ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 7816-9— 2011

Карты идентификационные

КАРТЫ НА ИНТЕГРАЛЬНЫХ СХЕМАХ

Часть 9

Команды для управления картами

(ISO/IEC 7816-9:2004, IDT)

Издание официальное

Москва
Стандартинформ
2018

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 перевода на русский язык англоязычной версии 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 13 декабря 2011 г. № 1008-ст

4 Настоящий стандарт идентичен международному стандарту 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», IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

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

7 ПЕРЕИЗДАНИЕ. Декабрь 2018 г.

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». 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.e-ecolog.ru

© ISO, 2004 — Все права сохраняются
© Стандартинформ, оформление, 2013, 2018

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 Обозначения и сокращения 1
5 Жизненный цикл 1
5.1 Жизненный цикл файла 2
6 Команды для управления картой 3
6.1 Команда СОЗДАТЬ ФАЙЛ (CREATE FILE) 3
6.2 Команда УДАЛИТЬ ФАЙЛ (DELETE FILE) 3
6.3 Команда ДЕЗАКТИВИРОВАТЬ ФАЙЛ (DEACTIVATE FILE) 4
6.4 Команда АКТИВИРОВАТЬ ФАЙЛ (ACTIVATE FILE) 5
6.5 Команда ЗАВЕРШИТЬ ДЕЙСТВИЕ DF (TERMINATE DF) 5
6.6 Команда ЗАВЕРШИТЬ ДЕЙСТВИЕ EF (TERMINATE EF) 6
6.7 Команда ЗАВЕРШИТЬ ИСПОЛЬЗОВАНИЕ КАРТЫ (TERMINATE CARD USAGE) 6
Приложение А (справочное) Примеры атрибутов секретности, используемых для загрузки 8
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 11
Библиография 12

Введение

Серия стандартов ИСО/МЭК 7816 устанавливает требования к параметрам карт на интегральных схемах и их применению в рамках обмена информацией. Данные идентификационные карты предназначены для обмена информацией, основанного на согласованиях между внешним источником и интегральной схемой карты. В результате информационного обмена карта выдает информацию (результат вычислений, хранимые данные) и/или изменяет свое содержимое (память данных, память событий).

В серию стандартов ИСО/МЭК 7816 входят пять стандартов, относящиеся к картам с гальваническими контактами, и три, определяющие 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.

Приведенные ниже стандарты не зависят от технологии физического интерфейса. Они применяются к картам, доступ к которым осуществляется при помощи контактов и/или радиочастоты:

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 для структурированного языка запросов для карты;

ИСО/МЭК 7816-8 — определяет команды, обеспечивающие операции защиты;

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

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

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

ИСО/МЭК 10536 определяет обмен данными при помощи поверхностного действия. ИСО/МЭК 14443 и ИСО/МЭК 15693 определяют доступ при помощи радиочастоты. Такие карты известны как бесконтактные карты.

ИСО/МЭК 7816-9:2004 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 9

Команды для управления картами

Identification cards. Integrated circuit cards. Part 9. Commands for card management

Дата введения — 2013—01—01

1 Область применения

Настоящий стандарт определяет межотраслевые команды для управления картой и файлами. Эти команды охватывают полный жизненный цикл карты, и поэтому некоторые команды могут использоваться до того, как карта будет выдана держателю карты или после того, как истечет срок действия карты.

Настоящий стандарт не распространяется на реализацию обмена данными внутри карты и/или внешнего окружения.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:

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

3 Термины и определения

В настоящем стандарте применен следующий термин с соответствующим определением:

3.1 **безопасный обмен сообщениями** (secure messaging): Совокупность средств криптографической защиты [частей] пары команда-ответ.

[ИСО/МЭК 7816-4, статья 3.39]

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения:

APDU — блок данных прикладного протокола (application protocol data unit);

FCP — контрольные параметры файла (file control parameters);

LCS — состояние жизненного цикла (life cycle status).

5 Жизненный цикл

Состояние жизненного цикла может быть связано с любым объектом в карте и с самой картой. Карта должна использовать состояние жизненного цикла в комбинации с дополнительными атрибута-

* Заменен на ГОСТ ИСО/МЭК 7816-4:2013.

Издание официальное

ми секретности, чтобы определить, находится ли операция над объектом в соответствии с политикой безопасности. Состояние жизненного цикла отражает использование объектов в соответствии со следующими правилами:

- если объект находится в состоянии создания, то к данному объекту не применяются атрибуты секретности;
- если объект находится в состоянии инициализации, то могут применяться любые атрибуты секретности, определенные для данного состояния;
- если объект находится в рабочем состоянии, то должны применяться все соответствующие атрибуты безопасности;
- если объект находится в состоянии завершения жизненного цикла, то значение объекта не должно изменяться, но объект может быть использован, как установлено в его атрибутах секретности, например, он может быть удален.

Переходы между основными состояниями жизненного цикла необратимы и происходят только от состояния создания к состоянию завершения. Кроме того, приложение может определять вторичные этапы жизненного цикла: каждое отдельное состояние может иметь обратимые вторичные состояния. Изменениями управляет карта, и они могут выполняться в предопределенном порядке, отражающем обратимые или необратимые изменения состояний. Следующие команды для управления картой и файлами могут быть использованы для инициализации переходов между состояниями жизненного цикла:

CREATE FILE	ACTIVATE FILE	TERMINATE EF
DELETE FILE	DEACTIVATE FILE	TERMINATE DF
	TERMINATE CARD USAGE	

Команды могут устанавливать значение состояния жизненного цикла, когда они выполняются. Однако карта должна поддерживать целостность этого значения в соответствии с настоящим стандартом.

5.1 Жизненный цикл файла

На рисунке 1 показаны концептуальное представление этапов жизненного цикла файла и команды, которые вызывают переход после успешного выполнения. Однако на данном рисунке не показаны состояния выполнения этих команд (см. ИСО/МЭК 7816-4).

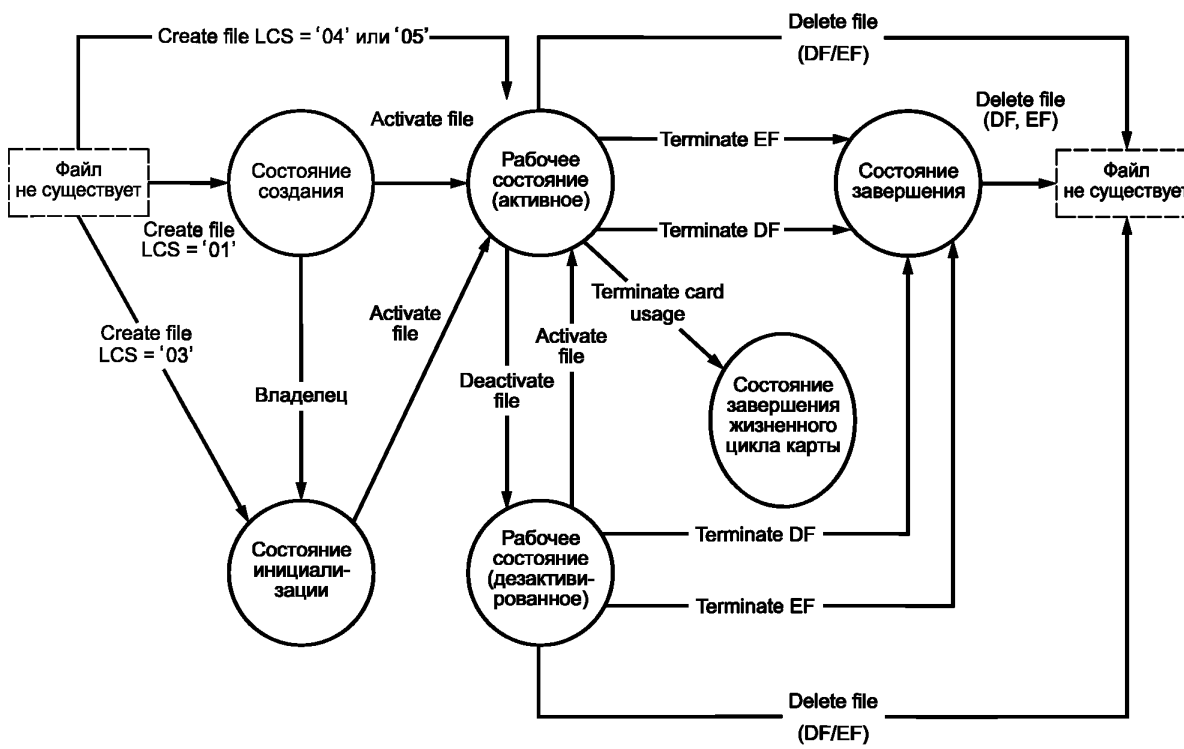

Рисунок 1 — Диаграмма жизненного цикла файла

6 Команды для управления картой

Поддерживание всех команд или всех опций команд не является обязательным для всех карт, удовлетворяющих требованиям настоящего стандарта.

Команды могут быть выполнены только в том случае, если состояние защиты удовлетворяет атрибутам секретности команды.

Для этих команд биты 4 и 3 не имеют смыслового содержания и должны игнорироваться.

Для каждой команды предусмотрен неисчерпывающий список состояний обработки команды (см. также ИСО/МЭК 7816-4).

6.1 Команда СОЗДАТЬ ФАЙЛ (CREATE FILE)

Команда CREATE FILE запускает создание файла (DF или EF), помещенного непосредственно под текущий назначенный файл DF. Команда может выделять память для создаваемого ею файла. Созданный файл должен быть установлен как текущий файл, пока не будет определено иначе.

В случае если в том же файле DF существует более одного элементарного файла EF с данным коротким идентификатором EF, то настоящий стандарт поведение карты не определяет.

Команда может быть выполнена только в том случае, если состояние защиты удовлетворяет атрибутам секретности текущего назначенного файла DF.

Байт дескриптора файла является обязательным. Он показывает, какой из файлов (назначенный DF или элементарный EF) должен быть создан. При этом:

- если создается назначенный файл DF, то должны быть указаны имя DF и/или идентификатор файла;
- если создается элементарный файл EF, то должны быть указаны идентификатор файла и/или короткий идентификатор EF.

Таблица 1 — CREATE FILE, пара команда-ответ

CLA INS P1-P2	Как определено в ИСО/МЭК 7816-4 'E0' '0000' Идентификатор файла и параметры файла закодированы в поле данных команды P1 не равно '00': Байт дескриптора файла P2 Короткий идентификатор EF в битах с 8 по 4; биты с 3 по 1 используются по собственному усмотрению
Поле L_c	Отсутствует для кодирования $N_c = 0$, присутствует для кодирования $N_c > 0$
Поле данных	Шаблон FCP (тег '62') и возможные добавочные шаблоны или отсутствует
Поле L_e	Отсутствует для кодирования $N_e = 0$

Поле данных	Отсутствует
SW1-SW2	См. ИСО/МЭК 7816-4, таблицы 5 и 6, соответствующие значения, например 6982, 6A84, 6A89, 6A8A
Примечание — Если N_c равно нулю, то созданный файл имеет контрольные параметры файла по умолчанию.	

6.2 Команда УДАЛИТЬ ФАЙЛ (DELETE FILE)

Команда DELETE FILE запускает удаление ссылочного элементарного файла EF непосредственно под текущим назначенным файлом DF или назначенного файла DF со всем его поддеревом. После успешного завершения данной команды удаленный файл не может уже быть выбран. Текущим файлом после удаления файла EF является текущий файл DF. Текущим файлом после удаления файла DF является родительский файл DF, если не определено иначе. Ресурсы, ранее выделенные файлу, должны быть возвращены, и память, используемая этим файлом, должна быть установлена в состояние логического удаления.

Удаление файла может дополнительно зависеть от состояния жизненного цикла файла. Главный файл MF не должен быть удален.

Если P1-P2 = ‘0000’ и поле данных команды отсутствует, то команда применяется к файлу, который был выбран командой, выполненной непосредственно перед командой DELETE FILE. Кроме того, если выбранный файл выбирается другим логическим каналом, то выполнение команды прерывается и в качестве ответа возвращается соответствующая ошибка.

Таблица 2 — DELETE FILE, пара команда-ответ

CLA INS P1-P2	Как определено в ИСО/МЭК 7816-4 ‘E4’ ‘0000’ Удаляет текущий файл Другие значения: как определено для команды SELECT (см. ИСО/МЭК 7816-4)
Поле L_c	Отсутствует для кодирования $N_c = 0$, присутствует для кодирования $N_c > 0$
Поле данных	Как определено для команды SELECT (см. ИСО/МЭК 7816-4)
Поле L_e	Отсутствует для кодирования $N_e = 0$

Поле данных	Отсутствует
SW1-SW2	См. ИСО/МЭК 7816-4, таблицы 5 и 6, соответствующие значения, например 6982, 6985

6.3 Команда ДЕЗАКТИВИРОВАТЬ ФАЙЛ (DEACTIVATE FILE)

Команда DEACTIVATE FILE запускает обратимую деактивацию файла. После успешного завершения команды, в дополнение к команде SELECT, только команды ACTIVATE FILE, DELETE FILE, TERMINATE FILE EF и в случае файла DF TERMINATE FILE DF будут разрешены.

Применительно к дезактивированному файлу команда SELECT будет выбирать файл и возвращать SW1-SW2 = ‘6283’ в качестве значения состояния предупреждения: выбранный файл становится недействительным, т. е. дезактивируется.

Если выбран файл EF, то команда будет применяться только к файлу EF и не применяться к родительскому файлу DF.

Если P1-P2 = ‘0000’ и поле данных команды отсутствует, то команда применяется к файлу, который был выбран командой, выполненной непосредственно перед командой DEACTIVATE FILE. Другие значения P1-P2, включая правила, определяющие уникальность идентификатора файла, определены в команде SELECT.

Следует использовать безопасный обмен сообщениями. Если ответный APDU не защищен, то способ проверить, что функция правильно выполняется, в стандартах серии ИСО/МЭК 7816 не определен.

Из соображений безопасности те же функциональные возможности могут быть достигнуты собственными средствами.

Таблица 3 — DEACTIVATE FILE, пара команда-ответ

CLA INS P1-P2	Как определено в ИСО/МЭК 7816-4 ‘04’ ‘0000’ Дезактивирует текущий файл Другие значения: как определено для команды SELECT (см. ИСО/МЭК 7816-4)
Поле L_c	Отсутствует для кодирования $N_c = 0$, присутствует для кодирования $N_c > 0$
Поле данных	Как определено для команды SELECT (см. ИСО/МЭК 7816-4)
Поле L_e	Отсутствует для кодирования $N_e = 0$

Поле данных	Отсутствует
SW1-SW2	См. ИСО/МЭК 7816-4, таблицы 5 и 6, соответствующие значения, например 6982, 6985

6.4 Команда АКТИВИРОВАТЬ ФАЙЛ (ACTIVATE FILE)

Команда ACTIVATE FILE запускает переход файла из одного состояния — или создания, или инициализации, или рабочего состояния (дезактивированного) в другое — действующее (активированное).

Активация корректно созданного файла всегда разрешена. Активация дезактивированного файла может выполняться только в том случае, если состояние защиты удовлетворяет атрибутам секретности, определенным для данного файла для функции активации.

Если ответный APDU не защищен безопасным обменом сообщений, то способ проверить, что функция правильно выполняется, в стандартах серии ИСО/МЭК 7816 не определен.

Если P1-P2 = ‘0000’ и поле данных команды отсутствует, то команда применяется к файлу, который был выбран командой, выполненной непосредственно перед командой ACTIVATE FILE. Другие значения P1-P2, включая правила, определяющие уникальность идентификатора файла, определены в команде SELECT.

Таблица 4 — ACTIVATE FILE, пара команда-ответ

CLA INS P1-P2	Как определено в ИСО/МЭК 7816-4 ‘44’ ‘0000’ Активирует текущий файл Другие значения: как определено для команды SELECT (см. ИСО/МЭК 7816-4)
Поле L_c	Отсутствует для кодирования $N_c = 0$, присутствует для кодирования $N_c > 0$
Поле данных	Как определено для команды SELECT (см. ИСО/МЭК 7816-4)
Поле L_e	Отсутствует для кодирования $N_e = 0$

Поле данных	Отсутствует
SW1-SW2	См. ИСО/МЭК 7816-4, таблицы 5 и 6, соответствующие значения, например 6982, 6985

6.5 Команда ЗАВЕРШИТЬ ДЕЙСТВИЕ DF (TERMINATE DF)

Команда TERMINATE DF запускает необратимый переход файла DF в состояние завершения. После успешного завершения команды файл DF находится в завершенном состоянии и функциональные возможности, доступные из файла DF и его поддерева, сокращаются. Файл DF должен быть выбираемым, и если выбрано значение состояния предупреждения, то SW1-SW2 = ‘6285’ (выбранный файл в состоянии завершения) должно быть возвращено. Дальнейшие возможные действия в стандартах серии ИСО/МЭК 7816 не определены.

Примечание — Назначение файла DF в состоянии завершения — сделать приложение непригодным для держателя карты.

Из соображений безопасности те же функциональные возможности могут быть достигнуты собственными средствами.

Если P1-P2 = ‘0000’ и поле данных команды отсутствует, то команда применяется к файлу, который был выбран командой, выполненной непосредственно перед командой TERMINATE DF. Другие значения P1-P2, включая правила, определяющие уникальность идентификатора файла, определены в команде SELECT.

Следует использовать безопасный обмен сообщениями. Если ответный APDU не защищен безопасным обменом сообщениями, то способ проверить, что функция правильно выполняется, в стандартах серии ИСО/МЭК 7816 не определен.

Таблица 5 — TERMINATE DF, пара команда-ответ

CLA	Как определено в ИСО/МЭК 7816-4
INS	‘E6’
P1-P2	‘0000’ Завершает действие текущего файла DF Другие значения: как определено для команды SELECT (см. ИСО/МЭК 7816-4)

Окончание таблицы 5

Поле L_c	Отсутствует для кодирования $N_c = 0$, присутствует для кодирования $N_c > 0$
Поле данных	Как определено для команды SELECT (см. ИСО/МЭК 7816-4)
Поле L_e	Отсутствует для кодирования $N_e = 0$

Поле данных	Отсутствует
SW1-SW2	См. ИСО/МЭК 7816-4, таблицы 5 и 6, соответствующие значения, например 6982, 6985

Примечание — В командах, где P1-P2 закодированы согласно команде SELECT (см. ИСО/МЭК 7815-4), биты 3 и 4 байта P2 не имеют смыслового содержания и должны игнорироваться.

6.6 Команда ЗАВЕРШИТЬ ДЕЙСТВИЕ EF (TERMINATE EF)

Команда TERMINATE EF запускает необратимый переход заданного файла EF в состояние завершения.

Для завершения файл EF должен быть в активированном или дезактивированном состоянии.

Из соображений безопасности те же функциональные возможности могут быть достигнуты собственными средствами.

Если P1-P2 = '0000' и поле данных команды отсутствует, то команда применяется к файлу, который был выбран командой, выполненной непосредственно перед командой TERMINATE EF. Другие значения P1-P2, включая правила, определяющие уникальность идентификатора файла, определены в команде SELECT.

Таблица 6 — TERMINATE EF, пара команда-ответ

CLA INS P1-P2	Как определено в ИСО/МЭК 7816-4 'E8' '0000' Завершает действие текущего файла EF Другие значения: как определено для команды SELECT (см. ИСО/МЭК 7816-4)
Поле L_c	Отсутствует для кодирования $N_c = 0$, присутствует для кодирования $N_c > 0$
Поле данных	Как определено для команды SELECT (см. ИСО/МЭК 7816-4)
Поле L_e	Отсутствует для кодирования $N_e = 0$

Поле данных	Отсутствует
SW1-SW2	См. ИСО/МЭК 7816-4, таблицы 5 и 6, соответствующие значения, например 6982, 6985

6.7 Команда ЗАВЕРШИТЬ ИСПОЛЬЗОВАНИЕ КАРТЫ (TERMINATE CARD USAGE)

Команда TERMINATE CARD USAGE запускает необратимый переход карты в состояние завершения. Использование данной команды дает неявный выбор файла MF.

Для карт, поддерживающих эту команду, состояние завершения должно показываться в Ответе-на-Восстановление.

После успешного завершения команды карта не должна поддерживать команду SELECT.

Из соображений безопасности те же функциональные возможности могут быть достигнуты собственными средствами.

Примечание — Назначение команды завершения использования карты — сделать карту непригодной для держателя карты.

Следует использовать безопасный обмен сообщениями. Если ответный APDU не защищен безопасным обменом сообщениями, то способ проверить, что функция правильно выполняется, в стандартах серии ИСО/МЭК 7816 не определен.

Таблица 7 — TERMINATE CARD USAGE, пара команда-ответ

CLA INS P1-P2	Как определено в ИСО/МЭК 7816-4 ‘FE’ ‘0000’
Поле L_c	Отсутствует для кодирования $N_c = 0$
Поле данных	Отсутствует
Поле L_e	Отсутствует для кодирования $N_e = 0$

Поле данных	Отсутствует
SW1-SW2	См. ИСО/МЭК 7816-4, таблицы 5 и 6, соответствующие значения, например 6982, 6985

Приложение А
(справочное)

Примеры атрибутов секретности, используемых для загрузки

А.1 Введение

В данном примере показано, как можно контролировать загрузку данных (безопасное скачивание) в карту средствами контроля прав доступа к загружаемому объекту и защиту передаваемых данных с помощью безопасного обмена сообщениями. Загруженные данные могут содержать, например, код, ключи, аплеты.

В примере были сделаны следующие допущения:

- файловая система согласно настоящему стандарту;
- структура команд, жизненный цикл и управление доступом согласно настоящему стандарту;
- текущий файл DF находится уже в рабочем состоянии (LCS = 4);
- данные для загрузки во вспомогательном прозрачном файле 1 (DF/EF в состоянии инициализации (LCS = 3));
- SEID = 2 для LCS = 3 (состояние инициализации) и онлайн коммуникации, присутствует в текущем файле DF;
- SEID = 3 для LCS = 3 (состояние инициализации) и оффлайн коммуникации, присутствует в текущем файле DF;
- SEID = 4 для LCS = 4 (рабочее состояние), присутствует в текущем файле DF;
- данные защищены для аутентификации (и произвольно зашифрованы) при помощи информационных объектов, используемых для безопасного обмена сообщениями;
- в онлайн коммуникации (SEID = 2) асимметричный процесс аутентификации был успешно выполнен ранее, например, при помощи обмена сеансовым ключом, используемого для защиты загрузочных данных посредством безопасного обмена сообщениями. Данные для загрузки защищены при помощи информационного объекта «криптографическая контрольная сумма» и дополнительно при помощи информационного объекта «криптограмма»;
- в оффлайн коммуникации (SEID = 3) данные для загрузки защищены при помощи информационного объекта «цифровая подпись» и дополнительно при помощи информационного объекта «криптограмма»;
- информация авторизации (авторизация держателя сертификата) может быть представлена внутри верифицируемого картой сертификата, связывающего объект загрузки с ключом аутентификации (SEID = 2, онлайн коммуникация) или с ключом цифровой подписи (SEID = 3, оффлайн коммуникация) и с его правами доступа.

А.2 Безопасная загрузка

Безопасная загрузка представлена в описаниях онлайн и оффлайн коммуникаций.

Онлайн коммуникация

1 Выбрать текущий файл DF (SELECT (имя DF = AID)).
2 Установить состояние инициализации для онлайн коммуникации (MSE: RESTORE SEID = 2).
3 Провести внешнюю аутентификацию (проверка сертификата, внешне аутентифицировать).
4 Выбрать файл 1 (SELECT (идентификатор файла)).
5 Загрузить данные в файл (например, WRITE BINARY) с использованием SM, защищенного при помощи информационного объекта «криптографическая контрольная сумма».
6 Провести активацию файла (ACTIVATE FILE).
7 Установить рабочее состояние (MSE: RESTORE SEID = 4).
8 Проверить аутентификацию пользователя (VERIFY (пароль)).
9 Выбрать файл 1 (SELECT (идентификатор файла)).
10 Считать информацию (READ BINARY).

Оффлайн коммуникация

1 Выбрать текущий файл DF (SELECT (DF имя = AID)).
2 Установить состояние инициализации для оффлайн коммуникации (MSE: RESTORE SEID = 3).
3 Провести верификацию сертификата (VERIFY CERTIFICATE).
4 Выбрать файл 1 (SELECT) (идентификатор файла)).
5 Загрузить данные в файл с использованием SM (например, WRITE BINARY), защищенного при помощи информационного объекта «цифровая подпись».
6 Провести активацию файла (ACTIVATE FILE).
7 Установить рабочее состояние (MSE: RESTORE SEID = 4).
8 Проверить аутентификацию пользователя (VERIFY (пароль)).
9 Выбрать файл 1 (SELECT (идентификатор файла)).
10 Считать информацию (READ BINARY).

А.3 Компактный формат кодирования для атрибутов секретности

Компактный формат кодирования иллюстрирует, что доступ в рабочем состоянии может отличаться от доступа в состоянии инициализации.

Онлайн коммуникация

Если команды WRITE BINARY и (после успешного завершения) ACTIVATE FILE разрешены в состоянии инициализации, а команда READ BINARY в рабочем состоянии для определенного состояния защиты, то кодирование AM байта и SC байтов будет, как указано далее.

Состояние инициализации

- AM байт (ACTIVATE FILE (бит 5 = 1), WRITE BINARY (бит 3 = 1));
- SC байт 1 (все состояния (бит 8=1), безопасный обмен сообщениями для ACTIVATE FILE (бит 7 = 1));
- SC байт 2 (все состояния (бит 8=1), внешняя аутентификация и безопасный обмен сообщениями для WRITE BINARY (бит с 7 по 6 = 11).

Рабочее состояние

- AM байт (READ BINARY (бит 1 = 1));
- SC байт (аутентификация пользователя (бит 5 = 1))
  - или биты с 4 по 1 кодируют идентификатор SE (2 как 0010, 4 как 0100) в байтах SC;
  - или соответствующий SE идентифицируется как текущий SE (0000); в данном случае атрибуты секретности кодируются в расширенном формате.

Оффлайн коммуникация

Если команды WRITE BINARY и (после успешного завершения) ACTIVATE FILE разрешены в состоянии инициализации, а команда READ BINARY разрешена в рабочем состоянии для определенного состояния защиты, то кодирование AM байта и SC байтов будет, как указано далее.

Состояние инициализации

- AM байт (ACTIVATE FILE (бит 5 = 1), WRITE BINARY (бит 3 = 1));
- SC байт 1 (все состояния (бит 8 = 1), безопасный обмен сообщениями для ACTIVATE FILE (бит 7 = 1));
- SC байт 2 (все состояния (бит 8 = 1), безопасный обмен сообщениями для WRITE BINARY (бит 7 = 1).

Рабочее состояние

- AM байт (READ BINARY (бит 1 = 1));
- SC байт (аутентификация пользователя (бит 5 = 1))
  - или биты с 4 по 1 кодируют идентификатор SE (3 как 0011, 4 как 0100) в байтах SC;
  - или соответствующий SE идентифицируется как текущий SE (0000); в данном случае атрибуты секретности кодируются в расширенном формате.

А.4 Расширенный формат кодирования для атрибутов секретности

Онлайн коммуникация

Если команды WRITE BINARY и (после успешного завершения) ACTIVATE FILE разрешены в состоянии инициализации, а команда READ BINARY в рабочем состоянии для определенного состояния защиты, то кодирование информационных объектов AM и информационных объектов SC может быть, как указано далее.

Состояние инициализации

- информационный объект AM 1 передает AM байт (WRITE BINARY (бит 3 = 1));
- информационный объект SC 1 передает AT, включая информационный объект «ссылка на ключ» и информационный объект «квалификатор использования CRT» для внешней аутентификации (бит 8 = 1);
- информационный объект SC 2 передает CCT, включая информационный объект «ссылка на ключ» и информационный объект «использование CRT» для безопасного обмена сообщениями (бит с 5 по 6 = 11);
- информационный объект AM 2 передает AM байт (ACTIVATE FILE (бит 5 = 1));
- информационный объект SC 3 передает CCT, включая информационный объект «ссылка на ключ» и информационный объект «использование CRT» для безопасного обмена сообщениями (бит с 5 по 6 = 11).

Рабочее состояние

- информационный объект AM передает AM байт (READ BINARY (бит 1 = 1));
- информационный объект SC передает AT, включая информационный объект «ссылка на ключ» и информационный объект «квалификатор использования CRT», который показывает аутентификацию пользователя (бит 4 = 1).

Соответствующий SE идентифицируется как текущий SE (биты с 4 по 1 = 0000). В этом случае атрибуты секретности кодируются в расширенном формате.

Оффлайн коммуникация

Если команды WRITE BINARY и (после успешного завершения) ACTIVATE FILE разрешены в состоянии инициализации, а команда READ BINARY в рабочем состоянии для определенного состояния защиты, то кодирование информационных объектов AM и информационных объектов SC может быть, как указано далее.

Состояние инициализации

- информационный объект AM 1 передает AM байт (WRITE BINARY (бит 3 = 1), ACTIVATE FILE (бит 5 = 1));
- информационный объект SC 1 передает DST, включая информационный объект «ссылка на ключ» и информационный объект «квалификатор использования CRT» для безопасного обмена сообщениями (биты с 5 по 6 = 11).

Рабочее состояние

- информационный объект AM передает AM байт (READ BINARY (бит 1 = 1));
- информационный объект SC передает AT, включая информационный объект «ссылка на ключ» и информационный объект «квалификатор использования CRT», который показывает аутентификацию пользователя (бит 4 = 1).

Соответствующий SE идентифицируется как текущий SE. В этом случае атрибуты секретности кодируются в расширенном формате.

A.5 Кодирование соответствующей среды безопасности

SEID = 2 внутри шаблона ('7B')

{'80' — L — '02'} — {'8A' — L — '03'} — {'A4' — L — {'83' — L — Ссылка на ключ} — {'95' — '01' — '80'} — {'5F4B' — L — Авторизация держателя сертификата}} — {'B4' — L — {'83' — L — Ссылка на ключ} — {'95' — '01' — '30'}}

SEID = 3 внутри шаблона ('7B')

{'80' — L — '03'} — {'8A' — L — '03'} — {'B6' — L — {'83' — L — Ссылка на ключ} — {'95' — '01' — '30'}

SEID = 4 внутри шаблона ('7B')

{'80' — L — '04'} — {'8C' — L — '04'} — {'A4' — L — {'83' — L — Ссылка на ключ} — {'95' — '01' — '08'}

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 7816-4:2005	IDT	ГОСТ Р ИСО/МЭК 7816-4—2013 «Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта: - IDT — идентичный стандарт.		

Библиография

[1] ISO/IEC 7816 (all parts) Identification cards — Integrated circuit cards (Карты идентификационные. Карты на интегральных схемах)

[2] ISO/IEC 10536 (all parts) Identification cards — Contactless integrated circuit(s) cards — Close-coupled cards (Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты поверхностного действия)

[3] ISO/IEC 14443 (all parts) Identification cards — Contactless integrated circuit cards — Proximity cards (Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия)

[4] ISO/IEC 15693 (all parts) Identification cards — Contactless integrated circuit(s) cards — Vicinity cards (Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты удаленного действия)

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.В. Таланова*
Технический редактор *В.Н. Прусакова*
Корректор *О.В. Лазарева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 05.12.2018. Подписано в печать 12.12.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,40.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru