ИКАО

Doc 9303

Машиносчитываемые проездные документы

Издание восьмое, 2021

Часть 10. Логическая структура данных (LDS) для хранения биометрических и других данных на бесконтактной интегральной схеме (ИС)

Утверждено и опубликовано с санкции Генерального секретаря

Международная организация гражданской авиации

ИКАО

Doc 9303

Машиносчитываемые проездные документы

Издание восьмое, 2021

Часть 10. Логическая структура данных (LDS) для хранения биометрических и других данных на бесконтактной интегральной схеме (ИС)

Утверждено и опубликовано с санкции Генерального секретаря

Международная организация гражданской авиации

Опубликовано отдельными изданиями на русском, английском,
арабском, испанском, китайском и французском языках
МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИЕЙ ГРАЖДАНСКОЙ АВИАЦИИ.
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Загрузить и получить дополнительную информацию можно на сайте
www.icao.int/Security/FAL/TRIP.

Doc 9303. ***Машиносчитываемые проездные документы***
Часть 10. ***Логическая структура данных (LDS) для хранения биометрических и других данных на бесконтактной интегральной схеме (ИС)***
Заказ №: 9303P10
ISBN 978-92-9265-533-4 (бумажная копия)

ПОПРАВКИ

Об издании поправок сообщается в дополнениях к *Каталогу продуктов и услуг;* Каталог и дополнения к нему имеются на веб-сайте ИКАО www.icao.int. Ниже приводится форма для регистрации таких поправок.

РЕГИСТРАЦИЯ ПОПРАВОК И ИСПРАВЛЕНИЙ

ПОПРАВКИ		
№	Дата	Кем внесено

ИСПРАВЛЕНИЯ		
№	Дата	Кем внесено

ОГЛАВЛЕНИЕ

Страница

1. СФЕРА ПРИМЕНЕНИЯ

В части 10 документа Doc 9303 определяется логическая структура данных (LDS) электронных МСПД, необходимая для обеспечения глобальной интероперабельности, и приводятся спецификации в отношении организации данных на бесконтактной интегральной схеме (ИС). Для этого необходимо определить все обязательные и факультативные элементы данных и упорядочить и/или сгруппировать их, что ДОЛЖНО соблюдаться для достижения глобальной интероперабельности при электронном считывании электронных паспортов.

В части 10 документа Doc 9303 содержатся спецификации, позволяющие государствам и соответствующим специалистам встроить бесконтактную ИС в электронный проездной документ. В настоящей части определяются все обязательные и факультативные элементы данных, структуры файлов и профили приложений для бесконтактной ИС.

В восьмом издании документа Doc 9303 содержатся спецификации, касающиеся факультативной регистрации информации о поездках, визах и дополнительных биометрических приложений (известных как приложения LDS2), рассматриваемые в качестве расширения обязательного приложения электронных МСПД (известного как LDS1).

Часть 10 рассматривается совместно с:

- частью 1 *"Введение"*;
- частью 3 *"Спецификации, общие для всех МСПД"*;
- частью 4 *"Спецификации машиносчитываемых паспортов (МСП) и других МСПД размера ПД3"*;
- частью 5 *"Спецификации машиносчитываемых официальных проездных документов (МСОПД) размера ПД1"*;
- частью 6 *"Спецификации машиносчитываемых официальных проездных документов (МСОПД) размера ПД2"*

и соответствующими частями, связанными с бесконтактной ИС:

- частью 9 *"Применение средств биометрической идентификации и электронного хранения данных в МСПД;*
- частью 11 *"Механизмы защиты МСПД"*;
- частью 12 *"Инфраструктура открытых ключей для МСПД"*.

2. СТРУКТУРА ЧАСТИ 10 ДОКУМЕНТА DOC 9303

Часть 10 документа Doc 9303 состоит из разделов, в которых рассматриваются:

Спецификации, общие для приложений LDS1 и LDS2:

- общие атрибуты;

- все команды, предусмотренные для LDS1 и LDS2;
- общие элементарные файлы (EF) для LDS1 и LDS2;

Спецификации для приложения LDS1 электронного МСПД;

Спецификации для приложения LDS2, касающиеся:

- записей о поездках;
- визовых записей;
- дополнительных биометрических параметров;
- условий доступа к файлам LDS2.

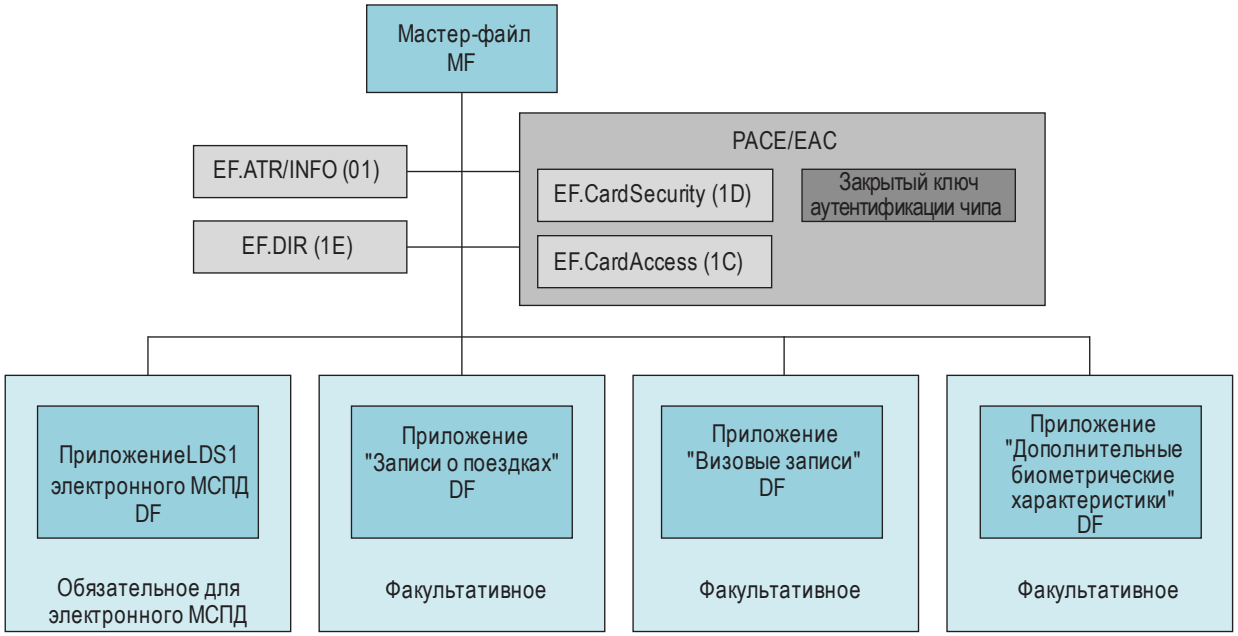

Рис. 1. Приложения для LDS1 и LDS2

Электронные МСПД могут поддерживать одно, несколько или все из перечисленных ниже приложений:

- приложение LDS1 электронного МСПД – ОБЯЗАТЕЛЬНОЕ;
- приложение LDS2, касающееся регистрации информации о поездках – ФАКУЛЬТАТИВНОЕ;
- приложение LDS2, касающееся регистрации информации о визах – ФАКУЛЬТАТИВНОЕ;
- приложение LDS2, касающееся дополнительных биометрических характеристик – ФАКУЛЬТАТИВНОЕ.

3. СПЕЦИФИКАЦИИ, ОБЩИЕ ДЛЯ LDS1 И LDS2

3.1 Минимальные требования к обеспечению интероперабельности

Нижеследующие требования ЯВЛЯЮТСЯ минимальными требованиями к обеспечению интероперабельности электронных паспортов, основанных на использовании бесконтактных ИС близкого действия:

- стандарты [ИСО/МЭК 14443-1], [ИСО/МЭК 14443-2], [ИСО/МЭК 14443-3], [ИСО/МЭК 14443-4] с учетом соответствующих поправок и исправлений;
- стандарт [ИСО/МЭК 10373-6], обеспечение соответствия спецификациям испытаний с учетом всех поправок и исправлений;
- интерфейс сигналов типа A или типа B;
- поддержка файловой структуры, определяемой стандартом [ИСО/МЭК 7816-4] для транспарентных файлов различной длины;
- поддержка одного или нескольких приложений и соответствующих команд, определяемых стандартом [ИСО/МЭК 7816-4], как указано в документе Doc 9303.

3.2 Электрические характеристики

Мощность высокочастотного сигнала и сигнальный интерфейс СООТВЕТСТВУЮТ спецификациям стандарта [ИСО/МЭК 14443-2]. Рекомендуется использовать скорость передачи сигнала равную как минимум 424 кбит/с. Применение характеристик электромагнитных помех (EMD), указанных в стандарте [ИСО/МЭК 14443-2], является ФАКУЛЬТАТИВНЫМ.

3.3 Физические характеристики

Рекомендуется, чтобы размер зоны соединения антенны соответствовал только классу 1 (размер антенны ID-1) стандарта [ИСО/МЭК 14443-1].

3.4 Протокол передачи данных

Электронный МСПД ПОДДЕРЖИВАЕТ протокол полудуплексной передачи, определяемой стандартом [ИСО/МЭК 14443-4]. Электронный МСПД ПОДДЕРЖИВАЕТ протоколы передачи типа A или типа B, и протоколы инициализации, предотвращения коллизий и передачи данных в соответствии со стандартом ИСО/МЭК 14443.

3.4.1 Команды Request и Answer to Request

Бесконтактная ИС ОТВЕЧАЕТ на команду запроса типа A (REQA) или команду запроса типа B (REQB), давая ответ на запрос типа A (ATQA) или ответ на запрос типа B (ATQB) в зависимости от конкретного случая.

3.4.2 Произвольный идентификатор в сравнении с фиксированным идентификатором для бесконтактной ИС

Электронный МСПД может служить своеобразным "маяком", в котором бесконтактная ИС при начальной активации выдает уникальный идентификатор (UID) для типа A и PUPI для типа B. Это может позволить идентифицировать полномочный орган выдачи. Стандарт [ИСО/МЭК 14443] позволяет сделать выбор, будет ли у электронного МСПД фиксированный, присвоенный только ему идентификатор, или будет использоваться произвольный номер, который меняется каждый раз, когда начинается коммуникационный обмен. Некоторые государства выдачи предпочитают применять уникальный номер по причинам безопасности или по иной причине. Другие государства выдачи больше руководствуются опасениями относительно конфиденциальности и возможности отслеживать лиц благодаря фиксированным идентификаторам ИС.

Выбор того или другого варианта не снижает интероперабельности, поскольку считывающий терминал, если он соответствует спецификациям стандарта [ИСО/МЭК 14443], понимает оба метода. РЕКОМЕНДУЕТСЯ использовать произвольные идентификаторы ИС, однако государства могут выбрать вариант с применением уникальных UID для типа A или уникальных PUPI для типа B.

3.5 Набор команд

Все команды, форматы и их байты состояния определяются стандартами [ИСО/МЭК 7816-4] и [ИСО/МЭК 7816-8], за исключением команды управления файлами и памятью (FILE AND MEMORY MANAGEMENT). Минимальный набор команд, поддерживаемый LDS1 электронного МСПД, ДОЛЖЕН быть следующим:

SELECT;
READ BINARY.

Признано, что для создания надлежащих условий безопасности и выполнения факультативных положений по защите, содержащихся в части 11 документа Doc 9303, требуются дополнительные команды. Для внедрения механизмов, указанных в части 11 документа Doc 9303, необходима поддержка следующих дополнительных команд:

GET CHALLENGE;
EXTERNAL AUTHENTICATE / MUTUAL AUTHENTICATE;
INTERNAL AUTHENTICATE;
MANAGE SECURITY ENVIRONMENT;
GENERAL AUTHENTICATE.

Если присутствуют факультативные приложения LDS2, то электронный МСПД дополнительно ПОДДЕРЖИВАЕТ следующие команды:

для приложения "Записи о поездках":
READ RECORD;
APPEND RECORD;
SEARCH RECORD;
FILE AND MEMORY MANAGEMENT;
PERFORM SECURITY OPERATION (PSO).

для приложения "Визовые записи":

READ RECORD;
APPEND RECORD;
SEARCH RECORD;
FILE AND MEMORY MANAGEMENT;
PERFORM SECURITY OPERATION (PSO).

для приложения "Дополнительные биометрические характеристики":

UPDATE BINARY;
READ RECORD;
APPEND RECORD;
SEARCH RECORD;
ACTIVATE;
FILE AND MEMORY MANAGEMENT;
PERFORM SECURITY OPERATION (PSO).

Дополнительная информация, касающаяся протоколов команд, приводится в части 11 документа Doc 9303.

3.5.1 Команда SELECT

LDS1 электронного МСПД поддерживает два метода выбора структуры, включающие идентификатор файлов и короткий идентификатор EF. Считыватели поддерживают по крайней мере один из этих двух методов. Идентификатор файла и короткий идентификатор EF являются ОБЯЗАТЕЛЬНЫМИ для операционной системы бесконтактной ИС, но ФАКУЛЬТАТИВНЫМИ для считывателя.

3.5.2 Команда READ BINARY

Поддержка электронным МСПД команды READ BINARY с нечетным байтом INS является УСЛОВНО ОБЯЗАТЕЛЬНОЙ. Электронный МСПД ПОДДЕРЖИВАЕТ этот вариант команды, если он поддерживает группы данных размером 32 68 байтов или более.

3.6 Форматы команд и параметрические варианты (LDS1 и LDS2)

3.6.1 Выбор приложения DF с использованием команды SELECT

Приложения должны выбираться по имени их DF, соответствующему идентификатору приложения (AID). После выбора приложения можно получить доступ к файлу в данном приложении.

Примечание. Имена DF должны быть уникальными. Поэтому выбор приложения с использованием имени DF может производиться из любого места.

3.6.1.1 Выбор мастер-файла (MF)

Таблица 1. Команда SELECT для выбора MF

CLA	‘00’
INS	‘A4’
P1	‘00’
P2	‘0C’
Поле Lc	Отсутствует
Поле данных	Отсутствует
Поле Le	Отсутствует

Ответ на команду SELECT

Поле данных	Отсутствует
SW1-SW2	Нормальная обработка ‘9000’ Другие значения для индикации ошибок контроля и выполнения

Примечание. РЕКОМЕНДУЕТСЯ не использовать команду SELECT MF.

3.6.1.2 Выбор приложения DF

Приложение DF ВЫБИРАЕТСЯ посредством команды SELECT с именем DF, соответствующем идентификатору приложения (AID). Параметры команды блока данных прикладного протокола (APDU) указаны ниже.

Таблица 2. Команда SELECT с AID для выбора приложения DF

CLA	‘00’
INS	‘A4’
P1	‘04’
P2	‘0C’
Поле Lc	Длина поля данных команды
Поле данных	Имя DF (AID)
Поле Le	Отсутствует

Ответ на команду SELECT

Поле данных	Отсутствует
SW1-SW2	Нормальная обработка ‘9000’ Другие значения для индикации ошибок контроля и выполнения

3.6.2 Выбор EF посредством команды SELECT

EF выбирается посредством команды SELECT с идентификатором EF. Когда выбирается файл EF, необходимо убедиться в том, что приложение DF, в котором хранятся файлы EF, уже выбрано.

Таблица 3. Команда SELECT с идентификатором файла для выбора EF

CLA	‘00’ / ‘0C’
INS	‘A4’
P1	‘02’
P2	‘0C’
Поле Lc	‘02’
Поле данных	Идентификатор файла
Поле Le	Отсутствует

Ответ на команду SELECT

Поле данных	Отсутствует
SW1-SW2	Нормальная обработка ‘9000’ Другие значения для индикации ошибок контроля и выполнения

Электронный МСПД ПОДДЕРЖИВАЕТ команду SELECT с использованием идентификатора файла, как указано в таблице 3. Система проверки ПОДДЕРЖИВАЕТ по крайней мере один из следующих способов:

- команду SELECT с использованием идентификатора файла, как указано в таблице 3;
- команду READ BINARY с использованием четного кода INS и короткого идентификатора EF, как указано в таблице 5.

3.6.3 Считывание данных с EF (команда READ BINARY)

Имеются два способа считывания данных с электронного МСПД: путем выбора EF с последующим считыванием данных выбранного EF или путем прямого считывания данных с использованием короткого идентификатора EF. Для МСПД поддержка короткого идентификатора EF является ОБЯЗАТЕЛЬНОЙ. В этой связи РЕКОМЕНДУЕТСЯ, чтобы система проверки использовала короткий идентификатор EF.

3.6.3.1 Считывание данных с выбранного файла EF (транспарентный файл)

Таблица 4. Команда READ BINARY для выбранного EF

CLA	‘00’ / ‘0C’
INS	‘B0’
P1	Смещение

P2	
Поле Lc	Отсутствует
Поле данных	Отсутствует
Поле Le	Присутствует для кодирования Ne > 0

Ответ на команду READ BINARY

Поле данных	Данные считывания
SW1-SW2	Нормальная обработка ‘9000’ Другие значения для индикации ошибок контроля и выполнения

3.6.3.2 Считывание данных идентификатора EF (транспарентный файл)

Таблица 5. Команда READ BINARY с коротким идентификатором EF

CLA	‘00’ / ‘0C’
INS	‘B0’
P1	Идентификатор короткого файла EF
P2	Смещение
Поле Lc	Отсутствует
Поле данных	Отсутствует
Поле Le	Присутствует для кодирования Ne > 0. Максимальное ожидаемое число байтов в поле данных ответа

Ответ на команду READ BINARY

Поле данных	Данные считывания
SW1-SW2	Нормальная обработка ‘9000’ Другие значения для индикации ошибок контроля и выполнения

3.6.4 Поддержка увеличенных Lc/Le

В зависимости от размера криптографических объектов (например, открытые ключи, подписи) для передачи этих данных на чип электронного МСПД ДОЛЖНЫ использоваться APDU с увеличенной длиной полей. Подробная информация об увеличенной длине поля приводится в стандарте [ИСО/МЭК 7816-4].

3.6.4.1 Поля увеличенной длины и чипы электронных МСПД

Применительно к чипам электронных МСПД поддержка поля увеличенной длины является УСЛОВНО ОБЯЗАТЕЛЬНОЙ. Если размеры криптографических алгоритмов и ключей, выбранные государством выдачи, требуют использования поля увеличенной длины, то чипы электронных МСПД ПОДДЕРЖИВАЮТ поле

увеличенной длины. Если чип электронного МСПД поддерживает поле увеличенной длины, то это ДОЛЖНО быть указано в ATS или в EF.ATR/INFO согласно стандарту [ИСО/МЭК 7816-4].

3.6.4.2 Терминалы

Для терминалов поддержка увеличенной длины поля является ОБЯЗАТЕЛЬНОЙ. Прежде чем использовать такой вариант, терминал ДОЛЖЕН проверить, содержится ли в ATR/ATS чипа электронного МСПД или в файле EF.ATR/INFO информация о поддержке увеличенной длины поля. Терминал НЕ ДОЛЖЕН использовать увеличенную длину поля для APDU, кроме нижеследующих команд, за исключением случаев, когда в ATR/ATS или в EF.ATR/INFO четко указаны точные размеры входного и выходного буфера электронного МСПД.

- MSE:Set KAT;
- GENERAL AUTHENTICATE.

3.6.5 Формирование цепочки команд

Для команды GENERAL AUTHENTICATE НЕОБХОДИМО сформировать цепочку команд, чтобы связать очередность команд с выполнением протокола. Формирование цепочки команд НЕ ДОЛЖНО использоваться для каких-либо иных целей, если это четко не предусмотрено чипом. Подробная информация о формировании цепочки команд содержится в стандарте [ИСО/МЭК 7816-4].

3.6.6 EF размером более 32 767 байтов

Максимальный размер EF обычно составляет 32 767 байтов, однако некоторые бесконтактные ИС поддерживают более крупные файлы. При смещении свыше 32 767 для доступа к зоне данных требуется иной параметрический вариант и формат команды READ BINARY. Этот формат команды СЛЕДУЕТ использовать после установления длины шаблона и потребности в доступе к данным в расширенной зоне данных. Например, если зона данных содержит несколько объектов биометрических данных, считывать всю зону данных, возможно, не требуется. Если смещение зоны данных свыше 32 767, то этот формат команды ИСПОЛЬЗУЕТСЯ. Смещение указывается в поле команд, а не в параметрах P1 и P2.

Таблица 6. Формат команды READ BINARY в случае смещения, превышающего 32 767 байтов

CLA	‘00’ / ‘0C’
INS	‘B1’
P1	См. таблицу 7
P2	
Поле Lc	Длина поля данных команды
Поле данных	Смещение DO’54’
Поле Le	Присутствует для кодирования Ne > 0. Максимальное ожидаемое число байтов в поле ответных данных

Ответ на команду READ BINARY

Поле данных	Дискреционный DO’53’
SW1-SW2	Нормальная обработка ‘9000’ Другие значения для индикации ошибок контроля и выполнения

Таблица 7. Кодирование P1-P2 команды READ BINARY с INS = B1

P1								P2								Смысловое содержание
b8	b7	b6	b5	b4	b3	b2	b1	b8	b7	b6	b5	b4	b3	b2	b1	
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Выбранный файл EF
0	0	0	0	0	0	0	0	0	0	0	Не все являются равными					Короткий идентификатор файла EF
Не все являются нулями											X	X	X	X	X	Идентификатор файла EF

Как поле длины, так и поле значения объекта данных BER-TLV имеют переменную длину и могут кодироваться различными способами (см. [ИСО/МЭК 7816-4]: "Поля длины данных BER-TLV").

В целях повышения эффективности СЛЕДУЕТ обеспечить, чтобы связь между электронным МСПД и терминалом была как можно короче. Поэтому поля длины и значения в объекте данных BER-TLV ДОЛЖНЫ быть как можно короче. Это применяется не только к объектам смещенных данных в командах READ BINARY с нечетным байтом INS, но также ко всем другим объектам данных BER-TLV, обмениваемым между электронным МСПД и терминалом.

Примеры закодированного смещения в поле данных:

- смещение: '0001' кодируется как тег = '54', длина = '01', значение = '01';
- смещение: 'FFFF' кодируется как тег = '54', длина = '02', значение = 'FFFF'.

Последующие команды READ BINARY УКАЗЫВАЮТ смещение в поле данных. Заключительной команде READ BINARY СЛЕДУЕТ запрашивать остальную зону данных.

В отношении стандарта [ИСО/МЭК 7816-4] отсутствуют какие-либо ограничения, предусмотренные для значения смещения, когда бит 1 INS установлен на 1 для обеспечения возможности более широкого использования.

Примечание 1. В некоторых случаях имеются электронные МСПД, в которых команда B1 и традиционная команда B0 READ BINARY не могут перекрывать друг друга. Иными словами, для считывания первых 32 767 байтов следует использовать только команду B0, а команду B1 – для считывания данных от 32 килобайт и далее. Для других целей возможно небольшое перекрытие в 256 байтов вокруг порога в 32 767, чтобы обеспечить более плавный переход между B0 и B1. Для указанной последней группы команду B1 можно использовать с самого начала файла, т. е. со смещением, начинающимся с 0, чтобы можно было использовать ту же самую команду для считывания полного содержания.

Примечание 2. Нечетный байт INS не должен использоваться системой проверки, если размер EF составляет 32 767 байтов или менее.

3.7 Обработка регистрационных записей и соответствующие команды

Регистрационные записи о поездках, визах и сертификатах ДОЛЖНЫ храниться в файлах EF под соответствующими приложениями и иметь линейную структуру с записями переменного размера. См. рис. 4 и 5.

В рамках каждого EF записи ДОЛЖНЫ обозначаться номером. Каждый номер записи ДОЛЖЕН быть уникальным и последовательным (выбранные записи с нулевой ссылкой рамками настоящего документа не охватываются).

В каждом EF, поддерживающем линейную структуру, номера записей при их внесении ДОЛЖНЫ присваиваться последовательно в порядке создания; первая запись (номер один) является записью, созданной первой.

Для доступа к записям должны использоваться указанные ниже команды, предусмотренные стандартом [ИСО/МЭК 7816-4]:

- APPEND RECORD — внесение регистрационных записей о поездках, визах, сертификатах;
- READ RECORD(S) — считывание одной или нескольких регистрационных записей о поездках, визах, сертификатах;
- SEARCH RECORD — поиск одной или нескольких регистрационных записей о поездках, визах, сертификатах.

Примечание. Сокращения, используемые в настоящем подразделе, определяются в стандарте [ИСО/МЭК 7816-4].

3.7.1 Команда APPEND RECORD

Эта команда инициирует регистрацию новой записи в конце линейной структуры.

Таблица 8. Команда APPEND RECORD

CLA	‘0C’
INS	‘E2’
P1	‘00’ (любое другое значение недействительно)
P2	См. таблицу 10
Поле Lc	Длина поля данных команды
Поле данных	Запись, подлежащая регистрации
Поле Le	Отсутствует

Таблица 9. Ответ на команду APPEND RECORD

Поле данных	Отсутствует
SW1-SW2	‘9000’ Нормальная обработка; ‘6A84’ Недостаточная емкость памяти в файле; ‘6700’ Неверно указанная длина (длина записи, подлежащей регистрации, превышает максимальную длину); Другие значения для индикации ошибок контроля или выполнения

Таблица 10. Кодирование P2 в команде APPEND RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Смысловое содержание
x	x	x	x	x	-	-	-	Короткий идентификатор EF
-	-	-	-	-	0	0	0	Любое другое значение является зарезервированным для использования в будущем (RFU)

3.7.2 Команда READ RECORD

Эта команда возвращает полное или частичное содержание одной или нескольких адресных записей выбранного EF. В зависимости от размера записи и содержания поля Le в поле данных ответа содержится один из следующих элементов:

- первая часть адресной записи;
- одна (или несколько) полная(ых) запись(ей);
- одна (или несколько) полная(ых) запись(ей), за которой(ыми) следует первая часть последующей записи.

Подробная информация содержится в стандарте [ИСО/МЭК 7816-4], а пример считывания зарегистрированных записей о поездках приводится в добавлении H.

Рисунок 2 иллюстрирует поле данных ответа. Сравнение Nr со структурой TLV показывает, является ли уникальная запись (считывание одной записи) или последняя запись (считывание всех записей) неполной, полной или заполненной незначащей информацией.

Таблица 11. Команда READ RECORD

CLA	‘0C’	
INS	‘B2’	
P1	Номер записи (‘00’ обозначает текущую запись)	
P2	См. таблицу 13	
Поле Lc	Отсутствует	
Поле данных	INS = ‘B2’	Отсутствует

Поле Le	Максимальное количество байтов, подлежащих считыванию, кодируются в качестве поля увеличенной длины; Le = ’00 00 00’ (любое другое значение рамками этой спецификации не охватывается)

Таблица 12. Ответ на команду READ RECORD

Поле данных	Считывание данных
SW1-SW2	‘9000’ Нормальная обработка; ‘6A83’ (запись не найдена); Другие значения для индикации ошибок контроля или выполнения

Таблица 13. Кодирование P2 с командой READ RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Смысловое содержание
x	x	x	x	x	-	-	-	Короткий идентификатор EF
-	-	-	-	-	1	x	x	**Номер записи в P1**
-	-	-	-	-	1	0	0	— Считывание записи P1
-	-	-	-	-	1	0	1	— Считывание всех записей от P1 до последней

Примечание 1. Другие комбинации битов в настоящей спецификации не рассматриваются. Если поле Le содержит только байты, установленные на ‘00’, то данная команда должна полностью обеспечивать считывание либо одной запрашиваемой записи, либо запрашиваемой последовательности записей, в зависимости от битов 3, 2 и 1 P2 и в рамках предельного значения максимально поддерживаемой длины доля расширенного поля Le.

Примечание 2. Команда READ RECORD с полями укороченной длины рамками настоящей спецификации не охватывается.

Случай a. Полное считывание одной записи (поле Le содержит только биты, установленные на ‘00’)

Запись

5F44	L	V	73	L	V	…	5F37	L	V	5F38	L	V

Ответ на команду READ RECORD (P2 = ‘04’, Le = 0):

5F44	L	V	73	L	V	…	5F37	L	V	5F38	L	V

Случай b. Считывание нескольких записей до конца файла (поле Le содержит только байты, установленные на ‘00’)

Запись 1								Запись 2								Запись X
5F44	L	V	...	5F38	L	V		5F44	L	V	...	5F38	L	V		...
Ответ на команду READ RECORD (P2 = ‘05’, Le = 0):																
5F44	L	V	...	5F38	L	V		5F44	L	V	...	5F38	L	V		...

Рис. 2. Поля данных ответа

3.7.3 Команда SEARCH RECORD

Эта команда инициирует поиск записей, хранимых в соответствующем EF. Поле данных команды содержит DO’7F76’ обработки записей, определяющее ссылку на файл, конфигурацию поиска и строку поиска (см. таблицу 17). Поле данных ответа возвращает DO’7F76’ обработки записей, содержащее одно или несколько DO’02’ и содержащее номер записи, соответствующий критериям поиска в рамках адресного EF.

В EF поддерживающем записи переменного размера в рамках линейной структуры этот поиск НЕ МОЖЕТ учитывать записи с окном поиска, более коротким, чем строка поиска.

Таблица14. Команда SEARCH RECORD

CLA	‘0C’
INS	‘A2’
P1	‘00’
P2	См. таблицу 16
Поле Lc	Длина поля данных команды
Поле данных	DO’7F76’ обработки записей (см. таблицу 17)
Поле Le	‘00’ (короткое) или’00 00’ (расширенное)

Таблица 15. Ответ на команду SEARCH RECORD

Поле данных	Шаблон обработки записей DO‘7F76‘, содержащий один DO‘51’ со ссылкой на файл и DO‘02‘ с одним или несколькими целыми числами , а также номер записи, совпадающий с критериями поиска
SW1-SW2	‘9000’ Нормальная обработка; ‘6282’ Предупреждение: неудачный поиск Другие значения для индикации ошибок контроля или выполнения

Примечание. Если совпадение не найдено, то поле данных ответа может отсутствовать.

Таблица 16. Кодирование P2 для команды SEARCH RECORD

b8	b7	b6	b5	b4	b3	b2	b1	Смысловое содержание
1	1	1	1	1	0	0	0	Поиск записи посредством нескольких EF
Любое другое значение является зарезервированным для использования в будущем (RFU)								

Таблица 17. Шаблон обработки записей для расширенного поиска множественных записей

Тег	Значение				Замечания
‘7F76’					DO обработки записей
	Тег	**Значение**			
	‘51’	Идентификатор файла или короткий идентификатор EF			DO "ссылка на файл"
	‘A1’				Шаблон конфигурации описка
		Тег	**Значение**		
		‘80’	‘00’ / ’30’		Параметр конфигурации поиска: - поиск по номеру записи в возрастающем порядке - ширина шага для поиска: побайтовый - окончание поиска: ‘00’ – поиск всех адресных записей ‘30’ – окончание поиска после первого совпадения
		‘B0’			Шаблон окна поиска
			Тег	**Значение**	
			‘02’	Смещение	
			‘02’	Количество байтов	
	Тег	**Значение**			
	‘A3’				Шаблон строки поиска
		Тег	**Значение**		
		‘B1’			
			Тег	**Значение**	
			‘81’	Строка поиска	

Примечание 1. Пустое смещение DO в шаблоне окна поиска не поддерживается.

Примечание 2. Если шаблон окна поиска использует значение ‘00’ для количества байтов, чип электронного МСПД LDS2 ДОЛЖЕН осуществлять поиск всех байтов из смещения в записях.

Примечание 3. Команда SEARCH RECORD поддерживает только DO, указанные в таблице 17. Это подразумевает, что команда SEARCH RECORD конкретно поддерживает DO "ссылка на файл" в DO "обработка записей" и конкретно одну строку поиска в шаблоне строк поиска. Эта команда МОЖЕТ игнорировать дополнительные DO или направлять ответ, содержащий код ошибки, если используются дополнительные DO.

3.8 Обработка транспарентных и других (LDS2) файлов

Транспарентные файлы EF, содержащие дополнительные биометрические характеристики, создаются органом, выпускающим электронные МСПД LDS2 в деактивизированном эксплуатационном состоянии (механизм создания рамками настоящей спецификации не охватывается). При наличии соответствующих разрешений в деактивизированном состоянии файлы EF могут выбираться, заполняться, обновляться и считываться.

При составлении и считывании транспарентных файлов EF ДОЛЖНЫ использоваться следующие команды, предусмотренные стандартом [ИСО/МЭК 7816-4]:

- UPDATE BINARY внесение дополнительных биометрических характеристик;
- READ BINARY считывание дополнительных биометрических характеристик.

Для инициирования транспарентного EF после успешного выполнения условий доступа к считыванию и записи LSD2 ДОЛЖНА использоваться следующая команда, предусмотренная стандартом [ИСО/МЭК 7816-9]:

- ACTIVATE инициирование файла, содержащего дополнительные биометрические характеристики EF.

Примечание. Акронимы, используемые в настоящем подразделе, определяются в стандарте [ИСО/МЭК 7816-4].

В активизированном состоянии EF может выбираться и считываться при наличии соответствующих разрешений (связанных с состоянием активизации) и никакое разрешение любого рода не позволяет осуществлять запись или дополнять транспарентный EF.

До записи информации для определения наличия достаточного объема памяти в EF НЕОБХОДИМО использовать команду FILE AND MEMORY MANAGEMENT (FMM).

Для файла EF.Biometrics IS ДОЛЖНА использовать следующую последовательность записи:

- Первая команда UPDATE BINARY (нечетный байт INS) ДОЛЖНА содержать в поле данных следующие DO:
  - DO’54’, содержащий смещение ‘00’;
  - DO’53’, который МОЖЕТ содержать первый блок данных, подлежащих хранению. Этот DO МОЖЕТ быть пустым (‘53 00’);
  - проприетарный DO’C0’, содержащий информацию об общем размере EF (объем памяти для распределения) является факультативным.

Примечание 1. Электронный МСПД с LDS2 МОЖЕТ использовать в DO'C0' информацию о размере EF для распределения внутренней памяти (например, для динамичного распределения памяти). Если электронный МСПД с LDS2 не поддерживает содержащуюся в DO информацию о размере EF (например, память распределена пользователем статически или электронный МСПД LDS2 поддерживает неявное динамичное перераспределение памяти EF), то электронный МСПД с LDS2 МОЖЕТ игнорировать DO'C0', приступить к записи первого блока EF и вернуть '9000', или он МОЖЕТ вернуть байт ошибки '6A80', свидетельствующий о неправильном параметре в поле данных команды.

Примечание 2. Если электронный МСПД с LDS2 возвращает любую ошибку в ответ на команду UPDATE BINARY с проприетарным DO'C0', то IS ДОЛЖНА направить предусмотренную стандартом [ИСО/МЭК 7816-4] команду UPDATE BINARY (нечетный байт INS) с нулевым смещением DO'54' и DO'53' без DO'C0'.

- Последующие команды UPDATE BINARY (нечетный байт INS, без DO'C0') ДОЛЖНЫ использовать смещение n+1, где n обозначает количество фактически записанных байтов в файл EF.Biometrics, т. е. терминалу СЛЕДУЕТ последовательно записывать данные EF без промежутка или перекрытия между двумя последующими командами UPDATE BINARY.

- Команда READ BINARY МОЖЕТ использоваться после любой команды UPDATE BINARY для проверки данных, записанных в EF.

- Команда ACTIVATE ДОЛЖНА завершать персонализацию файла EF.Biometrics путем перманентной блокировки записи в файл EF.

3.8.1 Команда UPDATE BINARY

Бесконтактная ИС, поддерживающая приложение "Дополнительные биометрические характеристики" ДОЛЖНА поддерживать команду UPDATE BINARY с нечетным байтом INS 'D7' в соответствии с таблицей 18.

Смещение определяет значение смещения объекта данных BER-TLV в поле данных команды; значение объекта дискретных данных BER-TLV в поле данных команды определяет данные, подлежащие внесению; значение факультативного объекта данных размера файла BER-TLV в поле данных команды определяет общий размер файла EF. При кодировании длина полей этих объектов данных BER-TLV должна быть как можно короче.

В тех случаях, когда поле данных команды UPDATE BINARY имеет проприетарный DO'C0', бит 8 байта CLA команды APDU ДОЛЖЕН быть установлен на 1 (CLA = '8C').

Таблица 18. Команда UPDATE BINARY с нечетным INS

CLA	'0C' / '8C'
INS	'D7'
P1	Идентификатор файла '00 00' идентифицирует текущий EF
P2	
Lc	Длина поля данных команды

Поле данных	Смещение объекта данных (тег ‘54’) || Объект дискретных данных (тег ‘53’) || Размер файла объекта данных (тег ‘C0’) (факультативно)
Le	Отсутствует

Таблица 19. Ответ на команду UPDATE BINARY

Поле данных	Отсутствует
SW1-SW2	‘9000’ Нормальная обработка; ‘6A84’ (Недостаточный объем памяти в файле) ‘6A80’ Неправильные параметры в поле данных команды (например, DO’C0 не поддерживается) ‘6982’ Неудовлетворительный статус защиты: файл EF.Biometrics находится в состоянии, инициированном EF Другие значения для индикации ошибок контроля или выполнения

Если IS не соблюдает последовательность UPDATE BINARY, как указано в разделе 3.8 (т. е., первая команда UPDATE BINARY не начинается со смещения 0), чип электронного МСПД с LDS2 МОЖЕТ прекратить выполнение команды UPDATE BINARY с ошибкой.

3.8.2 Команда ACTIVATE

Команда ACTIVATE инициирует переход выбранного файла дополнительных биометрических характеристик из состояния дезактивизации в состояние активизации.

Таблица 20. Команда ACTIVATE

CLA	‘0C’
INS	‘44’
P1	‘00’
P2	‘00’
Lc	Отсутствует
Поле данных	Отсутствует
Le	Отсутствует

Таблица 21. Ответ на команду ACTIVATE

Поле данных	Отсутствует
SW1-SW2	‘9000’ Нормальная обработка; Другие значения для индикации ошибок контроля или выполнения *Примечание 1. SW1-SW2 = ’61XX’ (нормальная обработка) и SW1-SW2 = ’62XX’ или ‘63XX’ (обработка с предупреждением) рамками настоящего документа не охватывается.*

После успешного выполнения этой команды выбранный файл EF.Biometrics ДОЛЖЕН быть переведен в активизированное состояние. В случае ошибки (SW отличается от ‘9000’) выбранный файл EF.Biometrics ДОЛЖЕН оставаться в дезактивизированном состоянии.

Сразу же после успешного выполнения этой команды (SW1-SW2 = ‘9000’) эффективная авторизация, необходимая для выполнения операции с использование файла EF.Biometrics, ДОЛЖНА соответствовать состоянию активизации (согласно таблице 98). Эффективная авторизация, соответствующая состоянию дезактивизации, НЕ ДОЛЖНА инициировать предоставление каких-либо прав доступа в отношении файла EF.Biometrics.

3.8.3 Команда FILE AND MEMORY MANAGEMENT

Команда FILE AND MEMORY MANAGEMENT (FMM) инициирует запрос относительно используемого или свободного объема памяти для адресного EF. Эта команда предоставляется для электронного МСПД с LDS2 в качестве проприетарной. Данная команда может использоваться для имеющегося свободного объема памяти адресного EF до начала записи или внесения изменений. Данная команда может также использоваться для получения номера последней внесенной записи с целью ее считывания. P1 индицирует метод адресации EF, и при этом могут использоваться текущий EF или DO’51’ "ссылка на файл". P2 индицирует содержание запроса. Предоставляется информация об общем количестве байтов в адресном EF с транспарентной структурой записи и количестве имеющихся или остающихся записей для адресной записи EF. Общее количество байтов включает в себя имеющиеся в EF без какой-либо структурной информации. Из этого количества исключена какая-либо информация, которая может потребоваться чипу электронного МСПД с LDS2. Допущение относительно количества остающихся записей заключается в том, что размер всех остающихся записей является максимальным. После успешного выполнения команды FMM ссылочный файл EF становится действующим файлом EF.

Таблица 22. Команда FILE AND MEMORY MANAGEMENT (FMM)

CLA	‘8C’	
INS	‘5F’	
P1	См. таблицу 23	
P2	См. таблицу 24	
Lc	Отсутствует для кодирования Nc = 0, присутствует для кодирования Nc > 0	
Поле данных	P1 = ’00’	Отсутствует
	P1 = ‘01’	DO’51’ "ссылка на файл" (см. [ИСО/МЭК 7816-4])
Le	‘00’	

P1 определяет метод выбора файла EF. P2 содержит поразрядную карту, определяющую информацию, которая ДОЛЖНА быть включена в ответ.

Таблица 23. Кодирование P1 в команде FFM

b8	b7	b6	b5	b4	b3	b2	b1	Смысловое содержание
0	0	0	0	0	0	0	0	Текущий EF
0	0	0	0	0	0	0	1	DO’51’ "ссылка на файл" в поле данных команды
Любое другое значение является зарезервированным для использования в будущем (RFU).								

Таблица 24. Кодирование P2 в команде FFM

b8	b7	b6	b5	b4	b3	b2	b1	Смысловое содержание
-	-	-	-	-	-	-	1	Общее количество байтов в адресном EF
-	-	-	-	-	-	1	-	Количество остающихся записей в адресной записи EF
-	-	-	-	-	1	-	-	Количество имеющихся записей в адресной записи EF
x	x	x	x	x	-	-	-	00000 (Любое другое значение является RFU)
Любое другое значение является зарезервированным для использования в будущем (RFU).								

Таблица 25. Кодирование DO’51’ в поле данных команды FMM

Тег	Длина	Значение
‘51’	1	Короткий идентификатор EF (биты b8–b4 кодируют номера с 1 по 30; биты b3–b1 устанавливаются на 000)
	2	Идентификатор файла

В ответе на команду FMM содержится набор DO, содержащих информацию о запрашиваемом файле и объеме памяти.

Таблица 26. Ответ на команду FMM

Поле данных	Отсутствует или контролирует информацию в соответствии с P2. См. таблицу 27.
SW1-SW2	‘9000’, ошибки контроля или выполнение в соответствии со стандартом [ИСО/МЭК 7816-4]

Таблица 27. Управление файлами и памятью

<table>
<tr><th>Тег</th><th>Длина</th><th colspan="3">Значение</th></tr>
<tr><td rowspan="4">‘7F78’</td><td rowspan="4">Var</td><td colspan="3">DO управления файлами и памятью</td></tr>
<tr><td>Тег</td><td>Длина</td><td>Значение</td></tr>
<tr><td>‘81’</td><td>Var</td><td>Общее количество байтов в адресном EF</td></tr>
<tr><td>‘82’</td><td>Var</td><td>Количество остающихся записей в адресной записи EF</td></tr>
<tr><td>‘83’</td><td>Var</td><td>Количество имеющихся записей в адресной записи EF</td></tr>
</table>

Примечание 1. Чип электронного МСПД с LDS2 ДОЛЖЕН возвращать только те объекты данных в DO FMM, которые запрашиваются посредством P2.

Примечание 2. Данные ответа FMM действительны только для указанного EF. Данные ответа FMM из других EF могут не быть независимыми, например, если различные EF совместно используют имеющуюся свободную память. IS должна это учитывать в случае комбинирования данных ответа FMM, содержащихся в различных EF.

Примечание 3. В случае применения к команде FMM безопасного обмена сообщениями ДОЛЖЕН использоваться DO’85’ "Безопасный обмен сообщениями (SM)" для инкапсулирования закодированных данных команды.

3.9 Спецификации структуры файла

Информация в электронном МСПД с LDS2 хранится в файловой системе, определяемой стандартом [ИСО/МЭК 7816-4]. Система файлов организуется иерархически и содержит выделенные (DF) и элементарные файлы (EF). Выделенные файлы DF содержат элементарные файлы (EF) или другие выделенные файлы. Факультативный мастер-файл (MF) может составлять основу файловой системы.

Примечание. Необходимость в мастер-файле определяется выбором операционных систем, приложениями LDS1 или LDS2 и условиями факультативного доступа.

3.9.1 Кодирование данных

В отношении элементов данных разрешается использовать следующие типы кодирования:

A = буквенный символ [a-z, A-Z];
N = цифровой символ [0-9];
S = специальный символ [‘<’];
B = бинарные данные;
U = символы UNICODE, закодированные в UTF-8.

Кодирование символов UNICODE в UTF-8:

- для любого символа, равного или меньшего 127 (hex ‘7F’), при кодировании в UTF-8 используется один байт, который повторяет значение ASCII;

- для символов равных или меньших 2047 (hex ‘07FF’) при кодировании в UTF-8 используется два байта:
  - первый байт имеет два набора старших битов и третий пустой бит (т. е. hex ‘C2’ до ‘DF’);
  - второй имеет набор старших битов и второй пустой бит (т. е. ‘80’ до ‘BF’);
- для всех символов, равных или больших 2048 и меньших 65 535 (hex ‘FFFF’) при кодировании в UTF-8 используются три байта.

3.10 Выбор приложения: DF

Электронный МСПД поддерживает по крайней мере одно приложение со следующими характеристиками:

- приложение LDS1 электронного МСПД является ОБЯЗАТЕЛЬНЫМ;
  - приложение LDS1 электронного МСПД СОСТОИТ из данных, записанных государством или организацией выдачи: группы данных 1–16 вместе с объектом защиты документа (EF.SOD);
  - объект защиты документа (EF.SOD) в рамках приложения LDS1 электронного МСПД состоит из указанных в частях 11 и 12 документа Doc 9303 значений хэшей используемых групп данных, и он необходим для валидации целостности данных, созданных органом выдачи или хранящихся в приложении LDS1 электронного МСПД.
- приложение LDS1 электронного МСПД МОЖЕТ факультативно поддерживать дополнительные приложения LDS2, описание которых приводится в документе Doc 9303:
  - приложение "Записи о поездках";
  - приложение "Визовые записи";
  - приложение "Дополнительные биометрические характеристики".

Кроме того, государства или организации выдачи могут принять решение об использовании других приложений. Структура файла ПОЗВОЛЯЕТ реализовать такие дополнительные приложения, однако подробное описание таких приложений выходит за рамки документа Doc 9303.

Приложения LDS1 и LDS2 ВЫБИРАЮТСЯ посредством использования идентификатора приложения (AID) в качестве зарезервированного имени DF. AID СОСТОИТ из идентификатора зарегистрированного приложения, присвоенного ИСО в соответствии со стандартом [ИСО/МЭК 7816-5], и проприетарного расширения идентификатора приложения (PIX), как определено в рамках настоящего документа:

В контексте приложения LDS1 электронного МСПД используются две различные схемы распределения тегов, касающиеся тегов классов приложений, как определено в части 10 документа Doc 9303 (тег LDS) и в стандарте [ИСО/МЭК 7816-6] (межотраслевой тег):

- файлы EF.ATR/INFO и EF.DIR используют межотраслевую схему распределения тегов;
- файлы DF и их EF используют схему распределения тегов LDS.

Отраслевые теги, указанные в настоящем документе, используются в контексте LDS, поэтому сосуществующая схема распределения тегов не требуется.

3.11 Общие элементарные файлы (EF)

В рамках MF МОГУТ иметь место следующие общие файлы EF для приложений LDS1 и LDS2:

- EF.ATR/INFO;
- EF.DIR;
- EF.CardAccess;
- EF.CardSecurity.

3.11.1 Файл EF.ATR/INFO (УСЛОВНО ОБЯЗАТЕЛЬНЫЙ)

Файл EF.ATR/INFO является транспарентным файлом EF, содержащимся в мастер-файле, и он является условно ОБЯЗАТЕЛЬНЫМ, если присутствует факультативное приложение LDS2. Этот файл EF является факультативным только в случае присутствия приложения LDS1. Коротким идентификатором файла EF на уровне MF является'01'.

Таблица 28. Файл EF.ATR/INFO

Имя файла	EF.ATR/INFO
ID файла	'2F01'
Короткий идентификатор EF	'01'
Доступ для выбора	ВСЕГДА
Доступ для считывания	ВСЕГДА
Доступ для записи/обновления/стирания	НИКОГДА
Структура файла	Транспарентная
Размер	Переменный

Содержание файла EF.ATR/INFO может быть извлечено посредством команды SELECT с последующей командой READ BINARY. Поле данных ответа на команду READ BINARY содержит содержание файла EF.ATR/INFO.

Таблица 29. Элементы данных файла EF.ATR/INFO для LDS2

<table>
<tr><th>Тег</th><th>Длина</th><th colspan="3">Значение</th><th>Примечание</th></tr>
<tr><td rowspan="5">‘47’</td><td rowspan="5">‘03’</td><td colspan="4">Возможности карточки</td></tr>
<tr><td colspan="3">байт 1 – первая программная функция</td><td>b8 = 1: выбор DF посредством полного имени DF
b7–b4 и b1 рамками документа Doc 9303 не охватываются
b3 = 1: короткий идентификатор файла EF поддерживается
b2 = 1: номер записи поддерживается</td></tr>
<tr><td colspan="3">байт 2 - вторая программная функция</td><td>b8, b7, b6 и b5 рамками документа Doc 9303 не охватываются
b4–b1 = 0001: размер единицы данных составляет один байт</td></tr>
<tr><td colspan="3">байт 3 - третья программная функция</td><td>b8 = 1: формирование цепочки команд поддерживается
b7 = 1: расширенные поля Lc и Le поддерживаются
b6 = 1: информация расширенной длины в файле EF.ATR/INFO
b5–b1 рамками документа Doc 9303 не охватываются</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td rowspan="4">‘7F66’</td><td rowspan="4">Var</td><td colspan="4">Информация расширенной длины</td></tr>
<tr><td>Тег</td><td>Длина</td><td>Значение</td><td>Примечания</td></tr>
<tr><td>‘02’</td><td>Var</td><td>Положительное целое число – максимальное количество байтов в команде APDU</td><td>Для LDS2 ДОЛЖНО, как минимум, составлять 1000 (десятичное значение)</td></tr>
<tr><td>‘02’</td><td>Var</td><td>Положительное целое число – максимальное количество байтов, ожидаемых в ответе APDU</td><td>Для LDS2 ДОЛЖНО, как минимум, составлять 1000 (десятичное значение)</td></tr>
</table>

Примечание 1. В файле EF.ATR/INFO МОГУТ присутствовать дополнительные объекты данных.

Примечание 2. Файл EF.ATR/INFO использует отраслевую схему распределения тегов, как определено в стандарте [ИСО/МЭК 7816-4].

3.11.2 Файл EF.DIR (УСЛОВНО ОБЯЗАТЕЛЬНЫЙ)

Файл EF.DIR является транспарентным файлом EF, содержащимся в мастер-файле, определяемом стандартом [ИСО/МЭК 7816-4]. Файл EF.DIR является условно ОБЯЗАТЕЛЬНЫМ, если присутствуют любые факультативные приложения LDS2. Если присутствует любое факультативное приложение LDS2, то файл EF.DIR ДОЛЖЕН включаться в структуру данных SecurityInfos, содержащуюся в файле EF.CardSecurity. Полное описание структуры данных SecurityInfo для EF.DIR приводится в части 11 документа Doc 9303.
Коротким идентификатором EF на уровне MF является‘1E’.

Таблица 30. Файл EF.DIR

Имя файла	EF.DIR
ID файла	‘2F00’
Короткий идентификатор EF	‘1E’
Доступ для выбора	ВСЕГДА
Доступ для считывания	ВСЕГДА
Доступ для записи/обновления/стирания	НИКОГДА
Структура файла	Транспарентная
Размер	Переменный

РЕКОМЕНДУЕТСЯ, чтобы в MF присутствовал файл EF.DIR. Файл EF.DIR ДОЛЖЕН присутствовать, если имеются более, чем одно обязательное приложение LDS1 и приводится перечень приложений, поддерживаемых электронным МСПД. В нем ДОЛЖЕН присутствовать набор шаблонов приложений, содержащих идентификатор приложения DO в любом порядке.

Таблица 31. Формат файла EF.DIR

Тег	**Длина**	**Значение**			**Описание**
‘61’	‘09’				Шаблон приложения LDS1 электронного МСПД
		Тег	**L**	**Значение**	Приложение LDS1 для международного применения электронных МСПД AID: ‘A0 00 00 02 47 10 01’
		‘4F’	‘07’	‘A0 00 00 02 47 10 01’	
‘61’	‘09’				Шаблон приложения "Записи о поездках"
		Тег	**L**	**Значение**	Международный AID приложения "Записи о поездках": ‘A0 00 00 02 47 20 01’
		‘4F’	‘07’	‘A0 00 00 02 47 20 01’	
‘61’	‘09’				Шаблон приложения "Визовые записи"

		Тег	L	Значение	Международный AID приложения "Визовые записи": ‘A0 00 00 02 47 20 02’
		‘4F’	‘07’	‘A0 00 00 02 47 20 02’	
‘61’	‘09’				Шаблон приложения "Дополнительные биометрические характеристики"
		Тег	L	Значение	Международный AID приложения "Дополнительные биометрические характеристики": ‘A0 00 00 02 47 20 03’
		‘4F’	‘07’	‘A0 00 00 02 47 20 03’	

Примечание. Файл EF.DIR использует стандартную схему распределения тегов, определенную в стандарте [ИСО/МЭК 7816-4].

3.11.3 Файл EF.CardAccess (УСЛОВНО ОБЯЗАТЕЛЬНЫЙ)

Файл EF.CardAccess представляет собой транспарентный EF, содержащийся в мастер-файле, и является условно ОБЯЗАТЕЛЬНЫМ, если используется факультативный контроль доступа PACE, как определено в части 11 документа Doc 9303. Полное описание структуры данных SecurityInfos для PACE приводится в части 11 документа Doc 9303.

Коротким идентификатором EF на уровне MF является ‘1C’.

Таблица 32. Файл EF.CardAccess

Имя файла	EF.CardAccess
ID файла	‘011C’
Короткий идентификатор EF	‘1C’
Доступ для выбора	ВСЕГДА
Доступ для считывания	ВСЕГДА
Доступ для записи/обновления/стирания	НИКОГДА
Структура файла	Транспарентная
Размер	Переменный

ФАЙЛ CardAccess, содержащийся в мастер-файле, является ОБЯЗАТЕЛЬНЫМ, если PACE поддерживается чипом электронного МСПД и СОДЕРЖИТ следующую структуру данных SecurityInfos, необходимую для PACE:

- `PACEInfo`;
- `PACEDomainParameterInfo`.

Таблица 33. Хранение файла EF.CardAccess на ИС

Имя файла	EF.CardAccess
ID файла	‘011C’
Короткий идентификатор EF	‘1C’
Доступ для считывания	ВСЕГДА
Доступ для записи	НИКОГДА
Размер	Переменный
Содержание	Структура данных SecurityInfos, закодированная в соответствии с DER. См. часть 11 документа Doc 9303

3.11.4 Файл EF.CardSecurity (УСЛОВНО ОБЯЗАТЕЛЬНЫЙ)

Файл EF.CardSecurity представляет собой транпарентный EF, содержащийся в мастер-файле, и является условно ОБЯЗАТЕЛЬНЫМ, если используется факультативное PACE с отображением для аутентификации чипа (Chip Authentication Mapping), как определено в части 11 документа Doc 9303. Полное описание структуры данных для PACE с отображением для аутентификации чипа приводится в части 11 документа Doc 9303.

Коротким идентификатором EF на уровне MF является ‘1D’.

Файл EF.CardSecurity, содержащийся в MF, является ОБЯЗАТЕЛЬНЫМ, если:

- PACE с отображением для аутентификации чипа поддерживается ИС;
- аутентификация терминала в MF поддерживается ИС; или
- аутентификация чипа в MF поддерживается ИС.

и ДОЛЖЕН содержать:

- ChipAuthenticationInfo, как предусмотрено аутентификацией чипа;
- ChipAuthenticationPublicKeyInfo, как предусмотрено PACE-CAM/аутентификацией чипа;
- TerminalAuthenticationInfo, как предусмотрено аутентификацией терминала;
- SecurityInfos, содержащуюся в файле EF.CardAccess.

Файл EF.CardSecurity, содержащийся в мастер-файле, является ОБЯЗАТЕЛЬНЫМ, если PACE с отображением для аутентификации чипа поддерживается чипом электронного МСПД и СОДЕРЖИТ следующую структуру данных SecurityInfos:

- ChipAuthenticationPublicKeyInfo, как предусмотрено для PACE-CAM;
- SecurityInfos, содержащуюся в файле CardAccess.

Таблица 34. Хранение файла EF.CardSecurity на ИС

Имя файла	EF.CardSecurity
ID файла	‘011D’
Короткий идентификатор EF	‘1D’
Доступ для чтения	PACE
Доступ для записи	НИКОГДА
Размер	Переменный

В соответствии с документом [RFC 3369] файл CardSecurity РЕАЛИЗУЕТСЯ в качестве файла SignedData с содержанием типа id-SecurityObject в поле encapContentInfo. Объекты защиты ПОДПИСЫВАЮТСЯ органами, подписывающими документы. Сертификат органа, подписывающего документы, ДОЛЖЕН включаться в SignedData. Приводимый ниже идентификатор объекта ИСПОЛЬЗУЕТСЯ для идентификации типа контента:

```
bsi-de OBJECT IDENTIFIER ::= {
    itu-t(0) identified-organization(4) etsi(0)
    reserved(127) etsi-identified-organization(0) 7
}
id-SecurityObject OBJECT IDENTIFIER ::= {
    bsi-de applications(3) eID(2) 1
}
```

Структура данных SignedData определяется следующим образом:

```
SignedData ::= SEQUENCE{
    version CMSVersion,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encapContentInfo EncapsulatedContentInfo,
    certificates [0] IMPLICIT CertificateSet OPTIONAL,
    crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
    signerInfos SignerInfos
}

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

EncapsulatedContentInfo ::= SEQUENCE {
    eContentType ContentType,
    eContent [0] EXPLICIT OCTET STRING OPTIONAL
}
```

```
ContentType ::= OBJECT IDENTIFIER

SignerInfos ::= SET OF SignerInfo

SignerInfo ::= SEQUENCE {
    version CMSVersion,
    sid SignerIdentifier,
    digestAlgorithm DigestAlgorithmIdentifier,
    signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
    signatureAlgoritm SignatureAlgorithmIdentifier,
    signature SignatureValue,
    unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL
}

SignerIdentifier ::= CHOICE {
    issuerAndSerialNumber IssuerAndSerialNumber,
    subjectKeyIdentifier [0] SubjectKeyIdentifier
}

SignatureValue ::= OCTET STRING
```

4. ПРИЛОЖЕНИЕ LDS1 ЭЛЕКТРОННОГО МСПД (ОБЯЗАТЕЛЬНОЕ)

Структура LDS1 электронного МСПД предоставляет емкость для хранения и цифровой подписи обязательных и факультативных элементов данных, которые могут использоваться для привязки обладателя к документу. Информация, хранимая в блоке приложения LDS1 электронного МСПД, в момент выдачи становится статической и никакими возможными средствами ее изменить нельзя. Этот элемент необходим для обеспечения защиты личной информации и упрощения обнаружения подделки документов. Несмотря на то, что версия LDS1 электронного МСПД предусматривает наличие факультативных полей данных, которые могут быть использованы для расширения применения электронных МСПД (т. е., дополнительные биометрические характеристики, автоматизированный пограничный контроль и т. д.), требование об обеспечении защиты приложения LDS1 электронного МСПД от внесения информации в момент выдачи является ОБЯЗАТЕЛЬНЫМ.

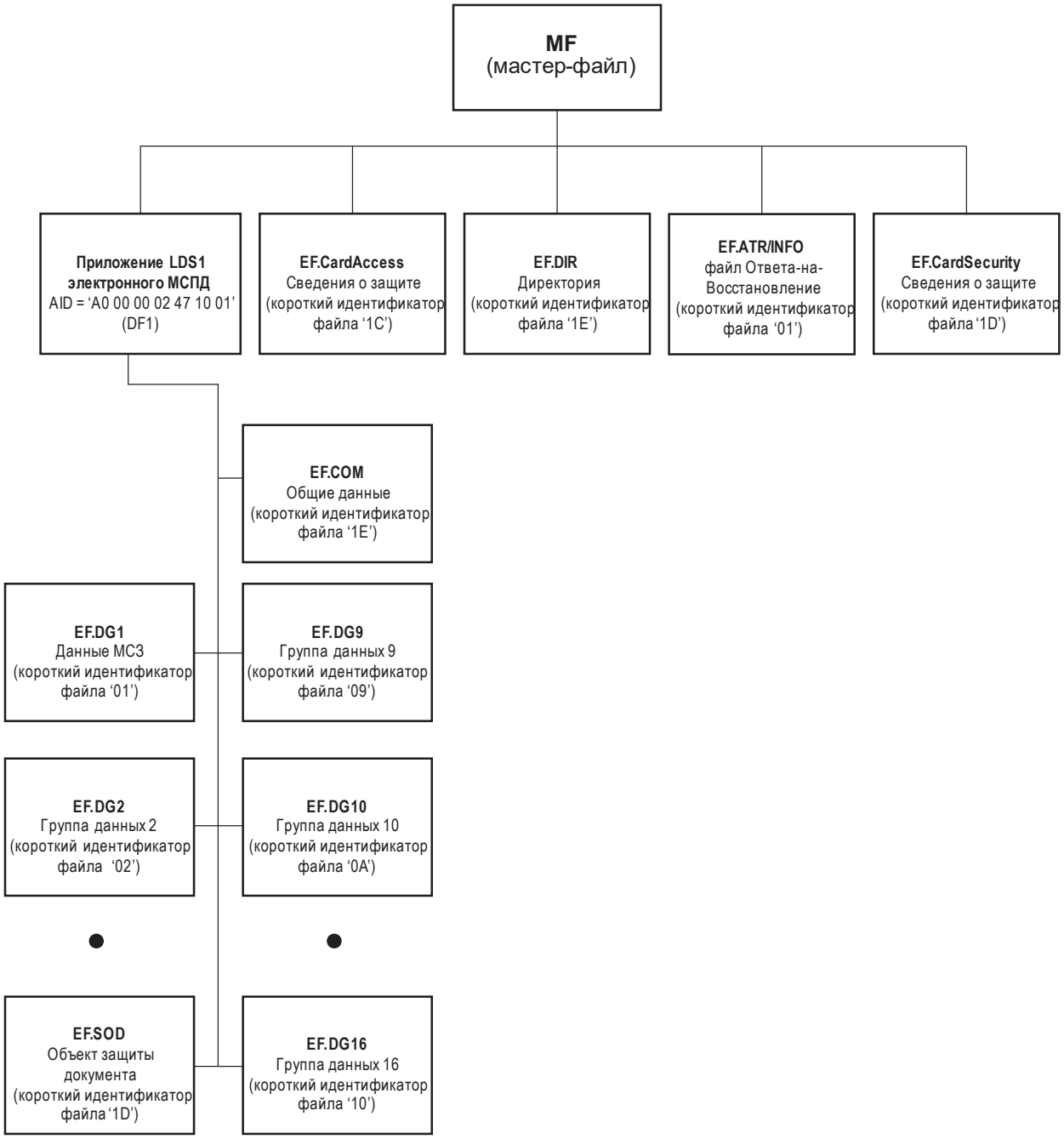

Рис. 3. Обобщенная структура файла приложения LDS1 электронного МСПД

4.1 Выбор приложения: DF

Приложение LDS1 электронного МСПД ВЫБИРАЕТСЯ посредством идентификации приложения (AID) в качестве зарезервированного названия DF. AID СОСТОИТ из зарегистрированного идентификатора приложения, установленного ИСО в соответствии со стандартом [ИСО/МЭК 7816-5], и проприетарного расширения идентификатора приложения (PIX), как определено в настоящем документе:

- зарегистрированный идентификатор приложения равен ’A000000247’;
- в приложении хранящихся данных выдающего органа ИСПОЛЬЗУЕТСЯ PIX = ’1001’;
- полный идентификатор AID приложения LDS1 электронного МСПД равен ‘A0 00 00 02 47 10 01’.

ИС ДОЛЖНА отклонять выбор приложения, если расширение для данного приложения отсутствует.

4.2 Схема произвольного упорядочения

Схема произвольного упорядочения позволяет регистрировать группы и элементы данных по принципу произвольного упорядочения, что соответствует способности технологии факультативного расширения возможностей обеспечивать прямое извлечение конкретных элементов данных даже в случае их неупорядоченной регистрации. Переменная длина элементов данных кодируется в качестве объектов данных TLV, указанных в ASN.1.

4.3 Представление файла с произвольным доступом

Представление файла с произвольным доступом определено с учетом следующих соображений и допущений.

Для поддержки широкого разнообразия реализаций LDS содержит большой диапазон факультативных элементов данных. Эти элементы данных включены с целью оказать содействие аутентификации электронных МСПД с LDS1, аутентификации законных обладателей и ускорения обработки документов/лиц на контрольно-пропускных пунктах.

Структура данных должна поддерживать:

- ограниченный или расширенный набор элементов данных;
- наличие многочисленных специфичных элементов данных;
- постоянную эволюцию конкретных реализаций;
- по крайней мере один комплект прикладных данных;
- использование других национальных специфичных приложений;
- факультативную активную аутентификацию документов с использованием хранимой ассиметричной пары ключей;
- обеспечение быстрого доступа выбранных элементов данных в целях упрощения оперативной обработки документов;
- немедленный доступ к необходимым элементам данных;
- прямой доступ к шаблонам данных и биометрическим характеристикам.

4.4 Группирование элементов данных

В LDS могут присутствовать или не присутствовать группы элементов данных, добавляемых государствами выдачи или утвержденными принимающими организациями. В LDS может содержаться несколько записей сгруппированных элементов данных, добавляемых принимающими государствами или утвержденными принимающими организациями.

В данном издании документа Doc 9303 возможность добавления данных к LDS принимающим государством или утвержденной принимающей организацией не обеспечивается.

LDS считается единой целостной структурой, содержащей ряд групп элементов данных, записанных на факультативном устройстве увеличения емкости на момент машинного считывания.

LDS спроектирована с достаточной степенью гибкости для применения ее ко всем видам электронных МСПД. Некоторые элементы данных, указанные в последующих таблицах и на рисунках, применимы только к машиносчитываемым визам и машиносчитываемым паспортам или требуют иной формы представления в отношении этих документов.

В рамках LDS установлены логические группы взаимосвязанных элементов данных. Эти логические группы именуются группами данных.

4.5 Требования логической структуры данных

Выбранная государством или организацией выдачи технология увеличения емкости памяти на бесконтактной ИС, применяемая в электронных МСПД, должна обеспечивать принимающим государствам доступ к соответствующим данным.

ИКАО установила, что предопределенная стандартная логическая структура данных (LDS) ОТВЕЧАЕТ ряду обязательных требований:

- обеспечивать эффективное и оптимальное упрощение формальностей по отношению к законному владельцу;
- обеспечивать защиту данных, хранящихся на факультативном устройстве увеличения емкости;
- обеспечивать глобальный обмен увеличенными объемами данных на основе использования единой LDS, общей для всех электронных МСПД;
- учитывать различные потребности государств и организаций выдачи в факультативном увеличении емкости;
- обеспечивать увеличение емкости по мере роста потребностей пользователей и развития технологии;
- поддерживать разнообразные варианты защиты данных;
- максимально использовать существующие международные спецификации, в частности новые международные спецификации для глобально совместимых биометрических данных.

4.5.1 Защита

Только государство или организация выдачи ИМЕЮТ доступ к этим группам данных с правом записи. Таким образом, требования в отношении обмена данными не устанавливаются и методы, используемые для обеспечения защиты от записи, не являются частью этой спецификации. Как только чип будет заблокирован (после персонализации и до выдачи), никакие данные приложения LDS1 не могут быть записаны на чип, модифицированы в нем или исключены из него. После выдачи заблокированный чип разблокировать нельзя.

4.5.2 Аутентичность и целостность данных

Для подтверждения аутентичности и целостности записанных данных предусматривается объект аутентичности/целостности. В этом объекте аутентичности/целостности ДОЛЖНА быть представлена каждая группа данных, которая записывается в отдельном элементарном файле ($EF.SO_D$). Путем использования единой структуры форматов обмена биометрической информацией (CBEFF), применяемой для групп данных 2–4 (закодированные идентификационные характеристики) и факультативных "дополнительных элементов биометрической защиты", определяемых в части 12 документа Doc 9303, по усмотрению государства или организации выдачи в индивидуальном порядке МОГУТ также защищаться данные, подтверждающие личность (например, биометрические шаблоны).

4.5.3 Упорядочение LDS

Для обеспечения международной интероперабельности ИСПОЛЬЗУЕТСЯ только схема произвольного упорядочения.

4.5.4 Емкость памяти бесконтактной ИС для хранения данных

Емкость памяти ИС определяется по усмотрению государства выдачи, но СОСТАВЛЯЕТ как минимум 32 килобайт. Эта минимальная емкость необходима для обязательного хранения данных изображения лица (обычно 15–20 килобайт) в МСЗ и необходимых элементов защиты данных. Хранение дополнительных изображений лица, отпечатков пальцев и/или радужной оболочки глаза может потребовать значительного увеличения емкости памяти для хранения данных. Максимальная емкость данных ИС не определяется.

В случае отсутствия в государстве инфраструктуры PKI, необходимой для подписания данных электронного МСПД в рамках персонализации, и невозможности задержки выдачи документа(ов), чип электронного МСПД РЕКОМЕНДУЕТСЯ оставлять пустым и блокировать. В приложении LDS1 электронного МСПД СЛЕДУЕТ напечатать соответствующее подтверждение на этот счет. Предполагается, что это будет исключительным обстоятельством.

4.5.5 Хранение других данных

Любое государство МОЖЕТ использовать емкость памяти бесконтактной ИС электронного МСПД для увеличения объема его машиносчитываемых данных сверх того, который установлен для глобального обмена данными. Это может делаться в таких целях, как предоставление машиносчитываемого доступа к информации исходных документов (например, свидетельства о рождении) и хранящимся данным, используемым для подтверждения личности (биометрические характеристики) и/или верификации подлинности документа.

4.5.6 Международный стандарт кодирования биометрических характеристик

Стандарт ИСО/МЭК 39794 заменит стандарт [ИСО/МЭК 19794:2005] в качестве международного стандарта кодирования биометрических характеристик. Ниже приводится информация об установленном графике перехода:

- оборудование для считывания паспортов ДОЛЖНО быть способно обрабатывать данные, предусмотренные стандартом ИСО/МЭК 39794, к 1 января 2025 года по истечении пятилетнего подготовительно периода, начавшегося 1 января 2020 года;

- в период между 2025 и 2030 годами органы, выдающие паспорта, могут использовать форматы данных, предусмотренные стандартом ИСО/МЭК 19794-X:2005 или стандартом ИСО/МЭК 39794-X в течение пятилетнего переходного периода. В течение этого переходного периода важным элементом будет проверка интероперабельности и соответствия;

- начиная с 1 января 2030 года для кодирования биометрических характеристик органы, выдающие паспорта, ДОЛЖНЫ использовать стандарт ИСО/МЭК 39794-X.

В стандарте ИСО/МЭК 49794 содержатся инструктивные указания относительно перехода от стандарта [ИСО/МЭК 19794:2005] к стандарту ИСО/МЭК 39794.

4.6 Элементарные файлы (EF) приложения LDS1 электронного МСПД

4.6.1 Информация о заголовке и присутствии групп данных EF.COM (ОБЯЗАТЕЛЬНАЯ)

Файл EF.COM размещается в приложении LDS1 электронного МСПД (короткий идентификатор файла = '1E') и содержит информацию о версии LDS, информацию о версии Unicode и перечень групп данных, присутствующих в приложении. Приложение LDS1 электронного МСПД ДОЛЖНО иметь только один файл EF.COM, содержащий общую информацию, касающуюся данного приложения.

Элементы данных, которые могут фигурировать в этом шаблоне, включают следующее:

Таблица 35. Нормативные теги EF.COM

Тег	**Длина**	**Значение**		
‘60’	Var	Информация об уровне приложения		
		Тег	**Длина**	**Значение**
		‘5F01’	‘04’	Номер версии LDS формата aabb, где aa обозначает версию LDS, а bb обозначает уровень обновления
		‘5F36’	‘06’	Номер версии Unicode формата aabbcc, где aa обозначает основную версию, bb – вспомогательную версию и cc – уровень версии программного продукта
		‘5C’	Var	Список тегов. Список всех присутствующих групп данных

ВКЛЮЧАЮТСЯ заголовок и карта отображения присутствия групп данных. Заголовок содержит нижеуказанную информацию, позволяющую принимающему государству или утвержденной принимающей организации обнаруживать и декодировать различные группы данных и элементы данных, содержащиеся в блоке данных, записанном государством или организацией выдачи.

РЕКОМЕНДУЕТСЯ как можно скорее модифицировать системы проверки, основанные на EF.COM, в целях использования SO_D, описание которого приводится в LDS версии 1.8.

4.6.1.1 Номер версии LDS

Номер версии LDS определяет версию формата LDS. Точный формат, подлежащий использованию для хранения этого значения, определен в разделе 4.6 настоящего документа. Стандартным форматом номера версии LDS является "aabb", где:

- "aa" – число (01–99), идентифицирующее основную версию LDS (т. е. существенные добавления к LDS);
- "bb" – число (01–99), идентифицирующее дополнительную версию LDS.

4.6.1.2 Номер версии UNICODE

Номер версии Unicode определяет применяемый метод кодирования при записи буквенно-цифровых и специальных символов, включая национальные символы. Точный формат, подлежащий использованию для хранения этого значения, определяется в разделе 4.7.1 настоящего документа. Стандартным форматом номера версии Unicode является "aabbcc", где:

- "aa" – число, идентифицирующее основную версию стандарта Unicode (т. е. значительные добавления к стандарту, опубликованные в виде справочника);
- "bb" – число, идентифицирующее вспомогательную версию стандарта Unicode (т. е. добавления к символам или более существенные нормативные изменения, опубликованные в виде технического доклада);
- "cc" – номер, идентифицирующий новую версию стандарта Unicode (т. е. любые другие изменения нормативных или важных информативных частей данного стандарта, которые могут изменить режим работы программы. Эти изменения отражаются в новых файлах символьной базы данных Unicode и на странице обновлений). Исторически сложилось так, что нумерация внутри каждого поля (т. е. a, b, c) не обязательно является последовательной.

Универсальный набор знаков (UCS) ДОЛЖЕН соответствовать стандарту [ИСО/МЭК 10646].

4.6.2 Объект защиты документа EF.SOD (ОБЯЗАТЕЛЬНЫЙ)

Помимо групп данных LDS бесконтактная ИС также содержит объект защиты документа (EF.SOD). Этот объект подписывается в цифровой форме государством выдачи и содержит хэшированные данные о содержании LDS.

Таблица 36. Теги EF.SOD

Тег	L	Значение
'77'	Var	Объект защиты документа

В настоящее время имеются две развернутые версии объекта защиты документа EF.SOD. Имеется устаревшая версия EF.SOD V0, информация о которой содержится в добавлении D, и РЕКОМЕНДУЕМАЯ версия EF.SOD V1, приводимая в настоящем разделе. ТРЕБУЕТСЯ и разрешается применять только один EF.SOD.

4.6.2.1 Объект защиты документа EF.SOD версии V1 для LDS версии 1.8

Объект защиты документа версии V1 для LDS версии v1.8 не расширен подписанным атрибутом, содержащим информацию о версии LDS и Unicode:

```
LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
DataGroupHash,
   ldsVersionInfo LDSVersionInfo OPTIONAL
   -- If present, version MUST be V1
}
LDSVersionInfo ::= SEQUENCE {
   ldsVersion PrintableString,
   unicodeVersion PrintableString }
```

4.6.2.2 Тип подписываемых данных для SO_D версии V1

Объект защиты документа реализуется как тип подписываемых данных, указанный в [RFC 3369]. Все объекты защиты ДОЛЖНЫ производиться в формате, определяемом особыми правилами кодирования (DER), для сохранения целостности содержащихся в них подписей.

Примечание 1. m ОБЯЗАТЕЛЬНОЕ – поле ДОЛЖНО присутствовать.

Примечание 2. x не использовать – поле НЕ ДОЛЖНО заполняться.

Примечание 3. o факультативное – поле МОЖЕТ присутствовать.

Примечание 4. c выбор – содержание поля выбирается из альтернатив.

Таблица 37. Тип подписываемых данных для SO_D версии V0

Значение		Замечания
Подписываемые данные		
Версия	m	Значение = v3
Алгоритмы представления в краткой форме	m	
Информация об инкапсулированном содержании	m	
Тип электронного содержания	m	id-icao – mrtd – security – ldsSecurityObject

Значение		Замечания
Электронное содержание	m	Закодированное содержание ldsSecurityObject
Сертификаты	o	Государства ДОЛЖНЫ включать сертификат органа, подписывающего документы (C_{DS}), который может использоваться для верификации подписи в поле информации о подписавшемся
Crl	x	Государствам рекомендуется не использовать это поле
Информация о подписавшемся	m	Государствам рекомендуется предоставлять в этом поле только одну единицу информации
Информация о подписавшемся	m	
Версия	m	Значение этого поля диктуется полем sid. См. правила, касающиеся этого поля, в RFC 3369, часть 12 документа Doc 9303
Sid	m	
Выдающий орган и серийный номер	c	Государствам рекомендуется поддерживать это поле над идентификатором ключа субъекта
Идентификатор ключа субъекта	c	
Алгоритм представления в краткой форме	m	Алгоритмный идентификатор алгоритма, используемого для выдачи хэш-значения над инкапсулированным содержанием и подписанными атрибутами
Подписанные атрибуты	m	Производящие государства могут пожелать включать дополнительные атрибуты для внесения в подпись, однако они должны обрабатываться принимающими государствами только для верификации значения подписи
Алгоритм подписи	m	Алгоритмный идентификатор алгоритма, используемого для выдачи значения подписи и любых связанных с ней параметров
Подпись	m	Результат процесса генерации подписи
Неподписанные атрибуты	o	Производящие государства могут пожелать использовать это поле, однако это не рекомендуется, и принимающие государства могут игнорировать их

4.6.2.3 Объект защиты документа LDS профиля ASN.1 для SO_D версии V1

```
LDSSecurityObjectV1 { joint-iso-itu-t(2) international(23) icao(136)
mrtd(1) security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
```

```
-- Imports from RFC 3280 [PROFILE]
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) };

-- Constants

ub-DataGroups INTEGER ::= 16

-- Object Identifiers

id-icao OBJECT IDENTIFIER::={joint-iso-itu-t(2) international(23)
icao(136) }
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-mrtd-security-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 1}

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {v0(0), v1(1)
-- If LDSSecurityObjectVersion is V1, ldsVersionInfo MUST be present }

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
   DataGroupHash
   ldsVersionInfo LDSVersionInfo OPTIONAL
   -- If present, version MUST be V1 }

DataGroupHash ::= SEQUENCE {
   dataGroupNumber DataGroupNumber,
   dataGroupHashValue OCTET STRING }

DataGroupNumber ::= INTEGER {
   dataGroup1            (1),
   dataGroup2            (2),
   dataGroup3            (3),
   dataGroup4            (4),
   dataGroup5            (5),
   dataGroup6            (6),
   dataGroup7            (7),
   dataGroup8            (8),
   dataGroup9            (9),
   dataGroup10          (10),
   dataGroup11          (11),
   dataGroup12          (12),
   dataGroup13          (13),
   dataGroup14          (14),
```

```
      dataGroup15          (15),
      dataGroup16          (16)}

   LDSVersionInfo ::= SEQUENCE {
      ldsVersion PrintableString
      unicodeVersion Printable String }
   END
```

Примечание 1. Поле `dataGroupHashValue` содержит вычисленное хэш-значение над полным содержанием файла группы данных EF, определяемого полем `dataGroupNumber`.

Примечание 2. В поле `DigestAlgorithmIdentifiers` НЕОБХОДИМО опустить параметры `NULL`, в то время как поле `SignatureAlgorithmIdentifier` (как указано в RFC 3447) ДОЛЖНО включать `NULL` в качестве этого параметра в случае отсутствия параметров, даже если используются алгоритмы SHA2 в соответствии с RFC 5754. Система проверки ДОЛЖНА принимать к обработке поле `DigestAlgorithmIdentifiers` в обоих случаях, т. е. при отсутствии параметров и с параметрами `NULL`.

4.7 Элементы данных, образующие группы данных 1–16

Каждая из групп данных 1 (DG1) – 16 (DG16) состоит из ряда обязательных, факультативных и условно обязательных элементов данных. В рамках группы данных СОБЛЮДАЕТСЯ установленный порядок следования элементов данных. Каждая группа данных ХРАНИТСЯ в одном транспарентном файле EF. Обращение к файлам EF осуществляется с помощью короткого идентификатора EF, как указано в таблице 38. EF имеют названия для этих файлов, которые ПРОНУМЕРОВАНЫ в соответствии с "n" (EF.DGn), где "n" является номером группы данных.

Таблица 38. Обязательные и факультативные элементы данных, образующие в совокупности структуру групп данных 1 (DG1) – 16 (DG16)

Группа данных	Название EF	Короткий идентификатор файла	Идентификатор EF	Тег
Общая	EF.COM	‘1E’	‘01 1E’	‘60’
DG1	EF.DG1	‘01’	‘01 01’	‘61’
DG2	EF.DG2	‘02’	‘01 02’	‘75’
DG3	EF.DG3	‘03’	‘01 03’	‘63’
DG4	EF.DG4	‘04’	‘01 04’	‘76’
DG5	EF.DG5	‘05’	‘01 05’	‘65’
DG6	EF.DG6	‘06’	‘01 06’	‘66’
DG7	EF.DG7	‘07’	‘01 07’	‘67’
DG8	EF.DG8	‘08’	‘01 08’	‘68’
DG9	EF.DG9	‘09’	‘01 09’	‘69’

Группа данных	Название EF	Короткий идентификатор файла	Идентификатор EF	Тег
DG10	EF.DG10	‘0A’	‘01 0A’	‘6A’
DG11	EF.DG11	‘0B’	‘01 0B’	‘6B’
DG12	EF.DG12	‘0C’	‘01 0C’	‘6C’
DG13	EF.DG13	‘0D’	‘01 0D’	‘6D’
DG14	EF.DG14	‘0E’	‘01 0E’	‘6E’
DG15	EF.DG15	‘0F’	‘01 0F’	‘6F’
DG16	EF.DG16	‘10’	‘01 10’	‘70’
Объект защиты документа	$EF.SO_D$	‘1D’	‘01 1D’	‘77’
Общая	EF.CARDACCESS	‘1C’	‘01 1C’	
Общая	EF.ATR/INFO	‘01’	‘2F 01’	
Общая	EF.CardSecurity	‘1D’	‘01 1D’	

4.7.1 ГРУППА ДАННЫХ 1. Информация машиносчитываемой зоны (ОБЯЗАТЕЛЬНАЯ)

Элементы данных группы данных 1 (DG1) предназначены для отражения всего содержания МСЗ независимо от того, содержатся ли в ней фактические данные или знаки-заполнители. Детализация применения МСЗ зависит от типа электронного МСПД с LDS1 (форматы ПД1, ПД2 или ПД3).

Настоящий элемент данных содержит в шаблоне '61' ОБЯЗАТЕЛЬНУЮ для этого документа информацию машиносчитываемой зоны (МСЗ). Указанный шаблон содержит один объект данных – МСЗ в объекте данных '5F1F'. Объект данных МСЗ представляет собой составной элемент данных, аналогичный информации OCR-B МСЗ, напечатанной на этом документе.

Таблица 39. Теги группы данных 1

Тег	L	Значение		
'61'	Var			
		Тег	**L**	**Значение**
		'5F1F'	Var	Объект данных МСЗ в виде составного элемента данных (ОБЯЗАТЕЛЬНЫЙ). (Этот элемент данных содержит все обязательные поля от "типа документа" до "составной контрольной цифры")

4.7.1.1 ГРУППА ДАННЫХ 1. Элементы данных EF.DG1 для электронного МСПД с LDS1 размера ПД1

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 1 (DG1). Предполагается, что требования к хранению, упорядочению и кодированию будут точно соответствовать требованиям, предъявляемым к печатной МСЗ и описанным в частях 3 и 5 документа Doc 9303. Элементы данных и их формат в каждой группе для ПД1 УКАЗАНЫ в нижеследующей таблице.

Примечание. A – буквенный символ [A..Z], N – цифровой символ [0..9], S – специальный символ['<'], F – поле фиксированной длины.

Таблица 40. Элементы данных для формата ПД1

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования
01	M	Код документа	2	F	A,S
02	M	Государство или организация выдачи	3	F	A,S
03	M	Номер документа (9 наиболее значимых знаков)	9	F	A,N,S
04	M	Контрольная цифра: номер документа или знак-заполнитель (<), указывающий, что длина номера документа превышает 9 знаков	1	F	N,S
05	M	Факультативные данные и/или, если номер документа превышает 9 знаков, наименее значимые знаки номера документа плюс контрольная цифра номера документа плюс знак-заполнитель	15	F	A,N,S
06	M	Дата рождения	6	F	N,S
07	M	Контрольная цифра: дата рождения	1	F	N
08	M	Пол	1	F	A,S
09	M	Дата истечения срока действия	6	F	N

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования
10	M	Контрольная цифра: дата истечения срока действия	1	F	N
11	M	Гражданство	3	F	A,S
12	M	Факультативные данные	11	F	A,N,S
13	M	Составная контрольная цифра	1	F	N
14	M	Имя владельца	30	F	A,N,S

4.7.1.2 ГРУППА ДАННЫХ 1. Элементы данных EF.DG1 для электронного МСПД размера ПД2

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 1 (DG1). Предполагается, что требования к хранению, упорядочению и кодированию будут точно соответствовать требованиям, предъявляемым к печатной МСЗ и описанным в частях 3 и 6 документа Doc 9303. Элементы данных и их формат в каждой группе для ПД2 УКАЗАНЫ в следующей таблице.

Примечание. A – буквенный символ [A..Z], N – цифровой символ[0..9], S – специальный символ['<'], F – поле фиксированной длины.

Таблица 41. Элементы данных для формата ПД2

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования
01	M	Код документа	2	F	A,S
02	M	Государство или организация выдачи	3	F	A,S
03	M	Имя владельца	31	F	A,N,S
04	M	Номер документа (9 основных знаков)	9	F	A,N,S
05	M	Контрольная цифра	1	F	N,S
06	M	Гражданство	3	F	A,S
07	M	Дата рождения	6	F	N,S
08	M	Контрольная цифра	1	F	N

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования
09	M	Пол	1	F	A,S
10	M	Дата истечения срока действия	6	F	N
11	M	Контрольная цифра	1	F	N
12	M	Факультативные данные плюс знак-заполнитель	7	F	A,N,S
13	M	Составная контрольная цифра: строка 2 МСЗ	1	F	N

4.7.1.3 ГРУППА ДАННЫХ 1. Элементы данных EF.DG1 для электронного МСПД с LDS1 размера ПД3

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 1 (DG1). Предполагается, что требования к хранению, упорядочению и кодированию будут точно соответствовать требованиям, предъявляемым к печатной МСЗ и описанным в частях 3 и 4 документа Doc 9303. Элементы данных и их формат в каждой группе для ПД3 УКАЗАНЫ в следующей таблице.

Примечание. A – буквенный символ [A..Z], N – цифровой символ [0-9], S – специальный символ ['<'], F – поле фиксированной длины.

Таблица 42. Элементы данных для формата ПД3

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования
01	M	Код документа	2	F	A,S
02	M	Государство или организация выдачи	3	F	A,S
03	M	Имя владельца	39	F	A,S
04	M	Номер документа	9	F	A,N,S
05	M	Контрольная цифра: номер документа	1	F	N,S
06	M	Гражданство	3	F	A,S
07	M	Дата рождения	6	F	N,S
08	M	Контрольная цифра: дата рождения	1	F	N

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования
09	M	Пол	1	F	A,S
10	M	Дата истечения срока действия	6	F	N
11	M	Контрольная цифра: дата истечения срока действия или дата "действителен до"	1	F	N
12	M	Факультативные данные	14	F	A,N,S
13	M	Контрольная цифра	1	F	N
14	M	Составная контрольная цифра	1	F	N

4.7.2 ГРУППА ДАННЫХ 2. Закодированные идентификационные характеристики: лицо (ОБЯЗАТЕЛЬНАЯ)

Группа данных 2 (DG2) составляет глобально интероперабельный биометрический параметр, используемый для машинного подтверждения личности с помощью машиносчитываемых проездных документов, каковым ЯВЛЯЕТСЯ изображение лица владельца, вводимое в систему распознавания черт лица. При наличии более одной записи первой является самая свежая закодированная глобально интероперабельная запись.

Таблица 43. Теги группы данных 2

Тег	L	Значение
'75'	Var	См. "Кодировка биометрических данных EF.DG2"

4.7.2.1 Кодировка биометрических данных EF.DG2

В группе DG2 ДОЛЖЕН использоваться шаблон группы вложенных шаблонов биометрической информации (BIT), отвечающих требованиям стандарта [ИСО/МЭК 7816-11], что обеспечивает возможность хранения нескольких биометрических образцов, соответствующих единому формату файлов обмена биометрическими данными (CBEFF). Биометрический подзаголовок определяет тип присутствующей биометрической информации и конкретную биометрическую характеристику. Вариант стандарта [ИСО/МЭК 7816-11], предусматривающий вложение, должен использоваться всегда и даже при кодировании одного биометрического шаблона. Последний случай указывается числовым кодированием, и при котором n=1.

Каждый вложенный шаблон имеет нижеследующую структуру.

Таблица 44. Группа данных 2. Теги кодировок биометрических характеристик

Тег	**L**	**Значение**				
'7F61'	Var	Шаблон группы биометрической информации				
		Тег	**L**	**Значение**		
		'02'	'01/	Целое число – количество образцов этого типа биометрического параметра		
		'7F60'	Var	Первый шаблон биометрической информации		
			Тег	**L**		
			‘A1’	Var	Шаблон заголовка биометрической информации (BHT)	
				Тег	**L**	**Значение**
				‘80’	‘02’	Версия 0101 заголовка ИКАО (факультативная информация) – версия основного формата заголовка CBEFF
				‘81’	‘01-03’	Биометрический тип (факультативная информация)
				‘82’	‘01’	Биометрический подтип (факультативная информация для DG2)
				‘83’	‘07’	Дата и время создания (факультативная информация)
				‘85’	‘08’	Срок действия (с … по) (факультативная информация)
				‘86’	‘04’	Создатель контрольных биометрических данных (PID) (факультативная информация)
				‘87’	‘02’	Владелец формата (ОБЯЗАТЕЛЬНАЯ ИНФОРМАЦИЯ)
				‘88’	‘02’	Тип формата (ОБЯЗАТЕЛЬНАЯ ИНФОРМАЦИЯ)
			‘5F2E’ или ‘7F2E’	Var	Биометрические данные (закодированные по правилам владельца формата), именуемые также блоком биометрических данных (BDB)	

Для указания CBEFF используется установленный по умолчанию идентификатор OID. Объект данных OID (тег '06'), находящийся непосредственно под шаблоном биометрической информации (BIT, тег '7F60') и указанный в стандарте [ИСО/МЭК 7816-11], в эту структуру не включается. Аналогичным образом в структуре не определяются полномочия на распределение тегов.

В целях обеспечения интероперабельности первая биометрическая информация, записываемая в каждой группе данных, КОДИРУЕТСЯ в соответствии со стандартом [ИСО/МЭК 19794-5].

Примечание. Стандарт ИСО/МЭК 39794 заменит стандарт ИСО/МЭК 19794:2005 в качестве международного стандарта кодирования биометрических характеристик. См. раздел 4.5.6.

4.7.2.2 ГРУППА ДАННЫХ 2. Элементы данных EF.DG2

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 2 (DG2). Элементы данных и их формат в каждой зоне группы данных УКАЗАНЫ в нижеследующих таблицах.

Примечание. A – буквенный символ [a-.z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Таблица 45. Элементы данных для DG2

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
01	M	Количество записанных кодировок биометрических характеристик лица	1	F	N	Цифры 1–9, указывающие количество уникальных кодировок данных о характеристиках лица
02	M	Заголовок		Var	A,N	Элемент данных может повторяться, как определено элементом данных DE 01
03	M	Кодировка(и) биометрических характеристик лица		Var	B	Элемент данных может повторяться, как определено элементом данных DE 01

4.7.3 ГРУППА ДАННЫХ 3. Дополнительные идентификационные характеристики: палец (пальцы) (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

ИКАО признает, что в поддержку машинного подтверждения личности государства-члены могут использовать в качестве дополнительных биометрических технологий технику распознавания отпечатков пальцев, изображения которых КОДИРУЮТСЯ в рамках группы данных 3 (DG3).

Таблица 46. Теги группы данных 3

Тег	L	Значение
'63'	Var	См. "Кодировка биометрических данных EF.DG3"

4.7.3.1 Кодировка биометрических данных EF.DG3

В группе DG3 ДОЛЖЕН использоваться шаблон группы вложенных шаблонов биометрической информации (BIT), отвечающих требованиям стандарта [ИСО/МЭК 7816-11], что обеспечивает возможность хранения нескольких биометрических образцов, соответствующих единому формату файлов обмена биометрическими данными (CBEFF). Биометрический подзаголовок определяет тип присутствующей биометрической информации и конкретную биометрическую характеристику. Даже для кодировок одного биометрического шаблона ДОЛЖЕН использоваться вариант стандарта [ИСО/МЭК 7816-11]. Последний случай указывается числовым кодированием, при котором n=1. Количество образцов в DG3 может быть ‘0...n’.

Каждый вложенный шаблон имеет нижеследующую структуру.

Таблица 47. Вложенные теги группы данных 3

Тег	**L**	**Значение**				
'7F61'	Var	Шаблон группы биометрической информации				
		Тег	**L**	**Значение**		
		'02'	'01'	Целое число – количество образцов этого типа биометрического параметра		
		'7F60'	Var	Первый шаблон биометрической информации		
			Тег	**L**		
			'A1'	Var	Шаблон заголовка биометрической информации (BHT)	
				Тег	**L**	**Значение**
				‘80’	‘02’	Версия '0101' заголовка ИКАО (факультативная информация) – версия основного формата заголовка CBEFF
				‘81’	‘01-03’	Биометрический тип (факультативная информация)
				‘82’	‘01’	Биометрический подтип (ОБЯЗАТЕЛЬНАЯ информация для DG3)
				‘83’	‘07’	Дата и время создания (факультативная информация)
				‘85’	‘08’	Срок действия (с … по) (факультативная информация)
				‘86’	‘04’	Создатель контрольных биометрических данных (PID) (факультативная информация)
				‘87’	‘02’	Владелец формата (ОБЯЗАТЕЛЬНАЯ информация)
				‘88’	‘02’	Тип формата (ОБЯЗАТЕЛЬНАЯ информация)

Тег	L	Значение				
			'5F2E' или '7F2E'	Var	Биометрические данные (закодированные по правилам владельца формата), именуемые также блоком биометрических данных (BDB)	
		Тег	**L**			
		'7F60'	Var	Второй шаблон биометрической информации		
			Тег	**L**		
			'A1'	Var	Шаблон заголовка биометрической информации (BHT)	
				Тег	**L**	**Значение**
				‘80’	‘02’	Версия '0101' заголовка ИКАО (факультативная информация) – версия основного формата заголовка CBEFF
				‘81’	‘01-03’	Биометрический тип (факультативная информация)
				‘82’	‘01’	Биометрический подтип (ОБЯЗАТЕЛЬНАЯ информация для DG3)
				‘83’	‘07’	Дата и время создания (факультативная информация)
				‘85’	‘08’	Срок действия (с … по) (факультативная информация)
				‘86’	‘04’	Создатель контрольных биометрических данных (PID) (факультативная информация)
				‘87’	‘02’	Владелец формата (ОБЯЗАТЕЛЬНАЯ информация)
				‘88’	‘02’	Тип формата (ОБЯЗАТЕЛЬНАЯ информация)
			'5F2E' или '7F2E'	Var	Биометрические данные (закодированные по правилам владельца формата), именуемые также блоком биометрических данных (BDB)	

Для указания CBEFF используется установленный по умолчанию идентификатор OID. Объект данных OID (тег '06'), находящийся непосредственно под шаблоном биометрической информации (BIT, тег '7F60') и указанный в стандарте [ИСО/МЭК 7816-11], в эту структуру не включается. Аналогичным образом в структуре не определяются полномочия на распределение тегов.

В целях обеспечения интероперабельности первая биометрическая информация, записываемая в каждой группе данных, КОДИРУЕТСЯ в соответствии со стандартом [ИСО/МЭК 19794-4].

Примечание. Стандарт ИСО/МЭК 39794 заменит стандарт ИСО/МЭК 19794:2005 в качестве международного стандарта кодирования биометрических данных. См. раздел 4.5.6.

4.7.3.2 ГРУППА ДАННЫХ 3. Элементы данных EF.DG3

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 3 (DG3). Элементы данных и их формат в каждой зоне группы данных УКАЗАНЫ в нижеследующей таблице.

Примечание. A – буквенный символ [a-z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Таблица 48. Элементы данных для DG3

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
01	M (Если закодированная характеристика пальца(ев) включена)	Количество записанных кодировок биометрических характеристик пальца(ев)	1	F	N	Цифры 0–n, указывающие количество уникальных кодировок данных о пальце(ах)
02	M (Если закодированная характеристика пальца(ев) включена)	Заголовок		Var	B	Элемент данных может повторяться, как определено элементом данных 01
03	M (Если закодированная характеристика пальца(ев) включена)	Кодировка(и) биометрических данных о пальце(ах)		Var	B	Элемент данных может повторяться, как определено элементом данных 01

4.7.3.2.1 Кодирование биометрического подтипа

Теги шаблона заголовка биометрических данных и установленные для них значения являются минимальной информацией, которую поддерживает каждый вариант реализации, как это показано в нижеследующей таблице. Каждый отдельный шаблон биометрической информации имеет следующую структуру.

Таблица 49. Схема кодирования подхарактеристик: CBEFF

b8	b7	b6	b5	b4	b3	b2	b1	Биометрический подтип
0	0	0	0	0	0	0	0	Информация не дается
						0	1	Правый
						1	0	Левый
			0	0	0			Не имеет значения
			0	0	1			Большой палец
			0	1	0			Указательный
			0	1	1			Средний
			1	0	0			Безымянный
			1	0	1			Мизинец
X	X	X						Зарезервировано для будущего использования

4.7.3.2.2 Кодирование при отсутствии образцов

Государствам, не выдающим электронные МСПД с LDS1 и отпечатками пальцев, НЕ СЛЕДУЕТ заполнять DG3. Недостатком группы данных 3 этой структуры является то, что результатом будет статический хэш DG3 в SO_D для всех электронных МСПД LDS1, когда на момент их выдачи биометрические характеристики отсутствуют и не внесены в них, хотя DG3 заявлена. Для целей обеспечения интероперабельности государства, предусматривающие наличие отпечатков пальцев в своих электронных МСПД с LDS1, ДОЛЖНЫ сохранять незаполненный шаблон группы биометрической информации в тех случаях, когда на момент выдачи электронного МСПД с LDS1 данные отпечатков пальцев отсутствуют. В этом случае счетчик шаблона устанавливает значение '00'.

РЕКОМЕНДУЕТСЯ добавлять тег '53' с содержанием, определяемым органом выдачи (например, произвольное число).

Таблица 50. Кодирование при отсутствии образцов

<table>
<tr><th>Тег</th><th>L</th><th colspan="5">Значение</th></tr>
<tr><td>'63'</td><td>Var</td><td colspan="5">Элемент LDS</td></tr>
<tr><td></td><td></td><td>Тег</td><td>L</td><td colspan="3">Значение</td></tr>
<tr><td></td><td></td><td>'7F 61'</td><td>'03'</td><td colspan="3">Шаблон группы биометрической информации</td></tr>
<tr><td></td><td></td><td></td><td>'02'</td><td>'01'</td><td>'00'</td><td>Означает отсутствие шаблонов биометрической информации, хранящихся в этой группе данных</td></tr>
<tr><td></td><td></td><td>'53'</td><td>Var</td><td colspan="3">Содержание, определяемое органом выдачи (например, произвольное число)</td></tr>
</table>

4.7.3.2.3 Кодирование одного образца

В случаях, когда имеется только один отпечаток пальца, кодирование этого одного образца ДОЛЖНО осуществляться следующим образом (пример для DG3: отпечаток пальца).

Таблица 51. Кодирование одного образца

<table>
<tr><th>Тег</th><th>L</th><th colspan="8">Значение</th></tr>
<tr><td>'63'</td><td>Var</td><td colspan="8">Элемент LDS, где aa – общая длина всего содержания данных LDS</td></tr>
<tr><td></td><td></td><td>Тег</td><td>L</td><td colspan="6">Значение</td></tr>
<tr><td></td><td></td><td>'7F 61'</td><td>Var</td><td colspan="6">Шаблон группы биометрической информации</td></tr>
<tr><td></td><td></td><td></td><td>'02'</td><td>'01'</td><td>'01'</td><td colspan="4">Означает общее число отпечатков пальцев, хранимых в виде нижеследующих шаблонов биометрической информации</td></tr>
<tr><td></td><td></td><td></td><td>'7F 60'</td><td>Var</td><td colspan="5">Первый шаблон биометрической информации, где cc – общая длина всего BIT</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'A1'</td><td>Var</td><td colspan="4">Шаблон заголовка биометрической информации</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>'81'</td><td>'01'</td><td>'08'</td><td>Биометрический тип "отпечаток пальца"</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>'82'</td><td>'01'</td><td>'0A'</td><td>Биометрический подтип "левый указательный палец"</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>'87'</td><td>'02'</td><td>'01 01'</td><td>Владелец формата JTC 1 SC 37</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>'88'</td><td>'02'</td><td>'00 07'</td><td>Тип формата стандарта [ИСО/МЭК 19794-4]</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td colspan="5">Следует иметь в виду, что BHT может содержать дополнительные факультативные элементы. Естественно, данный отпечаток пальца может быть отпечатком либо левого, либо правого пальца в зависимости от имеющегося изображения</td></tr>
<tr><td></td><td></td><td></td><td></td><td>'5F 2E'</td><td>Var</td><td colspan="4">Биометрические данные. Указанный блок биометрических данных ДОЛЖЕН содержать в точности одно изображение отпечатка пальца</td></tr>
</table>

Примечание. Стандарт ИСО/МЭК 39794 заменит стандарт ИСО/МЭК 19794:2005 в качестве международного стандарта кодирования биометрических характеристик. См. раздел 4.5.6.

4.7.3.2.4 Кодирование более одного образца

В целях достижения интероперабельности каждая характеристика ДОЛЖНА храниться в отдельном шаблоне биометрической информации. Если такая информация имеется, то расположение этой характеристики ДОЛЖНО быть указано в рамках биометрического подтипа CBEFF. Нижеследующая таблица содержит рассчитанный пример кодирования с использованием CBEFF интероперабельного элемента DG3 с двумя изображениями отпечатков пальцев.

Таблица 52. Кодирование более одного образца

Тег	L	Значение						
'63'	Var	Элемент LDS, где aa – общая длина всего содержания данных LDS						
		Тег	**L**	**Значение**				
		'7F 61'	Var	Шаблон группы биометрической информации				
			'02'	'01'	'02'	Означает общее число отпечатков пальцев, хранимых в виде нижеследующих шаблонов биометрической информации		
			'7F 60'	Var	Первый шаблон биометрической информации			
				'A1'	Var	Шаблон заголовка биометрической информации		
					'81'	'01'	'08'	Биометрический тип "отпечаток пальца"
					'82'	'01'	'0A'	Биометрический подтип "левый указательный палец"
					'87'	'02'	'01 01'	Владелец формата JTC 1 SC 37
					'88'	'02'	'00 07'	Тип формата стандарта [ИСО/МЭК 19794-4]
					Следует иметь в виду, что ВНТ может содержать дополнительные факультативные элементы. Порядок следования отпечатков пальцев (левый/правый) также может отличаться			
				'5F 2E'	Var	Блок биометрических данных. Указанный блок биометрических данных ДОЛЖЕН содержать в точности одно изображение отпечатка пальца		
			'7F 60'	Var	Второй шаблон биометрической информации			
				'A1'	Var	Шаблон заголовка биометрической информации		
					'81'	'01'	'08'	Биометрический тип "отпечаток пальца"
					'82'	'01'	'09'	Биометрический подтип "правый указательный палец"
					'87'	'02'	'01 01'	Владелец формата JTC 1 SC 37
					'88'	'02'	'00 07'	Тип формата стандарта [ИСО/МЭК 19794-4]
					Следует иметь в виду, что ВНТ может содержать дополнительные факультативные элементы. Порядок следования отпечатков пальцев (левый/правый) также может отличаться			
				'5F 2E'	Var	Блок биометрических данных. Указанный блок биометрических данных ДОЛЖЕН содержать в точности одно изображение отпечатка пальца		

Примечание. Стандарт ИСО/МЭК 39794 заменит стандарт ИСО/МЭК 19794:2005 в качестве международного стандарта кодирования биометрических данных. См. раздел 4.5.6.

4.7.4 ГРУППА ДАННЫХ 4. Дополнительные идентификационные характеристики: радужная оболочка глаза (глаз) (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

ИКАО признает, что в поддержку машинного подтверждения личности государства-члены могут использовать в качестве дополнительных биометрических технологий технику распознавания радужной оболочки глаза, изображение которого КОДИРУЕТСЯ в рамках группы данных 4 (DG4).

Таблица 53. Теги группы данных 4

Тег	L	Значение
'76'	Var	См. "Кодировка биометрических данных EF.DG4"

4.7.4.1 Кодировка биометрических характеристик EF.DG4

В группе DG4 ДОЛЖЕН использоваться шаблон группы вложенных шаблонов биометрической информации (BIT), отвечающих требованиям стандарта [ИСО/МЭК 7816-11], что обеспечивает возможность хранения нескольких биометрических образцов, соответствующих единому формату файлов обмена биометрическими данными (CBEFF). Биометрический подзаголовок определяет тип присутствующей биометрической информации и конкретную биометрическую характеристику. Даже для кодировок одного биометрического шаблона ДОЛЖЕН использоваться вариант стандарта [ИСО/МЭК 7816-11]. Последний случай указывается числовым кодированием, при котором n=1. Количество образцов в DG4 может быть ‘0...n’.

Каждый вложенный шаблон имеет нижеследующую структуру.

Таблица 54. Вложенные теги группы данных 4

Тег	L	Значение				
'7F61'	Var	Шаблон группы биометрической информации				
		Тег	**L**	**Значение**		
		'02'	'1'	Целое число – количество образцов этого типа биометрического параметра		
		'7F60'	Var	Первый шаблон биометрической информации		
			Тег	**L**		
			'A'	Var	Шаблон заголовка биометрической информации (BHT)	
				Тег	**L**	**Значение**
				'80'	'02'	Версия '0101' заголовка ИКАО (факультативная информация) – версия основного формата заголовка CBEFF
				'81'	'01–03'	Биометрический тип (факультативная информация)

Тег	L	Значение				
				'82'	'01'	Биометрический подтип (ОБЯЗАТЕЛЬНАЯ информация для DG4)
				'83'	'07'	Дата и время создания (факультативная информация)
				'85'	'08'	Срок действия (с … по) (факультативная информация)
				'86'	'04'	Создатель контрольных биометрических данных (PID) (факультативная информация)
				'87'	'02'	Владелец формата (ОБЯЗАТЕЛЬНАЯ информация)
				'88'	'02'	Тип формата (ОБЯЗАТЕЛЬНАЯ информация)
			'5F2E' или '7F2E'	Var	Биометрические данные (закодированные по правилам владельца формата), именуемые также блоком биометрических данных (BDB)	
		Тег	**L**			
		7F60'	Var	Второй шаблон биометрической информации		
			Тег	**L**		
			'A1'	Var	Шаблон заголовка биометрической информации (BHT)	
				Тег	**L**	**Значение**
				'80'	'02'	Версия '0101' заголовка ИКАО (факультативная информация) – версия основного формата заголовка CBEFF
				'81'	'01–03'	Биометрический тип (факультативная информация)
				'82'	'01'	Биометрический подтип (обязательная информация для DG4)
				'83'	'07'	Дата и время создания (факультативная информация)
				'85'	'08'	Срок действия (с … по) (факультативная информация)
				'86'	'04'	Создатель контрольных биометрических данных (PID) (факультативная информация)
				'87'	'02'	Владелец формата (ОБЯЗАТЕЛЬНАЯ ИНФОРМАЦИЯ)
				88	02	Тип формата (ОБЯЗАТЕЛЬНАЯ ИНФОРМАЦИЯ)
			'5F2E' или '7F2E'	Var	Биометрические данные (закодированные по правилам владельца формата), именуемые также блоком биометрических данных (BDB)	

Для указания CBEFF используется установленный по умолчанию идентификатор OID. Объект данных OID (тег '06'), находящийся непосредственно под шаблоном биометрической информации (BIT, тег '7F60') и указанный в стандарте [ИСО/МЭК 7816-11], в эту структуру не включается. Аналогичным образом в структуре не определяются полномочия на распределение тегов.

В целях обеспечения интероперабельности первая биометрическая информация, записываемая в каждой группе данных, КОДИРУЕТСЯ в соответствии со стандартом [ИСО/МЭК 19794-6].

Примечание. Стандарт ИСО/МЭК 39794 заменит стандарт ИСО/МЭК 19794:2005 в качестве международного стандарта кодирования биометрических данных. См. раздел 4.5.6.

4.7.4.2 ГРУППА ДАННЫХ 4. Элементы данных EF.DG4

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 4 (DG4*)*. Элементы данных и их формат в каждой зоне группы данных УКАЗАНЫ в нижеследующей таблице.

Примечание. A – буквенный символ [a-.z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Таблица 55. Элементы данных для DG4

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
01	M (если закодированная характеристика глаза (глаз) включена)	Количество записанных кодировок биометрических характеристик глаза (глаз)	1	F	N	Цифры 1–9, указывающие количество уникальных кодировок данных о глазе(ах)
02	M (если закодированная характеристика глаза (глаз) включена)	Заголовок		Var	B	Элемент данных может повторяться, как определено элементом данных 01
03	M (если закодированная характеристика глаза (глаз) включена)	Кодировка(и) биометрических характеристик глаза(з)		Var	B	Элемент данных может повторяться, как определено элементом данных 01

4.7.4.2.1 Кодирование биометрического подтипа

Теги шаблона заголовка биометрических данных и установленные для них значения являются минимальной информацией, которая поддерживает каждый вариант реализации, как это показано в нижеследующей таблице. Каждый отдельный шаблон биометрической информации имеет следующую структуру.

Таблица 56. Схема кодирования характеристик: CBEFF

b8	b7	b6	b5	b4	b3	b2	b1	Биометрический подтип
0	0	0	0	0	0	0	0	Информация не дается
						0	1	Правый
						1	0	Левый
			0	0	0			Зарезервировано для будущего использования
			0	0	1			Зарезервировано для будущего использования
			0	1	0			Зарезервировано для будущего использования
			0	1	1			Зарезервировано для будущего использования
			1	0	0			Зарезервировано для будущего использования
			1	0	1			Зарезервировано для будущего использования
X	X	X						Зарезервировано для будущего использования

4.7.4.2.2 Кодирование при отсутствии образцов

Государствам, не выдающим электронные МСПД LDS1 с изображением радужной оболочки глаз, НЕ СЛЕДУЕТ заполнять DG4. Недостатком группы данных 4 этой структуры является то, что результатом будет статический хэш DG4 в SO_D для всех электронных МСПД LDS1, в которых на момент их выдачи биометрические характеристики отсутствуют и не внесены в них, хотя DG4 заявлена. Для целей обеспечения интероперабельности государства, предусматривающие наличие изображения радужной оболочки глаз в своих электронных МСПД LDS1, ДОЛЖНЫ сохранять незаполненный шаблон группы биометрической информации в тех случаях, когда на момент выдачи электронного МСПД LDS1 данные изображений радужной оболочки глаз отсутствуют. В этом случае счетчик шаблона устанавливает значение '00'.

РЕКОМЕНДУЕТСЯ добавлять тег '53' с содержанием, определяемым органом выдачи (например, произвольное число).

Таблица 57. Кодирование при отсутствии образцов

<table>
<tr><th>Тег</th><th>L</th><th colspan="5">Значение</th></tr>
<tr><td>'76'</td><td>Var</td><td colspan="5">Элемент LDS</td></tr>
<tr><td></td><td></td><td>Тег</td><td>L</td><td colspan="3">Значение</td></tr>
<tr><td></td><td></td><td>'7F 61'</td><td>'03'</td><td colspan="3">Шаблон группы биометрической информации</td></tr>
<tr><td></td><td></td><td></td><td>'02'</td><td>'01'</td><td>'00'</td><td>Означает отсутствие шаблонов биометрической информации, хранящихся в этой группе данных</td></tr>
<tr><td></td><td></td><td>'53'</td><td>Var</td><td colspan="3">Содержание, определяемое органом выдачи (например, произвольное число)</td></tr>
</table>

4.7.4.2.3 Кодирование одного образца

В случаях, когда имеется изображение радужной оболочки только одного глаза, этот образец ДОЛЖЕН кодироваться.

4.7.4.2.4 Кодирование более одного образца

В целях достижения интероперабельности каждая характеристика ДОЛЖНА храниться в отдельном шаблоне биометрической информации. Если такая информация имеется, местоположение этой характеристики ДОЛЖНО быть указано в рамках биометрического подтипа CBEFF.

4.7.5 ГРУППА ДАННЫХ 5. Отображаемая фотография (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

Элементами данных, отнесенными к группе данных 5 (DG5), ЯВЛЯЮТСЯ следующие.

Таблица 58. Теги группы данных 5

<table>
<tr><th>Тег</th><th>L</th><th colspan="3">Значение</th></tr>
<tr><td>'65'</td><td>Var</td><td colspan="3"></td></tr>
<tr><td></td><td></td><td>Тег</td><td>L</td><td>Значение</td></tr>
<tr><td></td><td></td><td>'02'</td><td>Var</td><td>Количество образцов этого типа отображаемого изображения (ОБЯЗАТЕЛЬНАЯ ИНФОРМАЦИЯ в первом шаблоне. Не используется в последующих шаблонах)</td></tr>
<tr><td></td><td></td><td>'5F40'</td><td>Var</td><td>Отображаемая фотография</td></tr>
</table>

Применительно к указанному типу отображаемого изображения признаются следующие владельцы формата.

Таблица 59. Форматы DG5

Отображаемая фотография	Владелец формата
Отображаемое изображение лица	Стандарт [ИСО/МЭК 10918], вариант JFIF

4.7.5.1 ГРУППА ДАННЫХ 5. Элементы данных EF.DG5 (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 5 (DG5). Элементы данных и их формат в рамках группы данных 5 УКАЗАНЫ в нижеследующей таблице.

Примечание. A – буквенный символ [a-.z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Таблица 60. Элементы данных для DG5

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
01	M (если отображаемая фотография включена)	Количество записей: отображаемая фотография	1	F	N	Цифры 1–9, указывающие количество уникальных записей отображаемой фотографии
02	M (если отображаемая фотография включена)	Данные об отображаемой фотографии		Var	A,N	Элемент данных может повторяться, как определено элементом данных 01
03	M (если отображаемая фотография включена)	Количество байтов в представлении отображаемой фотографии	5	F	N	Цифры 00001–X9, указывающие количество байтов в представлении отображаемой фотографии
04	M (если отображаемая фотография включена)	Представление отображаемой фотографии		Var	B	Форматируется согласно [ИСО/МЭК 10918-1] или [ИСО/МЭК 15444]

Примечание. Элемент данных 02 КОДИРУЕТСЯ согласно стандарту [ИСО/МЭК 10918], используя вариант JFIF, или стандарту [ИСО/МЭК 15444], используя систему кодирования изображений JPEG 2000.

4.7.6 ГРУППА ДАННЫХ 6. Зарезервировано для будущего использования

Элементами данных, отнесенными к группе 6 (DG6), ЯВЛЯЮТСЯ следующие.

Таблица 61. Теги группы данных 6

Тег	L	Значение
'66'	Var	

4.7.6.1 ГРУППА ДАННЫХ 6. Элементы данных EF.DG6

Элементы данных для группы данных 6 (DG6) зарезервированы для будущего использования.

4.7.7 ГРУППА ДАННЫХ 7. Отображаемая подпись или обычная отметка (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

Элементами данных, отнесенными к группе данных 7 (DG7), ЯВЛЯЮТСЯ следующие.

Таблица 62. Теги группы данных 7

Тег	L	Значение		
'67'	Var			
		Тег	**L**	**Значение**
		'02'	Var	Количество образцов этого типа отображаемого изображения (ОБЯЗАТЕЛЬНАЯ информация в первом шаблоне. Не используется в последующих шаблонах)
		'5F43'	Var	Отображаемая подпись

Применительно к указанному типу отображаемого изображения признаются следующие владельцы формата.

Таблица 63. Форматы DG7

Отображаемое изображение	Владелец формата
Отображаемая подпись/обычная отметка	Стандарт [ИСО/МЭК 10918], вариант JFIF

4.7.7.1 ГРУППА ДАННЫХ 7. Элементы данных EF.DG7 (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 7 (DG7). Элементы данных и их формат в рамках группы данных 7 УКАЗАНЫ в нижеследующей таблице.

Примечание. A – буквенный символ [a-z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Таблица 64. Элементы данных для DG7

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
01	M (если отображаемая подпись или обычная отметка включена)	Количество записей: отображаемая подпись или обычная отметка	1	F	N	Цифры 1–9, указывающие количество уникальных записей отображаемой подписи или обычной отметки
02	M (если отображаемая подпись или обычная отметка включена)	Данные об отображаемой подписи или обычной отметке		Var	B	Элемент данных может повторяться, как определено элементом данных 01. Форматируется согласно [ИСО/МЭК 10918-1] или [ИСО/МЭК 15444]

Примечание. Элемент данных 02 КОДИРУЕТСЯ согласно стандарту [ИСО/МЭК 10918], используя вариант JFIF, или согласно стандарту [ИСО/МЭК 15444], используя систему кодирования изображений JPEG 2000.

4.7.8 ГРУППА ДАННЫХ 8. Элемент(ы) данных (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

Эту группу данных еще предстоит определить. Пока они представляются для временного собственного использования. Эти элементы данных могут использовать структуру, аналогичную структуре для биометрических шаблонов, верификации элементов защиты с помощью машины и для закодированного(ых) элемента(ов). Элементы данных, образующие в совокупности группу данных 8 (DG8), ВКЛЮЧАЮТ следующее.

Таблица 65. Теги группы данных 8

<table>
<tr><th>Тег</th><th>L</th><th colspan="3">Значение</th></tr>
<tr><td>'68'</td><td>Var</td><td colspan="3">Подлежит определению</td></tr>
<tr><td></td><td></td><td>Тег</td><td>L</td><td>Значение</td></tr>
<tr><td></td><td></td><td>'02'</td><td>'1'</td><td>Целое число – количество образцов этого типа шаблона (ОБЯЗАТЕЛЬНАЯ информация в первом шаблоне. Не используется в последующих шаблонах)</td></tr>
<tr><td></td><td></td><td></td><td>Var</td><td>Шаблон заголовка. Детали подлежат определению</td></tr>
</table>

4.7.8.1 ГРУППА ДАННЫХ 8. Элементы данных EF.DG8

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 8 (DG8). Элементы данных и их формат в рамках группы данных 8 УКАЗАНЫ в нижеследующей таблице.

Примечание. A – буквенный символ [a-.z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Таблица 66. Элементы данных для DG8

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
01	M (если закодированный информационный элемент включен)	Количество информационных элементов	1	F	N	Цифры 1–9, указывающие количество уникальных записей информационных элементов (охватывает элементы данных 02 и 03)
02	M (если закодированный информационный элемент включен)	Информация о заголовке (подлежит определению)	1			Определяются детали заголовка
03	M (если закодированный информационный элемент включен)	Данные об информационном элементе	999 макс.	Var	A,N,S, U, B	Формат определяется по усмотрению государства или организации выдачи

4.7.9 ГРУППА ДАННЫХ 9. Структурные элементы (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

Эту группу данных еще предстоит определить. Пока они предоставляются для временного собственного использования. Эти элементы данных могут использовать структуру, аналогичную структуре для биометрических шаблонов. Элементы данных, образующие в совокупности группу данных 9 (DG9). ВКЛЮЧАЮТ следующее.

Таблица 67. Теги группы данных 9

Тег	L	Значение		
'69'	Var	Подлежит определению		
		Тег	**L**	**Значение**
		'02'	'01'	Целое число – количество образцов этого типа шаблона (ОБЯЗАТЕЛЬНАЯ информация в первом шаблоне. Не используется в последующих шаблонах)
			X	Шаблон заголовка. Детали подлежат определению

4.7.9.1 ГРУППА ДАННЫХ 9. Элементы данных EF.DG9

Элементы данных группы данных 9 (DG9) и их формат в рамках каждой зоны группы данных УКАЗАНЫ в нижеследующей таблице.

Примечание. A – буквенный символ [a-z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Таблица 68. Элементы данных для DG9

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
01	M (если закодированный структурный элемент включен)	Количество структурных элементов	1	F	N	Цифры 1–9, указывающие количество уникальных закодированных структурных элементов (охватывает элементы данных 02 и 03)
02	M (если закодированный структурный элемент включен)	Информация о заголовке (подлежит определению)			N	Детали заголовка подлежат определению
03	M (если закодированный структурный элемент включен)	Данные о структурном элементе		Var	B	

4.7.10 ГРУППА ДАННЫХ 10. Вещественный(е) элемент(ы) (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

Эту группу данных еще предстоит определить. Пока они предоставляются для временного собственного использования. Эти элементы данных могут использовать структуру, аналогичную структуре для биометрических шаблонов. Элементы данных, образующие в совокупности группу данных 10 (DG10), ВКЛЮЧАЮТ следующее.

Таблица 69. Теги группы данных 10

<table>
<tr><th>Тег</th><th>L</th><th colspan="3">Значение</th></tr>
<tr><td>'6A'</td><td>Var</td><td colspan="3"></td></tr>
<tr><td></td><td></td><th>Тег</th><th>L</th><th>Значение</th></tr>
<tr><td></td><td></td><td>'02'</td><td>'01'</td><td>Целое число – количество образцов этого типа шаблона
(ОБЯЗАТЕЛЬНАЯ информация в первом шаблоне.
Не используется в последующих шаблонах)</td></tr>
<tr><td></td><td></td><td></td><td>Var</td><td>Подлежит определению</td></tr>
</table>

4.7.10.1 ГРУППА ДАННЫХ 10. Элементы данных EF.DG10

Элементы данных группы данных 10 (DG10) и их формат в рамках каждой зоны группы данных УКАЗАНЫ в нижеследующей таблице.

Примечание. A – буквенный символ [a-z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Таблица 70. Элементы данных для DG10

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
01	M (если закодированный вещественный элемент включен)	Количество вещественных элементов	1	F	N	Цифры 1–9, указывающие количество уникальных закодированных вещественных элементов (охватывает элементы данных 02 и 03)
02	M (если закодированный вещественный элемент включен)	Информация о заголовке (подлежит определению)	TBD	TBD	N	Детали подлежат определению

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
03	M (если закодированный вещественный элемент включен)	Данные о вещественном(ых) элементе(ах)	999 макс.	Var	A,N,S, U, B	Формат определяется по усмотрению государства или организации выдачи

4.7.11 ГРУППА ДАННЫХ 11. Дополнительные личные данные (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

Эта группа данных используется для представления дополнительных данных о владельце документа. Поскольку все элементы данных, входящие в эту группу, являются факультативными, для определения присутствующих элементов используется список тегов.

Примечание. Этот шаблон может содержать символы нелатинского шрифта.

Таблица 71. Теги группы данных 11

Тег	L	Значение				
'6B'	Var					
		Тег	**Дл.**	**Значение**		
		'5C'	Var			Список тегов с перечнем элементов данных в шаблоне
		'5F0E'	Var			Полное имя владельца документа буквами национального алфавита. Кодируется по правилам документа Doc 9303
		'A0'	Var			Категория, соответствующая конкретному содержанию
				Тег	**L**	**Значение**
				'02'	'01'	Количество других имен
				'5F0F'	Var	Другое имя, форматированное согласно документу Doc 9303. Объект данных повторяется столько раз, сколько указано других имен (объект данных с тегом ’02’)
		Тег	**L**	**Значение**		
		'5F10'	Var			Личный номер
		'5F2B'	08			Полная дата рождения yyyymmdd
		'5F11'	Var			Место рождения. Поля отделяются знаком ‘<’

Тег	L	Значение				
		'5F42'	Var			Постоянный адрес. Поля отделяются знаком ‘<’
		'5F12'	Var			Телефон
		'5F13'	Var			Профессия
		'5F14'	Var			Должность
		'5F15'	Var			Личное резюме
		'5F16'	Var			Доказательство гражданства. Сжатое изображение согласно [ИСО/МЭК 10918]
		'5F17'	Var			Номера других действительных ПД. Отделяются ‘<’
		'5F18'	Var			Информация о задержании

4.7.11.1 ГРУППА ДАННЫХ 11. Элементы данных EF.DG11

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 11 (DG11). Элементы данных и их формат в каждой зоне группы данных УКАЗАНЫ в нижеследующей таблице.

Примечание 1. Элемент данных 11 (DG11) КОДИРУЕТСЯ согласно стандарту [ИСО/МЭК 10918], используя вариант JFIF, или согласно стандарту [ИСО/МЭК 15444], используя систему кодирования изображений JPEG 2000.

Примечание 2. A – буквенный символ [a-.z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Таблица 72. Элементы данных для DG11

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
01	O	Имя владельца (полностью)	99 макс.	Var	B	Знаки-заполнители (<) ставятся согласно МСЗ. В конце строки заполнители не ставятся. Усечение не допускается
02	O	Другое имя (имена)	99 макс.	Var	B	Знаки-заполнители (<) ставятся согласно МСЗ. В конце строки заполнители не ставятся. Усечение не допускается

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
03	O	Личный номер	99 макс.	Var	U	Текст произвольного формата
04	O	Полная дата рождения	8	F	N	YYYYMMDD
05	O	Место рождения	99 макс.	Var	U	Текст произвольного формата
06	O	Адрес	99 макс.	Var	U	Текст произвольного формата
07	O	Телефон	99 макс.	Var	N,S	Текст произвольного формата. Рекомендуется кодирование в соответствии с МСЭ-Т E.164
08	O	Профессия	99 макс.	Var	U	Текст произвольного формата
09	M, если элемент данных 08 включен	Должность	99 макс.	Var	U	Текст произвольного формата
10	M, если элемент данных 09 включен	Личное резюме	99 макс.	Var	U	Текст произвольного формата
11	M, если элемент данных 10 включен	Доказательство гражданства		Var	B	Изображение документа о гражданстве форматируется согласно [ИСО/МЭК 10918-1]
12	O	Другой действительный проездной документ(ы). Номер проездного документа	99 макс.	Var	U	Текст произвольного формата, отделяемый знаком <
13	O	Информация о задержании	999 макс.	Var	U	Текст произвольного формата

Примечание. В случае, когда месяц (MM) или день (DD) неизвестны, интероперабельный способ указания этого факта в DG11 состоит в установлении соответствующих знаков на значение ‘00’. В случае, когда столетие и год (CCYY) неизвестны, интероперабельным способом указания этого факта в DG11

является установление соответствующих знаков на значение ‘0000’. Использование дат, устанавливаемых органом выдачи, ДОЛЖНО всегда быть последовательным.

4.7.12 ГРУППА ДАННЫХ 12. Дополнительные данные о документе (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

Эта группа данных используется для представления дополнительной информации об этом документе. Все элементы данных в этой группе являются факультативными.

Таблица 73. Теги группы данных 12

Тег	**L**	**Значение**				
'6C'	Var					
		Тег	**L**	**Значение**		
		'5C'	Var			Список тегов с перечнем элементов данных в шаблоне
		'5F19'	Var			Орган выдачи
		'5F26'	'08'			Дата выдачи yyyymmdd
		'A0'	Var			Категория, соответствующая конкретному содержанию
				Тег	**L**	**Значение**
				'02'	'01'	Количество других людей
				'5F1A'	Var	Имя другого лица, форматированное по правилам документа Doc 9303. Объект данных повторяется столько раз, сколько указано других имен в DE02 (объект данных с тегом ’02’)
		Тег	**L**	**Значение**		
		'5F1B'	Var			Подтвердительные записи, замечания
		'5F1C'	Var			Налоговые/выездные требования
		'5F1D'	Var			Изображение передней части документа. Изображение согласно [ИСО/МЭК 10918]
		'5F1E'	Var			Изображение задней части документа. Изображение согласно [ИСО/МЭК 10918]
		'5F55'	'0E'			Дата и время персонализации документа yyyymmddhhmmss
		'5F56'	Var			Серийный номер системы персонализации

РЕКОМЕНДУЕТСЯ, чтобы системы проверки поддерживали кодирование даты/времени в 8-байтовой системе ASCII и BCD.

4.7.12.1 ГРУППА ДАННЫХ 12. Элементы данных EF.DG12

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 12 (DG12). Элементы данных и их формат в рамках каждой группы данных УКАЗАНЫ в нижеследующей таблице.

Примечание 1. A – буквенный символ [a-z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Примечание 2. Элементы данных 07 и 08 кодируются согласно стандарту [ИСО/МЭК 10918], используя вариант JFIF, или согласно стандарту [ИСО/МЭК 15444], используя систему кодирования изображений JPEG 2000.

Таблица 74. Элементы данных для DG12

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
01	O	Полномочный орган выдачи	99 макс.	Var	U	Текст произвольного формата
02	O	Дата выдачи	8	F	N	Дата выдачи документа, т. е. YYYYMMDD
03	O	Другое(ие) включенное(ые) лицо(а)	99 макс.	Var	U	Текст произвольного формата
04	O	Подтвердительная(ые) надпись(и)/ замечание(я)	99 макс.	Var	U	Текст произвольного формата
05	O	Налоговые/выездные требования	99 макс.	Var	U	Текст произвольного формата
06	O	Изображение передней стороны электронного МСПД		Var	B	Форматируется согласно [ИСО/МЭК 10918-1]
07	O	Изображение задней стороны МСПД		Var	B	Форматируется согласно [ИСО/МЭК 10918-1]
08	O	Время персонализации	14	F	N	yyyymmddhhmmss
09	O	Серийный номер устройства персонализации	99 макс.	Var	U	Произвольный формат

4.7.13 ГРУППА ДАННЫХ 13. Факультативные данные (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

Элементы данных, образующие в совокупности группу данных 13 (DG13), определяемые по усмотрению государства или организации выдачи, ВКЛЮЧАЮТ следующее.

Таблица 75. Теги группы данных 13

Тег	L	Значение
‘6D’	Var	

4.7.14 ГРУППА ДАННЫХ 14. Альтернативные варианты защиты (УСЛОВНО ОБЯЗАТЕЛЬНАЯ ИНФОРМАЦИЯ)

Группа данных 14 (DG14) содержит альтернативные варианты защиты для обеспечения дополнительных механизмов защиты. Подробная информация приводится в части 11 документа Doc 9303. Файл DG14, содержащийся в приложении электронного МСПД, является ОБЯЗАТЕЛЬНЫМ, если чип электронного МСПД поддерживает аутентификацию чипа или механизм PACE-GM/-IM.

Таблица 76. Теги группы данных 14

Тег	L	Значение
'6E'	Var	См. "Сведения о защите группы данных 14" (часть 10 документа Doc 9303)

4.7.14.1 ГРУППА ДАННЫХ 14. Элементы данных EF.DG14

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 14 (DG14). Элементы данных и их формат в рамках каждой группы данных УКАЗАНЫ в нижеследующей таблице.

Примечание. A – буквенный символ [a-z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Таблица 77. Элементы данных для DG14

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
	O	Сведения о защите		Var	B	См. часть 10 документа Doc 9303. Сведения о защите DG 14, как определено в п. 4.7.14.2

4.7.14.2 Сведения о защите ГРУППЫ ДАННЫХ 14

Нижеследующая общая структура данных "Сведения о защите", кодируемых по ASN.1, позволяет применять альтернативные варианты защиты с использованием вспомогательных биометрических характеристик. В целях достижения интероперабельности РЕКОМЕНДУЕТСЯ, чтобы эта структура данных обеспечивалась чипом электронного МСПД в DG14 для указания поддерживаемых протоколов защиты. Упомянутая структура данных приводится ниже:

```
      SecurityInfos     ::=   SET of SecurityInfo

      SecurityInfo      ::=   SEQUENCE {
            protocol          OBJECT IDENTIFIER,
            requiredData      ANY DEFINED BY protocol,
            optionalData      ANY DEFINED BY protocol OPTIONAL
}
```

Элементы, содержащиеся в структуре данных "Сведения о защите", имеют следующее значение:

- протокол идентификатора объекта указывает поддерживаемый протокол;
- обязательные данные открытого типа содержат обязательные данные конкретно для этого протокола;
- факультативные данные открытого типа содержат факультативные данные конкретно для этого протокола.

4.7.15 ГРУППА ДАННЫХ 15. Информация об открытом ключе активной аутентификации (УСЛОВНО ОБЯЗАТЕЛЬНАЯ ИНФОРМАЦИЯ)

Эта ФАКУЛЬТАТИВНАЯ группа данных содержит открытый ключ активной аутентификации и является ОБЯЗАТЕЛЬНОЙ, когда применяется факультативная аутентификация чипа посредством активной аутентификации, как это описано в документе части 11 документа Doc 9303.

Таблица 78. Теги группы данных 15

Тег	Дл.	Значение
'6F'	Var	См. часть 11 документа Doc 9303

4.7.15.1 ГРУППА ДАННЫХ 15. Элементы данных EF.DG15

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 15 (DG15). Элементы данных и их формат в каждой зоне группы данных УКАЗАНЫ в нижеследующей таблице.

Примечание. A – буквенный символ [a-z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Таблица 79. Элементы данных для DG15

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
	O	Информация об открытом ключе активной аутентификации		Var	B	См. часть 11 документа Doc 9303

4.7.16 ГРУППА ДАННЫХ 16. Уведомляемое(ые) лицо(а) (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

В этой группе данных указывается информация, связанная со срочным уведомлением. Она кодируется как серия шаблонов с использованием тег-обозначения ‘Ax’. Группу данных DG16 (DG16) (как и другие группы данных) НЕ СЛЕДУЕТ обновлять после выдачи; DG16 представлена в SO_D хэш-значением, и SO_D подписывается только при выдаче.

Таблица 80. Теги группы данных 16

Тег	L	Значение		
'70'	Var			
		Тег	**L**	**Значение**
		'02'	'01'	Количество шаблонов (указывается только в первом шаблоне)
		'Ax'	Var	Начало шаблона, где x (x = 1,2,3…) возрастает с каждым последующим шаблоном
'5F50'	04'			Записанная дата
'5F51'	Var			Фамилия лица
'5F52'	Var			Телефон
'5F53'	Var			Адрес

4.7.16.1 ГРУППА ДАННЫХ 16. Элементы данных EF.DG16

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в группе данных 16 (DG16). Элементы данных и их формат в каждой зоне группы данных УКАЗАНЫ в нижеследующей таблице.

Примечание. A – буквенный символ [a-z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Таблица 81. Элементы данных для DG16

Элемент данных	Факультативный или ОБЯЗАТЕЛЬНЫЙ	Название элемента данных	Количество байтов	Фиксированный или переменный	Тип кодирования	Требования к кодированию
01	M, если DG16 включена	Количество идентифицируемых лиц	1	F	N	Указывает количество лиц, включенных в эту группу данных
02	M, если DG16 включена	Записанные данные о дате	8	F	N	Записанная дата уведомления; формат = YYYYMMDD
03	M, если DG16 включена	Имя уведомляемого лица. Основной и вторичный идентификаторы		Var	A,N,S	Знаки-заполнители (<) ставятся согласно МСЗ. Усечение не допускается
04	M, если элемент данных 03 включен	Номер телефона уведомляемого лица		Var	N,S	Номер телефона в международной форме (код страны и местный номер). Рекомендуется кодирование в соответствии с МСЭ-Т E.164
05	M	Адрес уведомляемого лица		Var	U	Текст произвольного формата

5. ПРИЛОЖЕНИЯ LDS2 (ФАКУЛЬТАТИВНЫЕ)

Логическая структура данных 2 (LDS2) является факультативным, обратно совместимым расширением к чипу электронного МСПД с LDS1, которая обеспечит возможность цифрового и надежного хранения информации о поездках после выдачи документа. LDS2 расширяет возможности использования электронных МСПД посредством введения дополнительных приложений, позволяющих в цифровом формате хранить данные о поездках (визы и путевые отметки) и другую информацию, способную оказать содействие выполнению поездки владельцем (дополнительная биометрическая информация) в течение срока действия его документа. Более эффективное использование полного потенциала электронных МСПД посредством "оцифровки" остальных данных, содержащихся в этих документах, предоставляет возможность использования преимуществ при одновременном повышении степени защиты документов от подделки, копирования и несанкционированного считывания или внесения информации.

В число дополнительных факультативных приложений LDS2 входят:

- записи (отметки) о поездках;
- электронные визы;
- дополнительные биометрические характеристики.

Для внедрения любого ФАКУЛЬТАТИВНОГО приложения LDS2 ОБЯЗАТЕЛЬНЫМ является наличие приложения LDS1 электронного МСПД.

5.1 Приложение "Записи о поездках" (УСЛОВНО ОБЯЗАТЕЛЬНОЕ)

Приложение "Записи о поездках" МОЖЕТ быть внедрено государством или организацией выдачи. В случае реализации факультативного приложения "Записи о поездках" условно ОБЯЗАТЕЛЬНЫМИ элементами являются следующие:

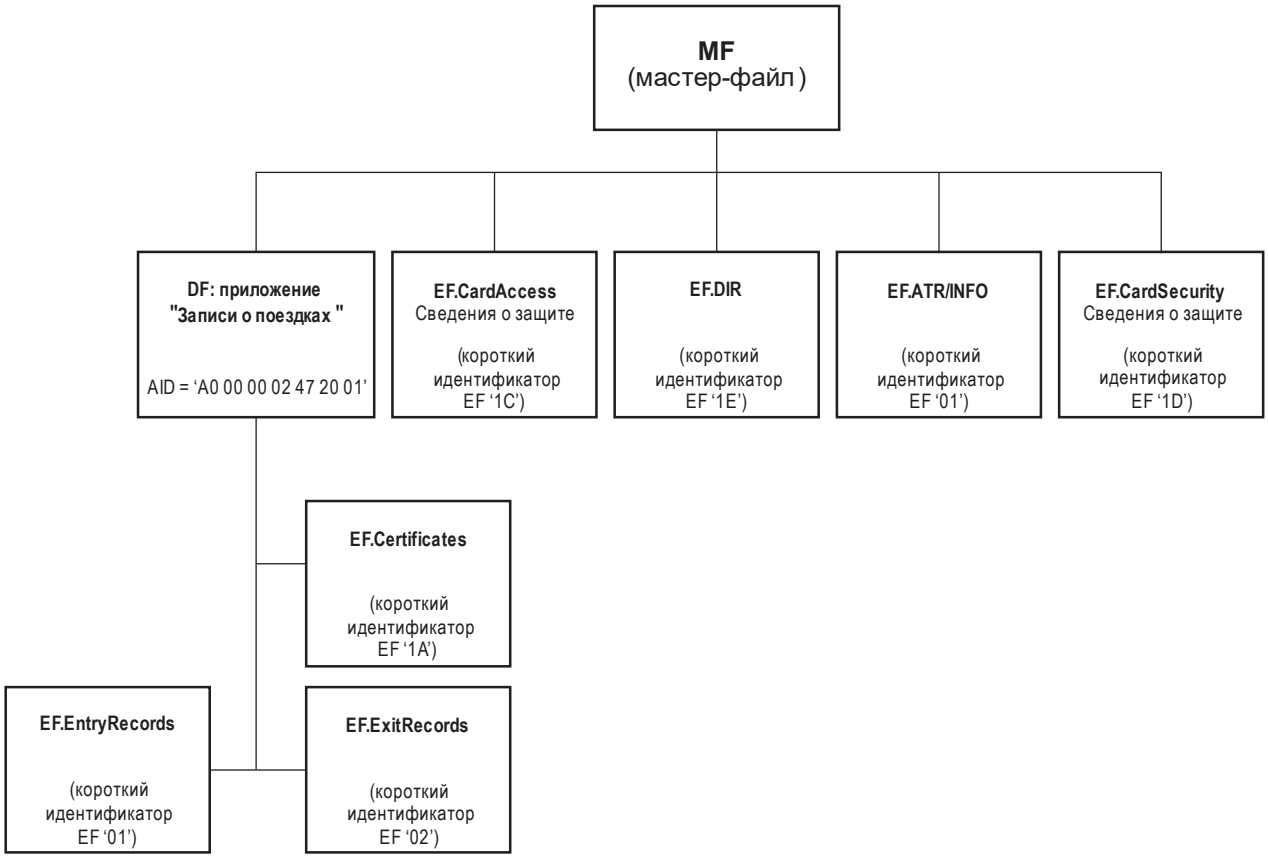

Рис. 4. Структура записей о поездках

Записи о поездках с указанием пункта въезда/выезда хранятся в двух отдельных элементарных файлах EF.EntryRecords и EF.ExitRecords DF приложения "Записи о поездках", каждый из которых имеет линейную структуру с записями переменного размера, как предусмотрено стандартом [ИСО/МЭК 7816-4]. Сертификаты органов, подписывающих записи о поездках, хранятся в отдельном элементарном файле EF.Certificates, имеющем линейную структуру с записями переменного размера.

5.1.1 Выбор приложения: DF

Приложение "Записи о поездках" ДОЛЖНО выбираться посредством использования идентификатора приложения (AID) в качестве зарезервированного имени DF. AID ДОЛЖЕН состоять из зарегистрированного идентификатора приложения, присвоенного ИСО в соответствии со стандартом [ИСО/МЭК 7816-5], и проприетарного расширения идентификатора приложения (PIX) "Записи о поездках":

- зарегистрированный идентификатор приложения равен ‘A0 00 00 02 47’;
- приложение "Записи о поездках" ДОЛЖНО использовать PIX = ‘20 01’;
- полный AID приложение "Записи о поездках" ДОЛЖЕН быть равен ‘A0 00 00 02 47 20 01’.

Если эффективная авторизация не предоставляет прав доступа к каким-либо данным в приложении LDS2, то ИС ДОЛЖНА отказать в выборе этого приложения.

5.1.2 Файл EF.Certificates (ОБЯЗАТЕЛЬНЫЙ)

Сертификаты органов, подписывающих записи о поездках, хранятся в EF внутри приложения DF и имеют линейную структуру с записями переменного размера. Эти сертификаты предназначены для использования IS при проведении дополнительной автономной валидации цифровых подписей каждой записи в файлах EF.ExitRecords и EF.EntryRecords.

Таблица 82. Файл EF.Certificates

Имя файла	EF.Certificates
ID файла	‘011A’
Короткий идентификатор EF	‘1A’
Доступ к командам Select / FMM Access	PACE+TA (согласно таблице 96 бит b3 авторизации записей о поездках)
Доступ для считывания записей / выбора записей	PACE+TA (согласно таблице 96 бит b3 авторизации записей о поездках)
Доступ для дополнения записей	PACE+TA (согласно таблице 96 бит b4 авторизации записей о поездках)
Доступ для записей / обновления записей	НИКОГДА
Доступ для стирания записей	НИКОГДА
Структура файла	Линейная структура с записями переменного размера
Размер	Переменный

Запись, касающаяся сертификата, содержит одиночный объект данных сертификата LDS2-TS Signer X.509. Сослаться на запись, касающуюся сертификата, МОЖНО посредством одной или нескольких записей о поездках, содержащих информацию о пунктах въезда и выезда.

Таблица 83. Формат записи файлф EF.Certificates

Тег	Содержание	Обязательный/ факультативный	Формат	Пример
‘5F3A’	Серийный номер сертификата	M	V(22)B	‘5F3A’ ‘Len’ {Код страны|| Серийный номер }
‘72’	Сертификат X.509	M	V (900) B	‘72’ ‘Len’ {Сертификат X.509 }

Примечание. Указанные в настоящей таблице межотраслевые теги используются в контексте LDS, поэтому сосуществующая схема распределения тегов не требуется.

DO ‘5F3A’ ДОЛЖЕН содержать двухбуквенный код страны, предусмотренный частью 3 документа Doc 9303 (кодирование и значение аналогичные X.509, содержащему название страны выдачи на сертификате субъекта), за которым следует серийный номер сертификата.

Каждый сертификат X.509 содержит набор закодированных элементов ASN.1, наглядно представленный в таблице 84. Подробные требования к сертификату X.509 содержатся в спецификации профиля сертификата, приводимого в части 12 документа Doc 9303.

Таблица 84. Пример структуры сертификата X.509

Поле	Описание	Иллюстративное значение
Сертификат		
версия	Должна быть версия 3	2
Серийный номер	Индивидуальное положительное целое число	макс. 20 байтов
подпись	Алгоритм подписи	ecdsa-with-SHA256
выдающий орган		
название страны	Название государства выдачи	‘США’
общее название	Название выдающего органа (макс. 9 символов)	‘DHSCA0001’
срок действия		
не ранее	Дата вступления сертификата в силу	‘131225000000Я’
не позднее	Дата истечения срока действия сертификата	‘230824235959Z’
субъект		
название страны	Название страны IS	‘США’
общее название	Название IS (макс. 9 символов)	‘SFO000001’
Информация об открытом ключе субъекта		
Алгоритм открытого ключа	ecОткрытыйКлюч	
Открытый ключ субъекта	Открытый ключ IS	Открытый ключ ECC256
расширения		
Идентификатор ключа полномочного органа		
Расширенная применимость ключей		
Алгоритм подписи	ecdsa-with-SHA256	
Подпись	Подпись выдающего органа	Подпись ECDSA256

Примечание. Настоящая таблица является лишь иллюстративным примером. Записи сертификатов вносятся в файлы EF.Certificates, расположенные под приложением "Записи о поездках" DF с использованием команды APPEND RECORD. Записи сертификатов могут быть считаны с файлов EF.Certificates с использованием команды READ RECORD. Записи сертификатов НЕ ДОЛЖНЫ обновляться или стираться. Максимальное количество записей в файле EF.Certificates под приложением "Записи о поездках" DF ДОЛЖНО составлять 254.

5.1.3 Файл EF.ExitRecords (ОБЯЗАТЕЛЬНЫЙ)

Файл Exit Records ДОЛЖЕН дополняться санкционированной IS после посадки на борт.

Таблица 85. Файл EF.ExitRecords

Имя файла	EF.ExitRecords
ID файла	’0102’
Короткий идентификатор EF	’02’
Доступ к команде Select / FMM Access	PACE+TA (согласно таблице 96 бит b1 авторизации записи о поездках)
Доступ для считывания записей / выбора записей	PACE+TA (согласно таблице 96 бит b1 авторизации записи о поездках)
Доступ для дополнения записей	PACE+TA (согласно таблице 96 бит b2 авторизации записи о поездках)
Доступ для записей / обновления записей	НИКОГДА
Доступ для стирания записей	НИКОГДА
Структура файла	Линейная структура с записями переменного размера
Размер	Переменный

Содержание файла Exit Record показано в таблице 86.

Примечание. Отраслевые теги, указанные в таблице ниже, используется в контексте LDS, поэтому сосуществующая схема распределения тегов не требуется.

Таблица 86. Формат записи пунктов въезда/выезда

Тег	Тег	Содержание	Обязательный /ФАКУЛЬТА-ТИВНЫЙ	Формат	Пример
‘5F44’		Государство посадки/высадки пассажиров (копия для SEARCH RECORD)	M	F (3) A	США
‘73’	Записи о пунктах въезда/выезда (подписываемая информация)				
	‘5F44’	Государство посадки/высадки пассажиров	M	F (3) A	США
	‘5F4C’	Утверждение, отказ и аннулирование виз	O	V (50) A,N,S,U	Текст произволь-ного формата
	‘5F45’	Дата поездки (дата въезда/выезда)	M	F (8) N	20120814 (yyyymmdd)
	‘5F4B’	Проверяющий полномочный орган	M	V (10) A,N,S	СВР
	‘5F46’	Место проведения проверки (пункт въезда/выезда)	M	V (10) A,N,S	SFO
	‘5F4A’	Рекомендации проверяющего	M	V (20) A,N,S	SFO00001234
	‘5F4D’	Результат проверки	O	V (50) A,N,S,U	Текст произволь-ного формата
	‘5F49’	Вид перевозки	O	F (1) A	A (воздушная), S (морская), L (наземная)
	‘5F48’	Продолжительность пребывания (дни)	O	V (2) B	‘00FF’ (255 дней)
	‘5F4E’	Условия, подлежащее соблюдению владельцем по время пребывания в выдающем государстве	O	V(50) A,N,S,U	Текст произволь-ного формата
‘5F37’	Жетон аутентичности (подпись)		M	V (140) B	‘5F’ ‘37’ Len {подпись}
‘5F38’	Ссылка (номер записи) на сертификат органа, подписывающего LDS2-TS в хранилище сертификатов		M	F (1) B	‘01’ …’FE’

Примечание.1 A – буквенный символ [a-z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины.

Примечание 2. Поскольку, по всей вероятности, сертификаты органа, подписывающего LDS2-TS, будут аналогичными в различных записях о поездках (например, при въезде или выезде из страны через тот же аэропорт, имеющий только один орган, подписывающий LDS2-TS), до внесения в файл EF.Certificates нового сертификата/добавления, IS следует изучить файлы EF.Certificates на предмет обнаружения копии аналогичного сертификата и ссылки на имеющийся сертификат. Это уменьшит размер файла EF.Certificates и позволит ускорить процесс просмотра.

Примечание 3. LDS2 электронного МСПД не следит за соблюдением того, что IS вносит записи о въезде только в файл EF.EntryRecords, а не в файлы EF.ExitRecords, и наоборот.

Примечание 4. Трехбуквенные коды государств посадки/высадки пассажиров соответствуют указанным в части 3 документа Doc 9303.

Порядок объектов данных в записи является фиксированным. IS ДОЛЖНА составлять содержание записи с использованием объектов данных в порядке, указанном в настоящей таблице.

Каждая запись ДОЛЖНА содержать цифровую подпись (жетон аутентичности), вычисленную над DO'73', включая тег 73 и длину. Подпись генерируется органом, подписывающим LDS2-TS.

Сертификаты органа, подписывающего LDS2-TS, необходимые для верификации подписи "Записей о поездках", ДОЛЖНЫ храниться в файлах EF.Certificates под DF приложением "Записи о поездках", если они уже не присутствуют в том же файле.

Записи о поездках вносятся (добавляются) в EF посредством команды APPEND RECORD. Записи о поездках НЕ ДОЛЖНЫ изменяться (обновляться) или исключаться. Максимально допустимое количество записей в каждом EF ЛОЖНО составлять 254.

5.1.4 Файл EF.EntryRecords (ОБЯЗАТЕЛЬНЫЙ)

Файл Entry Records ДОЛЖЕН дополняться санкционированной IS после высадки пассажиров.

Таблица 87. Файл EF.EntryRecords

Имя файла	EF.EntryRecords
ID файла	'0101'
Короткий идентификатор EF	'01'
Доступ к команде Select / FMM Access	PACE+TA (согласно таблице 96 бит b1 авторизации записи о поездках)
Доступ для считывания записей / выбора записей	PACE+TA (согласно таблице 96 бит b1 авторизации записи о поездках)
Доступ для дополнения записей	PACE+TA (согласно таблице 96 бит b2 авторизации записи о поездках)
Доступ для записей / обновления записей	НИКОГДА
Доступ для стирания записей	НИКОГДА
Структура файла	Линейная структура с записями переменного размера
Размер	Переменный

Структура записи информации о въезде идентична структуре записи информации о выезде, указанной в таблице 86.

5.2 Приложение "Визовые записи" (УСЛОВНО ОБЯЗАТЕЛЬНОЕ)

Приложение "Визовые записи" МОЖЕТ быть внедрено государством или организацией выдачи. В случае реализации факультативного приложения "Визовые записи", указанные ниже элементы являются УСЛОВНО ОБЯЗАТЕЛЬНЫМИ.

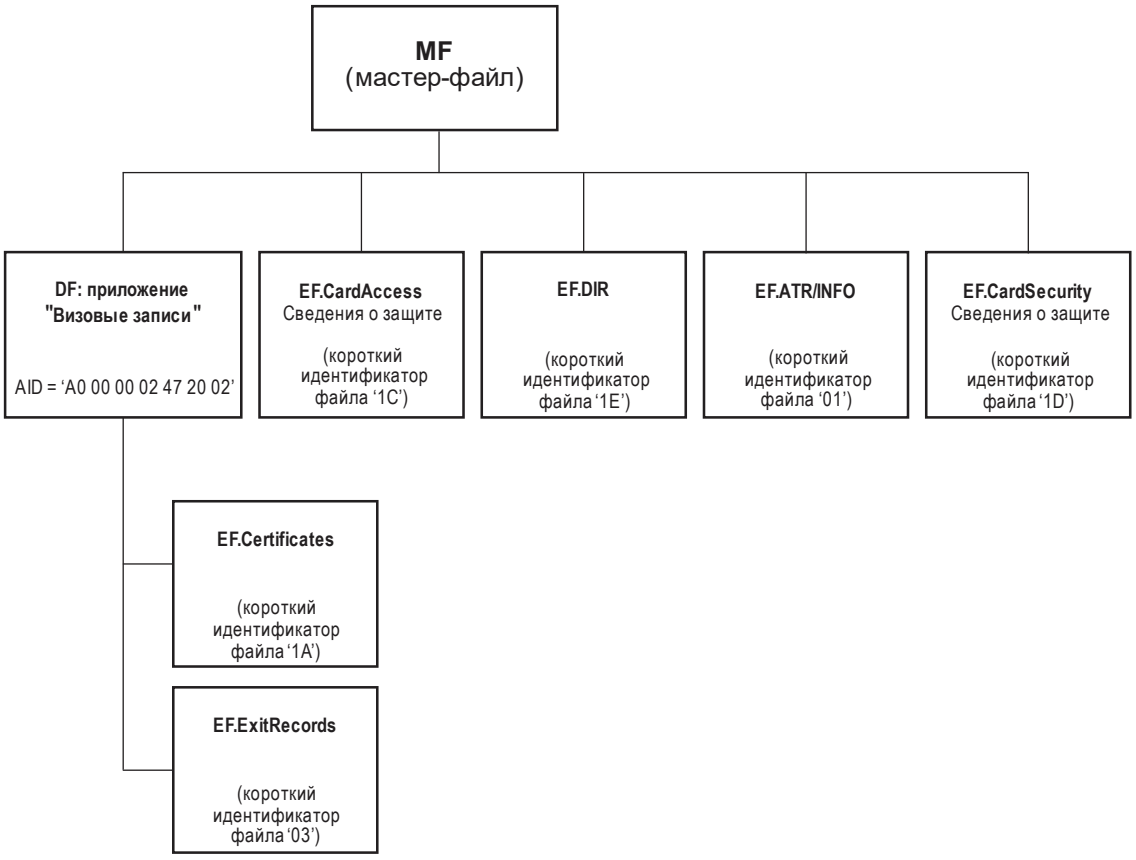

Рис. 5. Структура визовых записей

Визовые записи хранятся в элементарном файле EF.VisaRecords под приложением DF "Визовые записи". Файл EF ИМЕЕТ линейную структуру с записями переменного размера в соответствии со стандартом [ИСО/МЭК 7816-4]. Сертификаты органа, подписывающего записи о визах, хранятся отдельно в элементарном файле EF.Certificates, имеющим линейную структуру с записями переменного размера.

5.2.1 Выбор приложения: DF

Приложение "Визовые записи" ДОЛЖНО выбираться посредством использования идентификатора приложения (AID) в качестве зарезервированного файла DF. AID ДОЛЖЕН состоять из зарегистрированного идентификатора приложения, присвоенного ИСО в соответствии со стандартом [ИСО/МЭК 7816-5], и проприетарного расширения идентификатора приложения (PIX) приложения "Визовые записи":

- Зарегистрированный идентификатор приложения равен 'A0 00 00 02 47';

- Приложение "Визовые записи" ДОЛЖНО использовать PIX = ‘20 02’;
- Полный AID приложения "Визовые записи" равен ‘A0 00 00 02 47 20 02’.

Если эффективная авторизация не предоставляет прав доступа к каким-либо данным в приложении LDS2, то ИС ДОЛЖНА отказать в выборе этого приложения.

5.2.2 Файл EF.Certificates (ОБЯЗАТЕЛЬНЫЙ)

Сертификаты органов, подписывающих визовые записи, хранятся в EF.Certificates внутри приложения DF и имеют линейную структуру с записями переменного размера. Эти сертификаты предназначены для использования IS в целях проведения дополнительной автономной валидации цифровых подписей каждой записи в файлах EF.VisaRecords.

Таблица 88. Файл EF.Certificates

Имя файла	EF.Certificates
ID файла	‘011A’
Короткий идентификатор EF	‘1A’
Доступ к команде Select / FMM Access	PACE+TA (согласно таблице 97 бит b3 авторизации записи о визах)
Доступ для считывания записей / выбора записей	PACE+TA (согласно таблице 97 бит b3 авторизации записи о визах)
Доступ для дополнения записей	PACE+TA (согласно таблице 97 бит b4 авторизации записи о визах)
Доступ для записей / обновления записей	НИКОГДА
Доступ для стирания записей	НИКОГДА
Структура файла	Линейная структура с записями переменного размера
Размер	Переменный

Запись, касающаяся сертификата, содержит одиночный объект данных сертификата LDS2-TS Signer X.509. Сослаться на запись, касающуюся сертификата, МОЖНО посредством одной или нескольких визовых записей.

Структура записи, касающейся сертификата, в визовом приложении идентична структуре аналогичной записи в приложении "Записи о поездках", определяемой в таблице 83.

Записи, касающиеся сертификатов, вносятся в файл EF.Certificates, расположенный под приложением DF "Визовые записи" посредством команды APPEND RECORD. Записи, касающиеся сертификатов,

могут считываться с файла EF.Certificates посредством команды READ RECORD. Эти записи НЕ ДОЛЖНЫ обновляться или стираться. Максимальное количество записей в файле EF.Certificates под приложением DF "Визовые записи" ДОЛЖНО составлять 254.

5.2.3 Файл EF.VisaRecords (ОБЯЗАТЕЛЬНЫЙ)

Визовые записи ДОЛЖНЫ храниться в файле EF.VisaRecords, имеющим линейную структуру с записями переменного размера.

Таблица 89. Файл EF.VisaRecords

Имя файла	EF.VisaRecords
ID файла	‘0103’
Короткий идентификатор EF	‘03’
Доступ к команде Select / FMM Access	PACE+TA (согласно таблице 97 бит b1 авторизации записи о визах)
Доступ для считывания записей / выбора записей	PACE+TA (согласно таблице 97 бит b1 авторизации записи о визах)
Доступ для дополнения записей	PACE+TA (согласно таблице 97 бит b2 авторизации записи о визах)
Доступ для записей / обновления записей	НИКОГДА
Доступ для стирания записей	НИКОГДА
Структура файла	Линейная структура с записями переменного размера
Размер	Переменный

Каждая визовая запись ДОЛЖНА содержать последовательность объектов данных BER-TLV (DO ‘5F28’ и DO ‘71’), за которой следует жетон аутентичности (подпись) DO и DO, содержащий ссылку на сертификат подписывающего органа LDS2-V в файле EF.Certificates. DO ‘71’ содержит набор DO (поля), перечисленных в таблице ниже.

Примечание. Межотраслевые теги, указанные в таблице ниже, используются в контексте LDS, поэтому сосуществующая схема распределения тегов не требуется.

Таблица 90. Формат файла EF.VisaRecords

Тег	Тег	Содержание	ОБЯЗАТЕЛЬНЫЙ/ УСЛОВНО ОБЯЗАТЕЛЬНЫЙ	Формат	Пример
‘5F28’		Государство или организация выдачи (копия для команды SEARCH RECORD)	M	F (3) A	NLD
‘71’	Визовая запись (подписанная информация)				
	‘5F28’	Государство или организация выдачи	M	F (3) A	NLD
	‘43’	Тип документа	M	F (2) A,N,S	VS
	‘5F71’	Машиносчитываемая виза типа A	O	F (48) A,N,S	
	‘5F72’	Машиносчитываемая виза типа B	O	F (44) A,N,S	VCD<<DENT<<ARTHUR< PHILIP<<<<<<<<<<<
	‘5F73’	Количество въездов	O	V (1) B	‘01’ – ‘FF’
	‘5F74’	Продолжительность пребывания (дни, месяцы, годы)	O	F (3) B	‘010000’ – ‘FFFFFF’
	‘5F75’	Номер паспорта	O	F (9) A,N,S	XI85935F8
	‘5F76’	Тип/класс/категория визы	O	V (4) B	
	‘5F77’	Информация о территории	O	V (8) B	
	‘49’	Место выдачи (выдающий полномочный орган)	M	V (50) A, Sp	НЬЮ-ЙОРК
	‘5F25’	Дата вступления в силу (дата выдачи)	M	F (8) N	20120826 (yyyymmdd)
	‘5F24’	Дата истечения срока действия	M	F (8) N	20130826 (yyyymmdd)
	‘5A’	Номер документа	M	F (9) A,N,S	XI85935F8
	‘5F32’	Дополнительная информация (подтверждения: продолжительность, ограничения и уплаченные сборы)	O	V (50) A,N,S,U	Текст произвольного формата
	‘5B’	Имя владельца (полное имя)	M	V (50) A, Sp	VAN DER STEEN MARIANNE LOUISE
	‘5F33’	Основной идентификатор (фамилия)	M	V (50) A, Sp	VAN DER STEEN
	‘5F34’	Дополнительный идентификатор (имя)	M	V (50) A, Sp	MARIANNE LOUISE
	‘5F35’	Пол	M	F (1) A,S	F, M, or <
	‘5F2B’	Дата рождения	M	F (8) N,S	19870814 (yyyymmdd)

Тег	Тег	Содержание	ОБЯЗАТЕЛЬНЫЙ/ УСЛОВНО ОБЯЗАТЕЛЬНЫЙ	Формат	Пример
	‘5F2C’	Гражданство	M	F (3) A	NLD
	‘5F1F’	MCЗ	M	V (50) A,N,S	VAN<DER<STEEN<< MARIANNE<LOUISE
	‘5F40’	Ссылка на EF "Дополнительные биометрические характеристики"	O	F (2) B	’0201’
‘5F37’	Жетон аутентичности (подпись)		M	V (140), B	‘5F’ ‘37’ Len {подпись}
‘5F38’	Ссылка (номер записи) на орган, подписывающий сертификаты LDS2-V в хранилище сертификатов		M	F (1) B	‘01’ …’FE’

Примечание 1. A – буквенный символ [a-z, A-Z], N – цифровой символ [0-9], S – специальный символ ['<'], B – двоичные данные, F – поле фиксированной длины, Var – поле переменной длины, Sp – интервал.

Примечание 2. Трехбуквенный код выдачи, предусмотренный частью 3 документа Doc 9303.

Примечание 3. Факультативный DO’5F40’, если присутствует, ДОЛЖЕН содержат 2-байтный идентификатор в приложении "Дополнительные биометрические характеристики", содержащем биометрическую информацию. Этот DO может использоваться только при наличии на электронном МСПД приложения "Дополнительные биометрические характеристики".

Порядок расположения объектов данных в записи является фиксированным. IS ДОЛЖНА формировать содержание записи с использованием объектов данных в порядке, указанном в таблице.

Каждая визовая запись ДОЛЖНА содержать цифровую подпись (жетон аутентичности), рассчитанную над DO’71’, включая тег 71 и длину. Подпись генерируется органом, подписывающим LDS2-V.

Сертификаты органов, подписывающих LDS2-V, необходимые для проверки подписи визовой записи, хранятся в отдельном файле EF.Certificates store, расположенном под приложением DF "Визовые записи".

Каждая визовая запись ДОЛЖНА вноситься в файл EF.VisaRecords посредством команды APPEND RECORD. Visa Records и НЕ ДОЛЖНЫ изменяться (обновляться) или стираться. Максимально допустимое количество записей в файле EF.VisaRecords ДОЛЖНО составлять 254.

5.3 Приложение "Дополнительные биометрические характеристики" (УСЛОВНО ОБЯЗАТЕЛЬНОЕ)

Приложение "Дополнительные биометрические характеристики" МОЖЕТ быть внедрено государством или организацией выдачи. В случае реализации факультативного приложения "Дополнительные биометрические характеристики" или наличия в визовой записи ссылки на него условно ОБЯЗАТЕЛЬНЫМИ элементами являются.

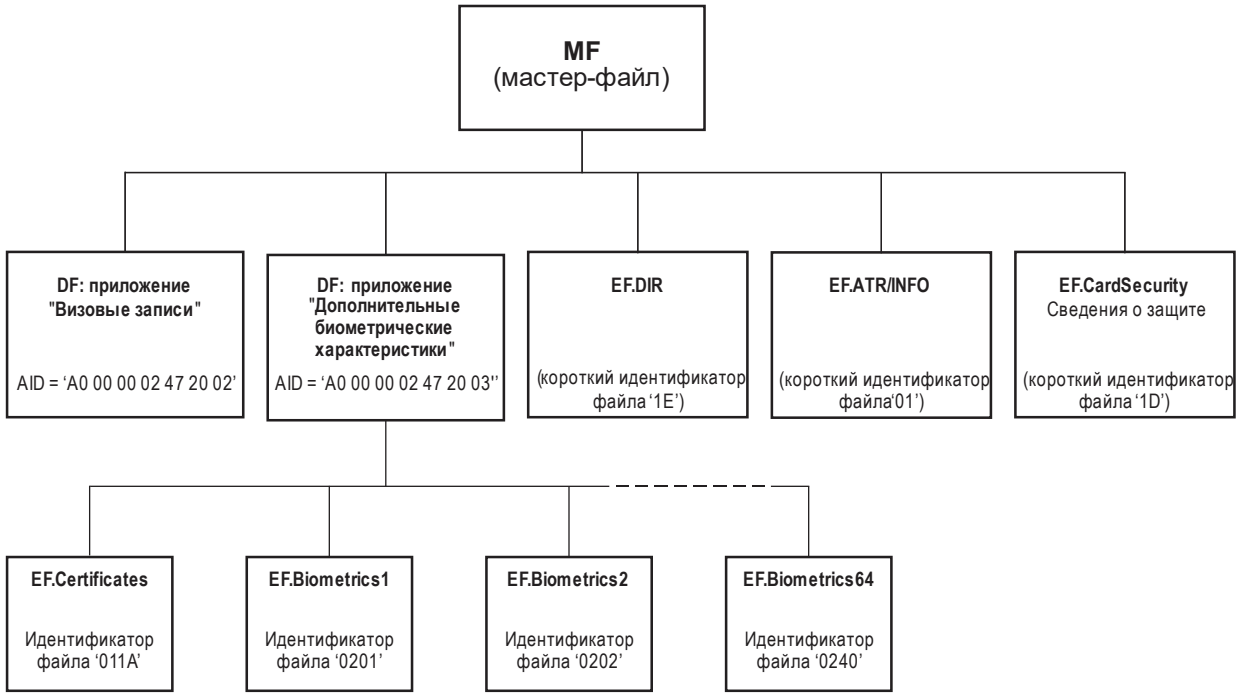

Рис. 6. Структура приложения "Дополнительные биометрические характеристики"

5.3.1 Выбор приложения: DF

Приложение "Дополнительные биометрические характеристики" ДОЛЖНО выбираться посредством использования идентификатора приложения (AID) в качестве зарезервированного имени DF. AID ДОЛЖЕН состоять из зарегистрированного идентификатора приложения, присвоенного ИСО в соответствии со стандартом [ИСО/МЭК 7816-5], и проприетарного расширения идентификатора приложения (PIX) приложения "Дополнительные биометрические характеристики":

- Зарегистрированный идентификатор приложения равен 'A0 00 00 02 47';
- Приложение "Дополнительные биометрические характеристики" ДОЛЖНО использовать PIX = '20 03';
- Полный идентификатор AID приложения "Дополнительные биометрические характеристики" ДОЛЖЕН быть равен 'A0 00 00 02 47 20 03'.

Если эффективная авторизация не предоставляет прав доступа к каким-либо данным в приложении LDS2, то ИС ДОЛЖНА отказать в выборе этого приложения.

5.3.2 Файл EF.Certificates (ОБЯЗАТЕЛЬНЫЙ)

Сертификаты органов, подписывающих дополнительные биометрические характеристики, хранятся в файле EF.Certificates внутри приложения DF и имеют линейную структуру с записями переменного размера. Эти сертификаты предназначены для использования IS в целях проведения дополнительной автономной валидации цифровой подписи в файле EF.Biometrics.

Таблица 91. Файл EF.Certificates

Имя файла	EF.Certificates
ID файла	‘011A’
Короткий идентификатор EF	‘1A’
Доступ к командам Select / FMM	PACE+TA (авторизация дополнительных биометрических характеристик, бит b1 байта 1 (см. таблицу 98)
Доступ к командам Read Record/Search Record	PACE+TA (авторизация дополнительных биометрических характеристик, бит b1 байта 1 (см. таблицу 98)
Доступ к команде Append Record	PACE+TA (авторизация дополнительных биометрических характеристик, бит b1 байта 1 (см. таблицу 98)
Доступ к командам Write/Update Record	НИКОГДА
Доступ к команде Erase Record	НИКОГДА
Структура файла	Линейная структура с записями переменного размера
Размер	Переменный

Запись, касающаяся сертификата, содержит одиночный объект данных органа, подписывающего сертификаты дополнительных биометрических характеристик X.509. На запись сертификата можно сослаться посредством одного или нескольких файлов EF "Дополнительные биометрические характеристики".

Структура записи, касающейся сертификата в приложении "Дополнительные биометрические характеристики," идентична структуре аналогичной записи в приложении "Дополнительные биометрические характеристики", определяемой в таблице 83.

Записи, касающиеся сертификатов, вносятся в файл EF.Certificates, расположенный под приложением DF "Дополнительные биометрические характеристики, посредством команды APPEND RECORD. Эти записи можно считать с файла EF.Certificates посредством команды READ RECORD. Записи сертификатов НЕ ДОЛЖНЫ обновляться или стираться. Максимальное количество записей в файле EF.Certificates под приложением DF "Дополнительные биометрические характеристики" ДОЛЖНО составлять 64.

5.3.3 Файл EF.Biometrics

Информации о дополнительных биометрических характеристиках ДОЛЖНА храниться в файлах EF "Дополнительные биометрические характеристики" и иметь транспарентную структуру, соответствующую стандарту [ИСО/МЭК 7816-4].

Каждый EF "Дополнительные биометрические характеристики" МОЖЕТ быть связан с одной или несколькими записями в EF "Визовые записи" приложения "Визовые записи" (или других EF и приложениях) посредством использования идентификатора EF "Дополнительные биометрические характеристики".

Таблица 92. Файлы EF.Biometrics1 – EF.Biometrics64

Имя файла	EF.Biometrics1 – EF.Biometrics64
ID файла	‘0201’ – ‘0240’
Короткий идентификатор EF	N/A
Команды Select / FMM / Read Access в дезактивизированном состоянии	PACE+TA (авторизация дополнительных биометрических характеристик в соответствии с таблицей 98, биты b2, b4, b6, b8 байтов 2-17)
Команда Write Access в дезактивизированном состоянии	PACE+TA (авторизация дополнительных биометрических характеристик в соответствии с таблицей 98, биты b2, b4, b6, b8 байтов 2-17)
Команда Activate Access в дезактивизированном состоянии	PACE+TA (авторизация дополнительных биометрических характеристик в соответствии с таблицей 98, биты b2, b4, b6, b8 байтов 2-17)
Команды Select / FMM / Read Access в активизированном состоянии	PACE+TA (авторизация дополнительных биометрических характеристик в соответствии с таблицей 98, биты b1, b3, b5, b7 байтов 2-17)
Команда Write Access в активизированном состоянии	НИКОГДА
Команда Activate Access в активизированном состоянии	НИКОГДА
Команда Erase Access	НИКОГДА
Структура файла	Транспарентая структура
Размер	Переменный

Каждый EF "Дополнительные биометрические характеристики" ДОЛЖЕН содержать объект данных DO’7F2E’ BER-TLV, инкапсулирующий три объекта данных: DO’5F2E’ биометрических данных, за которым следуют DO’5F37’ "жетон аутентичности" (подпись) и DO'5F38, содержащий ссылку на сертификат органа, подписывающего биометрические характеристики в файле EF.Certificates, как показано в таблице ниже.

Содержание DO’5F2E’ зависит от органа, определяющего дополнительные биометрические характеристики, и рамками настоящей спецификации не охватываются.

Механизм создания EF "Дополнительные биометрические характеристики" рамками настоящей спецификации не охватывается. Выдающему органу СЛЕДУЕТ заранее создать ряд EF "Дополнительные биометрические характеристики".

Примечание. Межотраслевые теги, указанные в таблице ниже, используются в контексте LDS, поэтому сосуществующая схема распределения тегов не требуется.

Таблица 93. Формат файла EF.Biometrics

Тег	Тег	Содержание	ОБЯЗАТЕЛЬНЫЙ/ УСЛОВНО ОБЯЗАТЕЛЬНЫЙ	Формат	Пример
‘7F2E’		Шаблон биометрических данных	M		‘7F’ ‘2E’ Len {DO’5F2E’ || DO’5F37’ || DO’5F38’}
	‘5F2E’	Дополнительные биометрические данные	M	V, B	‘5F’ ‘2E’ Len {биометрические данные}
	‘5F37’	Жетон аутентичности (подпись)	M	V (140), B	‘5F’ ‘37’ Len {подпись}
	‘5F38’	Ссылка (номер записи) на сертификат органа, подписывающего дополнительные биометрические характеристики в хранилище сертификатов	M	F (1) B	‘01’ …’40’

Примечание. B = бинарные данные, F = поле фиксированное длины, V = поле переменной длины.

Порядок объектов данных в EF является фиксированным.

Каждый EF "Дополнительные биометрические характеристики" ДОЛЖЕН содержать цифровую подпись (жетон аутентичности), рассчитанную посредством DO’5F2E’, включая тег и длину. Эта подпись генерируется органом, подписывающим "Дополнительные биометрические характеристики".

Сертификат органа, подписывающего "Дополнительные биометрические характеристики", необходимый для проверки подписи "Дополнительных биометрических характеристик", хранится в отдельном файле EF.Certificates, расположенном под приложением DF "Дополнительные биометрические характеристики".

Каждый EF "Дополнительные биометрические характеристики" ДОЛЖЕН записываться посредством команды UPDATE BINARY.

EF "Дополнительные биометрические характеристики" НЕ ДОЛЖЕН изменяться (обновляться) или стираться. Максимальное количество EF "Дополнительные биометрические характеристики" составляет 64.

Перечень всех возможных имен EF "Дополнительные биометрические характеристики", идентификаторов и коротких идентификаторов приводится в таблице 94.

Таблица 94. Идентификаторы EF.Biometrics

Имя EF	EF идентификатор	Короткий идентификатор EF	Имя EF	EF идентификатор	Короткий идентификатор EF
EF.Biometrics1	‘0201’	N/A	EF.Biometrics33	‘0221’	N/A
EF.Biometrics2	‘0202’	N/A	EF.Biometrics34	‘0222’	N/A
EF.Biometrics3	‘0203’	N/A	EF.Biometrics35	‘0223’	N/A
EF.Biometrics4	‘0204’	N/A	EF.Biometrics36	‘0224’	N/A
EF.Biometrics5	‘0205’	N/A	EF.Biometrics37	‘0225’	N/A
EF.Biometrics6	‘0206’	N/A	EF.Biometrics38	‘0226’	N/A
EF.Biometrics7	‘0207’	N/A	EF.Biometrics39	‘0227’	N/A
EF.Biometrics8	‘0208’	N/A	EF.Biometrics40	‘0228’	N/A
EF.Biometrics9	‘0209’	N/A	EF.Biometrics41	‘0229’	N/A
EF.Biometrics10	‘020A’	N/A	EF.Biometrics42	‘022A’	N/A
EF.Biometrics11	‘020B’	N/A	EF.Biometrics43	‘022B’	N/A
EF.Biometrics12	‘020C’	N/A	EF.Biometrics44	‘022C’	N/A
EF.Biometrics13	‘020D’	N/A	EF.Biometrics45	‘022D’	N/A
EF.Biometrics14	‘020E’	N/A	EF.Biometrics46	‘022E’	N/A
EF.Biometrics15	‘020F’	N/A	EF.Biometrics47	‘022F’	N/A
EF.Biometrics16	‘0210’	N/A	EF.Biometrics48	‘0230’	N/A
EF.Biometrics17	‘0211’	N/A	EF.Biometrics49	‘0231’	N/A
EF.Biometrics18	‘0212’	N/A	EF.Biometrics50	‘0232’	N/A
EF.Biometrics19	‘0213’	N/A	EF.Biometrics51	‘0233’	N/A
EF.Biometrics20	‘0214’	N/A	EF.Biometrics52	‘0234’	N/A
EF.Biometrics21	‘0215’	N/A	EF.Biometrics53	‘0235’	N/A
EF.Biometrics22	‘0216’	N/A	EF.Biometrics54	‘0236’	N/A
EF.Biometrics23	‘0217’	N/A	EF.Biometrics55	‘0237’	N/A
EF.Biometrics24	‘0218’	N/A	EF.Biometrics56	‘0238’	N/A
EF.Biometrics25	‘0219’	N/A	EF.Biometrics57	‘0239’	N/A
EF.Biometrics26	‘021A’	N/A	EF.Biometrics58	‘023A’	N/A
EF.Biometrics27	‘021B’	N/A	EF.Biometrics59	‘023B’	N/A
EF.Biometrics28	‘021C’	N/A	EF.Biometrics60	‘023C’	N/A
EF.Biometrics29	‘021D’	N/A	EF.Biometrics61	‘023D’	N/A
EF.Biometrics30	‘021E’	N/A	EF.Biometrics62	‘023E’	N/A
EF.Biometrics31	‘021F’	N/A	EF.Biometrics63	‘023F’	N/A
EF.Biometrics32	‘0220’	N/A	EF.Biometrics64	‘0240’	N/A

5.4 Условия доступа к файлу приложения LDS2 (УСЛОВНО ОБЯЗАТЕЛЬНЫЙ)

5.4.1 Функции и уровни авторизации по умолчанию (ОБЯЗАТЕЛЬНЫЕ)

В каждом сертификате CV содержится шаблон авторизации держателя сертификата (CHAT), идентифицирующий функции держателя сертификата (IS, DV, CVCA), и информация о правах доступа к DG3/DG4 ОБЯЗАТЕЛЬНОГО приложения LDS2 электронного МСПД (для учета предыдущих версий или других видов национального использования).

В CHAT содержится последовательность двух объектов:

a) идентификатор объекта, определяющий тип терминала и формат шаблона [TR-03110]:

```
id-roles OBJECT IDENTIFIER ::= {bsi-de applications(3) mrtd(1) 2}
id-IS       OBJECT IDENTIFIER ::= {id-roles 1}
```

b) объект дискретных данных (тег '53'), содержащий информацию о бит-кодированных функциях и правах доступа держателя сертификата только для считывания в соответствии с приводимой ниже таблицей:

Таблица 95. Авторизация CHAT по умолчанию

	Описание	Байт1							
		b8	b7	b6	b5	b4	b3	b2	b1
Функция	CVCA	1	1						
	DV (национальный)	1	0						
	DV (зарубежный)	0	1						
	IS	0	0						
Доступ для считывания	RFU								
	RFU								
	RFU								
	RFU								
	DG4 (радужная оболочка глаза)							1	
	DG3 (отпечаток пальца)								1

Примечание. LDS2 электронного МСПД ДОЛЖНА игнорировать значение битов RFU в авторизации держателя сертификата.

5.4.2 Уровни авторизации приложения (ОБЯЗАТЕЛЬНЫЕ)

Авторизации держателя сертификата для каждого приложения LDS2 кодируется в расширениях сертификатов CV (одно расширение на приложение). Расширение сертификата представляет собой дискретный

шаблон (тег ‘73’), включающий в себя два объекта данных: идентификатор объекта авторизации (тег ‘06’) для конкретного приложения и объект дискретных данных (тег ‘53’), содержащих информацию о бит-кодированных правах доступа держателя сертификата к специфичному приложению.

Для определения эффективной авторизации держателя сертификата чип электронного МСПД с LDS2 вычисляет поразрядное булевое ‘и’ прав доступа, содержащиеся в расширениях сертификата IS и сертификатах зарегистрированных DV и CVCA.

Для приложения "Записи о поездках" идентификаторы объектов аутентификации и права доступа кодируются следующим образом:

```
id-icao-lds2-travelRecords         OBJECT IDENTIFIER  ::= {id-icao-lds2 1}
id-icao-lds2-travelRecords-access OBJECT IDENTIFIER   ::= {id-icao-lds2-
travelRecords 3}
```

Таблица 96. Авторизации для приложения "Записи о поездках"

	Описание	Байт 1							
		b8	b7	b6	b5	b4	b3	b2	b1
Права доступа	RFU								
	RFU								
	RFU								
	RFU								
	Команда Append EF.Certificates					1			
	Команда Read/Search/Select/FMM EF.Certificates						1		
	Команда Append EF.EntryRecords/ExitRecords							1	
	Команда Read/Search/Select/FMM EF.EntryRecords/ExitRecords								1

Для приложения "Визовые записи" идентификаторы объектов аутентификации и права доступа кодируются следующим образом:

```
id-icao-lds2-visaRecords           OBJECT IDENTIFIER  ::= {id-icao-lds2 2}
id-icao-lds2-visaRecords-access OBJECT IDENTIFIER     ::= {id-icao-lds2-
visaRecords 3}
```

Таблица 97. Авторизации для приложения "Визовые записи"

	Описание	Байт 1							
		b8	b7	b6	b5	b4	b3	b2	b1
Права доступа	RFU								
	RFU								
	RFU								
	RFU								
	Append EF.Certificates					1			
	Read/Search/Select/FMM EF.Certificates						1		
	Append EF.VisaRecords							1	
	Read/Search/Select/FMM EF.VisaRecords								1

Для приложения "Дополнительные биометрические характеристики" идентификаторы объектов аутентификации и права доступа кодируются следующим образом:

```
id-icao-lds2-additionalBiometrics  OBJECT IDENTIFIER ::= {id-icao-lds2 3}

id-icao-lds2-additionalBiometrics-access   OBJECT   IDENTIFIER::=   {id-icao-lds2-
additionalBiometrics 3}
```

Таблица 98. Авторизации для приложения "Дополнительные биометрические характеристики"

	Описание	Идентификатор EF	Авторизации							
			b8	b7	b6	b5	b4	b3	b2	b1
Байт 1	RFU									
	RFU									
	RFU									
	RFU									
	RFU									
	RFU									
	Команда Append EF.Certificates	‘011A’							1	
	Команда Select/FMM/Read/Search EF.Certificates	‘011A’								1
Байт 2	Команда Select/FMM/Write/Activate/Read EF.Biometrics1 в дезактивизированном состоянии	‘0201’	1							
	Команда Select/FMM/Read EF.Biometrics1 в активизированном состоянии	‘0201’		1						

	Команда Select/FMM/Write/Activate/Read EF.Biometrics2 в дезактивизированном состоянии	‘0202’			1					
	Команда Select/FMM/Read EF.Biometrics2 в активизированном состоянии	‘0202’				1				
	Команда Select/FMM/Write/Activate/Read EF.Biometrics3 в дезактивизированном состоянии	‘0203’					1			
	Команда Select/FMM/Read EF.Biometrics3 в активизированном состоянии	‘0203’						1		
	Команда Select/FMM/Write/Activate/Read EF.Biometrics4 в дезактивизированном состоянии	‘0204’							1	
	Команда Select/FMM/Read EF.Biometrics4 в активизированном состоянии	‘0204’								1

…

Байт 17	Select/FMM/Write/Activate/Read EF.Biometrics61 в дезактивизированном состоянии	‘023D’	1							
	Select/FMM/Read EF.Biometrics61 в активизированном состоянии	‘023D’		1						
	Select/FMM/Write/Activate/Read EF.Biometrics62 в дезактивизированном состоянии	‘023E’			1					
	Select/FMM/Read EF.Biometrics62 в активизированном состоянии	‘023E’				1				
	Select/FMM/Write/Activate/Read EF.Biometrics63 в дезактивизированном состоянии	‘023F’					1			
	Select/FMM/Read EF.Biometrics63 в активизированном состоянии	‘023F’						1		
	Select/FMM/Write/Activate/Read EF.Biometrics64 в дезактивизированном состоянии	‘0240’							1	
	Select/FMM/Read EF.Biometrics64 в активизированном состоянии	‘0240’								1

Примечание 1. LDS2 электронного МСПД ДОЛЖНА игнорировать значения битов RFU в авторизации держателя сертификата.

Примечание 2. Государства или организации выдачи НЕ ДОЛЖНЫ выдавать IS сертификаты терминалов с авторизациями на запись/активизирование, если в отношении дополнительных биометрических характеристик они имеют авторизацию только на считывание.

6. ИДЕНТИФИКАТОРЫ ОБЪЕКТОВ

6.1 Сводная информация об идентификаторах объектов приложений LDS1 и LDS2

Таблица 99. OID приложений LDS1.7, LDS1.8 и LDS2

Идентификатор объекта	Значение	Замечания
id-icao	joint-iso-itu-t(2) international-organizations(23) icao(136)	OID ИКАО
id-icao-mrtd	id-icao 1	OID электронного МСПД
id-icao-mrtd-security	id-icao-mrtd 1	
id-icao-ldsSecurityObject	id-icao-mrtd-security 1	Объект защиты LDS
id-icao-mrtd-security-cscaMasterList	id-icao-mrtd-security 2	Мастер-список CSCA
id-icao-mrtd-security-cscaMasterListSigningKey	id-icao-mrtd-security 3	
id-icao-mrtd-security-documentTypeList	id-icao-mrtd-security 4	Список типов документов
id-icao-mrtd-security-aaProtocolObject	id-icao-mrtd-security 5	Протокол активной аутентификации
id-icao-mrtd-security-extensions	id-icao-mrtd-security 6	Изменение названия CSCA
id-icao-mrtd-security-extensions-nameChange	id-icao-mrtd-security-extensions 1	
id-icao-mrtd-security-extensions-documentTypeList	id-icao-mrtd-security-extensions 2	Тип документа DS
id-icao-mrtd-security-DeviationList	id-icao-mrtd-security 7	Базовые OID списка дефектов
id-icao-mrtd-security-DeviationListSigningKey	id-icao-mrtd-security 8	
id-icao-lds2	id-icao-mrtd-security 9	Идентификаторы объектов LDS2
id-icao-lds2-travelRecords	id-icao-lds2 1	Базовые OID приложения "Записи о поездках"
id-icao-lds2-travelRecords-application	id-icao-lds2-travelRecords 1	AID записей о поездках
id-icao-lds2-travelRecords-access	id-icao-lds2-travelRecords 3	Расширение сертификата авторизации
id-icao-lds2-visaRecords	id-icao-lds2 2	Базовый OID приложения "Визовые записи"
id-icao-lds2-visaRecords-application	id-icao-lds2-visaRecords 1	AID визовых записей
id-icao-lds2-visaRecords-access	id-icao-lds2-visaRecords 3	Расширение сертификата авторизации
id-icao-lds2-additionalBiometrics	id-icao-lds2 3	Базовый OID дополнительных биометрических характеристик
id-icao-lds2-additionalBiometrics-application	id-icao-lds2-additionalBiometrics 1	AID дополнительных биометрических характеристик
id-icao-lds2-additionalBiometrics-access	id-icao-lds2-additionalBiometrics 3	Расширение сертификата авторизации
id-icao-lds2Signer	id-icao-lds2 8	Идентификаторы объекта органа, подписывающего LDS2

id-icao-tsSigner	id-icao-lds2Signer 1	Сертификат органа, подписывающего путевые отметки LDS2
id-icao-vSigner	id-icao-lds2Signer 2	Сертификат органа, подписывающего визы LDS2
id-icao-bSigner	id-icao-lds2Signer 3	Сертификат органа, подписывающего биометрические характеристики LDS2
id-icao-spoc	id-icao-mrtd-security 10	Идентификаторы объектов SPOC
id-icao-spocClient	id-icao-spoc 1	Клиент
id-icao-spocServer	id-icao-spoc 2	Сервер

7. СПЕЦИФИКАЦИИ ASN.1

```
id-icao OBJECT IDENTIFIER ::= {joint-iso-itu-t(2) international-organizations(23)
icao(136) }
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 1}

id-icao-mrtd-security-cscaMasterList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 2}
id-icao-mrtd-security-cscaMasterListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 3}
id-icao-mrtd-security-documentTypeList OBJECT IDENTIFIER ::= {id-icao-mrtd-security
4}
id-icao-mrtd-security-aaProtocolObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security
5}

id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-mrtd-security 6}
id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::= {id-icao-mrtd-
security-extensions 1}
id-icao-mrtd-security-extensions-documentTypeList OBJECT IDENTIFIER ::= {id-icao-
mrtd-security-extensions 2}
id-icao-mrtd-security-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 7}
id-icao-mrtd-security-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-
security 8}

id-icao-lds2 OBJECT IDENTIFIER ::= {id-icao-mrtd-security 9}
```

Идентификаторы объекта приложения LDS2 "Записи о поездках"

```
id-icao-lds2-travelRecords OBJECT IDENTIFIER ::= {id-icao-lds2 1}
id-icao-lds2-travelRecords-application OBJECT IDENTIFIER ::= {id-icao-lds2-
travelRecords 1}
id-icao-lds2-travelRecords-access OBJECT IDENTIFIER ::= {id-icao-lds2-travelRecords
3}
```

Идентификаторы объекта приложения LDS2 "Визовые записи"

```
id-icao-lds2-visaRecords OBJECT IDENTIFIER ::= {id-icao-lds2 2}
id-icao-lds2-visaRecords-application OBJECT IDENTIFIER ::= {id-icao-lds2-visaRecords
1}
id-icao-lds2-visaRecords-access OBJECT IDENTIFIER ::= {id-icao-lds2-visaRecords 3}
```

Идентификаторы объекта приложения LDS2 "Дополнительные биометрические характеристики"

```
id-icao-lds2-additionalBiometrics OBJECT IDENTIFIER ::= {id-icao-lds2 3}
id-icao-lds2-additionalBiometrics-application OBJECT IDENTIFIER ::= {id-icao-lds2-
additionalBiometrics 1}
id-icao-lds2-additionalBiometrics-access OBJECT IDENTIFIER ::= {id-icao-lds2-
additionalBiometrics 3}

id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-lds2 8}
id-icao-tsSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 1}
id-icao-vSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 2}
```

```
id-icao-bSigner OBJECT IDENTIFIER ::=  {id-icao-lds2Signer  3}

id-icao-spoc OBJECT IDENTIFIER ::=  {id-icao-mrtd-security 10}
id-icao-spocClient OBJECT IDENTIFIER ::=  {id-icao-spoc 1}
id-icao-spocServer OBJECT IDENTIFIER ::=  {id-icao-spoc 2}
```

8. СПРАВОЧНЫЕ МАТЕРИАЛЫ (НОРМАТИВНЫЕ)

ИСО/МЭК 14443-1	ИСО/МЭК 14443-1:2016. *Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 1. Физические характеристики*
ИСО/МЭК 14443-2	ИСО/МЭК 14443-2:2016. *Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 2. Радиочастотный энергетический и сигнальный интерфейс*
ИСО/МЭК 14443-3	ИСО/МЭК 14443-3:2016. *Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 3. Инициализация и антиколлизия*
ИСО/МЭК 14443-4	ИСО/МЭК 14443-4:2016. *Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия. Часть 4. Протокол передачи*
ИСО/МЭК 10373-6	ИСО/МЭК 10373-6:2016. *Карты идентификационные. Методы испытаний. Часть 6. Карты близкого действия*
ИСО/МЭК 18745-2	ИСО/МЭК 18745-2:2016. *Информационные технологии. Методы испытаний машиносчитываемых паспортно-визовых документов (MRTD) и сопутствующих устройств. Часть 2. Методы испытаний бесконтактных интерфейсов*
ИСО/МЭК 7816-2	ИСО/МЭК 7816-2:2007. *Карты идентификационные. Карты на интегральных схемах. Часть 2. Карты с контактами. Размеры и расположение контактов*
ИСО/МЭК 7816-4	ИСО/МЭК 7816-4:2013. *Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена*
ИСО/МЭК 7816-5	ИСО/МЭК 7816-5:2004. *Карты идентификационные. Карты на интегральных схемах. Часть 5. Регистрация провайдеров прикладных программ*
ИСО/МЭК 7816-6	ИСО/МЭК 7816-6:2016. *Карты идентификационные. Карты на интегральных схемах с контактами. Часть 6. Элементы данных для межотраслевого обмена (включая сообщения о дефектах)*
ИСО/МЭК 7816-11	ИСО/МЭК 7816-11:2017. *Карты идентификационные. Карты на интегральных схемах. Часть 11. Верификация личности биометрическими методами*

ИСО/МЭК 8825-1	ИСО/МЭК 8825-1:2008. *Информационная технология. Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования*
ИСО/МЭК 19794-4	ИСО/МЭК 19794-4:2005. *Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца*
ИСО/МЭК 19794-5	ИСО/МЭК 19794-5:2005. *Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица*
ИСО/МЭК 19794-6	ИСО/МЭК 19794-6:2011. *Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза*
ИСО/МЭК 10646	ИСО/МЭК 10646:2012. *Информационные технологии. Универсальный набор кодированных символов (UCS).*
RFC 3369	Синтаксис криптографического сообщения 2002
ИСО/МЭК 10918-1	ИСО/МЭК 10918-1:1994. *Информационные технологии. Цифровое уплотнение и кодирование неподвижных изображений с непрерывным спектром тонов. Часть 1. Требования и руководящие указания*
ИСО/МЭК 15444	ИСО/МЭК 15444-n. *Система кодирования изображений JPEG 2000.*
ИСО/МЭК 19785	ИСО/МЭК 19785-n. *Информационные технологии. Единая структура форматов обмена биометрическими данными*
ИСО/МЭК 19795-6	ИСО/МЭК 19795-6:2012. *Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 6. Методология проведения оперативных испытаний*
ИСО/МЭК 39794-4	ИСО/МЭК 39794-4:2019. *Информационные технологии. Расширяемые форматы обмена биометрическими данными. Часть 4. Данные изображения пальцев*
ИСО/МЭК 39794-5	ИСО/МЭК 39794-5:2019. *Информационные технологии. Расширяемые форматы обмена биометрическими данными. Часть 5. Данные изображения лица*
ИСО/МЭК 39794-6	ИСО/МЭК 39794-6:2021. *Информационные технологии. Расширяемые форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза*

— — — — — — — —

Добавление A к части 10

ПРИМЕРЫ ОТОБРАЖЕНИЯ ЛОГИЧЕСКОЙ СТРУКТУРЫ ДАННЫХ (ИНФОРМАЦИОННОЕ)

В нижеследующем тексте информативного характера приводятся примеры отображения логической структуры данных (LDS версии 1.7) на бесконтактной интегральной схеме электронного МСПД с использованием метода представления данных путем произвольного доступа.

A.1 ОБЩИЕ ЭЛЕМЕНТЫ ДАННЫХ В ФАЙЛЕ EF.COM

Ниже приводится пример реализации версии 1.7 LDS с использованием версии 4.0.0 Unicode при наличии групп данных 1 (тег ‘61’), 2 (тег ‘75’), 4 (тег ‘76’) и 12 (тег ‘6C’).

В этом и других примерах теги печатаются **жирным шрифтом**, длина – *курсивом*, а значение – латинским шрифтом. Шестнадцатеричные теги, длина и значения приводятся в (‘xx’).

‘60’ *‘16’*
‘5F01’ *‘04’* ‘0107’
‘5F36’ *‘06’* ‘040000’
‘5C’ *‘04’* ‘6175766C’

В полном шестнадцатеричном представлении данный пример будет читаться следующим образом:

‘60’ *‘16’*
‘5F01’ *‘04’* ‘30313037’
‘5F36’ *‘06’* ‘303430303030’
‘5C’ *‘04’* ‘6175766C’

Гипотетическая версия 15.99 LDS будет кодироваться так:

‘60’ *‘16’*
‘5F01’ *‘04’* ‘1599’
‘5F36’ *‘06’* ‘040000’
‘5C’ *‘04’* ‘6175766C’

или так в шестнадцатеричном представлении:

‘60’ *‘16’*
‘5F01’ *‘04’* ‘31353939’
‘5F36’ *‘06’* ‘303430303030’
‘5C’ *‘04’* ‘6175766C’

A.2 ИНФОРМАЦИЯ МАШИНОСЧИТЫВАЕМОЙ ЗОНЫ В ФАЙЛЕ EF.DG1

A.2.1 Электронный МСПД размера ПД1

Ниже приводится пример DG1 с использованием этой информации в электронном МСПД с LDS1 размера ПД1. Длина элемента данных МСЗ составляет 90 байтов (‘5A’).

‘61’ *‘5D’* **‘5F1F’** *‘5A’*

```
I<NLDXI85935F86999999990<<<<<<7208148F1108268NLD<<<<<<<<<<<4VAN<DER<STEEN<<MARI
ANNE<LOUISE
```

A.2.2 Электронный МСПД размера ПД2

Ниже приводится пример DG1 с использованием этой информации в электронном МСПД с LDS1 размера ПД2. Длина элемента данных МСЗ составляет 72 байта (‘48’).

‘61’ *‘4B’* **‘5F1F’** *‘48’*

```
I<ATASMITH<<JOHN<T<<<<<<<<<<<<<<<<<<<<<<<<<123456789<HMD7406222M10123130121<<<
54
```

A.3 БИОМЕТРИЧЕСКИЕ ШАБЛОНЫ В ФАЙЛАХ EF.DG2 – EF.DG4

Группы DG2–DG4 используют вариант стандарта ИСО/МЭК 7816-11, предусматривающий вложение без использования карточки, для обеспечения возможности хранения нескольких биометрических образцов определенного типа, соответствующих единой структуре форматов обмена биометрическими данными (CBEFF), [NISTR 6529a]. Биометрический подзаголовок определяет тип имеющейся биометрической информации и конкретную биометрическую характеристику.

Пример. Один подписанный биометрический параметр лица с длиной блока биометрических данных 12 642 байта (‘3162’ байта), закодированный с использованием устройства, имеющего PID ‘00 01 00 01’, и типа формата ‘00 04’, принадлежащего провайдеру шаблона ‘00 0A’, был взят 15 марта 2002 года (без смещения относительно времени UTC) и действителен с 1 апреля 2002 года по 31 марта 2007 года. Используется основная версия 1.0 шаблона ИКАО.

Общая длина шаблона 12 704 байта. Шаблон записывается в начале EF.DG2 (SFID 02).

‘75’ *‘82319EC’*
- **‘7F61’** *‘823199’*
  - **‘02’** *‘01’* ‘01’
  - **‘7F60’** *‘823191’*
  - **‘A1’** *‘26’*
    - **‘80’** *‘02’* ‘0101’
    - **‘81’** *‘01’* ‘02’
    - **‘83’** *‘07’* ‘20020315133000’
    - **‘85’** *‘08’* ‘2002040120070331’
    - **‘86’** *‘04’* ‘00010001’
    - **‘87’** *‘02’* ‘0101’
    - **‘88’** *‘02’* ‘0008’
  - **‘5F2E’** *‘823162’* ‘… 12 642 байтов биометрических данных …’

A.4 ШАБЛОНЫ ОТОБРАЖАЕМОГО ИЗОБРАЖЕНИЯ В ФАЙЛАХ EF.DG5 – EF.DG7

Примечание. Один EF для каждой DG.

Пример. Шаблон изображения с длиной данных отображаемого изображения 2000 байтов. Длина шаблона составляет 2008 байтов (‘07D8’).

‘65’ *‘8207D8’*
‘02’ *‘01’* 1
‘5F40’ *‘8207D0’* ‘….2000 байтов данных изображения …’

A.5 ДОПОЛНИТЕЛЬНЫЕ ЛИЧНЫЕ ДАННЫЕ В ФАЙЛЕ EF.DG11

В нижеуказанном примере показаны следующие личные данные: полное имя (John J. Smith), место рождения (Anytown, MN), постоянный адрес (123 Maple Rd, Anytown, MN), номер телефона 1-612-555-1212 и профессия (Travel Agent). Длина шаблона 99 байтов (*‘63’*).

‘6B’ *‘63’*
‘5C’ *‘0A’* **‘5F0E’ ‘5F11’ ‘5F42’ ‘5F12’ ‘5F13’**
‘5F0E’ *‘0D’* SMITH<<JOHN<J
‘5F11’ *‘0A’* ANYTOWN<MN
‘5F42’ *‘17’* 123 MAPLE RD<ANYTOWN<MN
‘5F12’ *‘0E’* 16125551212
‘5F13’ *‘0C’* TRAVEL<AGENT

A.6 УВЕДОМЛЯЕМОЕ(ЫЕ) ЛИЦО(А) В ФАЙЛЕ EF.DG16

Пример с двумя записями: Charles R. Smith of Anytown, MN и Mary J. Brown of Ocean Breeze, CA. Длина шаблона составляет 162 байта (‘A2’).

‘70’ *‘81A2’*
‘02’ *‘01’* 2
‘A1’ ‘4C’
‘5F50’ *‘08’* 20020101
‘5F51’ *‘10’* SMITH<<CHARLES<R
‘5F52’ *‘0B’* 19525551212
‘5F53’ *‘1D’* 123 MAPLE RD<ANYTOWN<MN<55100
‘A2’ ‘4F’
‘5F50’ *‘08’* 20020315
‘5F51’ *‘0D’* BROWN<<MARY<J
‘5F52’ *‘0B’* 14155551212
‘5F53’ *‘23’* 49 REDWOOD LN<OCEAN BREEZE<CA<94000

— — — — — — — —

Добавление B к части 10

БЕСКОНТАКТНАЯ ИС В ЭЛЕКТРОННОМ МСП (ИНФОРМАЦИОННОЕ)

B.1 РАЗМЕР АНТЕННЫ И КЛАСС ЭЛЕКТРОННОГО МСПД

Размер антенны определяется по усмотрению государства выдачи. За исключением размера антенны, электронные МСПД с LDS1 и LDS2 ОТВЕЧАЮТ требованиям всех испытаний, указанных в стандарте [ИСО/МЭК 18745-2], с применением спецификаций класса 1.

РЕКОМЕНДУЕТСЯ, чтобы электронные МСПД также соответствовали спецификациям класса 1.

Не существует обязательного положения для ИС, которая МОЖЕТ быть расположена в произвольном месте. Место расположения бесконтактной антенны определяется по усмотрению государства выдачи при условии, что она расположена в одном из следующих мест:

страница данных:	ИС и антенна размещены внутри структуры страницы данных, составляющей внутреннюю страницу;
центр книжки:	ИС и ее антенна размещены между центральными страницами книжки;
обложка:	размещение внутри структуры или конструкции обложки;
отдельная вшитая страница:	ИС и ее антенна встроены в отдельную страницу, которая МОЖЕТ иметь форму пластиковой карты размера ID3, вшитой в книжку во время ее изготовления;
задняя часть обложки:	размещение внутри структуры или конструкции задней части обложки.

B.2 ЗАГРУЗКА И ОПРОС

Электронный МСПД, помещенный в переменное магнитное поле напряженностью 1,5 А/м, измеренной в соответствии со стандартом [ИСО/МЭК 18745-2], отвечает на любую соответствующую его типу команду REQ/WUP после воздействия немодулированного переменного магнитного поля в течение 10 мс. РЕКОМЕНДУЕТСЯ, чтобы он мог отвечать на любую соответствующую его типу команду REQ/WUP после воздействия немодулированного переменного магнитного поля в течение 5 мс.

B.3 АНТИКОНФЛИКТНОСТЬ И ТИП

Электронный МСПД может заявлять о соответствии типу A или типу B, как определено в стандарте [ИСО/МЭК 14443-2]. Он ИЗМЕНЯЕТ свой тип только в случае перезагрузки системой проверки, связанной с электронным МСПД.

B.4 ОБЯЗАТЕЛЬНЫЕ СКОРОСТИ ПЕРЕДАЧИ ДАННЫХ

Электронный МСПД в обязательном порядке обеспечивает как минимум следующие скорости передачи данных, как определено в стандарте [ИСО/МЭК 14443-2]: 106 кбит/с и 424 кбит/с в обоих направлениях между электронным МСПД и системой проверки, связанной с электронным МСПД.

Скорость передачи данных, равная 212 кбит/с, а также все скорости передачи данных от 848 кбит/с до 6,78 Мбит/с в обоих направлениях и от 10,17 Мбит/с до 27,12 Мбит/с в направлении от связанной с электронным МСПД системы проверки к электронному МСПД, как определено в стандарте [ИСО/МЭК 14443-2], являются факультативными.

B.5 ЭЛЕКТРОМАГНИТНЫЕ ПОМЕХИ (EMD)

Поддержка EMD не является обязательной.

Примечание. Функция EMD повышает устойчивость бесконтактной связи между электронным МСПД и связанной с электронным МСПД системой проверки к электромагнитным помехам, вызываемым электронным МСПД. Потребление рабочего тока электронным МСПД в процессе выполнения команды может вызвать эффект произвольной модуляции магнитного поля нагрузкой (которая может не быть чисто омической). В некоторых случаях связанная с электронным МСПД система проверки может неправильно интерпретировать EMD как данные, переданные электронным МСПД, и это может отрицательно сказаться на нормальном приеме ответа электронного МСПД.

B.6 ПОДДЕРЖКА ОБМЕНА ДОПОЛНИТЕЛЬНЫМИ ПАРАМЕТРАМИ (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

Электронный МСПД МОЖЕТ поддерживать обмен дополнительными параметрами, как определено в стандарте [ИСО/МЭК 14443-4], с тем чтобы согласовать скорости передачи данных свыше 106 кбит/с. Он МОЖЕТ также использовать те же дополнительные параметры для согласования кадров с возможностью коррекции ошибок, как определено в стандарте [ИСО/МЭК 14443-4].

B.7 ЭКРАНИРОВАНИЕ

РЕКОМЕНДУЕТСЯ не экранировать никакие страницы электронного МСПД.

B.8 УНИКАЛЬНЫЙ ИДЕНТИФИКАТОР (UID) И ПСЕВДОУНИКАЛЬНЫЙ ИДЕНТИФИКАТОР PICC (PUPI)(РЕКОМЕНДУЕМЫЕ)

Электронный МСПД МОЖЕТ предоставлять произвольный или фиксированный идентификатор UID/PUPI, как определено в стандарте [ИСО/МЭК 14443-3].

РЕКОМЕНДУЕТСЯ использовать произвольный идентификатор UID/PUPI в целях повышения уровня конфиденциальности личной информации владельца и уменьшения возможности отслеживания.

B.9 ДИАПАЗОН РЕЗОНАНСНЫХ ЧАСТОТ (РЕКОМЕНДУЕМЫЙ)

Требование относительно резонансной частоты для электронных МСПД отсутствует, поэтому заявители МОГУТ ограничить используемую ими резонансную частоту определенным диапазоном в целях повышения уровня интероперабельности.

B.10 РАЗМЕРЫ КАДРА (РЕКОМЕНДУЕМЫЕ)

Электронный МСПД МОЖЕТ поддерживать размеры кадра до 4 кбайт в соответствии со стандартом [ИСО/МЭК 14443]. Однако РЕКОМЕНДУЕТСЯ поддерживать размеры кадра по меньшей мере в 1 кбайт. Если поддерживаемый размер кадра превышает 1 кбайт, то РЕКОМЕНДУЕТСЯ использовать кадры с возможностью исправления ошибок, как определено в стандарте [ИСО/МЭК 14443-4].

Примечание. За счет большего размера кадра существенно сокращается общее время обработки приложения электронного МСПД.

B.11 ВРЕМЯ ОЖИДАНИЯ КАДРА, ЦЕЛОЕ ЧИСЛО (FWI) И ЗАПРОС В КОНТРОЛИРУЮЩЕМ БЛОКЕ НА ПРОДЛЕНИЕ ВРЕМЕНИ ОЖИДАНИЯ КАДРА [S(WTX)] (РЕКОМЕНДУЕМЫЕ)

РЕКОМЕНДУЕТСЯ в целях повышения эффективности устанавливать для электронного МСПД значение FWI меньшее или равное 11. РЕКОМЕНДУЕТСЯ использовать команды S(WTX) для продления времени ожидания кадра для каждой конкретной команды, требующей дополнительного времени, путем использования команд S(WTX) с коэффициентом WTXM, не превышающим 10.

В том случае, если электронный МСПД отправляет несколько запросов S(WTX), РЕКОМЕНДУЕТСЯ, чтобы общее время обработки текущего информационного блока не превышало 5 с.

Примечание. Уменьшение значений FWI, как РЕКОМЕНДУЕТСЯ в настоящем документе, существенно снижает потери времени из-за ошибок передачи, при этом запросы S(WTX) представляют собой оптимальный способ обеспечения дополнительного времени в случае необходимости.

— — — — — — — —

Добавление C к части 10

СИСТЕМЫ ПРОВЕРКИ (ИНФОРМАЦИОННОЕ)

C.1 РАБОЧИЙ ОБЪЕМ И ПОЛОЖЕНИЯ ДЛЯ ИСПЫТАНИЙ

Система проверки, связанная с электронным МСПД, имеет рабочий объем, соответствующий одному из типов систем проверки, определенных в стандарте [ИСО/МЭК 18745-2]. Рабочий объем – это объем, в котором выполняются все требования настоящего технического описания.

Примечание. Положения для испытаний более подробно представлены в [ИСО/МЭК 18745-2] для каждого типа систем проверки относительно 0 мм от поверхности (устройства) системы проверки, связанной с электронным МСПД.

C.2 КОНКРЕТНЫЕ ТРЕБОВАНИЯ К ФОРМЕ ВОЛНЫ И РАДИОЧАСТОТЕ

Формы волны переменного магнитного поля, используемого для связи, полностью соответствуют стандарту [ИСО/МЭК 14443-2]. В целом исключения из базового стандарта или отклонения от него отсутствуют, за исключением напряженности поля.

Для связанных с электронными МСПД систем проверки типов 1, 2 и 3 РЕКОМЕНДУЕТСЯ, чтобы напряженность поля составляла как минимум 2 А/м во всех положениях для класса 1. Для связанных с электронными МСПД систем проверок типа M напряженность поля составляет как минимум 1,5 А/м во всех положениях для класса 1.

Примечание. Может быть желательно, чтобы электронные МСПД также осуществляли связь с другими бесконтактными системами проверки и мобильными устройствами, например смартфонами с модулем NFC, использующими 1,5 А/м.

C.3 ПОСЛЕДОВАТЕЛЬНОСТИ ОПРОСА И ВРЕМЯ ОПРЕДЕЛЕНИЯ ЭЛЕКТРОННОГО МСПД

Последовательность опроса связанной с электронным МСПД системы проверки обеспечивает 10 мс немодулированной несущей частоты перед любыми командами REQA/WUPA или REQB/WUPB.

В целях быстрого определения и обработки система проверки электронного МСПД:

- проводит опрос для типа A и типа B с одинаковой повторяемостью запросов для обоих типов;
- для систем проверки типов 1, 2 и 3 следует производить один перезапуск посредством радиочастотного сигнала между любыми командами REQ/WUP одного типа;

- гарантирует как минимум одну команду опроса как для типа A, так и для типа B в течение 150 мс для электронного МСПД, присутствующего в минимальном обязательном рабочем объеме согласно стандарту [ИСО/МЭК 18745-2] в любом положении.

Система проверки электронного МСПД МОЖЕТ проводить опрос на предмет наличия бесконтактных объектов с любым другим типом модуляции на несущей частоте 13,56 МГц при условии соблюдения всех вышеприведенных требований.

Примечание. Для определения всех электронных МСПД в поле требуется немодулированная несущая частота, действующая в течение 10 мс и основанная на прежних спецификациях.

С.4 ОБЯЗАТЕЛЬНЫЕ СКОРОСТИ ПЕРЕДАЧИ ДАННЫХ

Связанная с электронным МСПД система проверки в обязательном порядке обеспечивает следующие значения скорости передачи данных: 106 кбит/с и 424 кбит/с от электронного МСПД к системе проверки, связанной с электронным МСПД, и в обратном направлении.

Скорость передачи данных, равная 212 кбит/с, а также все скорости передачи данных от 848 кбит/с до 6,78 Мбит/с в обоих направлениях и от 10,17 Мбит/с до 27,12 Мбит/с в направлении от связанной с электронным МСПД системы проверки к электронному МСПД, как определено в стандарте [ИСО/МЭК 14443-2], являются факультативными.

С.5 ЭЛЕКТРОМАГНИТНЫЕ ПОМЕХИ (EMD)

Поддержка EMD не является обязательной.

Примечание. Функция EMD повышает устойчивость бесконтактной связи между электронным МСПД и связанной с электронным МСПД системой проверки к электромагнитным помехам, вызываемым электронным МСПД. Потребление рабочего тока электронным МСПД в процессе выполнения команды может вызвать эффект произвольной модуляции магнитного поля нагрузкой (которая может не быть чисто омической). В некоторых случаях связанная с электронным МСПД система проверки может неправильно интерпретировать EMD как данные, переданные электронным МСПД, и это может отрицательно сказаться на нормальном приеме ответа электронного МСПД.

С.6 ПОДДЕРЖИВАЕМЫЕ КЛАССЫ АНТЕНН

Связанная с электронным МСПД система проверки типа 1 и типа 2 поддерживает как минимум электронные МСПД класса 1 в рабочем объеме.

В стандарте ИСО/МЭК 14443 класс 2 и класс 3 являются обязательными, но для системы проверки электронных МСПД – факультативными.

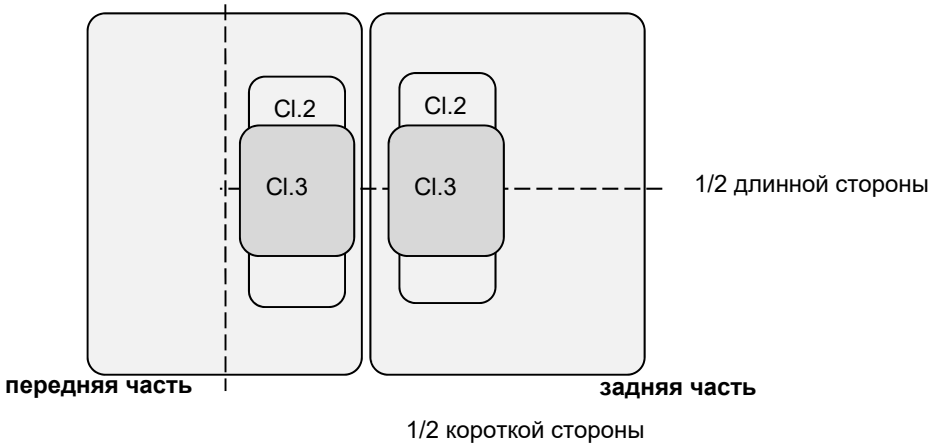

Рис. C-1. Обязательные положения в каждой поверхности ID-3, в которых антенна класса 2 и класса 3 считывается связанной с электронными МСПД системой проверки типа 1 и 2

C.7 РАЗМЕРЫ КАДРА И ИСПРАВЛЕНИЕ ОШИБОК (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

Связанная с электронным МСПД система проверки факультативно МОЖЕТ поддерживать все размеры кадра до 4 Кбайтов, как определено в стандарте [ИСО/МЭК 14443-3]. РЕКОМЕНДУЕТСЯ использовать кадры с возможностью исправления ошибок, как определено в стандарте [ИСО/МЭК 14443-3], для всех поддерживаемых размеров кадра свыше 1 Кбайта.

Примечание. Для связанных с электронными МСПД систем проверки типа M размеры кадра свыше 256 байтов в настоящее время не предусмотрены.

C.8 ПОДДЕРЖКА ДОПОЛНИТЕЛЬНЫХ КЛАССОВ (ФАКУЛЬТАТИВНАЯ ИНФОРМАЦИЯ)

Связанные с электронными МСПД системы проверки всех типов МОГУТ дополнительно поддерживать класс 4, класс 5 и класс 6, с тем чтобы быть интероперабельными, например, с мобильными устройствами, которые обеспечивают более слабую связь с катушкой антенны связанной с электронным МСПД системы проверки.

C.9 РАБОЧАЯ ТЕМПЕРАТУРА (РЕКОМЕНДУЕМАЯ)

РЕКОМЕНДУЕТСЯ, чтобы связанная с электронным МСПД система проверки работала при температурах от -10 до 50° по Цельсию.

C.10 ПОДДЕРЖКА НЕСКОЛЬКИХ ЭЛЕКТРОННЫХ МСПД И ДРУГИХ КАРТ ЛИБО ОБЪЕКТОВ ИЛИ НЕСКОЛЬКИХ ВЕДУЩИХ УСТРОЙСТВ (РЕКОМЕНДУЕМАЯ ИНФОРМАЦИЯ)

Настоятельно РЕКОМЕНДУЕТСЯ разрабатывать связанную с электронным МСПД систему проверки с возможностью обработки более одного электронного МСПД или одного электронного МСПД и любой другой карты или объекта, соответствующего стандарту [ИСО/МЭК 14443].

Среди прочих, может применяться одно из следующих правил или их сочетание:

- применение полных алгоритмов антиконфликтности, определенных в стандарте [ИСО/МЭК 14443-3];
- проверка наличия поддержки стандарта [ИСО/МЭК 14443-4] и отклонение всех карт, не поддерживающих его;
- проверка наличия приложения электронного МСПД;
- использование идентификатора карточки (CID) и адреса узла (NAD).

Примечание. NAD также может использоваться для мобильных устройств с несколькими ведущими устройствами.

С.11 РАЗМЕРЫ КАДРА (РЕКОМЕНДУЕМЫЕ)

Связанная с электронным МСПД система проверки МОЖЕТ поддерживать размеры кадра до 4 Кбайтов в соответствии со стандартом [ИСО/МЭК 14443-3]. Однако РЕКОМЕНДУЕТСЯ поддерживать размеры кадра по меньшей мере в 1 Кбайт. Если поддерживаются размеры кадра в 1 Кбайт и выше, то РЕКОМЕНДУЕТСЯ использовать кадры с возможностью исправления ошибок, как определено в стандарте [ИСО/МЭК 14443-4].

РЕКОМЕНДУЕТСЯ каким-либо образом разбивать полезные данные на уровне приложения на минимальное количество кадров с эффективной длиной, равной максимальному поддерживаемому размеру кадра, за исключением последнего кадра.

С.12 ВОССТАНОВЛЕНИЕ ПОСЛЕ ОШИБОК (РЕКОМЕНДУЕМАЯ ИНФОРМАЦИЯ)

После ошибки передачи или неполучения ответа от электронного МСПД рекомендуется, чтобы связанная с электронным МСПД система проверки отправила второй R-блок, содержащий отрицательные подтверждения (NAK), в соответствии с правилом 4 стандарта [ИСО/МЭК 14443-4], касающимся системы проверки.

С.13 МЕХАНИЗМ ВЫЯВЛЕНИЯ ОШИБОК И ВОССТАНОВЛЕНИЯ ПОСЛЕ НИХ (РЕКОМЕНДУЕМЫЙ)

При использовании факультативных скоростей передачи данных, а также факультативных размеров кадра свыше 256 байтов в том случае, если число ошибок передачи превышает обычное, РЕКОМЕНДУЕТСЯ снизить скорость передачи данных и эффективный размер кадра.

— — — — — — —

Добавление D к части 10

ВЕРСИЯ V0 ОБЪЕКТА ЗАЩИТЫ ДОКУМЕНТА EF.SOD ДЛЯ LDS V1.7 (ПРЕДЫДУЩАЯ ВЕРСИЯ) (ИНФОРМАЦИОННОЕ)

Объект защиты документа V0 для LDS версии 1.7 не содержит информацию о версии LDS и Unicode:

```
LDSSecurityObject ::= SEQUENCE {
    version LDSSecurityObjectVersion,
    hashAlgorithm DigestAlgorithmIdentifier,
    dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
    DataGroupHash}
```

D.1 ТИП ПОДПИСЫВАЕМЫХ ДАННЫХ ДЛЯ SO_D ВЕРСИИ V0

Объект защиты документа реализуется как тип подписываемых данных, указанный в [RFC 3369]. Все объекты защиты ДОЛЖНЫ представляться в формате, определяемом особыми правилами кодирования (DER), для сохранения целостности содержащихся в них подписей.

Примечание 1. m *ОБЯЗАТЕЛЬНОЕ – поле ДОЛЖНО присутствовать.*

Примечание 2. x *не использовать – поле НЕ ДОЛЖНО заполняться.*

Примечание 3. o *факультативное – поле МОЖЕТ присутствовать.*

Примечание 4. c *выбор – содержание поля выбирается из альтернатив.*

Таблица D-1. Тип подписываемых данных для SO_D версии V0

Значение		Замечания
Подписываемые данные		
Версия	m	Значение = v3
Алгоритмы представления в краткой форме	m	
Информация об инкапсулированном содержании	m	
Тип электронного содержания	m	id-icao – mrtd – security – ldsSecurityObject
Электронное содержание	m	Закодированное содержание ldsSecurityObject
Сертификаты	o	Государства могут решить включать сертификат лица, подписывающего документы (C_{DS}), который может использоваться для верификации подписи в поле информации о подписавшемся
Crl	x	Государствам рекомендуется не использовать это поле
Информация о подписавшемся	m	Государствам рекомендуется предоставлять в этом поле только одну единицу информации
Информация о подписавшемся	m	
Версия	m	Значение этого поля диктуется полем sid. См. правила, касающиеся этого поля, в RFC 3369, часть 12 документа Doc 9303
Sid	m	
Выдающее лицо и серийный номер	c	Государствам рекомендуется поддерживать это поле над идентификатором ключа субъекта
Идентификатор ключа субъекта	c	
Алгоритм представления в краткой форме	m	Алгоритмный идентификатор алгоритма, используемого для выдачи хэш-значения над инкапсулированным содержанием и подписанными атрибутами
Подписанные атрибуты	m	Производящие государства могут пожелать включать дополнительные атрибуты для внесения в подпись, однако они должны обрабатываться принимающими государствами только для верификации значения подписи
Алгоритм подписи	m	Алгоритмный идентификатор алгоритма, используемого для выдачи значения подписи и любых связанных с ней параметров
Подпись	m	Результат процесса генерации подписи

Значение		Замечания
Неподписанные атрибуты	o	Государства-изготовители могут принять решение об использовании этого поля, однако это не рекомендуется, поэтому принимающие государства могут игнорировать их.

D.2 ОБЪЕКТ ЗАЩИТЫ ДОКУМЕНТА LDS ПРОФИЛЯ ASN.1 ДЛЯ SO_D ВЕРСИИ V0

```
LDSSecurityObjectV0 {joint-iso-itu-t (2) international(23) icao(136) mrtd(1)
security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

-- Imports from RFC 3280 [PROFILE],
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) };

-- Constants

ub-DataGroups INTEGER ::= 16

-- Object Identifiers
id-icao   OBJECT IDENTIFIER::={joint-iso-itu-t(2) international(23) icao(136)}
id-icao-mrtd  OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security     OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-mrtd-security-ldsSecurityObject OBJECT  IDENTIFIER  ::=  {id-icao-mrtd-
security 1}

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {v0(0)}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
   version LDSSecurityObjectVersion,
   hashAlgorithm DigestAlgorithmIdentifier,
   dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
   DataGroupHash }

DataGroupHash ::= SEQUENCE {
   dataGroupNumber         DataGroupNumber,
   dataGroupHashValue      OCTET STRING }
DataGroupNumber ::= INTEGER {
```

```
        dataGroup1              (1),
        dataGroup2              (2),
        dataGroup3              (3),
        dataGroup4              (4),
        dataGroup5              (5),
        dataGroup6              (6),
        dataGroup7              (7),
        dataGroup8              (8),
        dataGroup9              (9),
        dataGroup10            (10),
        dataGroup11            (11),
        dataGroup12            (12),
        dataGroup13            (13),
        dataGroup14            (14),
        dataGroup15            (15),
        dataGroup16            (16)}
    END
```

Примечание 1. Поле `dataGroupValue` *содержит вычисленное хэш-значение над полным содержанием файла группы данных EF, определяемого полем* `dataGroupNumber`.

Примечание 2. В поле `DigestAlgorithmIdentifiers` ***НЕОБХОДИМО*** *опустить параметры "*`NULL`*", в то время как поле* `SignatureAlgorithmIdentifier` *(как указано в RFC 3447) ДОЛЖНО включать* `NULL` *в качестве этого параметра в случае отсутствия параметров, даже если используются алгоритмы SHA2 в соответствии с RFC 5754. Любые варианты реализации ДОЛЖНЫ принимать к обработке поле* `DigestAlgorithmIdentifiers` *в обоих случаях: при отсутствии параметров или с параметрами* `NULL`.

— — — — — — — —

Добавление E к части 10

СВОДНАЯ ИНФОРМАЦИЯ О СТРУКТУРАХ ФАЙЛОВ (ИНФОРМАЦИОННОЕ)

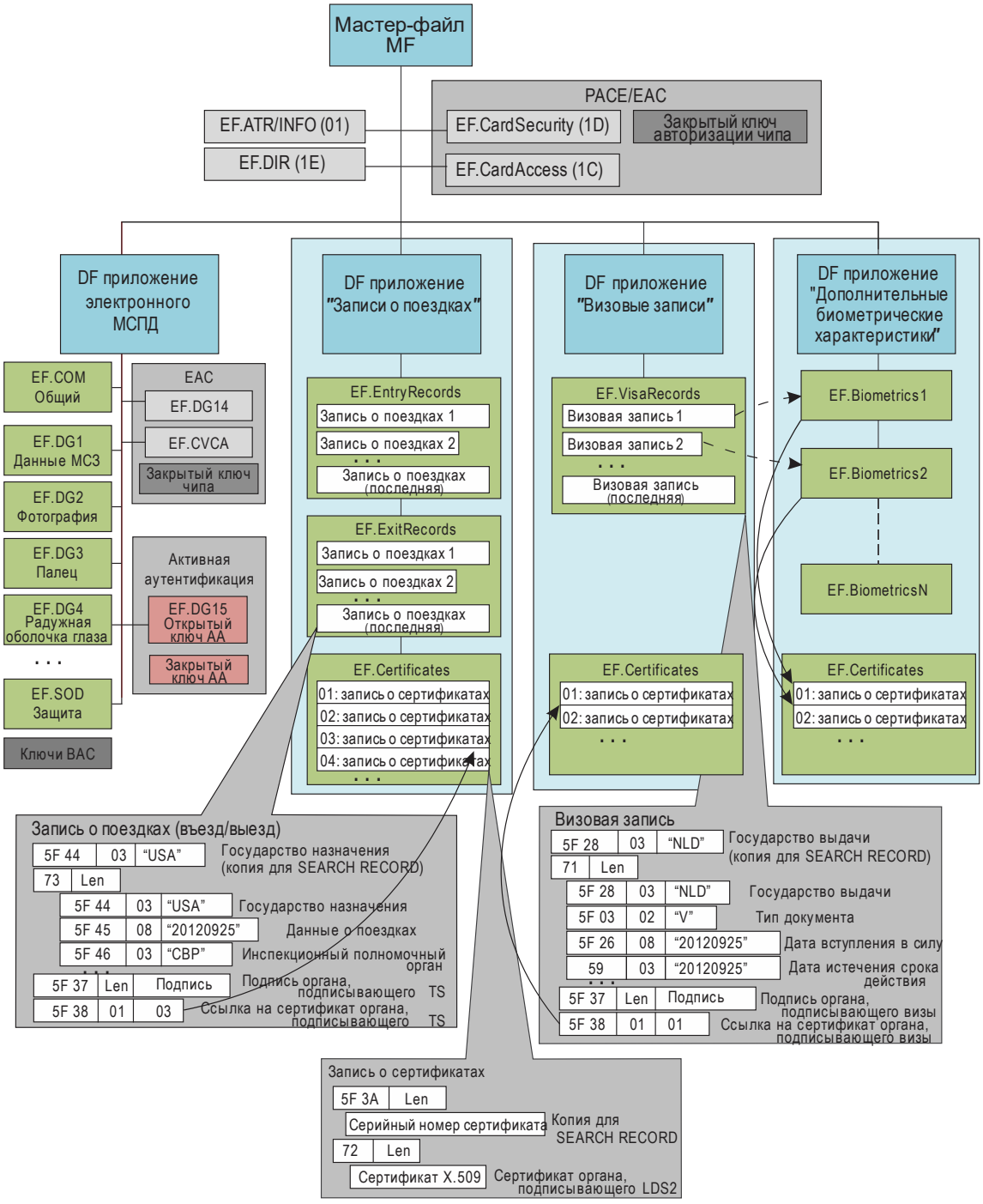

Рис. E-1. Сводная информация о структурах файлов

Добавление F к части 10

СВОДНАЯ ИНФОРМАЦИЯ ОБ АВТОРИЗАЦИИ LDS (ИНФОРМАЦИОННОЕ)

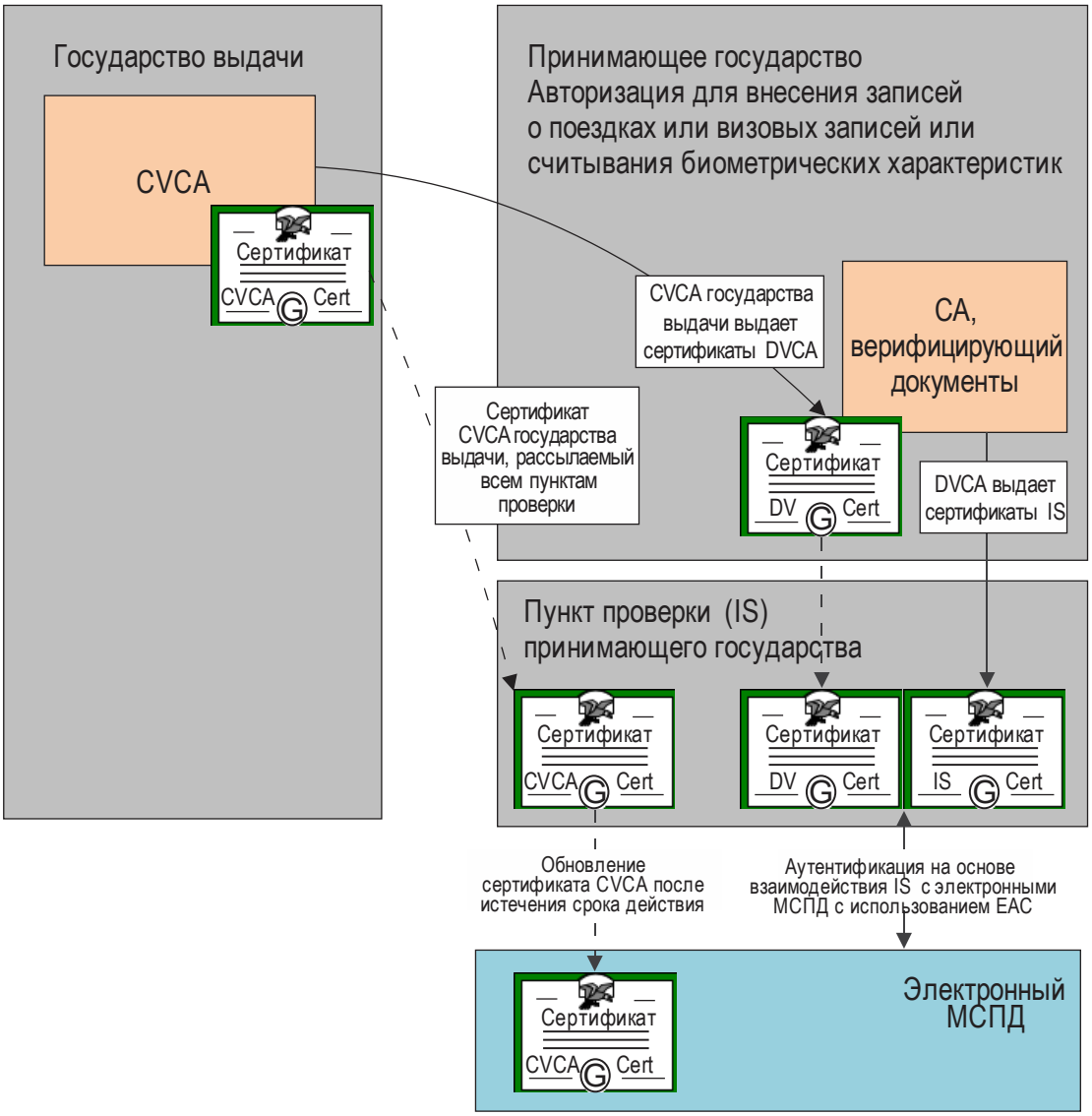

Рис. F-1. Сводная информация об авторизации LDS

Добавление G к части 10

СВОДНАЯ ИНФОРМАЦИЯ О ЦИФРОВОЙ ПОДПИСИ LDS (ИНФОРМАЦИОННОЕ)

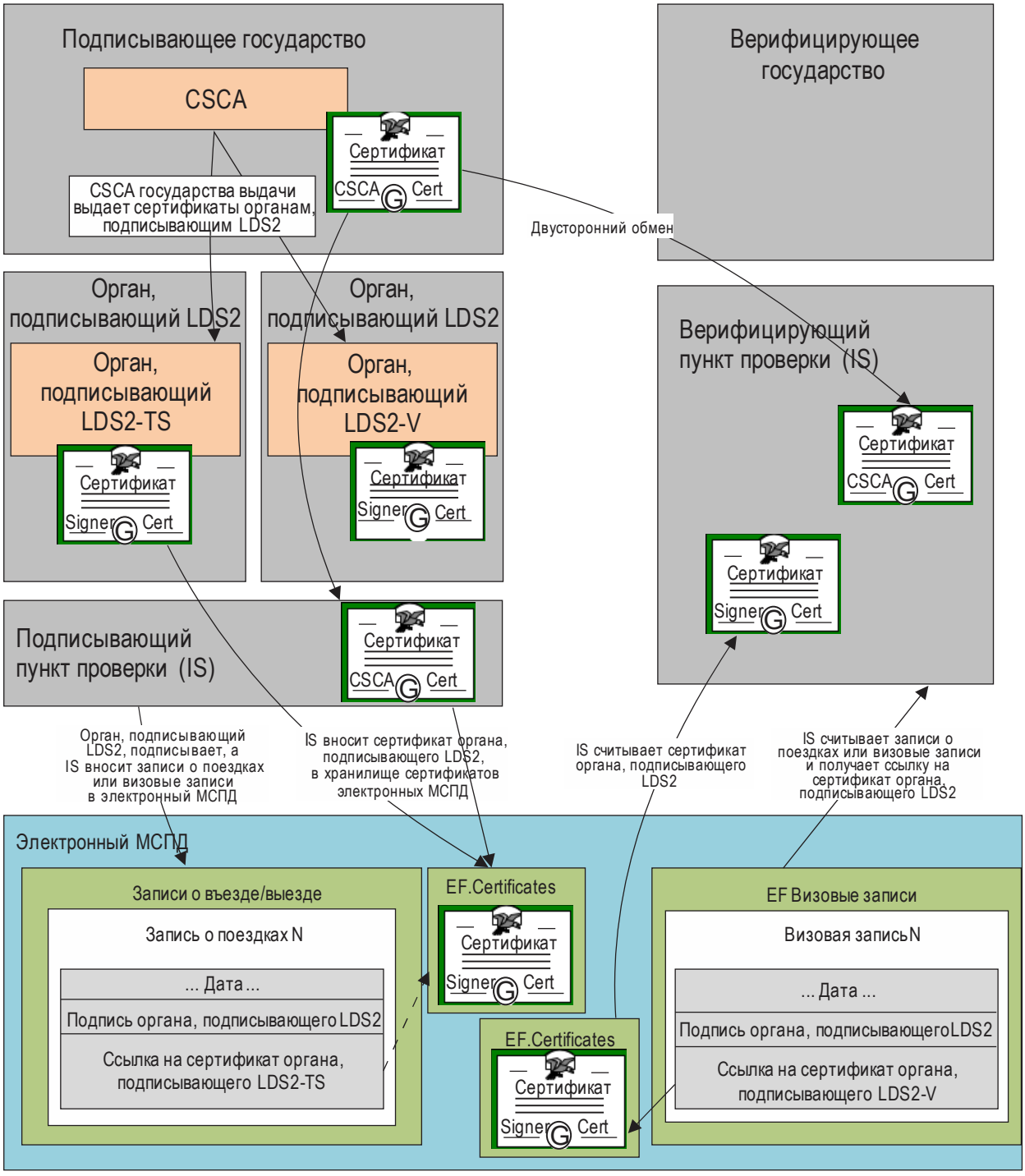

Рис. G-1. Цифровая подпись LDS

Добавление H к части 10

ПРИМЕР СЧИТЫВАНИЯ ЗАПИСЕЙ О ПОЕЗДКАХ (ИНФОРМАЦИОННОЕ)

H.1 КОМАНДА FMM НА ИЗВЛЕЧЕНИЕ ИНФОРМАЦИИ О КОЛИЧЕСТВЕ ЗАПИСЕЙ О ВЪЕЗДЕ

CLA	INS	P1	P2	Lc	Дата	Le
‘80’	‘5E’	‘01’	‘04’	‘04’	‘51 02 01 01’	‘00’

CLA: проприетарный класс / безопасный обмен сообщениями не обеспечивается
INS: FMM
P1: ‘01’ — идентификатор EF в поле данных команды
P2: ‘04’ — возврат существующего количества записей в EF записей
Lc: ‘04’
Дата: DO’51, содержащий идентификатор EF ‘0101’ записей о въезде
Le: ‘00’ (короткое поле Le)

Ответ: DO "Управление файлами и памятью", представляющий количество записей в файле EF.

Дата	SW1-SW2
‘7F78 03’ ‘83 01 FD’	‘90 00’

DO в данных ответа содержит последний номер записи, который может быть использован в следующей команде READ RECORD (P1).

Например, последний номер записи ‘00’ означает, что в этом файле записи отсутствуют, а ответ ‘FD’ означает, что количество записей составляет 253 (максимальное количество записей составляет 254).

H.2 КОМАНДА READ RECORD НА ИЗВЛЕЧЕНИЕ ПОСЛЕДНЕЙ ЗАПИСИ О ПОЕЗДКАХ ИЗ ИЗВЛЕЧЕННОГО СПИСКА

Команда, указанная ниже, может быть использована для извлечения одной записи посредством номера записи, возвращенного командой FMM:

CLA	INS	P1	P2	Le
‘00’	‘B2’	‘FD’	‘04’	‘00 00 00’

CLA: межотраслевой класс / безопасный обмен сообщениями не обеспечивается
INS: READ RECORD(S)
P1: номер записи из предыдущего ответа на команду
P2: номер записи в P1 / считывание записи P1
Le: ‘00 00 00’ (расширенное поле Le), считывание полной записи

Ответ: количество записей составляет 253 (‘FD’).

Дата	SW1-SW2
‘5F44’ ‘Len’ <Data> || ‘73’ ‘Len’ <Data> || ‘5F37’ ‘Len’ <Data> || ‘5F38’ ‘Len’ <Data>	‘90 00’

Н.3 КОМАНДА READ RECORD НА ИЗВЛЕЧЕНИЕ ПОСЛЕДНИХ ДВУХ ЗАПИСЕЙ О ПОЕЗДКАХ ИЗ ИЗВЛЕЧЕННОГО СПИСКА

Указанная ниже команда может быть использована для извлечения двух (или более) записей из списка, возвращенного командой FMM. Считывание нескольких записей при одном обмене APDU улучшает характеристики. Количество записей, которые можно извлечь посредством одной команды, можно определить на основе информации расширенной длины в файле EF.ATR/INFO и максимального размера записи о поездках.

CLA	INS	P1	P2	Le
‘00’	‘B2’	‘FC’	‘05’	‘00 00 00’

CLA: межотраслевой класс / безопасный обмен сообщениями не обеспечивается
INS: READ RECORD(S)
P1: уменьшенный номер записи из ответа FMM (253 - 1 = 252 = ‘FC’)
P2: номер записи в P1 / считать все записи с P1 до последней записи
Le: ‘00 00 00’ (расширенное Le), считывание полной записи.

Ответ: последние две записи 252 (‘FC’) и 253 (‘FD’) возвращены.

Дата	SW1-SW2
‘5F44’ ‘Len’ <Data> || ‘73’ ‘Len’ <Data> || ‘5F37’ ‘Len’ <Data> || ‘5F38’ ‘Len’ <Data> || ‘5F44’ ‘Len’ <Data> || ‘73’ ‘Len’ <Data> || ‘5F37’ ‘Len’ <Data> || ‘5F38’ ‘Len’ <Data>	‘90 00’

— — — — — — — —

Добавление I к части 10

ПРИМЕР ПОИСКА ЗАПИСЕЙ ПО ГОСУДАРСТВУ (ИНФОРМАЦИОННОЕ)

I.1 КОМАНДА SEARCH RECORD НА ПОИСК ЗАПИСИ(ЕЙ) О ПОЕЗДКАХ ПО ГОСУДАРСТВУ НАЗНАЧЕНИЯ

CLA	INS	P1	P2	Lc	Дата	Le
‘00’	‘A2’	‘00’	‘F8’	Var	‘7F 76’ ‘Len’ ‘51 01 01’ ‘A1 0B’ ‘80 01 00’ ‘B0 06’ ‘02 01 03’ ‘02 01 03’ ‘A3 07’ ‘B1 05’ ‘81 03’ xx xx xx	‘00’

CLA: межотраслевой класс / безопасный обмен сообщениями не обеспечивается
INS: SEARCH RECORD(S)
P1: номер записи= ‘00’
P2: поиск посредством различных EF
Lc: длина поля данных команды
Data: DO’7F76’ –DO обработки записей
DO’51’ – ссылка на файл DO (короткий идентификатор ‘01’ файла EF.EntryRecords)
DO’A1’ – шаблон конфигурации поиска
DO’80’ – параметр конфигурации поиска: ‘00’ (поиск всех записей)
DO’B0’ – шаблон окна поиска
DO’02’ – смещение: ‘03’
DO’02’ – количество байтов: ‘03’
DO’A3’ – шаблон строки поиска
DO’B1’ – строка поиска DO
DO’81’ – строка поиска (код страны): xx xx xx
Le: ‘00’ (короткое поле Le)

Ответ: DO’7F76’ –DO обработки записей
DO’51’ – короткий идентификатор ‘01’ EF.EntryRecords
Один или несколько DO’02’, содержащих подходящие номера записей

Дата	**SW1-SW2**
‘7F 76’ ‘Len’’ ‘51 01 01’ ‘02 01 03’ ‘02 01 04’	‘90 00’

— — — — — — — —

Добавление J к части 10

ПРИМЕР ВНЕСЕНИЯ ЗАПИСЕЙ О ПОЕЗДКАХ И СЕРТИФИКАТАХ (ИНФОРМАЦИОННОЕ)

J.1 КОМАНДА SEARCH RECORD НА ПОИСК ФАЙЛОВ EF.CERTIFICATES ПОСРЕДСТВОМ СЕРИЙНОГО НОМЕРА СЕРТИФИКАТА

IS проверяет наличие в файле EF.Certificates сертификата органа, подписывающего LDS2-TS, с требуемыми серийными номерами. Для поиска сертификатов можно использовать следующую команду:

CLA	INS	P1	P2	Lc	Дата	Le
'00'	'A2'	'00'	'F8'	Var	'7F 76' 'Len' '51 01 1A' 'A1 0B' '80 01 30' 'B0 06' '02 01 03' '02 01' {размер строки поиска} 'A3' 'Len' 'B1' 'Len' '81' 'Len' xx xx .. xx xx	'00'

CLA: межотраслевой класс / безопасный обмен сообщениями не обеспечивается
INS: SEARCH RECORD(S)
P1: номер записи = '00'
P2: поиск посредством нескольких EF
Lc: длина поля данных команды
Data: DO'7F76' –DO обработки записей
DO'51' – ссылка на файл DO (короткий идентификатор '1A' файла EF.Certificates)
DO'A1' – шаблон конфигурации поиска
DO'80' – параметр конфигурации поиска: '30' (останов, если запись найдена)
DO'B0' – шаблон окна поиска
DO'02' - смещение: '03'
DO'02' – количество байтов: размер строки поиска
DO'A3' – шаблон строки поиска
DO'B1' – DO строки поиска
DO'81' – конкатенация поиска кода страны и серийного номера сертификата: xx xx .. xx xx
Le: '00' (короткое поле Le)

Ответ: DO'7F76' – обработка записей DO
DO'51' – короткий идентификатор '1A' файла EF.Certificates
DO'02' – содержит подходящий номер записи

Data	SW1-SW2
‘7F 76 06’ ‘51 01 1A’ ‘02 01 01’	‘90 00’

или код предупреждения ‘62 82’, если никакая запись не соответствует критериям поиска:

SW1-SW2
‘62 82’

Если запись файла EF.Certificate отвечает критериям поиска, то IS может факультативно использовать возвращенный номер записи (‘01’) в команде READ RECORD для проверки того, является ли данный сертификат правильным. Если запись файла EF.Certificate не отвечает критериям поиска, то IS вносит этот сертификат в файл EF.Certificates посредством команды APPEND RECORD, информация о которой приводится в разделе J.2, и в конечном итоге делает входную запись посредством команды APPEND RECORD, информация о которой приводится в разделе J.3.

J.2 КОМАНДА APPEND RECORD НА ВНЕСЕНИЕ ЗАПИСИ О СЕРТИФИКАТЕ

IS записывает сертификат органа, подписывающего LDS2-TS, в файл EF.Certificates. Для записи сертификатов может быть использована следующая команда:

CLA	INS	P1	P2	Lc	Дата	Le
‘00’	‘E2’	‘00’	‘D0’	‘00’ XX XX	‘5F3A’ ‘Len’ {серийный номер сертификата} || ‘72’ ‘Len’ {сертификат X.509}”	Отсутствует

CLA: межотраслевой класс / безопасный обмен сообщениями не обеспечивается
INS: APPEND RECORD
P1: ‘00’ (любое другое значение не действительно)
P2: короткий идентификатор EF (= ‘1A’)
Lc: длина записи (увеличенное поле Lc)
Дата: дата записи

Ответ: код успешной операции или ошибки

SW1-SW2
‘90 00’

J.3 КОМАНДА APPEND RECORD НА ВНЕСЕНИЕ ЗАПИСИ О ПОЕЗДКАХ

IS генерирует запись о поездках, используя для этого ссылку на сертификат органа, подписывающего LDS2-TS, и вносит ее в файл EF.EntryRecords посредством следующей команды:

CLA	INS	P1	P2	Lc	Дата	Le
‘00’	‘E2’	‘00’	‘08’	‘00’ XX XX	‘5F44’ ‘Len’ {государство назначения} || ‘73’ ‘Len’ {запись о поездке, касающаяся въезда} || ‘5F37’ ‘Len’ {подпись} || ‘5F38’ ‘Len’ {ссылка на сертификат}	Отсутствует

CLA: межотраслевой класс / безопасный обмен сообщениями не обеспечивается
INS: APPEND RECORD
P1: ‘00’ (любое другое значение не действительно)
P2: короткий идентификатор EF (= ‘01’)
Lc: длина записи (увеличенное поле Lc)
Дата: дата записи

Ответ: код успешной операции или ошибки

SW1-SW2
‘90 00’

— КОНЕЦ —

ISBN 978-92-9265-533-4