ICAO

Doc 9303

机读旅行证件

第七版，2015 年

第 10 部分 在非接触式集成电路（IC）中存储生物特征和其他数据的逻辑数据结构（LDS）

经秘书长批准并由其授权出版

国际民用航空组织

ICAO

Doc 9303

机读旅行证件

第七版，2015 年

第 10 部分 在非接触式集成电路（IC）中存储生物特征和其他数据的逻辑数据结构（LDS）

经秘书长批准并由其授权出版

国际民用航空组织

国际民用航空组织分别以中文、阿拉伯文、英文、法文、俄文和西班牙文版本出版
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

下载文件和获取额外信息，请登录 www.icao.int/security/mrtd。

Doc 9303 号文件 —《机读旅行证件》
第 10 部分 —在非接触式集成电路（IC）中存储生物特征和
其他数据的逻辑数据结构（LDS）
ISBN 978-92-9249-962-4

修订

《产品和服务目录》的补篇中公布了各项修订；在国际民航组织网站 www.icao.int 上有本目录及其补篇。以下篇幅供记录修订之用。

修订和更正记录

修订		
编号	日期	换页人

更正		
编号	日期	换页人

本出版物中所用称谓和陈述材料之方式，并不代表国际民航组织对任何国家、领土、城市或地区或其当局的法律地位，或就其边境或疆界的划分，表达了任何意见。

目录

1. 范围

Doc 9303 号文件第七版对国际民航组织关于机读旅行证件的规范进行了结构调整。在 Doc 9303 号文件的这一新版本中并未纳入对规范的大量修改，而是对文件进行了重新编排，形成一套关于 1 型机读官方旅行证件（TD1）、2 型机读官方旅行证件（TD2）和 3 型机读旅行证件（TD3）以及签证的规范。这套规范由多个不同文件组成，其中对一般规范（适用于所有机读旅行证件）以及与特定尺寸的机读旅行证件相关的规范做了分类。

Doc 9303 号文件第 10 部分界定了全球互操作性所需要的电子机读旅行证件的逻辑数据结构（LDS）和非接触式 IC 上数据编排的规范。这需要识别所有必需和选择性数据元素和必须遵循的数据元素的规定性排序和/或编组以实现电子机读旅行证件的电子阅读的全球互操作性。

Doc 9303 号文件第 10 部分提供了使国家和集成商将非接触式 IC 芯片嵌入电子机读旅行证件的规范，界定了所有必需和可选的数据元素、文件结构以及非接触式 IC 芯片的应用规格。

第 10 部分应结合以下部分进行阅读：

- 第 1 部分 — 引言；
- 第 3 部分 — 所有机读旅行证件的通用规范；
- 第 4 部分 — 机读护照（MRP）和其他 TD 3 型机读旅行证件规范；
- 第 5 部分 — TD1 型机读官方旅行证件（MROTDs）规范；
- 第 6 部分 — TD2 型机读官方旅行证件（MROTDs）规范。

和相关非接触式 IC 部分：

- 第 11 部分 — 机读旅行证件的安全机制；
- 第 12 部分 — 机读旅行证件的公钥基础设施。

2. 逻辑数据结构的要求

由签发国或签发机构选择的电子机读旅行证件中所包含的非接触式 IC 扩容技术必须使数据可被接收国访问。

国际民航组织已确定预定义的、标准化的逻辑数据结构（LDS）应满足一些强制性要求：

- 确保以高效和最佳方式为合法持证人提供便利；
- 确保以选择性的扩容技术记录的信息得到保护；
- 在所有电子机读旅行证件使用通用的单一逻辑数据结构时，使扩容数据具有全球互操作性；
- 解决签发国和签发机构的各种选择性扩容需求；
- 随着用户需求和现有技术的演变提供扩容；
- 支持多种数据保护选项；
- 尽最大可能利用现有国际规范，尤其是关于全球互操作生物特征的新兴国际规范。

2.1 安全

数据完整性和真实性是可信的全球互操作性所必需的。

数据组 1 至 16 均应是被写保护的。每个使用的数据组的散列值均应被存储在证件安全对象（EF.SO_D）中。

只有签发国或签发机构有这些数据组的写访问权限。因此，没有任何交换要求，且实现写保护的方法不属于本规范的部分。

2.2 数据的真实性和完整性

要确认记录详细信息的真实性和完整性，需要包含一个真实性/完整性对象。每个数据组均必须体现在该真实性/完整性对象中，该对象记录在一个独立的基本文件（EF.SO_D）中。通过使用编码识别特征数据组 2-4 所利用的生物特征通用交换文件格式（CBEFF）结构和 Doc 9303 号文件第 12 部分界定的选择性“其他生物特征安全”特性，身份确认详细信息（如生物特征模板）也可由签发国或签发机构自行决定单独予以保护。

2.3 逻辑数据结构的排序

随机排序方案只应用于促进国际互操作性。

2.3.1 随机排序方案

随机排序方案可使数据组和数据元素在与选择性扩容技术能力相符的随机排序后被记录下来，以便可直接检索特定的数据元素，即使它们是被无序记录的。可变长度的数据元素被编码为 ASN.1 中界定的 TLV（标志长度值）数据对象。

2.3.2　随机访问文件表示方式

随机访问文件表示方式的确定出于以下考虑和假设。

- 支持多种实施方式。逻辑数据结构包括多种选择性数据元素。纳入这些数据元素是为了便利电子机读旅行证件认证、合法持有人认证，并加快证件/人员环节的处理。
- 数据结构必须支持：
  - o　数据元素有限或扩充集；
  - o　特定数据元素的多次出现；
  - o　特定实施方式的继续演变。
- 支持至少一个应用数据集；
- 考虑到其他国家特定应用；
- 使用存储的非对称密钥对来支持证件的选择性主动认证；
- 支持快速访问选定的数据元素以便利快速的证件处理：
  - o　即时访问必要的数据元素；
  - o　直接访问数据模板和生物特征数据。

2.3.3　数据元素的分组

由签发国或经批准的接收组织添加的数据元素的分组可以存在，也可以不存在于逻辑数据结构中。接收国或经批准的接收组织添加的分组数据元素的一次以上记录可存在于 LDS（逻辑数据结构）中。

在本版 Doc 9303 号文件中不支持接收国或经批准的接收组织对逻辑数据结构添加数据的能力。

LDS 机读时被认为是一个单独的内聚实体，包含采用选择性扩容技术记录的数据元素分组的数量。

逻辑数据结构的设计具有足够的灵活性，它可以适用于所有类型的电子机读旅行证件。在随后的图表中，一些数据项目只适用于机读签证和机读护照，或者需要一种关于这些证件的不同表示方式。

在逻辑数据结构中，相关数据元素的逻辑编组已经建立。这些逻辑编组被称为数据组。

各数据组被分配一个参考号。图 1 标示出分配给每个数据组的参考号，例如，“DG2”表示数据组 2，电子机读旅行证件持有人面部的编码识别特征（即面部生物特征详细信息）。

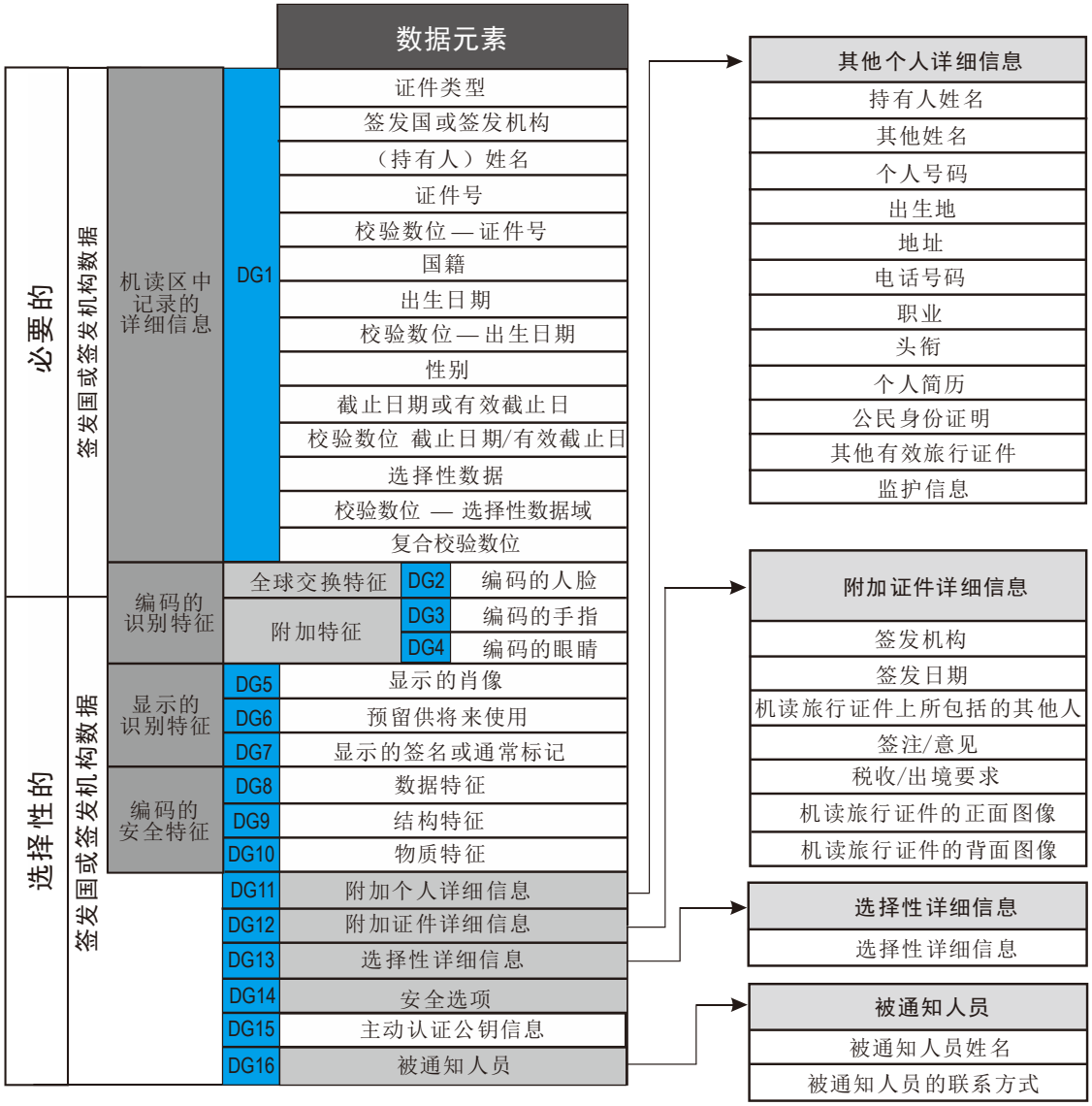

图 1　分配给逻辑数据组的数据组参考号

3. 非接触式 IC 的应用简介

3.1 互操作性最低要求

以下应是基于近场非接触式 IC 的电子机读旅行证件的最低互操作性要求：

- [ISO/IEC 14443-1]，[ISO/IEC 14443-2]，[ISO/IEC 14443-3]，[ISO/IEC 14443-4]包括所有相关的修订和更正；
- [ISO/IEC 10373-6]符合测试规范，包括所有相关的修订和更正；
- A 型或 B 型信号接口；
- 支持[ISO / IEC 7816-4]为可变长度透明文件定义的文件结构；
- 支持 Doc 9303 号文件规定的一个或多个应用和适当的[ISO/IEC 7816-4]命令；
- 应用系列标识符（AFI）为 0xE1（电子机读旅行证件）。应用标识符（AID: 0xA0000002471001）的 CRC_B 应为 0xF35E。

3.2 电气特性

射频功率和信号接口应符合[ISO/IEC14443-3]。建议每秒传输速度最少为 424 千比特。[ISO/IEC14443-2/Amd 1]中规定的电磁干扰特性的利用是选择性的。

3.3 物理特性

建议耦合天线面积的大小只参照[ISO/IEC14443-1]1 级（ID-1 天线尺寸）标准。

3.4 非接触式 IC 的数据存储容量

非接触式 IC 的数据存储容量由签发国自行决定，但应至少为 32 千字节。这一最小容量是存储强制存储的面部图像（通常为 15 至 20 千字节）、机读区数据以及确保数据安全的必要元素所必需的。其他面部、指纹和/或虹膜图像的存储可能需要显著增加数据存储的容量。非接触式 IC 的最大数据容量不做规定。

如果没有可用于作为个人化的一部分对电子机读旅行证件数据进行签名的国家公钥基础设施，并且证件的签发不能推迟，建议将电子机读旅行证件的非接触式 IC 留出空白并锁定。电子机读旅行证件应包含一个关于此事的适当签注。预计这是一种特殊情况。

3.5 其他数据的存储

一国可使用电子机读旅行证件中非接触式 IC 的存储容量，以便在为全球互操作性定义的机读数据容量基础上扩充电子机读旅行证件的机读数据容量。这样做的目的是便于机器读取身份证件信息（如出生证书细节）、存储的个人身份确认（生物特征）和/或证件真实性验证信息等。

3.6 存储于逻辑数据结构中的最低限度数据项

将存储于非接触式 IC 上的逻辑数据结构中的最低限度强制性数据项应是数据组 1 中的机读区数据和数据组 2 中的持有人面部图像的复制。此外，一个合规的电子机读旅行证件中的 IC 应包含验证签发人产生的数据完整性所必需的证件安全对象（EF.SO_D）。这些数据项被存储在逻辑数据结构中规定的、被称为电子机读旅行证件应用的专用文件（DF）中。该证件安全对象（EF.SOD）由使用的数据组的散列值组成。

3.7 符合 ISO/IEC 14443 的初始化、防冲突和传输协议

3.7.1 传输协议

电子机读旅行证件应支持[ISO/IEC14443-4]中定义的半双工传输协议。电子机读旅行证件应支持 A 型或 B 型传输协议。

3.7.2 请求命令和对请求的应答

非接触式 IC 应酌情以“应答 A 型请求”（ATQA）或“应答 B 型请求”（ATQB）来对“A 型请求命令”（REQA）或“B 型请求命令”（REQB）作出回应。

3.7.3 非接触式 IC 的随机与固定标识符

电子机读旅行证件可以作为一个“信标”，其中非接触式 IC 在最初启动时发出一个 A 型的唯一标识符（UID）和 B 型的伪唯一接触式集成电路卡标识符（PUPI）。这可用于签发机构的识别。[ISO/IEC14443]允许对以下选项进行选择，即电子机读旅行证件是提供一个仅为该证件唯一指定的固定标识符，还是一个在每次启动通信对话时都不相同的随机数。有些签发国出于安全考虑或其他原因更希望实施一个唯一的号码。另外一些签发人则更多关注采用固定 IC 标识符引发的数据隐私和跟踪持证人踪迹可能性的问题。

不管选择哪一个选项都不会削减互操作性，因为当符合 ISO/IEC 14443 时，阅读器终端都会理解这两种方法。建议使用随机 IC 标识符，但各国也可以选择应用 A 型的唯一标识符或 B 型的伪唯一接触式集成电路卡标识符（PUPI）。

3.8　命令集

所有的命令、格式及其返回代码在[ISO/ IEC78164]中都进行了定义。由 eMRTD 支持的最小命令集必须如下：

SELECT（选择）；
READ BINARY（读二进制）。

人们认识到，为建立正确安全的环境和实现 Doc9303 号文件第 11 部分所述的选择性安全规定，还需要一些其他的命令。实施 Doc9303 号文件第 11 部分规定的机制需要支持以下附加命令：

GET CHALLENGE（获得挑战）；
EXTERNAL AUTHENTICATE（外部认证）；
INTERNAL AUTHENTICATE（内部认证）；
MANAGE SECURITY ENVIRONMENT（管理安全环境）；
GENERAL AUTHENTICATE（通用认证）。

关于命令协议的进一步细节见 Doc9303 号文件第 11 部分。

3.8.1　选择

电子机读旅行证件支持两种结构选择方法，即文件标识符和短 EF（基本文件）标识符。阅读器至少支持这两种方法中的一种。文件标识符和短文件标识符对于非接触式 IC 操作系统来说是必要的，但对于阅读器来说是选择性的。

3.8.2　读二进制

电子机读旅行证件支持带一个奇数指令字节的 READ BINARY 命令是有条件的。电子机读旅行证件应支持该命令变体，如果它支持有 32 768 字节或以上的数据组的话。

3.9　命令格式和参数选项

3.9.1　应用选择

各种应用必须通过它们的文件标识符或应用名称来进行选择。选择一个应用之后，该应用内的文件可以被访问。

注：应用名称必须是唯一的。因此可以从任何需要的地方选择使用该应用名称的一个应用。

3.9.1.1 主文件的选择

表 1 主文件的选择

CLA	INS	P1	P2	发送数据长度 Lc	数据	响应数据长度 Le
00	A4	00	0C	空	空	空

注：建议不使用 SELECT MF（选择主文件）命令。

3.9.1.2 通过应用标识符选择一应用

应通过使用专用文件 DF 名称来选择应用。APDU（应用协议数据单元）命令的参数如下所示：

表 2 SELECT Application（选择应用）命令

CLA	INS	P1	P2	发送数据长度 Lc	数据	响应数据长度 Le
00	A4	04	0C	可变	应用标识符	–

第一个[ISO/IEC 7816-4]指令是“选择应用”，代码为 0x00A4040C07A0000002471001。每个电子机读旅行证件应用均支持该选择命令。

3.9.2 使用 SELECT 命令选择基本文件

必须通过文件标识符来选择文件。当通过文件标识符选择文件时，必须确保文件存储于其内的应用事先已被选择。

表 3 SELECT File（选择文件）命令

CLA	INS	P1	P2	发送数据长度 Lc	数据	响应数据长度 Le
00	A4	02	0C	02	文件标识符	–

电子机读旅行证件应支持带表 3 中指定的文件标识符的 SELECT（选择）命令。查验系统应至少支持下列方法中的一个：

- 带表 3 中指定的文件标识符的 SELECT 命令；
- 带表 5 中指定的偶数指令字节和短文件标识符的 READ BINARY 命令。

3.9.3　读取来自基本文件的数据（读二进制）

有两种方法读取来自电子机读旅行证件的数据：通过选择该文件，然后读取数据，或通过使用短文件标识符直接读取数据。对于电子机读旅行证件，支持短文件标识符是必要的。因此建议查验系统使用短文件标识符。

3.9.3.1　读取选定文件（透明文件）的数据

表 4　READ BINARY（读二进制）命令

CLA	INS	P1	P2	发送数据长度 Lc	数据	响应数据长度 Le
00	B0	偏移最高有效位	偏移最低有效位	–	–	最大重传次数

3.9.3.2　使用短文件标识符（透明文件）读取数据

表 5　用短文件标识符 READ BINARY（读二进制）命令

CLA	INS	P1	P2	发送数据长度 Lc	数据	响应数据长度 Le
00	B0	短文件标识符	偏移最低有效位	–	–	最大重传次数

3.9.4　扩展的 Lc/Le 支持

根据加密对象（如公钥、签名）的大小，必须使用带扩展长度域的 APDU 将该数据发送至机读旅行证件芯片。有关扩展长度的细节，见[ISO/IEC 7816-4]。

3.9.4.1　机读旅行证件芯片

对于机读旅行证件芯片来说，支持扩展长度是有条件的。如果签发国选择的加密算法和密钥大小需要使用扩展长度，则机读旅行证件芯片应支持扩展长度。如果机读旅行证件芯片支持扩展长度，则必须按照[ISO/IEC 7816-4]的规定，在复位应答/选择应答（ATR/ATS）或 EF.ATR/INFO 中指明。

3.9.4.2 终端

对于终端而言，支持扩展长度是必要的。在使用此选项之前，终端应检查是否支持机读旅行证件芯片中的 ATR/ATS 或 EF.ATR/INFO 中标明的扩展长度。除了下列命令，终端不得使用 APDU 的扩展长度，除非 ATR/ATS 或 EF.ATR/INFO 中明确说明机读旅行证件芯片输入输出缓冲区的大小。

- MSE: Set KAT；
- General Authenticate。

3.9.5 命令链

命令链必须用于 General Authenticate 命令，以便将命令的顺序与协议的执行连接。命令链不得用于其他目的，除非芯片明确说明。关于命令链的详细信息，见 [ISO/IEC 7816-4]。

3.9.6 大于 32 767 字节的基本文件

一个基本文件的最大尺寸通常是 32 767 字节，但一些非接触式 IC 支持更大的文件。当偏移大于 32 767 时，需要一个不同的 READ BINARY 参数选项和命令格式来访问数据区。该命令格式应在确定了模板长度并且确定了需要访问扩展数据区内的数据后予以使用。例如，如果数据区包含多个生物特征数据对象，就可能不必读取整个数据区。一旦数据区的偏移大于 32 767，就应使用该命令格式。偏移被置于命令域而不是置于参数 P1 和 P2 中。

表 6 大于 32 767 字节的基本文件命令格式

CLA	INS	P1	P2	发送数据长度 Lc	数据	响应数据长度 Le	备注
00	B1	00	00	可变	编码的偏移 TLV	00	读取大于 32 767 字节的文件

BER-TLV（基本编码规则-标志长度值）数据对象的长度域和值域均为可变长度，并能以不同的方式进行编码（见[ISO/IEC 7816-4]：“BER-TLV 长度域”）。

出于性能上的原因，电子机读旅行证件与终端之间的通信应该保持尽可能短。因此 BER-TLV 数据对象中的长度域和值域应该尽可能短。这不仅适用于奇数 INS READ BINARY 命令中的偏移数据对象，也适用于电子机读旅行证件与终端之间交换的所有其他 BER-TLV 数据对象。

数据域中偏移编码的例子：

- 偏移：0x0001 被编码为标志 = 0x54 长度 = 0x01 值 = 0x01;
- 偏移：0xFFFF 被编码为标志 = 0x54 长度 = 0x02 值 = 0xffff。

随后的 READ BINARY 命令应指明数据域中的偏移量。最终的 READ BINARY 命令应请求剩余数据区。

Le 字节包含 0x00 或者含有扩展的标志长度和值的字节数。

为了某些目的，B1 和传统的 B0 READ Binary 命令不能重叠。换言之，B0 只应当用于读取前 32 767 字节，B1 用于读取 32 千字节以上的部分。为其他目的，32 767 阈值周围可能有 256 字节的一个小重叠以使 B0 与 B1 之间有一个较顺畅的过渡。对于这后一组，B1 可以从文件的开始就使用，即从 0 开始有一个偏移以允许使用相同的命令来读取全部内容。关于[ISO / IEC 7816-4]，当 INS 的位 1 被设置成 1 时，没有规定对偏移值的约束以允许更广泛的使用。

如果一个基本文件的大小是 32 767 字节或更少，则查验系统不使用奇数 INS 字节。

4. 文件结构规范

电子机读旅行证件中的信息存储在[ISO/IEC 7816-4]定义的文件系统中。该文件系统按层次结构包括专用文件（DF）和基本文件（EF）。专用文件（DF）包含基本文件或其他专用文件。选择性的主文件（MF）可以是文件系统的根目录。该文件结构的图形表示见图 2。

注：是否需要主文件由操作系统和选择性的访问条件来决定。

4.1 应用选择 — 专用文件

电子机读旅行证件应支持以下至少一个应用：

- 应用应包括签发国或签发机构记录的数据、数据组 1 至 16 连同证件安全对象（EF. SO_D）；
- 证件安全对象（EF.SOD）包括 Doc 9303 号文件第 11 部分和第 12 部分中定义的数据组的散列值，它用于验证签发人创建并存储于电子机读旅行证件应用中的数据的完整性。

此外，签发国或签发机构似宜添加其他应用。文件结构应考虑到这种附加的应用，但这种应用的具体情况不属于 Doc 9303 号文件的范围。

电子机读旅行证件应用应通过使用作为预留 DF 名的应用标识符（AID）来选择。应用标识符应包括国际标准化组织根据[ISO/IEC7816-5]分配的注册应用标识符和本文件中规定的专有应用标识符扩展项（PIX）：

- 注册应用标识符是 0xA000000247；
- 签发机构存储的数据应用应使用 PIX = 0x1001;
- 电子机读旅行证件应用的全 AID 是 ‘A0 00 00 02 47 10 01’。

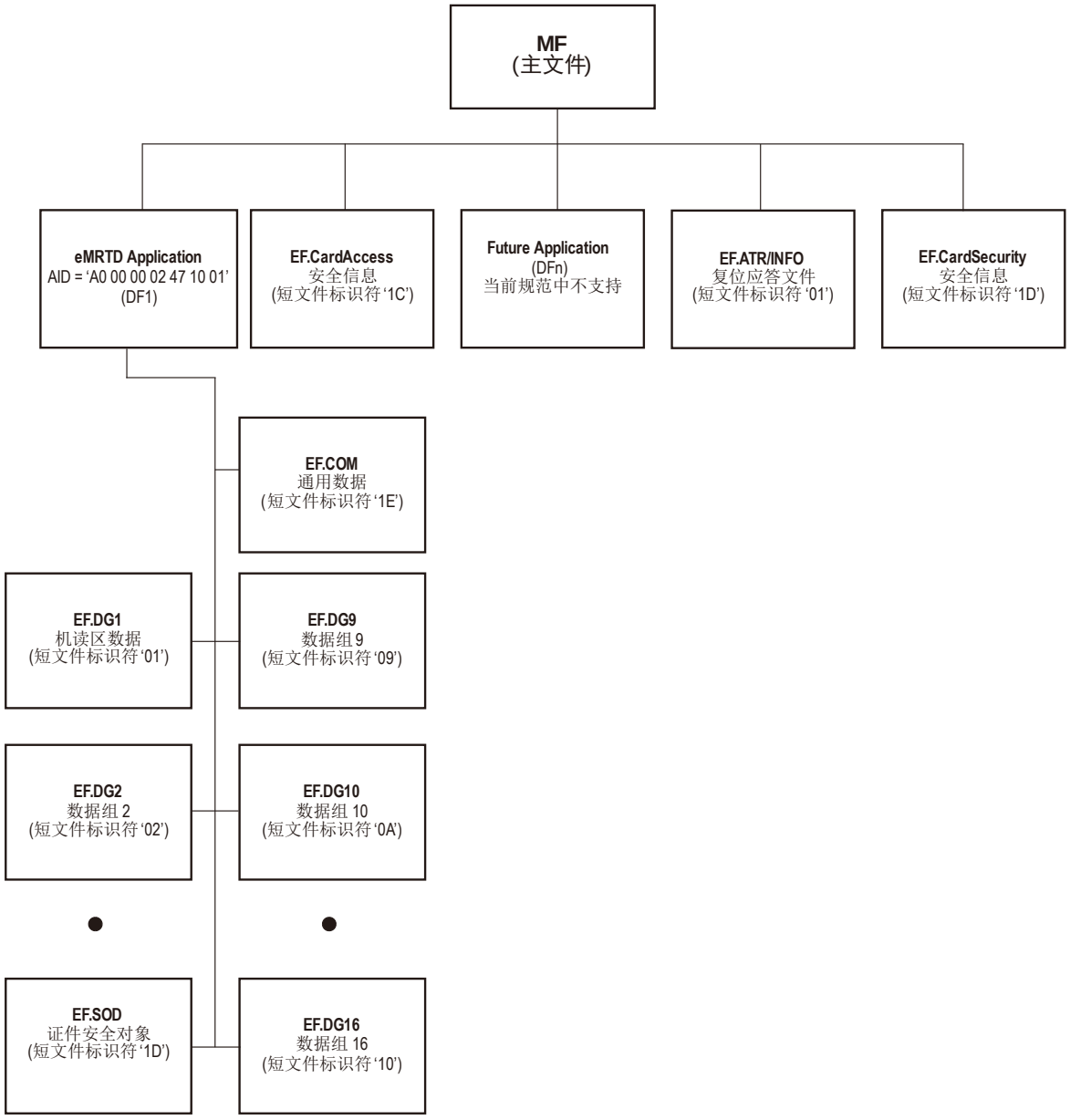

图 2　文件结构简表

4.2　数据组

在每个应用内可以有若干个数据组，有时被称为基本文件（EF）。签发国或签发机构应用最多可以有 16 个数据组。数据组 1（DG1），机读区（MRZ）和数据组 2，编码的人脸数据是必要的。其他数据组都是选择性的。所有的数据组均采用数据模板形式并有单独的 ASN.1 标记。每个数据组包含模板内的一系列数据对象。每个数据组均应存储在一个单独的基本文件（EF）中。数据组的各数据对象在确定了透明文件内的相对位置后可以直接被检索。

4.3　数据元素编码规则

文件包含作为模板内数据对象的数据元素。数据对象的结构和编码在[ISO/IEC 7816-4]和[ISO/IEC 7816-6]中进行了定义。每个数据对象均有一个以十六进制编码表示的识别标志（例如，0x5A）。本节中定义的标志使用共存编码选项。每个数据对象均有一个唯一的标志、长度和值。文件中可能存在的数据对象被标识为（M）或选择性的（0）。尽可能使用行业间标志。需要注意的是，已修改了一些标志的具体定义和格式以使它们与电子机读旅行证件应用相关。例如：

- 标志 0x5A 被定义为证件号，而不是主账号，采用格式 F9N 而非 V19N；
- 标志 0x5F20，持卡人的姓名，已被重新定义为“持有人姓名”，长度可达 39 个字符，按照 Doc9303 号文件格式进行编码；
- 标志 0x65 被定义为显示的肖像而不是持卡人相关数据；
- 根据需要，附加的标志定义在 0x5F01 至 0x5F7F 范围内。

4.3.1　数据元素编码规范说明

在逻辑数据结构（版本 1.7 和 1.8）规范与[ISO/IEC 8825-1]（BER/DER 编码规则）之间存在不匹配情况，其中[ISO/IEC8825-1]带有从零到 30（含）的数字标识符八位字节标志的国家应包括一个单独的八位组字节，其编码如下：

- 位 8 和位 7 应进行编码以表示标志的类别；
- 位 6 应是 0 或 1；
- 位 5 到位 1 应将标志数编码为二进制整数，位 5 作为最高有效位。

这意味着（例如）逻辑数据结构规范版本号的标志应定义为标志 0x41=0x01000001b：

- 其中 01 是指应用类（位 8 和位 7）；
- 其中 0 是指它是一个基本要素（位 6）；
- 其中 00001 是标志数 1（位 5-1）的编码。

在 Doc 9303 号文件中，逻辑数据结构规范的版本号标志被定义为标志 0x5F01= 0x0101111100000001b:

- 其中 01 是指应用类；
- 其中 0 是指它是一个基本要素（非构建的）；
- 其中 11111 是指该标志数在接下来的字节中被编码；

- 其中 0 是指它是编码标志数的最后字节；
- 其中 0000001 是标志数 1 的编码。

这计数从零到 30（含）的所有标志:

- 0x5F01, 0x5F08, 0x5F09, 0x5F0A, 0x5F0B, 0x5F0C, 0x5F0E, 0x5F0F, 0x5F10, 0x5F11, 0x5F12, 0x5F13, 0x5F14, 0x5F15, 0x5F16, 0x5F17, 0x5F18, 0x5F19, 0x5F1A, 0x5F1B, 0x5F1C, 0x5F1D, 0x5F1E。

实施者应该知晓这种不匹配并遵循 Doc9303 号文件所述的规范。但应该注意：

- 使用基于 ASN.1 的生成器不能实现创建电子机读旅行证件；
- ASN.1/基本编码规则解析器可能返回一个错误而不是正确解析 EF.COM；
- EF.COM 上的散列值不能通过解码 EF.COM 结构和之后对它进行再编码来重新创建。

4.3.2 数据元素存在图（DEPM）

存在图的概念与多个数据组一起使用，这些数据组包含制作记录的国家或组织可能自行决定纳入的一系列从属数据元素。这些称为数据元素存在图（DEPM）的存在图位于允许选择性扩展的特定数据组的开始。

数据元素存在图包含使接收国或经批准的接收组织能够确定数据组中存在哪些数据元素的信息。

数据元素存在图包含一个与识别电子机读旅行证件中记录的数据元素的约定相一致的标志列表，其中每个标志识别某个特定数据元素是否被记录在数据组中。这种形式的数据元素存在图被编码为相关数据组内的一个标志列表。

4.3.3 ASN.1 BER TLV 数据对象的长度编码规则

必须使用[ISO/IEC8825-1]中界定的 ANS.1 长度编码的确定形式。

表 7 长度编码规则

范围	字节数	第 1 字节	第 2 字节	第 3 字节
0 到 127	1	二进制值	无	无
128 到 255	2	81	二进制值	无
256 到 65 535	3	82	二进制值 最高有效位	最低有效位

4.4　逻辑数据结构语境中使用的规范标志

表 8　规范标志简表

标志	定义	使用地方
02	整数	生物特征和显示模板
5C	标志列表	EF.COM 和许多其他文件
5F01	LDS 版本号	EF.COM
5F08	出生日期（截取）	机读区
5F09	压缩图像（ANSI/NIST-ITL 1-2000）	显示的手指
5F0A	安全特征 — 编码数据	安全特征（细节待定）
5F0B	安全特征 — 结构	安全特征（细节待定）
5F0C	安全特征	安全特征（细节待定）
5F0E	以本国字符写的全名	附加个人详细信息
5F0F	其他姓名	附加个人详细信息
5F10	个人号码	附加个人详细信息
5F11	出生地	附加个人详细信息
5F12	电话	附加个人详细信息
5F13	职业	附加个人详细信息
5F14	头衔	附加个人详细信息
5F15	个人简历	附加个人详细信息
5F16	公民资格证明（10918 图像）	附加个人详细信息
5F17	其他有效的旅行证件号	附加个人详细信息
5F18	监护信息	附加个人详细信息
5F19	签发机构	附加证件详细信息
5F1A	证件上的其他人	附加证件详细信息
5F1B	批注/意见	附加证件详细信息
5F1C	税收/出境要求	附加证件详细信息
5F1D	证件正面图像	附加证件详细信息

标志	定义	使用地方
5F1E	证件背面图像	附加证件详细信息
5F1F	机读区数据元素	机读区数据对象
5F26	签发日期	附加证件详细信息
5F2B	出生日期（8 位）	附加个人详细信息
5F2E	生物特征数据分组	生物特征数据
5F36	Unicode 版本级别	EF.COM
5F40	压缩图像模板	显示的肖像
5F42	地址	附加个人详细信息
5F43	压缩图像模板	显示的签名或标记
5F50	记录的日期数据	被通知人
5F51	人员姓名	被通知人姓名
5F52	电话	被通知人电话号码
5F53	地址	被通知人地址
5F55	个人化的证件日期和时间	附加证件详细信息
5F56	个人化系统的序列号	附加证件详细信息
60	通用数据元素	EF.COM
61	机读区数据组模板	
63	手指生物特征数据组模板	
65	数字化人脸图像模板	
67	数字化签名或通常标记模板	
68	机器辅助安全模板 — 编码数据	
69	机器辅助安全模板 — 结构	
6A	机器辅助安全模板 — 物质	
6B	附加个人详细信息模板	
6C	附加证件详细信息模板	

标志	定义	使用地方
6D	选择性详细信息	
6E	预留将来使用	
70	被通知人	
75	面部生物特征数据组模板	
76	虹膜（眼睛）生物特征模板	
77	EF.SO_D（证件安全对象基本文件）	
7F2E	生物特征数据分组（加密）	
7F60	生物特征信息模板	
7F61	生物特征信息组模板	
8x	情况特定标志	生物特征通用交换格式框架
90	加密散列值	真实性/完整性码
A0	特定情况构建的数据对象	附加个人详细信息
Ax 或 Bx	重复模板，其中 x 定义事件	生物特征首标

4.4.1　中间处理标志（资料性）

表 9　中间标志

标志	定义	使用地方
53	选择性数据	部分机读区
59	截止日期	部分机读区
5A	证件号	部分机读区
5F02	校验数位 — 选择性数据（仅 TD3 型机读旅行证件）	部分机读区
5F03	证件类型	部分机读区
5F04	校验数位 — 证件号	部分机读区
5F05	校验数位 — 出生日期	部分机读区
5F06	校验数位 — 截止日期	部分机读区
5F07	校验数位 — 复合	部分机读区

标志	定义	使用地方
5B	证件持有人姓名	部分机读区
5F28	签发国或签发机构	部分机读区
5F2B	出生日期	部分机读区
5F2C	国籍	部分机读区
5F35	性别	部分机读区
5F57	出生日期（6 位）	部分机读区

4.4.1.1 预留标志（规范性）

表 10 预留标志

标志	定义	使用地方
5F44	入境/出境国家	旅行记录
5F45	入境/出境日期	旅行记录
5F46	入境/出境口岸	旅行记录
5F47	入境/出境指示	旅行记录
5F48	停留时间	旅行记录
5F49	类别（分类）	旅行记录
5F4A	检查员	旅行记录
5F4B	入境/出境指示	旅行记录
71	电子签证模板	
72	过境方案模板	
73	旅行记录数据组模板	

4.5 LDS 版本管理

已经预期电子机读旅行证件逻辑数据结构组织的未来升级，将由国际民航组织通过出版规范修订本来解决这个问题。将分配给每次升级一个版本号，以确保接收国和经批准的接收组织将能准确地解码所有版本的逻辑数据结构。

4.5.1　LDS 版本 1.7

LDS 版本 1.7 必须实施本文件第 5 节所载的证件安全对象 EF.SOD 版本 V0。

4.5.2　LDS 版本 1.8

LDS 版本 1.8 必须实施本文件第 5 节所载的证件安全对象 EF.SOD 版本 V1。

5.　基本文件

5.1　首标和数据组存在信息 EF.COM（必要的）

EF.COM 位于电子机读旅行证件应用（短文件标识符=0x1E）中，包含 LDS 版本信息、Unicode 版本信息和存在供应用的数据组列表。该电子机读旅行证件应用只允许有一个包含该应用通用信息的文件 EF.COM。

该模板中可能会存在的数据元素如下：

表 11　EF.COM 规范性标志

标志	长度	值		
60	可变	应用级信息		
		标志	长度	值
		5F01	04	LDS 版本号格式 aabb，其中 aa 定义 LDS 的版本，bb 定义更新级别。
		5F36	06	Unicode 版本号格式 aabbcc，其中 aa 定义主要版本， bb 定义次要版本，cc 定义发布级别。
		5C	可变	标志列表。目前所有数据组的列表。

首标和数据组存在图应被包括在内。首标应包含以下信息以使接收国或经批准的接收组织能够定位和解码签发国或签发机构记录的数据分组内所包含的各种数据组和数据元素。

5.1.1　LDS 版本号

LDS 版本号定义 LDS 的格式版本。用于存储该值的确切格式将在本文件第 6 节中加以定义。LDS 版本号的标准化格式为“aabb”，其中：

- “aa”=标识 LDS 主要版本（即对 LDS 的显著增加）的号码（01-99）；
- “bb”=标识 LDS 次要版本的号码（01-99）。

5.1.2 Unicode 版本号

Unicode 版本号标识记录字母字符、数字字符和特殊字符，及国家字符所用的编码方法。用于存储该值的确切格式将在本文件第 6 节中加以定义。Unicode 版本号的标准化格式为“aabbcc”，其中：

- “aa”= 标识 Unicode 规范主要版本（即对出版成书的规范的显著增加）的号码；
- “bb”= 标识 Unicode 规范次要版本（即作为技术报告出版的字符添加或较显著的规范性修改）的号码；和
- “cc”= 标识 Unicode 规范的更新版本（即可能会改变程序性能的对规范的规范性或重要资料性部分的任何其他修改）的号码。这些修改反映在新的 Unicode 字符数据库文件和更新页中）。由于历史原因，每个域（即 a，b，c）内的编号不一定是连续的。

通用字符集（UCS）必须符合[ISO/IEC 10646]。

5.2 证件安全对象 $EF.SO_D$（必要的）

除了 LDS 数据组，非接触式 IC 还包含一个存储在 $EF.SO_D$ 中的证件安全对象。该对象由签发国进行数字签名，内容包含逻辑数据结构内容的散列值。

表 12 $EF.SO_D$ 标志

标志	长度	值
77	可变	证件安全对象

当前有两个版本的证件安全对象 EF.SOD 可用。实施 EF.SOD V0 或者 EF.SOD V1 是必要的。只允许一个 EF.SOD。

5.2.1 证件安全对象 EF.SOD 版本 V0 LDS v1.7（必要的）

LDS V1.7 的证件安全对象 V0 不包含 LDS 和 Unicode 版本信息：

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

5.2.2　SOD V0 的 SignedData 类型

证件安全对象根据[RFC 3369]的规定实现为 SignedData 类型。所有安全对象均应以唯一编码规则（DER）格式产生以确保签名的完整性。

注 1：m　必要的 — 该域应存在。
注 2：x　不使用 — 该域不应该被填充。
注 3：o　选择性的 — 该域可以存在。
注 4：c　选择 — 该域内容是从备选内容中选出的。

表 13　SO_D V0 的签名数据类型

值		说明
SignedData		
Version	m	值 = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	标识符 — 国际民航组织 — 机读旅行证件 — 安全 — 逻辑数据结构安全对象
eContent	m	逻辑数据结构安全对象的编码内容。
Certificates	o	各国可选择包括证件签名者证书（C_{DS}），它可以用来验证签名者信息域中的签名。
Crls	x	建议各国不使用该域。
signerInfos	m	建议各国在该域内只提供 1 个签名者信息。
SignerInfo	m	
Version	m	此域的值是由安全标识符域决定的。关于此域的规则见 RFC3369 Doc 9303 号文件第 12 部分。
Sid	m	
issuerandSerialNumber	c	建议各国支持主题密钥标识符上面的该域。
subjectKeyIdentifier	c	
digestAlgorithm	m	该算法的算法标识符用于产生封装的内容和签名属性上面的散列值。
signedAttrs	m	制作国可能希望在签名中包括额外的属性，但这些不必由接收国处理，除非是为验证签名值。

值		说明
signatureAlgorithm	m	该算法的算法标识符用于产生签名值和任何相关参数。
Signature	m	签名生成过程的结果。
unsignedAttrs	o	制作国可能希望使用该域，但不建议使用，接收国可以选择忽略它们。

5.2.3 SOD VO 的 ASN.1 配置文件逻辑数据结构证件安全对象

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

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

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

— Constants

ub-DataGroups INTEGER ::= 16

— Object Identifiers
id-icao   OBJECT IDENTIFIER ::= {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
```

注 1：dataGroupValue（数据组值）域包含由 dataGroupNumber（数据组号）指定的在数据组基本文件完整内容上面的计算散列值。

注 2：DigestAlgorithmIdentifiers（摘要算法标识符）必须省略“空值”参数，而如果不存在参数的话，即使在按照 RFC5754 使用 SHA2 算法时，SignatureAlgorithmIdentifier（签名算法标识符）（如 RFC3447 中定义的）必须包括空值作为参数。实施中，必须接受两个条件的 DigestAlgorithmIdentifiers（摘要算法标识符），即没有参数或有空值参数。

5.2.4　证件安全对象 EF.SOD V1 LDS v1.8（必要的）

LDS v1.8 的证件安全对象 V1 经扩展后具有一个签名属性，包含 LDS 和 Unicode 版本信息：

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

LDSVersionInfo ::= SEQUENCE {
ldsVersion PRINTABLE STRING
    unicodeVersion PRINTABLE STRING }
```

注：DigestAlgorithmIdentifiers（摘要算法标识符）必须省略“空值”参数，而如果不存在参数的话，即使在按照 RFC5754 使用 SHA2 算法时，SignatureAlgorithmIdentifier（签名算法标识符）（如 RFC3447 中定义的）也必须包括空值作为参数。实施中，必须接受两个条件的 DigestAlgorithmIdentifiers（摘要算法标识符），即没有参数或有空值参数。

5.2.5 SOD V1 的 SignedData 类型

按照 2002 年 8 月的[RFC3369]，加密消息语法（CMS）中的规定，证件安全对象作为一个签名数据类型予以实现。所有安全对象均必须以唯一编码规则（DER）格式产生以保持签名的完整性。

注 1：m 必要的 — 该域应存在。
注 2：x 不使用 — 该域不应被填充。
注 3：o 选择性的 — 该域可以存在。
注 4：c 选择 — 该域内容是从备选内容中选出的。

表 14 SO_D V1 的签名数据类型

值		说明
SignedData		
Version	m	值 = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	标识符 — 国际民航组织 — 机读旅行证件 — 安全 — 逻辑数据结构安全对象
eContent	m	逻辑数据结构安全对象的编码内容。
Certificates	m	各国可选择包括证件签名者证书（C_{DS}），它可以用来验证签名者信息域中的签名。
Crls	x	建议各国不使用该域。
signerInfos	m	建议各国在该域内只提供 1 个签名者信息。
SignerInfo	m	
Version	m	此域的值是由安全标识符域决定的。关于此域的规则见 RFC3369 Doc 9303 号文件第 12 部分。
Sid	m	
issuerandSerialNumber	c	建议各国支持主题密钥标识符上面的该域。
subjectKeyIdentifier	c	

值		说明
digestAlgorithm	m	该算法的算法标识符用于产生封装的内容和签名属性上面的散列值。
signedAttrs	m	制作国可能希望在签名中包括额外的属性，但是这些不必由接收国处理，除非是为验证签名值。
signatureAlgorithm	m	该算法的算法标识符用于产生签名值和任何相关的参数。
Signature	m	签名生成过程的结果。
unsignedAttrs	o	制作国可能希望使用该域，但不建议使用，接收国可以选择忽略它们。

5.2.6　SOD V1 的 ASN.1 配置文件逻辑数据结构证件安全对象

```
LDSSecurityObject {iso(2) identified-organization(23) icao(136)
mrtd(1) security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

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

— Constants

ub-DataGroups INTEGER ::= 16

— Object Identifiers

id-icao OBJECT IDENTIFIER ::= {2.23.136}
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-mrtd-security-ldsSecurityObject OBJECT IDENTIFIER ::= {idicao-
mrtd-security 1}

— LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {V0(0), V1(1)
— If LDSSecurityObjectVersion is V1, ldsVersionInfo MUST be present }

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
      version LDSSecurityObjectVersion,
```

```
    hashAlgorithm DigestAlgorithmIdentifier,
    dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
    DataGroupHash
    ldsVersionInfo LDSVersionInfo OPTIONAL
    — If present, version MUST be V1 }

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

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

LDSVersionInfo ::= SEQUENCE {
    ldsVersion PRINTABLE STRING
    unicodeVersion PRINTABLE STRING }
END
```

注 1：dataGroupValue（数据组值）域包含由 dataGroupNumber（数据组号）指定的在数据组基本文件完整内容上面的计算散列值。

注 2：DigestAlgorithmIdentifiers（摘要算法标识符）必须省略“空值”参数，而如果不存在参数的话，即使在按照 RFC5754 使用 SHA2 算法时，SignatureAlgorithmIdentifier（签名算法标识符）（如 RFC3447 中定义的）也必须包括空值作为参数。实施中，必须接受两个条件的 DigestAlgorithmIdentifiers（摘要算法标识符），即没有参数或有空值参数。

5.3　EF.CardAccess（基本文件. 卡访问）（有条件的）

主文件中包含的 EF.CardAccess 是一个透明的基本文件。如果按照 Doc 9303 号文件第 11 部分的规定调用选择性的口令认证连接确立访问控制，EF.CardAccess 在某些情况下是必要的。关于口令认证连接确立 SecurityInfos（安全信息）的完整描述，见 Doc9303 号文件第 11 部分。

5.3.1　非接触式 IC 上的内存

如果口令认证连接确立得到机读旅行证件芯片支持，主文件中包含的卡访问文件是必要的，并应包含口令认证连接确立所必需的以下安全信息：

- 口令认证连接确立信息；
- 口令认证连接确立域参数信息。

表 15　集成电路上的 EF.CardAccess 内存

文件名	EF.CardAccess
文件标识符	0x011C
短文件标识符	0x1C
读取访问	随时
写访问	永不
大小	可变
内容	唯一编码规则编码的安全信息 见 Doc 9303 号文件第 11 部分。

5.4　EF.CardSecurity（基本文件. 卡安全）（有条件的）

主文件中包含的 EF.CardSecurity 是一个透明的基本文件，如果按照 Doc 9303 号文件第 11 部分的规定调用利用芯片认证映射的可选口令认证连接确立的话，EF.CardSecurity 在某些情况下是必要的。关于利用芯片认证映射的口令认证连接确立安全信息的完整描述，见 Doc9303 号文件第 11 部分。

5.4.1　非接触式 IC 上的内存

如果利用芯片认证映射的口令认证连接确立得到机读旅行证件芯片支持，主文件中包含的卡安全文件是必要的并应包含以下安全信息：

- 利用芯片认证映射的口令认证连接确立所必需的芯片认证公钥信息；
- 卡访问中包含的安全信息。

表 16　集成电路上的 EF.CardSecurity 内存

文件名	EF.CardSecurity
文件标识符	0x011D
短文件标识符	0x1D
读取访问	口令认证连接确立
写访问	永不
大小	可变
内容	唯一编码规则编码的签名数据见 Doc 9303 号文件第 11 部分。

6. 形成数据组 1 至 16 的数据元素

数据组 1（DG1）至 16（DG16）分别由许多的、选择性的和有条件的数据元素组成。数据组内数据元素的特定顺序应予遵循。每个数据组应存储在一个透明的基本文件中。寻址基本文件应使用表 16 所示的短文件标识符。基本文件应有这些文件的文件名，文件名应以号码 n，EF.DGn 标识，DGn 中的 n 是数据组号。

表 17　联合形成数据组 1（DG1）至 16（DG16）结构的必需和可选数据元素

数据组	基本文件名称	短文件标识符	文件标识符	标志
通用	EF.COM	1E	01 1E	60
数据组 1	EF.DG1	01	01 01	61
数据组 2	EF.DG2	02	01 02	75
数据组 3	EF.DG3	03	01 03	63
数据组 4	EF.DG4	04	01 04	76
数据组 5	EF.DG5	05	01 05	65
数据组 6	EF.DG6	06	01 06	66
数据组 7	EF.DG7	07	01 07	67
数据组 8	EF.DG8	08	01 08	68
数据组 9	EF.DG9	09	01 09	69
数据组 10	EF.DG10	0A	01 0A	6A
数据组 11	EF.DG11	0B	01 0B	6B

数据组	基本文件名称	短文件标识符	文件标识符	标志
数据组 12	EF.DG12	0C	01 0C	6C
数据组 13	EF.DG13	0D	01 0D	6D
数据组 14	EF.DG14	0E	01 0E	6E
数据组 15	EF.DG15	0F	01 0F	6F
数据组 16	EF.DG16	10	01 10	70
证件安全对象	$EF.SO_D$	1D	01 1D	77
通用	EF.CARDACCESS	1C	01 1C	
通用	EF.ATR/INFO			
通用	EF.CardSecurity	1D	01 1D	

6.1　数据组 1 — 机读区信息（必要的）

数据组 1（DG1）的数据元素旨在反映机读区的全部内容，无论它包含实际数据还是填充符。关于实施机读区的详细信息取决于电子机读旅行证件的类型（ TD1,TD2 或 TD3 型机读旅行证件格式）。

该数据元素包含模板 0x61 中的证件所必要的机读区（MRZ）信息。该模板包含一个数据对象，机读区在数据对象 0x5F1F 中。机读区数据对象是一个复合数据元素，与证件上所印的 OCR-B 机读区信息相同。

表 18　数据组 1 标志

标志	长度	值		
61	可变			
		标志	长度	值
		5F1F	F	作为复合数据元素的机读区数据对象。 （必要的） （该数据元素包含从证件类型到复合校验数位的所有必需域。）

6.1.1　数据组 1 — TD1 型电子机读旅行证件的 EF.DG1 数据元素

本节描述数据组 1（DG1）中可能存在的数据元素。数据组 1 的存储、排序和编码要求旨在与印刷的机读区中所发现的以及 Doc9303 号文件第 3 部分和第 5 部分中所描述的完全相同。TD1 型机读官方旅行证件每个数据组区域内的数据元素及其格式应如下表所示：

注：A =字母字符 [A..Z]，N = 数字字符 [0..9]，S = 特殊字符 [‘<’]，F = 固定长度域。

表 19　TD1 型机读官方旅行证件格式的数据元素

数据 要素	选择性的或 必要的	数据元素名称	字节数	固定或 可变的	编码类型
01	M	证件代码	2	F	A,S
02	M	签发国或签发机构	3	F	A,S
03	M	证件号（九个最高有效字符）	9	F	A,N,S
04	M	校验数位 — 证件号或表明证件号超过九个字符的填充符（<）	1	F	N,S
05	M	可选数据和/或在证件号超过 9 个字符的情况下，证件号的最低有效字符加证件号校验数位加填充符	15	F	A,N,S
06	M	出生日期	6	F	N,S
07	M	校验数位 — 出生日期	1	F	N
08	M	性别	1	F	A,S
09	M	到期日期	6	F	N
10	M	校验数位 — 到期日期	1	F	N
11	M	国籍	3	F	A,S
12	M	可选数据	11	F	A,N,S
13	M	复合校验数位	1	F	N
14	M	持有人姓名	30	F	A,N,S

6.1.2　数据组 1 — TD2 型电子机读旅行证件的 EF.DG1 数据元素

本节描述数据组 1（DG1）中可能存在的数据元素。数据组 1 的存储、排序和编码要求旨在与印刷的机读区中所发现的以及 Doc9303 号文件第 3 部分和第 6 部分中所描述的完全相同。TD2 型机读官方旅行证件每个数据组区域内的数据元素及其格式应如下表所示：

注：A = 字母字符[A..Z]，N = 数字字符 [0..9]，S = 特殊字符 ['<']，F = 固定长度域。

表 20　TD2 型机读官方旅行证件格式的数据元素

数据 要素	选择性的或 必要的	数据元素名称	字节数	固定或 可变的	编码类型
01	M	证件代码	2	F	A,S
02	M	签发国或签发机构	3	F	A,S
03	M	持有人姓名	31	F	A,N,S
04	M	证件号（九个主要字符）	9	F	A,N,S
05	M	校验数位	1	F	N,S
06	M	国籍	3	F	A,S
07	M	出生日期	6	F	N,S
08	M	校验数位	1	F	N
09	M	性别	1	F	A,S
10	M	到期日期	6	F	N
11	M	校验数位	1	F	N
12	M	可选数据加填充符	7	F	A,N,S
13	M	复合校验数位 — 机读区 第 2 行	1	F	N

6.1.3 数据组 1 — TD3 型电子机读旅行证件的 EF.DG1 数据元素

本节描述数据组 1（DG1）中可能存在的数据元素。数据组 1 的存储、排序和编码要求旨在与印刷的机读区中所发现的以及 Doc9303 号文件第 3 部分和第 4 部分中所描述的完全相同。TD3 型机读官方旅行证件每个数据组区域内的数据元素及其格式应如下表所示：

注：A = 字母字符 [A..Z]，N = 数字字符 [0..9]，S = 特殊字符 ['<']，F = 固定长度域。

表 21 TD3 型机读旅行证件格式的数据元素

数据 要素	选择性的或 必要的	数据元素名称	字节数	固定或 可变的	编码类型
01	M	证件代码	2	F	A,S
02	M	签发国或签发机构	3	F	A,S
03	M	持有人姓名	39	F	A,S
04	M	证件号	9	F	A,N,S
05	M	校验数位 — 证件号	1	F	N,S
06	M	国籍	3	F	A,S
07	M	出生日期	6	F	N,S
08	M	校验数位 — 出生日期	1	F	N
09	M	性别	1	F	A,S
10	M	到期日期	6	F	N
11	M	校验数位 — 到期日期 或有效期截止日	1	F	N
12	M	可选数据	14	F	A,N,S
13	M	校验数位	1	F	N
14	M	复合校验数位	1	F	N

6.2　数据组 2 — 编码识别特征 — 人脸（必要的）

数据组 2（DG 2）是用机读旅行证件进行机器辅助身份确认时的全球互操作生物特征，它应是对面部识别系统输入的持有人面部图像。如果有一个以上的记录，最新的国际互操作编码应是第一输入项。

表 22　数据组 2 标志

标志	长度	值
75	可变	见 EF.DG2 的生物特征编码

6.2.1　EF.DG2 的生物特征编码

数据组 2 必须使用[ISO/IEC7816-11]中指定的带有嵌套生物特征信息模板的生物特征信息模板（BIT）组模板，以便能够存储多个生物特征模板并与生物特征通用交换格式框架（CBEFF）和谐一致。生物特征子首标界定存在的生物特征类型和特定的生物特征。[ISO/IEC[7816-11]的嵌套选项必须被使用，即使用于一个单独的生物特征模板的编码。后一种情况以 n=1 开始的编号表示。

每个嵌套模板具有以下结构：

表 23　数据组 2 — 生物特征编码标志

标志	长度	值				
7F61	可变	生物特征信息组模板				
		标志	长度	值		
		02	01	整数 — 该类生物特征的样品号		
		7F60	可变	第一个生物特征信息模板		
			标志	长度		
			A1	可变	生物特征首标模板（BHT）	
				标志	长度	值
				80	02	国际民航组织首标版本 0101（选择性的）— 生物特征通用交换格式框架保护人首标格式的版本
				81	01-03	生物特征类型（选择性的）
				82	01	数据组 2 的生物特征子类型（选择性的）
				83	07	创建日期和时间（选择性的）

标志	长度	值				
				85	08	有效期（从___至___）（选择性的）
				86	02	生物特征参考数据（PID）的创建者（选择性的）
				87	02	格式所有者（必要的）
				88	02	格式类型（必要的）
			5F2E 或 7F2E	可变	生物特征数据（根据格式所有者编码）也称为生物特征数据分组（BDB）。	
		标志	长度			
		7F60	可变	第 2 生物特征信息模板		
			标志	长度		
			A1	可变	生物特征首标模板（BHT）	
				标志	长度	值
				80	02	国际民航组织首标版本 ‘0101’（选择性的） —生物特征通用交换格式框架保护人首标格式的版本
				81	01-03	生物特征类型（选择性的）
				82	01	数据组 2 生物特征子类型（选择性的）
				83	07	创建日期和时间（选择性的）
				85	08	有效期（从___至___）（选择性的）
				86	04	生物特征参考数据（PID）的创建者（选择性的）
				87	02	格式所有者（必要的）
				88	02	格式类型（必要的）
			5F2E 或 7F2E	可变	生物特征数据（根据格式所有者编码）也称为生物特征数据分组（BDB）。	

使用生物特征通用交换格式框架的默认对象标识符。[ISO/IEC7816-11]中指定的就在生物特征信息模板（BIT，标志 0x7F60）下面的对象标识符数据对象（标志 0x06）不包括在此结构中。同样，该结构中没有指定标志分配权限。

为了促进互操作性，每个数据组中记录的第一个生物特征应按[ISO/IEC19794-5]的规定进行编码。

6.2.2　数据组 2 — EF.DG2 数据元素

本节描述数据组 2（DG2）中可能存在的数据元素。每个数据组区域内的数据元素及其格式应如下表所示：

注：A = 字母字符[a..z, A..Z]，N = 数字字符[0..9]，S = 特殊字符[‘<’]，B= 8 位二进制数据（A，N 或 S 以外的任何数据），F = 固定长度域，Var = 可变长度域。

表 24　数据组 2 的数据元素

数据元素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
01	M	记录的面部生物特征编码号	1	F	N	用 1 至 9 标识面部数据的唯一编码号。
02	M	首标		Var	A,N	数据元素可按 DE 01 的规定重现。
03	M	面部生物特征数据编码		Var	A,N,S,B	数据元素可按 DE 01 的规定重现。

6.3　数据组 3 — 附加识别特征 — 手指（选择性的）

国际民航组织承认成员国可以选择使用指纹识别作为附加生物特征技术来支持机器辅助身份确认，这应被编码为数据组 3（DG3）。

表 25　数据组 3 标志

标志	长度	值
63	Var	见 EF.DG3 的生物特征编码

6.3.1　EF.DG3 的生物特征编码

数据组 3 必须使用[ISO/IEC7816-11]中指定的带有嵌套生物特征信息模板的生物特征信息组模板（BIT），以便能够存储多个生物特征模板并与生物特征通用交换格式框架（CBEFF）和谐一致。生物特征子首标界定存在的生物特征类型和特定的生物特征。[ISO/IEC7816-11]的嵌套选项必须被使用，即使用于一个单独的生物特征模板的编码。后一种情况是以 n=1 开始的编号表示。数据组 3 中的样品号可以是‘0...n’。

每个嵌套模板具有以下结构：

表 26　数据组 3 嵌套标志

标志	长度	值				
7F61	Var	生物特征信息组模板				
		标志	长度	值		
		02	01	整数 — 该类生物特征的样品号		
		7F60	Var	第 1 生物特征信息模板		
			标志	长度		
			A1	Var	生物特征首标模板（BHT）	
				标志	长度	值
				80	02	国际民航组织首标版本‘0101’（选择性的）— 生物特征通用交换格式框架保护首标格式的版本
				81	01-03	生物特征类型（选择性的）
				82	01	数据组 3 的生物特征子类型（必要的）
				83	07	创建日期和时间（选择性的）
				85	08	有效期（从___至___）（选择性的）
				86	02	生物特征参考数据（PID）的创建者（选择性的）
				87	02	格式所有者（必要的）
				88	02	格式类型（必要的）
			5F2E 或 7F2E	Var	生物特征数据（根据格式所有者编码）也称为生物特征数据分组（BDB）。	
		标志	长度			
		7F60	X	第 2 生物特征信息模板		
			标志	长度		
			A1	Var	生物特征首标模板（BHT）	
				标志	长度	值
				80	02	国际民航组织首标版本‘0101’（选择性的）—生物特征通用交换格式框架保护人首标格式的版本
				81	01-03	生物特征类型（选择性的）

标志	长度	值				
				82	01	数据组 3 的生物特征子类型（必要的）
				83	07	创建日期和时间（选择性的）
				85	08	有效期（从___至___）（选择性的）
				86	04	生物特征参考数据（PID）的创建者（选择性的）
				87	02	格式所有者（必要的）
				88	02	格式类型（必要的）
			5F2E 或 7F2E	Var	生物特征数据（根据格式所有者编码）也称为生物特征数据分组（BDB）。	

使用生物特征通用交换格式框架的默认对象标识符。[ISO/ IEC7816-11]中指定的就在生物特征信息模板（BIT，标志 0x7F60）下面的对象标识符数据对象（标志 0x06）不包括在此结构中。同样，该结构中没有指定标志分配权限。

为了促进互操作性，每个数据组中记录的第一个生物特征应按[ISO / IEC19794-5]的规定进行编码。

6.3.2　数据组 3 — EF.DG3 数据元素

本节描述数据组 3（DG3）中可能存在的数据元素。每个数据组区域内的数据元素及其格式应如下表所示：

注：A = 字母字符[a..z, A..Z]，N = 数字字符[0..9]，S = 特殊字符[‘<’]，B=8 位二进制数据（A，N 或 S 以外的任何数据），F = 固定长度域，Var = 可变长度域。

表 27　EF.DG3 的数据元素

数据元素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
01	M（如果记录了编码的手指特征）	记录的手指生物特征编码号	1	F	N	用 0 到 n 标识手指数据的唯一编码号。
02	M（如果记录了编码的手指特征）	首标		Var	B	数据元素可按 DE 01 的规定重现。
03	M（如果记录了编码的手指特征）	手指生物特征数据编码		Var	A,N,S, B	数据元素可按 DE 01 的规定重现。

6.3.2.1 生物特征子类型编码

生物特征首标模板标志及其分配的值是每次实施应按下表所示予以支持的最低要求。每个单独的生物特征信息模板具有以下结构：

表 28 用于编码子特征的子特征编码方案：生物特征通用交换格式框架

b8	b7	b6	b5	b4	b3	b2	b1	生物特征子类型
0	0	0	0	0	0	0	0	没有给信息
						0	1	右
						1	0	左
			0	0	0			没有意义
			0	0	1			拇指
			0	1	0			食指
			0	1	1			中指
			1	0	0			环指
			1	0	1			小指
X	X	X						留作将来使用

6.3.2.2 零样品的编码

没有签发带指纹的电子机读旅行证件的国家不应该填充数据组 3。本结构数据组 3 具有的缺点是它会导致所有电子机读旅行证件的证件安全对象中一个静态的数据组 3 散列，其中生物特征在签发电子机读旅行证件时不存在并被填充，但数据组 3 被公布。为互操作性目的，那些支持在其电子机读旅行证件中使用指纹的国家，在签发电子机读旅行证件时没有指纹可用的情况下必须存储一个空的生物特征信息组模板。这种情况下模板计数器表示一个 0x00 的值。

建议添加带签发人定义的内容（例如一个随机号）的标志 0x53。

表 29　对零样品编码

标志	长度	值				
63	Var	逻辑数据结构要素				
		标志	长度	值		
		7F 61	03	生物特征信息组模板		
			02	01	00	界定没有任何生物特征信息模板存储在该数据组中。
		53	Var	签发人定义的内容（例如一个随机号）。		

6.3.2.3　一个样品的编码

在只有一个指纹可用的情况下，必须以如下方式对该唯一样品编码（数据组 3 — 指纹的例子）：

表 30　对一个样品编码

标志	长度	值						
63	aa	逻辑数据结构要素，其中 aa 是整个逻辑数据结构数据内容的总长度。						
		标志	长度	值				
		7F 61	bb	生物特征信息组模板，其中 bb 是整个组模板内容的总长度。				
			02	01	01	界定作为随后的生物特征信息模板存储的指纹总数。		
			7F 60	cc	第一个生物特征信息模板，其中 cc 是整个生物特征信息模板的总长度。			
				A1	dd	生物特征首标模板，其中 dd 是生物特征首标模板的总长度。		
					81	01	08	生物特征类型“指纹”
					82	01	0A	生物特征子类型“左手食指”
					87	02	01 01	格式所有者 JTC 1 SC 37
					88	02	00 07	格式类型 [ISO/IEC 19794-4]
					注意生物特征首标模板可能包含附加可选要素。当然，这种指纹可以是一个左手指纹或右手指纹，取决于可用图像。			
				5F 2E	ee	生物特征数据分组，其中 ee 是编码的[ISO/ IEC19794-4]结构的总长度。该生物特征数据分组必须确切包含一个指纹图像。		

6.3.2.4 一个以上样品的编码

为实现互操作性，每个特征必须存储在一个单独的生物特征信息模板中。如果该信息是可用的，必须指定该特征在生物特征通用交换格式框架生物特征子类型内的位置。下表包含一个对有两个指纹图像的可互操作的数据组 3 要素进行生物特征通用交换格式框架编码的工作实例。

表 31 对一个以上样品编码

<table>
<tr><th>标志</th><th>长度</th><th colspan="8">值</th></tr>
<tr><td>63</td><td>aa</td><td colspan="8">逻辑数据结构要素，其中 aa 是整个逻辑数据结构数据内容的总长度</td></tr>
<tr><td></td><td></td><td>标志</td><td>长度</td><td colspan="6">值</td></tr>
<tr><td></td><td></td><td>7F 61</td><td>bb</td><td colspan="6">生物特征信息组模板，其中 bb 是整个组模板内容的总长度。</td></tr>
<tr><td></td><td></td><td></td><td>02</td><td>01</td><td>02</td><td colspan="4">界定作为随后的生物特征信息模板存储的指纹总数。</td></tr>
<tr><td></td><td></td><td></td><td>7F 60</td><td>cc</td><td colspan="5">第一个生物特征信息模板，其中 cc 是整个生物特征信息模板的总长度。</td></tr>
<tr><td></td><td></td><td></td><td></td><td>A1</td><td>Dd</td><td colspan="4">生物特征首标模板，其中 dd 是生物特征首标模板的总长度。</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>81</td><td>01</td><td>08</td><td colspan="2">生物特征类型“指纹”</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>82</td><td>01</td><td>0A</td><td colspan="2">生物特征子类型“左手食指”</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>87</td><td>02</td><td>01 01</td><td colspan="2">格式所有者 JTC 1 SC 37</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>88</td><td>02</td><td>00 07</td><td colspan="2">格式类型 [ISO/IEC 19794-4]</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td colspan="5">注意生物特征首标模板可能包含附加可选要素。也有可能指纹的次序（左/右）是不同的。</td></tr>
<tr><td></td><td></td><td></td><td></td><td>5F 2E</td><td>ee</td><td colspan="4">生物特征数据分组，其中 ee 是编码的[ISO/ IEC19794-4]结构的总长度。生物特征数据分组必须确切包含一个指纹图像。</td></tr>
<tr><td></td><td></td><td></td><td>7F 60</td><td>ff</td><td colspan="5">第二个生物特征信息模板，其中 ff 是整个生物特征信息模板的总长度。</td></tr>
<tr><td></td><td></td><td></td><td></td><td>A1</td><td>Gg</td><td colspan="4">生物特征首标模板，其中 gg 是生物特征首标模板的总长度。</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>81</td><td>01</td><td>08</td><td colspan="2">生物特征类型“指纹”</td></tr>
</table>

标志	长度	值						
					82	01	09	生物特征子类型“右手食指”
					87	02	01 01	格式所有者 JTC 1 SC 37
					88	02	00 07	格式类型 [ISO/IEC 19794-4]
					注意生物特征首标模板可能包含附加可选要素。也有可能指纹的次序（左/右）是不同的。			
				5F 2E	Hh	生物特征数据分组，其中 hh 是编码的[ISO/ IEC19794-4]结构的总长度。生物特征数据分组必须确切包含一个指纹图像。		

6.4　数据组 4 — 附加识别特征 — 虹膜（选择性的）

国际民航组织承认各成员国可以选择使用虹膜识别作为附加生物特征技术来支持机器辅助身份确认，这应被编码为数据组 4（DG4）。

表 32　数据组 4 标志

标志	长度	值
76	Var	见 EF.DG4 的生物特征编码

6.4.1　EF.DG4 的生物特征编码

数据组 4 必须使用[ISO/IEC7816-11]中指定的带有嵌套生物特征信息模板的生物特征信息组模板（BIT），以便能够存储多个生物特征模板并与生物特征通用交换格式框架（CBEFF）和谐一致。生物特征子首标界定存在的生物特征类型和特定的生物特征。[ISO/IEC7816-11]的嵌套选项必须被使用，即使用于一个单独的生物特征模板的编码。后一种情况是以 n=1 开始的编号表示。数据组 4 中的样品号可以是‘0...n’。

每个嵌套模板具有以下结构：

表 33　数据组 4 嵌套标志

标志	长度	值				
7F61	Var	生物特征信息组模板				
		标志	长度	值		
		02	1	整数— 该类生物特征的样品号		
		7F60	Var	第 1 个生物特征信息模板		
			标志	长度		
			A	Var	生物特征首标模板（BHT）	
				标志	长度	值
				80	02	国际民航组织首标版本‘0101’（选择性的）— 生物特征通用交换格式框架保护人首标格式的版本
				81	01-03	生物特征类型（选择性的）
				82	01	生物特征子类型，对于数据组 4 是必要的
				83	07	创建日期和时间（选择性的）
				85	08	有效期（从___至___）（选择性的）
				86	02	生物特征参考数据（PID）的创建者（选择性的）
				87	02	格式所有者（必要的）
				88	02	格式类型（必要的）
			5F2E 或 7F2E	Var	生物特征数据（根据格式所有者编码）也称为生物特征数据分组（BDB）。	
		标志	长度			
		7F60	Var	第 2 个生物特征信息模板		
			标志	长度		
			A1	Var	生物特征首标模板（BHT）	
				标志	长度	值
				80	02	国际民航组织首标版本‘0101’（选择性的）— 生物特征通用交换格式框架保护人首标格式的版本
				81	01-03	生物特征类型（选择性的）

标志	长度	值				
				82	01	生物特征子类型，对于数据组 4 是必要的
				83	07	创建日期和时间（选择性的）
				85	08	有效期（从___至___）（选择性的）
				86	04	生物特征参考数据（PID）的创建者（选择性的）
				87	02	格式所有者（必要的）
				88	02	格式类型（必要的）
			5F2E 或 7F2E	Var	生物特征数据（根据格式所有者编码）也称为生物特征数据分组（BDB）。	

使用生物特征通用交换格式框架的默认对象标识符。[ISO/IEC7816-11]中指定的就在生物特征信息模板（BIT，标志 0x7F60）下面的对象标识符数据对象（标志 0x06）不包括在此结构中。同样，该结构中没有指定标志分配权限。

为了促进互操作性，每个数据组中记录的第一个生物特征应按[ISO / IEC19794-5]的规定进行编码。

6.4.2　数据组 4 — EF.DG 4 数据元素

本节描述数据组 4（DG4）中可能存在的数据元素。每个数据组区域内的数据元素及其格式应如下表所示：

注：A = 字母字符[a..z, A..Z]，N = 数字字符 [0..9]，S = 特殊字符 [‘<’]，B= 8 位 二进制数据（A，N 或 S 以外的任何数据），F = 固定长度域，Var = 可变长度域。

表 34　数据组 4 的数据元素

数据元素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
01	M, 如果包括编码的眼特征	记录的眼生物特征编码号	1	F	N	用 1 至 9 标识眼数据的唯一编码号。
02	M, 如果包括编码的眼特征	首标		Var	B	数据元素可按 DE 01 的规定重现。
03	M, 如果包括编码的眼特征	眼生物特征数据编码		Var	A,N,S, B	数据元素可按 DE 01 的规定重现。

6.4.2.1 生物特征子类型编码

生物特征首标模板标志及其分配的值是每次实施应按下表所示予以支持的最低要求。每个单独的生物特征信息模板具有以下结构：

表 35 编码子特征的子特征编码方案：生物特征通用交换格式框架

b8	b7	b6	b5	b4	b3	b2	b1	生物特征子类型
0	0	0	0	0	0	0	0	没有给信息
						0	1	右
						1	0	左
			0	0	0			留作将来使用
			0	0	1			留作将来使用
			0	1	0			留作将来使用
			0	1	1			留作将来使用
			1	0	0			留作将来使用
			1	0	1			留作将来使用
X	X	X						留作将来使用

6.4.2.2 零样品的编码

没有签发带虹膜的电子机读旅行证件的国家不应该填充数据组 4。本结构数据组 4 具有的缺点是它会导致所有电子机读旅行证件的证件安全对象中一个静态的数据组 4 散列，其中生物特征在签发电子机读旅行证件时不存在并被填充，但数据组 4 被公布。为互操作性目的，那些支持在其电子机读旅行证件中使用虹膜的国家，在签发电子机读旅行证件时没有虹膜可用的情况下必须存储一个空的生物特征信息组模板。这种情况下模板计数器表示一个 0x00 的值。

建议添加具有签发人定义的内容（例如一个随机号）的标志 0x53。

表 36　对零样品编码

标志	长度	值				
76	Var	逻辑数据结构要素				
		标志	长度	值		
		7F 61	03	生物特征信息组模板		
			02	01	00	界定没有任何生物特征信息模板存储在该数据组中。
		53	Var	签发人定义的内容（例如一个随机号）。		

6.4.2.3　一个样品的编码

在只有一个虹膜可用的情况下，必须对该唯一样品编码。

6.4.2.4　一以上样品的编码

为实现互操作性，每个特征必须存储在一个单独的生物特征信息模板中。如果该信息是可用的，必须指定该特征在生物特征通用交换格式框架生物特征子类型内的位置。

6.5　数据组 5 — 显示的肖像（选择性的）

分配给数据组 5（DG5）的数据元素应如下：

表 37　数据组 5 标志

标志	长度	值		
65	Var			
		标志	长度	值
		02	Var	这类显示的图像的样品号（在第一个模板中是必要的，在后继模板中不使用。）
		5F40	Var	显示的肖像

确认指定类型显示图像的以下格式所有者。

表 38　数据组 5 格式

显示的图像	格式所有者
显示的面部图像	[ISO/IEC 10918]，JFIF 选项

6.5.1　数据组 5 — EF.DG5 数据元素（选择性的）

本节描述数据组 5（DG5）中可能存在的数据元素。数据组 5 内的数据元素及其格式应如下表所示：

注：A = 字母字符 [a..z, A..Z]，N = 数字字符 [0..9]，S = 特殊字符 ['<']，B= 8 位二进制数据（除 A，N 或 S 以外的任何数据），F = 固定长度域，Var = 可变长度域。

表 39　数据组 5 的数据元素

数据元素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
01	M（如果记录了显示的肖像）	记录的显示肖像号	1	F	N	用 1 至 9 标识显示的肖像的唯一记录号。
02	M（如果记录了显示的肖像）	显示的肖像表示法		Var	A,N	数据元素可按 DE 01 的规定重现。
	M（如果记录了显示的肖像）	显示的肖像表示法中的字节数	5	F	N	00001 至 X9，标识紧随其后的显示的肖像表示法的字节数
	M（如果记录了显示的肖像）	显示的肖像表示法		Var	A,N,S, B	按照 [ISO/IEC 10918-1] 或 [ISO/IEC 15444]进行格式化。

注：应按照[ISO/IEC10918]中的规定，使用 JFIF 选项或[ISO/IEC15444]，使用 JPEG 2000 图像编码系统对数据元素 02 进行编码。

6.6　数据组 6 — 留作将来使用

分配给数据组 6（DG6）的数据元素应如下：

表 40　数据组 6 标志

标志	长度	值
66	Var	

6.6　数据组 6 — EF.DG6 数据元素

数据组 6（DG 6）的数据元素留作将来使用。

6.7　数据组 7 — 显示的签名或通常标记（选择性的）

分配给数据组 7（DG 7）的数据元素应如下：

表 41　数据组 7 标志

标志	长度	值		
67	Var			
		标志	长度	值
		02	Var	这类显示的图像的样品号（在第一个模板中是必要的，在后继模板中不使用。）
		5F43	Var	显示的签名

确认指定类型显示图像的以下格式所有者：

表 42　数据组 7 格式

显示的图像	格式所有者
显示的签名/通常标记	[ISO/IEC 10918]，JFIF 选项

6.7.1 数据组 7 — EF.DG 7 数据元素（选择性的）

本节描述数据组 7（DG7）中可能存在的数据元素。每个数据组 7 内的数据元素及其格式应如下表所示：

注：A = 字母字符 [a..z, A..Z]，N = 数字字符 [0..9]，S = 特殊字符 ['<']，B= 8 位二进制数据（除 A，N 或 S 以外的任何数据），F = 固定长度域，Var = 可变长度域。

表 43 数据组 7 的数据元素

数据要素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
01	M（如果记录了显示的签名或通常标记）	显示的签名或通常标记号	1	F	N	用 1 至 9 标识显示的签名或通常标记的唯一记录号。
02	M（如果记录了显示的签名或通常标记）	显示的签名或通常标记表示法		Var	A,N,S, B	数据元素可按 DE 01 的规定重现。 按照 [ISO/IEC 10918-1] 或 [ISO/IEC 15444]进行格式化。

注：应按照[ISO/IEC10918]中的规定，使用 JFIF 选项或[ISO/IEC15444]，使用 JPEG 2000 图像编码系统对数据元素 02 进行编码。

6.8 数据组 8 — 数据特征（选择性的）

该数据组尚待界定。在此之前，它可供临时专有使用。此数据元素可以使用一个与生物特征模板、机器辅助安全特征验证和编码细节的结构相类似的结构。结合形成数据组 8（DG 8）的数据元素应如下：

表 44 数据组 8 标志

标志	长度	值		
68	Var	待界定		
		标志	长度	值
		02	1	整数 — 该类模板的样品号（在第一个模板中是必要的，在后继模板中不使用。）
			Var	首标模板。细节待界定。

6.8.1　数据组 8 — EF.DG 8 数据元素

本节描述数据组 8（DG8）中可能存在的数据元素。每个数据组区域内的数据元素及其格式应如下表所示：

注：A = 字母字符 [a..z, A..Z]，N = 数字字符 [0..9]，S = 特殊字符 ['<']，B= 8 位二进制数据（除 A，N 或 S 以外的任何数据），F = 固定长度域，Var = 可变长度域。

表 45　数据组 8 的数据元素

数据元素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
01	M（如果使用这一编码特征）	数据特征号	1	F	N	用 1 至 9 标识数据特征的唯一编码号（包括 DE02 至 DE04）。
02	M（如果使用这一编码特征）	首标（待界定）	1			首标细节待界定。
03	M（如果使用这一编码特征）	数据特征数据	999 最大	Var	A,N,S, B	格式由签发国或签发机构自行确定。

6.9　数据组 9 — 结构特征（选择性的）

该数据组尚待界定。在此之前，它可供临时专有使用。这些数据元素可以使用一个与生物特征模板的结构相类似的结构。结合形成数据组 9（DG 9）的数据元素应如下：

表 46　数据组 9 标志

标志	长度	值		
69	Var	待界定		
		标志	长度	值
		02	01	整数 — 该类模板的样品号（在第一个模板中是必要的，在后继模板中不使用。）
			X	首标模板。细节待界定。

6.9.1 数据组 9 — EF.DG9 数据元素

每个数据组区域内的数据组 9（DG 9）数据元素及其格式应如下表所示：

注：A = 字母字符 [a..z, A..Z]，N = 数字字符 [0..9]，S = 特殊字符 ['<']，B= 8 位二进制数据（除 A，N 或 S 以外的任何数据），F = 固定长度域，Var = 可变长度域。

表 47 数据组 9 的数据元素

数据元素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
01	M（如果使用这一编码特征）	结构特征号	1	F	N	用 1 至 9 标识结构特征的唯一编码号（包括 DE 02 至 DE 04）。
02	M（如果使用这一编码特征）	首标（待界定）			N	首标细节待界定
03	M（如果使用这一编码特征）	结构特征数据		Var		

6.10 数据组 10 — 物质特征（选择性的）

该数据组尚待界定。在此之前，它可供临时专有使用。这些数据元素可以使用一个与生物特征模板的结构相类似的结构。结合形成数据组 10（DG 10）的数据元素应如下：

表 48 数据组 10 标志

标志	长度	值		
6A	Var			
		标志	长度	值
		02	01	整数 — 该类模板的样品号（在第一个模板中是必要的，在后继模板中不使用。）
			Var	待界定。

6.10.1　数据组 10 — EF.DG 10 数据元素

本节描述数据组 10（DG10）中可能存在的数据元素。每个数据组区域内的数据元素及其格式应如下表所示：

注：A = 字母字符 [a..z, A..Z]，N = 数字字符 [0..9]，S = 特殊字符 ['<']，B= 8 位二进制数据（除 A，N 或 S 以外的任何数据），F = 固定长度域，Var = 可变长度域。

表 49　数据组 10 的数据元素

数据要素	选择性的或必需的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
01	M（如果使用这一编码特征）	记录的物质特征号	1	F	N	用 1 至 9 标识物质特征的唯一编码号（包括 DE 02 至 DE 04）。
02	M（如果使用这一编码特征）	首标（待界定）	TBD	TBD	N	细节待界定。
03	M（如果使用这一编码特征）	物质特征数据	999 最大	Var	A,N,S, B	格式由签发国或签发机构自行确定。

6.11　数据组 11 — 附加个人信息（选择性的）

该数据组用于有关证件持有人的附加信息。由于该组内的所有数据元素是选择性的，使用一个标志列表来界定那些存在的数据元素。结合形成数据组 11（DG 11）的数据元素应如下：

注：该模板可能包含非拉丁字符。

表 50　数据组 11 标志

标志	长度	值				
6B	Var					
		标志	长度	值		
		5C	Var			模板中的标志列表与数据元素列表。
		5F0E	Var			以本国字符显示的证件持有人全名。按照 Doc 9303 号文件的规则编码。
		A0	Var			内容特定类
				标志	长度	值
				02	01	其他名称号
				5F0F	Var	按照 Doc 9303 号文件格式化的其他姓名。数据对象如其他名称号（带标志'02'的数据对象）中所指示的重复多次。
		标志	长度	值		
		5F10	Var			个人号码
		5F2B	08			以 yyyymmdd 表示的出生年月日
		5F11	Var			出生地。用 '<'隔开的域
		5F42	Var			永久地址。用 '<'隔开的域
		5F12	Var			电话
		5F13	Var			职业
		5F14	Var			职衔
		5F15	Var			个人简历
		5F16	Var			公民身份证明。按照 [ISO/IEC 10918] 压缩的图像
		5F17	Var			其他有效的旅行证件号。用 '<'隔开
		5F18	Var			监护信息

6.11.1　数据组 11 — EF.DG 11 数据元素

本节描述数据组 11（DG11）中可能存在的数据元素。每个数据组区域内的数据元素及其格式应如下表所示：

注 1：应按照[ISO/IEC10918]中的规定，使用 JFIF 选项或[ISO/IEC15444]，使用 JPEG 2000 图像编码系统对数据元素 11 进行编码。

注 2：A = 字母字符 [a..z, A..Z]，N = 数字字符[0..9]，S = 特殊字符 ['<']，B = 8 位二进制数据（除 A，N 或 S 以外的任何数据），F = 固定长度域，Var = 可变长度域。

表 51　数据组 11 的数据元素

数据要素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
01	O	持有人姓名（全名）	99 最大	Var	B	按照机读区插入填充符（<）。行尾不插入填充符。不允许截取。
02	O	其他姓名	99 最大	Var	B	按照机读区插入填充符（<）。行尾不插入填充符。不允许截取。
03	O	个人号码	99 最大	Var	A,N,S	自由格式文本。
04	O	出生年月日	8	F	B	CCYYMMDD
05	O	出生地	99 最大	Var	B	自由格式文本。
06	O	地址	99 最大	Var	A,N,S, B	自由格式文本。
07	O	电话	99 最大	Var	N,S	自由格式文本。
08	O	职业	99 最大	Var	B	自由格式文本。
09	M, 如果包括 DE 08	职衔	99 最大	Var	B	自由格式文本。
10	M, 如果包括 DE 09	个人简历	99 最大	Var	B	自由格式文本。

数据要素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
11	M, 如果包括 DE 10	公民资格证明		Var	A,N,S, B	按照 [ISO/IEC 10918-1] 格式化的公民证件图像
12	O	其他有效旅行证件 旅行证件号	99 最大	Var	A,N,S, B	自由格式文本，用<隔开。
13	O	监护信息	999 最大	Var	B	自由格式文本。

注：在月（MM）或日（DD）是未知的情况下，在数据组 11 中指明这种情况的可互操作方式是将各自的字符设置为'00'。在世纪和年（CCYY）是未知的情况下，在数据组 11 中指明这种情况的可互操作方式是将各自的字符设置为'0000'。必须总是一贯使用签发人指定的日期。

6.12 数据组 12 — 附加证件详细信息（选择性的）

该数据组是用于有关证件的附加信息。该组内的所有数据元素都是选择性的。

表 52 数据组 12 标志

标志	长度	值				
6C	Var					
		标志	长度	值		
		5C	Var			模板中的标志列表与数据元素表
		5F19	Var			签发机构
		5F26	08			签发日期 yyyymmdd
		A0	Var			内容特定类
				标志	长度	值
				02	01	其他人的号码
				5F1A	Var	按照 Doc 9303 号文件规则格式化的其他人姓名。数据对象如其他名称号 DE02（带标志'02'的数据对象）中所指示的重复多次。

标志	长度	值				
		标志	长度	值		
		5F1B	Var			签注，意见
		5F1C	Var			税收/出境要求
		5F1D	Var			证件正面图像。按照 ISO/IEC 10918 的图像
		5F1E	Var			证件背面图像。按照 ISO/IEC 10918 的图像
		5F55	0E			证件个人化的日期和时间 yyyymmddhhmmss
		5F56	Var			个人化系统的序列号

建议查验系统支持 8 字节美国标准信息交换代码（ASCII）和二进制编码的十进制表示法（BCD）日期/时间编码。

6.12.1　数据组 12 — EF.DG 12 数据元素

本节描述数据组 12（DG12）中可能存在的数据元素。每个数据组区域内的数据元素及其格式应如下表所示：

注 1：A = 字母字符 [a..z, A..Z]，N = 数字字符 [0..9]，S = 特殊字符 ['<']，B = 8 位二进制数据（除 A，N 或 S 以外的任何数据），F = 固定长度域，Var = 可变长度域。

注 2：应按照[ISO/IEC10918]中的规定，使用 JFIF 选项或[ISO/IEC15444]，使用 JPEG 2000 图像编码系统对数据元素 07 和 08 进行编码。

表 53　数据组 12 的数据元素

数据元素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
01	O	签发机构	99 最大	Var	B	自由格式文本。
02	O	签发日期	8	F	N	证件签发日期；即 YYYYMMDD。
03	O	其他人详细信息	99 最大	Var	B	自由格式文本。
04	O	签注/ 意见	99 最大	Var	B	自由格式文本。
05	O	税收/出境要求	99 最大	Var	B	自由格式文本。

数据元素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
06	O	机读旅行证件的正面图像		Var	A,N,S,B	按照 [ISO/IEC 10918-1]进行格式化。
07	O	机读旅行证件背面图像		Var	A,N,S,B	按照[ISO/IEC 10918-1]进行格式化
08	O	个人化时间	14	F	N	ccyymmddhhmmss
09	O	个人化设备序列号	99 最大	Var	A,N,S	自由格式。

6.13 数据组 13 — 选择性的详细信息（选择性的）

结合形成数据组 13（DG 13）的数据元素由签发国或签发机构自行决定并应如下：

表 54 数据组 13 标志

标志	长度	值
‘6D’	Var	

6.14 数据组 14 — 安全选项（有条件的）

数据组 14 包含附加安全机制的安全选项。详情见 Doc 9303 号文件第 11 部分。电子护照应用中包含的文件数据组 14 是必要的，如果芯片认证映射或利用通用映射/集成映射的口令认证连接确立（PACE -GM/-）得到电子机读旅行证件芯片支持的话。

表 55 数据组 14 标志

标志	长度	值
6^E	Var	参考 Doc 9303 号文件第 10 部分的数据组 14 安全信息

6.14.1 数据组 14 — EF.DG 14 数据元素

本节描述数据组 14（DG14）中可能存在的数据元素。每个数据组区域内的数据元素及其格式应如下表所示：

注：A = 字母字符 [a..z, A..Z]，N = 数字字符 [0..9]，S = 特殊字符 [‘<’]，B= 8 位二进制数据（除 A，N 或 S 以外的任何数据），F = 固定长度域，Var = 可变长度域。

表 56　数据组 14 的数据元素

数据元素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
	O	安全信息		Var	B	参考 Doc 9303 号文件第 10 部分。第 6.14.2 中所界定的数据组 14 安全信息

6.14.2　数据组 14 安全信息

下面一般性的 ASN.1 数据结构 SecurityInfos（安全信息）允许次要生物特征安全选项的各种实施。出于互操作性考虑，建议该数据结构由数据组 14 中的电子机读旅行证件芯片提供支持以表示得到支持的安全协议。该数据结构具体如下：

```
SecurityInfos::=  SET of SecurityInfo

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

安全信息数据结构中包含的元素具有以下含义：

- 客体标识符协议标识支持的协议;
- 开放类必要的数据包含协议特定必要的数据；
- 开放类可选数据包含协议特定的可选数据。

6.15　数据组 15 — 主动认证公钥信息（有条件的）

当按照 Doc 9303 号文件第 11 部分所述实施选择性的主动认证芯片认证时，该选择性的数据组包含主动认证公钥并且是必要的。

表 57　数据组 15 标志

标志	长度	值
6F	Var	参考 Doc 9303 号文件第 11 部分

6.15.1　数据组 15 — EF.DG 15 数据元素

本节描述数据组 15（DG15）中可能存在的数据元素。每个数据组区域内的数据元素及其格式应如下表所示：

注：A =字母字符 [a..z, A..Z]，N = 数字字符 [0..9]，S = 特殊字符 [‘<’]，B= 8 位二进制数据（除 A，N 或 S 以外的任何数据），F = 固定长度域，Var = 可变长度域。

表 58　数据组 15 的数据元素

数据要素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
	O	主动认证公钥信息		Var	B	见 Doc 9303 号文件第 11 部分

6.16　数据组 16 — 被通知人（选择性的）

该数据组列出紧急通知信息。它被编码为使用标志‘Ax’命名的一系列模板。数据组 16（如所有其他数据组一样）在签发后不应更新；数据组 16 由证件安全对象中的一个散列值表示，证件安全对象仅在签发时签名一次。

表 59　数据组 16 标志

标志	长度	值		
70	Var			
		标志	长度	值
		02	01	模板号（只出现在第一模板中）
		Ax	Var	模板开始，其中 x（x=1,2,3…）随每次出现而递增
5F50	04			记录的日期数据
5F51	Var			人的姓名
5F52	Var			电话
5F53	Var			地址

6.16.1　数据组 16 — EF.DG16 数据元素

本节描述数据组 16（DG16）中可能存在的数据元素。每个数据组区域内的数据元素及其格式应如下表所示：

注：A = 字母字符 [a..z, A..Z]，N = 数字字符 [0..9]，S = 特殊字符 [‘<’]，B = 8 位二进制数据（除 A，N 或 S 以外的任何数据），F = 固定长度域，Var = 可变长度域。

表 60　数据组 16 的数据元素

数据元素	选择性的或必要的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
01	M, 如果包括数据组 16	标识的人数	2	F	N	标识该数据组中包括的人数。
02	M, 如果包括数据组 16	记录的详细日期	8	F	N	记录的日期、通知日期; 格式 = CCYYMMDD。
03	M, 如果包括数据组 16	被通知人姓名主要和次要标识符		Var	B	按照机读区插入填充符（<）。不允许截取。
04	M, 如果包括 DE 03	被通知人电话号码		Var	N,S	国际形式的电话号码（国家代码和本地号码）。
05	M	被通知人地址		Var	B	自由格式文本。

7. 参考文献（规范性）

ISO/IEC 14443-1　ISO/IEC 14443-1:2008，识别卡 — 非接触式 IC 卡 —感应卡 — 第 1 部分：物理特性

ISO/IEC 14443-1/Amd 1　ISO/IEC 14443-1:2008/Amd 1:2012，其他接触式集成电路卡类

ISO/IEC 14443-2　ISO/IEC 14443-2:2010，识别卡 — 非接触式 IC 卡 — 感应卡 — 第 2 部分：射频功率和信号接口

ISO/IEC 14443-2/Amd 1　ISO/IEC 14443-2:2010/Amd 1:2011，接触式集成电路卡产生的寄生电磁干扰水平极限

ISO/IEC 14443-2 /Amd 2　ISO/IEC 14443-2:2010/Amd 2:2012，其他接触式集成电路卡类

ISO/IEC 14443-2 /Amd 3　ISO/IEC 14443-2:2010/Amd 3:2012, fc/8、fc/4 和 fc/2 的比特率

ISO/IEC 14443-3　ISO/IEC 14443-3:2011，识别卡 — 非接触式 IC 卡 — 感应卡— 第 3 部分：初始化和防冲突

ISO/IEC 14443-3 /Amd 1　ISO/IEC 14443-3:2011/Amd 1:2011，电磁干扰处理和单一尺寸的唯一标识符

ISO/IEC 14443-3 /Amd 2　ISO/IEC 14443-3:2011/Amd 2:2012，FC/8、FC/4 和 FC/2 的比特率，从 512 字节到 4096 字节的帧长和最小 TR0

ISO/IEC 14443-4　ISO/IEC 14443-4:2008，识别卡— 非接触式 IC 卡 — 感应卡 —第 4 部分：传输协议

ISO/IEC 14443-4 /Amd 1　ISO/IEC 14443-4:2008/Amd 1:2012，附加参数交换

ISO/IEC 14443-4 /Amd 2	ISO/IEC 14443-4:2008/Amd 2:2012，fc/8、fc/4 和 fc/2 的比特率，接触式集成电路卡 A 型协议激活和从 512 字节到 4 096 字节的帧长
ISO/IEC 10373-6	ISO/IEC 10373-6:2011，识别卡 — 测试方法 — 第 6 部分：感应卡
ISO/IEC 10373-6 /Amd 1	ISO/IEC 10373-6:2011/Amd 1:2012，其他接触式集成电路卡类
ISO/IEC 10373-6 /Amd 2	ISO/IEC 10373-6:2011/Amd 2:2012，电磁干扰的测试方法
ISO/IEC 10373-6 /Amd 3	ISO/IEC 10373-6:2011/Amd 3:2012，附加参数交换、分组编号、不匹配的 AFI 和 TR2
ISO/IEC 10373-6 /Amd 4	ISO/IEC 10373-6:2011/Amd 4:2012，fc/8, fc/4 和 fc/2 的比特率及从 512 字节到 4096 字节的帧长
ISO/IEC 10373-6 /Amd 7	ISO/IEC 10373-6:2011/Amd 7:2010，识别卡 — 测试方法 — 第 6 部分：感应卡 — 电子护照阅读器的测试方法
ISO/IEC 7816-2	ISO/IEC 7816-2: 2007，识别卡 — 集成电路卡 — 第 2 部分：带触点的卡—触点的尺寸和位置
ISO/IEC 7816-4	ISO/IEC 7816-4: 2013，识别卡 — 集成电路卡 —第 4 部分：组织、安全及交换命令
ISO/IEC 7816-5	ISO/IEC 7816-5: 2004，识别卡 — 集成电路卡 — 第 5 部分：应用提供商的注册
ISO/IEC 7816-6	ISO/IEC 7816-6: 2004，识别卡 — 集成电路卡 —第 6 部分：行业间交换数据元素（包括缺陷报告）
ISO/IEC 7816-11	ISO/IEC 7816-11: 2004，识别卡 — 集成电路卡 — 第 11 部分：通过生物识别方法进行个人身份验证
ISO/IEC 8825-1	ISO/IEC 8825-1:2008，信息技术 — ASN.1 编码规则：基本编码规则（BER）、规范编码规则（CER）和唯一编码规则（DER）的规范
ISO/IEC 19794-4	ISO/IEC 19794-4:2005，信息技术 — 生物特征数据交换格式 — 第 4 部分：指纹图像数据
ISO/IEC 19794-5	ISO/IEC 19794-5:2005，信息技术 — 生物特征数据交换格式 — 第 5 部分：面部图像数据
ISO/IEC 10646	ISO/IEC 10646:2012，信息技术 — 通用编码字符集（UCS）
RFC 3369	加密消息语法 2002
ISO/IEC 10918-1	ISO/IEC 10918-1:1994，信息技术 — 连续色调静态图像的数字压缩及编码：要求和指南
ISO/IEC 15444	ISO/IEC 15444-n，JPEG 2000 图像编码系统
ISO/IEC 19785	ISO/IEC 19785-n，信息技术 — 生物特征通用交换格式框架

— — — — — — — —

第 10 部分附录 A

逻辑数据结构映射实例
（资料性）

以下资料性文本利用一种对电子机读旅行证件上非接触式 IC 的随机访问表示法描述逻辑数据结构（LDS V1.7）的映射例子。

A.1 EF.COM 通用数据元素

下面的例子表示使用存有数据组 1（标志‘61’）、数据组 2（标志‘75’）、数据组 4（标志‘76’）和数据组 12（标志‘6C’）的统一码版本 4.0.0 来实施 LDS 版本 1.7。

对于该例和所有其它例子来说，标志用**粗体字**印刷，长度用*斜体*印刷，值用罗马体印刷。十六进制标志、长度和值均在引号中（‘XX’）。

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

这个例子以十六进制表示法将读为：

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

一个假设的 LDS 版本 15.99 将被编码为：

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

或十六进制：

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

A.2 EF.DG1 机读区信息

A.2.1 TD1 型电子机读旅行证件

在 **TD1** 型电子机读旅行证件中使用该信息的数据组 1 的一个例子如下所示。机读区数据元素的长度是 90 字节（‘5A’）。

‘61’ *‘5D’* **‘5F1F’** *‘5A’*

I<NLDXI85935F86999999990<<<<<<7208148F1108268NLD<<<<<<<<<<<4VAN<DER<STEEN<<MARIANNE<LOUISE

A.2.2 TD2 型电子机读旅行证件

在 **TD2** 型电子机读旅行证件中使用该信息的数据组 1 的一个例子如下所示。机读区数据元素的长度是 72 字节（‘48’）。

‘61’ *‘4B’* **‘5F1F’** *‘48’*

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

A.3 EF.DG2 至 EF.DG4 生物特征模板

数据组 2 至数据组 4 使用[ISO/IEC7816-11]的嵌套离卡选项以便有可能存储一种与生物特征通用交换格式框架（CBEFF），[NISTR6529a]和谐一致的多生物特征模板。生物特征子首标界定存在的生物特征类型和特定的生物特征。

例：2002 年 3 月 15 日（没有世界协调时偏移）采集到一个签名的面部生物特征，其生物特征数据分组长度为 12 642 字节（‘3162’字节）、使用一个个人身份识别数据（PID）为‘00 01 00 01’的设备进行编码、使用模板提供商‘00 0A’所有的格式类型‘00 04’，该签名的面部生物特征从 2002 年 4 月 1 日至 2007 年 3 月 31 日有效。正在使用国际民航组织保护人模板版本 1.0 。

该模板的总长度是 12 704 字节。模板在 EF.DG2（SFID 02）的开始处开始存储。

‘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’* ‘… 12 642 字节的生物特征数据…’

A.4　EF.DG5 TO EF.DG7 显示的图像模板

注：每个数据组有一个基本文件。

例：显示的图像数据长度为 2000 字节的图像模板。模板的长度是 2 008 字节（‘07D8'）。

‘65’ *‘8207D8’*
　　‘02’ *‘01’* 1
　　‘5F40’ *‘8207D0’* ‘….2 000 字节的图像数据…’

A.5　EF.DG11 附加个人详细信息

下面的例子显示以下个人信息：全名（John J. Smith）、出生地（Anytown，MN）、永久地址（123 Maple Rd, Anytown, MN），电话号码 1-612-555-1212 和职业（旅行社）。模板长度是 99 字节（*‘63’*）。

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

A.6　EF.DG12 附加证件详细信息

下面的例子包含签发机构（美国）、签发日期（2002 年 5 月 31 日），证件上包括另外一人（Brenda P. Smith）。模板长度是 64 字节（*‘40’*）。

‘6C’ *‘45’*
　　‘5C’ *‘06’* **‘5F19’ ‘5F26’ ‘5F1A’**
　　‘5F19’ *‘18’* UNITED STATES OF AMERICA
　　‘5F26’ *‘08’* 20020531
　　‘**0A**’ *‘15’*
　　　　‘**02**’ *‘01’ ‘01’*
　　　　‘5F1A’ *‘0F’* SMITH<<BRENDA<P

A.7 EF.DG16 被通知人

有两个条目的例子：Anytown, MN 的 Charles R. Smith 和 Ocean Breeze, CA 的 Mary J. Brown。模板长度是 162 字节（‘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

— 完 —

ISBN 978-92-9249-962-4