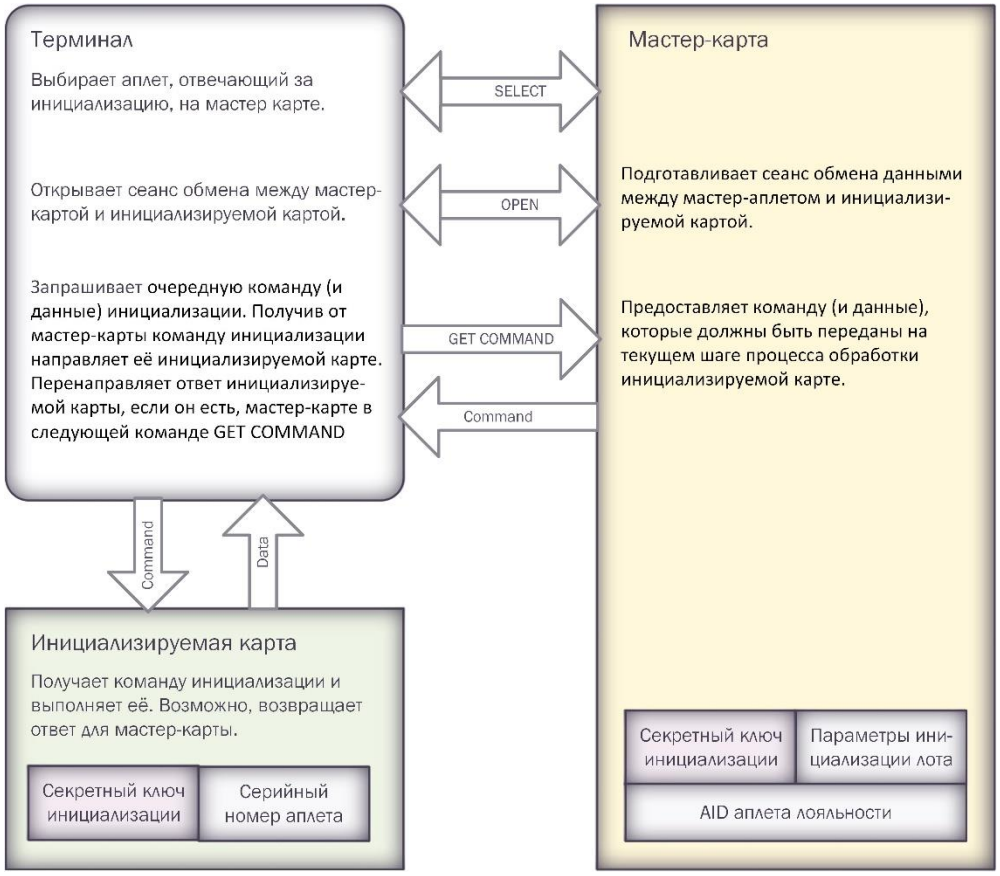


Рис. 4. Общая схема инициализации.

[1] Настройка аплета лояльности является безопасной, поскольку для настройки используются сессионные ключи, сгенерированные на основе ключа инициализации, который является внутренним объектом мастер-аплета и известен также аплет лояльности.

Таким образом, мастер-аплет не только является центральным звеном системы безопасности, но и инкапсулирует все секретные данные, необходимые для инициализации аплета лояльности. Процесс инициализации можно сравнить с лицензированием. Владелец аплета лояльности должен быть уверен, что использование аплета разрешено правообладателем. Только после инициализации аплет лояльности будет готов к работе (лицензирован).

Для терминала процесс инициализации всегда начинается с выбора мастер-аплета на мастер-карте с помощью команды SELECT. Затем терминал посылает мастер-аплету команду открытия сеанса обмена данными. В случае успешного открытия сеанса терминал запрашивает у мастер-аплета первую команду для настройки инициализируемого аплета (обычно, это команда SELECT для выбора инициализируемого аплета на карте[1]). Вместе с очередной командой инициализации мастер-аплет всегда передает терминалу индикатор, который определяет, каким образом команда инициализации должна завершиться и требуются ли мастер-карте какие-нибудь данные, полученные в результате выполнения команды.

Терминал посылает полученную команду инициализируемой карте и руководствуется индикатором, полученным от мастер-карты, для оценки результата её выполнения. Когда исключительные ситуации не обнаружены, терминал запрашивает у мастер-аплета следующую команду настройки.[2] Цикл получения очередной команды и направления её инициализируемой карте продолжается до тех пор, пока мастер-карта не сообщит, что инициализация завершена.

Инициализируемый аплет использует передаваемые ему данные для открытия канала безопасности на сессионном ключе[3] и для своей настройки. Все данные, которыми обмениваются мастер-карта и аплет лояльности зашифрованы. Терминал не должен анализировать ни команды, ни данные, которыми обмениваются мастер-карта и аплет лояльности. Протокол инициализации является закрытым. Только для общности в этом документе описана специальная команда, которая применяется для инициализации аплета лояльности.

---

[1] AID настраиваемого аплета лояльности – один из параметров настройки лота карт с аплетами лояльности.

[2] При этом мастер-карте могут быть переданы данные, возвращенные инициализируемым аплетом лояльности, если это требуется.

[3] В процессе открытия канала безопасности осуществляется также взаимная аутентификация мастер-аплета и аплета лояльности.

## Команда INITIALIZE

Эта команда используется для инициализации аплета, находящегося в состоянии LOADED. В процессе выполнения команды проверяется, имеет ли терминал право на инициализацию аплета[1], и выполняется установка серийного номера аплета.

Остальная информация из этого раздела является конфиденциальной. Она может быть получена после подписания Соглашения о неразглашении (Non-Disclosure Agreement – NDA). Обратитесь с запросом в СКАНТЕК.

[1] В разделе «Общая схема инициализации» описано, что терминал является всего лишь передаточным звеном между аплетом лояльности и мастер-картой. Таким образом можно сказать, что в команде осуществляется аутентификация мастер-карты. Здесь и в дальнейшем термин «терминал» используется только для того, чтобы окончательно не запутать читателя (для многих обмен данными между двумя картами может оказаться за гранью понимания). Читатели, которые внимательно прочли предыдущий раздел и поняли, что там написано, термин «терминал» могут заменить на «мастер-карту».

# 4

## Персонализация

Персонализация карты – это важная часть подготовки карты к работе, которую выполняет эмитент. В процессе персонализации аплет лояльности, загруженный на карту, настраивается таким образом, чтобы он мог выполнять функции элемента системы лояльности. Чтобы лучше понять процесс персонализации, нужно ознакомиться с некоторыми общими положениями 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 лояльности
- 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. В этом разделе обсуждается только третья фаза жизненного цикла, и подробное описание других фаз можно опустить, 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 карт системы лояльности. 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 находиться в зашифрованном виде.

Подробно весь процесс персонализации разбирается в документе EMV Card Personalization Specification. Version 1.1. July 2007. Поэтому остановимся только на общих положениях и особенностях персонализации аплета лояльности.

Следует иметь в виду, что персонализация аплета лояльности может быть выполнена только в том случае, если уже выполнена его инициализация (т. е. аплет находится в состоянии INITIALIZED). Если аплет уже персонализирован, то персонализация не может быть повторена (т. е. персонализация возможна только в том случае, когда аплет находится в состояние INITIALIZED).

[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, но для понимания принципов персонализации это не важно.

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

## Общая схема персонализации

Самая общая схема персонализации приложения лояльности приведена на рис. 5.

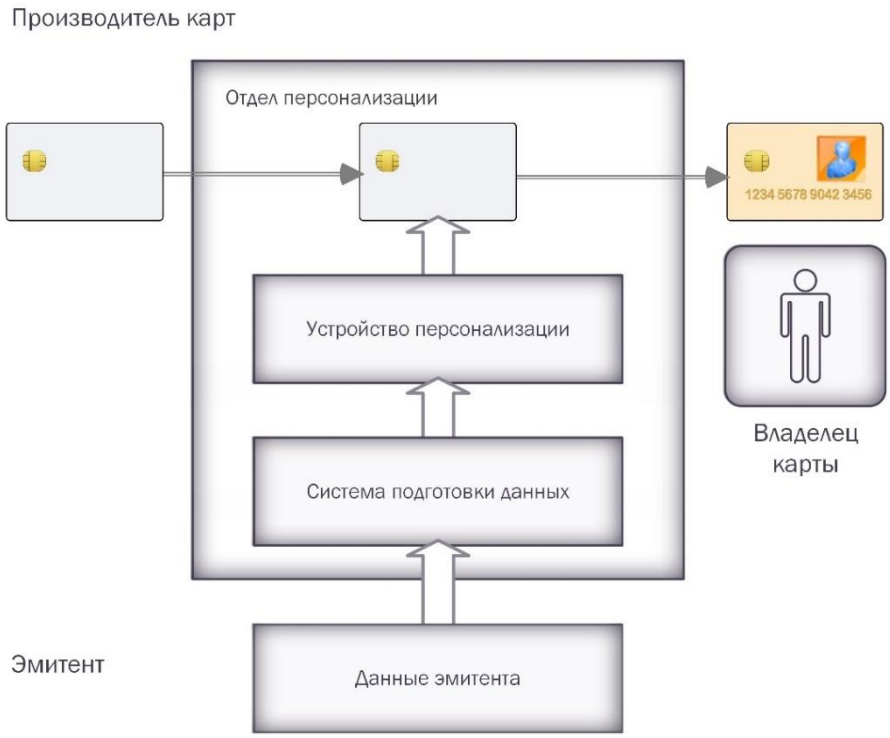


Рис. 5. Общая схема персонализации.

На этом рисунке присутствуют основные объекты, отвечающие за персонализацию приложения лояльности.

- Эмитент. Юридическое лицо, которое от своего имени выпускает карты лояльности для развития своей деятельности.
- Производитель карт. Юридическое лицо, отвечающее за правильную персонализацию карт в соответствии с данными эмитента.
- Система подготовки данных. Система, которая выполняет проверки, подготовки и форматирования данных, которые пересылаются устройству персонализации.
- Устройство персонализации. Устройство, которое принимает данные от системы подготовки данных и посылает команды персонализации карте.

В процессе персонализации принимают участие несколько физических модулей устройства персонализации (модули эмбоссирования, кодирования магнитной полосы, занесения данных на карту), каждому из которых требуется свой набор данных. Нас будет интересовать только один модуль – занесения данных на карту.

Чтобы персонализировать приложение лояльности, устройству персонализации должны быть предоставлены данные эмитента. Эти данные представляются в виде объектов персонализации приложения лояльности. С каждым объектом персонализации сопоставляется DGI (Data Group Identifier) – тэг, под которым объект персонализации известен приложению лояльности.

Существуют такие данные персонализации (ключи, PIN-коды), которые во время всего процесса персонализации должны находиться в зашифрованном виде. Будем их в дальнейшем называть конфиденциальными данными. Любой обмен конфиденциальными данными между объектами системы персонализации должен быть зашифрован на определенных ключах. Обычно ключи, на которых осуществляется обмен конфиденциальными данными, отличаются для различных объектов системы персонализации. Например, на приведенном рисунке конфиденциальные данные должны быть зашифрованы на уникальных ключах в следующих случаях:

- при передаче данных эмитента системе подготовки данных
- при пересылке отформатированных данных из системы подготовки данных в устройство персонализации
- в командах персонализации, которые посылаются на персонализируемую карту

Вопросы безопасности очень важны и здесь будут кратко рассмотрены. Начнем с обсуждения безопасного обмена данными с картой.

## Безопасный обмен данными с картой

Для персонализации аплета лояльности используется канал безопасности, по которому данные передаются карте. Чтобы понять, как организован процесс персонализации, необходимо иметь общие понятия о механизме безопасности карты, называемом Secure Channel Protocol версии 02, или просто SCP02, подробное описание которого приведено в документе GlobalPlatform. Card Specification. Version 2.2. March 2006. Принципы безопасного обмена данными с картой показаны на рис. 6.

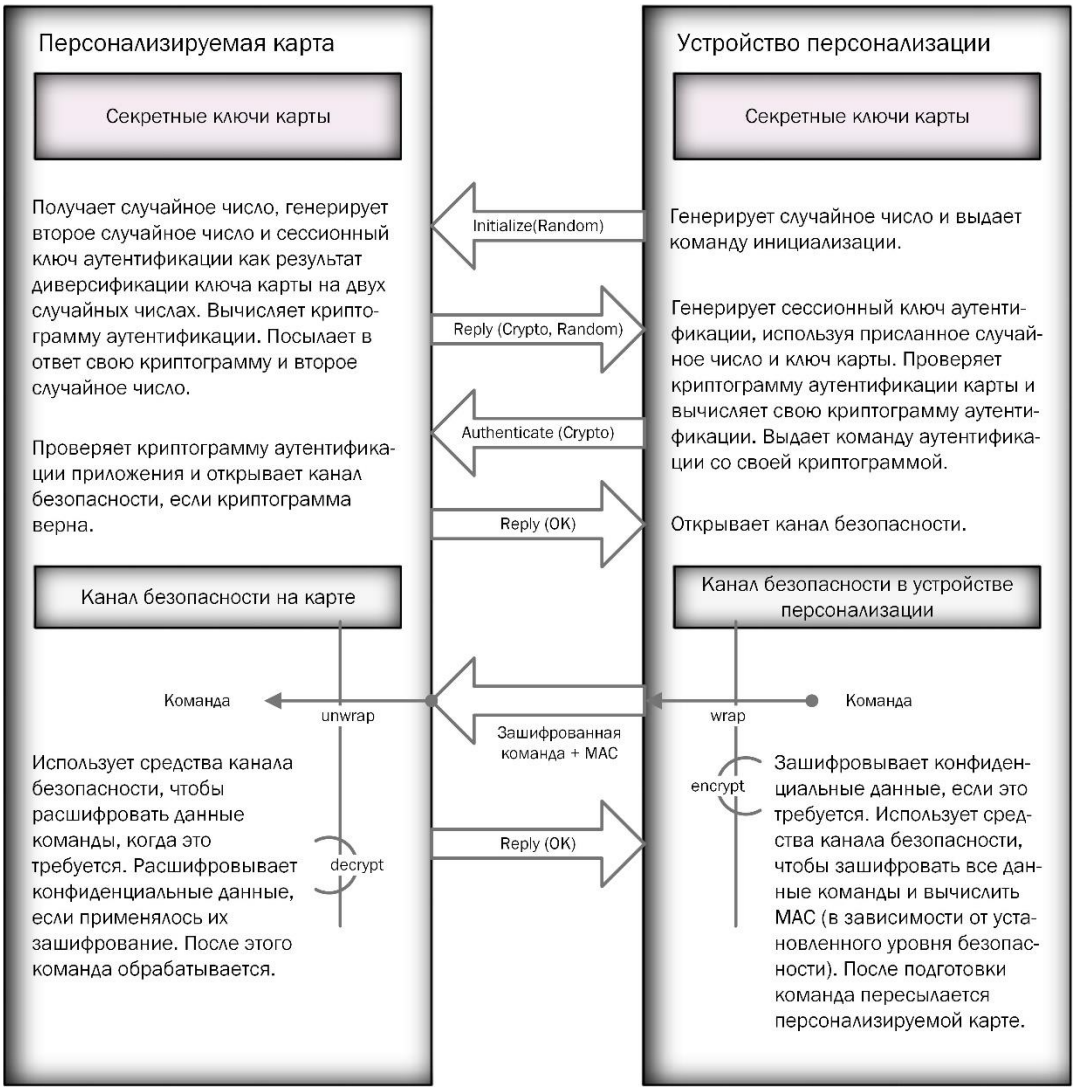


Рис. 6. Канал безопасности при работе с персонализируемой картой.

Чтобы организовать безопасный обмен с картой, устройству персонализации должны быть доступны секретные ключи карты.[1] Процесс создания канала безопасности начинается с того, что устройство персонализации выбирает на карте аплет, и посылает ему команду инициализации, с которой передает случайное число ($Random_1$).

Аплет, получив команду инициализации, направляет её домену безопасности. Домен безопасности – это специальный аплет карты, которому известны секретные ключи карты, и который имеет право на работу с ними. Получив команду инициализации, домен безопасности генерирует второе случайное число ($Random_2$) и получает сессионные ключи канала безопасности, диверсифицируя ключи карты на двух случайных числах. В канале безопасности используются следующие ключи:

- ключ аутентификации и зашифрования данных при обмене по каналу безопасности
- ключ целостности данных при обмене по каналу безопасности (ключ, на котором вычисляется MAC)
- ключ шифрования конфиденциальных данных

Чтобы объект, инициировавший открытие канала безопасности, мог аутентифицировать карту, домен безопасности вычисляет криптограмму аутентификации[2] на основе случайного числа $Random_1$, и посылает в ответе на команду инициализации криптограмму аутентификации и случайное число $Random_2$.

Устройство персонализации, получив ответ на команду инициализации, генерирует сессионные ключи канала безопасности по тем же принципам, что и домен безопасности, после чего проверяет криптограмму аутентификации, присланную в ответе. Если карта аутентифицирована (т. е. ключи карты и устройства персонализации совпадают), то устройство персонализации генерирует свою криптограмму аутентификации на основе случайного числа $Random_2$, после чего посылает на персонализируемую карту команду аутентификации с этой криптограммой, чтобы персонализируемая карта могла аутентифицировать объект, инициировавший открытие канала безопасности (такая взаимная аутентификация гарантирует, что обе стороны владеют одинаковым секретным ключом).

[1] Разумеется, секретные ключи хранятся в секретном модуле. Обычно, это Hardware Security Module (HSM). Устройству персонализации секретные ключи доступны через функции HSM.

[2] Для этого используется сессионный ключ аутентификации.

В команде аутентификации определяется также уровень безопасности, на котором должен функционировать канал безопасности.[1] Могут быть определены следующие уровни безопасности.

- Конфиденциальность и целостность. Данные команды зашифровываются на сессионном ключе аутентификации и для них вычисляется MAC (в терминологии GlobalPlatform – C-MAC) на сессионном ключе целостности данных.
- Целостность. Данные команды не зашифровываются, но для них вычисляется MAC на сессионном ключе целостности данных.
- Ни конфиденциальности, ни целостности. Данные команды не зашифровываются, и для них не вычисляется MAC.

Если домен безопасности на персонализируемой карте аутентифицировал объект, инициировавший открытие канала безопасности, то он открывает канал безопасности с указанным уровнем безопасности и посылает ответ с уведомлением, что канал открыт. Получив ответ, подтверждающий открытие канала безопасности, устройство персонализации открывает свой канал безопасности. Далее канал безопасности может использоваться разными способами. Но для персонализируемого аплета, которому ничего неизвестно о ключах карты, наиболее важны два способа.

Во-первых, аплет может обратиться к домену безопасности, чтобы он применил установленный уровень безопасности к пришедшим данным и проверил данные на соответствие уровню безопасности (для этого используется метод unwrap). Например, если установлен уровень безопасности «Конфиденциальность и целостность», то будет проверен MAC и данные будут расшифрованы.

Во-вторых, аплет может с помощью домена безопасности расшифровать конфиденциальные данные, зашифрованные устройством персонализации на сессионном ключе шифрования конфиденциальных данных (для этого используется метод decryptData).

Из всего вышеизложенного следует, что обмен данными персонализации с аплетом абсолютно безопасен. Все данные персонализации (или только конфиденциальные данные) могут быть зашифрованы на секретном ключе персонализируемой карты, и подтверждены криптографическими контрольными суммами, полученными на другом ключе персонализируемой карты.

[1] Домен безопасности не обязан безоговорочно принимать указанный уровень безопасности. Он может сообщить, что уровень безопасности должен быть повышен.

## Два метода персонализации

Как описано в документе EMV Card Personalization Specification. Version 1.1. July 2007, существует два подхода к персонализации. Поскольку они отличаются достаточно сильно, разберем оба эти метода. Первый из методов называется непрямой метод персонализации (Indirect Method). Общая схема этого метода показана на рис. 7.

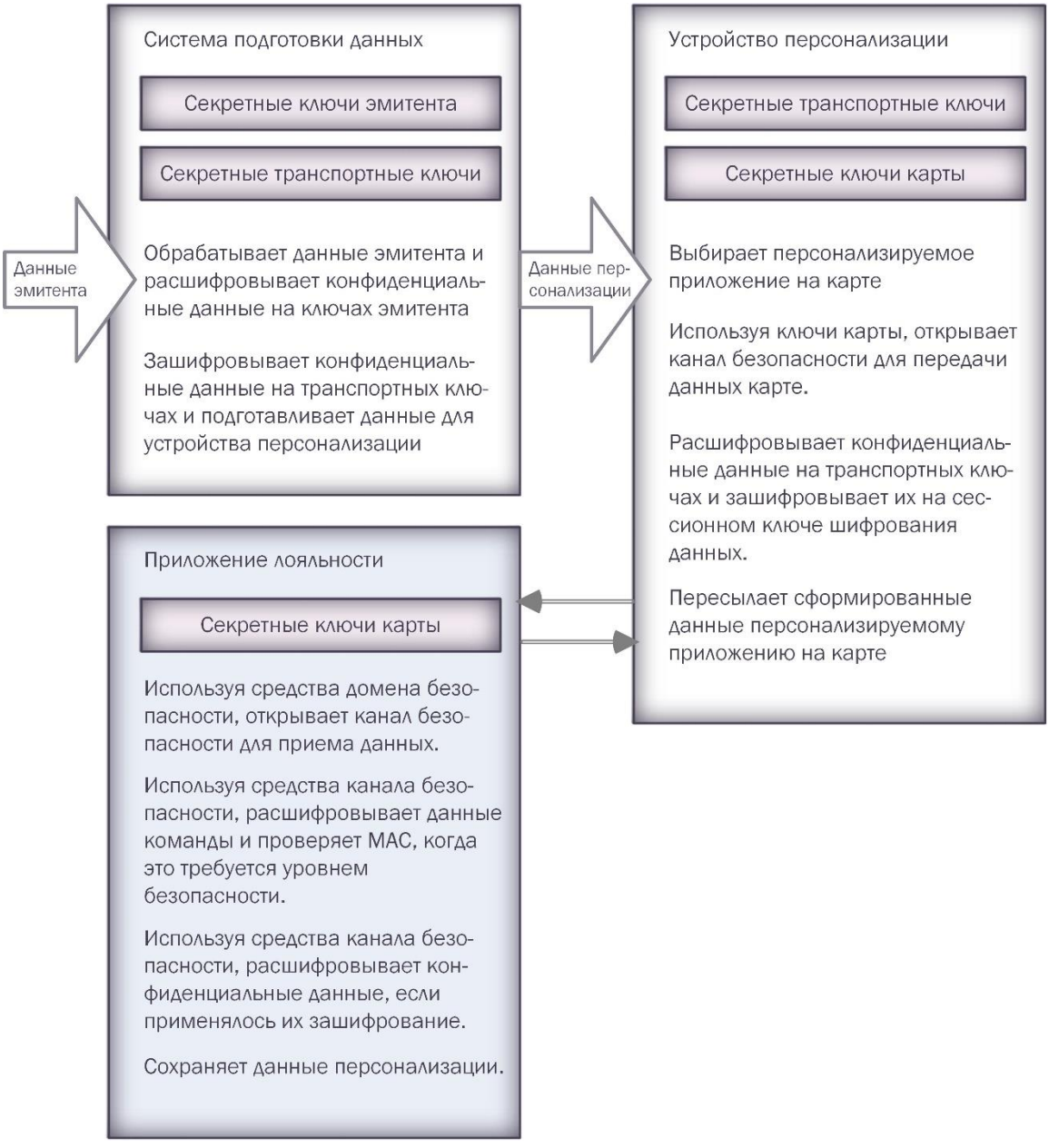


Рис. 7. Непрямой метод персонализации.

Непрямой метод персонализации был определен в ранних спецификациях персонализации EMV. Это стандартный подход, при котором данные эмитента поступают в систему подготовки данных, которая обрабатывает

данные эмитента и расшифровывает конфиденциальные данные на ключах эмитента. После этого система подготовки данных формирует данные для устройства персонализации. Но конфиденциальные данные не могут быть переданы устройству персонализации в открытом виде. Поэтому они зашифровываются на секретных транспортных ключах, которые известны как системе подготовки данных, так и устройству персонализации.

Устройство персонализации, получив данные от системы подготовки данных, выполняет персонализацию карты следующим образом:

- выбирает приложение лояльности на карте и открывает канал безопасности для передачи данных карте
- расшифровывает конфиденциальные данные на транспортных ключах и зашифровывает их на сессионном ключе шифрования конфиденциальных данных
- пересылает сформированные данные персонализируемому приложению лояльности

При таком подходе уровень безопасности, на котором функционирует канал безопасности не так важен. Конечно, рекомендуется использовать проверку целостности данных, но конфиденциальность является избыточной, поскольку конфиденциальные данные зашифрованы на сессионном ключе шифрования конфиденциальных данных.[1]

Второй метод называется прямой метод персонализации (Direct Method). Особенность этого метода (см. рис. 8) в том, что система подготовки данных и устройство персонализации объединены в единый объект (на рисунке он называется системой подготовки данных) и нет необходимости пересылать конфиденциальные данные устройству персонализации, зашифровывая их на транспортных ключах. Поэтому транспортные ключи при таком подходе отсутствуют. Но самое главное, система подготовки данных сама открывает канал безопасности и формирует команды для персонализации приложения лояльности.[2] При этом на систему подготовки данных накладываются определенные обязательства:

- система подготовки данных должна уметь получать данные от карты и их обрабатывать
- системе подготовки данных должны быть известны данные о персонализируемом приложении лояльности

[1] Если установлен уровень безопасности «Конфиденциальность и целостность», то будет выполняться двойное зашифрование конфиденциальных данных.

[2] Физическое устройство персонализации не исключается из системы персонализации, но оно просто выполняет уже сформированные команды.


Рис. 8. Прямой метод персонализации.

В результате того, что система подготовки данных формирует команды для персонализации приложения лояльности, можно отказаться от зашифрования конфиденциальных данных на сессионном ключе шифрования конфиденциальных данных. Действительно, намного проще установить уровень безопасности «Конфиденциальность и целостность» для канала безопасности и все данные передавать в зашифрованном виде. Именно такой подход и продемонстрирован на рис. 8.

Непрямой метод персонализации хорош тем, что позволяет максимально абстрагироваться от особенностей персонализируемой карты. Но у него есть существенный недостаток. По сравнению с прямым методом на персонализацию карты тратится намного больше времени.

Остальная информация из этого раздела является конфиденциальной. Она может быть получена после подписания Соглашения о неразглашении (Non-Disclosure Agreement – NDA). Обратитесь с запросом в СКАНТЕК.

# 5

## Команды аплета

После завершения персонализации аплет полностью готов к работе с учетом требований эмитента. В аплете реализована команда чтения данных лояльности с возможностью их офлайновой или онлайновой аутентификации. Информация лояльности предоставляется в виде сертификата данных лояльности, полученном на секретном RSA-ключе эмитента, или в виде данных, подписанных на секретном 3DES-ключе эмитента. Все данные могут быть считаны одной командой, в результате чего обеспечивается высокая скорость обработки транзакции, что принципиально важно при работе по бесконтактному интерфейсу.

Кроме команды чтения данных лояльности в аплете реализована команда получения случайного числа, которая используется в процессе инициализации аплета. Когда инициализация аплета выполнена, эта команда также может использоваться терминалом, если возникнет такая необходимость.

В аплете реализована команда VERIFY, которая предназначена для верификации владельца карты путем предъявления PIN-кода. Для выполнения операций с PIN-кодом на карте аплет лояльности поддерживает специальную команду PIN CHANGE/ UNBLOCK. Эта команда предназначена для установки нового значения PIN-кода и разблокирования PIN-кода (установки счетчика оставшихся попыток предъявлений PIN-кода равным максимальному количеству предъявлений).

Далее приводится описание всех команд аплета лояльности.

Остальная информация из этого раздела является конфиденциальной. Она может быть получена после подписания Соглашения о неразглашении (Non-Disclosure Agreement – NDA). Обратитесь с запросом в СКАНТЕК.

6

# Кодирование элементов данных

В этом разделе описывается кодирование элементов данных, используемых при обработке транзакции лояльности, которые не являются стандартными (не описаны в спецификациях EMV) или могут быть неправильно интерпретированы. Элементы данных приведены в алфавитном порядке. Большинство описанных элементов данных используется независимо от режима выполнения транзакции (контактного или бесконтактного). Если какой-либо элемент данных используется только в бесконтактном режиме, то это специально оговаривается.

Остальная информация из этого раздела является конфиденциальной. Она может быть получена после подписания Соглашения о неразглашении (Non-Disclosure Agreement – NDA). Обратитесь с запросом в СКАНТЕК.

7

# Криптографические алгоритмы

В этой части документа приведено описание криптографических алгоритмов, которые используются для обработки транзакции картой, терминалом и процессинговым центром лояльности. Большинство из этих алгоритмов аналогично алгоритмам, описанным в спецификациях EMV. Но в аплете лояльности используются также и проприетарные алгоритмы, используемые только для обеспечения безопасности системы лояльности.

Далее используются следующие соглашения по определению криптографических операций.

1. Для определения операций зашифрования и расшифрования данных с использованием алгоритма Triple DES используются следующие обозначения:
   - 3DESECB (Data, K) – зашифрование данных Data на ключе K в режиме ECB
   - $3DESECB^{-1}$ (Data, K) – расшифрование данных Data на ключе K в режиме ECB
   - 3DESCBC (Data, K, IV) – зашифрование данных Data на ключе K в режиме CBC с начальным вектором IV
   - $3DESCBC^{-1}$ (Data, K, IV) – расшифрование данных Data на ключе K в режиме CBC с начальным вектором IV
2. Для обозначения операция получения 8-ми байтной подписи данных по алгоритму Triple DES (MAC) используется следующая формула:
   - 3DESMAC (Data, K, IV) – получение подписи данных Data на ключе K в режиме CBC с начальным вектором IV

3. Операции зашифрования и расшифрования данных с использованием алгоритма DES обозначаются следующим образом:
   - DESECB (Data, K) – зашифрование данных Data на ключе K в режиме ECB
   - $DESECB^{-1}$ (Data, K) – расшифрование данных Data на ключе K в режиме ECB
4. Операция получения 8-ми байтной подписи данных по алгоритму DES (MAC) определяется через следующую формулу:
   - DESMAC (Data, K, IV) – получение подписи данных Data на ключе K в режиме CBC с начальным вектором IV
5. Для определения операций зашифрования и расшифрования данных с использованием алгоритма RSA используются следующие обозначения:
   - RSASPRV (Data, Ks) – получение подписи данных Data на секретном ключе Ks (т. е. зашифрование данных на секретном ключе)
   - RSARPUB (Sign, Kp) - восстановление данных из подписи Sign на открытом ключе Kp (т. е. расшифрование данных на открытом ключе)

Остальная информация из этого раздела является конфиденциальной. Она может быть получена после подписания Соглашения о неразглашении (Non-Disclosure Agreement – NDA). Обратитесь с запросом в СКАНТЕК.

8

# Приложения

Этот раздел содержит сведения справочного характера, которые могут использоваться для анализа обмена данными при выполнении транзакции и протекании процессов в терминале и приложении лояльности. Частично эти сведения представлены и других главах документа, но только в этой главе они систематизированы и сведены в таблицы.

## Объекты данных

В приведенной ниже таблице показаны элементы данных, которые используются при выполнении транзакции лояльности (или могут использоваться), и их отображение в объекты данных, которыми обмениваются терминал, приложение лояльности и эмитент. Элементы данных сгруппированы в алфавитном порядке.

В колонках S, F, T и L приведены следующие данные:

- S – источник данных:
  - T – терминал
  - ICC – карта
  - I – эмитент
  - IO – внутренний объект карты
- F – формат данных:
  - b – двоичные данные
  - n – десятичные цифры (по две цифры на байт), которые выровнены по правой границе и дополнены слева нулем
  - cn - десятичные цифры (по две цифры на байт), которые выровнены полевой границе и дополнены справа шестнадцатеричной цифрой F
  - an – алфавитно-цифровые символы (допускаются буквы A – Z в любом регистре и цифры 0 – 9)
  - ans – алфавитно-цифровые символы (допускаются буквы A – Z в любом регистре и цифры 0 – 9) и специальные символы из первой половины таблицы ANSI
- T – тэг объекта данных
- L – длина значения объекта данных.

В таблице цветом выделены строки для следующих объектов данных.

Объекты, которые используются только в PPSE

Опциональные объекты для онлайновой аутентификации

Внутренние объекты карты, используемые для принятия решения

Информация об объектах данных является конфиденциальной. Она может быть получена после подписания Соглашения о неразглашении (Non-Disclosure Agreement – NDA). Обратитесь с запросом в СКАНТЕК.

## Общие коды ошибок

При выполнении любой команды может быть зафиксирована ошибка, которая либо не связана с логикой выполнения команды (касается только синтаксиса), либо не может быть локализована (вернее, локализация которой не выполняется на уровне аплета лояльности, исполняющего команду). Для информирования о таких ошибках используются общие коды ошибок. Общие коды ошибок команд приведены в следующей таблице:

| SW1 | SW2 | Описание |
|---|---|---|
| 0x67 | 0x00 | Некорректная длина данных (в поле Lc или Le) |
| 0x6A | 0x86 | Некорректные параметры команды (P1/P2) |
| 0x6D | 0x00 | Неправильная инструкция (поле INS) |
| 0x6E | 0x00 | Неправильный класс команды (поле CLA) |
| 0x6F | 0x00 | Что-то не так (нет более конкретного объяснения) |

Ошибка «Неправильная инструкция» может возникнуть, если команда в данном состоянии аплета не разрешена. В зависимости от состояния аплета разрешены только определенные команды. В состоянии LOADED разрешены только команды аплета INITIALIZE и GET CHALLENGE. В состоянии INITIALIZED разрешены команды GlobalPlatform для организации канала безопасности (INITIALIZE и EXTERNAL AUTHENTICATE), а также команда STORE DATA. В состоянии PERSONALIZED допускаются все команды, кроме команд INITIALIZE и STORE DATA.

ДЛЯ ЗАМЕТОК