НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Карты идентификационные

КАРТЫ НА ИНТЕГРАЛЬНЫХ СХЕМАХ С КОНТАКТАМИ

Часть 6

Элементы данных для межотраслевого обмена

Издание официальное

БЗ 12—2002/266

ГОССТАНДАРТ РОССИИ
Москва

Предисловие

1 РАЗРАБОТАН Техническим комитетом по стандартизации ТК 22 «Информационные технологии», Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении» (ВНИИНМАШ), ОАО «Московский комитет по науке и технологиям»

ВНЕСЕН ТК 22 «Информационные технологии»

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 14 октября 2003 г. № 290-ст

3 Настоящий стандарт представляет собой аутентичный текст международного стандарта ИСО/МЭК 7816-6:1996 «Карты идентификационные. Карты на интегральной (ых) схеме (ах) с контактами. Часть 6. Межотраслевые элементы данных» с Поправкой № 1 (1998 г.) и Изменением № 1 (2000 г.)

4 ВВЕДЕН ВПЕРВЫЕ

Содержание

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Карты идентификационные

КАРТЫ НА ИНТЕГРАЛЬНЫХ СХЕМАХ С КОНТАКТАМИ

Часть 6

Элементы данных для межотраслевого обмена

Identification cards. Integrated circuit(s) cards with contacts. Part 6. Interindustry data elements

Дата введения 2004—07—01

1 Область применения

Настоящий стандарт устанавливает, непосредственно или через ссылку, элементы данных (в том числе составные), используемые при межотраслевом обмене данными, основанном на картах с интегральными схемами.

Стандарт определяет следующие характеристики каждого элемента данных:

- идентификатор;
- наименование;
- описание и ссылку на стандарт;
- формат и кодирование (при отсутствии в других стандартах).

Компоновка каждого элемента данных описана такой, какой она прослеживается на стыке между устройством сопряжения и картой. Определены средства поиска элементов данных на карте (байты предыстории, процедура восстановления, команда (ы) на выполнение и команды, установленные в стандартах серии ИСО/МЭК 7816).

Определение элементов данных дано без учета каких-либо ограничений на их применение.

Предполагается, что новые межотраслевые информационные объекты должны быть включены в настоящий стандарт (процедуру см. в разделе 7).

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты.

ГОСТ Р ИСО/МЭК 8825-1—2003 Информационная технология. Правила кодирования ASN.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования

ИСО 639—88* Коды для представления названий языков

ИСО/МЭК 646—91* Информационная технология. Семибитный набор кодированных символов ИСО для обмена информацией

ИСО 3166-1—97* Коды для представления названий стран и объектов их деления. Часть 1. Коды стран

ИСО 3166-2—98* Коды для представления названий стран и объектов их деления. Часть 2. Коды объектов деления стран

ИСО 3166-3—99* Коды для представления названий стран и объектов их деления. Часть 3. Коды ранее использовавшихся названий стран

ИСО 4217—2001* Коды для представления валют и денежных средств

ИСО 4909—2000* Карты банковские. Содержание данных на дорожке 3 магнитной полосы

ИСО 5218—77* Обмен информацией. Представление пола человека

* Международные стандарты (ИСО) ИСО/МЭК — во ВНИИКИ Госстандарта России.

Издание официальное

ИСО/МЭК 7501-1—97* Карты идентификационные. Машиночитаемые дорожные документы. Часть 1. Машиночитаемый паспорт

ИСО/МЭК 7813—2001* Карты идентификационные. Карты для финансовых операций

ИСО/МЭК 7816-4—95* Информационная технология. Карты идентификационные. Карты на интегральной (ых) схеме (ах) с контактами. Часть 4. Межотраслевые команды для обмена информацией

ИСО/МЭК 7816-5—94* Карты идентификационные. Карты на интегральной (ых) схеме (ах) с контактами. Часть 5. Система нумерации и процедура регистрации для идентификаторов приложений

ИСО 8583—93* Сообщения, инициируемые картами для финансовых операций. Требования к сообщениям для обмена информацией

ИСО/МЭК 8859-1—98* Информационная технология. Наборы восьмибитных однобайтовых кодированных графических символов. Часть 1. Латинский алфавит № 1

ИСО/МЭК 9798-2—99* Информационная технология. Способы защиты. Аутентификация объектов. Часть 2. Механизмы, использующие симметричные алгоритмы шифрования

ИСО/МЭК 9798-3—98* Информационная технология. Способы защиты. Аутентификация объектов. Часть 3. Механизмы, использующие криптографическую функцию проверки

ИСО 9992-2—98* Карты для финансовых операций. Сообщения между картами на интегральных схемах и приемным устройством. Часть 2. Функции, сообщения (команды и ответы), элементы данных и структуры

ИСО/МЭК 10918-1—94* Информационная технология. Цифровое уплотнение и кодирование неподвижных изображений с непрерывным спектром тонов. Требования и руководящие принципы

ИСО/МЭК 11544—93* Информационная технология. Кодированное представление графической и звуковой информации. Последовательное двухуровневое сжатие изображения

3 Определения, сокращения и обозначения

3.1 Определения

В настоящем стандарте используют следующие определения.

3.1.1 **составной элемент данных:** Элемент данных, образованный сцеплением нуля, одного или большего числа элементов данных.

3.1.2 **элемент данных:** По ИСО/МЭК 7816-4.

3.1.3 **информационный объект:** По ИСО/МЭК 7816-4.

3.1.4 **список элементов:** Единицы информации, касающиеся элементов данных.

3.1.5 **список заголовков:** Сцепление пар тег/длина без разграничителей.

3.1.6 **межотраслевой элемент данных:** Элемент данных для использования в межотраслевом обмене информацией.

3.1.7 **межотраслевой информационный объект:** Информационный объект для использования в межотраслевом обмене информацией.

3.1.8 **список тегов:** Сцепление тегов без разграничителей.

3.1.9 **шаблон:** Поле значения составного информационного объекта, заданное с целью обеспечения логического группирования информационных объектов.

3.2 Сокращения

В настоящем стандарте применяют следующие сокращения.

ACH.1 — абстрактно-синтаксическая нотация версии 1.

ATR — ответ-на-восстановление (Answer-to-reset).

DE — элемент данных (Data element).

DF — назначенный файл (Dedicated file).

DO — информационный объект (Data object).

EF — элементарный файл (Elementary file).

FCI — контрольная информация файла (File control information).

ICC — карта на интегральных схемах (Integrated circuit card).

IDE — межотраслевой элемент данных (Interindustry data element).

IDO — межотраслевой информационный объект (Interindustry data object).

---

* Международные стандарты (ИСО) ИСО/МЭК — во ВНИИКИ Госстандарта России

LRC — продольный контроль по избыточности (Longitudinal redundancy check).

PIN — персональный идентификационный номер (Personal identification number).

3.3 Обозначения

В настоящем стандарте применяют следующие обозначения.

a — буквенный символ.

n — цифра, кодированная в двоично-десятичном формате.

s — специальный символ.

an — буквенно-цифровой символ.

ans — буквенно-цифровые и специальные символы.

... — между двумя числами обозначает диапазон значений.

Любое число, следующее за обозначениями, означает количество цифр или символов. Например:

a3 означает три буквенных символа;

n...3 означает до трех двоично-кодированных десятичных цифр;

n...24 означает две, три или четыре двоично-кодированных десятичных цифры.

4 Идентификация элементов данных

4.1 Принципы

Для идентификации элементов DE применены следующие принципы.

4.1.1 В настоящем стандарте элемент данных, как правило, представляют в поле значения информационного объекта.

4.1.2 В настоящем стандарте информационный объект представляет собой сцепление следующей последовательности байтов:

- обязательного призначного поля, именуемого как тег;
- обязательного поля длины, указывающего длину L;
- условного поля значения, состоящего из L байтов (если L не равно '00').

4.1.3 Для целей поиска и обращения при обмене информацией:

- DE должен быть ассоциирован с тегом DO;
- DE может быть сформирован в этом DO.

4.1.4 Контекст, в соответствии с которым осуществляется идентификация DO, зависит:

- либо от вложения DO в шаблон;
- либо от выбранного в текущий момент приложения.

4.1.5 Когда приложение не выбрано, интерпретация всех DO должна осуществляться в соответствии с настоящим стандартом и стандартами серии ИСО/МЭК 7816.

4.1.6 Обращение к DE может осуществляться непосредственно через ассоциированный с ним тег. DE может быть связан с другим DE, указывающим контекст, к которому он принадлежит.

4.1.7 Обращение к DE может осуществляться косвенно при помощи одного или нескольких DO «команда на выполнение».

4.1.8 DO описаны такими, какими они прослеживаются на стыке между ICC и устройством сопряжения.

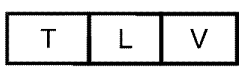
4.1.9 В настоящем стандарте и стандартах серии ИСО/МЭК 7816 тег обозначает тип DE.

4.1.10 В карте может иметь место множественное присутствие одного и того же IDO.

4.2 Структура информационного объекта

Поддержаны следующие структуры DO.

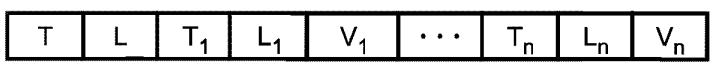
Простой DO:



,

где T — тег, L — длина, V — значение.

Составной DO:



,

где T — тег составного DO;

L — длина последовательности (шаблона) от T_1 до V_n;

$T_{1...n}$ — тег $DO_{1...n}$;

$L_{1 \ldots n}$ — длина $V_{1 \ldots n}$;
$V_{1 \ldots n}$ — значение $DO_{1 \ldots n}$.

4.2.1 Структура тега

Тег состоит из одного или двух байтов. Кодирование этих байтов не должно противоречить базовым правилам кодирования нотации АСН.1. В таблице 1 определен первый байт.

Таблица 1 — Структура первого байта тега

b8	b7	b6	b5	b4	b3	b2	b1	Содержание
0	0	—	—	—	—	—	—	Не определено в настоящем стандарте
0	1	—	—	—	—	—	—	Определено в настоящем стандарте. Прикладной класс, однозначная идентификация
1	0	—	—	—	—	—	—	Определено в настоящем стандарте. Следует использовать только в пределах шаблона. См. примечание
1	1	—	—	—	—	—	—	Не определено в настоящем стандарте. Зарезервировано для индивидуального использования
— —	— —	0 1	— —	— —	— —	— —	— —	Простой DO Составной DO
—	—	—	1	1	1	1	1	Номер тега (диапазон 31 ... 127) содержится в следующем байте
—	—	—	X	X	X	X	X	Номер тега (диапазон 0 ... 30). Не все биты равны 1
Примечание — Теги контекстно-зависимого класса (b8b7 = 10) используют вне шаблонов для контрольной информации файла и безопасного обмена сообщениями, см. ИСО/МЭК 7816-4.								

Кодирование второго байта, если он представлен, следующее:
b8 = 0;
b7 — b1 = двоичное значение номера тега в диапазоне 31 ... 127.

4.2.2 Структура длины

Все длины выражают в байтах.

Поле длины состоит из одного или большего числа байтов. Кодирование этих байтов не должно противоречить базовым правилам кодирования нотации АСН.1 и должно соответствовать таблице 2.

Таблица 2 — Кодирование значения длины

Диапазон	Количество байтов	Первый байт	Второй байт	Третий байт
0 ... 127	1	Двоичное значение	—	—
0 ... 255	2	’81’	Двоичное значение	—
0 ... 65535	3	’82’	Двоичное значение	
			Старший байт	Младший байт

4.2.3 Формат значения

Формат значения зависит от типа DE.

Когда длина DE не выражена через число байтов, отображение на строку байтов должно определяться в контексте соответствующего DE (см. раздел 8). Если не указано иначе, то соответствующее число младших битов последнего байта должно быть установлено в «1».

4.3 Косвенное обращение к DE

Используют следующие IDO:

- «оболочка» (тег ’63’), составленный согласно описанию в 5.6;

- «список тегов» (тег '5C'), значение которого представляет собой тег (сцепление тегов) без разграничителя;
- «список заголовков» (тег '5D'), значение которого представляет собой сцепление пар тег/длина без разграничителя;
- «список элементов» (тег '5F41'), предназначенный для применения только в пределах «оболочки» (тег '63');
- «команда на выполнение» (тег '52'), применяемый как определено в ИСО/МЭК 7816-4;
- «путь» (тег '51'), применяемый как определено в ИСО/МЭК 7816-4.

4.4 Схемы распределения тегов

Настоящий стандарт распределяет некоторые теги прикладного класса, контекстно-независимые, которые показаны в таблице 1 (прикладной класс тегов определен базовыми правилами кодирования нотации ACH.1). В стандарте определена стандартная (по умолчанию) схема распределения тегов для объектов IDO в ICC (см. таблицу 10).

4.4.1 Совместимые схемы распределения тегов

Эти схемы распределения тегов используют IDO, определяемые в настоящем стандарте и стандартах серии ИСО/МЭК 7816, а также дополнительные DO, которые должны:

- либо использовать теги контекстно-зависимого класса (начинающиеся с 8, 9, A, B) в пределах шаблонов, определяемых в настоящем стандарте (шаблоны '65', '66', '67', '6E');
- либо быть вложены в шаблоны с тегами от '70' до '77'. Содержание тегов прикладного класса в пределах этих шаблонов настоящий стандарт и стандарты серии ИСО/МЭК 7816 не определяют, за исключением тегов, определяемых в таблице 4.

Для идентификации совместимой схемы распределения тегов и источника, ответственного за эту схему, может быть использован DO «источник распределения тегов» с тегом '78' (определен в 4.4.4).

Если источник распределения тегов действителен только для данных в пределах файла DF, тогда FCI этого файла может содержать DO «источник распределения тегов».

Если источник распределения тегов действителен для карты в целом, тогда этот DO может присутствовать в строке начальных данных или в файле ATR (как определено в ИСО/МЭК 7816-4).

IDO, перечисленные в 4.4.4, могут быть включены в шаблоны с '70' по '77', указывая источник, ответственный за распределение тегов, используемых в таком шаблоне.

Примечание — Использование данных схем является либо неявным (использование контекстно-зависимых тегов), либо явным (наличие IDO с тегом '78').

4.4.2 Сосуществующие схемы распределения тегов

В этих схемах распределения тегов DO могут использовать теги с иной интерпретацией, чем принятая в настоящем стандарте и стандартах серии ИСО/МЭК 7816.

Для идентификации сосуществующей схемы распределения тегов должен быть использован DO «источник распределения тегов» с тегом '79' (определен в 4.4.4), идентифицирующий источник, ответственный за эту схему.

Если источник распределения тегов действителен только для данных в пределах файла DF, тогда FCI этого файла должна содержать DO «источник распределения тегов».

Если источник распределения тегов действителен для карты в целом, тогда этот DO должен присутствовать в строке начальных данных или в файле ATR (как определено в ИСО/МЭК 7816-4).

Все IDO должны быть вложены в шаблоны с тегом '7E'. В такой схеме теги '79' и '7E' не должны интерпретироваться иначе.

Помимо тегов '79' и '7E', сосуществующей схемой распределения тегов не должны перераспределяться теги из таблицы 3, определяемые в настоящем стандарте и стандартах серии ИСО/МЭК 7816.

Таблица 3 — Теги, зарезервированные за стандартами ИСО/МЭК

Тег	IDO
62	Обозначает шаблон контрольных параметров файла (FCP) по ИСО/МЭК 7816-4
64	Обозначает шаблон данных управления файлом (FMD) по ИСО/МЭК 7816-4
6F	Обозначает шаблон FCI по ИСО/МЭК 7816-4
7D	Зарезервирован за стандартами серии ИСО/МЭК 7816 для шаблона безопасного обмена сообщениями

4.4.3 Независимые схемы распределения тегов

В этих схемах распределения тегов DO также могут использовать теги с иной интерпретацией, чем принятая в настоящем стандарте и стандартах серии ИСО/МЭК 7816, которая не подчиняется требованиям 4.4.2. Такие схемы распределения тегов делают невозможным межотраслевой обмен информацией и не согласуются с настоящим стандартом.

Последовательное использование объектов IDO «произвольные данные» (тег '53') и «произвольные DO» (тег '73') дает возможность применения оригинальных объектов, сохраняя в то же время соответствие настоящему стандарту.

4.4.4 Источник распределения тегов

В пределах шаблонов '78' или '79' объекты IDO, представленные в таблице 4, показывают, какой источник является ответственным за распределение тегов.

Таблица 4 — Теги для размещения данных об источниках

Тег	IDO
06	Идентификатор объекта в соответствии со стандартами серии ИСО/МЭК 8825 (см. пример кодирования в приложении Б)
41	Определен в ИСО/МЭК 7816-4 и используется для указания, по меньшей мере, страны
42	Определен в ИСО/МЭК 7816-4 и используется для указания эмитента
4F	Указывает идентификатор приложения (AID) по ИСО/МЭК 7816-5

5 Поиск данных

Настоящий раздел определяет стандартные процедуры поиска элементов DE.

5.1 Принципы

До выбора приложения отбор объектов IDO должен осуществляться прямо или косвенно из:

- байтов предыстории;
- строки начальных данных;
- файла ATR;
- справочного файла (файла DIR)

в вышеприведенном порядке, если указанные источники представлены.

Интерпретация этих IDO должна соответствовать разделу 4.

Как только приложение выбрано, отбор объектов IDO должен осуществляться прямо или косвенно из:

- FCI файла DF;
- других специальных файлов EF в пределах текущего файла DF.

В этом случае поиск этих IDO может быть осуществлен также путем использования команды (команд) ИЗВЛЕЧЬ ДАННЫЕ.

5.2 Поиск объектов DO после ATR

Если имеется указание в байтах предыстории, DO могут быть отысканы после процедуры восстановления и возможной процедуры выбора типа протокола (PTS) путем использования начальных данных доступа по ИСО/МЭК 7816-4.

Все эти DO должны иметь теги, соответствующие 4.4.

5.3 Поиск данных в файлах

DO могут быть отысканы в зарезервированных файлах (файлах DIR и ATR). На эту возможность могут указывать байты предыстории. Выбор и считывание этих файлов определены в ИСО/МЭК 7816-4. Содержание файла DIR определено в ИСО/МЭК 7816-5. Информация, касающаяся содержания файла ATR, имеется в ИСО/МЭК 7816-4. Все эти DO должны иметь теги, определяемые настоящим стандартом и стандартами серии ИСО/МЭК 7816.

DE могут быть отысканы в других файлах, обозначенных через их путь в DE «оболочка» (см. 5.6). Выбор и считывание EF, известного по его пути, определены в ИСО/МЭК 7816-4.

5.4 Поиск данных в FCI

Данные могут быть представлены в FCI по ИСО/МЭК 7816-4.

5.5 Поиск данных с использованием команды ИЗВЛЕЧЬ ДАННЫЕ

DO могут быть отысканы с помощью команды ИЗВЛЕЧЬ ДАННЫЕ, как определено в ИСО/МЭК 7816-4.

5.6 Косвенный поиск элементов DE

Для косвенного обращения используют DO «оболочка». DO «оболочка» имеет тег '63', является составным и должен состоять из двух частей.

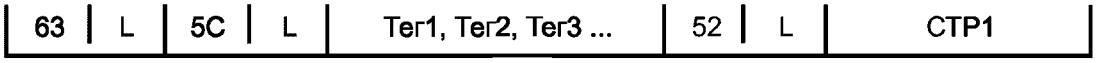
Первая часть содержит:

- либо IDO «список тегов» (тег '5C'), означающий, что искомые DE представлены в виде объектов DO;
- либо IDO «список заголовков» (тег '5D'), означающий, что искомые DE представлены в виде строки значений в том же порядке, что и в списке тегов;
- IDO «список элементов» (тег '5F41'), означающий, что искомые элементы не представлены в виде объектов DO, но находятся под управлением приложения. Структура списка элементов, а также выдаваемая информация находятся за пределами компетенции настоящего стандарта и стандартов серии ИСО/МЭК 7816.

Вторая часть содержит:

- путь к EF (тег '51');
- и/или один (или более) DO «команда на выполнение» (тег '52'), как определено в ИСО/МЭК 7816-5.

Следующая диаграмма представляет собой пример оболочки, содержащей список тегов и одну команду на выполнение (CTP):



В оболочке должна быть дана только одна косвенная ссылка. Может иметь место более чем одна оболочка.

DO, на который дана ссылка в списке тегов согласно настоящему стандарту и стандартам серии ИСО/МЭК 7816, или DE, на который дана ссылка иным способом в списке DE, должен:

- либо содержаться в файле, обозначенном через его путь (см. 5.3),
- либо быть ответом (его частью) на последнюю команду на выполнение, указанную в оболочке. Команды должны выполняться в порядке представления.

6 Кодирование отдельных DE

6.1 IDO «имя» (физического лица), тег '5B'

Составной DE переменной длины (до 39 символов), образованный из:

- фамилии;
- имени (имен);
- уточняющего дополнения к имени (например, младший, номер ...);
- символа (ов)-заполнителя (ей),

как определено и применяется в ИСО/МЭК 7501-1. Элементы данных должны быть закодированы в соответствии с ИСО/МЭК 8859-1.

Национальные языки с нелатинскими символами следует транслитерировать или транскрибировать в латинский алфавит, используя соответствующий стандарт ИСО.

В случаях, когда:

- имена не могут быть представлены полностью,
- или требуется специфический алфавит,
- или транслитерация либо транскрипция недостаточны,

следует использовать IDO «уточненное имя».

6.2 IDO «уточненное имя», тег '6B'

Составной DO переменной длины, образованный из:

- одного или нескольких идентификаторов объекта (тег '06'), дающих ссылки на стандарты, определяющие представление уточненного имени;
- имени (тег '80', если DO простой, или тег 'A0', если DO составной), значение и кодирование которого определены вышеупомянутыми стандартами;
- другой сопутствующей необязательной информации (например, пол, гражданство, место рождения).

6.3 IDO «шаблон начала сеанса», тег '6A'

Шаблон начала сеанса представляет собой составной объект переменной длины. Значение должно состоять из одного или большего числа простых объектов, таких как квалификаторы, номера, текст и время, как установлено ниже.

6.3.1 Квалификатор

Тег должен быть '80'. Значение (длиной от одного до девяти байтов) должно состоять из обязательного первого байта, кодирующего ранг, и следующих за ним, самое большое, восьми необязательных байтов, кодирующих мнемосхему. Оно должно квалифицировать последующие объекты в шаблоне, вплоть до следующего квалификатора, если таковой имеется.

Ранг представляет собой целое число со значением от 0 до 255. Если два или более квалификатора имеют один и тот же ранг в пределах одного и того же контекста, тогда имеет силу лишь набор объектов, квалифицируемых самым последним из них.

Мнемосхема представляет собой строку семибитных символов (бит b8 устанавливается в «0», см. ИСО/МЭК 646), предназначенную для визуализации в человеко-машинном интерфейсе.

6.3.2 Номер

Тег должен быть '81'. Значение должно состоять из четного числа полубайтов, где каждый полубайт кодирует один символ для представления номера телефона в соответствии с таблицей 5.

Таблица 5 — Декодирование полубайтов

Полубайт	Символ	Содержание
'0' — '9'	0 — 9	Десятичные цифры
'A'	(	Начальная скобка
'B'	)	Замыкающая скобка
'C'	C	Требование подключения к линии перед продолжением
'D'	+	Введение международного номера телефона
'E'	—	Если следует первым — введение номера, который должен использоваться без префикса; если следует не первым — требование задержки (2 с) перед продолжением
'F'		Зарезервировано для заполнения незначащей информацией

6.3.3 Текст

Тег должен быть '82'. Значение должно состоять из одного или большего числа байтов, где каждый байт кодирует один символ. Бит b8 устанавливает различие между символами данных (b8 установлен в «0») и управляющими символами (b8 установлен в «1»). Строка байтов состоит из одной или более строк символа данных (семибитные символы, см. ИСО/МЭК 646), разделенных строками управляющих символов. Определены следующие управляющие символы:

'80' — сообщение должно быть получено перед посылкой следующего символа;

'C0' — модуляция должна быть выполнена перед посылкой следующего символа;

'8X' — X символов должны быть получены в режиме эхопередачи перед ожиданием сообщения.

6.3.4 Время обнаружения конца сообщения

Тег должен быть '83'. Значение должно состоять из одиночного байта, кодирующего время согласно таблице 6. Это время должно использоваться для обнаружения конца сообщения. Значение по умолчанию должно составлять 2 с.

6.3.5 Время обнаружения начала сообщения

Тег должен быть '84'. Значение должно состоять из одиночного байта, кодирующего время согласно таблице 6. Это время должно использоваться для выявления отсутствия ответа. Значение по умолчанию должно составлять 60 с.

Таблица 6 — Декодирование времени

b8	b7	b6	b5	b4	b3	b2	b1
⇐ RFU ⇒		⇐ Единица времени ⇒		⇐ Число единиц времени ⇒			

b8—b7 — зарезервированы для будущего использования (00 в случае неиспользования);
b6—b5 — значение единицы времени:
00 = 100 мс,
01 = 1 с,
10 = 10 с,
11 = 100 с;
b4—b1 — число единиц времени.

Кроме того, данные начала сеанса могут быть представлены оригинальными структурами, не установленными настоящим стандартом и стандартами серии ИСО/МЭК 7816. Тег '5E' зарезервирован для вложения такого рода оригинальных данных начала сеанса.

6.4 IDO «стратегия использования PIN-кода», тег '5F2F'

DE «стратегия использования PIN-кода» состоит из двух байтов, указывающих проверки, которые должны быть выполнены терминалом для того, чтобы определить, применим ли PIN-код к текущей операции и, следовательно, должен ли терминал запросить введение PIN-кода. Бит 8 первого байта, если он установлен в «1», указывает, что PIN-код применим к данному приложению, и терминал должен его запросить. Содержание других 15 битов зависит от приложения. Если все биты установлены в «0», тогда терминал не должен запрашивать PIN-код.

Если бит 8 первого байта находится во включенном состоянии или какая-нибудь из выполненных проверок указывает, что PIN-код применяется, но он не может быть предоставлен, то действия, которые должны быть предприняты, зависят от приложения.

6.5 IDO «образцы держателя карты», тег '6C'

Этот составной IDO содержит, по меньшей мере, один IDO, определяемый в данном подразделе. Такому IDO может предшествовать указатель источника (см. 4.4.4), идентифицируя источник, ответственный за формат данных этого IDO.

6.5.1 IDO «биометрические данные держателя карты», тег '5F2E'

Этот IDO содержит биометрические данные, относящиеся к держателю карты. Биометрические данные предназначены обеспечить средства подтверждения требуемой идентичности человека, предъявляющего карту. Примерами биометрических данных являются отпечатки пальцев, ладоней, характеристики голоса, динамические характеристики подписи и т. д.

6.5.2 IDO «портретное изображение держателя карты», тег '5F40'

Формат портретного изображения держателя карты должен соответствовать ИСО/МЭК 10918-1, если иное не определено источником.

6.5.3 IDO «изображение рукописной подписи держателя карты», тег '5F43'

Формат изображения рукописной подписи держателя карты должен соответствовать ИСО/МЭК 11544, если иное не определено источником.

Примечание — Рекомендуется сочетать использование этого IDO с соответствующими защитными мерами.

6.6 IDO «шаблон образа приложения», тег '6D'

Этот IDO содержит, по меньшей мере, образ приложения (тег '5F44'). Он может также содержать указатель источника (см. 4.4.4), идентифицирующий орган, ответственный за формат данных образа приложения. Когда источник не представлен, формат должен соответствовать ИСО/МЭК 10918-1.

6.7 Данные магнитной полосы

Для представления объектов DO «дорожка 1», «дорожка 2» и «дорожка 3», относящихся к карте, установлены теги '5F21', '5F22' и '5F23' соответственно. Эти теги должны использоваться в случае, когда содержание данных этих DO идентично содержанию данных соответствующих дорожек магнитной полосы карты.

Для представления объектов DO «дорожка 1», «дорожка 2» и «дорожка 3», относящихся к

приложению, установлены теги '56', '57' и '58' соответственно. Эти теги должны использоваться в случае, когда формат данных этих DO соответствует ИСО/МЭК 7813 и ИСО 4909, но содержание может отличаться от содержания данных магнитной полосы карты.

6.8 IDO «управление отображением», тег '7F20'

В этом шаблоне может содержаться один или большее число IDO. Значение любого IDO, входящего в данный шаблон непосредственно или через составные DO, не предназначено для его визуализации и должно использоваться лишь для обработки передачи в соответствующих случаях.

6.9 Профиль обмена

Описание объектов IDO, связанных с профилем обмена у ICC (например, с имеющимися защитными функциями и методами аутентификации), может быть более подробно изложено в последующих стандартах серии ИСО/МЭК 7816.

Теги, представленные в таблице 7, зарезервированы для этой цели.

Таблица 7 — Теги, зарезервированные для профиля обмена

Тег	IDO
5F29	Профиль обмена
5F37	Статическая внутренняя аутентификация (одноступенчатая)
5F38	Статическая внутренняя аутентификация — первые ассоциированные данные
5F39	Статическая внутренняя аутентификация — вторые ассоциированные данные
5F3A	Динамическая внутренняя аутентификация
5F3B	Динамическая внешняя аутентификация
5F3C	Динамическая взаимная аутентификация

6.10 Регистрация изготовителей интегральных схем

6.10.1 Область применения

Данный подраздел устанавливает:

- систему нумерации;
- правила присвоения номеров и
- присвоенные значения

для идентификации изготовителей интегральных схем, используемых в картах на интегральных схемах с контактами и/или без контактов.

6.10.2 Система нумерации

Структура и кодирование идентификатора изготовителя интегральных схем представлены одним двоичным байтом с зарезервированным значением для будущего расширения ('FF' зарезервировано для будущего расширения).

Этот байт должен использоваться согласно таблице 8.

Таблица 8 — Кодирование элемента данных «идентификатор изготовителя интегральных схем»

Шестнадцатеричное значение	Использование
'00'	Зарезервировано для будущего использования
'01' — '7E'	Процедуру присвоения и регистрации см. в 6.10.3, зарегистрированные на текущий момент идентификаторы см. в 6.10.4 (таблица 9)
'7F', '80'	Зарезервированы для будущего использования
'81' — 'FE'	Для собственного использования
'FF'	Зарезервировано для будущего расширения

6.10.3 Присвоение идентификаторов изготовителей интегральных схем

Идентификаторы изготовителей интегральных схем (диапазон значений '01' — '7E') присваи-

вает и регистрирует секретариат* Подкомитета № 17 совместного Технического комитета № 1 ИСО/МЭК (ПК 17 СТК 1 ИСО/МЭК) по следующим правилам:

- присвоение совершается по запросу изготовителя интегральных схем или любой заинтересованной стороны;
- каждому изготовителю присваивается один номер (следующий имеющийся в наличии номер);
- копия реестра должна предоставляться по запросу, направляемому в секретариат ПК 17 СТК 1 ИСО/МЭК.

6.10.4 Реестр идентификаторов изготовителей интегральных схем

Информационный объект «идентификатор изготовителя интегральных схем» имеет тег '5F4B'. Присвоенные значения для связанного с ним элемента данных представлены в таблице 9.

Таблица 9 — Зарегистрированные изготовители интегральных схем

Идентификатор изготовителя интегральных схем	Компания	Реквизиты
'01'	Motorola	Адрес: MOS Memory & Microprocessor Division Colvilles Rd Kelvin Industrial Estate East Kilbride Glasgow G75 OTG Страна: Великобритания Телефон: +44 135 556 5731 Факс: +44 135 525 64582
'02'	S T Microelectronics	Адрес: IC Card Division 7, Ave Gallieni BP 93 94253 GENTILLY Cdx Страна: Франция Телефон: +33 1 4740 7575 Факс: +33 1 4740 7910
'03'	Hitachi, Ltd	Адрес: Semiconductor & Integrated Circuits Group 20-1, Jousuihon-cho 5 chome Kodaira-shi Tokyo 187-8588 Страна: Япония Телефон: +81 42 320 7301 (доб. 3313) Факс: +81 42 327 8693
'04'	Philips Semiconductors	Адрес: Productgroup Identification Stresemannallee 101 D-22529 Hamburg Страна: Германия Телефон: +49 40 5613 2995 Факс: +49 40 5613 3554
'05'	Infineon Technologies AG	Адрес: Security & Chip Card ICs P.O. Box 80 09 49 D 81609 Munchen Страна: Германия Телефон: +49 89 234-24145 Факс: +49 89 234-28925
'06'	Cylinc	Адрес: Sunnivale, CA Страна: США
'07'	Texas Instrument	Адрес: Smart Card Division BP 5 06271 Villeneuve Loubet Cdx Страна: Франция Телефон: +33 4 9322 2220 Факс: +33 4 9322 2637

* APACS, Mercury House, Triton Court, 14 Finsbury Square, London EC2 1LQ, UK-email: fjb@apacs.org.uk

Окончание таблицы 9

Идентификатор изготовителя интегральных схем	Компания	Реквизиты
'08'	Fujitsu Limited	Адрес: 1-1, Kamikodanaka 4-Chome nakahara-ku Kawasaki 211-8588 Страна: Япония Телефон: +81 44 754 3767 Факс: +81 44 754 3343
'09'	Matsushita Electronics Corporation	Адрес: 1-1 Saiwai-cho Takasuki Osaka 569-1193 Страна: Япония Телефон: +81 726 82 7530 Факс: +81 726 82 7093
'0A'	NEC	Адрес: 1-10 Nisshin-cho Fuchu-shi Tokyo 183 Страна: Япония Телефон: +81 423 33 1498 Факс: +81 423 33 1856
'0B'	Oki Electric Industry Co. Ltd	Адрес: LSI Division 550-1 Higashiasakawa-cho Hachioji-shi Tokyo 193-8550 Страна: Япония Телефон: +81 426 63 1111 Факс: +81 426 65 6536
'0C'	Toshiba Corp.	Адрес: 1-1, Shibaura 1-Chome Minato-Ku Tokyo 105-8001 Страна: Япония Телефон: +81 3 3457 8412 Факс: +81 3 5444 9218
'0D'	Mitsubishi Electric Corp.	
'0E'	Samsung Electronics Co. Ltd	Адрес: Smart Card LSI Division San 24 Nongseo-Ri Kiheung-Eup Yongin-City Kyungki-Do Страна: Республика Корея Телефон: +82 331 209 3437 Факс: +82 331 209 6533
'0F'	Hyundai Electronics Industries Co. Ltd	Адрес: San 136-1 Ami-ri, Bubal-eub Ichon-si Kyungki-do Страна: Республика Корея 467-701 Телефон: +82 336 30 2016 Факс: +82 336 30 2022
'10'	LG-Semiconductors Co. Ltd	Адрес: 106 138 Bdg. Sinlim-Dong Gwanak-Ku Seoul Страна: Республика Корея 151-742 Телефон: +82 2 883 5009 Факс: +82 2 882 0470
'11' — '7E'	Для следующего присвоения	

Примечание — Этот элемент данных может быть представлен в информационном объекте «данные, предваряющие эмиссию карты» (тег '46') на частной основе.

7 Ведение объектов IDO

Предполагается, что все IDO будут приведены в разделе 8 ИСО/МЭК 7816-6. Для введения, исключения или изменения любых IDO должны быть приняты следующие процедуры.

7.1 IDO из стандартов серии ИСО/МЭК 7816

Если новые IDO вводятся новыми стандартами серии ИСО/МЭК 7816, тогда эти IDO будут одобряться в процессе обычного голосования. Вслед за опубликованием нового стандарта объекты IDO будут включены в ИСО/МЭК 7816-6 без дополнительного голосования.

7.2 IDO из других стандартов

Для этих IDO потребуется изменение или дополнение к ИСО/МЭК 7816-6, которое будет подлежать обычным процедурам утверждения, принятым в ИСО. Вслед за успешным голосованием IDO будут включены в ИСО/МЭК 7816-6.

8 Перечень межотраслевых информационных объектов

8.1 Информационные объекты в алфавитном порядке

В таблице 10 представлен перечень межотраслевых DO (в алфавитном порядке) с описанием, ссылкой на стандарт, а также длиной и форматом в соответствующих случаях.

Таблица 10 — Объекты IDO в алфавитном порядке

Тег	Наименование элемента данных	Описание и ссылка на стандарт	Длина/ формат	Может быть найден в шаблоне
5F42	Адрес	Адрес физического лица	Переменные	65
5F2E	Биометрические данные держателя карты	Биометрические данные, относящиеся к держателю карты	Переменные	65
5F2C	Гражданство держателя карты	Указывает гражданство держателя карты (кодирование см. в ИСО 3166)	n 3	65
5E	Данные начала сеанса (оригинальные)	Оригинальная информация, предназначенная для установления связи интерфейсного устройства с удаленным главным компьютером, удаленным сервером или приложением в этих устройствах	Переменные	6E
43	Данные об услугах, предоставляемых картой	По ИСО/МЭК 7816-4	Один байт	—
46	Данные, предваряющие эмиссию карты	Оригинальный	Переменные	66
45	Данные эмитента	По ИСО/МЭК 7816-4	Переменные	66
5F26	Дата активации карты	Дата, начиная с которой карта может использоваться под ответственность ее эмитента	n 6 YYMMDD	66
5F25	Дата активации приложения	Дата, начиная с которой приложение может использоваться под ответственность провайдера приложения	n 6 YYMMDD	6E
59	Дата истечения срока действия карты	Дата, после которой карта считается недействительной	n 4 YYMM	66
5F24	Дата истечения срока действия приложения	Дата, после которой приложение находится в нерабочем состоянии	n 6 YYMMDD	6E

Продолжение таблицы 10

Тег	Наименование элемента данных	Описание и ссылка на стандарт	Длина/ формат	Может быть найден в шаблоне
5F33	Дата операции	Используется для определения даты и времени последней операции. Длина составляет четыре для формата YDDD и 10 для полного поля	n 4 или n 10 YDDD (HHMMSS)	6E
5F2B	Дата рождения	Дата рождения физического лица	n 8 YYYYMMDD	65
5F3C	Динамическая взаимная аутентификация	Составной DO, используемый для идентификации алгоритма и ключа, которые должны использоваться в процессе взаимной аутентификации (см. ИСО 9798-2, ИСО 9798-3)	Предстоит определить	67
5F3B	Динамическая внешняя аутентификация	Составной DO, используемый для идентификации алгоритма и ключа, которые должны использоваться в команде ВЫПОЛНИТЬ ВНЕШНЮЮ АУТЕНТИФИКАЦИЮ	Предстоит определить	67
5F3A	Динамическая внутренняя аутентификация	Составной DO, используемый для идентификации алгоритма и ключа, которые должны использоваться в команде ВЫПОЛНИТЬ ВНУТРЕННЮЮ АУТЕНТИФИКАЦИЮ	Предстоит определить	67
5F45	Дисплейное сообщение	DE, содержащий сообщение, предназначенное для его визуализации	Переменные	66
5F22	Дорожка 2 (карта)	Информация, закодированная на дорожке 2 магнитной полосы (в соответствии с ИСО/МЭК 7813), включая разделители полей, но исключая сигнальные метки начала и конца и символ LRC. Содержание данных то же, что и на магнитной полосе, с учетом произвольных данных (см. структуру в ИСО/МЭК 7813, кодирование — в ИСО 8583)	n...37	66
57	Дорожка 2 (приложение)	Информация, закодированная в соответствии с ИСО/МЭК 7813, включая разделители полей, но исключая сигнальные метки начала и конца и символ LRC (см. структуру в ИСО/МЭК 7813, кодирование — в ИСО 8583)	n...37	6E
5F21	Дорожка 1 (карта)	Информация, закодированная на дорожке 1 магнитной полосы (в соответствии с ИСО/МЭК 7813), включая разделители полей, но исключая сигнальные метки начала и конца и символ LRC. Содержание данных то же, что и на магнитной полосе, с учетом произвольных данных (см. структуру в ИСО/МЭК 7813, кодирование — в ИСО 8583)	ans...76	66

Продолжение таблицы 10

Тег	Наименование элемента данных	Описание и ссылка на стандарт	Длина/ формат	Может быть найден в шаблоне
56	Дорожка 1 (приложение)	Информация, закодированная в соответствии с ИСО/МЭК 7813, включая разделители полей, но исключая сигнальные метки начала и конца и символ LRC (см. структуру в ИСО/МЭК 7813, кодирование — в ИСО 8583)	ans...76	6E
5F23	Дорожка 3 (карта)	Информация, закодированная на дорожке 3 магнитной полосы (в соответствии с ИСО 4909), включая разделители полей, но исключая сигнальные метки начала и конца и символ LRC. Содержание данных то же, что и на магнитной полосе, с учетом произвольных данных (см. структуру в ИСО 4909, кодирование — в ИСО 8583)	n...104	66
58	Дорожка 3 (приложение)	Информация, закодированная в соответствии с ИСО 4909, включая разделители полей, но исключая сигнальные метки начала и конца и символ LRC (см. структуру в ИСО 4909, кодирование — в ИСО 8583)	n...104	6E
5F4B	Идентификатор изготовителя интегральных схем	Идентифицирует изготовителя интегральных схем	Один байт	—
06	Идентификатор объекта	По ИСО/МЭК 8825-1 (кодирование см. в приложении Б)	Переменные	—
4F	Идентификатор приложения	DE, который идентифицирует приложение в карте (см. ИСО/МЭК 7816-5)	Переменные	61/6E
5F43	Изображение рукописной подписи держателя карты	Изображение подписи держателя карты (см. ИСО/МЭК 11544)	Переменные	6C
5B	Имя	Имя физического лица (см. 6.1)	Переменные	65
5F20	Имя держателя карты	Указывает имя держателя карты (см. ИСО/МЭК 7813)	n 2...26	65
48	Информация о состоянии	По ИСО/МЭК 7816-4	1...3 байта	—
78	Источник распределения совместимых тегов	Используется для идентификации совместимой схемы распределения тегов и источника, ответственного за схему	Переменные	—
79	Источник распределения сосуществующих тегов	Используется для идентификации сосуществующей схемы распределения тегов и источника, ответственного за схему	Переменные	—
5F2A	Код валюты	Код для представления валют и денежных средств (см. ИСО 4217). Длина — два байта, если формат цифровой, и три байта, если формат буквенный	a 3 или n 3	6E
5F28	Код страны	Код для представления названия страны (см. ИСО 3166)	n 3	66

Продолжение таблицы 10

Тег	Наименование элемента данных	Описание и ссылка на стандарт	Длина/ формат	Может быть найден в шаблоне
52	Команда на выполнение	Командная APDU (см. ИСО/МЭК 7816-4)	Переменные	61
50	Метка приложения	DE для использования в человеко-машинном интерфейсе (см. ИСО/МЭК 7816-5)	Переменные	61/6E
44	Начальные данные доступа	По ИСО/МЭК 7816-4	Переменные	66
63	Оболочка	Используется для косвенного обращения и поиска (см. 4.3)	Переменные	—
5F44	Образ приложения	Видеоданные для пиктограммы или логотипа, связанных с приложением (см. ИСО/МЭК 10918-1)	Переменные	6D
68	Особые условия пользователя	Этот составной DO содержит, по меньшей мере, DO, указывающий ответственный источник (см. 4.4.4), и DO, при помощи которого этот источник указывает условия пользователя, возможно, связанные с неплатежеспособностью	Переменные	65
5F49	Открытый ключ держателя карты	DE, содержащий открытый ключ держателя карты для электронной цифровой подписи, использующей асимметричные механизмы	Переменные	65
5F4A	Открытый ключ органа по сертификации	DE, содержащий открытый ключ органа по сертификации для электронной цифровой подписи, используемой для подтверждения подлинности сертификата	Переменные	65
5A	Первичный идентификатор счета (PAN)	Ряд цифр, используемых для идентификации счета или клиента (см. структуру в ИСО/МЭК 7813, кодирование — в ИСО 8583)	n...19	6E
5F35	Пол	Пол физического лица (см. ИСО 5218)	Один байт	65
5F40	Портретное изображение держателя карты	Кодированные видеоданные, используемые для портретного изображения держателя карты	n 1	6C
5F34	Порядковый номер карты	Номер, посредством которого различаются отдельные карты с одним и тем же первичным идентификатором счета	n 2	66
53	Произвольные данные	Обеспечивает стандартный способ представления DE, не определяемого в настоящем стандарте и стандартах серии ИСО/МЭК 7816. Его использование в пределах контрольной информации файла и шаблона приложения определено в ИСО/МЭК 7816-4 и ИСО/МЭК 7816-5. Раздел 5 настоящего стандарта охватывает все случаи, где этот IDO можно отыскать	Переменные	Во всех шаблонах, определяемых в приложении А

Продолжение таблицы 10

Тег	Наименование элемента данных	Описание и ссылка на стандарт	Длина/ формат	Может быть найден в шаблоне
73	Произвольные DO	Обеспечивает стандартный способ представления связи объектов DO, не установленных в настоящем стандарте и стандартах серии ИСО/МЭК 7816. Его использование в пределах контрольной информации файла и шаблона приложения определено в ИСО/МЭК 7816-4 и ИСО/МЭК 7816-5. Раздел 5 настоящего стандарта охватывает все случаи, где этот IDO можно отыскать	Переменные	Во всех шаблонах, определяемых в приложении А
5F29	Профиль обмена	DE, описывающий возможности ICC для выполнения обменной операции	Предстоит определить	67
51	Путь	По ИСО/МЭК 7816-4	Переменные	61
5F48	Секретный ключ держателя карты	DE, содержащий секретный ключ держателя карты для электронной цифровой подписи, использующей асимметричные механизмы	Переменные	65
5F30	Сервисный код	Идентификация географической/сервисной доступности (см. структуру в ИСО/МЭК 7813, кодирование — в ИСО 8583)	n 3	6E
7F21	Сертификат держателя карты	Составной DO, содержащий открытый ключ держателя карты, дополнительную информацию, подпись органа по сертификации	Переменные	65
5D	Список заголовков	Сцепление пар тег/длина без разграничителя	Переменные	—
5C	Список тегов	Сцепление тегов без разграничителей	Переменные	—
5F41	Список элементов	Последовательность элементов и относящейся к ним информации без идентификаторов (см. 4.3)	Переменные	—
5F47	Ссылка на сообщение	DE, устанавливающий указатель сообщения	Переменные	66
5F37	Статическая внутренняя аутентификация (одноступенчатая)	DE, содержащий значение электронной цифровой подписи, который может быть использован либо отдельно, либо в сочетании с DE с тегами '5F38' и '5F39'	Предстоит определить	67
5F39	Статическая внутренняя аутентификация — вторые ассоциированные данные	Данные, дополняющие сертификат открытого ключа (тег '5F38'), используемые для получения заверенного открытого ключа	Предстоит определить	67
5F38	Статическая внутренняя аутентификация — первые ассоциированные данные	DE, содержащий сертификат открытого ключа и подлежащий использованию либо отдельно, либо в сочетании с DE с тегом '5F39' с целью предоставления возможности получить значение открытого ключа	Предстоит определить	67

Окончание таблицы 10

Тег	Наименование элемента данных	Описание и ссылка на стандарт	Длина/ формат	Может быть найден в шаблоне
5F2F	Стратегия использования PIN-кода	Устанавливает, требуется ли ввод PIN-кода и при каких условиях (см. 6.4)	Два байта	6E
5F32	Счетчик операций	Счетчик, обеспечивающий учет каждой последующей операции приложения карты	Двоичный формат. Переменные	6E
5F46	Таймер	DE, устанавливающий максимальное время (в десятых долях секунды) для процесса, который необходимо выполнить	Два двоичных байта. Второй байт младший	66
41	Указатель страны	См. 4.4.4	Переменные	—
42	Указатель эмитента	См. 4.4.4	Переменные	—
5F27	Управление обменом	Должен использоваться в сочетании с кодом страны, чтобы показать, разрешен ли международный обмен по карте (см. ИСО 4909)	n 1	66
7F20	Управление отображением	Шаблон, используемый для управления данными, выводимыми на экран терминала	Переменные	66
6B	Уточненное имя	Имя физического лица и сопутствующая информация, например пол, дата рождения и т. д. (см. 6.2)	Переменные	65
47	Функциональные возможности карты	По ИСО/МЭК 7816-4	Переменные	66
7D	Шаблон безопасного обмена сообщениями	См. 4.4.2	Переменные	—
6A	Шаблон начала сеанса	Данные, предназначенные для установления связи интерфейсного устройства с удаленным главным компьютером, удаленным сервером или приложением в этих устройствах (см. 6.3)	Переменные	6E
6D	Шаблон образа приложения	Шаблон, содержащий, по меньшей мере, образ приложения (см. ИСО/МЭК 10918-1)	Переменные	6E
6C	Шаблон образов держателя карты	Образы, относящиеся к держателю карты и хранимые на ICC	Переменные	65
6F	Шаблон FCI	См. 4.4.2	Переменные	—
62	Шаблон FCP	См. 4.4.2	Переменные	—
64	Шаблон FMD	См. 4.4.2	Переменные	—
5F36	Экспонента валюты	Кодирует число, в соответствии с которым количество валюты, указанное в карте, должно быть увеличено (см. ИСО 4217)	n 1	6E
5F2D	Языковые предпочтения	Указывает в порядке предпочтения до четырех языков для держателя карты (см. ИСО 639)	a 2...a 8	65

8.2 Информационные объекты в числовом порядке

В таблице 11 представлены теги и наименования объектов DO в числовом порядке.

Таблица 11 — Объекты IDO в числовом порядке

Тег	Наименование элемента данных
06	Идентификатор объекта
41	Указатель страны
42	Указатель эмитента
43	Данные об услугах, предоставляемых картой
44	Начальные данные доступа
45	Данные эмитента
46	Данные, предваряющие эмиссию карты
47	Функциональные возможности карты
48	Информация о состоянии
4F	Идентификатор приложения
50	Метка приложения
51	Путь
52	Команда на выполнение
53	Произвольные данные
56	Дорожка 1 (приложение)
57	Дорожка 2 (приложение)
58	Дорожка 3 (приложение)
59	Дата истечения срока действия карты
5A	Первичный идентификатор счета (PAN)
5B	Имя
5C	Список тегов
5D	Список заголовков
5E	Данные начала сеанса (оригинальные)
5F20	Имя держателя карты
5F21	Дорожка 1 (карта)
5F22	Дорожка 2 (карта)
5F23	Дорожка 3 (карта)
5F24	Дата истечения срока действия приложения
5F25	Дата активации приложения
F26	Дата активации карты
5F27	Управление обменом
5F28	Код страны
5F29	Профиль обмена
5F2A	Код валюты
5F2B	Дата рождения
5F2C	Гражданство держателя карты

Продолжение таблицы 11

Тег	Наименование элемента данных
5F2D	Языковые предпочтения
5F2E	Биометрические данные держателя карты
5F2F	Стратегия использования PIN-кода
5F30	Сервисный код
5F32	Счетчик операций
5F33	Дата операции
5F34	Порядковый номер карты
5F35	Пол
5F36	Экспонента валюты
5F37	Статическая внутренняя аутентификация (одноступенчатая)
5F38	Статическая внутренняя аутентификация — первые ассоциированные данные
5F39	Статическая внутренняя аутентификация — вторые ассоциированные данные
5F3A	Динамическая внутренняя аутентификация
5F3B	Динамическая внешняя аутентификация
5F3C	Динамическая взаимная аутентификация
5F40	Портретное изображение держателя карты
5F41	Список элементов
5F42	Адрес
5F43	Изображение рукописной подписи держателя карты
5F44	Образ приложения
5F45	Дисплейное сообщение
5F46	Таймер
5F47	Ссылка на сообщение
5F48	Секретный ключ держателя карты
5F49	Открытый ключ держателя карты
5F4A	Открытый ключ органа по сертификации
5F4B	Идентификатор изготовителя интегральных схем
62	Шаблон FCP
63	Оболочка
64	Шаблон FMD
68	Особые условия пользователя
6A	Шаблон начала сеанса
6B	Уточненное имя
6C	Шаблон образов держателя карты
6D	Шаблон образа приложения
6F	Шаблон FCI
73	Произвольные DO
78	Источник распределения совместимых тегов

Окончание таблицы 11

Тег	Наименование элемента данных
79	Источник распределения сосуществующих тегов
7D	Шаблон безопасного обмена сообщениями
7F20	Управление отображением
7F2I	Сертификат держателя карты

ПРИЛОЖЕНИЕ А
(обязательное)

Межотраслевые шаблоны

Следующие необязательные шаблоны (см. таблицы А.1—А.5) следует использовать в случае, когда существует потребность в группировании объектов IDO внутри шаблонов. Совместимые и сосуществующие схемы распределения тегов могут использовать дополнительные шаблоны (см. 4.4). Порядок шаблонов и порядок объектов IDO в пределах шаблонов несущественны.

Таблица А.1 — Шаблон приложения (тег '61')

Тег	Длина/формат	Элемент данных
4F	Переменные	Идентификатор приложения (AID)
50	Переменные	Метка приложения
52	Переменные	Команда на выполнение
53	Переменные	Произвольные данные
73	Переменные	Произвольные DO
51	Переменные	Путь

Таблица А.2 — Данные, относящиеся к держателю карты (тег '65')

Тег	Длина/формат	Элемент данных
5F42	Переменные	Адрес
5F2E	Переменные	Биометрические данные держателя карты
7F21	Переменные	Сертификат держателя карты
6C	Переменные	Образы держателя карты
5F20	Переменные	Имя держателя карты
5F2C	n 3	Гражданство держателя карты
5F40	Переменные	Портретное изображение держателя карты
5F49	Переменные	Открытый ключ держателя карты
5F48	Переменные	Секретный ключ держателя карты
5F2B	n 8 YYYYMMDD	Дата рождения
53	Переменные	Произвольные данные

Окончание таблицы А.2

Тег	Длина/формат	Элемент данных
73	Переменные	Произвольные DO
5F2D	a 2...a 8	Языковые предпочтения
5B	Переменные	Имя
5F4A	Переменные	Открытый ключ органа по сертификации
6B	Переменные	Уточненное имя
5F35	a 1	Пол
68	Переменные	Особые условия пользователя

Таблица А.3

Тег	Длина/формат	Элемент данных
47	Переменные	Функциональные возможности карты
5F26	n 6 YYMMDD	Дата активации карты
59	n 4 YYMM	Дата истечения срока действия карты
45	Переменные	Данные эмитента
5F34	n2	Порядковый номер карты
5F28	n3	Код страны
53	Переменные	Произвольные данные
73	Переменные	Произвольные DO
7F20	Переменные	Управление отображением
5F45	Переменные	Дисплейное сообщение
44	Переменные	Начальные данные доступа
5F27	n 1	Управление обменом
5F47	Переменные	Ссылка на сообщение
46	Переменные	Данные, предваряющие эмиссию карты
5F46	Два двоичных байта	Таймер
5F21	ans...76	Дорожка 1 (карта)
5F22	n...37	Дорожка 2 (карта)
5F23	n...104	Дорожка 3 (карта)

Таблица А.4 — Аутентификационные данные (тег '67')

Тег	Длина/формат	Элемент данных
53	Переменные	Произвольные данные
73	Переменные	Произвольные DO
5F3B	Предстоит определить	Динамическая внешняя аутентификация
5F3A	Предстоит определить	Динамическая внутренняя аутентификация
5F3C	Предстоит определить	Динамическая взаимная аутентификация

Окончание таблицы А.4

Тег	Длина/формат	Элемент данных
5F29	Предстоит определить	Профиль обмена
5F37	Предстоит определить	Статическая внутренняя аутентификация (одноступенчатая)
5F38	Предстоит определить	Статическая внутренняя аутентификация — первые ассоциированные данные
5F39	Предстоит определить	Статическая внутренняя аутентификация — вторые ассоциированные данные

Таблица А.5 — Данные, относящиеся к приложению (тег '6E')

Тег	Длина/формат	Элемент данных
5F25	n 6 YYMMDD	Дата активации приложения
5F24	n 6 YYMMDD	Дата истечения срока действия приложения
4F	Переменные	Идентификатор приложения
6D	Переменные	Шаблон образа приложения
50	Переменные	Метка приложения
5F2A	a 3 или n 3	Код валюты
5F36	n 1	Экспонента валюты
53	Переменные	Произвольные данные
73	Переменные	Произвольные DO
5E	Переменные	Данные начала сеанса (оригинальные)
6A	Переменные	Шаблон начала сеанса
5F2F	Два байта	Стратегия использования PIN-кода
5A	n...19	Первичный идентификатор счета (PAN)
5F30	n 3	Сервисный код
56	ans...76	Дорожка 1 (приложение)
57	n...37	Дорожка 2 (приложение)
58	n...104	Дорожка 3 (приложение)
5F32	Двоичный формат Переменные	Счетчик операций
5F33	n 4 или n 10 YDDD(HHMMSS)	Дата операции

ПРИЛОЖЕНИЕ Б
(справочное)

Примеры кодирования

В настоящем приложении представлены примеры кодирования в разных схемах распределения тегов. Разные DO пронумерованы следующим образом: DO1, DO2, DO3...

Байты закодированы в шестнадцатиричном формате, пробел использован в качестве разделителя. Для ясности в скобки заключены DO, сгруппированные внутри шаблонов; сами скобки не относятся к данным. Неопределенные байты обозначены XX.

Б.1 Идентификатор объекта, обозначающий стандарт ИСО

Кодирование идентификатора объекта определено в ГОСТ Р ИСО/МЭК 8825-1. Тег '06'. Первый байт значения составляет '28' (десятичное число 40). За данным байтом следует одна или несколько серий байтов, идентифицируемых тем, что b8 = 0 в последнем байте серии, b8 = 1 в других байтах серии. Биты с b7 по b1 байтов серии кодируют двоичное число. Первое число представляет собой номер стандарта, второе, если оно имеется, — номер части стандарта, состоящего из нескольких частей.

Для стандарта ИСО 9992-2 первая серия получается следующим образом:

- 9992 преобразуется в '2708'
- двоичное значение составляет 0010 0111 0000 1000
- двоичное значение составляет также 100 1110 000 1000
- после ввода бита b8 с соответствующим значением в каждый байт двоичное кодирование первой серии дает в результате 1100 1110 0000 1000, что эквивалентно 'CE08'.

Вторая серия представляет собой '02', так как номер части меньше 128. Следовательно, DO представляет собой 06 04 28 CE 08 02.

Б.2 Стандартная схема распределения тегов

DO1 = 59 02 95 02

DO2 = 5F 24 03 97 03 31

DO1 указывает дату истечения срока действия карты: февраль 1995 г.

DO2 указывает дату истечения срока действия приложения: 31 марта 1997 г.

Б.3 Совместимая схема распределения тегов, определяемая в ИСО 9992-2

DO1 = 78 06 (06 04 28 CE 08 02)

DO2 = 5F 24 03 97 03 31

DO3 = 70 04 (80 02 XX XX)

DO4 = 67 0A (5F 29 03 XX XX XX) (81 02 XX XX)

DO1 указывает совместимую схему распределения тегов, определяемую в ИСО 9992-2, обозначенном при помощи его идентификатора объекта. Данный IDO должен появляться в строке начальных данных, файле ATR или FCI файла DF.

DO2 указывает дату истечения срока действия приложения: 31 марта 1997 г.

DO3 содержит DO с тегом '80', определяемый в ИСО 9992-2; содержание тега '70' также определено в ИСО 9992-2.

DO4 содержит IDO «профиль обмена» (тег '5F29') и DO с тегом '81', определяемый в ИСО 9992-2; содержание тега '67' определено в настоящем стандарте.

Б.4 Другой пример совместимой схемы распределения тегов, определяемой в ИСО 9992-2

DO2 = 5F 24 03 97 03 31

DO3 = 70 0C (06 04 28 CE 08 02) (80 04 XX XX XX XX)

DO4 = 67 06 (5F 29 03 XX XX XX)

DO2 указывает дату истечения срока действия приложения: 31 марта 1997 г.

DO3 содержит DO (тег '06'), указывающий, что последующий DO (тег '80') определен в ИСО 9992-2. Содержание тега '70' также определено в ИСО 9992-2.

DO4 содержит IDO «профиль обмена» (тег '5F29'). Следует отметить, что DO4 не может содержать объекты DO, определяемые в ИСО 9992-2, из-за выбора не передавать IDO с тегом '78'.

Б.5 Сосуществующая схема распределения тегов, определяемая в стандарте ИСО

DO1 = 79 05 (06 03 28 XX XX)

DO2 = 7E 06 (5F 24 03 97 03 31)

DO3 = 70 06 XX XX XX XX XX XX

DO1 указывает сосуществующую схему распределения тегов, определяемую в стандарте ИСО, обозначенном при помощи идентификатора объекта со значением, начинающимся с '28'. В этом случае DO1 является обязательным. Данный IDO должен появляться либо в строке начальных данных, файле ATR, либо в FCI файла DF.

DO2 указывает дату истечения срока действия приложения: 31 марта 1997 г. Следует отметить, что IDO «дата истечения срока действия приложения» (тег '5F24') является вложенным.

DO3 можно интерпретировать исключительно в соответствии со стандартом, указанным в идентификаторе объекта.

УДК 336.77:002:006.354 ОКС 35.240.40 Э46 ОКП 40 8470

Ключевые слова: обработка данных, обмен информацией, идентификационные карты, IC-карты, элементы данных, кодирование (преобразование данных), форматы

Редактор *В.П. Огурцов*
Технический редактор *Л.А. Гусева*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *А.Н. Золотаревой*

Изд. лиц. № 02354 от 14.07.2000. Сдано в набор 27.10.2003. Подписано в печать 27.11.2003. Усл.печ.л. 3,72. Уч.-изд.л. 3,00.
Тираж 192 экз. С 12798. Зак. 1023.

ИПК Издательство стандартов, 107076 Москва, Колодезный пер., 14.
http: //www.standards.ru e-mail: info@standards.ru
Набрано в Издательстве на ПЭВМ
Отпечатано в филиале ИПК Издательство стандартов — тип. "Московский печатник", 105062 Москва, Лялин пер., 6.
Плр № 080102