Doc 9303

Машиносчитываемые проездные документы

Часть 1
Машиносчитываемые паспорта
Том 2
Спецификации на электронные паспорта со средствами биометрической идентификации

Утверждено Генеральным секретарем
и опубликовано с его санкции

Издание шестое — 2006

Международная организация гражданской авиации

Опубликовано Международной организацией гражданской авиации отдельными изданиями на русском, английском, арабском, испанском, китайском и французском языках. Всю корреспонденцию, за исключением заказов и подписки, следует направлять в адрес Генерального секретаря.

Заказы на данное издание направлять по одному из следующих нижеприведенных адресов, вместе с соответствующим денежным переводом в долл. США или в валюте страны, в которой размещается заказ. Во избежание задержек с доставкой заказчикам рекомендуется пользоваться кредитными карточками (MasterCard, Visa или American Express). Информация об оплате кредитными карточками и другими методами приводится в разделе "Как оформить заказ" *Каталога изданий и аудиовизуальных учебных средств ИКАО.*

International Civil Aviation Organization. Attention: Document Sales Unit, 999 University Street, Montreal, Quebec, Canada H3C 5H7
Telephone: +1 514-954-8022; Facsimile: +1 514-954-6769; Sitatex: YULCAYA; E-mail: sales@icao.int; World Wide Web: http://www.icao.int

Cameroon. KnowHow, 1, Rue de la Chambre de Commerce-Bonanjo, B.P. 4676, Douala / Telephone: +237 343 98 42; Facsimile: +237 343 89 25;
E-mail: knowhow_doc@yahoo.fr

China. Glory Master International Limited, Room 434B, Hongshen Trade Centre, 428 Dong Fang Road, Pudong, Shanghai 200120
Telephone: +86 137 0177 4638, Facsimile: +86 21 5888 1629; E-mail glorymaster@online.sh.cn

Egypt. ICAO Regional Director, Middle East Office, Egyptian Civil Aviation Complex, Cairo Airport Road, Heliopolis, Cairo 11776
Telephone: +20 2 267 4840; Facsimile: +20 2 267 4843; Sitatex: CAICAYA; E-mail: icaomid@cairo.icao.int

Germany. UNO-Verlag CmbH, August-Bebel-Allee 6, 53175 Bonn / Telephone: +49 0 228-94 90 2-0; Facsimile: +49 0 228-94 90 2-22;
E-mail: info@uno-verlag.de; World Wide Web: http://www.uno-verlag.de

India. Oxford Book and Stationery Co., 57, Medha Apartments, Mayur Vihar, Phase-1, New Delhi 110091
Telephone: +91 11 65659897; Facsimile: +91 11 22743532

India. Sterling Book House — SBH, 181, Dr. D. N. Road, Fort, Bombay 400001
Telephone: +91 22 2261 2521, 2265 9599; Facsimile: +91 22 2262 3551; E-mail: sbh@vsnl.com

India. The English Book Store, 17-L Connaught Circus, New Delhi 110001
Telephone: +91 11 2341-7936, 2341-7126; Facsimile: +91 11 2341-7731; E-mail: ebs@vsnl.com

Japan. Japan Civil Aviation Promotion Foundation, 15-12, 1-chome, Toranomon, Minato-Ku, Tokyo
Telephone: +81 3 3503-2686; Facsimile: +81 3 3503-2689

Kenya. ICAO Regional Director, Eastern and Southern African Office, United Nations Accommodation, P.O.Box 46294, Nairobi
Telephone: +254 20 7622 395; Facsimile: +254 20 7623 028; Sitatex: NBOCAYA; E-mail: icao@icao.unon.org

Mexico. Director Regional de la OACI, Oficina Norteamérica, Centroamérica y Caribe, Av. Presidente Masaryk No. 29, 3er. piso,
Col. Chapultepec Morales, C.P. 11570, México, D.F.
Teléfono: +52 55 52 50 32 11; Facsímile: +52 55 52 03 27 57; Correo-e: icao_nacc@mexico.icao.int

Nigeria. Landover Company, P.O. Box 3165, Ikeja, Lagos
Telephone: +234 1 4979780; Facsimile: +234 1 4979788; Sitatex: LOSLORK; E-mail: aviation@landovercompany.com

Peru. Director Regional de la OACI, Oficina Sudamérica, Av. Víctor Andrés Belaúnde No. 147, San Isidro, Lima (Centro Empresarial Real,
Via Principal No. 102, Edificio Real 4, Floor 4)
Teléfono: +51 1 611 8686; Facsímile: +51 1 611 8689; Correo-e: mail@lima.icao.int

Russian Federation. Aviaizdat, 48, Ivan Franco Street, Moscow 121351, Telephone: +7 095 417-0405; Facsímile: +7 095 417-0254

Senegal. Directeur régional de l'OACI, Bureau Afrique occidentale et centrale, Boîte postale 2356, Dakar
Téléphone: +221 839 9393; Fax: +221 823 6926; Sitatex: DKRCAYA; Courriel: icaodkr@icao.sn

Slovakia. Air Traffic Services of the Slovak Republic, Levoté prevádzkové služby Slovenskej Republiky, State Interprise, Letisco M.R. Štefánika,
823 07 Bratislava 21; Telephone: +421 2 4857 1111; Facsimile: +421 2 4857 2105; E-mail: sa.icao@lps.sk

South Africa. Avex Air Training (Pty) Ltd., Private Bag X102, Halfway House, 1685, Johannesburg
Telephone: +27 11 315-0003/4; Facsimile: +27 11 805-3649; E-mail: avex@iafrica.com

Spain. A.E.N.A. - Aeropuertos Españoles y Navegación Aérea, Calle Juan Ignacio Luca de Tena, 14, Planta Tercera, Despacho 3.11,
28027 Madrid; Teléfono: +34 91 321-3148; Facsímile: +34 91 321-3157; Correo e: sscc.ventasoaci@aena.es

Switzerland. Adeco-Editions van Diermen, Attn: Mr. Martin Richard Van Diermen, Chemin du Lacuez 41, CH-1807 Blonay
Telephone: +41 021 943 2673; Facsimile: +41 021 943 3605; E-mail: mvandiermen@adeco.org

Thailand. ICAO Regional Director, Asia and Pacific Office, P.O. Box 11, Samyaek Ladprao, Bangkok 10901
Telephone: +66 2 537 8189; Facsimile: +66 2 537 8199; Sitatex: BKKCAYA; E-mail: icao_apac@bangkok.icao.int

United Kingdom. Airplan Flight Equipment Ltd. (AFE), 1a Ringway Trading Estate, Shadowmoss Road, Manchester M22 5LH
Telephone: +44 161 499 0023; Facsimile: +44 161 499 0298; E-mail: enquiries@afeonline.com;
World Wide Web: http://www.afeonline.com

5/07

Каталог изданий и аудиовизуальных учебных средств ИКАО

Ежегодное издание с перечнем всех имеющихся в настоящее время публикаций и аудиовизуальных учебных средств. В дополнениях к Каталогу сообщается о новых публикациях, аудиовизуальных учебных средствах, поправках, дополнениях, повторных изданиях и т. п.

Рассылаются бесплатно по запросу, который следует направлять в Сектор продажи документов ИКАО.

Doc 9303

Машиносчитываемые проездные документы

Часть 1
Машиносчитываемые паспорта
Том 2
Спецификации на электронные паспорта со средствами биометрической идентификации

Утверждено Генеральным секретарем и опубликовано с его санкции

Издание шестое — 2006

Международная организация гражданской авиации

ПОПРАВКИ

Об издании поправок регулярно сообщается в *"Журнале ИКАО"* и в *дополнениях к Каталогу изданий и аудиовизуальных учебных средств ИКАО,* которыми рекомендуется пользоваться для справок. Ниже приводится форма для регистрации поправок.

РЕГИСТРАЦИЯ ПОПРАВОК И ИСПРАВЛЕНИЙ

ПОПРАВКИ		
№	Дата выпуска	Кем внесено

ИСПРАВЛЕНИЯ		
№	Дата выпуска	Кем внесено

ОГЛАВЛЕНИЕ

РАЗДЕЛ I

ВВЕДЕНИЕ

Спецификации, содержащиеся в настоящем томе части 1 документа Doc 9303, являются результатом нескольких лет работы, начатой в 1998 году, по систематическому изучению биометрических параметров и их потенциальных возможностей в повышении надежности подтверждения личности с использованием паспортов и других проездных документов и последующему определению технических спецификаций на включение средств биометрической идентификации в МСПД. Основная часть этой работы была выполнена Рабочей группой по новым технологиям (NTWG) Технической консультативной группы по машиносчитываемым проездным документам (TAG/MRTD).

Первым шагом было определение "верного биометрического параметра" для использования в проездных документах или вместе с проездными документами. Для этого сначала нужно было установить специфические *требования* в отношении выдачи и проверки проездных документов, а затем оценить совместимость каждого биометрического параметра с этими требованиями. Кратко говоря, установленными требованиями стали: совместимость с процессами выдачи и продления срока действия проездных документов; совместимость с требованиями к машинной верификации личности в процессах выдачи и проверки; избыточность; глобальное общественное восприятие биометрических параметров и процедуры их получения; требования к хранению данных и эффективность. По итогам оценки с учетом всех этих факторов, идентификация по *лицу* получила наивысший рейтинг совместимости, а идентификация по профилю *пальца* и идентификация по *радужной оболочке глаза* разделили второе место. В результате лицо было рекомендовано использовать в качестве основного биометрического параметра, обязательного для обеспечения глобальной интероперабельности систем проверки паспортов, а палец и радужную оболочку глаза – в качестве вспомогательных биометрических параметров, используемых по усмотрению государства выдачи паспорта.

Следующий шаг состоял в определении подходящего носителя для электронного хранения данных на документе. Такой носитель должен был обеспечивать достаточный объем памяти для хранения *изображений* лица и, возможно, других биометрических данных, поскольку концепция использования шаблонов была отклонена из-за отсутствия международных стандартов на шаблоны и устройства их считывания. Данная технология должна быть несобственнической, доступной для общественного пользования во всем мире, отвечающей интересам глобальной интероперабельности и применимой к документам в виде книжки, изготовленной из бумаги и материи. Удобство использования без необходимости помещать или вставлять документ в считывающее устройство было еще одним фактором. Бесконтактная интегральная схема (ИС) явилась тем техническим средством, которое отвечало всем этим требованиям, и после дополнительного изучения было решено, что из двух стандартных вариантов ИСО следует специфицировать тип схемы "с индуктивной связью через малый зазор" (ИСО/МЭК 14443).

Затем была специфицирована стандартная "логическая структура данных", предназначенная для программирования чипа, с тем чтобы чипы, запрограммированные в одной стране, можно было считывать в любой другой. Наконец, в связи с возможностью переписывания записанных на чипе данных потребовалась схема инфраструктуры открытых ключей (PKI) для придания уверенности считывателю чипа в том, что данные внесены уполномоченным лицом и

никоим образом не изменены. В этой связи экспертная группа в рамках NTWG разработала спецификации на специализированную PKI для применения при выдаче и проверке проездных документов.

В 2003 году Группа TAG/MRTD официально представила ИКАО рекомендацию, состоящую из четырех частей. Изображение лица в виде фотографии с высоким разрешением, хранящейся на бесконтактной ИС, отвечающей стандарту ИСО/МЭК 14443, должно быть всеобщим биометрическим стандартом. Отпечаток пальца и узор радужной оболочки глаза, хранящиеся в виде изображений, будут вспомогательными биометрическими параметрами. Биометрические параметры, дубликат данных МСЗ и целый ряд других данных должны храниться на ИС в соответствии с логической структурой данных и предохранятся от несанкционированного изменения путем использования специально приспособленной PKI. Эта рекомендация была принята и одобрена в качестве рабочего плана ИКАО.

Настоящий том формально закрепляет это решение, предоставляя детальные спецификации, приводимые в последующих разделах. В разделе II *"Применение средств биометрической идентификации*" определяются метод получения и использования биометрических данных и требования к бесконтактной ИС, используемой для хранения данных. В разделе III "*Логическая структура данных*" определяется метод хранения данных на ИС, а в разделе IV "*Инфраструктура открытых ключей*" описываются система и процедуры, используемые для защиты данных на ИС, и даются рекомендации в отношении базового контроля доступа с целью соответствующего ограничения доступа к данным.

РАЗДЕЛ II

ПРИМЕНЕНИЕ СРЕДСТВ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ И ЭЛЕКТРОННОГО ХРАНЕНИЯ ДАННЫХ В МАШИНОСЧИТЫВАЕМЫХ ПАСПОРТАХ

1. Сфера применения

1.1 В разделе II определяются технические спецификации в дополнение к спецификациям на базовый МСП, указанным в томе 1 части 1 документа Doc 9303, для использования государствами, решившими выдавать машиносчитываемый паспорт с электронной активацией (электронный паспорт), который может использоваться любым принимающим государством, имеющим соответствующее оборудование, для считывания с документа гораздо большего объема данных, касающихся самого МСП и его владельца. Они включают обязательные глобально интероперабельные биометрические данные, которые могут вводиться в системы распознавания черт лица и, факультативно, в системы распознавания отпечатков пальцев или радужной оболочки глаза. Этими спецификациями предусматривается хранение глобально интероперабельных биометрических данных в форме изображений высокой четкости на бесконтактной интегральной схеме (ИС) большой емкости, содержащей также дубликат закодированных данных МСЗ. Кроме того, спецификации допускают хранение ряда факультативных данных по усмотрению государства выдачи.

Примечание относительно Дополнения.

К настоящему стандартному документу Doc 9303 ИКАО будет периодически выпускаться "Дополнение к части 1 документа Doc 9303". Дополнение будет содержать информацию, предназначенную для пояснения, развития или конкретизации вопросов, касающихся стандартов на проездные документы, а также для исправления ошибок, выявленных в ходе внедрения. Предполагается, что содержащаяся в Дополнении информация будет расширять существующий инструктивный материал документа Doc 9303, а также технических докладов, выпущенных ИКАО. Дополнение будет выпускаться на постоянной и единообразной основе.

Спецификации документа Doc 9303 всегда следует рассматривать в сочетании с дополнительной информацией, указанной в последнем выпущенном Дополнении, которое будет размещаться на веб-сайте ИКАО http://www.icao.int/mrtd.

2. Электронный паспорт

2.1 *Соответствие спецификациям тома 1 части 1 документа Doc 9303.* МСП с электронной активацией (электронный паспорт) во всех отношениях соответствует спецификациям, содержащимся в томе 1 части 1 документа Doc 9303, а также спецификациям, указанным в настоящем томе.

2.2 *Срок действия электронного паспорта.* Срок действия электронного паспорта устанавливается по усмотрению государства выдачи; однако, принимая во внимание ограниченную износостойкость документов и изменение со временем внешнего вида владельца паспорта,

рекомендуется, чтобы срок действия составлял не более десяти лет. Государства могут рассмотреть вопрос об установлении более короткого срока с целью предоставления возможности для постепенной модернизации электронного паспорта по мере развития технологии.

2.3 В томе 2 части 1 документа Doc 9303 основное внимание уделяется биометрическим параметрам, относящимся к машиносчитываемым паспортам, и для простоты изложения употребляется термин "*электронные паспорта*", обозначающий такие глобально интероперабельные паспорта, обеспечивающие биометрическую идентификацию. МСП, не соответствующий спецификациям, указанным в настоящем томе, не может называться электронным паспортом и иметь логотип электронного паспорта.

3. Визуальная индикация того, что МСП является электронным паспортом

3.1 Все электронные паспорта содержат следующий символ (рис. II-1):

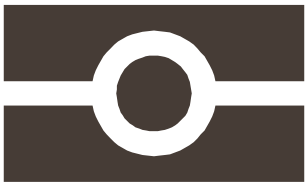


Рис. II-1

Электронный файл символа имеется на веб-сайте ИКАО. Символ может фигурировать только на МСП, содержащем бесконтактную микросхему с емкостью памяти не менее 32 кб, на которой хранятся как минимум закодированные в соответствии с логической структурой данных (раздел III настоящего тома) данные МСЗ, входящие в группу данных 1, и изображение лица, специфицированное в этом разделе в рамках группы данных 2, причем все внесенные данные защищаются цифровой подписью, специфицированной в разделе IV настоящего тома. Если паспорт не отвечает этим минимальным требованиям, он не может ни характеризоваться как электронный, ни содержать символ электронного паспорта. Данный символ располагается на лицевой обложке электронного паспорта (либо в верхней, либо в нижней части обложки). Вышеуказанный символ является позитивом, т. е. темная часть изображения печатается или изображается иным образом. Символ включается в изображение тиснением фольгой или в другое изображение на лицевой обложке. Кроме того, символ рекомендуется печатать в соответствующем цвете на странице, содержащей данные, в месте, не затрудняющем считывание данных. Государство выдачи может печатать символ также на внутренней странице или обложке электронного паспорта, содержащего бесконтактную ИС, или, по своему усмотрению, в любом другом месте паспорта.

3.2 На рис. II-2 указаны рекомендуемые размеры символа, располагаемого на обложке или на странице данных электронного паспорта.

Соответствующие размеры в дюймах: 9,0 мм (0,35 дюйма), 5,25 мм (0,21 дюйма), 3,75 мм (0,15 дюйма), 2,25 мм (0,09 дюйма), 0,75 мм (0,03 дюйма).

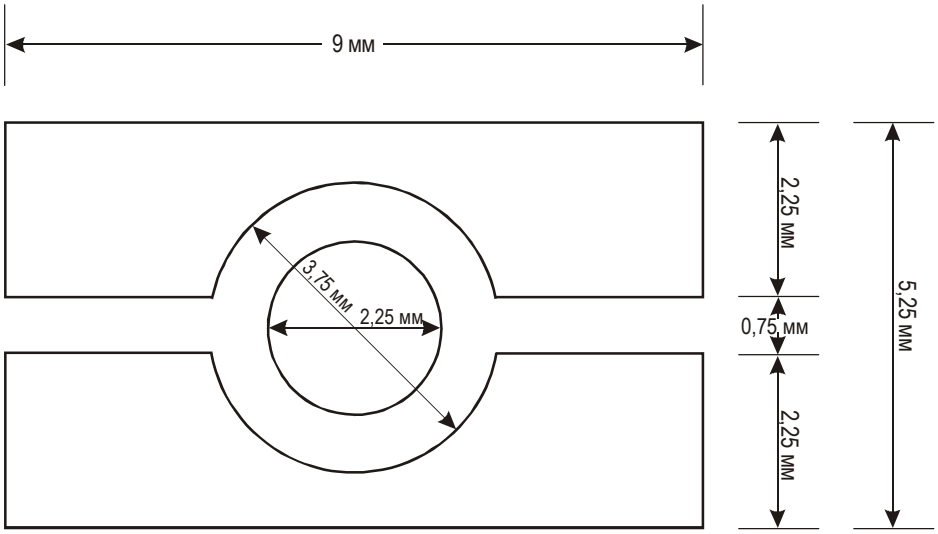


Рис. II-2

3.3 На электронных паспортах в форме карточки размера ID1 рекомендуется использовать пропорционально уменьшенный формат 4,2 мм × 7,2 мм (0,17 × 0,28 дюйма).

3.4 Размеры символа можно пропорционально изменять для использования, например, на фоновой композиции страниц или указательных знаках электронного паспорта.

3.5 *Предупреждение относительно бережного обращения с электронным паспортом.* В заметном месте паспортной книжки рекомендуется поместить уведомление, предупреждающее владельца электронного паспорта о необходимости бережного обращения с документом. Предлагается следующая формулировка:

"Настоящий паспорт содержит чувствительные электронные устройства. Для оптимального использования просьба не сгибать, не перфорировать и не подвергать паспорт воздействию крайних температур или избыточной влажности".

Кроме того, государство выдачи может обозначить часть страницы, на которой содержится ИС, и соответствующие части прилегающих страниц предостережением:

"Здесь печать не ставить"

4. Биометрическая идентификация

4.1 "Биометрическая идентификация" – общий термин, используемый для описания автоматизированных средств распознавания человека путем измерения отличительных физиологических или поведенческих черт.

4.2 "Биометрический шаблон" является автоматически закодированным представлением черты, созданной программно-реализованным алгоритмом; он позволяет производить сравнения (проверки на совпадение) с определенной степенью уверенности в том, что отдельно записанные черты идентифицируют (или не идентифицируют) одного и того же человека. Обычно биометрический шаблон представляет собой относительно небольшой объем данных; однако,

поскольку каждый изготовитель биометрической системы использует уникальный формат шаблона, взаимный обмен шаблонами между системами производиться не может.

4.3 В документе Doc 9303 рассматривается только три вида систем биометрической идентификации. Это физиологические системы:

- распознавания черт лица (обязательное),
- распознавания отпечатка пальца (факультативное),
- распознавания радужной оболочки глаза (факультативное).

Международный стандарт ИСО/МЭК 19794, состоящий из нескольких частей, устанавливает спецификации на эти виды биометрической идентификации. Государства выдачи обеспечивают соответствие этим спецификациям.

4.4 *Биометрические термины.* В контексте биометрической идентификации употребляются следующие термины:

- "*верифицировать*", т. е. производить проверку на совпадение "*один к одному*" между представленными биометрическими данными, полученными от владельца МСП в настоящий момент, и биометрическим шаблоном, созданным при занесении владельца в систему;

- "*идентифицировать*", т. е. производить поиск по принципу "*один ко многим*", сопоставляя представленные биометрические данные с коллекцией шаблонов, представляющих всех субъектов, занесенных в систему.

4.5 При выполнении функции идентификации биометрические параметры могут использоваться для повышения качества проверки анкетных данных в рамках процесса рассмотрения заявлений о выдаче паспорта, визы или иного проездного документа. При выполнении функции верификации они могут использоваться для установления точного соответствия между проездным документом и лицом, предъявляющим его.

5. Ключевые факторы

5.1 При определении выгод использования биометрических данных в МСП ключевыми факторами являются:

- *глобальная интероперабельность* – крайняя необходимость определения универсальной интероперабельной системы развертывания средств биометрической идентификации;

- *единообразие* – необходимость максимально возможного сокращения различных вариантов решения, которые потенциально могут применяться государствами-членами, путем установления конкретных стандартов;

- *техническая надежность* – необходимость предоставления норм и параметров с целью обеспечения развертывания государствами-членами проверенных технологий, гарантирующих высокую степень уверенности с точки зрения подтверждения личности, а также для того, чтобы государства, считывающие данные, закодированные другими государствами, могли быть уверены в том, что представленные им данные являются достаточно качественными и надежными для выполнения точной верификации в своих собственных системах;

- *практическая применимость* – необходимость обеспечения ввода в действие и выполнения технических требований государствами без потребности в введении множества различных систем и технических средств для обеспечения их соответствия всем возможным вариантам и интерпретациям стандартов;

- *долговечность* – требование о том, чтобы введенные системы сохранялись в течение максимального десятилетнего срока действия проездного документа, а будущие модификации были совместимы с прежними версиями.

6. Определения и термины

6.1 Термины, относящиеся к биометрии:

База данных. Любое хранилище биометрических образцов и соответствующей информации о конечном пользователе.

Бесконтактная интегральная схема. Электронный микрочип, соединенный с антенной, позволяющий производить передачу данных между чипом и кодирующим/считывающим устройством без необходимости в прямом электрическом контакте.

Биометрическая система. Автоматизированная система, способная:

1. брать биометрический образец у конечного пользователя для МСП;
2. извлекать биометрические данные из биометрического образца;
3. сравнивать конкретные значения биометрических данных с конкретными значениями в одном или нескольких контрольных шаблонах;
4. определять, насколько точно совпадают данные, т. е. выполнять на основе правил процесс проверки на совпадение, характерный для требований однозначной идентификации и аутентификации личности зарегистрированного пользователя в отношении соответствующей операции;
5. указывать, была ли достигнута идентификация или верификация личности.

Биометрические данные. Информация, извлекаемая из биометрического образца и используемая либо для создания контрольного шаблона (шаблонные данные) или для сравнения с ранее созданным контрольным шаблоном (сравнительные данные).

Биометрический образец. Исходные данные, взятые в качестве дискретного, однозначного, единственного и лингвистически нейтрального значения, отражающего биометрическую характеристику зарегистрированного пользователя, взятую биометрической системой (например, в целях аутентификации биометрические образцы могут включать изображение отпечатка пальца, а также его производные варианты).

Биометрический параметр. Измеряемая физическая характеристика или личностная поведенческая черта, используемая для опознания личности или для верификации предъявленной идентификационной информации зарегистрированного пользователя.

Валидация. Процесс демонстрации того, что рассматриваемая система во всех отношениях соответствует техническим требованиям к этой системе.

Верификация/верифицировать. Процесс сравнения представленного биометрического образца с биометрическим контрольным шаблоном одного зарегистрированного пользователя, в отношении которого предъявляется идентификационная информация, с целью определить, совпадает ли он с шаблоном зарегистрированного пользователя. Ср. с термином "*идентификация*".

Владелец. Обладающее электронным паспортом лицо, которое предоставляет биометрический образец для верификации или идентификации, предъявляя правильную или ложную идентификационную информацию. Лицо, взаимодействующее с биометрической системой для занесения в нее или проверки его идентификационной информации.

Галерея. База данных, содержащих биометрические шаблоны ранее зарегистрированных лиц, которые могут просматриваться с целью обнаружения пробника.

Глобальная интероперабельность. Способность систем проверки (автоматизированных или неавтоматизированных) различных государств мира принимать данные и производить обмен ими, обрабатывать данные, полученные из систем других государств, и использовать эти данные при проведении проверок в соответствующих государствах. Глобальная интероперабельность является основной целью применения стандартных спецификаций по размещению как визуально считываемых, так и машиносчитываемых данных во всех электронных паспортах.

Государство выдачи. Страна, записывающая биометрические параметры, чтобы позволить принимающему государству (которым может быть она сама) верифицировать их.

Дальность считывания. Практически возможное максимальное расстояние между бесконтактной ИС с антенной и считывающим устройством.

Занесение в систему. Процесс взятия у лица биометрических образцов и последующая подготовка и хранение биометрических контрольных шаблонов, идентифицирующих данное лицо.

Запоминающее устройство для данных (хранение). Средство хранения данных в таком документе, как МСП. В томе 2 части 1 документа Doc 9303 указано, что в электронном паспорте данные будут храниться на бесконтактной интегральной схеме.

Зарегистрированный пользователь. Человек, т. е. физическое лицо, которому государством или организацией выдан МСПД.

Захват. Метод взятия биометрического образца у конечного пользователя.

Идентификатор. Уникальный ряд данных, используемый в биометрической системе в качестве ключа к идентификации лица и его соответствующих атрибутов. Примером идентификатора является номер паспорта.

Идентификация/идентифицировать. Процесс сравнения представленного биометрического образца со всеми биометрическими контрольными шаблонами в файле по принципу "один ко многим" с целью определить, совпадает ли он с одним из шаблонов и, если совпадает, установить личность владельца электронного паспорта, чей шаблон оказался подходящим. Биометрическая система, используя принцип "один ко многим", стремится определить личность в базе данных, а не верифицировать предъявленную идентификационную информацию. Ср. с термином "*верификация*".

Извлечение. Процесс преобразования взятого биометрического образца в биометрические данные с тем, чтобы их можно было сравнить с контрольным шаблоном.

Изображение (лица) анфас. Фотография владельца МСП, изготовленная в соответствии с техническими требованиями, установленными в п. 7 раздела IV тома 1 части 1 документа Doc 9303.

Изображение. Воспроизведение биометрического параметра, обычно фиксируемого при помощи видеоаппаратуры, фотокамеры или сканирующего устройства. Для целей биометрической идентификации оно хранится в цифровой форме.

Конечный пользователь. Лицо, взаимодействующее с биометрической системой для занесения в нее или проверки его[1] идентификационной информации.

Коэффициент ложного допуска/FAR. Вероятность того, что биометрическая система ошибочно идентифицирует лицо или не сможет отказать самозванцу. Данный коэффициент обычно предполагает пассивные попытки самозванцев. Коэффициент ложного допуска определяется выражением *FAR = NFA / NIIA или FAR = NFA / NIVA,* где *FAR* – коэффициент ложного допуска, *NFA* – количество ложных допусков, *NIIA* – количество попыток идентификации со стороны самозванцев и *NIVA* – количество попыток верификации со стороны самозванцев.

Коэффициент ложного несовпадения. Альтернатива "коэффициенту ложного отказа"; используется во избежание путаницы в прикладных программах, отказывающих предъявителю при совпадении его биометрических данных с биометрическими данными зарегистрированного пользователя. В таких прикладных программах концепции допуска и отказа меняются местами и поэтому значение термина "ложный допуск" и термина "ложный отказ" меняется на обратное.

Коэффициент ложного отказа/FRR. Вероятность того, что биометрическая система не сможет идентифицировать зарегистрированного пользователя или произвести верификацию правильной идентификационной информации зарегистрированного пользователя. Коэффициент ложного отказа определяется выражением: *FRR = NFR / NEIA или FRR = NFR / NEVA,* где *FRR* – коэффициент ложного отказа, *NFR* – количество ложных отказов, *NEIA* – количество попыток идентификации со стороны зарегистрированных пользователей и *NEVA* – количество попыток верификации со стороны зарегистрированных пользователей. Эта оценка предполагает, что попытки идентификации/верификации со стороны зарегистрированных пользователей являются репрезентативными для всей группы зарегистрированных пользователей. Коэффициент ложного отказа, как правило, не включает ошибки, связанные с "невозможностью получения информации".

Коэффициент ложного совпадения. Альтернатива "коэффициенту ложного допуска"; используется во избежание путаницы в прикладных программах, отказывающих предъявителю при совпадении его биометрических данных с биометрическими данными зарегистрированного пользователя. В таких прикладных программах концепции допуска и отказа меняются местами и поэтому значение термина "ложный допуск" и термина "ложный отказ" меняется на обратное.

Личность. Совокупность отличительных персональных и физических признаков, данных и качеств, позволяющих однозначно идентифицировать лицо среди других лиц. В биометрической системе личность обычно устанавливается при регистрации лица в системе с использованием так называемых "исходных документов", таких, как свидетельство о рождении и свидетельство о гражданстве.

Ложный допуск. Случай, когда биометрическая система ошибочно идентифицирует лицо или ошибочно верифицирует личность самозванца по предъявленной идентификационной информации.

1. Во всех случаях, когда в настоящем документе употребляются грамматические формы мужского рода, их следует рассматривать, как относящиеся к лицам как мужского, так и женского пола.

Ложный отказ. Случай, когда биометрическая система не может идентифицировать зарегистрированного пользователя или не может произвести верификацию правильной идентификационной информации зарегистрированного пользователя.

Маркерное изображение. Фотография владельца МСП, обычно представляющая собой изображение анфас, размеры которого скорректированы для выдерживания фиксированного расстояния между глазами. Оно может быть также слегла повернуто так, чтобы воображаемая горизонтальная линия между центрами глаз была параллельна верхней кромке прямоугольной фотографии, если этого не было достигнуто, когда делалась или вводилась оригинальная фотография. (См. п. 13 раздела II в настоящем томе части 1 документа Doc 9303).

МСПД. Машиносчитываемый проездной документ (например, паспорт, виза или официальный документ, удостоверяющий личность), общепринятый для поездок.

Невозможность занесения в систему. Неспособность биометрической системы зарегистрировать лицо.

Невозможность получения информации. Неспособность биометрической системы получить необходимый биометрический параметр для регистрации лица.

"Один к нескольким". Сочетание идентификации "один ко многим" и верификации "один к одному". Как правило, процесс "один к нескольким" предполагает сравнение представленного биометрического образца с небольшим количеством биометрических контрольных шаблонов в файле. На него обычно делается ссылка при сопоставлении со списком "особого внимания", где указываются лица, требующие тщательной проверки идентификационной информации, или известные преступники, террористы и т. д.

"Один к одному". Синоним термина "верификация".

"Один ко многим". Синоним термина "идентификация".

Операционная система. Программа управления различными прикладными программами, используемыми компьютером.

Оценка. Число по шкале оценки от низкой до высокой, определяющее степень совпадения данных биометрического пробника (отыскиваемого лица) с конкретными данными из галереи (ранее зарегистрированного лица).

Порог. Контрольная оценка, выше которой степень соответствия между хранящимся биометрическим параметром и лицом считается допустимой, а ниже – неприемлемой.

Принимающее государство. Страна, считывающая биометрические параметры и желающая верифицировать их.

Пробник. Биометрический шаблон зарегистрированного пользователя, чью личность требуется установить.

Проверка. Осуществляемый государственным органом акт просмотра и верификации подлинности электронного паспорта, предъявленного ему пассажиром (владельцем электронного паспорта).

Проверять на совпадение/проверка на совпадение. Процесс сравнения биометрического образца с ранее записанным шаблоном и оценивания уровня сходства. Решение о допуске или отказе базируется на том, превышает ли оценка установленный порог.

Произвольный доступ. Способ хранения данных, при котором конкретные элементы данных можно извлекать без необходимости последовательно просматривать все хранящиеся данные.

Прямой захват. Процесс взятия биометрического образца путем взаимодействия между владельцем электронного паспорта и биометрической системой.

Размер шаблона. Объем памяти компьютера, забираемый биометрическими данными.

Регистрация. Процесс внесения идентификационной информации лица в биометрическую систему, увязки уникального идентификатора с данной личностью, а также сбора и записи соответствующих атрибутов лица в системе.

Самозванец. Лицо, предъявляющее биометрический образец в преднамеренной или невольной попытке выдать себя за другое лицо.

Сертифицирующий полномочный орган. Орган, выдающий биометрический документ и заверяющий подлинность хранящихся в документе данных способом, позволяющим обнаруживать мошенническое изменение.

Составная биометрическая характеристика. Использование более одного биометрического параметра.

Сравнение. Процесс сопоставления биометрического образца с ранее введенным в память контрольным шаблоном или шаблонами. См. также термины "*один ко многим*" и "*один к одному*".

Шаблон/контрольный шаблон. Данные, представляющие собой биометрические показатели зарегистрированного пользователя, используемые биометрической системой для сравнения с представляемыми впоследствии биометрическими образцами.

Электронный паспорт. Машиносчитываемый паспорт (МСП), содержащий чип бесконтактной интегральной схемы (ИС), на котором хранятся данные со страницы данных МСП, биометрический показатель владельца паспорта и элемент защиты данных с помощью криптографической технологии инфраструктуры открытых ключей (PKI), и соответствующий спецификациям части 1 документа Doc 9303.

JPEG и JPEG 2000. Стандарты на сжатие изображений, применяемые, в частности, в технологии хранения изображения лица.

LDS. Логическая структура данных, описывающая способ записи и форматирования биометрических данных в электронных паспортах.

PKI. Инфраструктура открытых ключей – методология, позволяющая обнаруживать подделку данных в электронном паспорте.

WSQ (коротковолновое скалярное квантование). Способ сжатия данных, применяемый, в частности, для хранения изображений отпечатков пальцев.

7. Ключевые процессы в отношении биометрических параметров

7.1 Основные компоненты биометрической системы:

Захват – получение исходного биометрического образца.
Извлечение – преобразование исходных данных биометрического образца в промежуточную форму.
Создание шаблона – преобразование промежуточных данных в шаблон для хранения.
Сравнение – сопоставление с информацией в хранящемся контрольном шаблоне.

7.2 Описание соответствующих процессов:

- Процесс занесения в систему состоит в захвате исходного биометрического образца. Он используется для взятия биометрических образцов у каждого нового лица (потенциального владельца МСП) в целях создания нового шаблона. Процесс захвата – это автоматическое получение биометрического параметра при помощи таких устройств, как дактилоскопический сканер, сканер для фотографий, цифровая камера прямой съемки или камера, изменяющая масштаб живого изображения радужной оболочки глаза. Для процесса захвата с помощью каждого снимающего устройства должны быть установлены определенные критерии и правила (например, обращение лицом к камере – стандартная поза при съемке для целей распознавания черт лица; каким образом – нажатием или перекатыванием – следует снимать отпечатки пальцев; глаза должны быть полностью открыты для фиксирования радужной оболочки глаза).

- Процесс создания шаблона сохраняет отличительные и повторяющиеся характеристики взятого биометрического образца и обычно осуществляется с помощью собственного программно реализованного алгоритма получения шаблона из зафиксированного изображения, который формирует это изображение так, чтобы его можно было впоследствии сравнить с другим зафиксированным изображением и дать сравнительную оценку степени совпадения. Неотъемлемым элементом этого алгоритма является контроль качества, благодаря которому посредством определенного механизма оценивается качество образца. Стандарты качества должны быть максимально высокими, так как все будущие проверки будут зависеть от качества первоначально зафиксированного изображения. Если качество является неудовлетворительным, процесс захвата следует повторить.

- В процессе идентификации берутся новые образцы и сравниваются с записанными шаблонами зарегистрированных конечных пользователей с целью определить, был ли конечный пользователь ранее зарегистрирован в системе и, если да, является ли он одним и тем же лицом.

- В процессе верификации берутся новые образцы владельца электронного паспорта и сравниваются с ранее записанными шаблонами этого владельца с целью определить, является ли данный владелец одним и тем же лицом.

8. Виды применения биометрического решения

8.1 Ключевым применением биометрического решения является верификация личности в плане определения связи между владельцем МСП и имеющимся у него паспортом.

8.2 В процессе занесения в систему при обращении за получением МСП имеет место ряд типичных видов применения биометрических параметров.

8.2.1 Биометрические данные конечного пользователя, полученные в процессе занесения, могут использоваться при поиске одной или нескольких баз биометрических данных (идентификация) с целью установить, известен ли конечный пользователь какой-либо из соответствующих систем (например, как имеющий паспорт под другим именем, как имеющий криминальное досье, как имеющий паспорт другого государства).

8.2.2 В момент получения паспорта или визы конечным пользователем (или его явки на любом этапе процесса выдачи после первоначального обращения за получением паспорта и взятия биометрических данных) его биометрические данные могут быть взяты еще раз и вновь верифицированы путем сопоставления с первоначально взятыми биометрическими данными.

8.2.3 Личность сотрудников, производящих занесение в систему, может верифицироваться для подтверждения того, что они уполномочены на выполнение порученных задач. Это может включать биометрическую аутентификацию для инициализации цифровой подписи в контрольных журналах на различных этапах процесса выдачи, позволяющую с помощью биометрических характеристик устанавливать связь между сотрудниками и действиями, за которые они несут ответственность.

8.3 Имеется также ряд типичных видов применения биометрических параметров на пунктах пограничного контроля.

8.3.1 Всякий раз, когда пассажир (т. е. владелец МСП) прибывает в государство или покидает его, личность пассажира может верифицироваться по изображению, созданному в момент выдачи его проездного документа. Это гарантирует, что владелец документа является именно тем лицом, которому он был выдан на законных основаниях, и повышает эффективность любой системы предварительной информации о пассажирах (API). В идеале, на проездном документе вместе с изображением следует хранить и биометрический шаблон или шаблоны, с тем чтобы верификация личности пассажира могла производиться в местах, где отсутствует доступ к центральной базе данных, или в пределах юрисдикции, где постоянное централизованное хранение биометрических данных не допускается.

8.3.2 *Двусторонняя проверка*. Взятые текущие биометрические данные пассажира в виде изображения и биометрический шаблон из его проездного документа (или из центральной базы данных) могут проверяться на совпадение с целью подтверждения того, что проездной документ не был изменен.

8.3.3 *Трехсторонняя проверка*. Текущие биометрические данные пассажира в виде изображения, изображение в его проездном документе и изображение, хранящееся в центральной базе данных, могут проверяться на совпадение (путем построения биометрических шаблонов каждого изображения) с целью подтверждения того, что проездной документ не был изменен. Этим методом определяется соответствие между лицом, его паспортом и базой данных, содержащей данные, внесенные в паспорт в момент его выдачи.

8.3.4 *Четырехсторонняя проверка*. Четвертая подтверждающая проверка (неэлектронная) представляет собой визуальное сравнение результатов трехсторонней проверки с цифровой фотографией на странице паспорта пассажира, содержащей данные.

8.4 Помимо применения биометрических параметров в целях занесения в систему и обеспечения безопасности на границах, демонстрируемого в процессах сравнения "один к одному" и "один ко многим", государствам следует также уделять внимание установлению собственных критериев в отношении:

– точности функций системы, связанных с сопоставлением биометрических данных; государства выдачи должны кодировать в МСП в соответствии со спецификациями LDS один или несколько биометрических параметров лица, отпечатка пальца или радужной оболочки глаза (они могут храниться также в базе данных, доступной принимающему государству); с учетом стандартизированного ИКАО биометрического изображения принимающие государства должны выбрать собственные программные средства биометрической верификации и определить собственные пороговые оценки биометрического совпадения для определения коэффициентов допуска при верификации личности и выявления самозванцев;

– пропускной способности (например, количество пассажиров в минуту) либо биометрической системы, либо системы контроля за пересечением границ в целом;

– пригодности конкретной биометрической технологии (идентификации по лицу, пальцу или глазу) для применения при осуществлении контроля за пересечением границ.

9. Ограничения в отношении биометрических решений

9.1 Общепризнано, что внедрение большинства биометрических технологий зависит от их дальнейшего (быстрого) развития. Принимая во внимание стремительные технологические изменения, любые спецификации (в том числе содержащиеся в этом документе) должны допускать и признавать возможность изменений, связанных с совершенствованием технологий.

9.2 Биометрическая информация, хранящаяся в проездных документах, должна соответствовать всем национальным законам о защите данных или законам о неприкосновенности частной жизни, принятым государством выдачи.

10. Взгляд ИКАО на биометрическую технологию

10.1 Концепция ИКАО в части применения биометрической технологии предусматривает:

– спецификацию основной интероперабельной формы биометрической технологии для использования на пунктах пограничного контроля (верификация, списки особого внимания), а также перевозчиками и органами, выдающими документы, и спецификацию согласованных дополнительных биометрических технологий;

– спецификацию биометрических технологий для использования органами, выдающими документы (идентификация, верификация и списки особого внимания);

– способность извлекать данные в течение максимального десятилетнего срока действия, как определено в документе Doc 9303;

– владение несобственническим элементом с целью обеспечения защиты любых государств, вкладывающих средства в биометрию, от меняющихся инфраструктур или поставщиков.

11. Выбор биометрических параметров, применимых к электронным паспортам

11.1 Давно известно, что указание в документе фамилии и презумпция честности его предъявителя не могут быть гарантией того, что владелец документа, удостоверяющего личность (МСП), предоставленного ему государством выдачи, является в принимающем государстве тем же лицом, которому был выдан этот документ.

11.2 Единственным методом безоговорочного установления связи человека с его проездным документом является получение его физиологической характеристики, относящейся к проездному документу, защищенным от несанкционированного доступа способом. Этой физиологической характеристикой является биометрический параметр.

11.3 В результате пятилетнего изучения операционных потребностей в биометрическом идентификаторе, пригодном для использования в процедуре выдачи МСП и в различных процессах, связанных с пересечением границ, в соответствии с законами различных государств о неприкосновенности частной жизни, ИКАО определила, что распознавание черт лица должно стать глобально интероперабельной биометрической технологией. В поддержку этой технологии каждое государство факультативно может использовать технологию распознавания отпечатка пальца и/или радужной оболочки глаза.

11.4 Сделав этот вывод, ИКАО отметила, что для большинства государств использование изображения лица человека связано с нижеуказанными преимуществами.

11.4.1 Фотографии с изображением лица не раскрывают информацию, которую человек обычно не раскрывает широкой публике.

11.4.2 Фотография (изображение лица человека) в социальном и культурном отношении уже принята на международном уровне.

11.4.3 Изображение лица уже в обычном порядке используется и верифицируется в рамках процесса обработки заявлений на получение МСП с целью выдачи паспорта в соответствии со стандартами документа Doc 9303.

11.4.4 Общество уже знакомо с процедурой получения изображения лица и использования его для целей верификации личности.

11.4.5 Получение изображения лица не является интрузивной процедурой. Для регистрации конечному пользователю не надо соприкасаться или взаимодействовать с физическим устройством в течение продолжительного времени.

11.4.6 Получение изображения лица не требует введения новых и дорогостоящих процедур занесения в систему.

11.4.7 Технология получения изображения лица может быть развернута практически незамедлительно, причем с возможностью также ретроспективного получения изображения.

11.4.8 Многие государства имеют действующие базы данных с изображениями лица, полученными в рамках изготовления паспортных фотографий в цифровой форме, которые могут быть закодированы в шаблоны изображения лица и верифицированы в целях сравнения идентификационной информации.

11.4.9 В соответствующих случаях по решению государства выдачи изображение лица можно снимать с заверенной фотографии без необходимости физического присутствия человека.

11.4.10 Для списков особого внимания фотография с изображением лица обычно является единственным биометрическим параметром, имеющимся для сравнения.

11.4.11 Верификация человеком биометрического параметра путем сравнения с фотографией/ субъектом является относительно простым и известным органам пограничного контроля процессом.

11.5 *Хранение биоматрического параметра лица*. Все производители средств распознавания черт лица используют собственные алгоритмы для создания своих биометрических шаблонов. Являясь интеллектуальной собственностью производителей, эти алгоритмы держатся ими в секрете и не могут быть воспроизведены путем обратной инженерии для создания распознаваемого изображения лица. Поэтому шаблоны распознавания черт лица не являются интероперабельными среди производителей, и единственный способ достижения интероперабельности изображения лица состоит в передаче принимающему государству снятой "оригинальной" фотографии. Затем принимающее государство использует алгоритм своего собственного производителя (который может быть или может не быть тем же производителем/вариантом, который используется государством выдачи) для сравнения снятого в реальном времени изображения лица владельца МСП с изображением лица, считанным с технического средства хранения данных в МСП.

12. Факультативные дополнительные биометрические параметры

12.1 Государства факультативно могут вводить дополнительные данные в свои процессы верификации личности (и процессы других государств) путем включения составной биометрической характеристики в свои проездные документы, т. е. комбинации изображений лица и/или отпечатка пальца и/или радужной оболочки глаза. Это уместно, в частности, там, где государства имеют действующие базы данных отпечатков пальцев и радужных оболочек глаза, в сопоставлении с которыми могут верифицироваться предоставляемые им биометрические параметры, например в рамках системы идентификационных карточек.

12.2 *Хранение факультативного биометрического параметра отпечатка пальца*. Технология биометрической идентификации по отпечаткам пальцев подразделяется на три класса: системы идентификации на основе изображения отпечатка пальца, системы идентификации на основе деталей дактилоскопического узора и системы идентификации на основе дактилоскопической карты. Хотя разработанные стандарты в рамках этих классов делают большинство систем интероперабельными в своем классе, системы, относящиеся к разным классам, интероперабельными не являются. В этой связи появляются три стандарта дактилоскопической интероперабельности: хранение данных изображения, хранение данных детального узора и хранение данных карты. Если государство выдачи решает предоставлять данные отпечатков пальцев в своих электронных паспортах, хранение изображения отпечатка пальца является обязательным для обеспечения глобальной интероперабельности между классами. Хранение соответствующего шаблона является факультативным и осуществляется по усмотрению государства выдачи.

12.3 *Хранение факультативного биометрического параметра радужной оболочки глаза*. Применение биометрических параметров радужной оболочки глаза осложняется нехваткой испытанных производителей. Фактический стандарт на биометрические параметры радужной оболочки глаза появился на базе методологии одного признанного производителя. Другие производители в будущем могут предложить технологию идентификации по радужной оболочке, однако в качестве отправной точки им, вероятно, потребуется изображение радужной оболочки глаза, а не шаблон, созданный нынешним производителем. Если государство выдачи решает

предоставлять данные о радужной оболочке глаза в своих электронных паспортах, хранение изображения радужной оболочки является обязательным для обеспечения глобальной интероперабельности. Хранение соответствующего шаблона является факультативным и осуществляется по усмотрению государства выдачи.

13. Хранение изображения: сжатие и обрезка

13.1 В структуре LDS элементом данных изменяемого размера, наиболее влияющим на размер LDS, является воспроизводимое изображение. В связи с этим встает вопрос: "До какого уровня государство выдачи может сжимать изображение без ухудшения результатов биометрического сравнения, проводимого принимающим государством?".

13.2 Биометрические системы уменьшают полученное исходное изображение (лицо/отпечаток пальца/радужная оболочка глаза) до размеров признакового пространства, используемого для проверки на совпадение; следовательно, сжатие может производиться с целью уменьшения потребности сохраняемых изображений в памяти при условии, что оно не искажает это признаковое пространство.

13.3 *Размер изображения лица*. Сканирование цветной фотографии стандартного формата ИКАО с разрешающей способностью 300 точек на дюйм дает изображение размером приблизительно 643 кб (килобайт) с примерно 90 пикселями между глазами. При минимальном сжатии оно может быть уменьшено до 112 кб (килобайт).

13.4 Проведенные исследования, в которых использовались стандартные фотографии, но с алгоритмами разных производителей и стандартами сжатия JPEG и/или JPEG2000, показали, что минимальный практичный размер изображения, подходящий для стандартной паспортной фотографии ИКАО, составляет приблизительно 12 кб (килобайт). Исследования показали, что степень сжатия сверх этого размера дает значительно менее надежные результаты распознавания черт лица. Емкость в 12 кб не всегда достижима, поскольку при одном и том же коэффициенте сжатия одни изображения компрессируются больше, чем другие, в зависимости от таких факторов, как материал, окраска и прическа. На практике средние размеры сжатого изображения лица в пределах 15–20 кб являются оптимальными для использования в электронных паспортах.

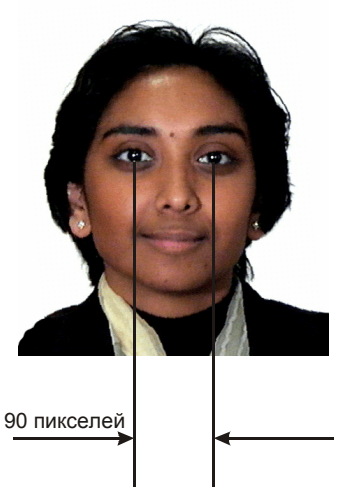
13.4.1 *Обрезка*. Для экономии пространства изображение можно обрезать и показать лишь глаза/нос/рот, однако это существенно снизит способность человека легко удостовериться в том, что данное изображение является изображением того же лица, которое стоит перед ним или фигурирует на фотографии на странице данных паспорта.

Например, изображение слева намного усложняет задачу распознавания по сравнению с изображением справа.

Следовательно, изображения, хранящиеся в LDS, рекомендуется:

- либо не обрезать, т. е. делать их идентичными фотографии, напечатанной на странице данных;
- либо минимально обрезать между подбородком и макушкой и между краями лица, как показано ниже.

13.4.2 Для содействия процессу опознания по лицу изображение лица хранится в виде либо полного изображения анфас, либо маркерного изображения в соответствии со спецификациями, установленными стандартом ИСО/МЭК 19794-5. Маркерное изображение – это изображение лица, которое при необходимости поворачивается, с тем чтобы воображаемая горизонтальная линия между центрами глаз была параллельна верхней кромки снимка и размер которого скорректирован. ИКАО рекомендует, чтобы пространство между центрами глаз составляло приблизительно 90 пикселей, как иллюстрируется ниже.



Оригинальное изображение

Маркерное изображение
(наклонено и размер изменен)

Логическая структура данных (см. раздел III) может обеспечивать хранение координат положения глаз. (О записи изображения лица в рамках LDS подробно говорится в п. 10.3.1 раздела III настоящего тома.)

13.4.3 *Лицевые украшения*. Государство выдачи определяет, в какой степени оно будет допускать наличие лицевых украшений на хранящихся (или отображаемых) фотографиях. В общем, если такие украшения носятся постоянно, они могут фигурировать на хранящемся изображении.

13.5 *Размер факультативного изображения отпечатка пальца*. Если государство решает хранить на ИС изображение(я) отпечатков пальцев, то оптимальный размер изображения должен составлять приблизительно 10 кб данных на один палец (например, при сжатии типичным методом компрессии WSQ).

13.6 *Размер факультативного изображения радужной оболочки глаза*. Если государство решает хранить на ИС изображение(я) радужной оболочки глаза, то оптимальный размер изображения должен составлять приблизительно 30 кб данных на один глаз.

14. Хранение биометрических и других данных в логическом формате на бесконтактной ИС

14.1 Настоящие спецификации также требуют, чтобы использовались цифровые изображения и чтобы эти изображения были "на борту", т. е. хранились в электронном формате в проездном документе.

14.2 Эти изображения должны быть стандартизированы.

14.3 Бесконтактная ИС большой емкости является электронным носителем данных, определенным ИКАО в качестве технологии увеличения емкости для использования в электронных паспортах при развертывании средств биометрической идентификации.

14.3.1 *Емкость памяти бесконтактной ИС для хранения данных*. Емкость памяти ИС определяется по усмотрению государства выдачи и должна составлять как минимум 32 килобайта. Эта минимальная емкость необходима для хранения обязательного изображения лица (обычно 15–20 кб), дубликата данных МСЗ и необходимых элементов защиты данных. Хранение дополнительных изображений лица, отпечатка пальца и/или радужной оболочки глаза, может потребовать значительного увеличения емкости памяти для хранения данных. Максимальная емкость данных ИС не определяется.

14.4 *Хранение других данных*. Любое государство может использовать емкость памяти ИС электронного паспорта для увеличения объема машиносчитываемых данных МСП сверх уровня, установленного 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 параметры) и/или верификации подлинности документа.

14.5 *Логическая структура данных*. С целью обеспечения глобальной интероперабельности машинного считывания хранящихся данных "логическая структура данных" или LDS определяет формат записи данных на бесконтактной ИС. LDS подробно описывается в разделе III настоящего тома.

14.6 *Защита и конфиденциальность хранящихся данных*. Как государство выдачи, так и любое принимающее государство должны быть уверены в том, что данные, хранящиеся на ИС, не были изменены со времени их внесения при выдаче документа. Кроме того, законы или практика государства выдачи в отношении неприкосновенности личной жизни могут требовать, чтобы доступ к данным предоставлялся исключительно уполномоченным лицам или организациям. В этой связи ИКАО разработала указанные в разделе IV спецификации, касающиеся применения и использования современных методов шифрования, в частности интероперабельных схем инфраструктуры открытых ключей (PKI), для использования государствами вместе со своими машиносчитываемыми проездными документами, изготовленными в соответствии со спецификациями, указанными в документе Doc 9303. Основной целью этого является усиление защиты путем применения автоматизированных средств аутентификации МСП и их законных владельцев на международном уровне. Кроме того, рекомендуется ряд способов и средств в целях внедрения технологии международной аутентификации электронного паспорта и указания путей использования электронных паспортов для упрощения применения биометрии или электронной торговли. Спецификации раздела IV позволяют государству выдачи защищать хранящиеся данные от несанкционированного доступа путем использования средств контроля доступа. Определено два метода контроля доступа – базовый контроль доступа и расширенный контроль доступа.

14.7 Настоящие спецификации позволяют записывать данные на ИС только в момент выдачи МСП.

14.8 *PKI*. Основная цель описываемой схемы PKI – позволить полномочным органам, проверяющим электронные паспорта (принимающим государствам), производить верификацию аутентичности и целостности данных, хранящихся в электронном паспорте. Данные спецификации не предписывают полного внедрения сложной структуры PKI, а указывают способ внедрения, при котором государства могут делать выбор в различных сферах (таких, как активная или пассивная аутентификация, борьба с копированием данных и контроль доступа, автоматизация процесса пересечения границ и т. д.) и иметь таким образом возможность поэтапно внедрять дополнительные элементы, не противореча всей структуре.

14.8.1 Сертификаты используются в целях безопасности вместе с методологией рассылки открытых ключей (сертификатов) государствам-членам, а инфраструктура приспособлена для достижения целей ИКАО.

14.8.2 Спецификации PKI подробно описываются в разделе IV настоящего тома.

14.9 *PKI и LDS*. В разделах, посвященных LDS и PKI, определяется способ обеспечения целостности и конфиденциальности данных в контексте применения средств биометрической идентификации в МСП.

14.10 *Бесконтактная ИС и кодирование.* Бесконтактные ИС, используемые в МСП, должны соответствовать стандарту ИСО/МЭК 14443 типа A или типа B. Встроенная операционная система соответствует стандарту ИСО/МЭК 7816-4. LDS должна кодироваться по методу произвольного доступа. Дальность считывания (достигаемая комбинацией электронного паспорта и считывающего устройства) должна составлять, как указано в стандарте ИСО/МЭК 14443, до 10 см.

14.11 *Минимум элементов данных, хранящихся в LDS*. Минимумом обязательных элементов данных, подлежащих хранению в LDS на бесконтактной ИС, является дубликат данных машиносчитываемой зоны, входящих в группу данных 1, и изображение лица владельца, входящее в группу данных 2. Кроме того, ИС в электронном паспорте, отвечающем стандартам, должна содержать данные системы защиты (EF.SOD), необходимые для валидации целостности данных, созданных лицом, выдавшим паспорт; они хранятся в специальном файле № 1, указанном в LDS (см. раздел III). Данные системы защиты (EF.SOD) состоят из используемых хэш-групп данных. Подробная информация содержится в разделе IV.

14.12 *Структура хранящихся данных*. Логическая структура данных, указанная в разделе III, детализирует обязательную и факультативную информацию, подлежащую включению в конкретные блоки биометрических данных в рамках LDS.

15. Размещение бесконтактной ИС в МСП

15.1 *Местоположение бесконтактной ИС и связанной с ней антенны в МСП.* Местоположение бесконтактной ИС со связанной с ней антенной в МСП определяется по усмотрению государства выдачи. Государства должны отдавать себе отчет в настоятельной необходимости предохранения бесконтактной ИС от физического искажения или случайного повреждения, в том числе в результате сгибания и искривления.

15.2 *Факультативные места размещения бесконтактной ИС и ее антенны.* Определены следующие места размещения:

Страница данных – размещение ИС и антенны в структуре страницы данных, составляющей внутреннюю страницу книжки.

Середина книжки – размещение ИС и антенны между центральными страницами книжки.

Обложка – размещение в структуре или конструкции обложки.

Отдельная вшитая страница – включение ИС и ее антенны в отдельную страницу, которая может иметь форму пластиковой карточки размера ID3, вшитой в книжку в процессе изготовления.

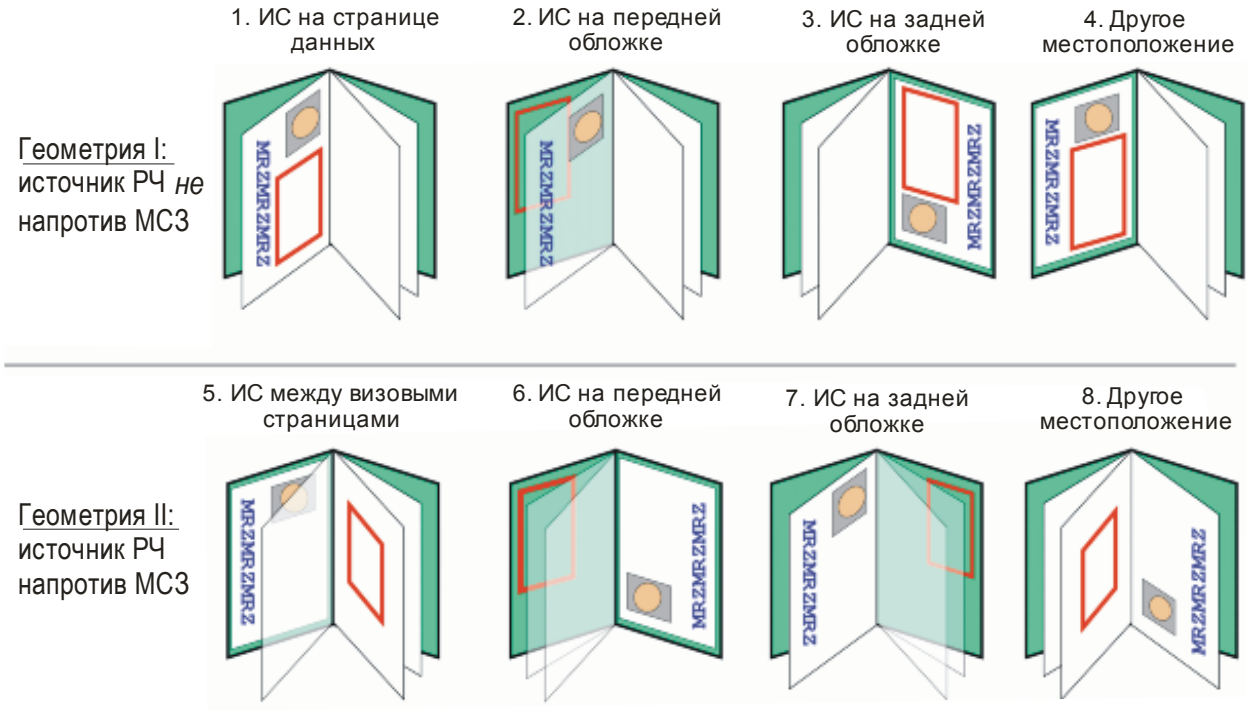


Рис. II-3

Рис. II-3 иллюстрирует вышеуказанные варианты.

Примечание. На этом рисунке ИС и ее антенна изображены в виде прямоугольника. Страница данных указана буквами MRZMRZMRZ, обозначающими МСЗ, и прямоугольником с кругом внутри, обозначающим фотографию.

15.3 *Меры предосторожности при изготовлении электронного паспорта.* Государства должны следить за тем, чтобы ИС или ее антенна не могли быть случайно повреждены в процессе изготовления книжки и в процессе персонализации. Например, перегрев при ламинировании или при перфорации изображения в зоне размещения ИС и антенны может повредить блок ИС. Аналогичным образом, в случае размещения ИС на передней обложке, тиснение фольгой на внутренней стороне обложки после монтирования блока также может повредить ИС или соединение с антенной.

15.4 *Считывание OCR и данных на ИС*. Настоятельно рекомендуется, чтобы принимающее государство считывало как данные OCR, так и данные, хранящиеся на ИС. В тех случаях, когда государство блокирует ИС в порядке защиты от несанкционированного перехвата информации, для получения доступа к данным ИС требуется производить считывание OCR. Для обеих операций желательно использовать только одно считывающее устройство, способное считывать оба вида данных. Если паспорт надо открывать на странице данных и класть на устройство считывания всей страницы, то следует учитывать, что одни МСП имеют ИС на обороте страницы, содержащей данные, а другие – в той части книжки, которая не захватывается устройством считывания всей страницы.

15.5 *Конструкция считывающего устройства*. Следовательно, государства должны устанавливать считывающую аппаратуру, способную обрабатывать МСП обеих геометрий и, по возможности, считывать OCR и ИС. На рис. II-4 показаны конфигурации считывающих устройств, каждое из которых может считывать OCR и ИС. Книга полуоткрыта и две антенны обеспечивают считывание ИС независимо от того, располагается она напротив МСЗ или нет. Показана также менее

удовлетворительная конфигурация, в которой электронный паспорт сначала кладется на считыватель OCR или протягивается через него для считывания МСЗ, а затем – на считыватель данных ИС. Эта схема менее удобна для сотрудников иммиграционных служб.

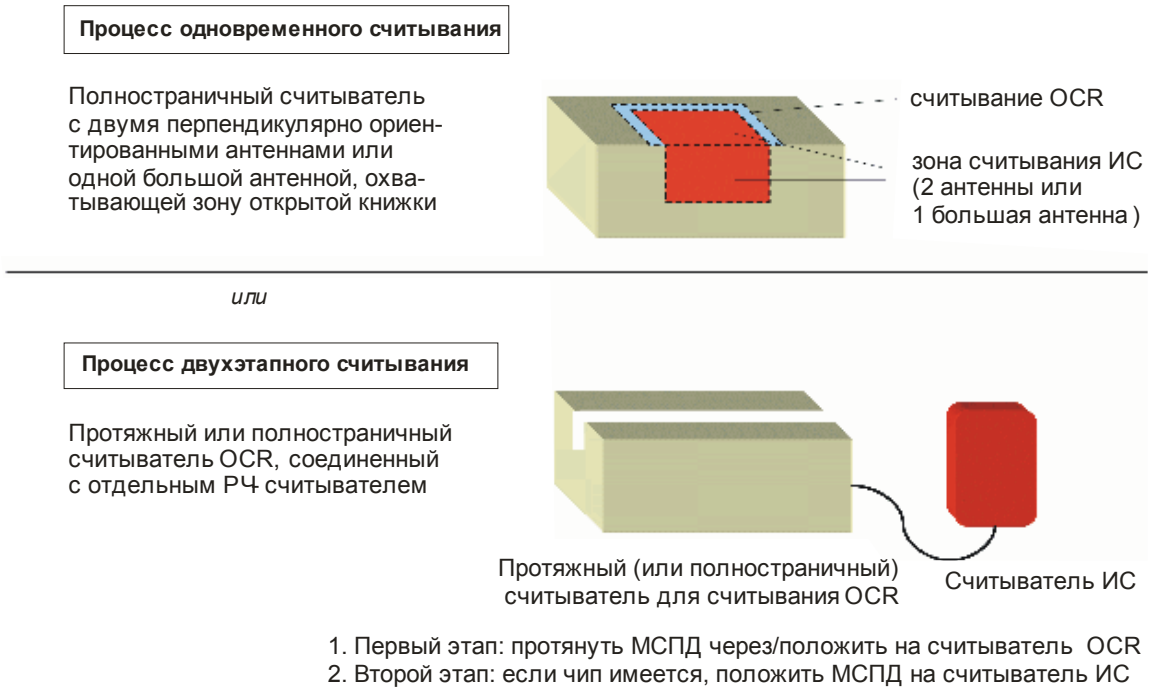


Рис. II-4

15.6 *Геометрии считывания*. Таким образом, изготовители считывающих устройств должны определять конструкторские решения машинного считывания, учитывающие различные возможности ориентации и (в идеале) позволяющие одновременно считывать МСЗ и бесконтактную ИС.

16. Процесс считывания электронного паспорта

16.1 На рис. II-5 показаны процессы, связанные со считыванием электронного паспорта до и во время биометрической верификации владельца.

17. Защита данных, хранящихся на бесконтактной ИС

17.1 Данные, хранящиеся на бесконтактной ИС, должны быть защищены от изменения. Это означает необходимость защиты, шифрования и аутентификации данных. Эти концепции подробно излагаются в разделах III (*LDS*) и IV (*PKI*).

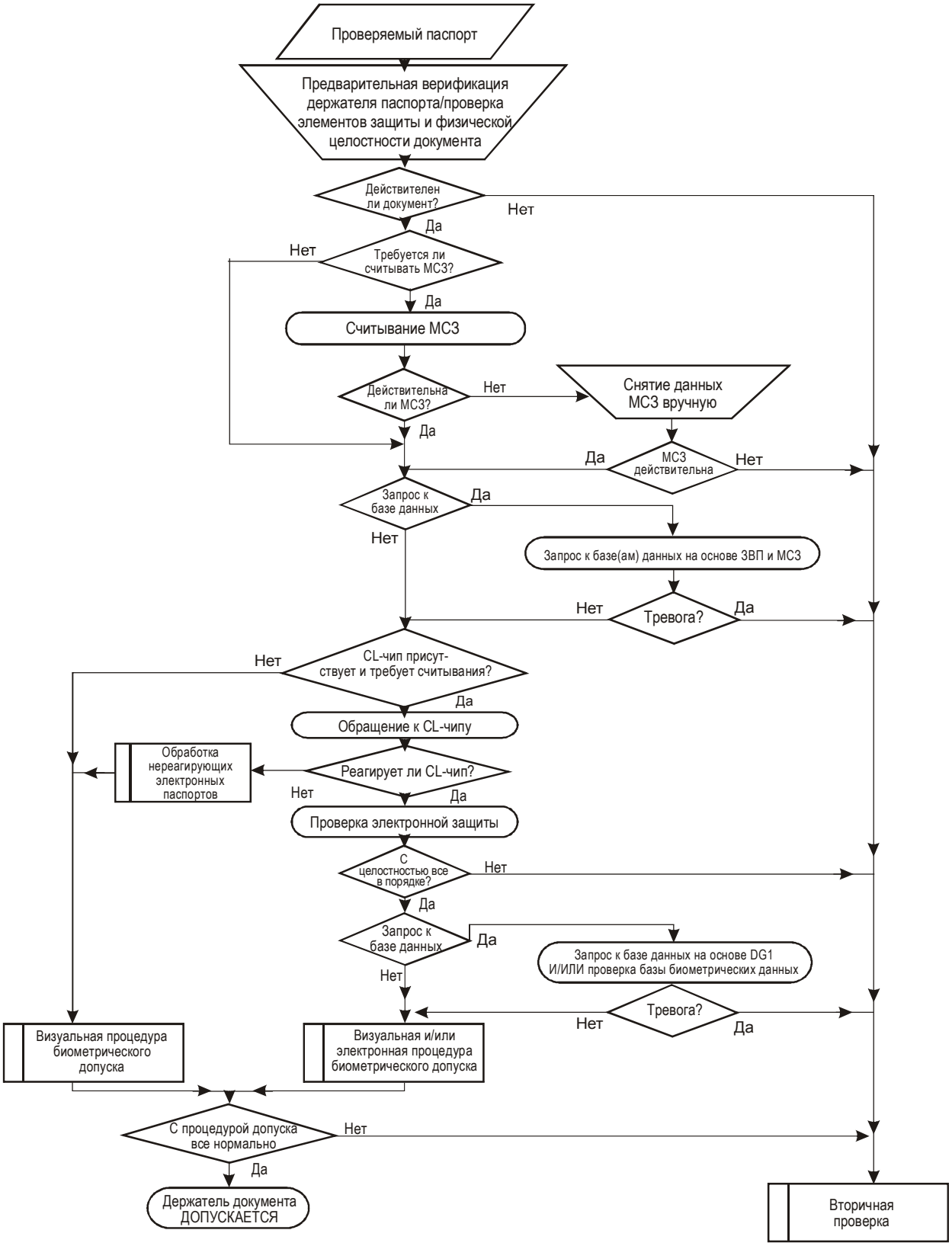

Проверяемый паспорт
Предварительная верификация держателя паспорта/проверка элементов защиты и физической целостности документа
Действителен ли документ?
Нет
Да
Требуется ли считывать МСЗ?
Нет
Да
Считывание МСЗ
Действительна ли МСЗ?
Нет
Снятие данных МСЗ вручную
Да
МСЗ действительна
Да
Нет
Запрос к базе данных
Да
Нет
Запрос к базе(ам) данных на основе ЗВП и МСЗ
Тревога?
Нет
Да
CL-чип присутствует и требует считывания?
Нет
Да
Обращение к CL-чипу
Обработка нереагирующих электронных паспортов
Реагирует ли CL-чип?
Нет
Да
Проверка электронной защиты
С целостностью все в порядке?
Нет
Да
Запрос к базе данных
Да
Нет
Запрос к базе данных на основе DG1 И/ИЛИ проверка базы биометрических данных
Тревога?
Нет
Да
Визуальная процедура биометрического допуска
Визуальная и/или электронная процедура биометрического допуска
С процедурой допуска все нормально
Нет
Да
Держатель документа ДОПУСКАЕТСЯ
Вторичная проверка

Рис. II-5

РАЗДЕЛ III

ЛОГИЧЕСКАЯ СТРУКТУРА ДАННЫХ ДЛЯ ТЕХНОЛОГИИ ХРАНЕНИЯ ДАННЫХ НА БЕСКОНТАКТНОЙ ИНТЕГРАЛЬНОЙ СХЕМЕ

1. Сфера применения

1.1 В настоящем разделе описывается логическая структура данных (LDS) электронных паспортов, необходимая для обеспечения глобальной интероперабельности. Здесь даются спецификации в отношении стандартной организации данных, записанных на техническом устройстве увеличения емкости (бесконтактная интегральная схема МСП), если эта технология выбрана государством или организацией выдачи, с тем чтобы принимающие государства могли иметь доступ к данным. Она требует идентификации всех обязательных и факультативных элементов данных и нормативного упорядочения и/или группирования элементов данных для достижения глобальной интероперабельности при считывании деталей (элементов данных), записанных на факультативном устройстве увеличения емкости, включенном в МСП (электронный паспорт).

2. Нормативные ссылки

2.1 Некоторые положения нижеуказанных международных стандартов, упоминаемых в этом тексте, составляют положения настоящего раздела. При наличии расхождений между новыми спецификациями, содержащимися в настоящем разделе, и упомянутыми стандартами, в интересах удовлетворения конкретным конструкторским требованиям к машиносчитываемым проездным документам, включая машиносчитываемые паспорта, приводимые здесь спецификации имеют преимущественную силу.

ИСО 3166-1: 1997	Коды для представления названий стран и единиц их административно-территориального деления. Часть 1. Коды стран
ИСО 3166-2: 1998	Коды для представления названий стран и единиц их административно-территориального деления. Часть 2. Коды единиц административно-территориального деления стран
ИСО 3166-3: 1999	Коды для представления названий стран и единиц их административно-территориального деления. Часть 3. Коды ранее использовавшихся названий стран
ИСО/МЭК 7816-1: 1998	Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 1. Физические характеристики
ИСО/МЭК 7816-2: 1998	Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 2. Размеры и расположение контактов
ИСО/МЭК 7816-3: 1997	Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 3. Электронные сигналы и протоколы передачи

ИСО/МЭК 7816-4: 2005	Карточки идентификационные. Карточки на интегральных схемах с контактами. Часть 4. Организация, защита и команды для обмена
ИСО/МЭК 7816-5: 2003	Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 5. Регистрация провайдеров прикладных программ
ИСО/МЭК 7816-6: 2003	Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 6. Элементы межотраслевых данных для обмена информацией (включая доклады о дефектах)
ИСО/МЭК 7816-7: 1998	Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 7. Межотраслевые команды для языка запросов структурированных карточек (SCQL)
ИСО/МЭК 7816-8: 2003	Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 8. Команды, обеспечивающие операции защиты
ИСО/МЭК 7816-9: 1999	Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 9. Команды для управления карточками и файлами
ИСО/МЭК 7816-10: 1999	Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 10. Электронные сигналы и отклик на возврат синхронных карточек в исходное положение
ИСО/МЭК 7816-11: 2003	Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 11. Персональный контроль с помощью биометрических методов
ИСО/МЭК 7816-15: 2003	Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 15. Применение криптографической информации
ИСО 8601: 2000	Элементы данных и форматы для обмена информацией. Обмен информацией. Представление дат и времени
ИСО/МЭК 8824-2: 1998	Рекомендация X.681 МСЭ-Т (1997). Информационные технологии. Нотация абстрактного синтаксиса № 1 (ASN.1). Спецификация информационных объектов
ИСО/МЭК 8824-3: 1998	Рекомендация X.682 МСЭ-Т (1997). Информационные технологии. ИСО/МЭК 8824-1: 1998
ИСО/МЭК 8824-4: 1998	Рекомендация X.683 МСЭ-Т (1997). Информационные технологии. Нотация абстрактного синтаксиса № 1 (ASN.1). Спецификация для параметризации ASN.1
ИСО/МЭК 8825-1: 2003	Информационные технологии. Правила кодирования ASN.1. Спецификация основных правил кодирования (BER), канонических правил кодирования (CER) и различительных правил кодирования (DER)
ИСО/МЭК 8825-2: 2003	Информационные технологии. Правила кодирования ASN.1. Спецификация правил уплотненного кодирования (PER)

ИСО/МЭК 8825-3: 2003 Информационные технологии. Правила кодирования ASN.1. Спецификация нотации контроля кодирования (ASN)

ИСО/МЭК 8825-4: 2003 Информационные технологии. Правила кодирования ASN.1. Правила кодирования XML (XER)

ИСО/МЭК 10373-6: 2001 Методы испытания карточек с малым зазором между индуктивной головкой и носителем

ИСО/МЭК 10373-6: 2001/FDAM1 Методы испытания карточек с малым зазором между индуктивной головкой и носителем. (Изменение 1. Протокол по методам испытания карточек с малым зазором между индуктивной головкой и носителем)

ИСО/МЭК 10373-6: 2001/AM2:2003 Методы испытания карточек с малым зазором между индуктивной головкой и носителем. (Изменение 2. Улучшенные методы испытаний RF)

ИСО/МЭК 10373-6: 2001/FDAM4 Методы испытания карточек с малым зазором между индуктивной головкой и носителем. (Изменение 4. Методы дополнительных испытаний интерфейса PCD RF и воздействия переменного поля PICC)

ИСО/МЭК 10373-6: 2001/FDAM5 Методы испытания карточек с малым зазором между индуктивной головкой и носителем. (Изменение 5. Скорость в битах fc/64, fc/32 и fc/16)

ИСО/МЭК 10918 Информационные технологии. Цифровое уплотнение и кодирование неподвижных изображений с непрерывным спектром тонов

ИСО/МЭК 14443-1: 2000 Карточки идентификационные. Бесконтактные карточки на интегральных схемах. Карточки с индуктивной связью через малый зазор. Часть 1. Физические характеристики

ИСО/МЭК 14443-2: 2001 Карточки идентификационные. Бесконтактные карточки на интегральных схемах. Карточки с индуктивной связью через малый зазор. Часть 2. Мощность высокочастотного сигнала и сигнальный интерфейс

ИСО/МЭК 14443-2: 2001/AM1:2005 Карточки идентификационные. Мощность высокочастотного сигнала и сигнальный интерфейс. (Изменение 2. Скорость в битах fc/64, fc/32 и fc/16)

ИСО/МЭК 14443-3 Карточки идентификационные. Бесконтактные карточки на интегральных схемах. Карточки с индуктивной связью через малый зазор. Часть 3. Инициализация и антиконфликтность

ИСО/МЭК 14443-3: 2001/AM1:2005 Карточки идентификационные. Мощность высокочастотного сигнала и сигнальный интерфейс. (Изменение 1. Скорость в битах fc/64, fc/32 и fc/16)

ИСО/МЭК 14443-4 Карточки идентификационные. Бесконтактные карточки на интегральных схемах. Карточки с индуктивной связью через малый зазор. Часть 4. Протокол передачи

ИСО/МЭК 15444	JPEG 2000
ИСО/МЭК 19785-1	Информационные технологии. Структура форматов обмена общей биометрической информацией. Часть 1. Спецификация элемента данных
ИСО/МЭК 19794-4	Информационные технологии. Форматы обмена биометрическими данными. Часть 4. Данные об изображении отпечатка пальца
ИСО/МЭК 19794-5	Информационные технологии. Форматы обмена биометрическими данными. Часть 5. Данные об изображении лица
ИСО/МЭК 19794-6	Информационные технологии. Форматы обмена биометрическими данными. Часть 6. Данные об изображении радужной оболочки
ИСО/МЭК 9797-1: 1999	Информационные технологии. Методы защиты. Коды аутентификации сообщений. Часть 1. Механизмы с использованием блочного шифра
Уникод 4.0.0	Консорциум Уникод. Стандарт Уникода, версия 4.0.0, установленная *стандартом Уникода, версия 4.0* (Boston, MA, Addison-Wesley, 2003. ISBN 0-321-18578-1) (Соответствует стандарту ИСО/МЭК 10646-1)

3. Определения

Для целей настоящего раздела применяются нижеуказанные дополнительные определения.

(*Примечание. Определения, касающиеся базового машиносчитываемого паспорта, визы и официального проездного документа, содержатся в разделе II тома 1 части 1 документа Doc 9303.)*

ASN.1. Нотация абстрактного синтаксиса № 1.

CBEFF. Структура форматов обмена общей биометрической информацией. Общий формат файлов, способствующий обмену и интероперабельности биометрических данных. Этот документ в настоящее время поддерживается Подкомитетом 37 Объединенного технического комитета 1 ИСО/МЭК (JTC1/SC37) в качестве проекта международного стандарта.

Уполномоченная принимающая организация. Уполномоченная на обработку официальных проездных документов организация (например, эксплуатант воздушных судов), которой, как таковой, в будущем может быть разрешено записывать данные на факультативном устройстве увеличения емкости.

Логическая структура данных (LDS). Набор групп элементов данных, хранящихся на факультативном устройстве увеличения емкости.

База данных. Ряд взаимосвязанных элементов данных, сгруппированных в рамках логической структуры данных.

Блок данных отправителя. Ряд групп данных, записанных государством или организацией выдачи на факультативном устройстве увеличения емкости.

Блок данных получателя. Ряд групп данных, записанных принимающим государством или уполномоченный принимающей организацией на факультативном устройстве увеличения емкости.

Аутентичность. Возможность подтвердить, что логическая структура данных и ее компоненты созданы государством или организацией выдачи.

Целостность. Возможность подтвердить, что логическая структура данных и ее компоненты, созданные государством или организацией выдачи, не изменены.

4. Потребность в логической структуре данных

4.1 Стандартная логическая структура данных (LDS) требуется для обеспечения глобальной интероперабельности при считывании данных, хранящихся на факультативном устройстве увеличения емкости, включаемом в МСПД по усмотрению государства или организации выдачи.

4.2 При разработке LDS ИКАО с самого начала определила в качестве главного требования наличие единой LDS для всех МСПД, использующих любую из рассматриваемых факультативных технологий увеличения емкости памяти. В результате проведенных дискуссий стало очевидно, что бесконтактная интегральная схема является единственной технологией, которая может удовлетворить все потребности ИКАО.

Примечание. LDS продолжает развиваться по мере подтверждения потребностей государств – членов ИКАО и других организаций, которые будут использовать LDS, в увеличении емкости памяти. На LDS может влиять, в частности, эволюция требований к защите данных по мере накопления знаний о необходимости обеспечения целостности и конфиденциальности данных.

5. Требования к логической структуре данных

5.1 ИКАО установила, что предопределенная стандартная LDS должна отвечать 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 одной LDS, общей для всех 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;

- обеспечивать обновление данных государством или организацией выдачи, если они того желают;

- обеспечивать внесение дополнительных данных принимающим государством или утвержденной принимающей организацией, сохраняя аутентичность[2] и целостность[3] данных, созданных государством или организацией выдачи;

- максимально использовать существующие международные стандарты, в частности новые международные стандарты по глобальному обмену интероперабельными биометрическими данными.

6. Обязательные и факультативные элементы данных

6.1 В целях удовлетворения глобальным требованиям, связанным с оформлением лиц, предъявляющих МСПД, для LDS определена серия обязательных и факультативных элементов данных, как это иллюстрируется на рис. III-1.

7. Упорядочение и группирование элементов данных

7.1 Для серии обязательных и факультативных элементов данных установлен логический порядок[4], обеспечиваемый упорядоченными группами взаимосвязанных элементов данных, как это иллюстрируется на рис. III-1.

7.2 Упорядоченные группы элементов данных затем группируются в зависимости от того, записаны ли они: 1) государством или организацией выдачи или 2) принимающим государством или утвержденной принимающей организацией.

Примечание. Возможность добавления данных к LDS принимающим государством или утвержденной принимающей организацией не обеспечивается LDS, определяемой в настоящем издании части 1 документа Doc 9303.

7.3 Если LDS записывается на факультативном устройстве увеличения емкости (бесконтактная ИС), обязательными являются четыре группы элементов данных:

- данные, определяющие содержание машиносчитываемой зоны (МСЗ) электронного паспорта (группа данных 1);

- закодированное изображение лица владельца электронного паспорта, как определяется в томе 1 и разделе II тома 2 части 1 документа Doc 9303;

- файл EF.COM, содержащий информацию о версии и перечень тегов;

- файл EF.SOD, содержащий информацию о целостности данных и аутентичности.

---

2. *Аутентичность*. Возможность подтвердить, что LDS и ее компоненты созданы государством или организацией выдачи.
3. *Целостность.* Возможность подтвердить, что LDS и ее компоненты, созданные государством или организацией выдачи, не изменены.
4. Логический порядок следования элементов данных стандартизирован в соответствии с установленными глобальными требованиями в отношении повышения уровня упрощения формальностей и безопасности при оформлении лиц, предъявляющих МСПД. Фактический порядок записи сгруппированных элементов данных определяется спецификациями, установленными в целях обеспечения эффективного функционирования устройства увеличения емкости в виде бесконтактной интегральной схемы. Эти спецификации указаны в добавлении 1.

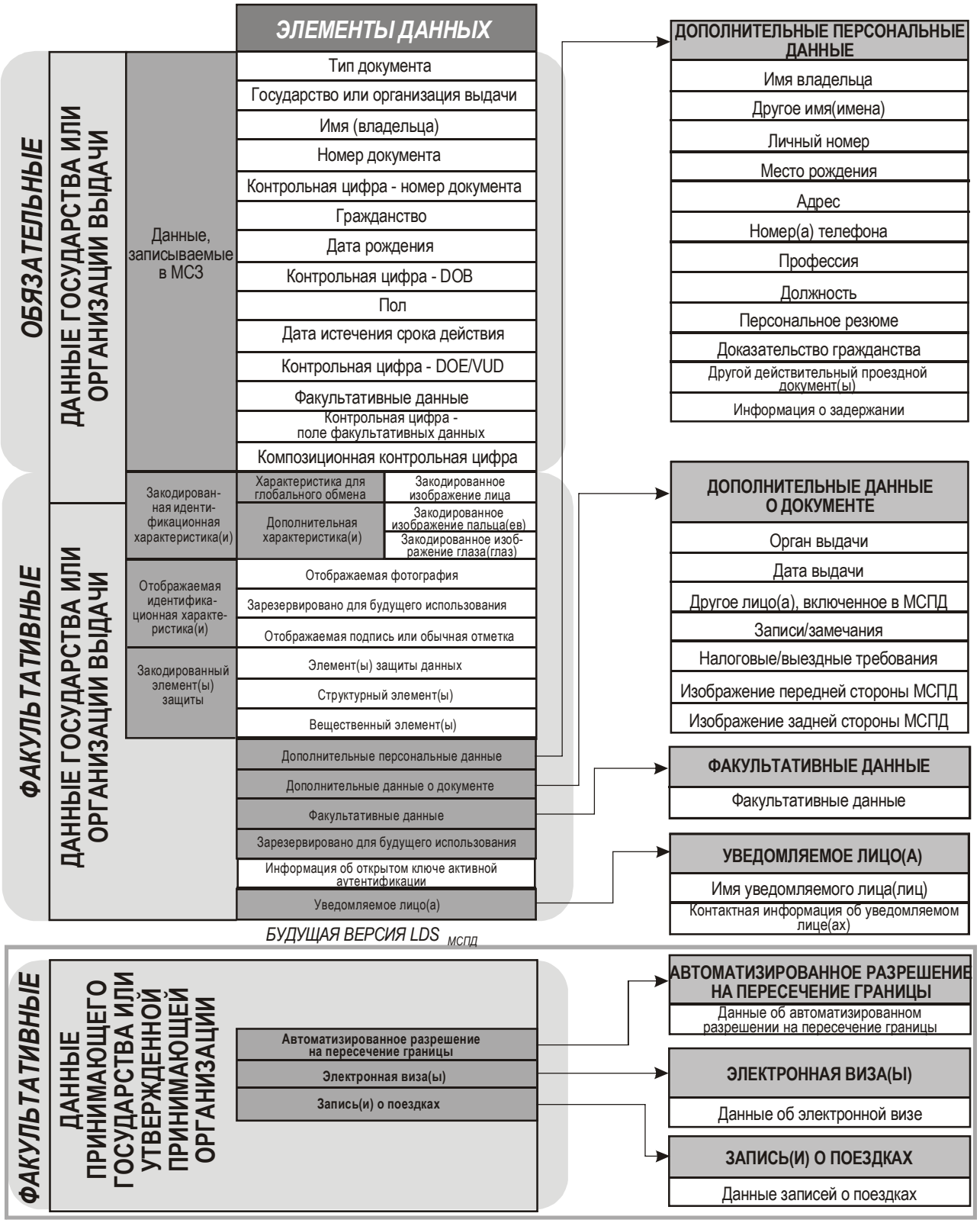


Рис. III-1. Обязательные и факультативные элементы данных, установленные для LDS

7.4 Все остальные элементы данных, установленные для записи государством или организацией выдачи, являются факультативными.

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

Примечание. Возможность добавления данных к LDS принимающим государством или утвержденной принимающей организацией не обеспечивается в настоящем издании части 1 документа Doc 9303.

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

Примечание. LDS спроектирована с достаточной степенью гибкости для применения ее ко всем видам МСПД. Некоторые элементы данных, указанные в последующих таблицах и на рисунках, применимы только к машиносчитываемым визам и официальным машиносчитываемым документам, удостоверяющим личность, или требуют иной формы представления в отношении данных документов. Эти элементы следует игнорировать в контексте электронного паспорта.

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

7.8 Каждой группе данных присваивается ссылочный номер. На рис. III-2 указан ссылочный номер каждой группы; например, "DG2" означает группу данных 2 "закодированная идентификационная характеристика(и)" лица законного владельца МСПД (т. е. биометрические детали лица).

Примечание. Группы данных принимающего государства (группы 17–19) не детализируются в настоящем издании части 1 документа Doc 9303.

8. Закодированные группы данных для обеспечения подтверждения аутентичности и целостности данных

8.1 Для подтверждения аутентичности и целостности записанных данных включен объект аутентичности/целостности. Каждая группа данных представляется в этом объекте аутентичности/целостности, который записывается в отдельном элементарном файле (EF.SOD). (См. раздел IV "*PKI*"). Путем использования структуры CBEFF, применяемой для групп данных 2-4 (закодированные идентификационные характеристики) и факультативных "дополнительных элементов биометрической защиты", определяемых в разделе IV *"PKI"*, по усмотрению государства или организации выдачи индивидуально могут также защищаться данные, подтверждающие личность (например, биометрические шаблоны).

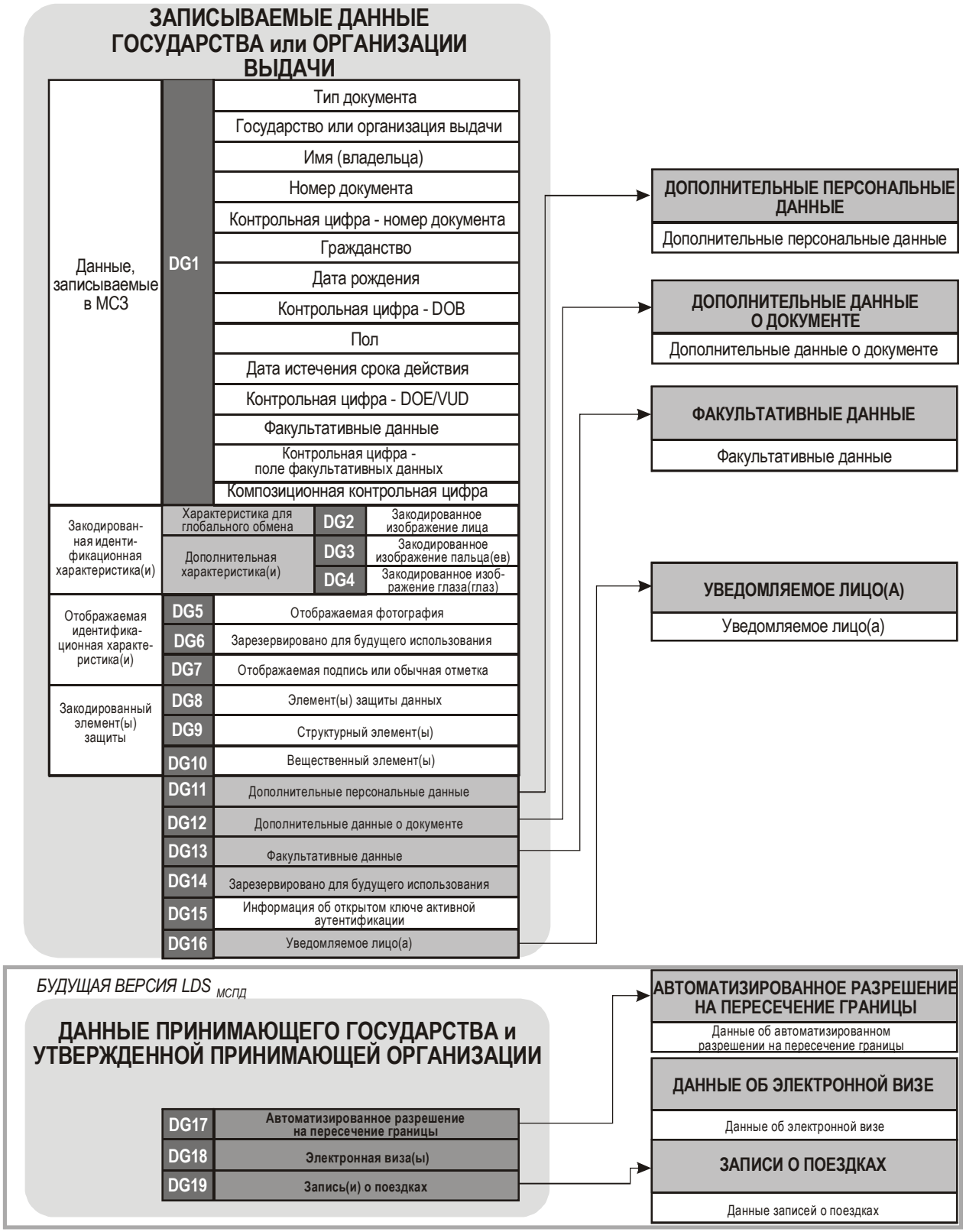


Рис. III-2. Справочные номера групп данных в LDS

Примечание к рис. III-2. Вариант добавления принимающим государством данных о разрешении на пересечение границы, электронных визах и поездках пока не допускается, но, тем не менее, включен в качестве указания перспективы развития.

9. Группы данных, записываемых государством или организацией выдачи

В следующей таблице указаны обязательные и факультативные группы данных, в целом образующие ту часть LDS, которая записывается государством или организацией выдачи.

Группа данных	Обязательные (M)/ факультативные (O)	Элемент данных	
Данные, записываемые в МСЗ МСПД			
1	M	Данные машиносчитываемой зоны (МСЗ)	
Данные машинного подтверждения личности. Закодированная идентификационная характеристика(и)			
2	M	**ХАРАКТЕРИСТИКА ДЛЯ ГЛОБАЛЬНОГО ОБМЕНА**	Закодированное изображение лица
3	O	Дополнительная характеристика	Закодированное изображение пальца(ев)
4	O	Дополнительная характеристика	Закодированное изображение радужной(ых) оболочки(ек)
Данные машинного подтверждения личности. Отображаемая идентификационная характеристика(и)			
5	O	Отображаемая фотография *[См. п. 10.3]*	
6	O	Зарезервировано для будущего использования	
7	O	Отображаемая подпись или обычная отметка	
Машинная верификация элементов защиты. Закодированный элемент(ы) защиты			
8	O	Элемент(ы) данных	
9	O	Структурный элемент(ы)	
10	O	Вещественный элемент(ы)	
Дополнительные персональные данные			
11	O	Дополнительные элементы персональных данных	
Дополнительные данные о документе			
12	O	Дополнительные элементы данных о документе	
Факультативные данные			
13	O	Элемент(ы) данных, определяемый по усмотрению государства или организации выдачи	
Зарезервировано для будущего использования			
14	O	Зарезервировано для будущего использования	
15	O	Информация об открытом ключе активной аутентификации	
Уведомляемое лицо(а)			
16	O	Элемент(ы) данных об уведомляемом лице(ах)	

10. Элементы данных, образующие группы данных 1–16

10.1 Группы данных 1(DG1) – 16 (DG16) в отдельности состоят из ряда обязательных и факультативных элементов данных. Порядок следования элементов данных в рамках группы данных стандартизирован.

10.2 В следующих таблицах указаны обязательные и факультативные элементы данных, которые в целом образуют структуру групп данных 1 (DG1) – 16 (DG16).

10.2.1 *Данные, записываемые в МСЗ МСПД.* Ниже приводятся элементы данных, включаемые в группу данных 1 (DG1). Элементы данных DG1 отражают все содержание МСЗ независимо от того, что она содержит – фактические данные или знаки-заполнители. Подробная информация о применении МСЗ содержится в томе 1 части 1 документа Doc 9303.

Группа данных	**Номер элемента данных**	**Фиксирован./ переменный**	**Обязательный/ факультативный**	**Элемент данных**
DG1			**M**	**МСЗ (Перечень данных, записываемых в МСПД. Ссылка на Doc 9303)**
	01	F	M	Тип документа
	02	F	M	Организация или государство выдачи
	03	F	M	Имя (*владельца*)
	04	F	M	Номер документа (*Девять наиболее значимых знаков*)
	05	F	M	Контрольная цифра. Номер документа или знак-заполнитель (<), указывающий, что номер документа состоит из более чем девяти знаков. *[См. п 10.2.2]*
	06	F	M	Гражданство
	07	F	M	Дата рождения
	08	F	M	Контрольная цифра – дата рождения
	09	F	M	Пол
	10	F	M	Дата истечения срока действия *(Для МСП, ПД-1 и ПД-2)*
	11	F	M	Контрольная цифра – дата истечения срока действия или дата, до которой действителен документ
	12	F	M	Факультативные данные и/или, в случае использования ПД-1, наименее значимые знаки номера документа плюс контрольная цифра номера документа и знак-заполнитель
	13	F	M	Контрольная цифра – поле факультативных данных
	14	F	M	Составная контрольная цифра

10.2.2 Подробная информация о расчете контрольных цифр приводится в томе 1 части 1 документа Doc 9303.

10.3 *Данные, связанные с машинным подтверждением личности. Закодированная идентификационная характеристика(и).* В группы данных 2 (DG2) – 4 (DG4) включаются следующие элементы данных:

Группа данных	Номер элемента данных	Обязательный/ факультативный	Элемент данных
DG2		**M**	**ИДЕНТИФИКАЦИОННАЯ ХАРАКТЕРИСТИКА ДЛЯ ГЛОБАЛЬНОГО ОБМЕНА. ЛИЦО** *[См. п. 10.3.1]*
	01	M	Количество записанных закодированных биометрических характеристик лица
	02[5]	M	Заголовок *[см. A.13.3]*
	03[6]	M	Закодированные биометрические данные лица *[см. A.13.3]*
ДОПОЛНИТЕЛЬНАЯ ИДЕНТИФИКАЦИОННАЯ ХАРАКТЕРИСТИКА(и) *[см. п. 10.3.2]*			
DG3		**O**	**ДОПОЛНИТЕЛЬНАЯ ИДЕНТИФИКАЦИОННАЯ ХАРАКТЕРИСТИКА. ПАЛЕЦ (ПАЛЬЦЫ)** *[см. п. 10.3.2]*
	01	M *(если записана закодированная характеристика пальца (пальцев))*	Количество записанных закодированных биометрических характеристик пальца (пальцев)
	02[6]	M *(если записана закодированная характеристика пальца (пальцев))*	Заголовок *[см. A.13.3]*
	03[6]	M *(если записана закодированная характеристика пальца (пальцев))*	Закодированные биометрические данные пальца (пальцев) *[см. A.13.3]*

5. Элемент данных повторяется в группе данных при наличии более одной записи биометрической характеристики, что определяется посредством элемента данных 01. Для конкретного внедрения см. технологическую схему в добавлении 1.

6. Элемент данных повторяется в группе данных при наличии более одной записи отображаемой подписи или обычной отметки/закодированного элемента защиты, что определяется посредством элемента данных 01.

Группа данных	Номер элемента данных	Обязательный/ факультативный	Элемент данных
DG4		**O**	**ДОПОЛНИТЕЛЬНАЯ ИНДЕНТИФИКАЦИОННАЯ ХАРАКТЕРИСТИКА. РАДУЖНАЯ ОБОЛОЧКА (РАДУЖНЫЕ ОБОЛОЧКИ)** *[см. п. 10.3.2]*
	01	M *(если записана закодированная характеристика глаза (глаз))*	Количество записанных закодированных характеристик радужной оболочки (радужных оболочек)
	02[6]	M *(если записана закодированная характеристика глаза (глаз))*	Заголовок *[см. A.13.3]*
	03[6]	M *(если записана закодированная характеристика глаза (глаз))*	Закодированные биометрические данные радужной оболочки (радужных оболочек) глаза *[см. A.13.3]*

10.3.1 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. Основная цель использования микросхемной технологии – обеспечение возможности захвата биометрических параметров в проездных документах. Изображение лица, используемое для обмена биометрическими данными и записываемое в DG2, получается из паспортной фотографии, используемой для создания отображаемого портрета, печатаемого на странице данных электронного паспорта, и кодируется согласно формату либо полного, либо маркерного изображения анфас, указанному в последней версии стандарта ИСО/МЭК 19794-5. По усмотрению государства выдачи DG2 содержит либо полное, либо маркерное изображение лица анфас в формате, используемом для обмена биометрическими данными, либо оба изображения. При включении полного изображения анфас наряду с ним могут включаться также данные о положении глаз с использованием факультативного блока данных о конкретных координатах, описываемого в стандарте ИСО/МЭК 19794-5. Государство выдачи, желающее записывать отображаемую фотографию, например, когда изображение лица в формате для обмена биометрическими данными существенно отличается от изображения на отображаемой фотографии, должны записывать изображение в группе DG5.

10.3.2 ИКАО признает, что в поддержку машинного подтверждения личности государства-члены могут использовать в качестве дополнительных биометрических технологий технику распознавания отпечатков пальцев и/или радужной оболочки глаза, изображения которых кодируются в рамках группы данных 3 (DG3) и группы данных 4 (DG4) соответственно.

10.4 *Данные для машинного подтверждения личности. Отображаемая идентификационная характеристика(и).* В группы данных 5 (DG5) – 7 (DG7) включены следующие элементы данных:

Группа данных	Номер элемента данных	Обязательный/ факультативный	Элемент данных
DG5		**O**	**ОТОБРАЖАЕМАЯ ФОТОГРАФИЯ**
	01	M *(если отображаемая фотография записана)*	Количество записанных отображаемых фотографий
	02[7]	M *(если отображаемая фотография записана)*	Формат(ы) представления отображаемой фотографии *[см. п. 10.4.1]*
DG6		**O**	**Зарезервировано для будущего использования**
DG7		**O**	**ОТОБРАЖАЕМАЯ ПОДПИСЬ ИЛИ ОБЫЧНАЯ ОТМЕТКА**
	01	M *(если отображаемая подпись или обычная отметка записаны)*	Количество отображаемых подписей или обычных отметок
	02[6]	M *(если отображаемая подпись или обычная отметка записаны)*	Формат представления отображаемой подписи или обычной отметки *[см. п. 10.4.1]*

10.4.1 Элемент данных 02 группы данных 5 (DG5) и группы данных 7 (DG7) кодируется согласно стандарту ИСО/МЭК 10918-1 с использованием варианта JFIF или стандарта ИСО/МЭК 15444 (JPEG2000).

10.5 *Машинная верификация элементов защиты. Закодированные данные.* В группы данных 8 (DG8) – 10 (DG10) в целом входят следующие элементы данных:

Группа данных	Номер элемента данных	Обязательный/ факультативный	Элемент данных
DG8		**O**	**ИНФОРМАЦИННЫЙ ЭЛЕМЕНТ(Ы)**
	01	M *(если этот закодированный элемент используется)*	Количество информационных элементов

7. Элемент данных повторяется в группе данных при наличии более одной записи отображаемой характеристики, что определяется посредством элемента данных 01.

Группа данных	Номер элемента данных	Обязательный/ факультативный	Элемент данных
	02[6]	M *(если этот закодированный элемент используется)*	Заголовок *(подлежит определению)*
	03	M *(если этот закодированный элемент используется)*	Данные об информационном элементе(ах)
DG9		**O**	**СТРУКТУРНЫЙ ЭЛЕМЕНТ(Ы)**
	01	M *(если этот закодированный элемент используется)*	Количество структурных элементов
	02	M *(если этот закодированный элемент используется)*	Заголовок *(подлежит определению)*
	03	M *(если этот закодированный элемент используется)*	Данные о структурном элементе(ах)
DG10		**O**	**ВЕЩЕСТВЕННЫЙ ЭЛЕМЕНТ(Ы)**
	01	M *(если этот закодированный элемент используется)*	Количество записанных вещественных элементов
	02	M *(если этот закодированный элемент используется)*	Заголовок *(подлежит определению)*
	03	M *(если этот закодированный элемент используется)*	Данные о вещественном элементе(ах)

10.6 *Дополнительные персональные данные.* В группу данных 11 (DG11) в целом входят следующие элементы данных:

Группа данных	Номер элемента данных	Обязательный/ факультативный	Элемент данных
DG11		**O**	**ДОПОЛНИТЕЛЬНЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ**
	01	O	Имя владельца (основной и вторичный идентификаторы, полностью)
	02	O	Другое имя (имена)
	03	O	Личный номер
	04	O	Место рождения
	05	O	Дата рождения (полностью)
	06	O	Адрес
	07	O	Телефонный номер(а)
	08	O	Профессия
	09	O	Должность
	10	O	Персональное резюме
	11	O	Доказательство гражданства *[см. п. 10.6.1]*
	12	M* ** если элемент данных 13 записан*	Количество других действительных проездных документов
	13	O	Номера других проездных документов
	14	O	Информация о задержании

10.6.1 Элемент данных 11 кодируется в соответствии со стандартом *ИСО/МЭК 10918-1* или стандартом ИСО/МЭК 15444 (JPEG2000).

10.7 *Дополнительные данные о документе(ах)*. В группу данных 12 (DG12) в целом входят следующие элементы данных:

Группа данных	Номер элемента данных	Обязательный/ факультативный	Элемент данных
DG12			**ДОПОЛНИТЕЛЬНЫЕ ДАННЫЕ О ДОКУМЕНТЕ**
	01	O	Полномочный орган выдачи *(МСПД)*
	02	O	Дата выдачи *(МСПД)*
	03	M* ** если другое лицо(а) включено в МСПД*	Количество других лиц в МСПД *(только МСВ)*
	04	O	Другое лицо(а), включенное в МСПД *(только МСВ)*
	05	O	Надписи/замечания *(относящиеся к МСПД)*
	06	O	Налоговые/выездные требования
	07	O	Изображение передней стороны МСПД *[см. п. 10.7.1]*
	08	O	Изображение задней стороны МСПД *[см. п. 10.7.1]*

Группа данных	Номер элемента данных	Обязательный/ факультативный	Элемент данных
	09	O	Время персонализации МСПД
	10	O	Машина, использованная для персонализации МСПД

10.7.1 Элементы данных 07 и 08 кодируются в соответствии со стандартом *ИСО/МЭК 10918-1* или стандартом ИСО/МЭК 15444 (JPEG2000).

10.8 *Факультативные данные.* Группу данных 13 (DG13) в целом образуют следующие элементы данных:

Группа данных	Номер элемента данных	Обязательный/ факультативный	Элемент данных
DG13		**O**	**ФАКУЛЬТАТИВНЫЕ ДАННЫЕ**
	01	M *(Если группа данных 13 записана)*	Данные, определяемые государством или организацией выдачи

10.9 *Группа данных 14: неопределенная группа данных*. Зарезервировано для будущего использования.

Группа данных	Номер элемента данных	Обязательный/ факультативный	Элемент данных
DG14		**O**	**Зарезервировано для будущего использования**

10.10 Группа данных 15 (DG15): информация об открытом ключе активной аутентификации. Эта группа данных содержит факультативный открытый ключ активной аутентификации (см. раздел IV PKI).

Группа данных	Номер элемента данных	Обязательный/ факультативный	Элемент данных
DG15		**O**	**Информация об открытом ключе активной аутентификации**

10.11 *Уведомляемое лицо(а).* Группу данных 16 (DG16) в целом образуют следующие элементы данных:

Группа данных	Номер элемента данных	Обязательный/ факультативный	Элемент данных
DG16		**O**	**УВЕДОМЛЯЕМОЕ ЛИЦО(А)**
	01	M *(Если группа данных 16 записана)*	Количество идентифицированных лиц
	02	M *(Если группа данных 16 записана)*	Записанные данные о датах
	03	M *(Если группа данных 16 записана)*	Имя уведомляемого лица
	04	M *(Если группа данных 16 записана)*	Телефон уведомляемого лица
	05	O	Адрес уведомляемого лица

11. Группы данных, записываемых принимающим государством или утвержденной принимающей организацией

11.1 В следующей таблице указаны факультативные группы данных, образующие в целом ту часть LDS, которая в будущем может быть доступна для записи данных принимающим государством или утвержденной принимающей организацией.

Примечание. В рамках настоящего издания части 1 документа Doc 9303 принимающему государству или утвержденной принимающей организации не разрешается записывать эти данные. Следовательно, группы данных 17–19 недействительны и в настоящее время не поддерживаются методикой LDS. В этот документ они включены для указания перспективы развития.

Группа данных	Обязательные (M) / Факультативные (O)	Элемент данных
Данные, касающиеся автоматизированного разрешения на пересечение границы		
DG17	O	Автоматизированное разрешение на пересечение границы
Электронные визы		
DG18	O	Электронная виза(ы)
Данные записей о поездках		
DG19	O	Запись(и) о поездках

12. Формат элементов данных

12.1 *Указатель элементов данных*

В настоящем разделе описываются элементы данных, которые могут присутствовать в каждой группе данных.

12.1.1 Элементы данных государства выдачи или утвержденной организации выдачи

Группы данных 1 (DG1) – 16 (DG16). Элементы данных и их формат в каждой группе данных указаны ниже.

A – буквенный знак [a..z, A..Z], N – цифровой знак [0..9], S – специальный знак ['<', ' '], B – 8-битные двоичные данные (любые, кроме A, N или S), F – поле фиксированной длины, Var – поле переменной длины.

Элемент данных	**Факультат. или обязат.**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. или перемен.**	**Тип кодиро-вания**	**Требования к кодированию**
ГРУППА ДАННЫХ 1. Данные, записываемые в МСЗ						
01	M	Тип документа	2	F	A,S	Тип документа (согласно МСЗ в Doc 9303)
02	M	Государство или организация выдачи	3	F	A,S	Государство или организация выдачи (согласно МСЗ в Doc 9303)
03	M	Имя владельца				
	M	*Основной и вторичный идентифика-торы*	39	F	A,S	Одинарные и двойные знаки-заполнители (<), включаемые согласно МСЗ в Doc 9303
04	M	Номер документа	9	F	A,N,S	Номер документа (согласно МСЗ) Примечание. В соответствии со спецификациями ПД-1 в части 3 Doc 9303, если номер документа состоит из более чем девяти знаков, на позиции контрольной цифры (DE 05) ставится знак-заполнитель (<), а остальные знаки, составляющие номер документа, записываются в начале DE 12, после чего указывается контрольная цифра номера документа и знак-заполнитель (<)
05	M	Контрольная цифра – *Номер документа*	1	F	N,S	Контрольная цифра элемента данных 04 (согласно МСЗ в Doc 9303)
06	M	Гражданство	3	F	A,S	3-буквенный код (согласно МСЗ)
07	M	Дата рождения	6	F	N,S	Формат = YYMMDD согласно МСЗ в Doc 9303. Полная дата рождения (DOB) может храниться в DG11 в формате CCYYMMDD во избежание неясности в кодировании года
08	M	Контрольная цифра – *Дата рождения*	1	F	N	Контрольная цифра элемента данных 07 (согласно МСЗ в Doc 9303)
09	M	Пол	1	F	A,S	Согласно МСЗ в Doc 9303
10	M Если это МСП, ПД-1, ПД-2	Дата истечения срока действия	6	F	N	Формат = YYMMDD согласно МСЗ

Элемент данных	Факультат. или обязат.	Название элемента данных	Коли-чество байтов	Фиксир. или перемен.	Тип кодиро-вания	Требования к кодированию
	M Если это MCB-A, MCB-B	Действительно до определенной даты	6	F	N	Формат = YYMMDD согласно MC3
11	M	Контрольная цифра – *Дата истечения срока действия или действительно до определенной даты*	1	F	N	Контрольная цифра элемента данных 10 (согласно MC3 в Doc 9303)
12	M *Если факульта-тивные данные в MC3*	Факультативные данные				
	M *Если факульта-тивные данные в MC3*	*Факульта-тивные данные*	14	F	A,N,S	Согласно MC3
13	M	Контрольная цифра – *Поле факультатив-ных данных*	1	F	N	Контрольная цифра элемента данных 12 (согласно MC3 в Doc 9303)
14	M	Контрольная цифра – *Составная контрольная цифра*	1	F	N	Согласно MC3 в Doc 9303
ГРУППА ДАННЫХ 2. Закодированные идентификационные характеристики: ЛИЦО						
01	M *Если закодиро-ванная характе-ристика лица включена*	Количество записанных кодировок биометрических характеристик лица	1	F	N	Цифры 1–9, указывающие количество уникальных кодировок данных о лице
02	M *Если закодиро-ванная характе-ристика лица включена*	Заголовок		F		Подробная информация о кодировании содержится в *Нормативном добавлении 1 (A13.3)*. Элемент данных может повторяться, как определено элементом данных 01 (DE 01)
03	M *Если закодиро-ванная характе-ристика лица включена*	Кодировка(и) биометрических данных о лице	99999 Макс.	Var	A,N,S,B	Подробная информация о кодировании содержится в *Нормативном добавлении 1 (A13.3)*. Элемент данных может повторяться, как определено элементом данных 01 (DE 01)

Элемент данных	Факультат. или обязат.	Название элемента данных	Коли-чество байтов	Фиксир. или перемен.	Тип кодиро-вания	Требования к кодированию
ГРУППА ДАННЫХ 3. Закодированные идентификационные характеристики: ПАЛЕЦ (ПАЛЬЦЫ)						
01	M *Если закодиро-ванная характе-ристика пальца (пальцев) включена*	Количество записанных кодировок биометрических характеристик пальца	1	F	N	Цифры 1–9, указывающие количество уникальных кодировок данных о пальце (пальцах)
02	M *Если закодиро-ванная характе-ристика пальца (пальцев) включена*	Заголовок		F		Подробная информация о кодировании содержится в *Нормативном добавлении 1 (A13.3)*. Элемент данных может повторяться, как определено элементом данных 01 (DE 01)
03	M *Если закодиро-ванная характе-ристика пальца (пальцев) включена*	Кодировка(и) биометрических данных о пальце	99999 Макс.	Var	A,N,S,B	Подробная информация о кодировании содержится в *Нормативном добавлении 1 (A13.3)*. Элемент данных может повторяться, как определено элементом данных 01 (DE 01)
ГРУППА ДАННЫХ 4. Закодированные идентификационные характеристики: РАДУЖНАЯ ОБОЛОЧКА (РАДУЖНЫЕ ОБОЛОЧКИ)						
01	M *Если закодиро-ванная характе-ристика глаза (глаз) включена*	Количество записанных кодировок биометрических характеристик глаза	1	F	N	Цифры 1–9, указывающие количество уникальных кодировок данных о глазе (глазах)
02	M *Если закодиро-ванная характе-ристика глаза (глаз) включена*	Заголовок		F		Подробная информация о кодировании содержится в *Нормативном добавлении 1*. Элемент данных может повторяться, как определено элементом данных 01 (DE 01)
03	M *Если закодиро-ванная характе-ристика глаза (глаз) включена*	Кодировка(и) биометрических данных о глазе	99999 Макс.	Var	A,N,S,B	Подробная информация о кодировании содержится в *Нормативном добавлении 1*. Элемент данных может повторяться, как определено элементом данных 01 (DE 01)

Элемент данных	Факультат. или обязат.	Название элемента данных	Коли-чество байтов	Фиксир. или перемен.	Тип кодиро-вания	Требования к кодированию
ГРУППА ДАННЫХ 5. Отображаемая идентификационная характеристика(и): ФОТОГРАФИЯ						
01	M *Если отобра-жаемая фотогра-фия включена*	Количество записей: отображаемая фотография	1	F	N	Цифры 1–9, указывающие количество уникальных записей отображаемой фотографии
02	M *Если отобра-жаемая фотогра-фия включена*	Данные об отображаемой фотографии		F		Элемент данных может повторяться, как определено элементом данных 01
	M Если отобра-жаемая фотогра-фия включена	*Количество байтов в представлении отображаемой фотографии*	5	F	N	Цифры 00001–99999, указывающие количество байтов в представлении отображаемой фотографии
	M Если отобра-жаемая фотогра-фия включена	*Представление отображаемой фотографии*	99999 Макс.	Var	A,N,S,B	Форматируется согласно ИСО/МЭК 10918-1 или ИСО/МЭК 15444
ГРУППА ДАННЫХ 6. Зарезервировано для будущего использования						
ГРУППА ДАННЫХ 7. Отображаемые идентификационные характеристики: ПОДПИСЬ или ОБЫЧНАЯ ОТМЕТКА						
01	M *Если отобра-жаемая 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 отобра-жаемая подпись или обычная отметка включена*	Данные об отображаемой подписи или обычной отметке		Var		Элемент данных может повторяться, как определено элементом данных 01

Элемент данных	Факультат. или обязат.	Название элемента данных	Количество байтов	Фиксир. или перемен.	Тип кодирования	Требования к кодированию
	M Если отображаемая подпись или обычная отметка включена	*Представление отображаемой подписи или обычной отметки*	99999 Макс.	Var	A,N,S,B	Форматируется согласно ИСО/МЭК 10918-1 или ИСО/МЭК 15444
ГРУППА ДАННЫХ 8. Закодированные элементы защиты: ИНФОРМАЦИОННЫЙ ЭЛЕМЕНТ(Ы)						
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 02–04)
02	M *Если закодированный информационный элемент включен*	Информация о заголовке	1	TBD		Определяются детали заголовка
03	M *Если закодированный информационный элемент включен*	Данные об информационном элементе		Var		
	M Если закодированный информационный элемент включен	*Закодированный информационный элемент*	999 Макс.	Var	B	Формат определяется по усмотрению государства или организации выдачи
ГРУППА ДАННЫХ 9. Закодированные элементы защиты: СТРУКТУРНЫЙ ЭЛЕМЕНТ(Ы)						
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 02–04)

Элемент данных	Факультат. или обязат.	Название элемента данных	Коли-чество байтов	Фиксир. или перемен.	Тип кодиро-вания	Требования к кодированию
02	M *Если закодиро-ванный структур-ный элемент включен*	Информация о заголовке	TBD	TBD	N	Определяются детали заголовка
03	M *Если закодиро-ванный структур-ный элемент включен*	Данные о структурном элементе		Var		
	M Если закодиро-ванный структур-ный элемент включен	*Закодированный структурный элемент*	999 Макс.	Var	B	Формат определяется по усмотрению государства или организации выдачи
ГРУППА ДАННЫХ 10. Закодированные элементы защиты: ВЕЩЕСТВЕННЫЙ ЭЛЕМЕНТ(Ы)						
01	M *Если закодиро-ванный вещест-венный элемент включен*	Количество вещественных элементов	1	F	N	Цифры 1–9, указывающие количество уникальных закодированных вещественных элементов (охватывает элементы данных 02–04)
02	M *Если закодиро-ванный вещест-венный элемент включен*	Информация о заголовке	TBD	TBD	N	Определяются детали
03	M *Если закодиро-ванный вещест-венный элемент включен*	Данные о вещественном элементе		Var		
	M Если закодиро-ванный вещест-венный элемент включен	*Закодированный вещественный элемент*	999 Макс.	Var	B	Формат определяется по усмотрению государства или организации выдачи

Элемент данных	Факультат. или обязат.	Название элемента данных	Коли-чество байтов	Фиксир. или перемен.	Тип кодиро-вания	Требования к кодированию
ГРУППА ДАННЫХ 11. Дополнительные персональные данные						
См. указатель элементов данных: дополнительные персональные данные [см. п. 12.1.2]						
ГРУППА ДАННЫХ 12. Дополнительные данные о документе						
См. указатель элементов данных: дополнительные данные о документе [см. п. 12.1.3]						
ГРУППА ДАННЫХ 13. Факультативные данные						
См. указатель элементов данных: факультативные данные [см. п. 12.1.4]						
ГРУППА ДАННЫХ 14. Зарезервировано для будущего использования						
Зарезервировано						
ГРУППА ДАННЫХ 15. Информация об открытом ключе активной аутентификации						
Информация об открытом ключе активной аутентификации приводится в разделе IV настоящего тома "PKI для машиносчитываемых проездных документов с доступом к ICC только для чтения"						
ГРУППА ДАННЫХ 16. Уведомляемое лицо(а)						
См. указатель элементов данных: данные об уведомляемом лице(ах) [см. п. 12.1.5]						

12.1.2 *Группа данных 11 (DG11)*. Элементы данных и их формат в **DG11 "Дополнительные персональные данные"** указаны ниже.

A – буквенный знак [a..z, A..Z], N – цифровой знак [0..9], S – специальный знак ['<' ' '], B – 8-битные двоичные данные (любые, кроме A, N или S), F – поле фиксированной длины, Var – поле переменной длины.

ГРУППА ДАННЫХ 11. Дополнительные персональные данные						
Элемент данных	**Факультат. или обязат.**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. или перемен.**	**Тип кодиро-вания**	**Требования к кодированию**
01	O	Имя владельца (полностью)				
	M, если элемент данных 01 включен	*Основной и вторичный идентификаторы*	99 Макс.	Var	A,S	Знаки-заполнители (<) ставятся согласно МСЗ. В конце строки заполнители не ставятся. Усечение не допускается
02	O	Другое имя (имена)				
		Основной и вторичный идентификаторы	99 Макс.	Var	A,S	Знаки-заполнители (<) ставятся согласно МСЗ. В конце строки заполнители не ставятся. Усечение не допускается
03	O	Личный номер				
		Личный номер	99 Макс.	Var	A,N,S	Текст произвольного формата
04	O	Место рождения				
		Место рождения	99 Макс.	Var	A,N,S	Текст произвольного формата

ГРУППА ДАННЫХ 11. Дополнительные персональные данные						
Элемент данных	**Факультат. или обязат.**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. или перемен.**	**Тип кодиро-вания**	**Требования к кодированию**
05	O	Адрес				
		Адрес	99 Макс.	Var	A,N,S	Текст произвольного формата
06	O	Полная дата рождения				
		Дата рождения	8	F	N	CCYYMMDD
07	O	Телефон				
	M, если элемент данных 07 включен	*Телефон*	99 Макс.	Var	N,S	Текст произвольного формата
08	O	Профессия				
	M, если элемент данных 08 включен	*Профессия*	99 Макс.	Var	A,N,S	Текст произвольного формата
09	O	Должность				
	M, если элемент данных 09 включен	*Должность*	99 Макс.	Var	A,N,S	Текст произвольного формата
10	O	Персональное резюме				
	M, если элемент данных 10 включен	*Персональное резюме*	99 Макс.	Var	A,N,S	Текст произвольного формата
11	O	Доказательство гражданства		Var		
	M, если элемент данных 11 включен	*Информация о гражданстве*	9999999 Макс.	Var	B	Изображение документа о гражданстве форматируется согласно ИСО/МЭК 10918-1
12	O	Другой действительный проездной документ(ы)		Var		
	M, если элемент данных 12 включен	*Номер проездного документа*	99 Макс.		A,N,S	Текст произвольного формата, отделяемый знаком <

ГРУППА ДАННЫХ 11. Дополнительные персональные данные						
Элемент данных	**Факультат. или обязат.**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. или перемен.**	**Тип кодиро-вания**	**Требования к кодированию**
13	O	Информация о задержании		Var		
	M, если элемент данных 13 включен	*Информация о задержании*	999 Макс.	Var	A,N,S	Текст произвольного формата

12.1.3 *Группа данных 12 (DG12).* Элементы данных и их формат в **DG12 "Дополнительные данные о документе"** указаны ниже.

A – буквенный знак [a..z, A..Z], N – цифровой знак [0..9], S – специальный знак [‘<’ ‘ ’], B – 8-битные двоичные данные (любые, кроме A, N или S), F – поле фиксированной длины, Var – поле переменной длины.

ГРУППА ДАННЫХ 12. Дополнительные данные о документе						
Элемент данных	**Факультат. или обязат.**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. или перемен.**	**Тип кодиро-вания**	**Требования к кодированию**
01	O	Полномочный орган выдачи				
		Полномочный орган выдачи	99 Макс.	Var	A,N,S	Текст произвольного формата
02	O	Дата выдачи	8	F	N	Дата выдачи документа, т. е. YYYYMMDD
03	O	Другое включенное лицо(а)				** Действителен только с МСВ **
		Данные о другом лице	99 Макс.	Var	A,N,S	Текст произвольного формата
04	O	Подтвердительная надпись(и)/ замечание(я)				
		Подтвердительная надпись(и)/ замечание(я)	99 Макс.	Var	A,N,S	Текст произвольного формата
05	O	Налоговые/выездные требования				
		Налоговые/выездные требования	99 Макс.	Var	A,N,S	Текст произвольного формата
06	O	Изображение передней стороны МСПД				
		Изображение МСПД (передняя сторона)	9999999 Макс.	Var	B	Форматируется согласно ИСО/МЭК 10918-1
07	O	Изображение задней стороны МСПД				
		Изображение МСПД (задняя сторона)	9999999 Макс.	Var	B	Форматируется согласно ИСО/МЭК 10918-1

ГРУППА ДАННЫХ 12. Дополнительные данные о документе						
Элемент данных	**Факультат. или обязат.**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. или перемен.**	**Тип кодиро-вания**	**Требования к кодированию**
08	O	Время персонализации				
		Время персонализации документа		F	F 14N	ccyymmddhhmmss
09	O	Серийный номер персонализации				
		Серийный номер устройства персонализации		Var	V 99ANS	Произвольный формат

12.1.4 *Группа данных 13 (DG13).* Элементы данных и их формат в **DG13 "Факультативные данные"** указаны ниже.

A – буквенный знак [a..z, A..Z], N – цифровой знак [0..9], S – специальный знак [‘<’ ‘ ’], B – 8-битные двоичные данные (любые, кроме A, N или S), F – поле фиксированной длины, Var – поле переменной длины.

ГРУППА ДАННЫХ 13. Факультативные данные						
Элемент данных	**Факультат. или обязат.**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. или перемен.**	**Тип кодиро-вания**	**Требования к кодированию**
TBD	O	Факультативные данные		Var		По усмотрению государства или организации выдачи

12.1.5 *Группа данных 16 (DG16).* Элементы данных и их формат в **DG16 "Уведомляемое лицо(а)"** указаны ниже.

A – буквенный знак [a..z, A..Z], N – цифровой знак [0..9], S – специальный знак [‘<’ ‘ ’], B – 8-битные двоичные данные (любые, кроме A, N или S), F – поле фиксированной длины, Var – поле переменной длины.

ГРУППА ДАННЫХ 16. Уведомляемое лицо(а)						
Элемент данных	**Факультат. или обязат.**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. или перемен.**	**Тип кодиро-вания**	**Требования к кодированию**
01	M, *если DG 16 включена*	Количество идентифицируемых лиц	2	F	N	Указывает количество лиц, включенных в эту группу данных
02	M, *если DG 16 включена*	Записанные данные о дате	8	F	N	Записанная дата уведомления; формат = CCYYMMDD
03	M, *если DG 16 включена*	Имя уведомляемого лица *Основной и вторичный идентификаторы*		Var	A,S	Знаки-заполнители (<) ставятся согласно МСЗ. Усечение не допускается

ГРУППА ДАННЫХ 16. Уведомляемое лицо(а)						
Элемент данных	**Факультат. или обязат.**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. или перемен.**	**Тип кодиро-вания**	**Требования к кодированию**
04	M, *если элемент данных 03 включен*	Номер телефона уведомляемого лица		Var	N,S	Номер телефона в международной форме (код страны и местный номер)
05	M	Адрес уведомля-емого лица		Var	A,N,S	Текст произвольного формата

13. Принципы безопасности

13.1 Дополнительная информация о принципах безопасности, применяемых для защиты записанной логической структуры данных (LDS) и обеспечения возможности подтверждения принимающим государством или утвержденной принимающей организацией аутентичности и целостности данных, считываемых с факультативного устройства увеличения емкости, содержится в разделе IV "*PKI*".

ИНФОРМАЦИЯ О ЗАГОЛОВКЕ И ПРИСУТСТВИИ ГРУПП ДАННЫХ

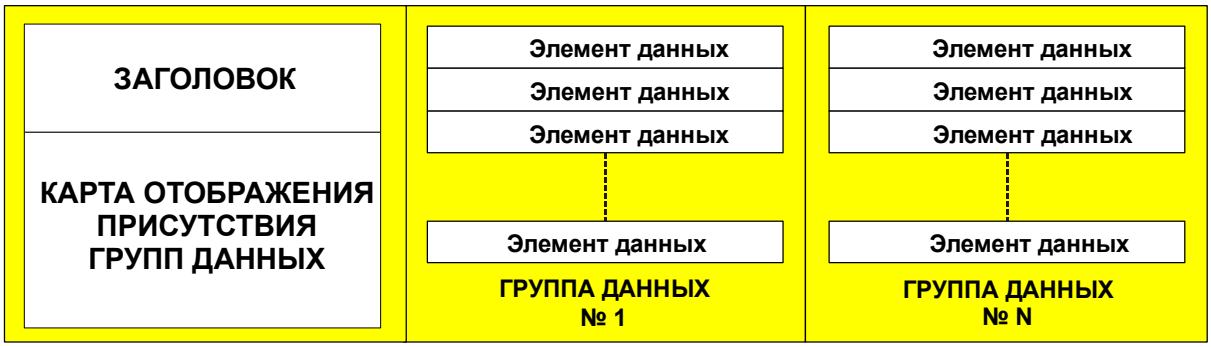


Рис. III-3. Информация об обязательном заголовке и присутствии групп данных

14. Принципы отображения применительно к технологии расширения объема данных на бесконтактной ИС

14.1 *Упорядочение LDS*. Только схема произвольного упорядочения позволяет обеспечивать международную интероперабельность. Она описывается в Нормативном добавлении 1 к настоящему разделу.

14.2 *Схема произвольного упорядочения.* Схема произвольного упорядочения позволяет записывать группы данных и элементы данных, следуя произвольному порядку в соответствии со способностью факультативной технологии увеличения емкости, обеспечивать прямое извлечение конкретных элементов данных даже в случае их беспорядочной записи. Элементы данных переменной длины кодируются как *значения длины* и длина указывается в нотации ASN.1.

Карта отображения *обязательного* заголовка и присутствия групп данных включена. Эта информация хранится в EF.COM. См. добавление 1.

14.2.1 *Заголовок.* Заголовок содержит нижеуказанную информацию, позволяющую принимающему государству или утвержденной принимающей организации локализовать и декодировать различные группы данных и элементы данных, содержащиеся в блоке данных, записанном государством или организацией выдачи.

ИДЕНТИФИКАТОР ПРИЛОЖЕНИЯ (AID)
НОМЕР ВЕРСИИ LDS
НОМЕР ВЕРСИИ UNICODE

14.2.2 *Номер версии LDS.* Номер версии LDS определяет версию формата LDS[8]. Точный формат, подлежащий использованию для хранения этого значения, будет определен в добавлении, касающемся технологии отображения. Стандартным форматором номера версии LDS является "aabb", где:

"aa" – число (01–99), идентифицирующее версию LDS (т. е. существенное добавление к LDS);

"bb" – число (01-99), идентифицирующее модификацию LDS.

14.2.3 *Номер версии Unicode*[9]. Номер версии Unicode определяет применяемый метод кодирования при записи буквенных, цифровых и специальных знаков, включая национальные знаки. Точный формат, подлежащий использованию для хранения этого значения, будет определен в добавлении, касающемся технологии отображения. 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 знакам 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 обновления).

Примечание. Исторически сложилось так, что нумерация внутри каждого поля (т. е. a, b, c) не обязательно является последовательной.

14.3 *Карта отображения присутствия групп данных.* Карта отображения присутствия групп данных (DGPM) содержит информацию, позволяющую принимающему государству или утвержденной принимающей организации определять, какие группы данных присутствуют в блоке данных, записанных государством или организацией выдачи.

8. Предполагается, что в будущем стандартная организация LDS будет модифицироваться; такие модификации будут рассматриваться в публикуемых поправках к спецификациям ИКАО. Каждой модификации будет присваиваться номер версии, с тем чтобы принимающие государства и утвержденные принимающие организации могли точно декодировать все версии LDS.

9. *Unicode* базируется на ИСО/МЭК 10646. Подробная информация о *Unicode* содержится на сайте www.unicode.org.

14.3.1 DGPM, используемая при внедрении интегральных схем, состоит из списка "тегов" согласно правилам идентификации элементов данных, записанных на контактной и бесконтактной интегральной схеме(ах), в котором каждый тег указывает, записана ли конкретная группа данных в блоке данных, записанных государством или организацией выдачи. Эта DGPM реализуется как список тегов; тег = '5C' в EF.COM. См. добавление 1.

Группа данных "n" ТЕГ

•
•

Группа данных "m" ТЕГ

Присутствие ТЕГА = Группа данных присутствует.
Отсутствие ТЕГА = Группа данных отсутствует.

14.4 *Карты отображения присутствия элементов данных.* Аналогичная концепция карт отображения присутствия используется применительно к ряду групп данных, содержащих серию подчиненных элементов данных, которые могут включаться по усмотрению государства или организации, делающих запись. Эти карты отображения присутствия, именуемые картами отображения присутствия элементов данных (DEPM), размещаются в начале этих конкретных групп данных, допускающих факультативное расширение объема данных, как иллюстрируется на рис. III-4.

Группы данных, требующие использования карты отображения присутствия элементов данных, определяются в добавлении 1.

Рис. III-4. Карта отображения присутствия элементов данных

14.4.1 DEPM содержит информацию, позволяющую принимающему государству или утвержденной принимающей организации определить, какие элементы данных присутствуют в группе данных.

14.4.2 DEPM состоит из списка "тегов" согласно правилам идентификации элементов данных, записанных на контактной и бесконтактной интегральной схеме(ах), в котором каждый тег указывает, записан ли конкретный элемент данных в группе данных. Эта форма DEPM кодируется как список тегов в соответствующей группе данных.

Элемент данных “n” ТЕГ

•
•

Элемент данных “m” ТЕГ

Присутствие ТЕГА = Элемент данных присутствует.
Отсутствие ТЕГА = Элемент данных отсутствует.

Примечание. Количество байтов, выделяемых для DEPM, определяется в нормативном добавлении к разделу III.

Нормативное добавление 1 к разделу III

ОТОБРАЖЕНИЕ LDS НА БЕСКОНТАКТНЫХ ИНТЕГРАЛЬНЫХ СХЕМАХ (ИС) С ИСПОЛЬЗОВАНИЕМ МЕТОДА ПРЕДСТАВЛЕНИЯ ДАННЫХ ПУТЕМ ПРОИЗВОЛЬНОГО ДОСТУПА

A.1 *Сфера применения.* В добавлении 1 определяются текущие спецификации, регулирующие отображение логической структуры данных – LDS [версия 1.7] на интегральных схемах (ИС) МСПД с использованием метода *представления данных путем произвольного доступа*, с целью обеспечения расширения емкости машиносчитываемых данных по усмотрению государства или организации выдачи.

Примечание. Спецификации, приводимые в добавлении 1, применяются только к LDS, поддерживающей биометрическую аутентификацию без использования карточки, т. е. в тех случаях, когда МСПД предоставляет LDS для машинного подтверждения личности, при котором требуется, чтобы МСПД был только носителем данных.

A.2 *Нормативные ссылки.* См. раздел III.2.

A.3 *Представление файла путем произвольного доступа.* Метод представления файла путем произвольного доступа определен исходя из следующих соображений и предположений:

- Поддерживать широкий спектр реализации. LDS включает множество факультативных элементов данных. Эти элементы включаются для упрощения аутентификации МСПД, аутентификации законного владельца и ускорения процесса обработки в пунктах проверки документов/лиц.

- Структура данных должна поддерживать:
  – ограниченный или обширный набор элементов данных;
  – многократное повторение конкретных элементов данных;
  – постоянную эволюцию конкретных видов реализации.

- Поддерживать по крайней мере один набор данных прикладной программы.

- Допускать использование других национальных специализированных приложений.

- Поддерживать факультативный метод активной аутентификации документа с использованием хранимой ассиметричной пары ключей и ассиметричного шифрования данных на чипе. Подробная информация об активной аутентификации приводится в разделе IV "*PKI*".

- Поддерживать быстрый доступ к отдельным элементам данных для ускорения процесса оформления владельца документа:

  – непосредственный доступ к необходимым элементам данных;
  – прямой доступ к шаблонам данных, в частности, к биометрическим данным.

A.3.1 В целях обеспечения интероперабельности в добавлении 1 определяются:

- протокол инициализации, предотвращения коллизий и передачи данных;
- набор команд;
- использование команд, включая ссылки на защиту;
- структура файла для применения LDS МСПД ИКАО;
- набор знаков.[10]

A.4 *Требования к защите.* Для надежного обмена данными необходимо обеспечивать целостность и аутентичность данных. Подробные спецификации содержатся в разделе IV "*PKI*".

A.5 *Совместимость с существующими международными стандартами.* Совместимость с существующими стандартами имеет важнейшее значение для содействия реализации и обеспечения интероперабельности. Поэтому настоящие спецификации обеспечивают максимальную совместимость со стандартами, упомянутыми в разделе III.2.

A.6 *Определения.* См. раздел III.3.

A.7 *Физические характеристики.* Физические характеристики документа соответствуют физическим характеристикам, указанным в томе 1.

A.8 *Местоположение и размеры зон сцепления*

A.8.1 Размер зоны сцепления соответствует стандарту ИСО/МЭК 14443.

A.8.2 Местоположение зоны сцепления определяется в соответствии со стандартом ИСО/МЭК 14443 для документов размера ПД-1 и, по усмотрению выдающего органа, – для документов ПД-3.

A.9 *Электронные сигналы.* Мощность радиочастотного сигнала и интерфейс сигналов определяются в стандарте ИСО/МЭК 14443.

A.10 *Протоколы передачи и ответ на запрос*

A.10.1 *Протокол передачи.* МСПД поддерживает протокол полудуплексной передачи, определяемой стандартом ИСО/МЭК 14443-4. МСПД может поддерживать протокол передачи либо типа A, либо типа B.

A.10.2 *Запрос команды.* ИС отвечает на запрос команды типа A (REQA) или запрос команды типа B (REQB), давая ответ на запрос типа A (ATQA) или ответ на запрос типа B (ATQB) в зависимости от конкретного случая.

10. Используется стандарт кодирования UTF-8. Большинство элементов данных, используемых в LDS, представляют собой основные знаки латинского алфавита (ASCII) или двоичные знаки. Такие элементы данных, как "имя, написанное буквами национального алфавита", "место рождения" и т. д., не всегда могут кодироваться с помощью кодового набора для знаков латинского алфавита. Поэтому знаки кодируются с использованием стандарта Unicode: UTF-8. Это кодирование с переменной длиной, сохраняющее транспарентность стандарта ASCII. UTF-8 полностью согласуется со стандартом Unicode и ИСО/МЭК 10646. UTF-8 использует 1 байт для кодирования стандартных знаков ASCII (кодовое значение 0…127). Многие знаки неидеографического письма представляются 2 байтами. Остальные знаки представляются 3 или 4 байтами. Использование UTF-8 обеспечивает простое включение знаков, не соответствующих ASCII, без непроизводительных издержек 2, 3 или 4-байтового представления всех знаков.

A.10.3 *Выбор прикладной программы.* Карточки на ИС поддерживают по крайней мере одну прикладную программу машиносчитываемого проездного документа (МСПД):

- Одна прикладная программа состоит из данных, записанных государством или организацией выдачи [группы данных 1–16], и данных системы защиты (EF.SOD), необходимых для подтверждения целостности данных, созданных выдающим органом и хранящихся в DF1. Данные системы защиты (EF.SOD) состоят из используемых хэш-групп данных. Подробная информация приводится в разделе IV "*PKI*".

- Вторая прикладная программа (не поддерживается в настоящем издании части 1 документа Doc 9303) будет состоять из данных, включаемых принимающими государствами или утвержденными принимающими организациями [группы данных 17–19].

Кроме того, государства или организации выдачи могут пожелать добавить другие прикладные программы. Структура файла вмещает дополнительные прикладные программы, однако описание делателей таких прикладных программ выходит за рамки этого нормативного добавления.

Прикладные программы МСПД выбираются путем идентификации прикладной программы (AID) в качестве зарезервированного наименования DF. AID состоит из зарегистрированного идентификатора прикладной программы (RID), установленного ИСО в соответствии со стандартом ИСО/МЭК 7816-5, и собственного добавления к идентификатору прикладной программы (PIX), указанного в настоящем документе.

RID **=** ‘A0 00 00 02 47’.
Прикладная программа хранящихся данных выдающего органа использует PIX = ‘1001’.

A.10.4 *Защита*

Группы данных 1–15 включительно защищены от записи. Хэш для каждой используемой группы данных хранится в данных системы защиты (EF.SOD). Данные системы защиты также содержат цифровую подпись используемых хэшей. См. раздел IV "*PKI*".

Только государство или организация выдачи имеют доступ к этим группам данных с правом записи. Таким образом, требования в отношении обмена данными не предъявляются и средства, используемые для достижения защиты от записи, не являются частью этой спецификации.

Группа данных 16 защищена от записи. Только государство или организация выдачи имеют доступ к элементам данных этой группы с правом записи.

Группы данных 17, 18 и 19 подлежат определению в версии 2 LDS.

A.11 *Структура файла*. Информация о карточке на интегральной схеме хранится в файловой системе, определяемой стандартом ИСО/МЭК 7816-4. Система карточных файлов организуется иерархически и содержит выделенные файлы (DF) и элементарные файлы (EF). Выделенные файлы DF содержат элементарные файлы или другие выделенные файлы. Факультативный[11] мастер-файл (MF) может составлять основу файловой системы.

DF1 (обязательный), определяемый настоящей спецификацией, содержит выдаваемые элементы данных. Для прикладной программы этот DF имеет название ‘A0 00 00 02 47 10 01’

11. Потребность в мастер-файле обуславливается выбором операционных систем.

(зарегистрированный RID и PIX) и отбирается по этому названию. Если карточка имеет MF, он может помещаться в любом месте дерева DF, присоединяемого к MF карточки.

В каждой прикладной программе может быть определенное количество "групп данных". Прикладная программа государства или организации выдачи может иметь до 16 групп данных. Группа данных 1 [DG1], составляющая машиносчитывающую зону МСЗ, и группа данных 2, составляющая закодированное изображение лица, являются обязательными. Все остальные группы данных являются факультативными. Прикладная программа принимающего государства или утвержденной принимающей организации может иметь три группы данных (DG17–19). Эти три группы являются факультативными. Все группы данных представляются в форме шаблонов данных и имеют индивидуальные теги ASN.1.

A.11.1 *DF1*

DF1 имеет один файл (называется EF.COM), который содержит общую информацию для прикладной программы. Кратким идентификатором, служащим в качестве файлового идентификатора этого файла, является 30 (‘1E’). Этот файл содержит информацию о версии LDS, информацию о версии Unicode и перечень групп данных, имеющихся для прикладной программы. Каждая группа данных хранится в одном транспарентном EF. Файлы EF адресуются краткими файловыми идентификаторами, указанными в таблице IIIA-1. EF имеют названия для этих файлов, которые составляются согласно схеме: номер n, EF.DGn, где n – номер группы данных. Названием файла EF, содержащего данные системы защиты, является EF.SOD. Графическое представление структуры файлов делается на рис. IIIA-1.

Каждая группа данных состоит из серии объектов данных, входящих в шаблон. Каждая группа данных хранится в отдельном элементарном файле (EF). Индивидуальные объекты данных могут непосредственно извлекаться из группы данных после установления относительной позиции в транспарентном файле.

Файлы содержат элементы данных в качестве объектов данных внутри шаблона. Структура и кодирование объектов данных определяются стандартами ИСО/МЭК 7816-4 и 7816-6. Каждый объект данных имеет идентификационный тег, который устанавливается по шестнадцатеричной системе кодирования (например, ‘5A’). Теги, определяемые в настоящем добавлении, используют вариант кодирования в смешанной структуре. Каждый объект данных имеет уникальный тег, длину и значение. Объекты данных, которые могут присутствовать в файле, идентифицируются как обязательные (M) или факультативные (O). Определение содержит конкретную ссылку на номер элемента данных, определяемый в разделе 13. По мере возможности используются межотраслевые теги. Следует отметить, что конкретное определение и формат некоторых тегов изменены для приведения их в соответствие с прикладной программой МСПД. Например:

Тег 5A определяется как номер документа, а не как номер основного счета, и имеет формат F9N, а не V19N.

Тег 5F20 (имя владельца карточки) переопределен как "Имя владельца" длиной до 39 знаков, кодируемых согласно формату, указанному в Doc 9303.

Тег 65 определяется как отображаемая фотография, а не как данные, относящиеся к владельцу карточки.

По мере необходимости дополнительные теги определяются в диапазоне 5F01–5F7F.

Таблица III-A1. Обязательная прикладная программа государства или организации выдачи

Группа данных	Название EF	Краткий идентификатор EF	FID	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’
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’
Данные системы защиты	$EF.SO_D$	‘1D’	‘01 1D’	‘77’

A.12 *Набор команд.* Минимальный набор команд, поддерживаемый МСПД:

– SELECT;
– READ BINARY.

Обязательные и факультативные параметры команд указаны в п. A.17 настоящего добавления. В п. A.23 описывается вариант команды для доступа к файлам длиной более 32 767 байтов.

Все команды, форматы и коды их возврата определяются стандартом ИСО/МЭК 7816-4. См. п. A.22 настоящего добавления.

Признается, что для надежной загрузки и обновления данных, создания надлежащих условий безопасности и выполнения факультативных положений по защите, указанных в разделе IV "*PKI*", требуются дополнительные команды. Такие команды выходят за рамки настоящей спецификации в отношении интероперабельности, но могут включать:

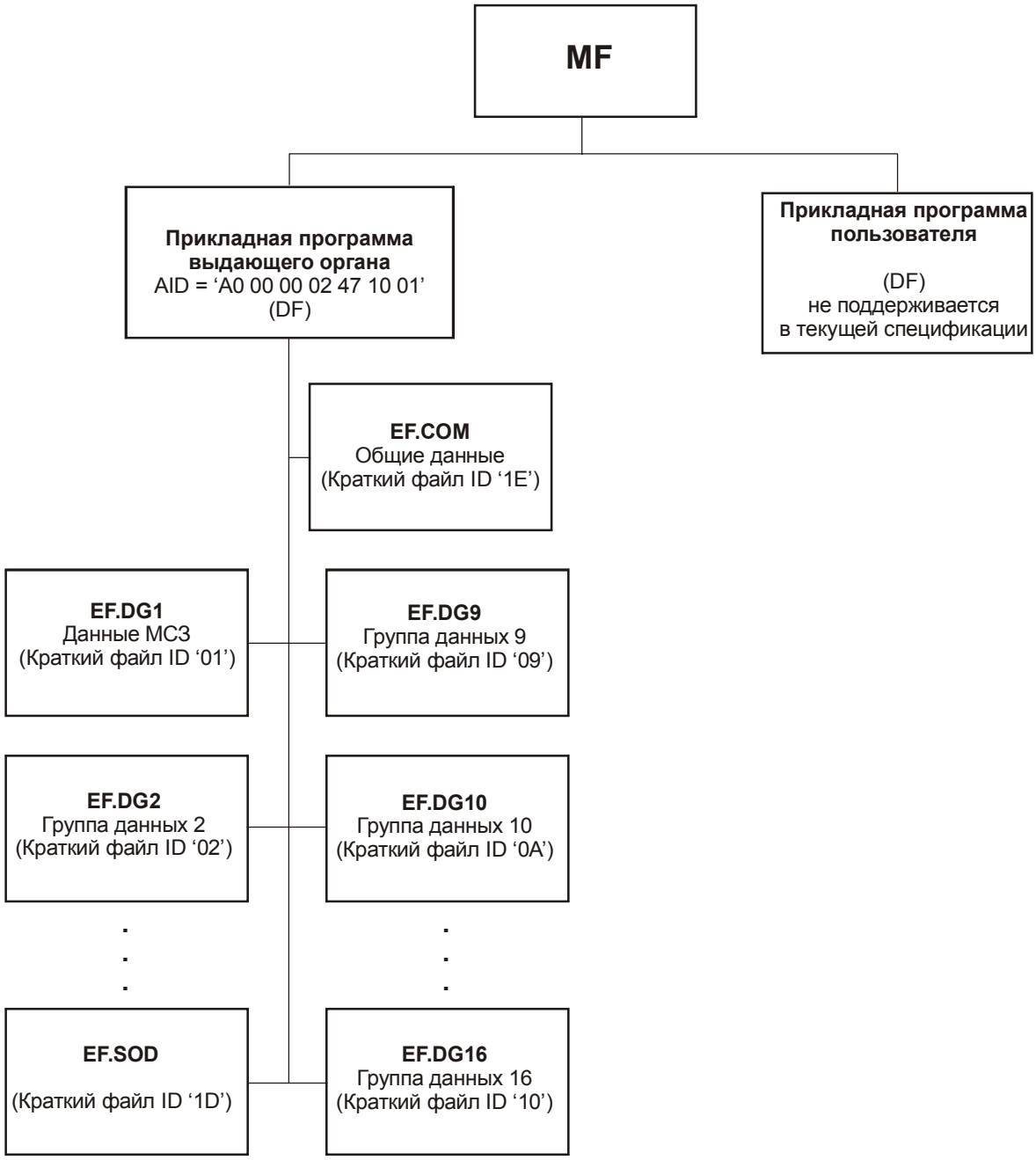

MF
Прикладная программа выдающего органа
AID = ‘A0 00 00 02 47 10 01’
(DF)
Прикладная программа пользователя
(DF)
не поддерживается
в текущей спецификации
EF.COM
Общие данные
(Краткий файл ID ‘1E’)
EF.DG1
Данные МСЗ
(Краткий файл ID ‘01’)
EF.DG9
Группа данных 9
(Краткий файл ID ‘09’)
EF.DG2
Группа данных 2
(Краткий файл ID ‘02’)
EF.DG10
Группа данных 10
(Краткий файл ID ‘0A’)
EF.SOD
(Краткий файл ID ‘1D’)
EF.DG16
Группа данных 16
(Краткий файл ID ‘10’)

Рис. IIIA-1

– GET CHALLENGE;
– EXTERNAL AUTHENTICATE;
– VERIFY CERTIFICATE.

A.13 *Данные прикладной программы выдающего органа*

Данные прикладной программы выдающего органа, AID = ‘A0 00 00 02 47 10 01’. Прикладная программа выдающего органа состоит из двух обязательных групп данных и четырнадцати факультативных групп данных. Информация, общая для всех групп данных, хранится в прикладном шаблоне ‘60’. Этот шаблон хранится в обязательном файле EF.COM.

A.13.1 *EF.COM. Общие элементы данных (краткий файл ID = 30 (‘1E’))*

Тег прикладного шаблона ‘60’ – информация об уровне прикладной программы.

Примечание. Этот шаблон в настоящее время содержит только информацию об уровнях пересмотренных версий и список тегов ‘5C’. Структура шаблона определена для поддержки будущих разработок, таких, как динамические подписи и шаблоны биометрической информации (BIT). В этом шаблоне могут иметь место нижеуказанные элементы данных.

Тег	**Дл.**	**Значение**
‘5F01’	04	Номер версии LDS в формате aabb, где aa обозначает версию LDS, a bb – уровень модификации
‘5F36’	06	Номер версии Unicode в формате aabbcc, где aa обозначает основную версию, bb – вспомогательную версию, a cc – уровень версии программного продукта
‘5C’	X	Список тегов. Список всех имеющихся групп данных

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.13.2 *EF.DG1. Информационный тег машиносчитываемой зоны = ‘61’ – обязательная информация*

Этот EF содержит обязательную информацию машиносчитываемой зоны (МСЗ) документа в шаблоне ‘61’. Шаблон содержит один объект данных (МСЗ в объекте данных ‘5F1F’). Объект данных МСЗ является составным элементом данных, который идентичен информации МСЗ, напечатанной в документе знаками OCR-B.

Тег	Дл.	Значение
‘5F1F’	F	Объект данных МСЗ как составной элемент данных (обязательный). (Этот элемент данных содержит все тринадцать примитивных полей – от типа документа до составной контрольной цифры)

Элемент данных МСЗ имеет нижеуказанную структуру.

Следует отметить, что теги не используются в рамках этого составного элемента данных. Они включаются только для ссылок. Их можно использовать после разбивки объекта данных на индивидуальные элементы данных.

Поле	Содержание	Обязательн./ факультат.	Формат	Пример	Тег (только для информации)
1	Тип документа	M	F 2A,S	P<	5F03
2	Государство или организация выдачи	M	F 3A,S	ATA	5F28
3	Имя владельца[12]	M	F 39ANS	Smith<<John<T	5B
4	Номер документа	M	F 9ANS[13]	123456789	5A
5	Контрольная цифра – номер документа	M	F 1N,S	1 или <	5F04

12. Правила усечения имен, длиной более 39 знаков, содержатся в томе 1.
13. Если длина номера документа превышает 9 знаков, то в следующем поле контрольной цифры (поле 5) ставится знак ‘<‘, а остальные цифры номера документа ставятся в факультативном поле данных, следующим сразу за контрольной цифрой номера документа. В вышеприведенном примере общая длина номера документа составляет 12 (значение = 123456789012), а контрольная цифра = 1.

Поле	Содержание	Обязательн./ факультат.	Формат	Пример	Тег (только для информации)
6	Гражданство	M	F 3A,S	HMD	5F2C
7	Дата рождения	M	F 6N,S	740622 (yymmdd)	5F57
8	Контрольная цифра – дата рождения	M	F 1N	2	5F05
9	Пол	M	F 1A,S	F, M, или <	5F35
10	Дата истечения срока действия или действителен до (дата)	M	F 6N	101231 (yymmdd)	59
11	Контрольная цифра – дата истечения срока действия	M	F 1N	3	5F06
12	Факультативные данные	M	F14ANS	0121	53
13	Контрольная цифра – факультативные данные (только документы ID-3)	M	F 1N	5	5F02
14	Контрольная цифра – составная	M	F 1N	4	5F07

Ниже приводится пример DG1 с использованием этой информации. Длина элемента данных MC3 составляет 88 байтов (‘58’).

‘61’ *‘5B’* **‘5F1F’** *‘58’*
P<ATASMITH<<JOHN<T<<<<<<<<<<<<<<<<<<<<<<<<123456789<HMD7406222M10123130121<<<<<<<<<<54

Другой пример:

‘61’ *‘5B’* **‘5F1F’** *‘58’*
P<NLDMEULENDIJK<<LOES<ALBERTINE<<<<<<<<<<<<XA00277324NLD7110195F0610010123456782<<<<<08

A.13.3 *EF.DG2 – EF.DG4 (Один EF для каждой DG) Теги биометрических шаблонов = ‘’75’ ‘63’ ‘76’*

Группы DG2–DG4 используют вариант стандарта ИСО/МЭК 7816-11, предусматривающий вложение без использования карточки (таблица C-10), для обеспечения возможности хранения нескольких биометрических образцов определенного типа, соответствующих общему формату файлов обмена биометрическими данными (CBEFF), NISTR 6529a. Биометрический подзаголовок определяет тип имеющейся биометрической информации и конкретную биометрическую характеристику.

Каждый вложенный шаблон имеет нижеуказанную структуру.

Примечания:

Вариант стандарта ИСО/МЭК 7816-11, предусматривающий вложение (таблица C-10), должен использоваться всегда и даже при кодировании одного биометрического шаблона. Последний случай указывается числовым кодированием n=1.

Для указания CBEFF используется установленный по умолчанию идентификатор OID. Элемент данных '06', указанный в стандарте ИСО/МЭК 7816-11, в эту структуру не включается. Аналогичным образом в структуре не определяется полномочие на распределение тегов.

В целях обеспечения интероперабельности первой биометрической информацией, записываемой в каждой группе данных, является интероперабельный на международном уровне блок биометрических данных (JTC1/SC37 ИСО/МЭК). См. раздел II.

Для секретности блок биометрических данных может шифроваться с использованием шаблонов безопасного обмена сообщениями, определяемых в добавлении D к стандарту 7816-11. Такая реализация не входит в рамки настоящей спецификации.

Тег	**Дл.**	**Значение**				
'7F61'	**X**	**Шаблон группы биометрической информации**				
		Тег	**Дл.**	**Значение**		
		'02'	1	Целое число – количество примеров этого типа биометрического параметра		
		'7F60'	X	Первый шаблон биометрической информации		
			Тег	**Дл.**		
			'A1'	X	Шаблон заголовка биометрической информации (BHT)	
				Тег	**Дл.**	**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, обязательная для DG3, DG4)
				'83'	'07'	Дата и время создания (факультативная информация)
				'84'	'08'	Срок действия (с … по) (факультативная информация)
				'86'	'02'	Создатель контрольных биометрических данных (PID) (факультативная информация)
				'87'	'02'	Владелец формата (обязательная информация)
				'88'	'02'	Тип формата (обязательная информация)
			'5F2E' или '7F2E'	x	Биометрические данные (закодированные по правилам владельца формата), именуемые также блоком биометрических данных (BDB)	
		Тег	**Дл.**			
		'7F60'	X	Второй шаблон биометрической информации		
			Тег	**Дл.**		
			'A1'	X	Шаблон заголовка биометрической информации (BHT)	
				Тег	**Дл.**	**Значение**
				'80'	'02'	Версия '0101' заголовка ИКАО (факультативная информация) – версия основного формата заголовка CBEFF
				'81'	'01'	Биометрический тип (факультативная информация)

Тег	Дл.	Значение				
				‘82’	‘01’	Биометрический подтип (факультативная информация для DG2, обязательная для DG3, 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’	x	Биометрические данные (закодированные по правилам владельца формата), именуемые также блоком биометрических данных (BDB)	

Каждый отдельный шаблон биометрической информации имеет нижеуказанную структуру. Заданные теги шаблонов заголовков биометрической информации и их заданные значения являются тем минимумом, который должен поддерживаться каждой реализацией.

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’* ‘000A’
‘88’ *‘02’* ‘0004’
‘5F2E’ *‘823162’* ‘… 12642 байтов биометрических данных …’

A.13.4 *EF.DG5 – EF.DG7 (один EF для каждой DG). Шаблон отображаемого изображения*

Тег = ‘65’ отображаемые фотографии Тег = ‘67’ отображаемая подпись или обычная отметка

Тег	Дл.	Значение
‘02’	1	Целое число – количество примеров этого типа отображаемого изображения (обязательная информация в первом шаблоне. Не используется в последующих шаблонах)

Тег	Дл.	Значение
‘5F40’ или ‘5F43’	X	Отображаемая фотография Отображаемая подпись или отметка

Пример. Шаблон изображения с длиной данных отображаемого изображения 2 000 байтов. Длина шаблона составляет 2 008 байтов (‘07D8’).

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

Для конкретного типа отображаемого изображения распознаются следующие владельцы форматов:

Отображаемое изображение	Владелец формата
Отображаемое изображение лица	ИСО/МЭК 10918, вариант JFIF
Отображаемый отпечаток пальца	ANSI/NIST-ITL 1-2000
Отображаемая подпись/обычная отметка	ИСО/МЭК 10918, вариант JFIF

A.13.5 *EF.DG8–EF.DG10. Элементы защиты с помощью машины, теги ‘68’ ‘69’ ‘6A’*

Эти три группы данных еще предстоит определить. Пока они предоставляются для временного собственного использования. Эти элементы данных могут использовать структуру, аналогичную структуре биометрических шаблонов.

Тег	Дл.	Значение
‘02’	1	Целое число – количество примеров этого типа шаблона (обязательная информация в первом шаблоне. Не используется в последующих шаблонах)
	x	Шаблон заголовка. Детали надлежит определить

A.13.6 *EF. DG11. Дополнительные персональные данные, тег = 6B*

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 знаки нелатинского шрифта.

Тег	Дл.	Значение
‘5C’	X	Список тегов с перечнем элементов данных в шаблоне
‘5F0E’	X	Полное имя владельца документа буквами национального алфавита. Кодируется по правилам Doc 9303
‘A0’	‘X’	Объект данных об именах, строящийся в зависимости от содержания
‘02’	01	Количество других имен
‘5F0F’	X	Другое имя, форматированное согласно Doc 9303. Объект данных повторяется столько раз, сколько указано в элементе данных ‘02’
‘5F10’	X	Личный номер
‘5F2B’	04	Полная дата рождения yyyymmdd (закодированные данные BCD)

Тег	Дл.	Значение
‘5F11’	X	Место рождения. Поля отделяются знаком ‘<‘
‘5F42’	X	Постоянный адрес. Поля отделяются знаком ‘<‘
‘5F12’	X	Телефон
‘5F13’	X	Профессия
‘5F14’	X	Должность
‘5F15’	X	Личное резюме
‘5F16’	X	Доказательство гражданства. Сжатое изображение согласно ИСО/МЭК 10918
‘5F17’	X	Номера других действительных ПД. Отделяются ‘<’
‘5F18’	X	Информация о задержании

В нижеуказанном примере показаны следующие персональные 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’* 1-612-555-1212
‘5F13’ *‘0C’* TRAVEL<AGENT

A.13.7 *EF.DG12. Дополнительные данные о документе, тег = 6C*

Это группа данных используется для представления дополнительной информации о документе. Все элементы данных в этой группе являются факультативными.

Тег	Дл.	Значение
‘5C’	X	Список тегов с перечнем элементов данных в шаблоне
‘5F19’	X	Орган выдачи
‘5F26’	‘04’	Дата выдачи. yyyymmdd (кодирование BCD)
‘A0’	X	Объект данных о других людях, строящийся в зависимости от содержания
‘02’	‘01’	Количество других людей
‘5F1A’	X	Имя другого лица, форматированное по правилам Doc 9303
‘5F1B’	X	Подтвердительные записи, замечания
‘5F1C’	X	Налоговые/выездные требования
‘5F1D’	X	Изображение передней части документа. Изображение согласно ИСО/МЭК 10918
‘5F1E’	X	Изображение задней части документа. Изображение согласно ИСО/МЭК 10918
‘5F55’	‘07’	Дата и время персонализации документа yyyymmddhhmmss
‘5F56’	X	Серийный номер системы персонализации

В следующем примере указывается государство выдачи (Соединенные Штаты Америки), дата выдачи (31 мая 2002 года) и одно другое лицо, включенное в документ (Brenda P Smith). Длина шаблона составляет 64 байта (‘40’).

‘6C’ *‘40’*

‘5C’ *‘06’* **‘5F19’ ‘5F26’ ‘5F1A’**
‘5F19’ *‘18’* UNITED STATES OF AMERICA
‘5F26’ *‘08’* 20020531
‘5F1A’ *‘0F’* SMITH<<BRENDA<P

A.13.8 *EF.DG13. Факультативные данные*

Эта группа данных зарезервирована для конкретных национальных данных. Ее формат определяет страна.

A.13.9 *EF.DG15. Информация об открытом ключе активной аутентификации, тег = ‘6F’*

Эта группа данных содержит информацию об открытом ключе активной аутентификации согласно RFC3280.

Тег	**Дл.**	**Значение**
‘6F’	X	См. раздел IV "*PKI"*

A.13.10 *EF.DG16. Уведомляемое лицо(а), тег ‘70’*

В этой группе данных указывается информация, связанная со срочным уведомлением. Она кодируется как серия шаблонов с использованием тег-обозначения ‘Ax’. Эти данные не подписываются, что позволяет владельцу документа обновлять их.

Тег	**Дл.**	**Значение**
‘02’	01	Количество шаблонов (указывается только в первом шаблоне)
‘Ax’	X	Начало шаблона, где x (x=1,2,3…) возрастает с каждым экземпляром
‘5F50’	‘04’	Записанная дата
‘5F51’	X	Имя лица
‘5F52’	X	Телефон
‘5F53’	X	Адрес

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

A.13.11 *EF.SOD LDS. Данные системы защиты, тег = ‘77’*

Этот EF содержит подписываемую структуру данных согласно RFC3369.

Тег	**Дл.**	**Значение**
‘77’	X	См. раздел IV "PKI"

A.14 *Прикладная программа принимающего государства*

Не поддерживается структурой LDS в настоящем издании части 1 документа Doc 9303.

A.15 *Используемые теги*

A.15.1 Нормативные теги, используемые в LDS

Тег	*Определение*	*Использование*
‘02’	Целое число	Биометрические и отображаемые шаблоны
‘5C’	Список тегов	EF.COM и многие другие
‘5F01’	Номер версии LDS	EF.COM
‘5F08’	Дата рождения (усеченная)	MC3
‘5F09’	Сжатое изображение (ANSI/NIST-ITL 1-2000)	Отображаемый отпечаток пальца
‘5F0A’	Элементы защиты. Закодированные данные	Элементы защиты (детализация TBD)
‘5F0B’	Элементы защиты. Структура	Элементы защиты (детализация TBD)
‘5F0C’	Элементы защиты	Элементы защиты (детализация TBD)
‘5F0E’	Полное имя (знаками национального алфавита)	Дополнительные персональные данные
‘5F0F’	Другие имена	Дополнительные персональные данные
‘5F10’	Личный номер	Дополнительные персональные данные
‘5F11’	Место рождения	Дополнительные персональные данные
‘5F12’	Телефон	Дополнительные персональные данные
‘5F13’	Профессия	Дополнительные персональные данные
‘5F14’	Должность	Дополнительные персональные данные
‘5F15’	Персональное резюме	Дополнительные персональные данные
‘5F16’	Доказательство гражданства (изображение 10918)	Дополнительные персональные данные

Тег	*Определение*	*Использование*
‘5F17’	Номера других действительных ПД	Дополнительные персональные данные
‘5F18’	Таможенная информация	Дополнительные персональные данные
‘5F19’	Орган выдачи	Дополнительные данные о документе
‘5F1A’	Другие лица в документе	Дополнительные данные о документе
‘5F1B’	Подтвердительные надписи/замечания	Дополнительные данные о документе
‘5F1C’	Налоговые/выездные требования	Дополнительные данные о документе
‘5F1D’	Изображение передней части документа	Дополнительные данные о документе
‘5F1E’	Изображение задней части документа	Дополнительные данные о документе
‘5F1F’	Элементы данных МСЗ	Объекты данных МСЗ
‘5F26’	Дата выдачи	Дополнительные данные о документе
‘5F2B’	Дата рождения (8 цифр)	Дополнительные персональные данные
‘5F2E’	Блок биометрических данных	Биометрические данные
‘5F36’	Уровень версии Unicode	EF.COM
‘5F40’	Шаблон сжатого изображения	Отображаемая фотография
‘5F42’	Адрес	Дополнительные персональные данные
‘5F43’	Шаблон сжатого изображения	Отображаемая подпись или отметка
‘5F50’	Записанная дата	Уведомляемое лицо
‘5F51’	Имя лица	Имя уведомляемого лица
‘5F52’	Телефон	Номер телефона уведомляемого лица
‘5F53’	Адрес	Адрес уведомляемого лица
‘5F55’	Дата и время персонализации документа	Дополнительные данные о документе
‘5F56’	Серийный номер системы персонализации	Дополнительные данные о документе
‘60’	Общие элементы данных	EF.COM
‘61’	Шаблон для группы данных МСЗ	
‘63’	Шаблон для группы биометрических данных (палец)	
‘65’	Шаблон для цифрового изображения лица	
‘67’	Шаблон для цифровой подписи или обычной отметки	
‘68’	Шаблон для машинной защиты. Закодированные данные	
‘69’	Шаблон для машинной защиты. Структура	

Тег	*Определение*	*Использование*
‘6A’	Шаблон для машинной защиты. Вещество	
‘6B’	Шаблон для дополнительных персональных данных	
‘6C’	Шаблон для дополнительных данных о документе	
‘6D’	Факультативные данные	
‘6E’	Зарезервировано для будущего использования	
‘70’	Уведомляемое лицо	
‘75’	Шаблон для группы биометрических данных (лицо)	
‘76’	Шаблон для биометрического шаблона (радужная оболочка глаза)	
‘77’	EF.SOD (EF данных системы защиты)	
‘7F2E’	Блок биометрических данных (зашифрованный)	
‘7F60’	Шаблон биометрической информации	
‘7F61’	Шаблон группы биометрической информации	
‘8x’	Теги, зависящие от контекста	CBEFF
‘90’	Зашифрованный хэш-код	Код аутентичности/целостности
‘A0’	Объекты данных, строящиеся в зависимости от контекста	Дополнительные персональные данные Дополнительные данные о документе
‘Ax’ или ‘Bx’	Повторяющийся шаблон, где x обозначает экземпляр	Заголовок биометрической информации

15.2 Теги, используемые для промежуточной обработки (информативные)

Тег	*Определение*	*Использование*
‘53’	Факультативные данные	Часть MC3
‘59’	Дата истечения срока действия или действителен до (дата)	Часть MC3
‘5A’	Номер документа	Часть MC3
‘5F02’	Контрольная цифра. Факультативные данные (только ID-3)	Часть MC3
‘5F03’	Тип документа	Часть MC3
‘5F04’	Контрольная цифра – номер документа	Часть MC3
‘5F05’	Контрольная цифра – дата рождения	Часть MC3
‘5F06’	Контрольная цифра – дата истечения срока действия	Часть MC3
‘5F07’	Контрольная цифра – составная	Часть MC3
‘5B’	Имя владельца документа	Часть MC3
‘5F28’	Государство или организация выдачи	Часть MC3
‘5F2B’	Дата рождения	Часть MC3
‘5F2C’	Гражданство	Часть MC3
‘5F35’	Пол	Часть MC3

Тег	*Определение*	*Использование*
'5F57'	Дата рождения (6 цифр)	Часть МСЗ

15.3 Теги, зарезервированные для будущего использования (нормативные)

Тег	*Определение*	*Использование*
'5F44'	Страна въезда/выезда	Записи о поездках
'5F45'	Дата въезда/выезда	Записи о поездках
'5F46'	Порт въезда/выезда	Записи о поездках
'5F47'	Указатель въезда/выезда	Записи о поездках
'5F48'	Продолжительность пребывания	Записи о поездках
'5F49'	Категория (классификация)	Записи о поездках
'5F4A'	Ссылка на инспектора	Записи о поездках
'5F4B'	Указатель въезда/выезда	Записи о поездках
'71'	Шаблон для электронных виз	
'72'	Шаблон для схем пересечения границы	
'73'	Шаблон для групп данных с записями о поездках	

A.16 *Минимальные требования к обеспечению интероперабельности.* Ниже указываются минимальные требования к обеспечению интероперабельности МСПД, основанных на использовании бесконтактной ИС с индуктивной связью через малый зазор (ИСО/МЭК 14443):

- ИСО/МЭК 14443, части 1–4, и ИСО/МЭК 10373-6 с учетом поправок к обеим сериям стандартов;
- интерфейс сигналов типа A или типа B[14];
- поддержка файловой структуры, определяемой стандартом ИСО/МЭК 7816-4 для записи различной длины;
- поддержка одной или нескольких прикладных программ и соответствующих команд, определяемых стандартом ИСО/МЭК 7816-4, 5.

Более подробная информация содержится в разделе II.

A.17 *Команды и параметры команд, которые могут использоваться устройством интерфейса*

A.17.1 Ниже приводится типичная последовательность обработки для выбора прикладной программы DF1 и извлечения данных из элементарного файла. Аналогичный процесс извлечения (считывания) используется для всех элементарных файлов в DF. Действительность групп данных из DF1 может затем верифицироваться путем исчисления хеш-значения группы данных и сравнения его с хеш-значением, полученным из данных системы безопасности $EF.SO_D$.

Типичная последовательность операций:

- Документ вводится в поле действия устройства бесконтактного сцепления (PCD).

- IC отвечает на запрос команды типа A (REQA) или запрос команды типа B (REQB), давая ответ на запрос типа A (ATQA) или ответ на запрос типа B (ATQB) в зависимости от конкретного случая.

[14] Это означает, что считыватели (устройства бесконтактного сцепления) должны быть способны считывать тип A и тип B.

- PCD обнаруживает и устраняет любую коллизию, которая может иметь место при нахождении нескольких документов в поле действия.

- Выполнение команд 7816 указывается
  – типом A: SAK (подтверждение выбора) бит 6 = 1, бит 3 = 0;
  – типом B: протокол_тип = "0001".

- Выбирается прикладная программа государства выдачи МСПД ИКАО.

- Затем элементарные файлы выбираются и считываются по мере необходимости. Аналогичный процесс отбора и считывания используется для всех EF. Форматы команд описываются в конце добавления.

  – EF может выбираться путем использования команды SELECT. Данные считываются с EF с помощью серии основных команд READ BINARY, при этом каждая команда указывает следующую зону данных, подлежащую считыванию. Эта команда является обязательной.

  – При желании EF может выбираться путем указания SFID файла EF в первой команде READ BINARY (первоначальная зона данных). Остальные данные затем считываются с помощью серии основных команд READ BINARY, при этом каждая команда указывает следующую зону данных, подлежащую считыванию. Примечание: поддержка этого метода выбора является факультативной.

- Сначала считывается общий файл данных EF.COM (краткий идентификатор файла = '1E'), содержащий идентификатор прикладной программы, уровни версии и список тегов в шаблоне '60'.

- Список тегов в EF.COM перечисляет группы данных (элементарные файлы), присутствующие в DF1. Устройство интерфейса определяет, какая группа данных (EF) должна считываться и использоваться. Затем в каждом EF производится поиск для получения группы данных из EF.

- Машиносчитываемая зона (МСЗ) обычно является первым считываемым EF.

- Другие EF считываются для получения соответствующих групп данных по мере необходимости.

- Затем $EF.SO_D$ считывается для подтверждения целостности групп данных, считанных с DF1. Примечание, при желании, сначала может считываться $EF.SO_D$.

A.18 *Детали инициализации и предотвращения коллизий в соответствии со стандартом ИСО/МЭК 14443, тип A.*

A.18.1 *REQA И WUPA (запуск типа A).* Бесконтактная карточка на интегральной схеме (PICC) после приведения в действие должна находиться в режиме ожидания. Она ждет команды и должна признавать команды REQA И WUPA. Оба сигнала передаются в коротких рамках (7 бит).

Команда	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**
REQA = ‘26’	0	1	0	0	1	1	0
WUPA = ‘52’	1	0	1	0	0	1	0

Совместимая PICC должна отвечать на эти команды; все другие значения в данном контексте не допускаются.

A.18.2 *ATQA*. После передачи команды REQA устройством PCD все PICC, находящиеся в состоянии ожидания, синхронно дают ответ ATQA.

После передачи устройством PCD команды WUPA все PICC, находящиеся в состоянии ОЖИДАНИЯ или ПРИОСТАНОВКИ, синхронно дают ответ ATQA.

Ответ ATQA состоит из 2 байтов. В соответствии со стандартом ИСО/МЭК 14443-3 MSB содержит только RFU и частные биты, поэтому эти байты должны игнорироваться любым соответствующим программным обеспечением.

Биты 7 и 8 LSB определяют размер PICC UID согласно следующей таблице:

b8	**b7**	**Значение**
0	0	Размер UID: одинарный
0	1	Размер UID: двойной
1	0	Размер UID: тройной
1	1	RFU

Совместимая PICC должна подтверждать один из трех действительных размеров UID.

Биты 1–5 LSB указывают биткадровую антиколлизию. Один и только один из этих битов должен быть установлен. Бит 6 является RFU и не должен оцениваться никаким программным обеспечением.

A.18.3 *Антиколлизия и выбор.* В соответствии с размером UID, определяемым ответом ATQA, команда выбора должна посылаться для каждого каскадного уровня. Если имеет место коллизия, выполняется антиколлизионный цикл.

A.18.3.1 Для команды выбора допускаются только значения ‘93’ (каскадный уровень 1), ‘95’ (каскадный уровень 2) и ‘97’ (каскадный уровень 3).

A.18.3.2 После выполнения антиколлизионного цикла выбирается одна PICC и производится возврат ответа SAK. SAK состоит из одного байта, где только два бита являются значимыми. Бит 3 указывает, что UID еще не полностью передан, означая, что должен быть выполнен еще один отборный/антиколлизионный цикл на следующем каскадном уровне.

A.18.3.3 Если бит 3 не установлен, бит 6 определяет, соответствует ли PICC стандарту ИСО/МЭК 14443-4. Поскольку все PICC, используемые для хранения данных LDS, должны поддерживать 14443-4, этот бит должен быть установлен.

A.18.4 *Запрос ответа на выбор (RATS).* После выполнения антиколлизионного и отборного цикла на PICC должен быть послан RATS. RATS состоит из фиксированного начального байта ‘E0’ и параметрического байта, который указывает максимальный размер кадра PCD и CID. CID указывается в наименее значимом полубайте; он используется для идентификации PICC, когда она находится в активном состоянии.

Наиболее значимый полубайт (FDSI) содержит максимальный размер кадра (FSD) в соответствии со следующей схемой конверсии:

FDSI	‘0’	‘1’	‘2’	‘3’	‘4’	‘5’	‘6’	‘7’	‘8’	‘9’ — ‘F’
FSD	16	24	32	40	48	64	96	128	256	RFU (>256)

Для передачи данных LDS соответствующее считывающее устройство должно обеспечивать размер кадра в 256 байтов; поэтому наиболее значимый полубайт параметрического байта должен быть ‘8’.

A.18.5 *Ответ на выбор.* Ответ на выбор указывает информацию о возможностях PICC. Он содержит до трех интерфейсных байтов. Первый интерфейсный байт TA (1) содержит параметр PICC по скорости передачи данных в битах. Второй байт TB (1) передает информацию для определения времени ожидания кадра и начала защитного временного интервала кадра. Третий интерфейсный байт TC (1) указывает протокольный параметр. Наименее значимый байт должен быть 1, если PICC поддерживает NAD. Второй байт должен быть 1, если PICC поддерживает CID.

Все остальные биты являются RFU и должны игнорироваться любым соответствующим программным обеспечением.

За интерфейсными байтами следуют исторические байты. Они содержат общую информацию о PICC и не должны оцениваться соответствующим программным обеспечением.

A.19 *Данные о форматах команд и параметрических вариантах ИСО/МЭК 7816*

A.19.1 *Выбор прикладной программы*

Прикладные программы должны выбираться либо по их файловому идентификатору, либо по названию прикладной программы. После выбора прикладной программы можно получить доступ к файлу в данной программе.

Примечание. Названия прикладных программ должны быть уникальными. Поэтому выбор прикладной программы с использованием ее названия может производиться в любом месте где бы то ни было.

A.19.2 *Выбор мастер-файла*

CLA	**INS**	**P1**	**P2**	**Lc**	**Данные**	**Le**
‘00’	‘A4’	‘00’	‘00’	–	Незаполнено	–

A.19.3 *Выбор прикладной программы по идентификатору*

Прикладная программа выбирается путем использования названия DF. Параметры команды APDU указаны ниже.

CLA	**INS**	**P1**	**P2**	**Lc**	**Данные**	**Le**
‘00’	‘A4’	‘04’	‘0C’	Var.	AID	–

A.20 *Выбор EF путем использования команды SELECT*

Файлы должны выбираться по их файловому идентификатору. Когда файлы выбираются по FID, необходимо убедиться в том, что прикладная программа, в которой хранятся файлы, предварительно выбрана.

CLA	INS	P1	P2	Lc	Данные	Le
‘00’	‘A4’	‘02’	‘0C’	‘02’	Файл ID	–

A.21 *Считывание данных с EF*

В целом имеется два способа считывания данных: путем выбора файла и затем считывания данных (рекомендуется) или путем прямого считывания данных с использованием SFI.

A21.1.1 ***Считывание данных выбранного файла (транспарентный файл)***

CLA	INS	P1	P2	Lc	Данные	Le
‘00’	‘B0’	Смещение MSB	Смещение LSB	–	–	MaxRet

Определение P1 и P2:

	b7	b6	b5	b4	b3	b2	b1	b0
Смещение MSB	0	X	X	X	X	X	X	X
Смещение LSB	X	X	X	X	X	X	X	X

A21.1.2 ***Считывание данных с использованием SFI (транспарентный файл)***

CLA	INS	P1	P2	Lc	Данные	Le
‘00’	‘B0’	SFI	Смещение LSB	–	–	MaxRet

Определение P1 и P2:

	b7	b6	b5	b4	b3	b2	b1	b0
SFI	1	0	0	X	X	X	X	X
Смещение LSB	X	X	X	X	X	X	X	X

A.22 Примеры использования ИСО/МЭК 7816 с LDS

A.22.1 *Считывание данных МСЗ с использованием выбора файла*

Считывание данных группы данных 1 (МСЗ) может производиться в следующей последовательности:

CLA	INS	P1	P2	Lc	Данные	Le	Замечания
‘00’	‘A4’	‘04’	‘0C’	‘07’	‘A0 00 00 02 47 10 01’	–	Выбор приложения выдающего органа
‘00’	‘A4’	‘02’	‘0C’	‘02’	‘01 01’	–	Выбор DG1
‘00’	‘B0’	‘00’	‘00’	–	–	‘00’	Считывание макс. 256 байтов

A.22.2 *Считывание группы данных 2*

A.22.2.1 Считывание данных группы данных 2 (закодированное изображение лица) может производиться в нижеуказанной последовательности. Заданная длина шаблона составляет 12 543 байта. Общая область данных составляет 12 547 байтов (плюс один байт на тег шаблона и три байта на поле длины). Это требует 49 блоков в 256 байтов каждый плюс заключительный блок в 3 байта.

A22.2.2 Следующая часть шаблона считывается путем увеличения смещения на 256 байтов (‘01 00’). Общий объем считываемых данных определяется по длине шаблона. Команду READ BINARY рекомендуется выдавать только для остаточного объема данных. Заключительное смещение – ‘31 00’.

CLA	INS	P1	P2	Lc	Данные	Le	Замечания
‘00’	‘A4’	‘04’	‘0C’	‘07’	‘A0 00 00 02 47 10 01’	–	Выбор приложения выдающего органа
‘00’	‘A4’	‘02’	‘0C’	‘02’	‘01 02’	–	Выбор DG2
‘00’	‘B0’	‘00’	‘00’	–	–	‘00’	Считывание первых 256 байтов
‘00’	‘B0’	‘01’	‘00’	–	–	‘00’	Считывание следующих 256 байтов
‘00’	‘B0’	‘02’	‘00’	–	–	‘00’	Считывание следующих 256 байтов
‘00’	‘B0’	‘03’	‘00’	–	–	‘00’	:

A22.3 При последовательном считывании более одной группы данных выбор прикладной программы выдающего органа должен производиться только один раз (перед считыванием первого файла).

A.22.4 *Считывание данных МСЗ с использованием глобального SFI*

CLA	INS	P1	P2	Lc	Данные	Le	Замечания
‘00’	‘B0’	‘81’	‘00’	–	–	‘00’	Прямое считывание 256 байтов

A22.5 *Считывание группы данных 2 с использованием глобального SFI*

Первый байты файла могут считываться с использованием команды Read Binary в сочетании с SFI. Следующие байты должны считываться с использованием “стандартной” команды Read Binary.

CLA	INS	P1	P2	Lc	Данные	Le	Замечания
‘00’	‘B0’	‘82’	‘00’	–	–	‘00’	Прямое считывание 256 байтов
‘00’	‘B0’	‘01’	‘00’	–	–	‘00’	Считывание следующих 256 байтов
‘00’	‘B0’	‘02’	‘00’	–	–	‘00’	Считывание следующих 256 байтов
‘00’	‘B0’	‘03’	‘00’	–	–	‘00’	:

A.23 *EF размером более 32 767 байтов*

A.23.1 Максимальный размер EF обычно составляет 32 767 байтов, однако некоторые ИС поддерживают более крупные файлы. При смещении свыше 32 767 для доступа к области 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 области данных. Например, если область данных содержит несколько объектов биометрических данных, считывать всю область данных, возможно, не требуется. При смещении на область данных свыше 32 767 этот формат команды используется. Смещение ставится в поле команд, а не в параметрах P1 и P2.

CLA	INS	P1	P2	Lc	Данные	Le	Замечания
‘00’	‘B1’	‘00’	‘00’	Var.	*Закодированное смещение TLV*	‘00’	Считывание файлов размером более 32 767 байтов

Пример закодированного смещения в поле данных:
Смещение: ‘FF FF’ кодируется как ‘54 02 ff ff’.

A23.2 Последующие команды READ BINARY указывают смещение в поле данных. Заключительная команда READ BINARY должна запрашивать остальную область данных.

A.24 *Правила кодирования длины ASN.1 BER*

Диапазон	**№ байтов**	**1-й байт**	**2-й байт**	**3-й байт**
0–127	1	двоичное значение	нет	нет
128–255	2	‘81’	двоичное значение	нет
256–65 535	3	‘82’	двоичное значение MS байт LS байт	
MS – наиболее значимый байт; LS – наименее значимый байт				

Примечание. Знак (‘ ’) используется для визуального разделения шестнадцатеричных знаков. Они не кодируются в LDS.

A.24.1 Примеры, основанные на вышесформулированных правилах:

Пример 1: длина в тридцать девять (39) кодируется как ‘27’ в шестнадцатеричном представлении.

Пример 2: длина в сто девяносто девять (199) кодируется как ‘81C7’ в шестнадцатеричном представлении.

Пример 3: длина в одну тысячу (1000) кодируется как ‘8203E8’ в шестнадцатеричном представлении.

A.25 *Кодирование биометрических подхарактеристик.* В следующей таблице указывается схема кодирования подхарактеристик:

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

РАЗДЕЛ IV

PKI ДЛЯ МАШИНОСЧИТЫВАЕМЫХ ПРОЕЗДНЫХ ДОКУМЕНТОВ С ДОСТУПОМ К ICC ТОЛЬКО ДЛЯ ЧТЕНИЯ

1. СФЕРА ПРИМЕНЕНИЯ

1.1 В настоящем разделе приводятся спецификации, позволяющие государствам и поставщикам внедрить схему аутентификации, включающую конкретную инфраструктуру применения и использования современных схем инфраструктуры открытых ключей (PKI) для внедрения и использования электронных цифровых подписей для машиносчитываемых проездных документов (МСПД), предоставляющих доступ к ICC только для чтения.

1.2 Базируясь на предположении о возможности эффективного внедрения в 2006 году, данные спецификации не предписывают полного внедрения сложной структуры PKI в каждой стране. Они предназначены скорее для предоставления способа внедрения, при котором государства могут делать выбор в различных сферах (таких, как активная или пассивная аутентификация, защита от скимминга и контроль доступа или автоматизированное пересечение границ) и иметь таким образом возможность поэтапно вводить дополнительные элементы, не нарушая структуры.

2. ДОПУЩЕНИЯ

2.1 Предполагается, что читатель знаком с концепциями и механизмами, предоставляемыми криптографией с открытым ключом и инфраструктурами открытых ключей.

2.2 Хотя использование техники криптографии с открытым ключом усложняет введение паспортов, включающих интегральную схему, такая техника полезна тем, что она предоставляет передовым пунктам пограничного контроля дополнительное средство установления подлинности такого документа, как паспорт. Предполагается, что ее использование является единственной мерой установления подлинности и что она НЕ ДОЛЖНА зависеть от одного определяющего фактора.

2.3 Изображение лица, хранящееся в цифровой форме, как предполагается, не является информацией, затрагивающей частную жизнь. Изображение лица владельца МСПД также печатается в документе и может быть легко получено.

2.4 Хранящиеся в цифровой форме изображения пальца(ев) и/или радужной оболочки глаза являются дополнительными биометрическими характеристиками, которые МОГУТ выбираться государствами для внутреннего использования. Они, как правило, считаются информацией, затрагивающей частную жизнь, и, следовательно, должны защищаться в соответствии с национальным законодательством государства выдачи.

2.5 Маловероятно, что ИКАО или какая-то другая центральная организация сможет устанавливать, поддерживать или контролировать защищенные закрытые ключи для любого государства. Несмотря на множество стратегических альянсов среди участников, этот вариант не будет признан в качестве решения, заслуживающего доверия.

2.6 В случае невозможности использования данных чипа, например в результате отзыва сертификата или недействительной верификации подписи, или если чип был умышленно оставлен пустым (как описывается в п. 7.1.1 настоящего раздела), МСПД вовсе не обязательно становится недействительным. В таком случае принимающее государство МОЖЕТ полагаться на другие элементы защиты документа в целях валидации.

2.7 Листы отзыва сертификатов (CRL) используются только для сертификатов подписывающегося CA страны и сертификатов лиц, подписывающих документы. CRL не применяются к индивидуальным объектам защиты и конкретным парам ключей активной аутентификации документов.

3. ТЕРМИНОЛОГИЯ

3.1 Ключевые слова "ДОЛЖЕН", "ТРЕБУЕТСЯ", "СЛЕДУЕТ", "РЕКОМЕНДУЕТСЯ" и "МОЖЕТ", употребляемые в настоящем разделе, следует толковать, как указано в [R4], *RFC 2119 (С. Браднер "Ключевые слова, употребляемые в RFC для указания уровней требовательности", BCP 14, RFC 2119, март 1997 г.*).

3.2 В случае внедрения ФАКУЛЬТАТИВНЫХ элементов они ДОЛЖНЫ внедряться, как указано в настоящем разделе.

3.1 CA, ключи и сертификаты

В рамках настоящего раздела значение имеют следующие ключи и сертификаты:

Название	**Сокращение**	**Замечания**
Подписывающийся CA страны	CSCA	
Сертификат подписывающегося CA страны	C_{CSCA}	Выдается CSCA (самоподписывающийся). Содержит открытый ключ подписывающегося CA страны (KPu_{CSCA}). Хранится в системе проверки
Закрытый ключ подписывающегося CA страны	KPr_{CSCA}	Подписывание сертификата лица, подписывающего документы (C_{DS}). Хранится в условиях (повышенной) защиты в государстве выдачи
Открытый ключ подписывающегося CA страны	KPu_{CSCA}	Для верификации подлинности сертификата лица, подписывающего документы (C_{DS})
Лицо, подписывающее документы	DS	
Сертификат лица, подписывающего документы	C_{DS}	Выдается подписывающимся CA страны (CSCA). Содержит открытый ключ лица, подписывающего документы (KPu_{DS}). Хранится в системе проверки и/или на чипе МСПД

Название	**Сокращение**	**Замечания**
Закрытый ключ лица, подписывающего документы	KPr_{DS}	Подписывание объекта защиты документа (SO_D). Хранится в условиях (повышенной) защиты в государстве выдачи
Открытый ключ лица, подписывающего документы	KPu_{DS}	Для верификации подлинности объекта защиты документа (SO_D)
Объект защиты документа	SO_D	Подписанная структура данных RFC3369 CMS, подписываемая лицом, подписывающим документы (DS). Содержит хэшированные группы данных LDS. Хранится на чипе МСПД. МОЖЕТ содержать сертификат лица, подписывающего документы (C_{DS})
Закрытый ключ активной аутентификации	KPr_{AA}	ФАКУЛЬТАТИВНЫЙ. Вычисление подписи в механизме активной аутентификации чипа МСПД. Хранится в защищенной памяти чипа
Открытый ключ активной аутентификации	KPu_{AA}	ФАКУЛЬТАТИВНЫЙ. Верификация подписи в механизме активной аутентификации чипа МСПД
Базовые ключи доступа к документу	K_{ENC} и K_{MAC}	ФАКУЛЬТАТИВНЫЕ. Для получения доступа к открытым данным МСПД и для защиты передачи сообщений между чипом МСПД и системой проверки

3.2 Сокращения

Сокращение	
APDU	Протокольный блок данных приложения
BLOB	Массивный двоичный объект
CA	Сертифицирующий полномочный орган
CRL	Лист отзыва сертификатов
DO	Объект данных
ICC	Карточка на интегральной схеме
IFD	Устройство интерфейса
LDS	Логическая структура данных
NTWG	Рабочая группа по новым технологиям
PCD	Устройство соединения через малый зазор
PICC	Карточка на интегральной схеме с индуктивной связью через малый зазор
PKI	Инфраструктура открытых ключей
SM	Безопасный обмен сообщениями
TAG	Техническая консультативная группа
ДОК	Директория открытых ключей
ИКАО	Международная организация гражданской авиации
МСЗ	Машиносчитываемая зона
МСПД	Машиносчитываемый проездной документ

4. СПРАВОЧНАЯ ДОКУМЕНТАЦИЯ

В настоящем разделе нижеуказанные документы служат справочным материалом.

Оценка угрозы PKI, ИКАО-NTWG, сентябрь 03 (заключительная версия 3, октябрь 2003 г.).

Технический доклад: цифровые подписи PKI для машиносчитываемых проездных документов, версия 4.

Технический доклад: разработка логической структуры данных. LDS для факультативных технологий увеличения емкости.

RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002.

RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003.

FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard, August 2002.

FIPS 186-2, Federal Information Processing Standards Publication (FIPS PUB) 186-2 (+ Change Notice), Digital Signature Standard, 27 January 2000. (Supersedes FIPS PUB 186-1 dated 15 December 1998.)

FIPS 186-3, Federal Information Processing Standards Publication (FIPS PUB) 186-3, Digital Signature Standard.

X9.62, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", 7 January 1999.

ИСО/МЭК 7816-4:2005. Карточки идентификационные. Карточки на интегральных схемах. Часть 4. Организация, защита и команды для обмена.

ИСО/МЭК 7816-8. Карточки идентификационные. Карточки на интегральных схемах. Часть 8. Команды, обеспечивающие операции защиты.

RFC 3369, Cryptographic Message Syntax, August 2002.

Документ ИКАО Doc 9303 "Машиносчитываемые проездные документы", издание пятое, 2003 год.

ИСО/МЭК 3166. Коды для представления названий стран и единиц их административно-территориального деления, 1997.

ИСО/МЭК 9796-2. Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы на основе целочисленной факторизации, 2002.

ИСО 11568-2:2005. Банковское дело. Управление ключами (розничная торговля). Часть 2. Методика управления ключами для симметричных алгоритмов шифрования (только на английском языке).

5. ОБЩИЕ ПОЛОЖЕНИЯ

5.1 Принципы схем PKI получили развитие в процессе их использования и стали весьма сложными в применении к современным сценариям. Они используются прежде всего в операциях по Интернету, требующих доверия к ключам со стороны широкого круга пользователей и агентств; в результате появились сложные системы сертификатов ключей, где открытые ключи выдаются в "сертификатах", которые в цифровой форме подписываются доверенными организациями выдачи, именуемыми сертифицирующими полномочными органами (CA). Доверие к этим CA далее подтверждается CA более высокого уровня в иерархической лестнице доверия, причем каждый в этой иерархии выдает ключ и подписывает сертификат в отношении нижестоящего по иерархии подчинения. Высшим уровнем в такой иерархии является так называемый "корневой CA". Различные иерархии перекрестно сертифицируют друг друга с целью создания уверенности в совместно выдаваемых ключах.

5.2 Осложняющим фактором является потребность в листах отзыва сертификатов (CRL), указывающих, какой ключ (сертификат) утратил силу по какой-либо причине. Фактически актом отзыва сертификата и опубликования информации об отзыве в CRL, орган, выдавший сертификат, информирует принимающие стороны о том, что его содержанию доверять больше нельзя. Необходимость верифицировать сертификаты при каждой и всякой операции часто предполагает многократные обращения к записям CA и записям CRL в различных базах данных. Это является сложным требованием.

5.3 Условия использования МСПД, отвечающих стандартам ИКАО, отличаются от вышеупомянутых коммерческих условий, где вопрос отзыва открытых ключей решается иным способом (по сравнению с индивидуальными пользователями), поскольку маловероятный случай компрометации закрытого ключа государства, который использовался в течение определенного периода для подписания многих МСПД, не может быть отрицанием того, что документы действительно подписывались с использованием этого ключа. Этими (действительными) документами их владельцы по-прежнему пользуются для совершения поездок. Применяемые электронные цифровые подписи рассчитаны на весь срок действия МСПД и не предназначены для целей повседневных операций. В случае компрометации ключа ДОЛЖЕН использоваться механизм предостережения для предупреждения государств о необходимости более тщательного просмотра таких документов.

5.4 В связи с этим в настоящем томе документа Doc 9303 излагается специализированный подход, позволяющий сообществу пользователей МСПД быстро внедрить этот вид применения МСПД с доступом к ICC только для чтения и воспользоваться его преимуществами, и не предпринимается никаких попыток рассмотреть более крупные вопросы политики PKI и сложные иерархии. Сертификаты используются в целях безопасности наряду с предлагаемой методологией рассылки открытых ключей (сертификатов) государствам-членам, и данная инфраструктура приспособлена к целям ИКАО.

5.5 Обязанности

Применение PKI ИКАО осуществляется на полностью равноправных условиях между пользователями, причем каждое государство является независимым и самостоятельным в вопросах МСПД и безопасности. Тем не менее неотъемлемой частью программы является наличие эффективного и общепринятого средства совместного использования и обновления в любой момент набора действующих открытых ключей ко всем существующим действительным МСПД всех участвующих государств.

5.5.1 Государства выдачи

Каждое участвующее государство ДОЛЖНО иметь собственные надежные средства создания наборов ключей на различные периоды времени; каждый такой набор ДОЛЖЕН использоваться для вычисления электронных цифровых подписей, применяемых для подписания сертификатов. Эти системы или средства ДОЛЖНЫ надежно предохраняться от любого внешнего или несанкционированного доступа за счет собственной конструкции и средств защиты аппаратуры.

Подписывающийся CA страны

Иерархия CA, в которой генерируются ключи, имеет отношение к настоящему разделу лишь в той мере, в какой она включает сертификаты, направляемые принимающим государствам. Направленный сертификат высшего уровня ДОЛЖЕН быть предметом доверия для принимающего государства. В настоящем разделе такой сертификат именуется сертификатом подписывающегося CA страны (C_{CSCA}). Сертификат подписывающегося CA страны (C_{CSCA}) ДОЛЖЕН самоподписываться и выдаваться подписывающимся CA страны (CSCA).

РЕКОМЕНДУЕТСЯ, чтобы пары ключей подписывающегося CA страны (KPu_{CSCA}, $KPru_{CSCA}$) генерировались и хранились в надежно защищенной автономной инфраструктуре CA государством выдачи.

Сертификаты подписывающегося CA страны (C_{CSCA}) ДОЛЖНЫ распределяться только по надежным дипломатическим каналам (внеполосное распределение).

Каждый сертификат подписывающегося CA страны (C_{CSCA}), создаваемый каждым государством, ДОЛЖЕН также направляться в ИКАО (с целью валидации сертификатов лиц, подписывающих документы (C_{DS}).

Закрытый ключ подписывающегося CA страны (KPr_{CSCA}) используется для подписания сертификатов лиц, подписывающих документы (C_{DS}).

В добавлении 1 указаны профили сертификатов.

Лицо, подписывающее документы

РЕКОМЕНДУЕТСЯ, чтобы пары ключей лица, подписывающего документы (KPu_{DS}, KPr_{DS}), генерировались и хранились в надежно защищенной инфраструктуре CA государством выдачи.

Каждый сертификат лица, подписывающего документы (C_{DS}), генерируемый каждым государством, ДОЛЖЕН направляться в ИКАО и МОЖЕТ храниться на чипе МСПД.

Закрытый ключ лица, подписывающего документы (KPr_{DS}), используется для подписания объектов защиты документов (SO_D).

Каждый объект защиты документов (SO_D), генерируемый каждым государством, ДОЛЖЕН храниться на соответствующем чипе МСПД.

В добавлении 1 указаны профили сертификатов.

Отзыв сертификатов

В случае инцидента (например компрометации ключа) государства выдачи могут отзывать сертификаты. Информация о таком отзыве ДОЛЖНА направляться в двустороннем порядке всем другим участвующим государствам и в директорию открытых ключей ИКАО в течение 48 ч.

При отсутствии инцидентов государствам выдачи СЛЕДУЕТ направлять "рутинные" CRL друг другу и в директорию открытых ключей ИКАО по крайней мере каждые 90 дней.

5.5.2 Директория открытых ключей (ДОК) ИКАО

В целях эффективного совместного использования сертификатов лиц, подписывающих документы (C_{DS}), всех государств ИКАО определит и будет предоставлять услуги службы директории открытых ключей (ДОК) всем участвующим государствам. Эта служба ДОЛЖНА принимать информацию об открытых ключах государств, хранить их в директории и делать ее доступной для всех других государств.

Доступ для обновления списков сертификатов, хранящихся в ДОК, ДОЛЖЕН предоставляться только участвующим государствам.

Контроль доступа для считывания ДОК (например, с целью скачивания информации ДОК) осуществляться НЕ ДОЛЖЕН.

Сертификаты подписывающегося СА страны

Сертификаты подписывающегося СА страны (C_{CSCA}) не являются частью услуг ДОК ИКАО. Однако ДОК ДОЛЖНА использовать сертификаты подписывающегося СА страны (C_{CSCA}) для верификации подлинности и целостности получаемых от участвующих государств сертификатов лиц, подписывающих документы (C_{DS}), перед их опубликованием.

ИКАО не предоставляет доступ к сертификату подписывающегося СА страны (C_{CSCA}).

Сертификаты лиц, подписывающих документы

ДОК ИКАО предназначена быть репозитарием всех сертификатов лиц, подписывающих документы (C_{DS}), используемых в любое время всеми участвующими государствами. Они включают сертификаты, активно используемые в любое время для целей подписания, а также уже не используемые, но еще действительные сертификаты на все выданные МСПД.

ДОК ИКАО будет основным механизмом распределения всех сертификатов лиц, подписывающих документы (C_{DS}), и, следовательно, ДОЛЖНА пополняться и обновляться всеми участвующими государствами.

Информация об открытых ключах какого-либо государства выдачи, хранящаяся в ДОК ИКАО, ДОЛЖНА также предоставляться другим сторонам (помимо государств-участников), нуждающимся в такой информации для валидации аутентичности данных, хранящихся в МСПД в цифровой форме.

Листы отзыва сертификатов

ДОК будет являться также репозиторием всех листов отзыва сертификатов (CRL), выпущенных каждым участвующим государством. Хотя государства ДОЛЖНЫ направлять CRL прежде всего друг другу, они ДОЛЖНЫ также посылать их в ДОК. Таким образом, ДОК будет вспомогательным механизмом распределения CRL.

5.5.3 Принимающие государства

Пользователи ДОК ДОЛЖНЫ иметь доступ к услугам ДОК ИКАО на регулярной основе и иметь возможность скачивать новую информацию о сертификатах ключей для хранения и использования их внутренними системами пограничного контроля.

Таким образом, обязанностью принимающего государства является поддержание кэш-памяти текущих CRL, а именно текущего набора CRL, который ДОЛЖЕН быть частью скачиваемой из ДОК ИКАО информации.

Каждое принимающее государство ДОЛЖНО обеспечивать внутреннюю рассылку сертификатов подписывающегося СА страны (C_{CSCA}), сертификатов лиц, подписывающих документы (C_{DS}) и CRL в своей системе проверки.

Обязанностью государства является надежное хранение сертификатов подписывающегося СА страны (C_{DS}), как предметов доверия, в своих системах пограничного контроля.

5.5.4 Другие стороны

Каждый, кто имеет соответствующее оборудование, может считывать содержание чипов МСПД, однако лишь стороны, обладающие соответствующими сертификатами открытых ключей и листами отзыва сертификатов, будут иметь возможность верифицировать аутентичность и целостность содержания чипов. Эти стороны МОГУТ получать эту информацию из директории открытых ключей ИКАО, однако набор сертификатов подписывающегося СА страны (C_{CSCA}) они должны будут получать при помощи других средств, так как они не публикуются в ДОК ИКАО.

5.6 Аутентификация данных

5.6.1 Пассивная аутентификация

Помимо групп данных LDS чип содержит также объект защиты документа (SO_D). Этот объект подписывается в цифровой форме государством выдачи и содержит хэшированные данные о содержании LDS (см. п. 7 настоящего раздела).

Система проверки, содержащая открытый ключ лица, подписывающего документы (KPu_{DS}), каждого государства, или считавшая с МСПД сертификат лица, подписывающего документы (C_{DS}), может верифицировать объект защиты документа (SO_D). Таким способом через содержание объекта защиты документа (SO_D) производится аутентификация содержания LDS.

Этот механизм верификации не требует использования процессорных возможностей микросхемы МСПД. В этой связи он называется "пассивной аутентификацией" содержания чипа.

Пассивная аутентификация доказывает, что содержание объекта защиты документа (SO_D) и LDS является подлинным и не было изменено. Она не предотвращает точное копирование содержания чипа или подмену чипа.

Следовательно, систему пассивной аутентификации СЛЕДУЕТ поддерживать дополнительной физической проверкой МСПД.

Пассивная аутентификация определяется в п. 7.2.2.

5.6.2 Активная аутентификация

Государство выдачи МОЖЕТ пожелать защитить свои МСПД от подмены чипа. Это может быть сделано путем внедрения механизма активной аутентификации.

Если механизм активной аутентификации поддерживается, то посредством запросно-ответного протокола между системой проверки и микросхемой МСПД он ДОЛЖЕН обеспечивать невозможность подмены чипа.

С этой целью чип содержит собственную пару ключей активной аутентификации (KPr_{AA} и KPu_{AA}). Хэш-представление группы данных 15 (информация об открытом ключе (KPu_{AA})) хранится в объекте защиты документа (SO_D) и, следовательно, аутентифицируется цифровой подписью выдающего лица. Соответствующий закрытый ключ (KPr_{AA}) хранится в защищенной памяти чипа.

Путем аутентификации визуальной МСЗ (через хэшированную МСЗ в объекте защиты документа (SO_D)) в сочетании с запросом-ответом система проверки, используя пару ключей активной аутентификации (KPr_{AA} и KPu_{AA}) МСПД, подтверждает, что объект защиты документа считан с подлинного чипа и хранится в подлинном МСПД.

Активная аутентификация требует использования процессорных возможностей микросхемы МСПД.

Активная аутентификация определяется в п. 7.2.2.

5.7 Контроль доступа

Сравнение МСПД, оснащенного бесконтактной интегральной схемой, с обычным МСПД, свидетельствует о двух различиях:

- Хранящиеся на чипе данные можно считать с помощью электронного устройства, не открывая документ (скимминг).
- Передача нешифрованных данных между чипом и считывающим устройством может быть перехвачена с расстояния в несколько метров.

Несмотря на наличие возможных мер физической защиты от скимминга, они не решают проблемы перехвата. В этой связи предполагается, что государства МОГУТ пожелать внедрить механизм базового контроля доступа, т. е. механизм контроля доступа, фактически требующий, чтобы держатель МСПД знал о том, что хранящиеся на чипе данные, считываются безопасным способом. Такой механизм базового контроля доступа предотвращает скимминг, а также перехват.

Эта рекомендуемая передовая практика призвана защищать частную жизнь и уважать права пассажиров на такую защиту посредством предотвращения скимминга и перехвата.

Этот механизм контроля доступа является ФАКУЛЬТАТИВНЫМ. Содержащиеся в настоящем разделе описание и спецификации, касающиеся базового контроля доступа и безопасного обмена сообщениями, применяются только к МСПД и системам проверки, поддерживающим этот вариант. Если данный механизм поддерживается, он ДОЛЖЕН обеспечивать возможность считывания содержания чипа только после сознательного предоставления МСПД его держателем.

Чип, защищенный механизмом базового контроля доступа, отказывает в предоставлении доступа к своему содержанию, если система проверки не может доказать, что ей разрешен доступ к чипу. Это доказательство предоставляется по запросно-ответному протоколу, в соответствии с которым система проверки доказывает знание индивидуальных базовых ключей доступа к документу на чипе (K_{ENC} и K_{MAC}), которые извлекаются из информации в МСЗ.

Система проверки ДОЛЖНА быть обеспечена этой информацией до считывания чипа. Данная информация снимается оптически/визуально с МСПД (например с МСЗ). Проверяющий ДОЛЖЕН также иметь возможность ввести эту информацию в систему проверки вручную в случае невозможности машинного считывания МСЗ.

Кроме того, после успешной аутентификации системой проверки, ТРЕБУЕТСЯ, чтобы чип обеспечил шифрование канала передачи данных между системой проверки и чипом МСПД методом безопасной передачи сообщений.

Предположение о том, что базовые ключи доступа к документу (K_{ENC} и K_{MAC}) не могут быть получены с нераскрытого документа (поскольку они извлекаются из оптически считываемой МСЗ), позволяет допускать, что паспорт сознательно предоставлен для проверки. Ввиду шифрования канала перехват передаваемых сообщений потребует значительных усилий.

Механизм контроля доступа определяется в п. 7.2.2.

5.8 Защита дополнительных биометрических параметров

Персональными данными, хранящимися на чипе, которые определяются как обязательный минимум для обеспечения глобальной интероперабельности, являются МСЗ и изображение лица держателя, хранящееся в цифровой форме. Оба элемента могут также просматриваться (считываться) визуально после раскрытия МСПД и предоставления его для проверки.

Помимо хранящегося цифрового изображения лица, как основного биометрического параметра для обеспечения глобальной интероперабельности, ИКАО одобряет использование хранящихся цифровых изображений пальцев и/или радужной оболочки глаза в дополнение к изображению лица. Для внутреннего или двустороннего использования государства МОГУТ предпочесть хранить шаблоны и/или ограничивать доступ или шифровать эти данные по собственному усмотрению.

Доступ к этим более конфиденциальным персональным данным СЛЕДУЕТ ограничивать в большей степени. Это может делаться двумя способами: расширением контроля доступа или шифрованием данных. Хотя эти варианты упоминаются в этом разделе, ИКАО в настоящее время не предлагает и не определяет никаких стандартов или практических методов в этих сферах.

5.8.1 Расширенный контроль доступа

Механизм ФАКУЛЬТАТИВНОГО расширенного контроля доступа аналогичен уже описанному механизму базового контроля доступа, однако для расширенного контроля доступа используется набор расширенных ключей контроля доступа к документу вместо базовых ключей контроля доступа к документу (K_{ENC} и K_{MAC}).

Определение (индивидуального для чипа) набора расширенных ключей доступа к документу производится по усмотрению внедряющего государства. Набор расширенных ключей доступа к документу МОЖЕТ состоять либо из симметричных ключей (например, полученных из МСЗ и национального мастерключа) или из пары ассиметричных ключей с соответствующим верифицируемым карточкой сертификатом.

Расширенный контроль доступа требует использования процессорных возможностей микросхемы МСПД.

5.8.2 Шифрование

Ограничение доступа к дополнительным биометрическим параметрам МОЖЕТ также производиться путем их шифрования. Чтобы иметь возможность расшифровать зашифрованные данные, система проверки ДОЛЖНА иметь ключ расшифрования. Определение алгоритма шифрования/расшифровки и ключей, подлежащих использованию, осуществляется по усмотрению внедряющего государства и выходит за рамки применения настоящего документа.

6. ЗАЩИТА ЭЛЕКТРОННЫХ ДАННЫХ В МСПД (РЕЗЮМЕ)

Помимо пассивной аутентификации с помощью цифровых подписей государства МОГУТ выбрать дополнительные средства обеспечения безопасности с использованием более сложных способов защиты микросхемы и ее данных. Варианты, приводимые в таблице IV-1, могут быть надлежащим образом объединены в целях усиления защиты в соответствии с существующими стандартами ИСО/МЭК.

Таблица IV-1. Базовый метод защиты

Метод	Выдающий орган	Система проверки	Преимущества	Недостатки
Пассивная аутентификация (5.6.1)	**M**	**M**	Доказывает, что содержание SO_D и LDS являются подлинными и не изменены	Не предотвращает точное копирование или подмену чипа. Не предотвращает несанкционированный доступ. Не предотвращает скимминг
УСОВЕРШЕНСТВОВАННЫЕ МЕТОДЫ ЗАЩИТЫ				
Сравнение обычной МСЗ (OCR-B) и МСЗ (LDS), базирующейся на чипе	N/A	O	Доказывает, что содержание чипа и МСПД соответствуют друг другу	Вносит (некоторую) сложность. Не предотвращает точное копирование чипа и обычного документа
Активная аутентификация (5.6.2)	O	O	Предотвращает копирование SO_D и доказывает, что он считан с аутентичного чипа. Доказывает, что чип не подменен	Вносит сложность. Требует использования микропроцессора
Базовый контроль доступа (5.7)	O	O	Предотвращает скимминг и злоупотребление. Предотвращает перехват	Не предотвращает точное копирование или подмену чипа (требует также копирования

Метод	Выдающий орган	Система проверки	Преимущества	Недостатки
			передачи сообщений между МСПД и системой проверки (при использовании для установки зашифрованного канала передачи)	обычного документа). Вносит сложность. Требует использования микропроцессора
Расширенный контроль доступа (5.8.1)	O	O	Предотвращает несанкционированный доступ к дополнительным биометрическим параметрам. Предотвращает скимминг дополнительных биометрических параметров	Требует дополнительного управления ключами. Не предотвращает точное копирование или подмену чипа (требует также копирования обычного документа). Вносит сложность. Требует использования микропроцессора
Шифрование данных (5.8.2)	O	O	Защищает дополнительные биометрические параметры. Не требует использования микропроцессора	Требует сложного управления ключами шифрования. Не предотвращает точное копирование или подмену чипа. Вносит сложность

МСПД, выдаваемые государствами, решившими использовать усовершенствованные методы защиты, будут полностью совместимы с требованиями ИКАО и считаться отвечающими стандартам глобальной интероперабельности.

7. СПЕЦИФИКАЦИИ

7.1 Изготовление и персонализация МСПД

7.1.1 Изготовление и персонализация МСПД являются обязанностью государства выдачи.

Однако государствам РЕКОМЕНДУЕТСЯ принимать меры по обеспечению безопасности транспортировки и хранения чипов, встраивания чипов в МСПД и процесса персонализации.

Настоящее издание тома 2 части 1 документа Doc 9303 базируется на предположении о том, что МСПД после персонализации записываться не будут. Поэтому в качестве заключительного шага в процессе персонализации чип СЛЕДУЕТ блокировать.

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

7.1.2 Информация, хранящаяся на чипе

Ниже схематически указано содержание чипа:

MF	
|---------DF — LDS	ОБЯЗАТЕЛЬНЫЙ
|---------K_{ENC}	ФАКУЛЬТАТИВНЫЙ
|---------K_{MAC}	ФАКУЛЬТАТИВНЫЙ
|---------KPr_{AA}	ФАКУЛЬТАТИВНЫЙ
|---------EF — COM	ОБЯЗАТЕЛЬНЫЙ
|---------EF — SO_D	ОБЯЗАТЕЛЬНЫЙ
|---------EF — Группа данных_1 (МСЗ)	ОБЯЗАТЕЛЬНЫЙ
|---------EF — Группа данных_2 (Закодированное изображение лица)	ОБЯЗАТЕЛЬНЫЙ
//	
|---------EF — Группа данных_n	ФАКУЛЬТАТИВНЫЙ

K_{ENC} , K_{MAC}

Базовые ключи доступа к документу (K_{ENC} и K_{MAC}) (ФАКУЛЬТАТИВНЫЕ) хранятся в DF. Получение этих ключей из МСЗ описывается в п. 7.2.2.

KPr_{AA}

Закрытый ключ активной аутентификации (KPr_{AA}) (ФАКУЛЬТАТИВНЫЙ) хранится в DF.

EF-COM

См. раздел III, *LDS.*

EF—группа данных 1-n

См. раздел III, *LDS.*

EF-SO_D

Файл EF-SO_D содержит объект защиты документа (SO_D). Объект защиты документа (SO_D) содержит хэш-значения используемых групп данных LDS. (Эта структура называется объектом защиты LDS (SO_{LDS}.)) Спецификация объекта защиты документа (SO_D), включая форматированный по ASN.1 пример объекта защиты LDS (SO_{LDS}), приводится в добавлении 3.

7.2 Проверка

7.2.1 Система проверки

В целях обеспечения выполнения требуемых функций и определенных вариантов, внедряемых на предоставляемых МСПД, система проверки должна удовлетворять некоторым предварительным условиям.

Базовый контроль доступа к МСПД

Хотя описываемый базовый контроль доступа является ФАКУЛЬТАТИВНЫМ, системы проверки, поддерживающие его, ДОЛЖНЫ удовлетворять следующим предварительным условиям:

1. Система проверки оснащена считывателем МСЗ или каким-то устройством ручного ввода данных (например клавиатурой) для выведения базовых ключей доступа к документу (K_{ENC} и K_{MAC}) с МСПД.

2. Программное обеспечение системы проверки поддерживает протокол, описываемый в п. 7.2.2, в случае, когда системе предоставляется МСПД с базовым контролем доступа, включая шифрование передачи данных с безопасным обменом сообщениями.

Пассивная аутентификация

Для осуществления пассивной аутентификации данных, хранящихся на чипе МСПД, система проверки должна знать ключевую информацию государств выдачи:

1. Сертификат подписывающегося СА страны (C_{CSCA}) каждого участвующего государства выдачи ДОЛЖЕН храниться в системе проверки.

2. Сертификат лица, подписывающего документы (C_{DS}), каждого участвующего государства выдачи ДОЛЖЕН храниться в системе проверки.

Активная аутентификация

Поддержка активной аутентификации системами проверки является ФАКУЛЬТАТИВНОЙ.

Если система проверки поддерживает ФАКУЛЬТАТИВНУЮ активную аутентификацию, ТРЕБУЕТСЯ, чтобы система проверки была способна считывать визуальную МСЗ.

Если система проверки поддерживает ФАКУЛЬТАТИВНУЮ активную аутентификацию, программное обеспечение систем проверки ДОЛЖНО поддерживать протокол активной аутентификации, описываемый в п. 7.2.2.

Расширенный контроль доступа к дополнительным биометрическим параметрам

Осуществление защиты ФАКУЛЬТАТИВНЫХ дополнительных биометрических параметров зависит от внутренних спецификаций государства или спецификаций, согласованных на двусторонней основе между государствами, обменивающимися такой информацией.

Расшифровка дополнительных биометрических параметров

Осуществление защиты ФАКУЛЬТАТИВНЫХ дополнительных биометрических параметров зависит от внутренних спецификаций государства или спецификаций, согласованных на двусторонней основе между государствами, обменивающимися такой информацией.

7.2.2 Последовательность этапов процесса проверки

В настоящем пункте описываются этапы процесса проверки в порядке их следования. Дается описание как ФАКУЛЬТАТИВНЫХ, так и ОБЯЗАТЕЛЬНЫХ этапов.

Базовый контроль доступа к МСПД (ФАКУЛЬТАТИВНЫЙ)

Когда МСПД с механизмом ФАКУЛЬТАТИВНОГО базового контроля доступа предоставляется системе проверки, оптически или визуально считываемая информация используется для выведения базовых ключей доступа к документу (K_{ENC} и K_{MAC}) с целью получения доступа к чипу и установления защищенного канала передачи данных между чипом МСПД и системой проверки.

Чип МСПД, поддерживающий базовый контроль доступа, ДОЛЖЕН давать на неаутентифицированные попытки считывания (включая *выбор* (защищенных) файлов в LDS) ответ "Статус защиты неудовлетворителен" (0x6982). Для аутентификации системы проверки ДОЛЖНЫ быть выполнены следующие этапы:

1. Система проверки считывает "информацию МСЗ", состоящую из конкатенации номера документа, даты рождения и даты истечения срока действия, включая соответствующие контрольные цифры (описывается в пп. 9 и 15 части 1 тома 1 документа Doc 9303) в машиносчитываемой зоне, используя считыватель знаков OCR-B. В качестве альтернативы нужная информация может впечатываться; в этом случае она ДОЛЖНА впечатываться в том виде, в каком фигурирует в МСЗ. 16 наиболее значимых байтов алгоритма хэширования (SHA-1) этой "информации МСЗ" используются в качестве начального заполнения генератора ключей с целью установить базовые ключи доступа к документу, используя механизм выведения ключей, описываемый в добавлении 5.1.

2. Система проверки и чип МСПД взаимно аутентифицируются и устанавливают сеансовые ключи. Протокол аутентификации и установления ключей, описываемый в добавлении 5.2, ДОЛЖЕН использоваться.

3. После успешной аутентификации последующая передача данных ДОЛЖНА защищаться безопасным обменом сообщениями, который описывается в добавлении 5.3.

Пассивная аутентификация (ОБЯЗАТЕЛЬНАЯ)

Система проверки выполняет следующие этапы:

1. Объект защиты документа (SO_D) (ФАКУЛЬТАТИВНО содержащий сертификат лица, подписывающего документы (C_{DS})), считывается с чипа.

2. Подпись лица, подписывающего документы (DS), считывается с объекта защиты документа (SO_D).

3. Цифровая подпись объекта защиты документа (SO_D) верифицируется системой проверки с использованием открытого ключа лица, подписывающего документы (KPu_{DS}). Сертификат лица, подписывающего документы (C_{DS}), для этого ключа хранится в системе проверки, в качестве скаченной из ДОК ИКАО информации, и также МОЖЕТ храниться на чипе МСПД. Это гарантирует, что объект защиты документа (SO_D) является аутентичным и что он выдан полномочным органом, упомянутым в объекте защиты документа (SO_D), и не изменен. Следовательно, содержанию объекта защиты документа (SO_D) можно доверять и его СЛЕДУЕТ использовать в процессе проверки.

4. Система проверки считывает соответствующие группы данных с LDS.

5. Путем хэширования содержания и сравнения результата с соответствующим хэш-значением в объекте защиты документа (SO_D) система гарантирует, что содержание группы данных является аутентичным и не изменено.

Теперь биометрическая информация может использоваться для биометрической верификации лица, предъявляющего МСПД.

Активная аутентификация (факультативная)

Если биометрической системе предоставляется МСПД с ФАКУЛЬТАТИВНОЙ группой данных 15, МОЖЕТ использоваться механизм активной аутентификации с целью гарантировать, что данные считываются с подлинного чипа и что чип и данные принадлежат друг другу.

Система проверки и чип выполняют следующие этапы:

1. Вся МСЗ визуально считывается со страницы данных МСПД (если она еще не считана в рамках процедуры базового контроля доступа) и сравнивается со значением МСЗ в группе данных 1. Поскольку аутентичность и целостность группы данных 1 проверены посредством пассивной аутентификации, сходство гарантирует, что визуальная МСЗ является аутентичной и не изменена.

2. Пассивная аутентификация также доказала аутентичность и целостность группы данных 15. Это гарантирует, что открытый ключ активной аутентификации (KPu_{AA}) является аутентичным и не изменен.

3. Чтобы гарантировать, что объект защиты документа (SO_D) не является копией, система проверки использует пару ключей активной аутентификации МСПД (KPr_{AA}. и KPu_{AA}) по запросно-ответному протоколу с чипом МСПД, как описывается в добавлении 4, A4.2.

Успешное выполнение запросно-ответного протокола доказывает, что объект защиты документа (SO_D) принадлежит странице данных, чип является подлинным и чип и данные принадлежат друг другу.

Расширенный контроль доступа к дополнительным биометрическим параметрам (ФАКУЛЬТАТИВНЫМ)

Осуществление защиты ФАКУЛЬТАТИВНЫХ дополнительных биометрических параметров зависит от внутренних спецификаций государства или спецификаций, согласованных на двусторонней основе между государствами, обменивающимися этой информацией.

Расшифровка дополнительных биометрических параметров (ФАКУЛЬТАТИВНЫХ)

Осуществление защиты ФАКУЛЬТАТИВНЫХ дополнительных биометрических параметров зависит от внутренних спецификаций государства или спецификаций, согласованных на двусторонней основе между государствами, обменивающимися этой информацией.

7.2.3 Дополнительный набор команд

Минимальный набор команд ДОЛЖЕН по крайней мере содержать команды:

SELECT (см. ИСО/МЭК 7816-4),
READ BINARY (см. ИСО/МЭК 7816-4).

Выполнение рекомендаций, которые в настоящем разделе определяются как ФАКУЛЬТАТИВНЫЕ, требуют поддержки следующих дополнительных команд:

EXTERNAL AUTHENTICATE (см. ИСО/МЭК 7816-4),
INTERNAL AUTHENTICATE (см. ИСО/МЭК 7816-4),
GET CHALLENGE (см. ИСО/МЭК 7816-4).

8. АЛГОРИТМЫ

8.1 Обзор

Государства ДОЛЖНЫ поддерживать один и тот же алгоритм для использования в своих подписывающихся СА страны, ключах подписи документов и, где это применимо, парах ключей активной аутентификации, несмотря на то, что могут требоваться различные размеры ключей в зависимости от выбранного алгоритма.

Государства ДОЛЖНЫ поддерживать все алгоритмы в пунктах, где они желают проверять подлинность подписей на документах в виде паспортов и где они обмениваются информацией об управлении ключами с другими государствами.

Содержащиеся здесь рекомендации по размерам ключей предполагают максимальные рекомендации в отношении периодов выдачи ключей и максимальный десятилетний срок действия документа.

Для генерирования подписи в механизме активной аутентификации государства ДОЛЖНЫ использовать схему цифровой подписи 1 стандарта ИСО/МЭК 9796-2 ([R17], *ИСО/МЭК 9796-2 "Информационная технология. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений", часть 2 "Механизмы на основе целочисленной факторизации", 2002*).

Для использования в своих подписывающихся СА страны, ключах подписи документов и, где применимо, объектах защиты документов государства ДОЛЖНЫ поддерживать один из нижеуказанных алгоритмов.

8.2 RSA

Государства, реализующие алгоритм RSA для генерирования подписи и верификации сертификатов и объекта защиты документа (SO_D), ДОЛЖНЫ использовать документ RFC3447 ([R7], *RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003).* RFC 3447 определяет два механизма подписи: RSASSA-PSS и RSASSA-PKCS1_v15. Подписи РЕКОМЕНДУЕТСЯ генерировать в соответствии с RSASSA-PSS, но принимающие государства ДОЛЖНЫ также быть готовы верифицировать подписи в соответствии с RSASSA-PKCS1_v15.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер модуля n для ключей подписывающегося CA страны, использующих RSA, составлял *3072 бит*.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер модуля n для ключей лица, подписывающего документы, использующих RSA, составлял *2048 бит*.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер модуля n для ключей активной аутентификации, использующих RSA, составлял *1024 бит*.

8.3 DSA

Государства, реализующие алгоритм DSA для генерирования или верификации подписей, ДОЛЖНЫ использовать стандарт FIPS 186-2 ([R9], *FIPS 186-2, Federal Information Processing Standards Publication (FIPS PUB) 186-2 (+ Change Notice), Digital Signature Standard, 27 January 2000. (Заменяет FIPS PUB 186-1 от 15 декабря 1998 г.)).*

Нынешняя спецификация для DSA FIPS 186-2 поддерживает только длину ключа 1024. Новая версия стандарта FIPS 186-3 проходит испытание, однако дату его готовности в настоящее время установить невозможно.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер модулей p и q для ключей подписывающегося CA страны, использующих DSA, составлял *3072 и 256 бит* соответственно.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер модулей p и q для ключей лица, подписывающего документы, использующих DSA, составлял *2048 и 224 бит* соответственно.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер модулей p и q для ключей активной аутентификации, использующих DSA, составлял *1024 и 160 бит* соответственно.

8.4 DSA с эллиптической кривой

Государства, реализующие алгоритм ECDSA для генерирования или верификации подписи, ДОЛЖНЫ использовать стандарт X9.62 ([R11], *X9.62, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", 7 January 1999).* Параметры области эллиптической кривой, используемые для генерирования пары ключей ECDSA, ДОЛЖНЫ быть ясно описаны в параметрах открытого ключа, т. е. параметры ДОЛЖНЫ быть типа EC параметров (без наименованных кривых, без подразумеваемых параметров) и ДОЛЖНЫ включать факультативный вспомогательный фактор. EC точки ДОЛЖНЫ быть в неуплотненном формате.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер для последовательности базовых точек для ключей подписывающегося CA страны, использующих ECDSA, составлял *256 бит*.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер для последовательности базовых точек для ключей лица, подписывающего документы, использующих ECDSA, составлял *224 бит*.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер для последовательности базовых точек для ключей активной аутентификации, использующих ECDSA, составлял *160 бит*.

8.5 Алгоритмы хэширования

SHA-1, SHA-224 (проект), SHA-256, SHA-384 и SHA-512 являются разрешенными алгоритмами хэширования. См. [R8], *FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard, August 2002.*

Для выбранного алгоритма подписи СЛЕДУЕТ отобрать алгоритм хэширования соответствующего размера. Например:

- SHA-1 с RSA 1024;
- SHA-224 с ECDSA 224.

9. УПРАВЛЕНИЕ КЛЮЧАМИ

9.1 Обзор

Государства выдачи ДОЛЖНЫ иметь по крайней мере два типа ключей, которые именуются:

- ключи подписывающегося CA страны,
- ключи лиц, подписывающих документы.

Государства выдачи МОГУТ иметь дополнительные типы ключей:

- ключи активной аутентификации.

Ключи подписывающегося CA страны и ключи лиц, подписывающих документы, выдаются с использованием сертификатов X.509 (RFC 3280, см. [R6], *RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002),* а открытые ключи, содержащиеся в них, используются для валидации ключей лиц, подписывающих документы (в случае использования ключей подписывающегося CA страны), или объектов защиты документов (SO_D), выдаваемых этим государством (в случае использования ключей лиц, подписывающих документы).

Все сертификаты, выдаваемые государствами, должны соответствовать профилю сертификата, указанному в добавлении 1.

Государства ДОЛЖНЫ периодически выпускать лист отзыва сертификатов; см. п. 9.5, касающийся отзыва.

9.2 Ключи активной аутентификации

ФАКУЛЬТАТИВНЫЕ пары ключей активной аутентификации (KPr_{AA}. и KPu_{AA}) ДОЛЖНЫ генерироваться безопасным способом.

Открытый ключ активной аутентификации (KPu_{AA}) и закрытый ключ активной аутентификации (KPr_{AA}.) вносятся в чип МСПД. После этого процедура управления ключами не применяется к этим ключам.

9.3 Ключи лиц, подписывающих документы

Сертификаты лиц, подписывающих документы (C_{DS}), используются для верификации действительности объектов защиты документа (SO_D). Поэтому для принятия электронного паспорта другого государства принимающее государство ДОЛЖНО предварительно поместить в определенное доверительное хранилище копии исходящих сертификатов лиц, подписывающих документы (C_{DS}).

Сертификат лица, подписывающего документы (C_{DS}), РЕКОМЕНДУЕТСЯ хранить в объекте защиты документа (SO_D). См. добавление 3.

Сертификат лица, подписывающего документы (C_{DS}), может считываться с чипа МСПД, если государство выдачи обеспечивает хранение этого сертификата на чипе.

Срок службы ключа лица, подписывающего документы

Срок службы (т. е. период действия сертификата) ключа лица, подписывающего документы, определяется путем конкатенации следующих двух периодов:

- продолжительность времени использования ключа для выдачи паспортов и
- срок действия [наиболее длительный] любого паспорта, выданного под этим ключом.[15]

Сертификат лица, подписывающего документы (C_{DS}), ДОЛЖЕН быть действительным в течение всего этого общего периода, чтобы позволять осуществлять верификацию подлинности паспортов. Однако ключ СЛЕДУЕТ использовать только для выдачи документов на ограниченный период времени; по истечении срока действия последнего документа, для выдачи которого он использовался, открытый ключ больше не требуется.

После выдачи последнего документа государствам РЕКОМЕНДУЕТСЯ стирать закрытый ключ поддающимся проверке и учету способом.

Период выдачи ключа лица, подписывающего документы

При развертывании своих систем государства могут пожелать учитывать количество документов, которые будут подписываться каким-либо одним индивидуальным ключом лица, подписывающего документы. Государство, ежедневно выдающее большое количество документов и использующее только один ключ лица, подписывающего документы, может пожелать использовать короткий период выдачи для сокращения эксплуатационных расходов по обеспечению непрерывности в случае отзыва ключа лица, подписывающего документы (см. п. 9.5). В качестве альтернативы государство может также пожелать использовать большое количество ключей подписи для сокращения накладных расходов на любой отдельный ключ.

Однако если государство выдает лишь небольшое количество сертификатов, потребности в таком коротком периоде выдачи ключа лица, подписывающего документы, нет и, следовательно, он МОЖЕТ быть более продолжительным.

В этой связи РЕКОМЕНДУЕТСЯ, чтобы максимальный период выдачи ключа лица, подписывающего документы, который используется для подписи паспортов, составлял три месяца.

[15] Некоторые государства могут выдавать паспорта до того, как они становятся действительными (например, при смене фамилии после вступления в брак). В результате этого срок действия увеличивается на самый продолжительный период, возможный для предварительной выдачи паспорта.

Для государств, изготавливающих большое количество МСПД, в любой определенный момент МОЖЕТ выпускаться несколько ключей подписи находящихся в обращении документов.

9.4 Ключи подписывающегося СА страны

Сертификаты подписывающегося СА страны (C_{CSCA}) используются для верификации действительности ключей лиц, подписывающих документы. Поэтому для принятия электронного паспорта другого государства принимающее государство ДОЛЖНО предварительно поместить в какое-либо доверительное хранилище, доступное его системе пограничного контроля, копию исходящего из государства сертификата подписывающегося СА страны (C_{CSCA}).

Срок службы ключа подписывающегося СА страны

Срок службы (т. е. период действия сертификата) ключа подписывающегося СА страны определяется путем конкатенации следующих периодов:

- промежуток времени, в течение которого ключ подписывающегося СА страны будет использоваться для выдачи сертификатов лиц, подписывающих документы (C_{DS});
- срок службы ключей лиц, подписывающих документы, состоящий из:
  - промежутка времени, в течение которого ключ будет использоваться для выдачи паспортов;
  - наиболее продолжительного периода действия любого паспорта, выданного под этим ключом.

Период выдачи ключа подписывающегося СА страны

Период выдачи ключа подписывающегося СА страны представляет собой тонкий баланс между следующими факторами:

- В маловероятном случае компрометации государственного ключа подписывающегося СА страны действительность всех паспортов, выданных с использованием ключей лиц, подписывающих документы, выданных под данным ключом подписывающегося СА страны, подвергается сомнению. В этой связи государства МОГУТ пожелать выдерживать довольно короткий период выдачи.
- Однако выдерживание очень короткого периода выдачи ведет к наличию весьма большого количества ключей подписывающегося СА страны в определенный момент времени. Это может усложнить управление сертификатами в пограничных системах обработки.
- Если смена ключа подписывающегося СА страны будет осуществляться слишком редко, то вполне возможно, что государствам будет сложно делать это из-за нехватки знаний или средств.

В этой связи государственный ключ подписывающегося СА страны РЕКОМЕНДУЕТСЯ заменять каждые три-пять лет.

Замена ключа подписи страны

Ключи подписывающегося CA страны являются предметами доверия во всей системе, без которых система разрушится. Поэтому государствам СЛЕДУЕТ тщательно планировать замену своих ключей подписывающегося CA страны. По истечении первоначального периода подписания государство всегда должно будет иметь по крайней мере два одновременно действующих сертификата подписывающегося CA страны (C_{CSCA}).

Государства ДОЛЖНЫ за 90 дней уведомлять о предстоящей замене своих сертификатов CSCA и затем в двустороннем порядке рассылать свои новые сертификаты CSCA. Для аутентификации своих новых сертификатов государствам следует также подтверждать свои новые сертификаты CSCA, используя внеполосный метод.

Государства МОГУТ дополнительно производить связующие сертификаты для обратной поддержки совместимости с ранее выданными сертификатами CSCA. В тех случаях, когда государства решают выдавать связующие сертификаты, им нет необходимости выдавать сертификаты CSCA с использованием внеполосного метода.

Государствам следует воздерживаться от использования своих сертификатов CSCA в первые два дня после выдачи.

9.5 Отзыв

Все национальные полномочные органы, выдающие сертификаты лиц, подписывающих документы (C_{DS}), ДОЛЖНЫ периодически вырабатывать информацию в виде листов отзыва сертификатов (CRL). Выпущенные CRL ДОЛЖНЫ соответствовать профилю, определяемому в добавлении 2.

Государства ДОЛЖНЫ производить по крайней мере один CRL каждые 90 дней. Государства МОГУТ производить CRL чаще, чем каждые 90 дней, но не чаще, чем каждые 48 ч.

Уведомление об отзыве

Если государство желает отозвать ключ лица, подписывающего документы, для выпуска нового CRL ему не надо ждать до тех пор, пока истечет очередной период обновления текущего CRL. Новый CRL РЕКОМЕНДУЕТСЯ выпускать в течение 48 ч с момента уведомления об отзыве.

Отзыв ключа подписывающегося CA страны

Отзыв ключа подписывающегося CA страны является одновременно крайней и сложной мерой. После информирования соответствующего государства об отзыве ключа подписывающегося CA страны все другие ключи, выданные с использованием этого ключа, фактически отзываются.

Если государство использовало старый ключ подписывающегося CA страны для аутентификации нового ключа подписывающегося CA страны (см. п. 9.4 "Замена ключа подписи страны"), отзыв старого ключа подписывающегося CA страны ДОЛЖЕН влечь за собой также отзыв нового ключа подписывающегося CA страны.

Для выдачи новых документов выдающее государство в сущности ДОЛЖНО снова вернуться к начальной загрузке своего процесса аутентификации путем двустороннего установления

новых сертификатов подписывающегося CA страны (C_{CSCA}), выданных им с использованием внеполосного метода.

10. РАССЫЛКА СЕРТИФИКАТОВ И CRL

Государствам необходимо планировать свои стратегии смены сертификатов как для ключей подписывающегося CA страны, так и для ключей лиц, подписывающих документы, с целью обеспечения своевременной передачи сертификатов и CRL в системы пограничного контроля принимающих государств. В идеальном случае, передача будет происходить в течение 48 ч, однако некоторые принимающие государства могут иметь удаленные и плохо подключенные пограничные посты, для передачи сертификатов и CRL в которые может требоваться больше времени. Принимающим государствам СЛЕДУЕТ делать все возможное для рассылки сертификатов и CRL всем пограничным пунктам в течение 48 ч.

Рассылка сертификатов подписывающегося CA страны

Государствам выдачи следует ожидать, что сертификаты подписывающегося CA страны (C_{CSCA}) будут распространяться принимающими государствами в течение 48 ч.

Рассылка сертификатов лиц, подписывающих документы

Государствам выдачи следует ожидать, что сертификаты лиц, подписывающих документы (C_{DS}), будут распространяться принимающими государствами в течение 48 ч.

Государства выдачи могут обеспечивать своевременное распространение сертификатов лиц, подписывающих документы (C_{DS}), путем включения таких сертификатов в объекты защиты документов (SO_D).

Рассылка CRL

Государствам СЛЕДУЕТ делать все возможное, используя либо электронные, либо другие средства, для предпринятия действий по CRL, выпущенным в исключительных обстоятельствах.

В отношении рассылки CRL см. также п. 5.5.2.

10.1 Рассылка через ДОК ИКАО

Основным каналом распределения сертификатов лиц, подписывающих документы (C_{DS}), будет директория открытых ключей ИКАО. Для CRL ДОК будет вспомогательным каналом. Сертификаты подписывающегося CA страны (C_{CSCA}) не публикуются и не доступны в ДОК, однако они используются ДОК для верификации сертификатов лиц, подписывающих документы (C_{DS}), представленных в нее для опубликования.

Связь

Вся связь с директорией открытых ключей ИКАО ДОЛЖНА базироваться на аутентифицированном серверном SSL. С этой целью ИКАО ДОЛЖНА получить единый серверный ключ (на каждый сайт) от коммерческой стороны.

Обновление директории

Открытые ключи ДОЛЖНЫ посылаться в директорию как сертификаты в формате X.509, подписанные государством выдачи, с использованием ключа подписывающегося CA страны, относящегося к данному государству. Эти сертификаты должны отвечать требованиям, изложенным в добавлении 1.

Обновление ДОЛЖНО осуществляться с использованием протокола LDAP, по которому директория меняется путем посылки изменений. Ввиду необходимости проявления ИКАО должной осмотрительности в этом процессе, ДОК ДОЛЖНА состоять из "директории для записи", куда посылаются предлагаемые изменения к сертификатам и CRL, и "директории для чтения", которая используется для содержания новых сертификатов, по завершении данного процесса, требующего должной осмотрительности, и доступ к которой предоставляется сообществу пользователей МСПД для скачивания этой информации.

В силу своего характера сертификаты и CRL подписываются государством выдачи. Эта подпись ДОЛЖНА верифицироваться ИКАО перед опубликованием сертификата или CRL в "директории для чтения".

Скачивание директории

ДОК будет создана как директория стандарта X.500. Предполагаемый объем ДОК составит 15–20 МБ.

Поскольку ДОК относительно невелика, государствам РЕКОМЕНДУЕТСЯ ежедневно скачивать всю директорию.

Доступ к ДОК с правом считывания ДОЛЖЕН предоставляться не только участвующим государствам. ДОК будет полностью открытым и функционирующим через Интернет ресурсом, доступ к которому только для чтения (скачивания) будет предоставляться также авиакомпаниям и подобным сторонам.

10.2 Рассылка с помощью двусторонних средств

Основным распределительным каналом для CRL и сертификатов подписывающегося CA страны (C_{CSCA}) будет двусторонний обмен между участвующими государствами и государствами-пользователями.

Государства, как правило, имеют двусторонние соглашения и средства взаимного обмена информацией (например, электронная почта или служба каталогов по протоколу LDAP). Государствам СЛЕДУЕТ использовать эти существующие каналы для обмена сертификатами и CRL.

Государствам, которые в настоящее время не имеют двусторонних соглашений или средств двустороннего обмена информацией, СЛЕДУЕТ заключить такие соглашения и установить такие каналы связи с другими участвующими государствами.

НОРМАТИВНОЕ ДОБАВЛЕНИЕ 1

ПРОФИЛЬ СЕРТИФИКАТА

Государства, удовлетворяющие данным техническим условиям, ДОЛЖНЫ выдавать сертификаты, соответствующие этому профилю. Все объекты защиты ДОЛЖНЫ производиться в формате особых правил кодирования (DER) в целях сохранения целостности содержащихся в них подписей.

Нижеуказанный профиль использует для каждого поля в сертификате X.509 следующую терминологию:

m обязательное – поле ДОЛЖНО присутствовать,
x не использовать – поле НЕ СЛЕДУЕТ заполнять,
o факультативное – поле МОЖЕТ присутствовать,
c критическое – обозначение критического расширения; принимающие прикладные программы ДОЛЖНЫ быть способны обрабатывать это расширение.

A.1.1 Основная часть сертификата

Компонент сертификата	**Раздел в RFC 3280**	**Сертификат подписывающегося CA страны**	**Сертификат лица, подписывающего документы**	**Замечания**
Сертификат	4.1.1	m	m	
Сертификат TBS	4.1.1.1	m	m	См. следующую часть таблицы
Алгоритм подписи	4.1.1.2	m	m	Вводимое здесь значение зависит от выбранного алгоритма
Значение подписи	4.1.1.3	m	m	Вводимое здесь значение зависит от выбранного алгоритма
Сертификат TBS	4.1.2			
Версия	4.1.2.1	m	m	ДОЛЖНА быть v3
Серийный номер	4.1.2.2	m	m	
Подпись	4.1.2.3	m	m	Вводимое здесь значение ДОЛЖНО соответствовать OID в алгоритме подписи
Выдающий	4.1.2.4	m	m	См. A1.5
Действительность	4.1.2.5	m	m	Ввод в действие ДОЛЖЕН указываться с использованием времени UTC до 2049, а затем с использованием обобщенного времени
Субъект	4.1.2.6	m	m	См. A1.5
Информация об открытом ключе субъекта	4.1.2.7	m	m	

Компонент сертификата	Раздел в RFC 3280	Сертификат подписы-вающегося CA страны	Сертификат лица, подпи-сывающего документы	Замечания
Уникальная идентификационная информация выдающего	4.1.2.8	x	x	
Уникальная идентификационная информация субъекта	4.1.2.8	x	x	
Расширения	4.1.2.9	m	m	См. следующую таблицу, где указано, какие расширения СЛЕДУЕТ включать

A1.2 Расширения

Название расширения	Раздел в RFC 3280	Сертификат подписы-вающегося CA страны	Сертификат лица, подпи-сывающего документы	Замечания
Идентификатор ключа полномочного органа	4.2.1.1	o	m	Обязательный во всех сертификатах, за исключением самоподписывающихся сертификатов подписывающегося CA страны
Идентификатор ключа субъекта	4.2.1.2	m	o	
Использование ключа	4.2.1.3	mc	mc	Это расширение ДОЛЖНО обозначаться как КРИТИЧЕСКОЕ
Период использования закрытого ключа	4.2.1.4	o	o	Это будет периодом выдачи закрытого ключа
Политика сертификата	4.2.1.5	o	o	
Отображение политики	4.2.1.6	x	x	
Альтернативное имя субъекта	4.2.1.7	x	x	
Альтернативное имя выдающего	4.2.1.8	x	x	
Атрибуты субъектов директории	4.2.1.9	x	x	
Основные ограничения	4.2.1.10	mc	x	Это расширение ДОЛЖНО обозначаться как КРИТИЧЕСКОЕ
Ограничения в отношении имени	4.2.1.11	x	x	
Ограничения в отношении политики	4.2.1.12	x	x	
Внешнее использование ключей	4.2.1.13	x	x	

Название расширения	**Раздел в RFC 3280**	**Сертификат подписывающегося CA страны**	**Сертификат лица, подписывающего документы**	**Замечания**
Пункты распределения CRL	4.2.1.14	o	o	Если государства решают использовать это расширение, они ДОЛЖНЫ включить ДОК ИКАО в качестве распределительного пункта. Внедрение может также включать относительные CRL DP для местных целей; они могут игнорироваться другими государствами
Любая политика запрета	4.2.1.15	x	x	
Самый свежий CRL	4.2.1.16	x	x	
Частные расширения в Интернете	4.2.2	x	x	
Другие частные расширения	–	o	o	При включении любого частного расширения для национальных целей, оно не должно маркироваться. Государствам не рекомендуется включать никакие частные расширения
Идентификатор ключа полномочного органа	**4.2.1.1**			
Идентификатор ключа		m	m	Если это расширение используется, данное поле ДОЛЖНО как минимум поддерживаться
Лицо, выдающее сертификат полномочного органа		o	o	См. A1.5
Порядковый номер сертификата полномочного органа		o	o	
Идентификатор ключа субъекта	**4.2.1.2**			
Идентификатор ключа субъекта		m	m	
Использование ключа	**4.2.1.3**			
Цифровая подпись		x	m	
Невозможность отрицания		x	x	
Шифрование ключа		x	x	
Шифрование данных		x	x	
Согласование ключа		x	x	
Подпись сертификата ключа		m	x	
Подпись CRL		m	x	
Только шифратор		x	x	

Название расширения	Раздел в RFC 3280	Сертификат подписывающегося CA страны	Сертификат лица, подписывающего документы	Замечания
Только дешифратор		x	x	
Основные ограничения	**4.2.1.10**			
cA		m	x	ВЕРНО для сертификатов CA
Ограничение длины пути		m	x	0 – для нового сертификата подписывающегося CA страны, 1 – для связанного с ним сертификата подписывающегося CA страны
Пункты распределения CRL	**4.2.1.14**			
Пункт распределения		m	x	
Причины		m	x	
Выдающий CRL		m	x	
Политика сертификата	**4.2.1.5**			
Информация о политике				
Идентификатор политики		m	m	
Квалификаторы политики		o	o	

A1.3 Алгоритм подписи

Идентификаторы объекта, определяемые в разделе 2.2 [R5], *RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", апрель 2002 г.,* и в разделе A.2 [R7], *RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", февраль 2003 г.*, ДОЛЖНЫ использоваться для алгоритмов, определяемых в п. 8 раздела IV.

A1.4 Значение подписи

Структуры подписи, хранящиеся в поле значения подписи, ДОЛЖНЫ соответствовать указанным в разделе 2.2 [R5], *RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", апрель 2002 г.*, для алгоритмов, определяемых в п. 8 раздела IV.

A1.4 Информация об открытом ключе субъекта

Поля информации об открытом ключе субъекта для алгоритмов, определяемых в п. 8 раздела IV, ДОЛЖНЫ заполняться в соответствии с разделом 2.3 [R5], *RFC 3279, W. Polk, R. Housley,*

L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", апрель 2002 г.

A1.5 Соглашения о сертификатах и именовании

РЕКОМЕНДУЕТСЯ нижеуказанные соглашения об именовании и адресации для поля выдающего и поля субъекта в сертификатах как CSCA, так и DS, и для поля выдающего в листах отзыва сертификатов.

СЛЕДУЕТ использовать следующие атрибуты:

- страна (коды страны ДОЛЖНЫ следовать формату двухбуквенных кодов страны, указанных в [R16], *ИСО/МЭК 3166, Коды для представления названий стран и единиц их административно-территориального деления. 1997 г.*);
- организация;
- организационное подразделение;
- общее название.

Дополнительно некоторые страны МОГУТ использовать:

- порядковый номер.

Государства, желающие использовать существующие инфраструктуры PKI для поддержки своих систем выдачи паспортов, могут быть связаны обязательствами по существующим соглашениям об именовании.

НОРМАТИВНОЕ ДОБАВЛЕНИЕ 2

ПРОФИЛЬ CRL

Нижеуказанный профиль использует для каждого поля в листе отзыва сертификатов X.509 следующую терминологию:

m обязательное – поле ДОЛЖНО присутствовать,
x не использовать – поле НЕ СЛЕДУЕТ заполнять,
o факультативное – поле МОЖЕТ присутствовать,
c критическое – обозначение критического расширения; принимающие прикладные программы ДОЛЖНЫ быть способны обрабатывать это расширение.

Компонент перечня сертификатов	**Раздел в RFC 3280**	**CRL подписывающегося CA страны**	**Замечания**
Перечень сертификатов	5.1.1	m	
Перечень сертификатов tBS	5.1.1.1	m	См. следующую часть таблицы
Алгоритм подписи	5.1.1.2	m	Вводимое здесь значение зависит от выбранного алгоритма
Значение подписи	5.1.1.3	m	Вводимое здесь значение зависит от выбранного алгоритма
Перечень сертификатов tBS	5.1.2		
Версия	5.1.2.1	m	ДОЛЖНА быть v2
Подпись	5.1.2.2	m	Вводимое здесь значение зависит от выбранного алгоритма
Выдающий	5.1.2.3	m	ТРЕБУЕТСЯ кодирование UTF8
Это обновление	5.1.2.4	m	Ввод в действие ДОЛЖЕН указываться с использованием времени UTC до 2049, а затем с использованием обобщенного времени
Следующее обновление	5.1.2.5	m	Ввод в действие ДОЛЖЕН определяться с использованием времени UTC до 2049, а затем с использованием обобщенного времени
Отозванные сертификаты	5.1.2.6	m	
Расширения crl	5.1.2.7	m	

Название расширения	Раздел в RFC 3280	CRL подписывающегося CA страны	Замечания
Идентификатор ключа полномочного органа	5.2.1	m	Это поле ДОЛЖНО иметь то же значение, что и поле идентификатора ключа субъекта в сертификате выдающего CRL
Альтернативное имя выдающего	5.2.2	x	
Номер cRL	5.2.3	m	
Дельта индикатор CRL	5.2.4	x	
Выдающий пункт распределения	5.2.5	x	
Самый свежий CRL	5.2.6	x	
Расширение записей CRL			
Код причины	5.3.1	x	
Код указания о задержке	5.3.2	x	
Дата недействительности	5.3.3	x	
Лицо, выдающее сертификат	5.3.4	x	

Примечание. CRL может содержать другую связанную с отзывом информацию, касающуюся, например, сертификатов оператора системы или полномочного органа регистрации.

НОРМАТИВНОЕ ДОБАВЛЕНИЕ 3

ОБЪЕКТ ЗАЩИТЫ ДОКУМЕНТА

Объект защиты документа реализуется как тип подписываемых данных, указанный в [R14] *RFC 3369, Cryptographic Message Syntax, август 2002 г.* Все объекты защиты ДОЛЖНЫ производиться в формате, определяемом особыми правилами кодирования (DER), для сохранения целостности содержащихся в них подписей.

A3.1 Тип подписываемых данных

Применяются правила обработки, изложенные в RFC3369.

m обязательное – поле ДОЛЖНО присутствовать,
x не использовать – поле НЕ ДОЛЖНО заполняться,
o факультативное – поле МОЖЕТ присутствовать,
c выбор – содержание поля выбирается из альтернатив.

Значение		Замечания
Подписываемые данные		
Версия	m	Значение = v3
Алгоритмы представления в краткой форме	m	
Информация об инкапсулированном содержании	m	
Тип электронного содержания	m	id-ИКАО – lds объекта защиты
Электронное содержание	m	Закодированное содержание lds объекта защиты
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 RFC3369, раздел 5.3
Sid	m	
Выдающее лицо и порядковый номер	c	Государствам рекомендуется поддерживать это поле над идентификатором ключа субъекта
Идентификатор ключа субъекта	c	

Значение		Замечания
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

A3.2 Объект защиты LDS профиля ASN.1

```
LDSSecurityObject    {iso(1)    identified-organization(3)    icao(ccc)    mrtd(1)
security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Imports from RFC 3280 [PROFILE], Appendix A.1
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 ::= {2.23.136}
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}

-- 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.

Поле `dataGroupValue` содержит вычисленное хэш-значение над полным содержанием файла группы данных EF, определяемого номером группы данных.

НОРМАТИВНОЕ ДОБАВЛЕНИЕ 4

ИНФОРМАЦИЯ ОБ ОТКРЫТОМ КЛЮЧЕ АКТИВНОЙ АУТЕНТИФИКАЦИИ

A4.1 Информация об открытом ключе активной аутентификации

ФАКУЛЬТАТИВНЫЙ открытый ключ активной аутентификации хранится в группе данных 15 LDS. Формат структуры (информация об открытом ключе субъекта) специфицирован в [R6], *RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, апрель 2002 г*. Все объекты защиты ДОЛЖНЫ производиться в формате, определяемом особыми правилами кодирования (DER), для сохранения целостности содержащихся в них подписей.

Информация об открытом ключе активной аутентификации ::= информация об открытом ключе субъекта:

```
SubjectPublicKeyInfo ::= SEQUENCE {
        algorithm           AlgorithmIdentifier,
        subjectPublicKey    BIT STRING }

AlgorithmIdentifier ::= SEQUENCE {
        algorithm           OBJECT IDENTIFIER,
        parameters          ANY DEFINED BY algorithm OPTIONAL }
```

A4.2 Механизм активной аутентификации

Активная аутентификация производится с использованием команды INTERAL AUTHENTICATE (ИСО/МЭК 7816). Вводимыми данными является специальное для этого случая сообщение (RND.IFD), которое ДОЛЖНО быть равно 8 байтам. В тех случаях, когда используется механизм факторизации целого числа, ICC вычисляет подпись в соответствии со схемой цифровой подписи 1 стандарта ИСО/МЭК 9796-2 ([R17], *ИСО/МЭК 9796-2, Информационная технология. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы на основе целочисленной факторизации, 2002 г.*).

M ДОЛЖНО состоять из M1 и M2, где M1 ДОЛЖНО быть специальным сообщением длиной c — 4 бит, а M2 является RND.IFD. Завершающий вариант 1 ДОЛЖЕН использоваться в случае SHA-1; без SHA-1 ДОЛЖЕН использоваться вариант 2.

Результатом вычисления подписи ДОЛЖНА быть подпись σ без невосстановимой части сообщения M2.

Конкретно, IFD (система проверки) и ICC (микросхема МСПД) выполняют следующие этапы:

1) IFD генерирует специальное значение RND.IFD и посылает его на ICC, используя команду INTERNAL AUTHENTICATE.

2) ICC выполняет следующие операции:
   a) создает заголовок,
   b) генерирует M1,
   c) вычисляет h(M),

d) создает завершитель,
e) вычисляет репрезентативное значение сообщения F,
f) вычисляет подпись σ и посылает ответ на IFD.

3) IFD верифицирует ответ по посланной команде INTERNAL AUTHENTICATE и проверяет, выдало ли ICC правильное значение.

НОРМАТИВНОЕ ДОБАВЛЕНИЕ 5

БАЗОВЫЙ КОНТРОЛЬ ДОСТУПА И БЕЗОПАСНЫЙ ОБМЕН СООБЩЕНИЯМИ

A5.1 Механизм установления ключей

Вычисление двух 3DES ключей из начального числа ключа (K_{seed}) используется как для установления базовых ключей доступа к документу (K_{ENC} и K_{MAC}), так и для установления сеансовых ключей для безопасного обмена сообщениями.

32-битный счетчик с используется для выведения нескольких ключей из одного начального числа. В зависимости от того, используется ли ключ для шифрования или для вычисления MAC ДОЛЖНЫ использоваться следующие значения:

- c = 1 (т. е. ‘0x 00 00 00 01’) для шифрования;
- c = 2 (т. е. ‘0x 00 00 00 02’) для вычисления MAC.

Для выведения двух 3DES ключей из начального числа K_{seed} и c выполняются следующие этапы:

1. Пусть D является конкатенацией K_{seed} и c ($D = K_{seed} || c$).
2. Вычислить H = SHA-1(D), SHA-1 хэш D.
3. Байты 1..8 H формируют ключ K_a, а байты 9..16 H формируют ключ K_b.
4. Скорректировать биты четности ключей K_a и K_b для формирования правильных DES ключей.

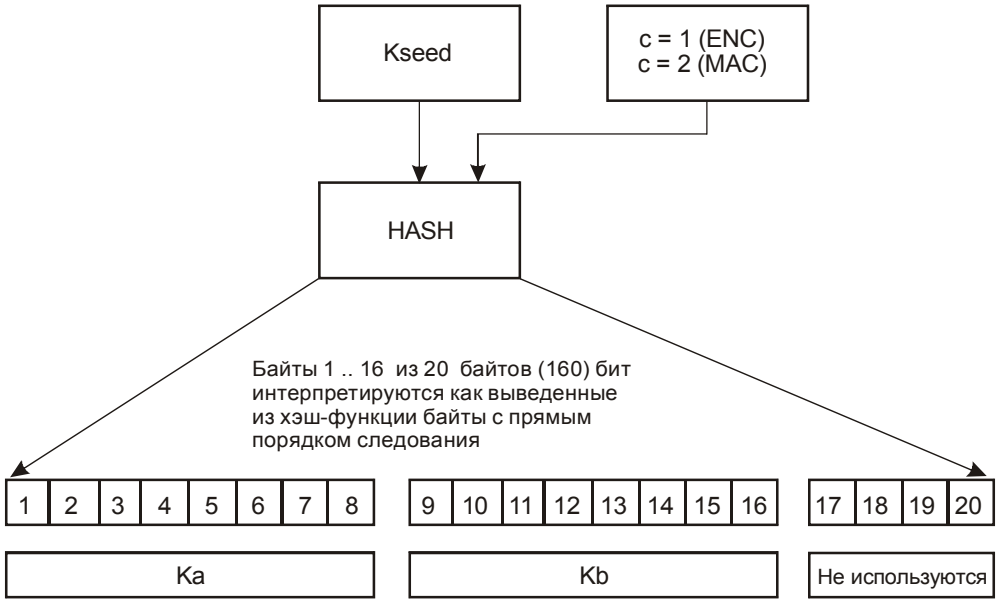


Рис. IV-5-1. Схема вычисления ключей из начального числа ключа

A5.2 Аутентификация и установление ключей

Аутентификация и установление ключей обеспечиваются трехпроходным запросно-ответным протоколом в соответствии с механизмом установления ключей 6 стандарта ИСО/МЭК 11770-2 с использованием 3DES как блочного шифра. Криптографическая контрольная сумма согласно МАК алгоритму 3 ИСО/МЭК 9797-1 вычисляется и добавляется к шифртекстам. Режимы работы, описываемые в добавлении 5.4, ДОЛЖНЫ использоваться. Размер специальных обмениваемых сообщений ДОЛЖЕН составлять 8 байтов, а обмениваемого ключевого материала – 16 байтов. Отличительные идентификаторы НЕ ДОЛЖНЫ использоваться.

IFD и ICC конкретно выполняют следующие этапы:

1) IFD запрашивает RND.ICC, посылая команду GET CHALLENGE. ICC генерирует и отвечает специальным значением RND.ICC.

2) IFD выполняет следующие операции:
   a) Генерирует специальное значение RND.IFD и ключевой материал K.IFD.
   b) Генерирует конкатенацию S = RND.IFD || RND.ICC || K.IFD.
   c) Вычисляет криптограмму E_IFD = E[K_ENC](S).
   d) Вычисляет контрольное число M_IFD = MAC[K_MAC](E_IFD).
   e) Посылает команду MUTUAL AUTHENTICATE с использованием данных E_IFD || M_IFD.

3) ICC выполняет следующие операции:
   a) Проверяет контрольную сумму M_IFD криптограммы E_IFD.
   b) расшифровывает криптограмму E_IFD.
   c) Извлекает RND.ICC из S и проверяет, выдало ли IFD правильное значение.
   d) Генерирует ключевой материал K.ICC.
   e) Генерирует конкатенацию R = RND.ICC || RND.IFD || K.ICC
   f) Вычисляет криптограмму E_ICC = E[K_ENC](R).
   g) Вычисляет контрольное число M_ICC = MAC[K_MAC](E_ICC).
   h) Посылает ответ с использованием данных E_ICC || M_ICC.

4) IFD выполняет следующие операции:
   a) Проверяет контрольную сумму M_ICC криптограммы E_ICC.
   b) Расшифровывает криптограмму E_ICC.
   c) Извлекает RND.IFD из R и проверяет, выдало ли ICC правильное значение.

A5.3 Безопасный обмен сообщениями

После успешного выполнения протокола аутентификации IFD и ICC вычисляют сеансовые ключи KS_ENC и KS_MAC с использованием механизма установления ключей, описываемого в добавлении 5.1, с (K.ICC xor K.IFD) в качестве начального заполнения генератора ключей. Вся дальнейшая передача данных ДОЛЖНА защищаться методом безопасного обмена сообщениями в режиме MAC_ENC.

A5.3.1 *Структура сообщений SM APDU*

Объекты данных SM ДОЛЖНЫ использоваться в соответствии с таблицей IV-1 в следующем порядке:

- APDU команды: [DO‘87’] [DO‘97’] DO‘8E’.
- APDU ответа: [DO‘87’] DO‘99’ DO‘8E’.

Все объекты данных SM ДОЛЖНЫ быть закодированы в BER TLV, как указано в ИСО/МЭК 7816-4. Заголовок команды ДОЛЖЕН быть включен в вычисление в MAC, поэтому ДОЛЖЕН использоваться байт класса CLA = 0x0c.

Фактическое значение Lc будет изменено на Lc’ после применения безопасного обмена сообщениями. При необходимости соответствующий объект данных факультативно можно включать в данные APDU для передачи исходного значения Lc. В защищенном APDU команды *новый Le* байт ДОЛЖЕН быть ‘00’.

Таблица IV-1. Использование объектов данных SM

	DO‘87’	**DO‘97’**	**DO‘99’**	**DO‘8E’**
Значение	Байт индикатора заполнения содержания (‘01’ для заполнения согласно ИСО), за которым следует криптограмма	Le (защищается CC)	Статус обработки (SW1-SW2, защищается MAC)	Криптографическая контрольная сумма (MAC)
APDU команды	Обязательный, если данные посылаются, в противном случае отсутствует	Обязательный, если данные запрашиваются, в противном случае отсутствует	Не используется	Обязательный
APDU ответа	Обязательный, если данные возвращаются, в противном случае отсутствует	Не используется	Обязательный, отсутствует только, если имеет место ошибка SM	Обязательный, если DO‘87’ и/или DO‘99’ присутствует

На рис. IV-5-2 показана схема преобразования незащищенного APDU команды в защищенный APDU команды в случае наличия *данных* и *Le*. Если *данных* нет, построение DO ‘87’ опускается. Если *Le* нет, построение DO ‘97’ опускается.

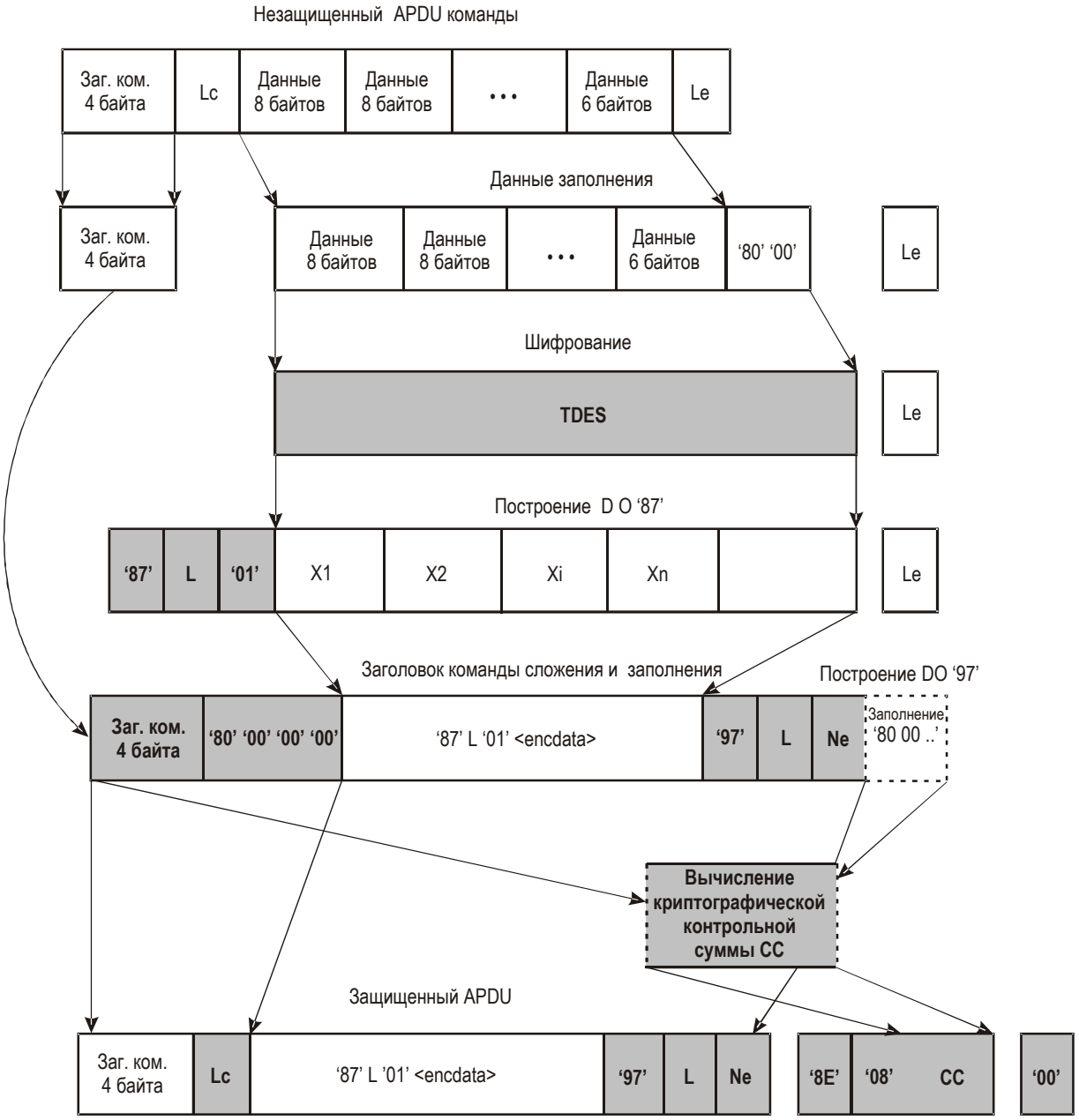


Рис. IV-5-2. Вычисление SM APDU команды

На рис. IV-5-3 показана схема преобразования незащищенного APDU ответа в защищенный APDU ответа в случае наличия *данных*. Если *данных нет,* построение DO ‘87’ опускается.

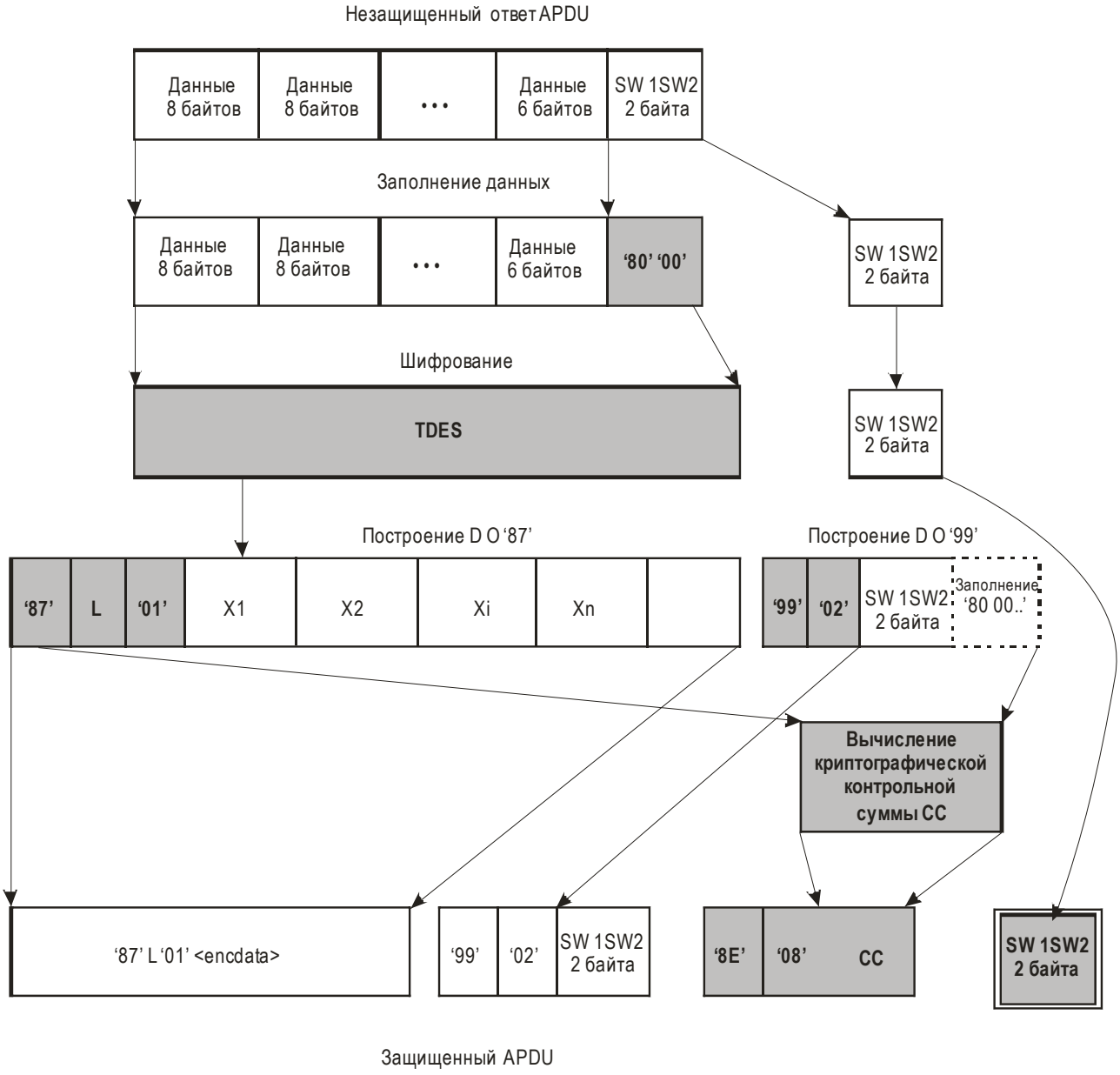


Рис. IV-5-3. Вычисление SM APDU ответа

A5.3.2 *Ошибки SM*

Когда ICC распознает ошибку SM, интерпретируя команду, байты состояния должны возвращаться без SM. В ИСО/МЭК 7816-4 определены следующие байты состояния для указания ошибок SM:

- '6987': ожидаемые объекты данных SM отсутствуют,
- '6988': объекты данных SM неверны.

Примечание. Дополнительные байты состояния SM могут иметь место в специфических контекстах приложений. Когда ICC возвращает байты состояния без SM DO или с ошибочным SM DO, безопасный сеанс прерывается. Сеанс не прерывается при исправлении ошибки.

A5.4 Режимы работы 3DES

A5.4.1 *Шифрование*

Используется двухключевой 3DES в режиме CBC с нулем IV (т. е. 0x00 00 00 00 00 00 00 00) в соответствии со стандартом ИСО 11568-2 (см. рис. IV-5-4). При выполнении команды MUTUAL AUTHENTICATE заполнение для вводимых данных не используется. При вычислении SM APDU используется заполнение в соответствии с методом заполнения 2 стандарта ИСО/МЭК 9797-1.

A5.4.2 *Аутентификация сообщений*

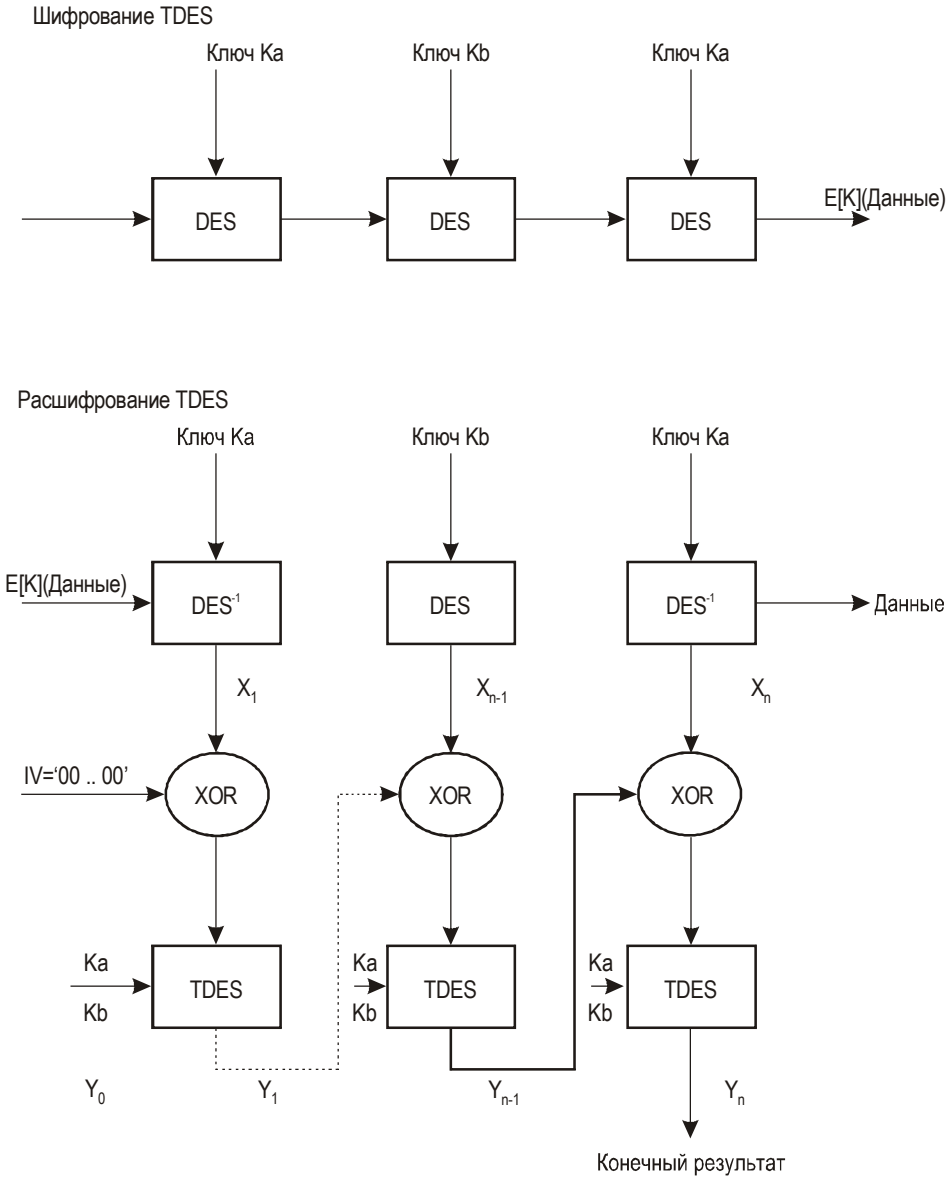
Криптографические контрольные суммы вычисляются с использованием MAC алгоритма 3 стандарта ИСО/МЭК 9797-1 с блочным шифром DES (ноль IV (8 байтов)) и метода заполнения 2 стандарта ИСО/МЭК 9797-1. Длина MAC ДОЛЖНА быть 8 байтов (см. рис. IV-5-5).

После успешной аутентификации датаграмма, подлежащая кодированию с помощью MAC, ДОЛЖНА быть добавлена к началу счетчиком посылаемых команд. Счетчик посылаемых команд вычисляется путем конкатенации четырех наименее значимых байтов RND.ICC и RND.IFD соответственно:

SSC = RND.ICC (4 наименее значимых байта) || RND.IFD (4 наименее значимых байта).

Значение счетчика посылаемых команд увеличивается каждый раз перед вычислением MAC, т. е. если начальное значение составляет x, то в следующей команде значение SSC составляет x+1. Значение первого ответа тогда составляет x+2.

Для команды MUTUAL AUTHENTICATE первоначальный проверочный блок Y_0 ДОЛЖЕН быть установлен на ноль '0000000000000000'.



IV – нулевая инициализация/вектор,

'X_1II ... II$^{X}_{n}$' – открытый текст (сообщение подлежит шифрованию), где длина каждого блока X_1 составляет 64-бита,

'Y_1II ... II$^{Y}_{n}$' – итоговая криптограмма (зашифрованное сообщение), где длина каждого блока Y_1 составляет 64-бита.

Рис. IV-5-4. Шифрование/расшифрование DES в режиме CBC

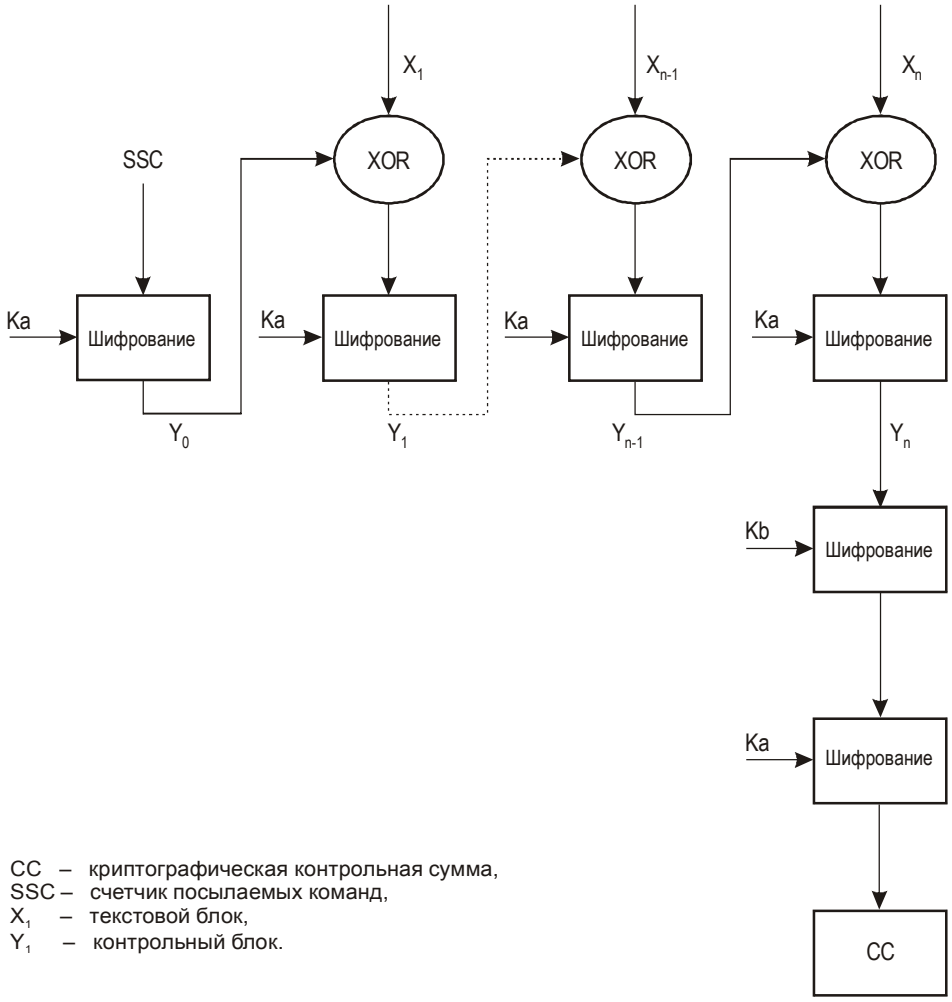


Рис. IV-5-5. Вычисление MAC

ИНФОРМАТИВНОЕ ДОБАВЛЕНИЕ 6

ПРИМЕРЫ С РЕШЕНИЯМИ

A6.1 Последовательность команд

A6.1.1 *Базовый контроль доступа и безопасный обмен сообщениями на основе МСЗ*

Вычисление ключей из начального числа ключа (K_{seed})

Ввод:

K_{seed} = '239AB9CB282DAF66231DC5A4DF6BFBAE'.

Вычисление ключа шифрования (c = '00000001'):

1. Конкатенация K_{seed} и c:
   D = '239AB9CB282DAF66231DC5A4DF6BFBAE00000001'.

2. Вычисление SHA-1 хэш D:
   H_{SHA-1}(D) = 'AB94FCEDF2664EDFB9B291F85D7F77F27F2F4A9D'.

3. Формирование ключей K_a и K_b:
   K_a = 'AB94FCEDF2664EDF';
   K_b = 'B9B291F85D7F77F2'.

4. Корректировка битов четности:
   K_a = 'AB94FDECF2674FDF';
   K_b = 'B9B391F85D7F76F2'.

Вычисление ключа расчета MAC (c = '00000002'):

1. Конкатенация K_{seed} и c:
   D = '239AB9CB282DAF66231DC5A4DF6BFBAE00000002'.

2. Вычисление SHA-1 хэш D:
   H_{SHA-1}(D) = '7862D9ECE03C1BCD4D77089DCF131442814EA70A'.

3. Формирование ключей K_a и K_b:
   K_a = '7862D9ECE03C1BCD';
   K_b = '4D77089DCF131442'.

4. Корректировка битов четности:
   K_a = '7962D9ECE03D1ACD';
   K_b = '4C76089DCE131543'.

Выведение базовых ключей доступа к документу (K_{ENC} и K_{MAC}):

1. Считывание МСЗ:
   МСЗ = `P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<<`
   `L898902C<3UTO6908061F9406236ZE184226B<<<<<14.`

2. Построение ‘МСЗ_информации’ из МСЗ:
   Номер документа = `L898902C<`, контрольная цифра = `3.`
   Дата рождения = `690806`, контрольная цифра = `1.`
   Дата истечения срока действия = `940623`, контрольная цифра = `6.`
   МСЗ_информация = `L898902C<3690806194062360.`

3. Вычисление SHA-1 хэш ‘МСЗ_информации’:
   H_{SHA-1}(МСЗ_информация) = `‘239AB9CB282DAF66231D`
   `C5A4DF6BFBAEDF477565’.`

4. Использование наиболее значимых 16 байтов для формирования K_{seed}:
   K_{seed} = `‘239AB9CB282DAF66231DC5A4DF6BFBAE’.`

5. Вычисление базовых ключей доступа (K_{ENC} и K_{MAC}) с использованием добавления 5.1:

   K_{ENC} = `‘AB94FDECF2674FDFB9B391F85D7F76F2’;`
   K_{MAC} = `‘7962D9ECE03D1ACD4C76089DCE131543’.`

Аутентификация и установление сеансовых ключей

Система проверки:

1. Запрос 8-байтового случайного числа у чипа МСПД:

   APDU команды:

CLA	INS	P1	P2	LE
00h	84h	00h	00h	08h

   APDU ответа:

Поле данных ответа	SW1SW2
RND.ICC	9000h

   RND.ICC = `‘4608F91988702212’.`

2. Генерирование 8-байтового и 16-байтового случайного числа:
   RND.IFD = `‘781723860C06C226’.`
   K_{IFD} = `‘0B795240CB7049B01C19B33E32804F0B’.`

3. Конкатенация RND.IFD, RND.ICC и K_{IFD}:
   S = ‘781723860C06C2264608F91988702212
   0B795240CB7049B01C19B33E32804F0B’.

4. Шифрование S с ключом TDES K_{ENC}, вычисленным в добавлении 5.2:
   E_{IFD} = ‘72C29C2371CC9BDB65B779B8E8D37B29
   ECC154AA56A8799FAE2F498F76ED92F2’.

5. Вычисление MAC по E_{IFD} с ключом TDES K_{MAC}, вычисленным в добавлении 5.2:
   M_{IFD} = ‘5F1448EEA8AD90A7’.

6. Построение данных команды MUTUAL AUTHENTICATE и посылка APDU команды на чип МСПД:
   cmd_data = ‘72C29C2371CC9BDB65B779B8E8D37B29ECC154AA
   56A8799FAE2F498F76ED92F25F1448EEA8AD90A7’.

   APDU команды:

CLA	INS	P1	P2	LC	Поле данных команды	LE
00h	82h	00h	00h	28h	cmd_data	28h

Чип МСПД:

7. Расшифрование и верификация полученных данных и сравнение RND.ICC с ответом на команду GET CHALLENGE.

8. Генерирование 16-байтового случайного числа:
   K_{ICC} = ‘0B4F80323EB3191CB04970CB4052790B’.

9. Вычисление XOR K_{IFD} и K_{ICC}:
   K_{seed} = ‘0036D272F5C350ACAC50C3F572D23600’.

10. Вычисление сеансовых ключей (KS_{ENC} и KS_{MAC}) с использованием добавления 5.1:
    KS_{ENC} = ‘979EC13B1CBFE9DCD01AB0FED307EAE5’.
    KS_{MAC} = ‘F1CB1F1FB5ADF208806B89DC579DC1F8’.

11. Вычисление счетчика посылаемых команд:
    SSC = ‘887022120C06C226’.

12. Конкатенация RND.ICC, RND.IFD и K_{ICC}:
    R = ‘4608F91988702212781723860C06C226
    0B4F80323EB3191CB04970CB4052790B’.

13. Шифрование R с ключом TDES K_{ENC}, вычисленным в добавлении 5.2:
    E_{ICC} = ‘46B9342A41396CD7386BF5803104D7CE
    DC122B9132139BAF2EEDC94EE178534F’.

14. Вычисление MAC по E_{ICC} с ключом TDES K_{MAC}, вычисленным в добавлении 5.2:
    M_{ICC} = ‘2F2D235D074D7449’.

15. Построение данных ответа на команду MUTUAL AUTHENTICATE и посылка APDU ответа в систему проверки:

    resp_data = ‘46B9342A41396CD7386BF5803104D7CEDC122B91
    32139BAF2EEDC94EE178534F2F2D235D074D7449’.

    APDU ответа:

Поле данных ответа	SW1SW2
resp_data	9000h

Система проверки:

16. Расшифрование и верификация полученных данных и сравнение полученного RND.IFD с генерированным RND.IFD.

17. Вычисление XOR K_{IFD} и K_{ICC}:

    K_{seed} = ‘0036D272F5C350ACAC50C3F572D23600’.

18. Вычисление сеансовых ключей (KS_{ENC} и KS_{MAC}) с использованием добавления 5.1:

    KS_{ENC} = ‘979EC13B1CBFE9DCD01AB0FED307EAE5’.
    KS_{MAC} = ‘F1CB1F1FB5ADF208806B89DC579DC1F8’.

19. Вычисление счетчика посылаемых команд:

    SSC = ‘887022120C06C226’.

Безопасный обмен сообщениями

После аутентификации и установления сеансовых ключей система проверки выбирает EF.COM (файл ID = ‘011E’) и считывает данные, используя метод безопасного обмена сообщениями. Будут использоваться вычисленные KS_{ENC}, KS_{MAC} и SSC (предыдущие этапы 18 и 19).

Сначала выбирается EF.COM, затем первые четыре байта этого файла считываются для определения длины структуры файла, после чего считываются остальные байты.

1. Выбор EF.COM

   Незащищенный APDU команды:

CLA	INS	P1	P2	LC	Поле данных команды
00h	A4h	02h	0Ch	02h	01h 1Eh

a. Маскирование байта класса и заполнение заголовка команды:
Заголовок команды = ‘0CA4020C80000000’.
b. Данные заполнения:
Данные = ‘011E800000000000’.
c. Шифрование данных с KS_{ENC}:
Зашифрованные данные = ‘6375432908C044F6’.
d. Построение DO‘87’:
DO87 = ‘8709016375432908C044F6’.
e. Конкатенация заголовка команды и DO87:
M = ‘0CA4020C800000008709016375432908C044F6’.

f. Вычисление MAC от M:
   i. приращение SSC на 1:
      SSC = ‘887022120C06C227’.
   ii. конкатенация SSC и M и добавление заполнения:
      N = ‘887022120C06C2270CA4020C80000000
      87090163754329 08C044F68000000000’.
   iii. Вычисление MAC по N с KS_{MAC}:
      CC = ‘BF8B92D635FF24F8’.
g. Построение DO‘8E’:
   DO8E = ‘8E08BF8B92D635FF24F8’.
h. Построение и посылка защищенного APDU:
Защищенный APDU = ‘0CA4020C158709016375432908C0
   44F68E08BF8B92D635FF24F800’.
i. Получение APDU ответа чипа МСПД:
RAPDU = ‘990290008E08FA855A5D4C50A8ED9000’.
j. Верификация RAPDU CC путем вычисления MAC DO’99’:
   i. Приращение SSC на 1:
   SSC = ‘887022120C06C228’.
   ii. Конкатенация SSC и DO‘99’ и добавление заполнения:
      K = ‘887022120C06C2289902900080000000’.
   iii. Вычисление MAC с KS_{MAC}:
      CC’ = ‘FA855A5D4C50A8ED’.
   iv. Сравнение CC’ с данными DO‘8E’ RAPDU.
      ‘FA855A5D4C50A8ED’ == ‘FA855A5D4C50A8ED’ ? ДА.

2. Считывание двоичного файла первых четырех байтов:

Незащищенный APDU команды:

CLA	INS	P1	P2	LE
00h	B0h	00h	00h	04h

a. Маскирование байта класса и заполнение заголовка команды:
Заголовок команды = ‘0CB0000080000000’.
b. Построение DO‘97’:
DO97 = ‘970104’.
c. Конкатенация заголовка команды и DO97:
M = ‘0CB0000080000000970104’.
d. Вычисление MAC от M:
   i. Приращение SSC на 1:
      SSC = ‘887022120C06C229’.
   ii. Конкатенация SSC и M и добавление заполнения:
      N = ‘887022120C06C2290CB00000
      8000000097010480000000 00’.
   iii. Вычисление MAC по N с KS_{MAC}:
      CC = ‘ED6705417E96BA55’.
e. Построение DO‘8E’:
   DO8E = ‘8E08ED6705417E96BA55’.
f. Построение и посылка защищенного APDU:
   Защищенный APDU = ‘0CB000000D9701048E08ED6705417E96BA5500’.

g. Получение APDU ответа чипа МСПД:
RAPDU = '8709019FF0EC34F992265199029000
8E08AD55CC17140B2DED9000'.
h. Верификация RAPDU CC путем вычисления MAC конкатенации DO'87' и DO'99':
i. Приращение SSC на 1:
SSC = '887022120C06C22A'.
ii. Конкатенация SSC, DO'87' и DO'99' и добавление заполнения:
K = '887022120C06C22A8709019F
F0EC34F99226519902900080'.
iii. Вычисление MAC с KS_{MAC}:
CC' = 'AD55CC17140B2DED'.
iv. Сравнение CC' с данными DO'8E' RAPDU:
'AD55CC17140B2DED' == 'AD55CC17140B2DED' ? ДА.
i. Расшифрование данных DO'87' с KS_{ENC}:
Расшифрованные данные = '60145F01'.
j. Определение длины структуры:
L = '14' + 2 = 22 байта.

3. Считывание остальных 18 байтов от смещения 4:

Незащищенный APDU команды:

CLA	INS	P1	P2	LE
00h	B0h	00h	04h	12h

a. Маскирование байта класса и заполнение заголовка команды:
Заголовок команды = '0CB0000480000000'.
b. Построение DO'97':
DO97 = '970112'.
c. Конкатенация заголовка команды и DO97:
M = '0CB00004800000000970112'.
d. Вычисление MAC от M:
i. Приращение SSC на 1:
SSC = '887022120C06C22B'.
ii. Конкатенация SSC и M и добавление заполнения:
N = '887022120C06C22B0CB00004
8000000097011280000000000'.
iii. Вычисление MAC по N с KS_{MAC}:
CC = '2EA28A70F3C7B535'.
e. Построение DO'8E':
DO8E = '8E082EA28A70F3C7B535'.
f. Построение и посылка защищенного APDU:
Защищенный APDU = '0CB000040D9701128E082EA28A70F3C7B53500'.
g. Получение APDU ответа чипа МСПД:
RAPDU = '871901FB9235F4E4037F2327DCC8964F1F9B8C30F42
C8E2FFF224A990290008E08C8B2787EAEA07D749000'.
h. Верификация RAPDU CC путем вычисления MAC конкатенации DO'87' и DO'99':
i. Приращение SSC на 1:
SSC = '887022120C06C22C'.

ii. Конкатенация SSC, DO‘87’ и DO‘99’ и добавление заполнения:
K = ‘887022120C06C22C871901FB9235F4E4037F232
7DCC8964F1F9B8C30F42C8E2FFF224A99029000’.

iii. Вычисление MAC по KS_{MAC}:
CC’ = ‘C8B2787EAEA07D74’.

i.v Сравнение CC’ с данными DO‘8E’ RAPDU:
‘C8B2787EAEA07D74’ == ‘C8B2787EAEA07D74’ ? YES.

i. Расшифровка данных DO‘87’ с KS_{ENC}:
Расшифрованные данные = ‘04303130365F36063034303030305C026175’.

РЕЗУЛЬТАТ:
данные EF.COM = ‘60145F0104303130365F36063034303030305C026175’.

A6.1.2 Пассивная аутентификация

Этап 1: считывание объекта защиты документа (SO_D) (факультативно содержит сертификат лица, подписывающего документы (C_{DS})) с чипа.
Этап 2: считывание данных лица, подписывающего документы (DS), с объекта защиты документа (SO_D).
Этап 3: верификация SO_D системой проверки путем использования открытого ключа лица, подписывающего документы (KPu_{DS}).
Этап 4: верификация C_{DS} системой проверки путем использования открытого ключа подписывающегося CA страны (KPu_{CSCA}).

Если обе верификации на этапе 3 и 4 правильные, то это означает, что содержанию SO_D можно доверять и его СЛЕДУЕТ использовать в процессе проверки.

Этап 5: считывание соответствующих групп данных с LDS.
Этап 6: вычисление хэш-значений соответствующих групп данных.
Этап 7: сравнение вычисленных хэш-значений соответствующими хэш-значениями в SO_D.

Если хэш-значения на этапе 7 идентичны, это означает, что содержание группы данных является аутентичным и не изменено.

A6.1.3 Активная аутентификация

В этом примере используются следующие установочные параметры:

1. Механизм, основанный на факторизации целого числа: **RSA**

2. Длина модуля: **1024 бит (128 байтов)**

3. Алгоритм хэширования: **SHA1**

Система проверки:

1. Генерирование 8-байтового случайного числа:
RND.IFD = ‘F173589974BF40C6’.

2. Построение команды внутренней аутентификации и посылка APDU команды на чип МСПД:

APDU команды

CLA	INS	P1	P2	LC	Поле данных команды	LE
0xh	88h	00h	00h	08h	RND.IFD	00h

Чип МСПД:

3. Определение M_2 из входящего APDU:
   M_2 = ‘F173589974BF40C6’.

4. Создание завершителя:
   T = ‘BC’ (i.e. SHA1).

5. Определение длины:
   a. $c = k – L_h – 8t – 4 = 1024 – 160 – 8 – 4 = 852$ бит;
   b. $L_{M1} = c – 4 = 848$ бит.

6. Генерирование специального сообщения M_1 длиной L_{M1}:
   M_1 = ‘9D2784A67F8E7C659973EA1AEA25D95B
   6C8F91E5002F369F0FBDCE8A3CEC1991
   B543F1696546C5524CF23A5303CD6C98
   599F40B79F377B5F3A1406B3B4D8F967
   84D23AA88DB7E1032A405E69325FA91A
   6E86F5C71AEA978264C4A207446DAD4E
   7292E2DCDA3024B47DA8’.

7. Создание M:
   $M = M_1 | M_2$ = ‘9D2784A67F8E7C659973EA1AEA25D95B
   6C8F91E5002F369F0FBDCE8A3CEC1991
   B543F1696546C5524CF23A5303CD6C98
   599F40B79F377B5F3A1406B3B4D8F967
   84D23AA88DB7E1032A405E69325FA91A
   6E86F5C71AEA978264C4A207446DAD4E
   7292E2DCDA3024B47DA8F173589974BF
   40C6’.

8. Вычисление SHA1 краткой формы M:
   H = SHA1(M) = ‘C063AA1E6D22FBD976AB0FE73D94D2D9
   C6D88127’.

9. Построение репрезентатива сообщения:
   $F = ‘6A’ | M_1 | H | T$ =
   ‘6A9D2784A67F8E7C659973EA1AEA25D9
   5B6C8F91E5002F369F0FBDCE8A3CEC19
   91B543F1696546C5524CF23A5303CD6C
   98599F40B79F377B5F3A1406B3B4D8F9
   6784D23AA88DB7E1032A405E69325FA9
   1A6E86F5C71AEA978264C4A207446DAD
   4E7292E2DCDA3024B47DA8C063AA1E6D
   22FBD976AB0FE73D94D2D9C6D88127BC’.

10. Шифрование F с помощью открытого ключа активной аутентификации для формирования подписи:
    S = ‘756B683B036A6368F4A2EB29EA700F96
    E26100AFC0809F60A91733BA29CAB362
    8CB1A017190A85DADE83F0B977BB513F
    C9C672E5C93EFEBBE250FE1B722C7CEE
    F35D26FC8F19219C92D362758FA8CB0F
    F68CEF320A8753913ED25F69F7CEE772
    6923B2C43437800BBC9BC028C49806CF
    2E47D16AE2B2CC1678F2A4456EF98FC9’.

11. Построение данных ответа на команду INTERNAL AUTHENTICATE и посылка APDU ответа в систему проверки:

    APDU ответа:

Поле данных ответа	**SW1SW2**
S	9000h

Система проверки:

12. Расшифровка подписи с помощью открытого ключа:
    F = ‘6A9D2784A67F8E7C659973EA1AEA25D9
    5B6C8F91E5002F369F0FBDCE8A3CEC19
    91B543F1696546C5524CF23A5303CD6C
    98599F40B79F377B5F3A1406B3B4D8F9
    6784D23AA88DB7E1032A405E69325FA9
    1A6E86F5C71AEA978264C4A207446DAD
    4E7292E2DCDA3024B47DA8C063AA1E6D
    22FBD976AB0FE73D94D2D9C6D88127BC’.

13. Определение хэш-алгоритма по завершителю T*:
    T = ‘BC’ (i.e. SHA1).

14. Выделение краткой формы:
    D = ‘C063AA1E6D22FBD976AB0FE73D94D2D9
    C6D88127’.

15. Выделение M_1:
    M1 = ‘9D2784A67F8E7C659973EA1AEA25D95B
    6C8F91E5002F369F0FBDCE8A3CEC1991
    B543F1696546C5524CF23A5303CD6C98
    599F40B79F377B5F3A1406B3B4D8F967
    84D23AA88DB7E1032A405E69325FA91A
    6E86F5C71AEA978264C4A207446DAD4E
    7292E2DCDA3024B47DA8’.

16. Заголовок указывает частичное восстановление, но подпись имеет длину модуля для конкатенации M_1 с известным M_2 (т. е. RND.IFD):
    M* = `'9D2784A67F8E7C659973EA1AEA25D95B`
    `6C8F91E5002F369F0FBDCE8A3CEC1991`
    `B543F1696546C5524CF23A5303CD6C98`
    `599F40B79F377B5F3A1406B3B4D8F967`
    `84D23AA88DB7E1032A405E69325FA91A`
    `6E86F5C71AEA978264C4A207446DAD4E`
    `7292E2DCDA3024B47DA8F173589974BF`
    `40C6'.`

17. Вычисление SHA1 краткой формы M*:
    D* = `'C063AA1E6D22FBD976AB0FE73D94D2D9`
    `C6D88127'.`

18. Сравнение D и D*:
    D равняется D*, т. е. верификация прошла успешно.

A6.2 Срок службы

Нижеуказанные примеры поясняют, как следует вычислять срок службы ключей, описываемый в разделе 9.

A6.2.1 *Пример 1*

Первый пример демонстрирует систему, при которой государство желает, чтобы общий срок службы всех его сертификатов оставался минимальным. Паспорта государства действительны в течение пяти лет, и поскольку государство ежегодно выдает относительно большое количество паспортов, оно решает, что периоды выдачи ключей должны быть минимальными.

Период	Истекшее время	
Выдача ключа лица, подписывающего документы		1 мес
Срок действия паспорта	5 лет	—
Срок действия сертификата лица, подписывающего документы	5 лет	1 мес
Выдача ключа подписывающегося CA страны	3 года	—
Срок действия сертификата подписывающегося CA страны	8 лет	1 мес

Последствиями этого варианта является то, что ко времени истечения срока действия первого сертификата подписывающегося CA страны будет выдано по крайней мере 36 ключей подписи документов (один на каждый период в 1 мес) и в течение нескольких последних месяцев действия этого ключа подписывающегося CA страны по крайней мере два других ключа подписи страны будут действительны для верификации подписей.

A6.2.2 *Пример 2*

Второй пример иллюстрирует систему, при которой государство применяет менее жесткий подход. Паспорта действительны в течение 10 лет; государство решает сохранять средние периоды выдачи для всех ключей.

Период	**Истекшее время**	
Выдача ключа лица, подписывающего документы		2 мес
Срок действия паспорта	10 лет	—
Срок действия сертификата лица, подписывающего документы	10 лет	2 мес
Выдача ключа подписывающегося CA страны	4 года	—
Срок действия сертификата подписывающегося CA страны	14 лет	2 мес

Последствиями этого варианта является то, что ко времени истечения срока действия первого сертификата подписывающегося CA страны будет выдано по крайней мере 24 ключа лица, подписывающего документы, и в течение нескольких последних месяцев действия ключа подписывающегося CA страны по крайней мере три других ключа подписывающегося CA страны будут действительны для верификации подписей.

A6.2.3 *Пример 3*

Последний пример иллюстрирует систему, при которой государство решает использовать максимальные пределы, рекомендуемые данной структурой. Паспорта действительны в течение десяти лет; ключ подписывающегося CA страны заменяется каждые пять лет, а ключи лица, подписывающего документы, заменяются каждые три месяца.

Период	**Истекшее время**	
Выдача ключа лица, подписывающего документы		3 мес
Срок действия паспорта	10 лет	—
Срок действия сертификата лица, подписывающего документы	10 лет	3 мес
Выдача ключа подписывающегося CA страны	5 лет	—
Срок действия сертификата подписывающегося CA страны	15 лет	3 мес

Последствиями этого варианта является то, что ко времени истечения срока действия первого сертификата подписывающегося CA страны будет выдано по крайней мере 20 ключей лица, подписывающего документы, и в течение нескольких последних месяцев действия ключа подписывающегося CA страны по крайней мере три других ключа подписывающегося CA страны, будут действительны для верификации подписей.

ИНФОРМАТИВНОЕ ДОБАВЛЕНИЕ 7

PKI И УГРОЗЫ НАРУШЕНИЯ БЕЗОПАСНОСТИ

A7.1 Управление ключами

A7.1.1 *Ключи подписывающегося CA страны и лиц, подписывающих документы*

В целях защиты закрытых ключей РЕКОМЕНДУЕТСЯ использовать для генерации подписей защищенное аппаратное оборудование (защищенное устройство создания подписей SSCD); SSCD генерирует новые пары ключей, надежно хранит и уничтожает (после истечения срока действия) соответствующий закрытый ключ. Для защиты от атак на SSCD, в том числе от атак через побочные каналы (например, тайминг, энергопотребление, электромагнитные излучения, внесение неисправностей) и атак на генераторы случайных чисел, РЕКОМЕНДУЕТСЯ использовать SSCD сертифицированные/проверенные сертифицирующим органом, отвечающим требованиям CCRA, в соответствии с надлежащим профилем общих критериев защиты с уровнем EAL 4+ SOF-High.

При распределении самоподписывающихся сертификатов CA страны по дипломатическим каналам необходимо проявлять крайнюю осторожность для предотвращения внесения жульнического сертификата подписывающегося CA страны. Кроме того, РЕКОМЕНДУЕТСЯ, чтобы государства надежно хранили полученные сертификаты подписывающегося CA страны и чтобы доступ к ним предоставлялся считывающим устройствам безопасным образом. Для защиты от атак на CAD, РЕКОМЕНДУЕТСЯ использовать CAD, сертифицированные/проверенные сертифицирующим органом, отвечающим требованиям CCRA, в соответствии с надлежащим профилем общих критериев защиты с уровнем EAL 4+ SOF-High.

A7.1.2 *Ключи активной аутентификации*

Пары ключей активной аутентификации РЕКОМЕНДУЕТСЯ генерировать безопасным способом. Поскольку закрытый ключ хранится на чипе в защищенной памяти, а конструкция чипа должна противостоять атакам на протяжении всего срока действия МСПД, РЕКОМЕНДУЕТСЯ использовать чипы, сертифицированные/проверенные сертифицирующим органом, отвечающим требованиям CCRA, в соответствии с надлежащим профилем общих критериев защиты с уровнем EAL 4+ SOF-High.

Существующая микросхемная технология влияет на максимальную длину ключей, используемых внутри чипа для активной аутентификации. Многие чипы в настоящее время не поддерживают длину ключей, превышающую безопасный уровень в 80 бит, что является причиной выбора этого значения в качестве рекомендуемого минимума. Это относительно невысокий уровень безопасности с учетом срока действия МСПД. В этой связи РЕКОМЕНДУЕТСЯ использовать более длинные ключи, если они поддерживаются чипом.

Государствам, использующим механизм активной аутентификации для подтверждения подлинности иностранного МСПД, следует также иметь в виду, что механизм отзыва скомпрометированных ключей активной аутентификации не специфицирован.

A7.1.3 *Атаки, вызывающие отказ в обслуживании*

При использовании государствами директории для распределения сертификатов лиц, подписывающих документы, и CRL необходимо учитывать возможность отказа в обслуживании в результате атаки. Такие атаки предотвратить невозможно. В этой связи РЕКОМЕНДУЕТСЯ, чтобы сертификат лица, подписывающего документы, требующийся для валидации объекта защиты документа, включался также в сам объект защиты. Принимающим государствам СЛЕДУЕТ использовать предоставленный сертификат лица, подписывающего документы.

Для двустороннего распределения CRL РЕКОМЕНДУЕТСЯ установить несколько каналов (например, Интернет, телефон, факсимильная связь, почта и т. д.) с другими государствами и подтверждать получение поступивших CRL.

A7.2 Угрозы дублирования

По сравнению с МСПД на бумажном носителе, копирование подписанных данных, хранящихся на РЧ-чипе, в целом можно произвести довольно легко. Государствам, обеспокоенным возможностью перекопирования данных своих граждан на другой чип, следует осуществлять активную аутентификацию, которая предотвращает его в некоторой степени.

A7.2.1 *Пассивная аутентификация*

Пассивная аутентификация не предотвращает копирования данных, хранящихся на чипе. Следовательно, чип МСПД может быть заменен поддельным чипом, хранящим данные, скопированные с чипа другого МСПД. Принимающим государствам СЛЕДУЕТ убеждаться в том, что считанные с чипа данные действительно принадлежат предъявленному МСПД. Это может делаться путем сравнения DG1, хранящейся на чипе, с MRZ, напечатанной на странице данных паспорта. Если DG1 и MRZ сопоставимы, объект защиты документа действителен, а предъявленный МСПД не искажен (не подделан), то можно считать, что МСПД и хранящиеся на чипе данные принадлежат друг другу.

A7.2.2 *Активная аутентификация*

Активная аутентификация усложняет подмену чипа, но не делает ее невозможной. МСПД, предъявленный злоумышленником системе проверки, может быть оснащен специальным чипом. Этот чип действует в качестве заменителя подлинного чипа, находящегося в уединенном месте; чип взаимодействует со злоумышленником, злоумышленник взаимодействует с другим злоумышленником, и этот другой злоумышленник получает доступ (временно) к подлинному чипу. Система проверки не способна заметить, что она аутентифицирует не предъявленный чип, а чип, находящийся на некотором расстоянии. Такое нападение называется гроссмейстерской атакой.

A7.3 Угроза нарушения конфиденциальности

A7.3.1 *Отсутствие контроля доступа*

Использование чипов, действующих через малый зазор, уже свело к минимуму риски нарушения конфиденциальности, так как считывающие устройства должны находиться на очень близком расстоянии от чипа; в этой связи скимминг не является серьезной угрозой. Однако перехват

передач данных между чипом и считывателем возможен с большего расстояния. Государствам, желающим устранить эту угрозу, СЛЕДУЕТ осуществлять базовый контроль доступа.

A7.3.2 *Базовые ключи доступа*

Базовые ключи доступа, используемые для аутентификации считывателя и настройки сеансовых ключей для шифрования передач данных между чипом и считывателем, генерируются из девятицифрового номера документа, даты рождения и даты истечения срока действия. Таким образом, энтропия ключей является относительно низкой. У МСПД со сроком действия десять лет энтропия составляет максимум 56 бит. При наличии дополнительных сведений (например, приблизительный возраст держателя или связь между номером документа и датой истечения срока действия) энтропия снижается еще больше. Вследствие относительно низкой энтропии, злоумышленник в принципе может записать зашифрованный сеанс, вычислить грубым методом базовые ключи доступа на основе аутентификации, вывести сеансовые ключи и расшифровать записанный сеанс. Однако это все-таки требует значительных усилий по сравнению с получением данных из других источников.

A7.3.3 *Активная аутентификация (трассировка данных)*

В запросно-ответном протоколе, используемом для активной аутентификации, чип помечает битовую строку, выбранную более или менее случайно системой проверки. Если принимающее государство использует текущую дату, время и местонахождение для генерации этой битовой строки непредсказуемым, но поддающимся проверке способом (например, с использованием защищенного аппаратного оборудования), третья сторона впоследствии может быть уверена в том, что подписавшийся находился в определенный день и время в определенном месте.

A7.4 Криптографические угрозы

Рекомендуемая минимальная длина ключей выбрана с таким расчетом, чтобы для расшифрования этих ключей необходимо было приложить определенные (как предполагается) усилия вне зависимости от выбранного алгоритма подписи.

Тип ключа	Уровень защиты
Подписывающийся СА страны	128 бит
Лицо, подписывающее документы	112 бит
Активная аутентификация	80 бит

A7.4.1 *Прогресс математики и нестандартное вычисление*

В соответствии с законом Мура вычислительные возможности удваиваются каждые 18 месяцев. Однако защита алгоритма подписи зависит не только от вычислительных возможностей; достижения в области математики (криптоанализ) и наличие новых нестандартных методов вычисления (например, квантовые компьютеры) также необходимо учитывать.

В связи с продолжительным сроком действия ключей весьма сложно делать предсказания относительно математического прогресса и наличия нестандартных вычислительных устройств. Поэтому рекомендации в отношении длины ключей базируются главным образом на

экстрапалированных вычислительных возможностях. По вышеупомянутым причинам государствам СЛЕДУЕТ часто пересматривать длину ключей для своих собственных, а также для получаемых МСПД.

Генерирование пар ключей специальной формы может в целом улучшить функционирование алгоритма подписи, но может также использоваться для криптоанализа в будущем. Поэтому применение таких специальных пар ключей СЛЕДУЕТ избегать.

A7.4.2 *Коллизия хэш-функции*

Хотя обнаружение другого сообщения, выдающего такое же хэш-значение, как и данное сообщение в вычислительном отношении представляется нереальным, обнаружить два сообщения, выдающих одинаковые хэш-значения, значительно легче. Это называется парадоксом дня рождения.

В целом, все подписываемые сообщения производятся самим лицом, подписывающим документы. Поэтому обнаружение хэш-коллизии не может значительно помочь злоумышленнику. Однако если фотографии, представленные просителем в цифровой форме, принимаются лицом, подписывающим документы, без дополнительной рандомнизированной модификации, может иметь место следующая атака.

- Два лица совместно используют свои цифровые фотографии. Они многократно "жонглируют" небольшим числом бит в каждой фотографии до тех пор, пока две фотографии не произведут одно и то же хэш-значение.

- Оба лица просят выдать новый МСПД, используя манипулированные фотографии. Каждое лицо может теперь использовать МСПД другого лица, при том условии, что цифровую фотографию на чипе можно заменить (например, путем подмены чипа).

Хэш-функция SHA-1 дает только 80 бит защиты от хэш-коллизии. Таким образом, обнаружить хэш-коллизию значительно легче, чем расшифровать ключ лица, подписывающего документы, который предоставляет 112 бит защиты. В этой связи в случае обеспокоенности проблемой хэш-коллизии (например, как описано выше) РЕКОМЕНДУЕТСЯ не использовать SHA-1 в качестве хэш-функции.

– КОНЕЦ –

ИЗДАНИЯ ИКАО И СВЯЗАННЫЕ С НИМИ МАТЕРИАЛЫ ПО ВОПРОСАМ ВОЗДУШНОГО ТРАНСПОРТА

Ниже приводится краткая информация о различных изданиях и связанных с ними материалах по вопросам воздушного транспорта, выпускаемых Международной организацией гражданской авиации:

- *Международные стандарты и Рекомендуемая практика (SARPS)* принимаются Советом в соответствии со статьями 37, 54 и 90 Конвенции о международной гражданской авиации и для удобства пользования называются Приложениями к Конвенции. Приложение 9 *"Упрощение формальностей"* содержит SARPS, касающиеся таможни, карантина, здравоохранения, иммиграции, а также вопросов здравоохранения, связанных с международной аэронавигацией. Приложение 17 *"Безопасность"* содержит SARPS по всем вопросам, относящимся к защите международной гражданской авиации от актов незаконного вмешательства. В соответствии со статьей 38 Конвенции необходимо уведомлять Совет о всех случаях расхождения национальных правил и практики государства с положениями Международных стандартов. Совет также предлагает Договаривающимся государствам сообщать о расхождениях с положениями Рекомендуемой практики.

- *Политика ИКАО* в области регулирования международного воздушного транспорта, аэропортовых сборов и сборов за аэронавигационное обслуживание, а также налогообложения в области международного воздушного транспорта.

- *Технические характеристики* машиносчитываемых проездных документов (МСПД).

- *Тарифы* на аэропортовое и аэронавигационное обслуживание, включая сборы, взимаемые с пользователей в более чем 180 государствах.

- *Руководства,* содержащие информацию или инструктивный материал, представляющие интерес для Договаривающихся государств по таким вопросам, как регулирование международного воздушного транспорта, управление финансовой деятельностью аэропортов и аэронавигационных служб, методы прогнозирования воздушных перевозок и соблюдение положений Приложения 17.

- *Циркуляры,* содержащие специализированную информацию, представляющую интерес для Договаривающихся государств. Они включают исследования о среднесрочных и долгосрочных тенденциях в отрасли воздушного транспорта на глобальном и региональном уровне и специальные исследования мирового характера, охватывающие такие вопросы, как экономические и финансовые аспекты внедрения систем CNS/ATM, региональные различия в эксплуатационной деятельности авиакомпаний, экономический вклад гражданской авиации, приватизация аэропортов и аэронавигационных служб и нормативно-правовые последствия распределения "слотов".

- *Учебные комплекты по авиационной безопасности (УКАБ) и курсы* по ряду тем, предназначенные для оказания помощи специалистам по авиационной безопасности, управленческому звену и сотрудникам в формировании более всестороннего понимания SARPS, а также в целях предложения специального практического опыта в реализации и отслеживании мер и положений в соответствии с местными программами. Дополнительную информацию можно получить на сайте avsec@icao.int или прочитать на учебной странице web-сайта AVSEC ИКАО по адресу www.icao.int/avsec.

- *Издания в электронной форме*, содержащиеся в базе данных и интерактивном формате, такие, как международные соглашения о воздушных сообщениях и разработанные ИКАО образцы соглашений о воздушных сообщениях. *Статистические данные о гражданской авиации* можно получить по ежегодной подписке на одну или несколько серий данных, распространяемых ИКАО через ее коммерческий web-сайт по адресу www.icaodata.com. Вопросы, касающиеся статистики ИКАО или специальных заказов на статистические данные, следует направлять по адресу sta@icao.int.

- *Доклады о совещаниях в области воздушного транспорта,* включая доклады специализированных совещаний по упрощению формальностей и статистике и доклады конференций по авиационной безопасности, регулированию международного воздушного транспорта и экономике аэропортов и аэронавигационного обслуживания.

10/07, R/P1/75

Заказ № 9303P1-2
Отпечатано в ИКАО

ISBN 978-92-9231-004-2