ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 7816-13— 2013

Карты идентификационные

КАРТЫ НА ИНТЕГРАЛЬНЫХ СХЕМАХ

Часть 13

Команды для управления приложениями в мульти-прикладной среде

ISO/IEC 7816-13:2007
Identification cards — Integrated circuit cards — Part 13: Commands for application management in a multi-application environment (IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении» (ВНИИНМАШ) и Техническим комитетом по стандартизации ТК 22 «Информационные технологии» на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013 г. № 1633-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 7816-13:2007 «Карты идентификационные. Карты на интегральных схемах. Часть 13. Команды для управления приложениями в мульти-прикладной среде» (ISO/IEC 7816-13:2007 «Identification cards — Integrated circuit cards — Part 13: Commands for application management in a multi-application environment»).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за идентификацию подобных патентных прав

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2014

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения ... 1
2 Нормативные ссылки ... 1
3 Термины и определения ... 1
4 Сокращения и обозначения ... 2
5 Мульти-прикладная среда и жизненный цикл приложения ... 2
5.1 Мульти-прикладная среда ... 2
5.2 Жизненный цикл приложения ... 3
5.3 Информационный объект «распределение ресурсов памяти» для операционной совместимости ... 5
6 Классификация системы управления картой ... 6
6.1 Шаблон системы управления картой ... 6
6.2 Извлечение шаблона системы управления картой ... 7
7 Команды для управления приложением ... 8
7.1 Команда APPLICATION MANAGEMENT REQUEST ... 8
7.2 Команда LOAD APPLICATION ... 9
7.3 Команда REMOVE APPLICATION ... 10
7.4 Принципы управления приложением ... 11
Приложение А (справочное) Пример управления приложением карты для модели независимых эмитента карты и провайдера приложения ... 12
Приложение В (справочное) Пример практического осуществления управления приложением карты ... 14
Приложение С (справочное) Дополнительные практические примеры управления приложением карты ... 17
Приложение D (справочное) Дополнительные практические примеры управления приложением карты ... 19
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации ... 21
Библиография ... 22

Введение

Настоящий стандарт — один из серии стандартов, описывающих параметры карт на интегральных схемах и их применение для обмена информацией. Данные карты представляют собой идентификационные карты, предназначенные для обмена информацией между внешним источником и интегральной схемой карты. В ходе обмена карта поставляет информацию (результаты вычислений, хранимые данные) и/или изменяет свое содержимое (память данных, память событий).

Пять стандартов из серии ИСО/МЭК 7816 относятся к картам с гальваническими контактами, а три из них определяют электрический интерфейс:

ИСО/МЭК 7816-1 — определяет физические характеристики карт с контактами;

ИСО/МЭК 7816-2 — определяет размеры и расположение контактов;

ИСО/МЭК 7816-3 — определяет электрический интерфейс и протоколы передачи для асинхронных карт;

ИСО/МЭК 7816-10 — определяет электрический интерфейс и ответ на восстановление для синхронных карт;

ИСО/МЭК 7816-12 — определяет электрический интерфейс и рабочие процедуры для USB карт.

Все остальные стандарты серии ИСО/МЭК 7816 не зависят от технологии физического интерфейса. Они применяются к картам, доступ к которым осуществляется при помощи контактов и/или технологии бесконтактной связи:

ИСО/МЭК 7816-4 — определяет организацию, защиту и команды для обмена информацией;

ИСО/МЭК 7816-5 — определяет регистрацию провайдеров прикладных программ;

ИСО/МЭК 7816-6 — определяет элементы данных для межотраслевого обмена;

ИСО/МЭК 7816-7 — определяет команды языка структурированных запросов карты;

ИСО/МЭК 7816-8 — определяет команды, обеспечивающие операции по защите информации;

ИСО/МЭК 7816-9 — определяет команды для управления картами;

ИСО/МЭК 7816-11 — определяет верификацию личности биометрическими методами;

ИСО/МЭК 7816-13 — определяет команды для управления приложениями в мульти-прикладной среде;

ИСО/МЭК 7816-15 — определяет приложение с криптографической информацией.

Стандарты серии ИСО/МЭК 10536 определяют доступ к картам при помощи связи через поверхность терминального оборудования. Стандарты серий ИСО/МЭК 14443 и ИСО/МЭК 15693 определяют доступ к картам при помощи радиочастотной связи. Такие карты известны также как бесконтактные карты.

Международный стандарт ИСО/МЭК 7816-13 подготовлен подкомитетом № 17 «Карты и идентификация личности» совместного технического комитета № 1 ИСО/МЭК «Информационные технологии».

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Карты идентификационные

КАРТЫ НА ИНТЕГРАЛЬНЫХ СХЕМАХ

Часть 13

Команды для управления приложениями в мульти-прикладной среде

Identification cards. Integrated circuit cards.
Part 13. Commands for application management in a multi-application environment

Дата введения — 2015—01—01

1 Область применения

Настоящий стандарт определяет команды для управления приложениями в мульти-прикладной среде. Данные команды охватывают полный жизненный цикл приложений в мульти-прикладной карте на интегральной схеме; команды можно использовать до и после того, как карта будет выдана держателю карты. Настоящий стандарт не распространяется на реализацию внутри карты и/или во внешнем окружении.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты. Для датированных ссылок следует использовать только указанное издание, для недатированных ссылок следует использовать последнее издание указанного документа, включая все поправки:

ИСО/МЭК 7816-4:2005[1)] Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена (ISO/IEC 7816-4:2005, Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange)

ИСО/МЭК 7816-9:2004 Карты идентификационные. Карты на интегральных схемах. Часть 9. Команды для управления картами (ISO/IEC 7816-9:2004, Identification cards — Integrated circuit cards — Part 9: Commands for card management)

ИСО/МЭК 8825-1:2002[2)] Информационная технология. Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования (ISO/IEC 8825-1, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER))

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1

приложение (application): Структуры, элементы данных и программные модули, необходимые для выполнения определенных функций.

[ИСО/МЭК 7816-4]

[1)] Заменен на ИСО/МЭК 7816-4:2013.
[2)] Заменен на ИСО/МЭК 8825-1:2008.

Издание официальное

3.2

провайдер приложения (application provider): Организация, предоставляющая компоненты, которые составляют приложение в карте.

[ИСО/МЭК 7816-4]

3.3 **платформа карты** (card platform): Элемент на карте, отвечающий за базовые функции карты.

3.4 **приложение для управления картой** (card manager application): Приложение карты, которое обеспечивает функционирование системы управления приложениями и контроль за распределением ресурсов карт.

4 Сокращения и обозначения

В настоящем стандарте применяют следующие сокращения:

AID — идентификатор приложения (application identifier);

APP — приложение (application);

DF — назначенный файл (dedicated file);

DO — информационный объект (data object);

ICC — карта на интегральной схеме (integrated circuit card);

P1—P2 — байты параметров (parameter bytes) (указаны для ясности, тире не является существенным);

RID — зарегистрированный идентификатор провайдера приложения (registered application provider identifier).

5 Мульти-прикладная среда и жизненный цикл приложения

5.1 Мульти-прикладная среда

Мульти-прикладная среда в контексте настоящего стандарта имеет следующие характеристики:

a) приложение — это однозначно адресуемый набор функциональных возможностей на мульти-прикладной карте, которые обеспечивают хранение данных и вычислительные услуги;

b) приложение может быть добавлено на карту до или после выдачи карты держателю;

c) на карту можно добавить более одного приложения;

d) платформа карты обеспечивает механизмы для управления ресурсами карты, например, памятью,

e) платформа карты обеспечивает механизмы создания границ зоны безопасности для каждого приложения для предотвращения несанкционированного взаимодействия и нарушения безопасности какого-либо другого приложения на карте;

f) провайдер приложения — это организация, которая предоставляет услуги держателю карты, используя приложение карты, и отвечает за работу этого приложения;

g) провайдер приложения на карте может не быть эмитентом карты;

h) жизненный цикл приложения не зависит от жизненного цикла какого-либо другого приложения на той же карте;

i) жизненный цикл приложения не зависит от жизненного цикла карты, за исключением случая, когда карта находится в состоянии завершения жизненного цикла по ИСО/МЭК 7816-9;

j) все приложения должны быть, как минимум, выбираемыми с использованием команды SELECT при указании их AID в качестве имени DF, как определено в ИСО/МЭК 7816-4;

k) приложение для управления картой должно присутствовать, быть уникальным и выбираемым, используя команду SELECT, при указании его AID в качестве имени DF. Остальные приложения на карте могут предлагать функциональные возможности по управлению приложениями;

l) значение AID по умолчанию для приложения для управления картой — "E8 28 BD 08 0D".

На рисунке 1 показано концептуальное представление возможной структуры мульти-прикладной IC карты.

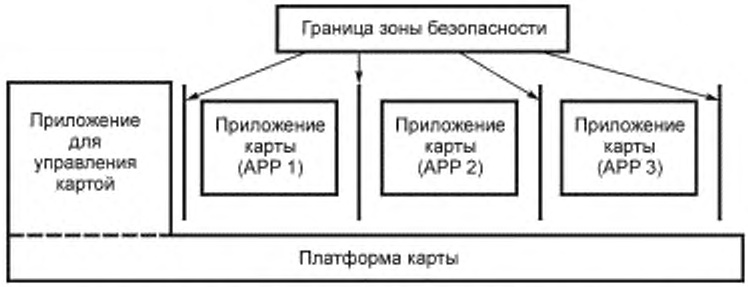


Рисунок 1 — Возможная структура мульти-прикладной карты

5.2 Жизненный цикл приложения

Состояние жизненного цикла должно быть связано с каждым приложением.

Приложение может использовать состояние жизненного цикла в комбинации с атрибутами секретности для того, чтобы убедиться, что любая операция, которую оно выполняет, соответствует политике безопасности этого приложения. Приложение для управления картой должно обеспечивать траекторию перехода жизненного цикла от состояния «Не существует» до «Рабочего Активированного» состояния.

Следующие команды инициируют переходы между состояниями жизненного цикла:

- APPLICATION MANAGEMENT REQUEST[1];
- LOAD APPLICATION[2];
- REMOVE APPLICATION[3].

На рисунке 2 показаны концептуальное представление состояний жизненного цикла и команды, которые активизируют переход в каждое из состояний. Диаграмма показывает только устойчивые (постоянные) состояния приложения, которые можно достигнуть при завершении перехода жизненного цикла. Остальные, промежуточные, состояния могут существовать во время перехода жизненного цикла (например, из состояния «Не существует» в состояние «Создание»), но при этом они не сохраняются, если обработка прерывается.

[1] ЗАПРОС НА УПРАВЛЕНИЕ ПРИЛОЖЕНИЕМ.
[2] УСТАНОВИТЬ ПРИЛОЖЕНИЕ.
[3] УДАЛИТЬ ПРИЛОЖЕНИЕ.

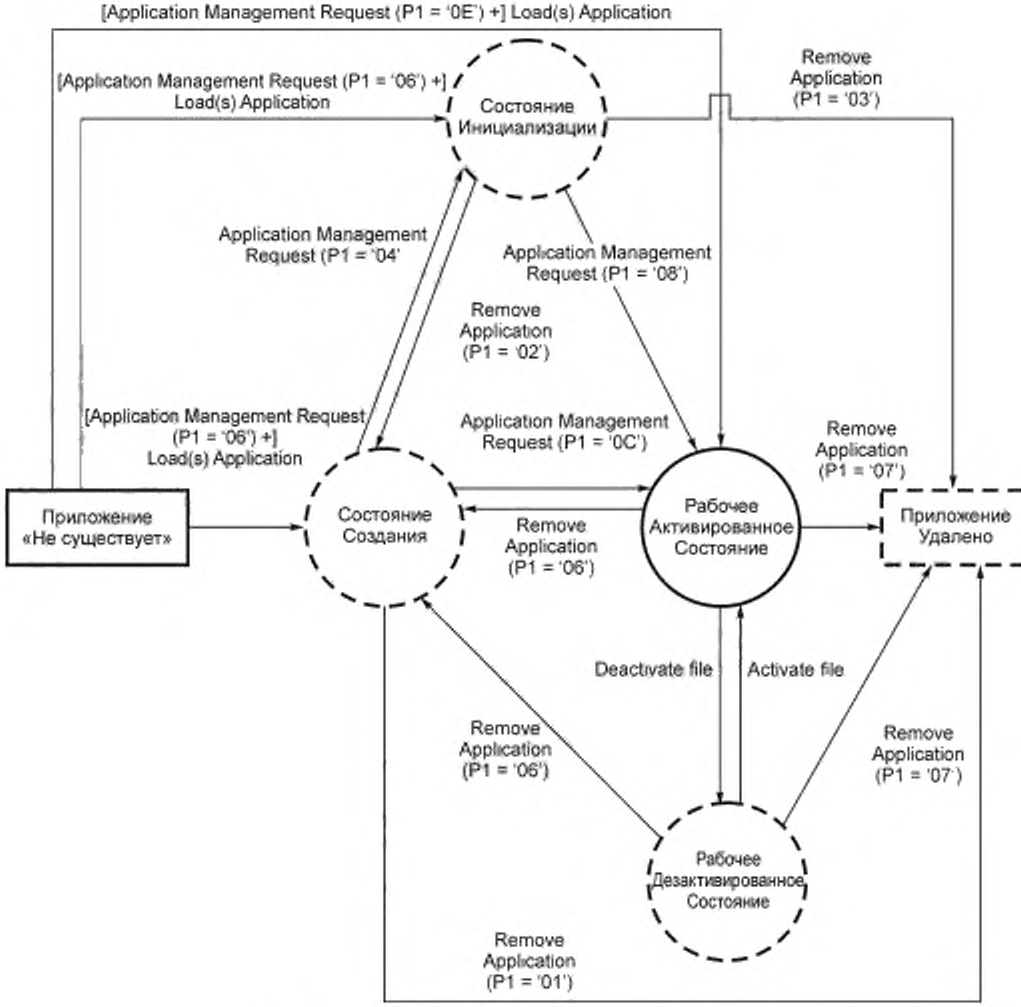


Рисунок 2 — Диаграмма жизненного цикла приложения

Примечание 1 — Диаграмма говорит о следующем: например, после выполнения команд APPLICATION MANAGEMENT REQUEST (P1 = '0E') и LOAD APPLICATION приложение находится в Рабочем Активированном Состоянии жизненного цикла, т.е. выполняемом и выбираемом.

Примечание 2 — Прямоугольники представляют состояния памяти карты, а окружности представляют состояния жизненного цикла приложения. Пунктирные окружности представляют дополнительные состояния жизненного цикла приложения.

Примечание 3 — Команды ACTIVATE FILE и DEACTIVATE FILE определены в ИСО/МЭК 7816-9.

Состояния жизненного цикла приложения определены в таблице 1.

Кодирование состояний жизненного цикла должно соответствовать кодированию байта состояний жизненного цикла (байт LCS) по ИСО/МЭК 7816-4.

Таблица 1 — Состояния жизненного цикла приложения

Приложение «Не существует»	Приложение (с точки зрения приложения для управления картой) не присутствует
Состояние Создания	Приложение (с точки зрения приложения для управления картой) присутствует, не выполняемое и не выбираемое
Состояние Инициализации	Приложение присутствует, выполняемое с ограничением по функционированию и не выбираемое
Рабочее Активированное Состояние	Приложение присутствует, выполняемое и выбираемое
Рабочее Дезактивированное Состояние	Приложение присутствует, выполняемое с ограничением по функционированию, а команда SELECT возвращает предупреждение, что приложение дезактивированное
Приложение Удалено	Приложение не присутствует, не выбираемое и не выполняемое. Отведенные ранее ресурсы памяти могут быть только частично освобождены и использоваться повторно
- Некоторые платформы карт могут иметь дополнительные специфичные состояние жизненного цикла. Описание дополнительных состояний выходит за рамки настоящего стандарта. Если карта поддерживает дополнительные состояния жизненного цикла и переходы состояний, то они не должны мешать состояниям жизненного цикла и переходам между состояниями, описанным на рисунке 2. - Состояния, выделенные курсивом, представляют собой состояния памяти карты. Состояния, обозначенные нормальным шрифтом, представляют собой состояния жизненного цикла приложения.	

5.3 Информационный объект «распределение ресурсов памяти» для операционной совместимости

Шаблон «распределение ресурсов памяти» (тег "7F65"), описывающий распределение ресурсов памяти в приложении, может быть связан с каждым приложением.

В таблице 2 определены информационные объекты «распределение ресурсов памяти» для каждого типа памяти: постоянное запоминающее устройство и энергозависимая память, где:

- резервная память — это объем памяти, отведенный исключительно для приложения;
- квота памяти — это максимальный объем памяти, который приложение может запросить.

Информационный объект «распределение ресурсов памяти» представляет собой объем ресурсов памяти, отсчитываемый в байтах и кодированный как целое число, см. ИСО/МЭК 8825-1.

Таблица 2 — Информационный объект «распределение ресурсов памяти»

Тег	Описание	Требование
'80'	Объем резервной памяти в постоянной памяти для кода приложения. Если разделения между кодом и данными не требуется, то '80' должен использоваться для указания зарезервированного объема постоянного запоминающего устройства для кода приложения и данных	Обязательное
'81'	Объем зарезервированной энергозависимой памяти во время выбора приложения для данных приложения	Дополнительное
'82'	Объем зарезервированного постоянного запоминающего устройства для данных приложения. Если '82' не присутствует, то '80' указывает суммарный объем постоянного запоминающего устройства для кода приложения и данных	Дополнительное
'83'	Объем квоты памяти постоянного запоминающего устройства для кода приложения. Если разделения между кодом и данными не требуется, то '83' должен использоваться для указания квоты памяти постоянного запоминающего устройства для кода приложения и данных	Дополнительное

Окончание таблицы 2

Тег	Описание	Требование
'84'	Объем квоты памяти энергозависимой памяти во время выбора приложения для данных приложения	Дополнительное
'85'	Объем квоты памяти постоянной памяти для данных приложения. Если '85' не присутствует, то '85' указывает суммарный объем постоянного запоминающего устройства для кода приложения и данных	Дополнительное
- В данном контексте ИСО/МЭК СТК1/ПК 17 зарезервировал прочие информационные объекты контекстно-зависимого класса (первый байт от '80' до 'BF').		

При использовании значений информационного объекта «распределение ресурсов памяти» следует применять следующие правила:

- распределение резервной памяти приложению уменьшает ресурсы памяти, доступные для других приложений на карте;
- распределение квоты памяти приложению не уменьшает ресурсы памяти, доступные для других приложений на карте;
- значение квоты памяти больше или равно значению резервной памяти;
- во время успешного создания приложения (например, при переходе из состояния «Не существует» в Рабочее Активированное состояние) объем памяти, выделенный этому приложению, загружается в первую очередь за счет резервной памяти, предназначенной для этого приложения, до тех пор, пока она не будет полностью исчерпана. Когда резервная память приложения будет исчерпана, объем выделенной памяти будет уменьшать ресурсы памяти, доступные для других приложений на карте, до тех пор, пока он не превысит квоту памяти этого приложения. Когда квота памяти будет превышена или ресурсы памяти, доступные на карте в данный момент, будут исчерпаны, то при создании приложения будет сбой;
- во время успешного удаления приложения (т.е. при переходе в состояние «Приложение Удалено») ресурсы памяти, доступные для других приложений на карте, расширяются за счет фактически освобожденного объема памяти, и каждая неиспользованная часть резервной памяти перераспределяется для ресурсов памяти, доступных для других приложений на карте.

6 Классификация системы управления картой

6.1 Шаблон системы управления картой

Шаблон системы управления картой (тег '7F64') должен присутствовать. В таблице 3 определено содержание шаблона системы управления картой.

Таблица 3 — Шаблон системы управления картой

Тег	Длина/Формат	Описание	Требование
'80'	2 байта	Функциональные возможности управления картой, поддерживаемые картой: значением является комбинация бит, определенных в таблицах 4 и 5	Обязательное
'81'	Переменная	Наименование и версия схемы управления картой: значение идентификатора объекта (см. ИСО/МЭК 8825-1), указывающее наименование и версию схемы (основную и неосновную), используемую для управления картой и ее приложениями	Обязательное
'82'	Переменная	Индикатор процедуры идентификации карты: значение идентификатора объекта (см. ИСО/МЭК 8825-1), указывающее процедуру, используемую для однозначной идентификации карты. Он определяет, как осуществить доступ к локальному идентификатору на карте (например, серийному номеру ICC) и является ли этот идентификатор глобально уникальным	Дополнительное

Окончание таблицы 3

Тег	Длина/Формат	Описание	Требование
'4F'	Переменная	AID приложения для управления картой: идентификатор приложения для выбора приложения для управления картой, если его значение отличается от 'E8 28 BD 08 0D'	Дополнительное
- В данном контексте ИСО/МЭК СТК 1/ПК 17 зарезервировал остальные информационные объекты контекстно-зависимого класса (первый байт от '80' до 'BF').			

Таблица 4 — Функциональные возможности управления картой: Первый байт

b8	b7	b6	b5	b4	b3	b2	b1	Значение поддерживаемых переходов между состояниями жизненного цикла
-	-	-	-	-	-	-	1	От «Не существует» до «Создание»
-	-	-	-	-	-	1	-	От «Создание» до «Инициализация»
-	-	-	-	-	1	-	-	От «Инициализация» до «Рабочее Активированное»
-	-	-	-	1	-	-	-	От «Создание» до «Рабочее Активированное»
-	-	-	1	-	-	-	-	От «Не существует» до «Рабочее Активированное»
-	-	1	-	-	-	-	-	От «Рабочее Активированное» до «Рабочее Дезактивированное»
-	1	-	-	-	-	-	-	От «Рабочее Дезактивированное» до «Рабочее Активированное»
1	-	-	-	-	-	-	-	От «Рабочее Активированное» до «Приложение Удалено»

Таблица 5 — Функциональные возможности управления картой: Второй байт

b8	b7	b6	b5	b4	b3	b2	b1	Значение поддерживаемых переходов между состояниями жизненного цикла
0	0	0	-	-	-	-	1	От «Создание» до «Приложение Удалено»
0	0	0	-	-	-	1	-	От «Инициализация» до «Приложение Удалено»
0	0	0	-	-	1	-	-	От «Инициализация» до «Создание»
0	0	0	-	1	-	-	-	От «Рабочее Активированное» до «Создание»
0	0	0	1	-	-	-	-	От «Рабочее Дезактивированное» до «Приложение Удалено»
- Любые другие значения зарезервированы ИСО/МЭК СТК1/ПК 17 для использования в будущем.								

6.2 Извлечение шаблона системы управления картой

Извлечение шаблона системы управления картой использует услуги карты, не зависимые от приложения, по ИСО/МЭК 7816-4.

Порядок, в котором различные процедуры извлечения, определенные в настоящем подразделе, должны быть опробованы, в настоящем стандарте не определен. Если все процедуры, описанные ниже, не в состоянии вернуть шаблон системы управления картой, то это означает, что карта не соответствует настоящему стандарту.

Можно применить две процедуры для извлечения шаблона системы управления картой, когда выбран MF или неявно выбираемый DF приложения:

- чтение EF.ATR, где DO '7F64' может присутствовать;
- использование команды GET DATA с P1—P2, установленными в '7F64', которая может вернуть шаблон системы управления картой в поле данных ответа.

Другие процедуры могут применяться и состоять из выбора приложения с AID 'E8 28 BD 08 0D', за которым следует команда GET DATA с P1—P2, установленными в '7F64', которая может вернуть шаблон системы управления картой в поле данных ответа.

7 Команды для управления приложением

После выбора приложения для управления картой и необязательной процедуры аутентификации процедура управления для приложения на карте является результатом использования одной или нескольких из трех следующих команд:

- команды APPLICATION MANAGEMENT REQUEST;
- команды LOAD APPLICATION;
- команды REMOVE APPLICATION.

Приложение для управления картой должно поддерживать, как минимум, первые две команды.

Если приложение для управления картой поддерживает команду, определенную в настоящем разделе, то, по крайней мере, одна опция команды должна поддерживаться.

Команда для управления приложением может быть выполнена, только если состояние защиты удовлетворяет условиям секретности, которые определены приложением для управления картой.

7.1 Команда APPLICATION MANAGEMENT REQUEST

Команда APPLICATION MANAGEMENT REQUEST запускает методику управления приложением. Приложение для управления картой проверяет информацию о запросе на управление приложением, присутствующую в поле данных команды. Данная команда может следовать за командой LOAD APPLICATION, описанной в 7.2. Если поддерживается управление ресурсами памяти, то распределение ресурсов памяти для приложения, как описано в шаблоне распределения ресурсов памяти (тег '7F65') должно соответствовать правилам, определенным в 5.3.

Таблица 6 — Пара команда-ответ APPLICATION MANAGEMENT REQUEST

CLA	По ИСО/МЭК 7816-4
INS	'40' или '41'
P1	Контроль состояния жизненного цикла приложения в соответствии с таблицей 7
P2	Контроль управления приложением в соответствии с таблицей 8
Поле L_c	Число байт в поле данных команды
Поле данных	Информация о запросе на управление приложением, формат и содержание которой неявно известны приложению для управления (INS = '40') или закодированы в следующем информационном объекте (INS = '41'): AID (тег '4F') целевого приложения (обязательно); Распределение ресурсов памяти (тег '7F65'); Один или несколько блок(ов) цифровой подписи (тег '7F2D'), содержащий(е) DO цифровой подписи (тег '9E') и возможно дальнейшие DO, например, DO значения хэш (тег '90') с хэш кодом приложения;
Поле L_e	Отсутствует для кодирования $N_e = 0$, присутствует для кодирования $N_e > 0$

Поле данных	Дополнительная информация или отсутствует
SW1-SW2	См. ИСО/МЭК 7816-4:2005, таблицы 6 и 7 в соответствующих случаях, например '6982', '6985'
- Информация о запросе на управление приложением может содержать и другие информационные объекты, например, номер идентификации эмитента (тег '42'), ссылка на файл (тег '51') или произвольные данные (тег '53' или '73'); - Кодирование блока цифровой подписи (тег '7F3D') выходит за рамки настоящего стандарта.	

Таблица 7 — Контроль искомого состояния жизненного цикла приложения в P1

b8	b7	b6	b5	b4	b3	b2	b1	Значение
0	0	0	0	0	0	0	0	Информация не предоставлена
0	0	0	0	0	0	1	0	Переход из состояния «Не существует» в состояние «Создание»
0	0	0	0	0	1	0	0	Переход из состояния «Создание» в состояние «Инициализация»
0	0	0	0	0	1	1	0	Переход из состояния «Не существует» в состояние «Инициализация»

Окончание таблицы 7

b8	b7	b6	b5	b4	b3	b2	b1	Значение
0	0	0	0	1	0	0	0	Переход из состояния «Инициализация» в состояние «Рабочее Активированное»
0	0	0	0	1	1	0	0	Переход из состояния «Создание» в состояние «Рабочее Активированное»
0	0	0	0	1	1	1	0	Переход из состояния «Не существует» в состояние «Рабочее Активированное»
- Любые другие значения зарезервированы ИСО/МЭК СТК1/ПК 17 для использования в будущем.								

Таблица 8 — Контроль управления приложением в P2

b8	b7	b6	b5	b4	b3	b2	b1	Значение
0	0	0	0	0	0	0	0	Информация не предоставлена
0	0	0	0	0	0	0	1	Проверка запроса на управление приложением
0	0	0	0	0	0	1	0	Фиксация запроса на управление приложением
0	0	0	0	0	0	1	1	Проверка и фиксация запроса на управление приложением
- Любые другие значения зарезервированы ИСО/МЭК СТК1/ПК 17 для использования в будущем.								

7.2 Команда LOAD APPLICATION

Команда LOAD APPLICATION пересылает приложение карте. Приложение может быть разделено на несколько компонентов, а каждый компонент может быть разделен на несколько блоков для передачи в карту. Каждая команда LOAD APPLICATION пересылает в карту один блок. Данная команда может предшествовать команде APPLICATION MANAGEMENT REQUEST, см. 7.1.

Если команда LOAD APPLICATION предшествует команде APPLICATION MANAGEMENT REQUEST, то распределение ресурсов памяти обеспечивается непосредственно предшествующей командой APPLICATION MANAGEMENT REQUEST. Успешное выполнение данной последовательности команд совершает переход жизненного цикла, указанного в непосредственно предшествующей команде APPLICATION MANAGEMENT REQUEST.

Если команда LOAD APPLICATION не предшествует команде APPLICATION MANAGEMENT REQUEST, то распределение ресурсов памяти и установление состояния жизненного цикла приложения в соответствующее значение осуществляется на основе информации, предоставленной последовательностью команд LOAD APPLICATION.

Если поддерживается распределение ресурсов памяти, то объем памяти, выделенный на успешно созданное приложение, должен соответствовать правилам, определенным в 5.3.

Таблица 9 — Пара команда-ответ LOAD APPLICATION

CLA	По ИСО/МЭК 7816-4
INS	'EA' или 'EB'
P1- P2	См. таблицу 10
Поле L_c	Число байт в поле данных команды
Поле данных	Компоненты приложения, формат и содержание которых неявно известны приложению для управления картой (INS = 'EA') или закодированы как индивидуальные информационные объекты (INS = 'EB')
Поле L_e	Отсутствует для кодирования $N_e = 0$, присутствует для кодирования $N_e > 0$

Поле данных	Дополнительная информация или отсутствует
SW1-SW2	См. ИСО/МЭК 7816-4:2005, таблицы 6 и 7 в соответствующих случаях, например '6982', '6985'

Таблица 10 — Порядковый номер или смещение в P1 и P2

P1								P2	Значение
b8	b7	b6	b5	b4	b3	b2	b1		
0	0	0	0	0	0	0	0	00	Информация не предоставлена
-	x	x	x	x	x	x	x	xx	Порядковый номер или смещение
-	0	x	x	x	x	x	x	xx	- Смещение
-	1	x	x	x	x	x	x	xx	- Порядковый номер
0	-	-	-	-	-	-	-	-	Следующий блок
1	-	-	-	-	-	-	-	-	Последний блок

- Если b7 для P1 установлен на 0, то остаток от P1—P2 (четырнадцать бит) кодирует смещение от нуля до 16383, а если b7 для P1 установлен на 1, то остаток от P1—P2 (четырнадцать бит) кодирует порядковый номер команды.

- Если b8 для P1 установлен на 0, то ожидается следующий блок, а если b8 для P1 установлен на 1, то эта команда содержит последний блок.

- Смещение исчисляется в байтах от начала передачи приложения.

- Порядковый номер увеличивается на единицу для каждого блока от начала передачи приложения.

7.3 Команда REMOVE APPLICATION

Команда REMOVE APPLICATION (см. таблицу 11) удаляет приложение и возможно восстанавливает ресурсы памяти, которые были выделены для этого приложения.

Приложение для управления картой проверяет информацию об удалении приложения, когда она присутствует в поле данных команды.

Если поддерживается управление ресурсами памяти, то успешное удаление приложения должно увеличить ресурсы памяти, доступные для приложений на карте, в соответствии с правилами, определенными в 5.3.

Таблица 11 — Пара команда-ответ REMOVE APPLICATION

CLA	По ИСО/МЭК 7816-4
INS	'EC' или 'ED'
P1	Контроль состояния удаления в соответствии с таблицей 12
P2	'00' Информация не предоставлена (любое другое значение зарезервировано для использования в будущем ИСО/МЭК СТК1/ПК 17)
Поле L_c	Отсутствует или число байт в поле данных команды
Поле данных	Отсутствует или информация об удалении приложения, формат и содержание которой неявно известны приложению для управления картой (INS = 'EC') Или информация об удалении приложения, кодированная в следующем информационном объекте (INS = 'ED'): AID (тег '4F') целевого приложения (обязательно); Один или несколько блок(ов) цифровой подписи (тег '7F3D'), содержащий(е) DO цифровой подписи (тег '9E').
Поле L_e	Отсутствует для кодирования $N_e = 0$, присутствует для кодирования $N_e > 0$

Поле данных	Дополнительная информация или отсутствует
SW1-SW2	См. ИСО/МЭК 7816-4:2005, таблицы 6 и 7 в соответствующих случаях, например '6982', '6985'

- Информация об удалении приложения может содержать и другие информационные объекты, например, произвольные данные (тег '53' или '73');

- Кодирование блока цифровой подписи (тег '7F3D') выходит за рамки настоящего стандарта.

Таблица 12 — Контроль состояния удаления в Р1

b8	b7	b6	b5	b4	b3	b2	b1	Значение
0	0	0	0	0	0	0	0	Информация не предоставлена
0	0	0	0	0	0	0	1	Переход из состояния «Создание» в состояние «Приложение Удалено»
0	0	0	0	0	0	1	0	Переход из состояния «Инициализация» в состояние «Создание»
0	0	0	0	0	0	1	1	Переход из состояния «Инициализация» в состояние «Приложение Удалено»
0	0	0	0	0	1	1	0	Переход из состояния «Рабочее (Активированное или Дезактивированное)» в состояние «Создание»
0	0	0	0	0	1	1	1	Переход из состояния «Рабочее (Активированное или Дезактивированное)» в состояние «Приложение Удалено»
- Любые другие значения зарезервированы ИСО/МЭК СТК1/ПК 17 для использования в будущем.								

7.4 Принципы управления приложением

Схема управления картой и/или установки эмитентов карт определяют требуемые тип и число подписей:

- подпись эмитента карты;
- подпись провайдера приложения;
- подпись органа, выдающего схему управления картой.

Карта должна быть способной обеспечить соблюдение данных установок и обрабатывать соответствующие ключи проверки подписей.

Установки, касающиеся управления приложением, принимаемые на взаимной основе эмитентом карты и провайдером приложения, а также их реализация выходят за рамки настоящего стандарта.

Приложение А
(справочное)

Пример управления приложением карты для модели независимых эмитента карты и провайдера приложения

А.1 Введение

Данный пример показывает, как управлять приложением на карте в случае независимых эмитента карты и провайдера приложения. Приняты следующие допущения.

- Приложение можно добавить к карте с помощью независимого провайдера приложения после выпуска карты. Данная модель показана на рисунке А.1;
- Сертификат создания приложения может выпускаться во время онлайн или оффлайн коммуникации.

Примечание — Следующее поколение IC Card System Study Group[1)] (NICSS) использует данную модель.



Рисунок А.1 — Модель независимых эмитента карты и провайдера приложения

А.2 Примеры процедур управления приложением

А.2.1 Случай APR, независимого от CI (удаленный CI): проверка сертификата до установки приложения

a) SELECT приложения с AID 'E8 28 BD 08 0D'.
b) GET DATA для извлечения шаблона системы управления картой (тег '7F64').
c) SELECT приложения для управления картой с AID (тег '4F'), указанным в шаблоне системы управления картой.
d) Взаимная аутентификация.
e) Получение сертификата создания приложения от эмитента карты (онлайн/оффлайн). Сертификат может содержать AID, хэш-значение приложения, подтверждение ID, ID карты и цифровую подпись эмитента карты.
f) APPLICATION MANAGEMENT REQUEST с сертификатом.
g) Установка приложения с помощью LOAD APPLICATION.

А.2.2 Случай удаленного CI: проверка сертификата после установки приложения

a) SELECT приложения с AID 'E8 28 BD 08 0D'.
b) GET DATA для извлечения шаблона системы управления картой (тег '7F64').

[1)] Рабочая группа системы идентификационных карт

c) SELECT приложения для управления картой с AID (тег '4F'), указанным в шаблоне системы управления картой.
d) Взаимная аутентификация.
e) Получение сертификата создания приложения от эмитента карты.
f) APPLICATION MANAGEMENT REQUEST без сертификата для выделения памяти.
g) Установка приложения с помощью LOAD APPLICATION.
h) APPLICATION MANAGEMENT REQUEST с сертификатом.

A.3 Примеры процедур удаления

A.3.1 Случай удаленного CI: проверка сертификата во время удаления приложения

a) SELECT приложения с AID 'E8 28 BD 08 0D'.
b) GET DATA для извлечения шаблона системы управления картой (тег '7F64').
c) SELECT приложения для управления картой с AID (тег '4F'), указанным в шаблоне системы управления картой.
d) Взаимная аутентификация.
e) Получение сертификата удаления приложения от эмитента карты (онлайн/оффлайн). Сертификат может содержать AID, подтверждение ID, ID карты и цифровую подпись эмитента карты.
f) REMOVE APPLICATION с сертификатом.

A.3.2 Случай удаленного CI: проверка сертификата до удаления приложения

a) SELECT приложения с AID 'E8 28 BD 08 0D'.
b) GET DATA для извлечения шаблона системы управления картой (тег '7F64').
c) SELECT приложения для управления картой с AID (тег '4F'), указанным в шаблоне системы управления картой.
d) Взаимная аутентификация.
e) Получение сертификата удаления приложения от эмитента карты.
f) APPLICATION MANAGEMENT REQUEST с сертификатом.
g) REMOVE APPLICATION без сертификата.

Приложение В
(справочное)

Пример практического осуществления управления приложением карты

В.1 Введение

Данный пример показывает двухступенчатую модель создания и активации приложения: вначале установка кода приложения, затем установка и активация экземпляра приложения.

Примечание — Данную модель использует GlobalPlatform (GP).

Приложение составляет код приложения и данные приложения. Код приложения (но не данные приложения) устанавливается в карту с помощью объекта «Load». При инсталляции приложения создается экземпляр объекта «Load» и, возможно, некоторые данные приложения.

В данном примере создание и активация приложения требуют дополнительно:
- предыдущую аутентификацию системы управления приложением для карт (CAMS);
- защиту команд и запросов с помощью безопасного обмена сообщениями;
- проверку сертификатов эмитентов карт.

В.2 Команды для управления приложением

В.2.1 Команда APPLICATION MANAGEMENT REQUEST

Команда APPLICATION MANAGEMENT REQUEST выдается для того, чтобы запустить и выполнить различные шаги для установки объекта «Load» и инициализации и активации экземпляра приложения.

Таблица В.1 — Пара команда-ответ APPLICATION MANAGEMENT REQUEST

CLA	По ИСО/МЭК 7816-4
INS	'40'
P1	Контроль целевого состояния жизненного цикла приложения: см. таблицу В.2
P2	Контроль управления приложением: см. таблицу В.3
Поле L_c	Число байт в поле данных команды
Поле данных	Информация о запросе на управление приложением
Поле L_e	Отсутствует для кодирования $N_e = 0$, присутствует для кодирования $N_e > 0$

Поле данных	Отсутствует или информация о подтверждении управления приложением
SW1-SW2	См. ИСО/МЭК 7816-4:2005, таблицы 6 и 7 в соответствующих случаях, например '6982', '6985'

Параметр P1 в команде APPLICATION MANAGEMENT REQUEST описывает назначение команды и закодирован в соответствии с таблицей В.2.

Таблица В.2 — Контроль целевого состояния жизненного цикла приложения в P1

b8	b7	b6	b5	b4	b3	b2	b1	Значение
0	0	0	0	1	1	0	0	Переход из состояния «Создание» в состояние «Рабочее Активированное»
0	0	0	0	1	0	0	0	Переход из состояния «Инициализация» в состояние «Рабочее Активированное»
0	0	0	0	0	1	0	0	Переход из состояния «Создание» в состояние «Инициализация»
0	0	0	0	0	0	1	0	Переход из состояния «Не Существует» в состояние «Создание»
x	x	x	x	-	-	-	-	RFU

b4 = 1 указывает на активацию приложения, идентифицированного в поле данных команды. Это распространяется на приложение, которое только создано (текущее состояние жизненного цикла — «Создание») или которое уже инициализировано (текущее состояние жизненного цикла — «Инициализация»).

b3 = 1 указывает на инициализацию приложения, идентифицированного в поле данных команды (текущее состояние жизненного цикла — «Создание»).

b2 = 1 указывает на создание приложения, идентифицированного в поле данных команды (текущее состояние жизненного цикла — «Не существует»).

Таблица В.3 — Контроль управления приложением в P2

b8	b7	b6	b5	b4	b3	b2	b1	Значение
0	0	0	0	0	0	0	1	Проверка запроса на управление приложением
0	0	0	0	0	0	1	1	Проверка и фиксация запроса на управление приложением

В данном примере команда APPLICATION MANAGEMENT REQUEST вызывается дважды:

- С b2 = 1 в параметре P1 и P2, установленном на '01', для того, чтобы запустить установку кода приложения (объект «Load»). Поле данных команды содержит идентификационную информацию объекта «Load», идентификационную информацию провайдера приложения, информацию распределения ресурсов памяти объекта «Load», хэш-информацию объекта «Load» и сертификат создания приложения, выпускаемый эмитентом карты. Поле данных ответа не возвращается в ответном сообщении. Следует одна или несколько команд LOAD APPLICATION. При успешном выполнении последней команды LOAD APPLICATION создание запроса на управления приложением неявно фиксируется и состояние жизненного цикла приложения устанавливается в состояние «Создание».

- С комбинацией b4 = 1 и b3 = 1 в параметре P1 и P2, установленном в '03' для того, чтобы синхронизировано установить и активировать экземпляр приложения. Поле данных команды содержит идентификационную информацию об уже установленном объекте «Load», идентификационную информацию экземпляра приложения, информацию распределения ресурсов памяти на экземпляр приложения и сертификат инициализации и активации приложения, выданный эмитентом карты. При успешном выполнении команда состояние жизненного цикла приложения меняется с состояния «Создание» на «Рабочее Активированное». Поле данных ответа может быть возвращено в ответное сообщение. Если имеется, информационное наполнение поля данных ответа содержит длину (кодированную в соответствии с правилами ACH.1, определенными в ИСО/МЭК 8825-1) и значение подтверждения инициализации и активации приложения.

В.2.2 Команда LOAD APPLICATION

Объект «Load» делится на множество блоков: блоки «Load» для передачи в карту. Команда LOAD APPLICATION запускает передачу блока Load в карту. Для передачи объекта «Load» в карту может потребоваться множество команд LOAD APPLICATION.

Таблица В.4 — Пара команда-ответ LOAD APPLICATION

CLA	По ИСО/МЭК 7816-4
INS	'EA'
P1	Порядковый номер самого старшего байта блока Load, см. таблицу В.5
P2	Порядковый номер самого младшего байта блока Load, см. таблицу В.6
Поле L_c	Число байт в поле данных команды
Поле данных	Блок Load
Поле L_e	Отсутствует для кодирования $N_e = 0$, присутствует для кодирования $N_e > 0$

Поле данных	Отсутствует или информация о подтверждении создания приложения
SW1-SW2	См. ИСО/МЭК 7816-4:2005, таблицы 6 и 7 в соответствующих случаях, например '6982', '6985'

Параметры P1 и P2 команды LOAD APPLICATION описывают последовательность блоков Load и кодированы в соответствии с таблицами В.5 и В.6.

Таблица В.5 — Порядковый номер самого старшего байта в P1

b8	b7	b6	b5	b4	b3	b2	b1	Значение
0	1	x	x	x	x	x	x	Дополнительные блоки, порядковый номер самого старшего байта
1	1	x	x	x	x	x	x	Последний блок, порядковый номер самого старшего байта

b8 = 0 указывает, что ожидаются дополнительные блоки Load.

b8 = 1 указывает последний блок Load в последовательности.

b8 = 1 указывает порядковый номер блока Load, закодированного на четырнадцати битах от 0 до 16383.

Таблица В.6 — Порядковый номер самого младшего байта в P2

b8	b7	b6	b5	b4	b3	b2	b1	Значение
x	x	x	x	x	x	x	x	Порядковый номер самого младшего байта

Первая команда LOAD APPLICATION предшествует APPLICATION MANAGEMENT REQUEST для команды создания (b2 в P1 установлен на 1).

Порядковый номер блока Load (младше четырнадцати бит P1-P2) начинается с нуля. Нумерация блока Load строго последовательная и увеличивается на единицу. Карте передаются данные о последнем блоке объекта «Load» (b8 в P1 команды LOAD APPLICATION устанавливается на 1).

Поле данных ответа может быть возвращено в ответном сообщении. Если имеется, информационное наполнение поля данных ответа содержит длину (кодированную в соответствии с правилами ACH.1 по ИСО/МЭК 8825-1) и значение подтверждения создания приложения. Оно присутствует только в поле данных ответа команды LOAD APPLICATION, передающей последний блок Load (b8 в P1 установлен на 1).

Для команд LOAD APPLICATION, отличных от последней команды LOAD APPLICATION, передающей последний блок Load (b8 в P1 установлен на 1), поля данных ответа нет.

В.3 Порядок управления приложением

Типовой порядок управления приложением для создания и активации приложения в данной модели выглядит следующим образом:

a) SELECT приложение с AID 'E8 28 BD 08 0D'.
b) GET DATA для извлечения шаблона системы управления картой (тег '7F64').
c) SELECT приложения для управления картой с AID (тег '4F'), указанным в шаблоне системы управления картой.
d) APPLICATION MANAGEMENT REQUEST для создания с параметрами P1 = '02' и P2 = '01'.
e) Первая команда LOAD APPLICATION с параметрами P1 = '40' и P2 = '00'.
f) Множество команд LOAD APPLICATION с последовательно возрастающими параметрами P1-P2.
g) Последняя команда LOAD APPLICATION с P1 = 'Cx' и P2 = 'yz', где 'xyz' — порядковый номер последнего блока Load (предполагается, что 'xyz' меньше, чем 4095).
h) APPLICATION MANAGEMENT REQUEST для инициализации и активации с P1 = '0C' и P2 = '03'.

Приложение С
(справочное)

Дополнительные практические примеры управления приложением карты

С.1 Введение

Данный пример показывает трехступенчатую модель создания и активации приложения: назначить ресурсы карты, установить код приложения и данные и провести активацию рабочего состояния.

Примечание — Данную модель использует MULTOS.

Начальная команда APPLICATION MANAGEMENT REQUEST обеспечивает доступность ресурсов карты и подготавливает карту для последующих запросов на управление информационным наполнением карты. Далее приложение устанавливается в карту с помощью команды LOAD APPLICATION. Приложение состоит из кода приложения и данных приложения, контрольной информации файла по умолчанию, вхождения файла в каталог, цифровой подписи и блока преобразования ключей. Все это устанавливается в карту как Модуль Установки Приложения. Вторая и окончательная команда APPLICATION MANAGEMENT REQUEST завершает создание приложения и процессы активации, включая проверку авторизаций эмитента карты и цифровую подпись (провайдера услуг приложения) Модуля Установки Приложения.

С.2 Команды для управления приложением

С.2.1 Команда APPLICATION MANAGEMENT REQUEST

Команду APPLICATION MANAGEMENT REQUEST вызывают для инициализации и завершения процессов установки приложения.

Таблица С.1 — Пара команда-ответ APPLICATION MANAGEMENT REQUEST

CLA	По ИСО/МЭК 7816-4
INS	'EA'
P1	Назначение APPLICATION MANAGEMENT REQUEST: см. таблицу С.2
P2	Назначение APPLICATION MANAGEMENT REQUEST: см. таблицу С.3
Поле L_c	Число байт в поле данных команды
Поле данных	Сертификат установки приложения
Поле L_e	Отсутствует для кодирования $N_e = 0$, присутствует для кодирования $N_e > 0$

Поле данных	Отсутствует или Сертификат открытого ключа карты
SW1-SW2	См. ИСО/МЭК 7816-4:2005, таблицы 6 и 7 в соответствующих случаях, например '6982', '6985'

Параметр P1 команды APPLICATION MANAGEMENT REQUEST описывает назначение команды и кодирован в соответствии с таблицей С.2.

Таблица С.2 — Кодирование P1 в команде APPLICATION MANAGEMENT REQUEST

b8	b7	b6	b5	b4	b3	b2	b1	Значение
0	0	0	0	1	1	1	0	Переход из состояния «Не существует» в состояние «Рабочее Активированное»

Параметр P2 команды APPLICATION MANAGEMENT REQUEST описывает назначение команды и кодирован в соответствии с таблицей С.3.

Таблица С.3 — Кодирование P2 в команде APPLICATION MANAGEMENT REQUEST

b8	b7	b6	b5	b4	b3	b2	b1	Значение
0	0	0	0	0	0	0	1	Проверка запроса на управление приложением
0	0	0	0	0	0	1	1	Проверка и фиксирование запроса на управление приложением

С.2.2 Команда LOAD APPLICATION

Модуль Установки Приложения делится для передачи в карту на меньшие Компоненты. Команда LOAD APPLICATION запускает передачу Компонента в карту. Для передачи Модуля Установки Приложения в карту может быть использовано множество команд LOAD APPLICATION.

Таблица С.4 — Пара команда-ответ LOAD APPLICATION

CLA	По ИСО/МЭК 7816-4
INS	'EA'
P1	Самый старший байт порядкового номера блока Load, см. таблицу С.5
P2	Самый младший байт порядкового номера блока Load, см. таблицу С.6
Поле L_c	Число байт в поле данных команды
Поле данных	Блок Load
Поле L_e	Отсутствует для кодирования $N_e = 0$, присутствует для кодирования $N_e > 0$

Поле данных	Отсутствует
SW1-SW2	См. ИСО/МЭК 7816-4:2005, таблицы 6 и 7 в соответствующих случаях, например '6982', '6985'

Параметры P1 и P2 команды LOAD APPLICATION описывают порядковый номер Компонентов и кодированы в соответствии с таблицами С.5 и С.6.

Таблица С.5 — Кодирование P1 в команде LOAD APPLICATION

b8	b7	b6	b5	b4	b3	b2	b1	Значение
0	1	x	x	x	x	x	x	Дополнительные блоки, самый старший байт порядкового номера
1	1	x	x	x	x	x	x	Последний блок, самый старший байт порядкового номера

b8 = 0 указывает, что ожидаются дополнительные блоки Load.

b8 = 1 указывает последний блок Load в последовательности.

b7 = 1 указывает порядковый номер блока Load, закодированного в четырнадцати битах, от 0 до 16383.

Таблица С.6 — Кодирование P2 в команде LOAD APPLICATION

b8	b7	b6	b5	b4	b3	b2	b1	Значение
x	x	x	x	x	x	x	x	Самый младший байт порядкового номера

Первая команда LOAD APPLICATION предшествует команде APPLICATION MANAGEMENT REQUEST.

Порядковый номер блока Load (младшие четырнадцать бит P1—P2) начинается с нуля. Нумерация блока Load строго последовательна и возрастает на единицу. Карте передаются данные последнего блока объекта Load (b8 в P1 установлен на 1).

С.3 Порядок управления приложением

Типовой порядок управления приложением для создания и активации приложения в данной модели выглядит следующим образом:

a) Команда SELECT для выбора приложения с AID 'E8 28 BD 08 0D'.
b) Команда GET DATA для извлечения шаблона системы управления картой (тег '7F64').
c) Команда SELECT для выбора приложения для управления картой.
d) Команда APPLICATION MANAGEMENT REQUEST для проверки запроса на рабочую активацию P1 = '0E' и P2 = '01'.
e) Первая команда LOAD APPLICATION с параметрами P1 = '40' и P2 = '00'.
f) Множество команд LOAD APPLICATION с последовательно возрастающими параметрами P1—P2.
g) Последняя команда LOAD APPLICATION с P1 = 'Cx' и P2 = 'yz', где 'xyz' — порядковый номер последнего блока Load.
h) Команда APPLICATION MANAGEMENT REQUEST для рабочей активации с P1 = '0E' и P2 = '03'.

Приложение D
(справочное)

Дополнительные практические примеры управления приложением карты

Следующий пример показывает использование команды LOAD APPLICATION в качестве оболочки команд для инсталляции приложения. Это позволяет контролировать весь цикл установки, используя правило однократного доступа для команды LOAD APPLICATION, например, внешнюю аутентификацию с необходимым согласованием ключей для безопасного обмена сообщениями. Такая процедура аутентификации может быть выполнена системой управления приложением для карт (CAMS).

Примечание 1 — Последовательность команд может быть отправлена с использованием безопасного обмена сообщениями.

Примечание 2 — Команда-на-выполнение в поле данных команды кодируется без использования безопасного обмена сообщениями.

Таблица D.1 — Пара команда-ответ LOAD APPLICATION

CLA	По ИСО/МЭК 7816-4, бит 5, установленный на 1, указывает, что команда не является последней в цепочке команд
INS	'EB'
P1-P2	'0000'
Поле L_c	Число байт в поле данных команды
Поле данных	Команда-на-выполнение (тег '52') '52'-L-... (команда CREATE FILE (DF))
Поле L_e	Отсутствует

Поле данных	Отсутствует
SW1-SW2	'9000' или специфичные байты состояний

Таблица D.2 — Пара команда-ответ LOAD APPLICATION

CLA	По ИСО/МЭК 7816-4, бит 5, установленный на 1, указывает, что команда не является последней в цепочке команд
INS	'EB'
P1-P2	'0000'
Поле L_c	Число байт в поле данных команды
Поле данных	Команда-на-выполнение (тег '52') '52'-L-... (команда CREATE FILE (EF))
Поле L_e	Отсутствует

Поле данных	Отсутствует
SW1-SW2	'9000' или специфичные байты состояний

Таблица D.3 — Пара команда-ответ LOAD APPLICATION

CLA	По ИСО/МЭК 7816-4, бит 5, установленный на 1, указывает, что команда не является последней в цепочке команд
INS	'EB'
P1-P2	'0000'

Поле L_c	Число байт в поле данных команды
Поле данных	Команда-на-выполнение (тег '52') '52'-L-… (команда UPDATE BINARY)
Поле L_e	Отсутствует

Поле данных	Отсутствует
SW1-SW2	'9000' или специфичные байты состояний

Таблица D.4 — Пара команда-ответ LOAD APPLICATION

CLA	По ИСО/МЭК 7816-4, бит 5, установленный на 0, указывает, что команда является последней в цепочке команд
INS	'EB'
P1-P2	'0000'
Поле L_c	Число байт в поле данных команды
Поле данных	Команда-на-выполнение (тег '52') '52'-L-… (команда ACTIVATE FILE (DF))
Поле L_e	Отсутствует

Поле данных	Отсутствует
SW1-SW2	'9000' или специфичные байты состояний

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 7816-4	IDT	ГОСТ Р ИСО/МЭК 7816-4—2013 «Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена»
ИСО/МЭК 7816-9:2004	IDT	ГОСТ Р ИСО/МЭК 7816-9—2011 «Карты идентификационные. Карты на интегральных схемах. Часть 9. Команды для управления картами»
ИСО/МЭК 8825-1	IDT	ГОСТ Р ИСО/МЭК 8825-1—2003 «Информационная технология. Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1] ISO/IEC 7816 (all parts) Identification cards — Integrated circuit cards
[ИСО/МЭК 7816 (все части) Идентификационные карты — Карты на интегральных схемах]

[2] GlobalPlatform Card specification V2.1.1 or higher, gost.e-ecolog.ru

[3] NICSS Prerequisites Version 1.20, The Next generation IC Card System Study group, April 24.2011, http://www.nicss.or.jp/

[4] Guide to Loading and Deleting Applications, MAO-DOC-REF-008, MAOSCO, http://www.multos.com/

[5] Guide to Generating Application Load Units, MAO-DOC-REF-009, MAOSCO, gost.e-ecolog.ru

УДК 336.77:002:006.354 ОКС 35.240.15 Э46 ОКП 40 8470

Ключевые слова: обработка данных, обмен информацией, идентификационные карты, IC-карты, сообщения, способы защиты, аутентификация

Редактор *Н.А. Аргунова*
Технический редактор *В.Н. Прусакова*
Корректор *М.В. Бучная*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 21.07.2014. Подписано в печать 05.08.2014. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,70. Тираж 47 экз. Зак. 3043.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ» 123995 Москва, Гранатный пер., 4
www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru