ICAO

Doc 9303

机读旅行证件

第八版，2021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）

经秘书长批准并授权出版

国际民用航空组织

ICAO

Doc 9303

机读旅行证件

第八版，2021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/FAL/TRIP。

Doc 9303 号文件 一《机读旅行证件》
第 10 部分 一 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）
订购编号：9303P10
ISBN 978-92-9265-545-7（印刷版）
ISBN 978-92-9275-542-3（电了版）

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
1	14/6/24	ICAO

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 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（集成电路）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/或编组以实现电子护照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。

Doc 9303 号文件第八版纳入了选择性的旅行记录、签证记录和附加生物特征应用（称为逻辑数据结构 2 应用）的规范，作为强制性电子机读旅行证件应用（称为逻辑数据结构 1）的扩展。

第 10 部分必须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（MRPs）和其他 TD3 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 9 部分 — 生物特征识别技术的运用和机读旅行证件的电子数据存储；
- 第 11 部分 — 机读旅行证件的安保机制；
- 第 12 部分 — 机读旅行证件的公钥基础设施。

2. DOC 9303 号文件第 10 部分的结构

Doc 9303 号文件第 10 部分分为以下章节，包括：

逻辑数据结构 1 和逻辑数据结构 2 应用的通用规范：

- 共同属性；
- 逻辑数据结构 1 和逻辑数据结构 2 的所有命令；和
- 逻辑数据结构 1 和逻辑数据结构 2 的通用基本文件（EFs）；

逻辑数据结构 1 电子机读旅行证件应用规范；

逻辑数据结构 2 应用规范：

- 旅行记录；
- 签证记录；
- 附加生物特征；和
- 逻辑数据结构 2 文件访问条件规范。

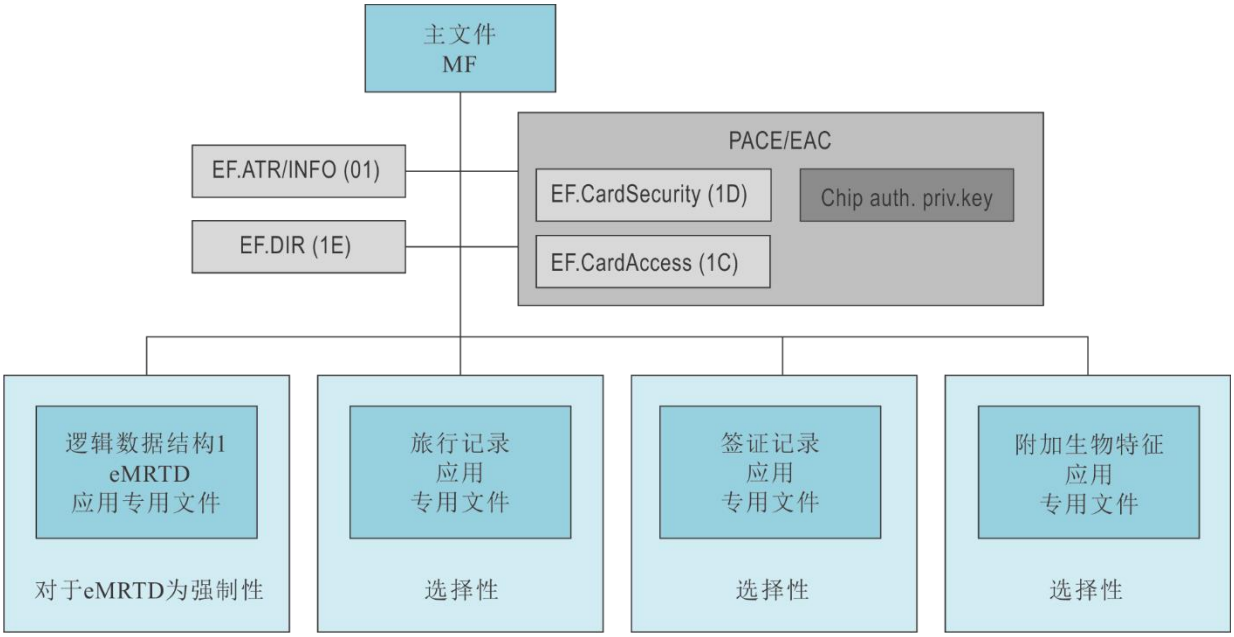

图 1. 逻辑数据结构 1 和逻辑数据结构 2 应用

电子机读旅行证件可支持以下一项、多项或全部：

- 逻辑数据结构 1 电子机读旅行证件应用为强制性；
- 逻辑数据结构 2 旅行记录应用为选择性；
- 逻辑数据结构 2 签证记录应用为选择性；
- 逻辑数据结构 2 附加生物特征应用为选择性。

3. 逻辑数据结构 1 和逻辑数据结构 2 的通用规范

3.1 互操作性最低要求

以下应是基于近场非接触式 IC 的电子护照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；

3.2 电气特性

射频功率和信号接口应符合[ISO/IEC14443-2]中的界定。建议每秒传输速度最少为 424 千比特。[ISO/IEC14443-2]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 天线大小）标准。

3.4 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，以及根据 ISO/IEC 14443 进行的初始化、防撞和传输协议。

3.4.1 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。

3.4.2 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。有些签发国出于安保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）。

3.5 命令集

除 FILE AND MEMORY MANAGEMENT（文件和内存管理）命令外，所有的命令、格式及其状态字节在[ISO/ IEC78164]和[ISO/IEC 7816-8]中都进行了定义。由逻辑数据结构 1 电子机读旅行证件支持的最小命令集必须如下：

SELECT（选择）；
READ BINARY（读二进制）。

认识到的是，为建立正确安保的环境和实现 Doc9303 号文件第 11 部分所述的选择性安保规定，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/ MUTUAL AUTHENTICATE（外部认证/相互认证）；
INTERNAL AUTHENTICATE（内部认证）；
MANAGE SECURITY ENVIRONMENT（管理安保环境）；
GENERAL AUTHENTICATE（通用认证）。

如果出现选择性的逻辑数据结构 2 应用，则电子机读旅行证件必须额外支持以下命令：

对于旅行记录应用：

READ RECORD（读记录）；
APPEND RECORD（加记录）；
SEARCH RECORD（查记录）；
FILE AND MEMORY MANAGEMENT（文件和内存管理）；
PERFORM SECURITY OPERATION (PSO)（执行安保运行）。

对于签证记录应用：

READ RECORD（读记录）；
APPEND RECORD（加记录）；
SEARCH RECORD（查记录）；
FILE AND MEMORY MANAGEMENT（文件和内存管理）；
PERFORM SECURITY OPERATION (PSO)（执行安保运行）。

对于附加的生物特征应用：

UPDATE BINARY（更新二进制）；
READ RECORD（读记录）；
APPEND RECORD（加记录）；
SEARCH RECORD（查记录）；
ACTIVATE（激活）；
FILE AND MEMORY MANAGEMENT（文件和内存管理）；
PERFORM SECURITY OPERATION (PSO)（执行安保运行）。

关于命令协议的进一步细节见 Doc9303 号文件第 11 部分。

3.5.1　选择

逻辑数据结构 1 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。文件标识符和短基本文件标识符对于非接触式 IC 操作系统来说是强制性的，但对于阅读器来说是选择性的。

3.5.2　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。

3.6　命令格式和参数选项（逻辑数据结构 1 和逻辑数据结构 2）

3.6.1　使用 SELECT 命令的应用专用文件选择

各种应用必须通过它们的表示应用标识符 (AID) 的专用文件名来进行选择。选择一个应用之后，该应用内的文件可以被访问。

注：专用文件名必须是唯一的。因此可以从任何需要的地方选择使用该专用文件名的一个应用。

3.6.1.1　主文件的选择

表 1.　用于主文件选择的 SELECT 命令

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

SELECT 命令的响应

数据域	空
SW1-SW2	‘9000’正常处理 显示检查或执行错误的其他值

注：建议不使用 SELECT MF（选择主文件）命令。

3.6.1.2 选择应用专用文件

应用专用文件必须使用 SELECT 命令进行选择，其中专用文件名表示应用标识符（AID）。应用协议数据单元 (APDU) 命令的参数如下所示：

表 2. 用于应用专用文件选择的具有应用标识符的 SELECT 命令

CLA	‘00’
INS	‘A4’
P1	‘04’
P2	‘0C’
发送数据长度Lc域	命令数据域的长度
数据域	专用文件名（AID）
响应数据长度Le域	空

SELECT 命令的响应

数据域	空
SW1-SW2	9000’正常处理 显示检查或执行错误的其他值

3.6.2 使用SELECT命令的基本文件选择

基本文件由带有基本文件标识符的 SELECT 命令进行选择。在选择基本文件时，必须确保之前已经选择了存储基本文件的应用专用文件。

表 3. 用于基本文件选择的具有文件标识符的 SELECT 命令

CLA	‘00’ / ‘0C’
INS	‘A4’
P1	‘02’
P2	‘0C’
发送数据长度Lc域	‘02’
数据域	文件标识符
响应数据长度Le域	空

SELECT 命令的响应

数据域	空
SW1-SW2	9000’ 正常处理 显示检查或执行错误的其他值

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 中指定的偶数指令代码和短基本文件标识符的 READ BINARY 命令。

3.6.3　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：通过选择该基本文件，然后读取选定的基本文件的数据，或通过使用短基本文件标识符直接读取数据。对于电子机读旅行证件，支持短基本文件标识符是强制性的。因此建议查验系统使用短基本文件标识符。

3.6.3.1　读取来自选定的基本文件的数据（透明文件）

表 4.　所选定基本文件的读二进制命令

CLA	‘00’/‘0C’
INS	‘B0’
P1	偏移
P2	
发送数据长度Lc域	空
数据域	空
响应数据长度Le域	编码Ne > 0时存在

READ BINARY 命令的响应

数据域	数据已读取
SW1-SW2	9000’正常处理 显示检查或执行错误的其他值

3.6.3.2 利用基本文件标识符（透明文件）读取数据

表 5. 有短基本文件标识符的 READ BINARY 命令

CLA	‘00’/‘0C’
INS	‘B0’
P1	短基本文件标识符
P2	偏移
发送数据长度Lc域	空
数据域	空
响应数据长度Le域	编码Ne > 0时存在。 预计响应数据域中的最大字节数

READ BINARY 命令的响应

数据域	数据已读取
SW1-SW2	9000’正常处理 显示检查或执行错误的其他值

3.6.4 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将该数据发送至电子机读旅行证件芯片。有关扩展长度域的细节，见[ISO/IEC 7816-4]。

3.6.4.1 扩展长度和电子机读旅行证件芯片

对于电子机读旅行证件芯片来说，支持扩展长度域是有条件的。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域，则电子机读旅行证件芯片应支持扩展长度域。如果电子机读旅行证件芯片支持扩展长度域，则必须按照[ISO/IEC 7816-4]的规定，在选择应答（ATS）或 EF.ATR/INFO 中指明。

3.6.4.2 终端

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

- MSE：Set KAT；
- GENERAL AUTHENTICATE。

3.6.5　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]。

3.6.6　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**必须**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.　偏移大于 32 767 字节的 READ BINARY 的命令格式

CLA	‘00’ / ‘0C’
INS	‘B1’
P1	见表 7
P2	
发送数据长度Lc域	命令数据域的长度
数据域	偏移 DO’54’
响应数据长度Le域	编码Ne > 0时存在。 预计响应数据域中的最大字节数

READ BINARY 命令的响应

数据域	自定义 DO’53’
SW1-SW2	9000’ 正常处理 显示检查或执行错误的其他值

表 7.　INS = B1 时 READ BINARY 命令的 P1-P2 编码

P1								**P2**								**含义**
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b8**	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	选定的基本文件
0	0	0	0	0	0	0	0	0	0	0	不全部平等					短基本文件标识符
不全部为零											X	X	X	X	X	基本文件标识符

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：‘0001’被编码为标志 = ’54’长度 = ’01’ 值 = ’01’;
- 偏移：‘FFFF’被编码为标志 = ’54’长度 = ’02’ 值 = ’FFFF’。

随后的READ BINARY 命令**必须**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。

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。

注 1: 在某些情况下，电子机读旅行证件的 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。

注 2: 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。

3.7 记录的处理和命令（逻辑数据结构 2）

旅行记录、签证记录和证书**必须**存储在各自应用下的基本文件中，并且具有可变大小的记录线性结构。见图4和图5。

每个基本文件中的记录都**必须**通过记录号进行编号。每个记录编号**必须**是唯一且连续的（零编号的选定记录不在本文件的范围内）。

在每个支持线性结构的 基本文件 中，记录编号**必须**在添加时按顺序分配，例如按照创建顺序；第一项记录（1号）是首先创建的记录。

以下 [ISO/IEC 7816-4] 命令**必须**用于记录访问：

- APPEND RECORD 添加旅行记录、签证、证书；
- READ RECORD(S) 读取一项或多项旅行记录、签证、证书；
- SEARCH RECORD 搜索一项或多项旅行记录、签证、证书。

注：[ISO/IEC 7816-4]对本小节使用的首字母缩略词进行了定义。

3.7.1 APPEND RECORD 命令

该命令开始在线性结构的结尾添加新的记录。

表 8.　APPEND RECORD 命令

CLA	‘0C’
INS	‘E2’
P1	‘00’（任何其他值均无效）
P2	见表 10
发送数据长度Lc域	命令数据域的长度
数据域	拟添加的记录
响应数据长度Le域	空

表 9.　APPEND RECORD 的响应

数据域	空
SW1-SW2	9000’正常处理； ‘6A84’文件内存空间不足； ‘6700’长度错误(拟添加记录的长度超过了所规定的最大长度)； 显示检查或执行错误的其他值

表 10.　P2 在 APPEND RECORD 命令中的编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
x	x	x	x	x	-	-	-	短基本文件标识符
-	-	-	-	-	0	0	0	所有其他值为预留

3.7.2 READ RECORD 命令

该命令返回所选 基本文件的一个或多个寻址记录的全部或部分内容。根据响应数据长度Le域的记录大小和内容，响应数据域包含以下之一：

- 寻址记录的第一部分；
- 一个（或多个）完整寻址记录；
- 一个（或多个）完整寻址的记录，后接下一记录的第一部分。

详细信息，参见 [ISO/IEC 7816-4]，有关读取旅行记录的示例，参见附录 H。

图 2 描述了响应数据域。Nr 与 TLV 结构的比较表明唯一记录（读取一项记录）或最后一项记录（读取所有记录）是否不完整、完整或进行了填补。

表 11. READ RECORD 命令

CLA	‘0C’	
INS	‘B2’	
P1	记录号（‘00’参照当前记录）	
P2	See表13	
发送数据长度Lc域	空	
数据域	INS = ‘B2’	空
响应数据长度Le域	拟读取作为扩展长度域的最大字节数；Le = ’00 00 00’ （所有其他值不在规范范围内）	

表 12. READ RECORD 的响应

数据域	数据已读取
SW1-SW2	9000’正常处理； ‘6A83’（未找到记录）； 显示检查或执行错误的其他值

表 13. 有 READ RECORD 命令的 P2 编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
x	x	x	x	x	-	-	-	短基本文件标识符
-	-	-	-	-	1	x	x	**P1中的记录号**
-	-	-	-	-	1	0	0	— 读记录P1
-	-	-	-	-	1	0	1	— 读取P1直到最后的所有记录

注1：其他位元组合不在本规范的范围内。如果响应数据长度Le域仅包含设置为'00'的字节，则该命令应该完整读取单个请求的记录或请求的记录序列，具体取决于P2的第3、第2和第1位元以及扩展响应数据长度Le域的最大支持长度。

注2：带有短长度域的READ RECORD命令不在本规范的范围内。

案例a — 完整读取一条记录（响应数据长度Le域只包含设置为‘00’的字节）

记录													
	5F44	L	V	73	L	V	…	5F37	L	V	5F38	L	V
READ RECORD 的响应 (P2 = ‘04’, Le = 0):													
	5F44	L	V	73	L	V	…	5F37	L	V	5F38	L	V

案例b — 读取直到的文件结束多条记录（响应数据长度Le域只包含设置为‘00’的字节）

记录 1								记录 2								记录X
5F44	L	V	...	5F38	L	V		5F44	L	V	...	5F38	L	V		...
READ RECORD 的响应 (P2 = ‘05’, Le = 0):																
5F44	L	V	...	5F38	L	V		5F44	L	V	...	5F38	L	V		...

图 2.　响应数据域

3.7.3　SEARCH RECORD 命令

该命令启动对存储在相应基本文件中的记录的搜索。命令数据域包含记录处理 DO’7F76’，并界定文件参照、搜索配置和搜索字符串（参见表 17）。响应数据域返回记录处理 DO'7F76'，其中包含一个或多个 DO'02'，并包含与寻址基本文件中的搜索指标匹配的记录号。

在支持具有线性结构的可变大小记录的基本文件中，搜索**可能不会**虑及短于搜索字符串的搜索窗口的记录。

表 14.　SEARCH RECORD 命令

CLA	‘0C’
INS	‘A2’
P1	‘00’
P2	见表16
发送数据长度Lc域	命令数据域的长度
数据域	记录处理DO’7F76’(见表17)
响应数据长度Le域	‘00’(短长度)或’00 00’(扩展长度)

表 15. SEARCH RECORD 的响应

数据域	记录处理模板DO'7F76' 包含一个文件编号DO'51'和一个或多个整数DO'02'并包含一个与搜索指标匹配的记录号
SW1-SW2	9000’正常处理; ‘6282’警告：搜索不成功 显示检查或执行错误的其他值

注：如果找不到匹配，则响应数据域可能是空值。

表 16. 用于 SEARCH RECORD 命令的 P2 编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
1	1	1	1	1	0	0	0	通过多个基本文件进行的搜索记录
所有其他值为预留。								

表 17. 用于加强多记录搜索的记录处理模板

标志	值			注
‘7F76’				记录处理DO
	标志	值		
	‘51’	文件标识符或短基本文件标识符		文件编号DO
	‘A1’			搜索配置模板
		标志	值	
		‘80’	‘00’ / ’30’	搜索配置参数： — 按记录号升序搜索 — 搜索的步长：逐字节 — 搜索终止： ‘00’ — 搜索所有寻址记录 ‘30’ — 在第一次匹配后终止搜索
		‘B0’		搜索窗口模板
			标志	值
			‘02’	偏移
			‘02’	字节数
	标志	值		
	‘A3’			搜索字符串模板
		标志	值	
		‘B1’		
			标志	值
			‘81’	搜索字符串

注 1：不支持搜索窗口模板中的空白偏移 DO。

注 2：如果搜索窗口模板使用值“00”作为字节数，则逻辑数据结构 2 电子机读旅行证件芯片必须从记录偏移中搜索所有字节。

注 3：SEARCH RECORD 命令仅支持表 17 所规定的 DO。这意味着 SEARCH RECORD 命令恰好支持记录处理 DO 中的一个文件编号 DO 和搜索字符串模板中的一个搜索字符串。如果使用了附加的 DO，该命令可以忽略附加的 DO 或回答错误代码。

3.8　透明文件的处理及其他（逻辑数据结构 2）

附加的生物特征透明基本文件由逻辑数据结构 2 电子机读证件签发人在操作停用状态下创建（创建机制不在本规范范围内）。在停用状态下，可以根据适当授权选择、写入、更新和读取基本文件。

以下[ISO/IEC 7816-4]命令**必须**用于写入和读取附加生物特征的透明基本文件：

- UPDATE BINARY　　写入附加的生物特征；
- READ BINARY　　读取其他生物特征信息。

在成功满足 LSD2 读写访问条件后，**必须**使用以下[ISO/IEC 7816-9]命令激活透明基本文件：

- ACTIVATE　　激活附加生物特征基本文件。

注：本小节使用的首字母缩略语的定义载于 [ISO/IEC 7816-4] 。

在激活状态下，可以选择和读取具有适当授权（与激活状态相关）的 基本文件，任何类型的授权都不允许写入或附加透明 基本文件。

在写入之前**必须**使用 FILE AND MEMORY MANAGEMENT（FMM）命令来确定基本文件中是否有足够的可用内存空间。

查验系统**必须**对 EF.Biometrics 使用以下写入顺序：

- 第一个 UPDATE BINARY (奇数 INS) 命令必须在数据域中包含以下 DO：
  - — DO'54'包含偏移'00'；

— DO'53' **可能**包含拟存储数据的第一个组块。这个 DO **可能**是空的（'53 00'）；和

— 表示总基本文件 大小（拟分配的内存大小）的专有 DO'C0' 是选择性的。

注 1：逻辑数据结构 2 电子机读旅行证件可以使用 DO'C0'中的 基本文件大小的信息进行内存分配（例如，用于显式动态内存分配）。如果逻辑数据结构 2 电子机读旅行证件不支持基本文件大小的信息 DO（例如，内存已被签发人静态分配，或逻辑数据结构 2 电子机读旅行证件支持隐式动态基本文件内存重新分配），则逻辑数据结构 2 电子机读旅行证件证件可以忽略 DO'C0'，继续写入基本文件的第一个组块并返回'9000'，或者它可以在命令数据域中为不正确的参数返回'6A80'错误。

注 2：如果逻辑数据结构 2 电子机读旅行证件返回带有专有 DO'C0'的 UPDATE BINARY 的任何错误，则查验系统**必须**发送带有零偏移 DO'54'和 DO'53'，但没有 DO'C0'的标准 [ISO/IEC 7816-4] UPDATE BINARY（奇数 INS）命令。

- 后续 UPDATE BINARY（奇数 INS，没有 DO'C0'）命令**应该**使用偏移 n+1，其中 n 表示到目前为止写入 EF.Biometrics 的字节数，即终端**应该**按顺序写入基本文件数据，在两个连续的 UPDATE BINARY 命令之间没有间隙或重叠。

- **可以**在任何 UPDATE BINARY 命令后使用 READ BINARY 命令来验证写入基本文件的数据。

- ACTIVATE 命令**必须**通过永久停止禁止写入基本文件来最终确定 EF.Biometrics 的个性化。

3.8.1 UPDATE BINARY 命令

根据表 18，支持附加生物特征应用的非接触式集成电路必须支持带有奇数 INS 字节"D7"的 UPDATE BINARY 命令。

命令数据域中的 BER-TLV 偏移数据对象的值指定，对偏移进行了规范；命令数据域中的 BER-TLV 自定义数据对象的值，对拟写入的数据进行了规范；命令数据域中选择性的 BER-TLV 文件大小数据对象的值，对总基本文件大小进行了规范。这些 BER-TLV 数据对象的长度域应尽可能短地进行编码。

当 UPDATE BINARY 命令的命令数据域具有专有的 DO'C0' 时，命令 APDU 的 CLA 字节的第 8 位**必须**设置为 1（CLA = '8C'）。

表 18.　带奇数 INS 的 UPDATE BINARY 命令

CLA	’0C’ / ‘8C’
INS	‘D7’
P1	文件标识符 ‘00 00’标识当前的基本文件
P2	
Lc	命令数据域的长度
数据域	偏移数据对象（标志 ‘54’）‖ 自定义数据对象（标志 ‘53’）‖ 文件大小数据对象（标志 ‘C0’）（选择性的）
Le	空

表 19.　UPDATE BINARY 的响应

数据域	空
SW1-SW2	9000’ 正常处理; ‘6A84’（文件内存空间不足） ‘6A80’命令数据域中的参数不正确（例如：不支持DO’C0） ‘6982’安保状态不满足：EF.Biometrics 处于基本文件激活状态 显示检查或执行错误的其他值

如果查验系统不遵循 3.8 节规定的 UPDATE BINARY 序列（即第一个 UPDATE BINARY 不在偏移 0 处开始），逻辑数据结构 2 电子机读旅行证件芯片**可能**错误终止 UPDATE BINARY 命令。

3.8.2　ACTIVATE 命令

ACTIVATE 命令启动当前选定的附加生物特征基本文件从停用状态到激活状态的过渡。

表 20.　ACTIVATE 命令

CLA	‘0C’
INS	‘44’
P1	‘00’
P2	‘00’
Lc	空
数据域	空
Le	空

表 21. ACTIVATE 的响应

数据域	空
SW1-SW2	9000’ 正常处理; 显示检查或执行错误的其他值 注1：SW1-SW2 = '61XX'（正常处理）和SW1-SW2 = '62XX' 或 '63XX'（警告处理）不在本文件的范围内。

成功执行此命令后，当前选定的 EF.Biometrics **必须**切换到激活状态。 如果发生错误（SW 不同于‘9000’），当前选选定的 EF.Biometrics 必须保持在停用状态。

成功执行此命令后（SW1-SW2 = ‘9000’），对 EF.Biometrics 执行行动所需的有效授权**必须**是对应于激活状态的授权（根据表 98)。 对应于停用状态的有效授权**不得**为 EF.Biometrics 提供任何访问权限。

3.8.3 FILE AND MEMORY MANAGEMENT 命令

FILE AND MEMORY MANAGEMENT (FMM) 命令启动对寻址基本文件的已用或可用内存大小的查询。此命令为逻辑数据结构 2 电子机读旅行证件专用。此命令可用于在写入或附加之前检查寻址基本文件的可用空间。此命令也可用于获取最后附加的记录号以供读取。P1 表示基本文件寻址方式，可以使用当前基本文件或文件编号 DO’51’。P2 表示查询的内容。提供具有透明或记录结构的寻址基本文件中的总字节数以及寻址记录基本文件的现有或剩余记录号。总字节数包括基本文件中可用的字节数，没有任何结构信息。这一数字不包括逻辑数据结构 2 电子机旅行证件芯片可能需要的任何结构信息。剩余记录号的假设是所有剩余记录的大小处于最大状态。在一个成功的 FMM 命令之后，被参照的基本文件变成了当前的基本文件。

表 22. FILE AND MEMORY MANAGEMENT（FMM）命令

CLA	‘8C’	
INS	‘5F’	
P1	见表23	
P2	见表24	
Lc	对Nc = 0的编码为空值，对Nc > 0的编码占位填写	
数据域	P1 = ’00’	空
	P1 = ‘01’	文件编号 DO’51’ (见 [ISO/IEC 7816-4])
Le	‘00’	

P1 指定基本文件选择方法。P2 包含一个位图，说明响应中**必须**包含哪些信息。

表 23.　FFM 命令中的 P1 编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	0	0	当前的基本文件
0	0	0	0	0	0	0	1	命令数据域中的文件编号DO’51’
所有其他值为预留								

表 24.　FFM 命令中的 P2 编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
-	-	-	-	-	-	-	1	寻址基本文件中的总字节数
-	-	-	-	-	-	1	-	寻址记录 基本文件中的剩余记录号
-	-	-	-	-	1	-	-	寻址记录基本文件中的现有记录号
x	x	x	x	x	-	-	-	00000（所有其他值为预留）
所有其他值为预留.								

表 25　FMM 命令数据域中的 DO’51’编码

标志	长度	值
‘51’	1	短基本文件标识符（b8位到b4位编码一个从1到30的数字；b3位到b1位设置为000）
	2	文件标识符

FMM 命令的响应包含一组代表所请求文件和内存大小信息的 DOs。

表 26.　FMM 命令的响应

数据域	根据P2为空值或控制信息。见表27。
SW1-SW2	‘9000’，根据 [ISO/IEC 7816-4] 为检查或执行错误

表 27. FILE AND MEMORY MANAGEMENT（文件和内存管理）

标志	长度	值		
‘7F78’	Var	文件和内存管理 DOs		
		标志	长度	值
		‘81’	Var	寻址 基本文件 中的总字节数
		‘82’	Var	寻址记录 基本文件 中的剩余记录数
		‘83’	Var	寻址记录 基本文件 中的现有记录数

注 1：逻辑数据结构 2 电子机读旅行证件芯片**必须**仅返回 FMM DO 中通过 P2 请求的数据对象。

注 2：FMM 的响应数据仅对规定的基本文件有效。来自不同 基本文件的 FMM 响应数据可能不是独立的，例如：如果不同的基本文件共享可用内存。如果合并不同基本文件的 FMM 的响应数据，查验系统应该考虑到这一点。

注 3：当安全消息传递适用于 FMM 命令时，安全消息传递(SM) DO'85'**必须**用于封装加密的命令数据。

3.9 文件结构规范

逻辑数据结构 2 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。

注：是否需要主文件由操作系统、逻辑数据结构 1 或逻辑数据结构 2 应用和选择性的访问条件来决定。

3.9.1 数据编码

数据元素允许使用以下类型的编码：

A = 字母字符 [a-z, A-Z]；
N = 数字字符 [0-9]；
S = 特殊字符 [‘<’]；
B = 二进制数据；
U = UTF-8 编码的 UNICODE 字符。

UNICODE 字符的 UTF-8 编码：

- 对于任何等于或小于 127（十六进制 ‘7F’ ）的字符，UTF-8 编码使用一个与 ASCII 的值相同的字节；

- 对等于或小于 2 047（十六进制 ‘07FF’ ）的字符，UTF-8 编码使用两个字节;
  - — 第一个字节有两个高位元，且第三个位元清零（即十六进制‘C2’到‘专用文件’）;
  - — 第二个字节有高位元，且第二个位元清零（即‘80’到‘BF’）;
- 对等于或大于 2 048 且小于 65 535（十六进制 ‘FFFF’ ）的所有字符，UTF-8 编码使用三个字节。

3.10　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：

- The 逻辑数据结构 1 电子机读旅行证件应用是强制性的;
  - — 逻辑数据结构 1 电子机读旅行证件应用应包括签发国或签发机构记录的数据、数据组 1 至 16 连同证件安保对象（EF. SO_D）;
  - — 逻辑数据结构 1 电子机读旅行证件应用中的证件安保对象（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逻辑数据结构 1 电子机读旅行证件应用中的数据的完整性。
- 逻辑数据结构 1 电子机读旅行证件应用可以选择性地支持 Doc 9303 号文件中描述的其他逻辑数据结构 2 应用，如：
  - — 旅行记录应用；
  - — 签证记录应用；和
  - — 附加生物特征应用。

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。

逻辑数据结构1和逻辑数据结构2应用必须通过使用应用标识（AID）作为保留的专用文件名来选择。应用标识必须由ISO根据[ISO/IEC 7816-5]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（PIX）组成：

逻辑数据结构1电子机读旅行证件应用的环境使用两种不同的应用类别标志分配方案，如Doc 9303号文件第10部分（逻辑数据结构标志）和[ISO/IEC 7816-6]（行业间标志）所定义：

- EF.ATR/INFO 和 EF.DIR 使用行业间标志分配方案;
- 专用文件及其基本文件 使用逻辑数据结构标志分配方案。

本文件规定的行业间标志用于逻辑数据结构环境，因此不需要共存标志分配方案。

3.11 常见基本文件（EFs）

主文件下可能存在以下用于逻辑数据结构 1 和逻辑数据结构 2 应用的常见基本文件：

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

3.11.1 EF.ATR/INFO（有条件的）

如果存在任选的逻辑数据结构 2 应用，则 EF.ATR/INFO 是包含在主文件中的透明基本文件，并且是有条件的必需要求。如果仅存在 逻辑数据结构 1 应用，则此基本文件是任选的。主文件级别的短基本文件标识符是‘01’。

表 28. EF.ATR/INFO

文件名	EF.ATR/INFO
文件标识	‘2F01’
短基本文件标识符	‘01’
选择访问	随时
读取权限	随时
写/更新/擦除访问	永不
文件结构	透明
大小	可变

EF.ATR/INFO的内容可以通过使用SELECT命令后跟READ BINARY命令来检索。READ BINARY命令的响应数据域包含EF.ATR/INFO的内容。

表 29.　逻辑数据结构 2 的 EF.ATR/INFO 的数据元素

<table>
<tr><th>标志</th><th>长度</th><th colspan="3">值</th><th>注</th></tr>
<tr><td rowspan="4">‘47’</td><td rowspan="4">‘03’</td><td colspan="4">卡的功能</td></tr>
<tr><td colspan="3">字节1 — 第一软件功能</td><td>b8 = 1：全专用文件名
b7 到 b4 和 b1专用文件的选择不在Doc 9303号文件的范围内，b3=1：支持短基本文件标识符
b2 = 1：支持记录号</td></tr>
<tr><td colspan="3">字节2 — 第二软件功能</td><td>b8、b7、b6和b5不在Doc9303号文件的范围内，b4到b1 = 0001：一字节数据单元大小</td></tr>
<tr><td colspan="3">字节3 — 第三软件功能</td><td>b8 = 1：支持命令链接
b7 = 1：支持扩展Lc 和Le域，b6 = 1: EF.ATR/INFO中的扩展长度信息
b5到b1不在Doc9303号文件的范围内，</td></tr>
<tr><td rowspan="3">‘7F66’</td><td rowspan="3">Var</td><td colspan="4">扩展长度信息</td></tr>
<tr><td>标志</td><td>长度</td><td>值</td><td>注</td></tr>
<tr><td>‘02’</td><td>Var</td><td>正整数 — 命令APDU中的最大字节数</td><td>对于 逻辑数据结构2，必须至少为 1 000（十进制）</td></tr>
<tr><td>‘02’</td><td>Var</td><td>正整数 — 响应APDU中预期的最大字节数</td><td>对于 逻辑数据结构2，必须至少为 1 000（十进制）</td></tr>
</table>

注1：EF.ATR/INFO中可能存在更多数据对象。

注2：EF.ATR/INFO使用 [ISO/IEC 7816-4] 界定的行业间标志分配方案。

3.11.2　EF.DIR（有条件的）

F.DIR 是包含在[ISO/IEC 7816-4]定义的主文件中的透明基本文件。如果存在任何任选的 逻辑数据结构 2 应用，则 EF.DIR 是有条件的必要要求。如果存在任何任选的逻辑数据结构 2 应用，则 EF.DIR 必须包含在 EF.CardSecurity 的 SecurityInfos 当中。关于 EF.DIR 的 SecurityInfo 的完整描述，可参见 Doc 9303 号文件第 11 部分。

主文件级的短基本文件标识符为‘1E’。

表 30. EF.DIR

文件名	EF.DIR
文件标识	‘2F00’
短基本文件标识符	‘1E’
选择访问	随时
读取权限	随时
写/更新/擦除访问	永不
文件结构	透明
大小	可变

建议将EF.DIR填写在 主文件 当中。如果存在超过强制性 逻辑数据结构1的应用，则**必须**填写EF.DIR，并标明电子机读旅行证件支持的应用列表。它**必须**包含一组应用模板，其中以任何顺序包含应用标识符DO。

表 31. EF.DIR 格式

<table>
<tr><th>标志</th><th>L</th><th colspan="3">值</th><th>描述</th></tr>
<tr><td>‘61’</td><td>‘09’</td><td colspan="3"></td><td>逻辑数据结构1电子机读旅行证件应用模板</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>标志</td><td>L</td><td>值</td><td rowspan="2">逻辑数据结构1电子机读旅行证件应用国际AID：‘A0 00 00 02 47 10 01’</td></tr>
<tr><td>‘4F’</td><td>‘07’</td><td>‘A0 00 00 02 47 10 01’</td></tr>
<tr><td>‘61’</td><td>‘09’</td><td colspan="3"></td><td>旅行记录应用模板</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>标志</td><td>L</td><td>值</td><td rowspan="2">旅行记录国际应用标识：
‘A0 00 00 02 47 20 01’</td></tr>
<tr><td>‘4F’</td><td>‘07’</td><td>‘A0 00 00 02 47 20 01’</td></tr>
<tr><td>‘61’</td><td>‘09’</td><td colspan="3"></td><td>签证记录应用模板</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>标志</td><td>L</td><td>值</td><td rowspan="2">签证记录国际应用标识：
‘A0 00 00 02 47 20 02’</td></tr>
<tr><td>‘4F’</td><td>‘07’</td><td>‘A0 00 00 02 47 20 02’</td></tr>
<tr><td>‘61’</td><td>‘09’</td><td colspan="3"></td><td>附加的生物特征应用模板</td></tr>
<tr><td colspan="2" rowspan="2"></td><td>标志</td><td>L</td><td>值</td><td rowspan="2">附加的生物特征国际应用标识：
‘A0 00 00 02 47 20 03’</td></tr>
<tr><td>‘4F’</td><td>‘07’</td><td>‘A0 00 00 02 47 20 03’</td></tr>
</table>

注：EF.DIR 使用[ISO/IEC 7816-4]定义的标准标志分配方案。

3.11.3　EF.CardAccess（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的完整描述，见Doc9303号文件第11部分。

主文件级别的短基本文件标识符是‘1C’。

表 32.　EF.CardAccess

文件名	EF.CardAccess
文件标识	‘011C’
短基本文件标识符	‘1C’
选择访问	随时
读取权限	随时
写/更新/擦除访问	永不
文件结构	透明
大小	可变

如果口令认证连接确立得到电子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**必须**包含口令认证连接确立所必需的以下安保信息：

- 口令认证连接确立信息;
- 口令认证连接确立域参数信息。

表 33　集成电路上的 EF.CardAccess 内存

文件名	EF.CardAccess
文件标识符	‘011C’
短文件标识符	‘1C’
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保信息。见 Doc 9303 号文件第 11 部分。

3.11.4 EF.CardSecurity（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保信息的完整描述，见 Doc9303 号文件第 11 部分。

主文件级别的短基本文件标识符是‘1D’。

如果出现以下情况，则主文件中包含的 EF.CardSecurity 是必需的：

- IC 支持芯片认证映射的口令认证连接确立；
- 主文件中的终端认证由集成电路支持；或
- 主文件中的芯片认证由集成电路支持。

并且**必须**包含：

- 芯片认证所要求的 ChipAuthenticatio；
- PACE-CAM/芯片认证所要求的 ChipAuthenticationPublicKeyInfo；
- 终端认证所要求的 TerminalAuthenticationInfo；
- EF.CardAccess 中包含的 SecurityInfos。

如果利用芯片认证映射的口令认证连接确立得到电子机读旅行证件芯片支持，主文件中包含的卡安保文件是必要的并**必须**包含以下安保信息：

- 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；
- 卡访问中包含的安保信息。

表 34. 集成电路上的 EF.CardSecurity 内存

文件名	EF.CardSecurity
文件标识符	‘011D’
短文件标识符	‘1D’
读取访问	口令认证连接确立
写访问	永不
大小	可变

根据[RFC 3369]，文件 CardSecurity **必须**实施为 SignedData，具有 encapContentInfo 域中的 id-SecurityObject 的内容类型。安保对象**必须**由证件签名人签署。证件签名者证书**必须**包含在 SignedData 中。以下对象标识符**必须**用于标识内容类型：

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

对 SignedData 数据结构的定义如下：

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

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

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

ContentType ::= OBJECT IDENTIFIER

SignerInfos ::= SET OF SignerInfo

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

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

SignatureValue ::= OCTET STRING
```

4. 逻辑数据结构1电子机读旅行证件应用（强制性）

逻辑数据结构 1 电子读旅行证件结构提供了存储和数字签署可用于将持有人链接到证件的强制性和选择性的数据元素的空间。电子机读旅行证件的逻辑数据结构 1 电子机读旅行证件部分中存储的信息在签发时成为静态，不得以任何可能方式进行修改。此功能是确保个人信息受到保护所必需的，并且可以更容易地检测到对证件的篡改。虽然逻辑数据结构 1 版的电子机读旅行证件包括可用于扩展电子机读旅行证件的使用（即附加生物特征、自动通关等）的选择性的数据域，但在签发时对逻辑数据结构 1 电子机读旅行证件芯片应用进行写保护的要求是**强制性**的。

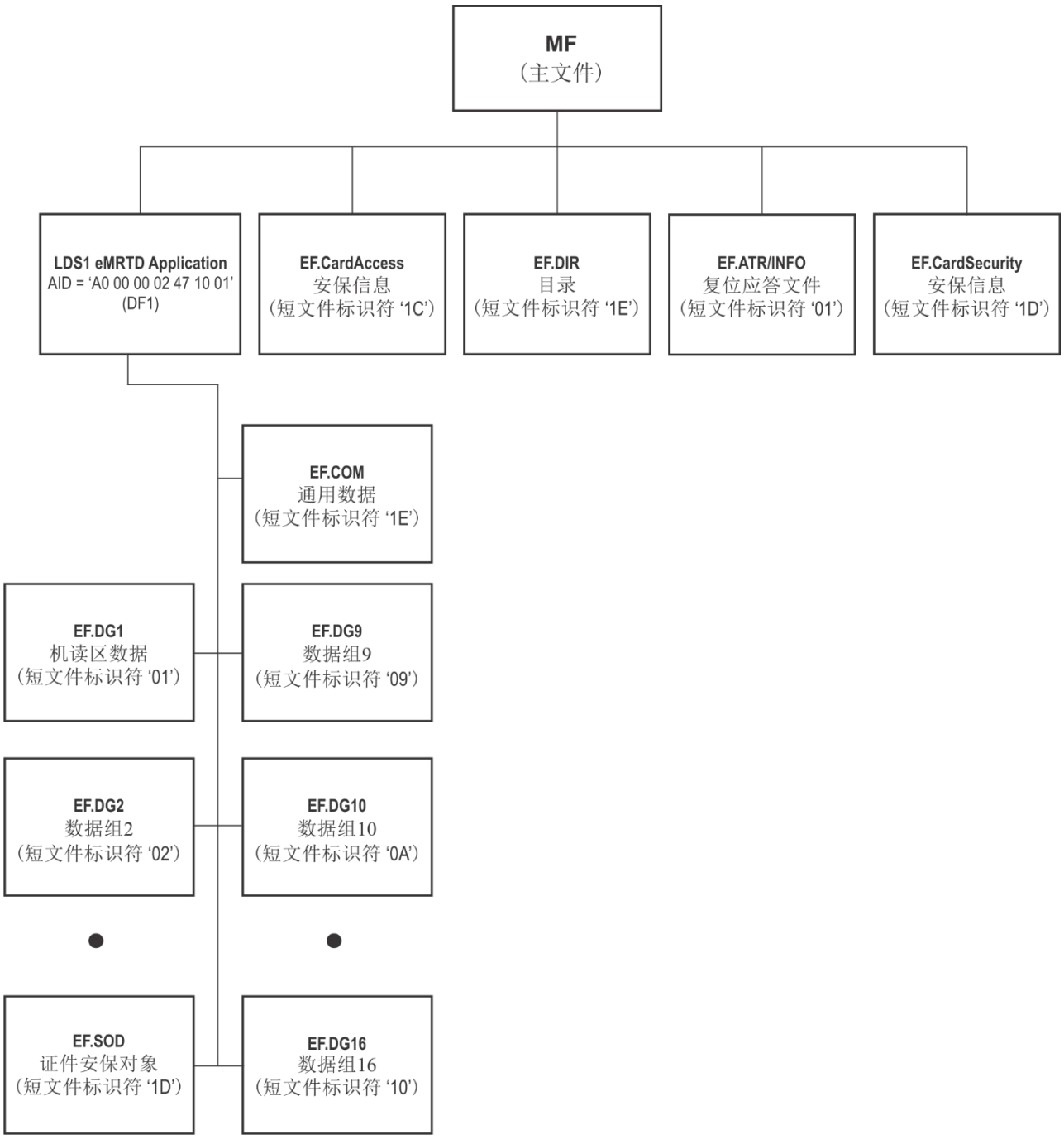

图 3.　逻辑数据结构 1 电子机读旅行证件文件结构摘要

4.1 应用选择 — 专用文件

逻辑数据结构 1 电子机读旅行证件应用应通过使用作为预留专用文件名的应用标识符（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'A000000247'；
- 签发机构存储的数据应用应使用 PIX = '1001'；
- 逻辑数据结构 1 电子机读旅行证件应用的全 AID 是 'A0 00 00 02 47 10 01'。

如果此应用的扩展是空的，IC **必须**拒绝选择该应用。

4.2 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。

4.3 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。

为支持多种实施方式，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逻辑数据结构 1 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：

- 数据元素有限或扩充集；
- 特定数据元素的多次出现；
- 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：
- 即时访问必要的数据元素；和

- 直接访问数据模板和生物特征数据。

4.4　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。

4.5　逻辑数据结构要求

签发国或签发机构选择的逻辑数据结构 1 电子机读旅行证件中包含的非接触式 IC 扩容技术必须允许接收国访问数据。

国际民航组织已确定预定义的、标准化的逻辑数据结构（LDS）必须满足多项强制要求：

- 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。

4.5.1 安保

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。一旦芯片被锁定（在个性化之后和发行之前），就不能向/在/从芯片写入、修改或删除 逻辑数据结构 1 应用数据。被锁定的芯片发行后无法解锁。

4.5.2 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.SOD）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“其他生物特征安保”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。

4.5.3 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。

4.5.4 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、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逻辑数据结构 1 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，建议将逻辑数据结构 1 电子机读旅行证件的非接触式 IC 留出空白并锁定。逻辑数据结构 1 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。

4.5.5 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逻辑数据结构 1 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。

4.5.6 编码生物特征的国际标准

ISO/IEC 39794 接替 [ISO/IEC 19794:2005] 成为生物特征编码的国际标准。对过渡时间表的界定如下：

- 查验系统**必须**在 2020 年 1 月 1 日开始的六年准备期后，于 2026 年 1 月 1 日之前能够处理 ISO/IEC 39794 数据；

- 在 2026 年至 2030 年之间，签发国和签发机构可以在四年过渡期内使用 ISO/IEC 19794-X:2005 或 ISO/IEC 39794-X 中规定的数据格式。在此过渡期间，互操作性和一致性测试将至关重要；和

- 从 2030 年 1 月 1 日起，护照签发人**必须**使用 ISO/IEC 39794-X 对生物特征数据进行编码。

国际民航组织技术报告：ISO/IEC 39794-5 电子机读旅行证件[1]应用简介，为从 [ISO/IEC 19794:2005] 过渡到 ISO/IEC 39794 提供指导。

电子机读旅行证件的逻辑数据结构，包括人脸数据组 2（强制性的）、指纹数据组 3（选择性的）和虹膜数据组 4（选择性的）。每个数据组均包含按照国际标准编码的生物特征数据，以保持国际互操作性。

上述所有数据组（数据组 2、数据组 3 和数据组 4）都必须使用带嵌套生物特征信息模板（BIT）的生物特征信息模板组模板（见 Doc 9303-10 号文件）。嵌套生物特征信息模板的结构包含可使用 ISO/IEC 19794 系列第一版或 ISO/IEC 39794 系列两种标准之一编码的生物特征数据。

ISO/IEC 19794 系列第一版中编码的生物特征数据存储在标志‘5F2E’标识的数据对象当中。ISO/IEC 39794 系列中编码的生物特征数据存储在标志‘7F2E’标识的数据对象当中。

表 1：生物特征数据标志

标志	标准编号
5F2E	ISO/IEC 19794 系列第一版
7F2E	ISO/IEC 39794 系列

标志‘7F2E’标识的数据对象中编码的生物特征数据必须使用下表中的数据结构。

表 2：数据对象‘7F2E’之下的数据结构

<table>
<tr><th>标志</th><th>长度</th><th colspan="4">值</th></tr>
<tr><td>7F2E</td><td>可变</td><td colspan="4">ISO/IEC 7816-11 中界定的生物特征数据模板。</td></tr>
<tr><td></td><td></td><td>标志</td><td>长度</td><td colspan="2">值</td></tr>
<tr><td></td><td></td><td>A1</td><td>可变</td><td colspan="2">标准化格式的生物特征数据 (构建)</td></tr>
<tr><td></td><td></td><td></td><td></td><td>标志</td><td>长度</td><td>值</td></tr>
<tr><td></td><td></td><td></td><td></td><td>64, 65 或 66</td><td>可变</td><td>ISO/IEC 39794 系列表 3 中界定的数据对象。</td></tr>
</table>

[1] 可参见：www.icao.int/security/fal/trip

表 3：ISO/IEC 39794 界定的数据对象的标志

标准编号	标志
ISO/IEC 39794-4	64
ISO/IEC 39794-5	65
ISO/IEC 39794-6	66

4.6 逻辑数据结构 1 电子机读旅行证件基本文件（EFS）

4.6.1 首标和数据组存在信息 EF.COM（强制性的）

EF.COM 位于逻辑数据结构 1 电子机读旅行证件应用（短文件标识符='1E'）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。该逻辑数据结构 1 电子机读旅行证件应用**必须**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 35 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。

建议对依赖于 EF.COM 的查验系统进行修改，以尽快使用 LDS1.8 版中所述的 SOD。

4.6.1.1 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在本文件第 4.6 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）。

4.6.1.2　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在本文件第 4.7.1 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]。

4.6.2　证件安保对象 EF.SO$_D$（强制性的）

除了 LDS 数据组，非接触式 IC 还包含一个存储在 EF.SO$_D$ 中的证件安保对象。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 36　EF.SO$_D$ 标志

标志	长度	值
‘77’	可变	证件安保对象

当前有两个采用了证件安保对象 EF.SOD 的版本。在附录 D 中可以找到旧版 EF.SOD V0，在本节中可以找到建议的 EF.SOD V1。只要求并且只允许一个 EF.SOD。

4.2.6.1　证件安保对象 EF.SOD V1 LDS v1.8

LDS v1.8 的证件安保对象 V1 经扩展后具有一个签名属性，包含逻辑数据结构和 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 PrintableString,
    unicodeVersion PrintableString }
```

4.6.2.2 SO_D V1 的 SignedData 类型

按照 2002 年 8 月的[RFC3369]，加密消息语法（CMS）中的规定，证件安保对象作为一个签名数据类型予以实现。所有安保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 — 该域必须填写。

注 2：x = 不使用 — 该域不应被填充。

注 3：o = 选择性的 — 该域可以填写。

注 4：c = 选择 — 该域内容是从备选内容中选出的。

表 37. 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 — 安保 — 逻辑数据结构安保对象
eContent	m	逻辑数据结构安保对象的编码内容。
Certificates	m	各国需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。

4.6.2.3　SOD V1 的 ASN.1 配置文件逻辑数据结构证件安保对象

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

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

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

-- Constants

ub-DataGroups INTEGER ::= 16

-- Object Identifiers

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

-- LDS Security Object

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

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

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

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

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

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

注 1: dataGroupHashValue（数据组哈希值）域包含由 dataGroupNumbe（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“NULL”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。检查系统必须接受两个条件的 DigestAlgorithmIdentifiers（摘要算法标识符）的域，即没有参数和空值参数。

4.7 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 38 所示的短基本文件标识符。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 38　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	短基本文件标识符	基本文件标识符	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 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’
证件安保对象	$EF.SO_D$	‘1D’	‘01 1D’	‘77’
通用	EF.CARDACCESS	‘1C’	‘01 1C’	
通用	EF.ATR/INFO	‘01’	‘2F 01’	
通用	EF.CardSecurity	‘1D’	‘01 1D’	

4.7.1　数据组 1 — 机读区信息（强制性的）

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逻辑数据结构 1 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‘5F1F’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 39　数据组 1 标志

标志	长度	值		
‘61’	可变			
		标志	长度	值
		‘5F1F’	可变	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。）

4.7.1.1　数据组 1 — TD1 型逻辑数据结构 1 电子机读旅行证件的 EF.DG1 数据元素

本节描述数据组 1 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 40　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 强制性的	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

数据 要素	选择性的或 强制性的	数据元素名称	字节数	固定或 可变的	编码类型
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

4.7.1.2　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 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**必须**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 41　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 强制性的	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

4.7.1.3　数据组 1 — TD3 型逻辑数据结构 1 电子机读旅行证件的 EF.DG1 数据元素

本节描述数据组 1 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**必须**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 42　TD3 型机读旅行证件格式的数据元素

数据 要素	选择性的或 强制性的	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

4.7.2　数据组 2 — 编码识别特征 — 人脸（强制性的）

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 43　数据组 2 标志

标志	长度	值
‘75’	可变	见 EF.DG2 的生物特征编码

4.7.2.1 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 44 数据组 2 — 生物特征编码标志

<table>
<tr><th>标志</th><th>长度</th><th colspan="5">值</th></tr>
<tr><td>‘7F61’</td><td>可变</td><td colspan="5">生物特征信息组模板</td></tr>
<tr><td></td><td></td><td>标志</td><td>长度</td><td colspan="3">值</td></tr>
<tr><td></td><td></td><td>‘02’</td><td>‘01’</td><td colspan="3">整数 — 该类生物特征的样品号</td></tr>
<tr><td></td><td></td><td>‘7F60’</td><td>可变</td><td colspan="3">第一个生物特征信息模板</td></tr>
<tr><td></td><td></td><td></td><td>标志</td><td>长度</td><td colspan="2"></td></tr>
<tr><td></td><td></td><td></td><td>‘A1’</td><td>可变</td><td colspan="2">生物特征首标模板（BHT）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>标志</td><td>长度</td><td>值</td></tr>
<tr><td></td><td></td><td></td><td></td><td>‘80’</td><td>‘02’</td><td>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版本</td></tr>
<tr><td></td><td></td><td></td><td></td><td>‘81’</td><td>‘01-03’</td><td>生物特征类型（选择性的）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>‘82’</td><td>‘01’</td><td>数据组 2 的生物特征子类型</td></tr>
<tr><td></td><td></td><td></td><td></td><td>‘83’</td><td>‘07’</td><td>创建日期和时间（选择性的）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>‘85’</td><td>‘08’</td><td>有效期（从___至___）（选择性的）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>‘86’</td><td>‘04’</td><td>生物特征参考数据（PID）的创建者（选择性的）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>‘87’</td><td>‘02’</td><td>格式所有者（必要的）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>‘88’</td><td>‘02’</td><td>格式类型（必要的）</td></tr>
<tr><td></td><td></td><td></td><td>‘5F2E’ 或 ‘7F2E’</td><td>可变</td><td colspan="2">生物特征数据（根据格式所有者编码）也称为生物特征数据组块（BDB）。见 4.5.6。</td></tr>
</table>

使用生物特征通用交换格式框架的默认对象标识符。[ISO/IEC 7816-11]中指定的就在生物特征信息模板（BIT，标志‘7F60’）下面的对象标识符数据对象（标志‘06’）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/IEC 19794-5]的规定进行编码。

注：ISO/IEC 39794 将接替 ISO/IEC 19794:2005 成为生物特征编码的国际标准。见第 4.5.6 节。

4.7.2.2　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=二进制数据，F = 固定长度域，Var = 可变长度域。

表 45　数据组 2 的数据元素

数据元素	选择性的或强制性的	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	数据元素可按数据元素 01 的规定重现。
03	M	面部生物特征数据编码		Var	B	数据元素可按数据元素 01 的规定重现。

4.7.3　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 46　数据组 3 标志

标志	长度	值
'63'	Var	见 EF.DG3 的生物特征编码

4.7.3.1　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 47 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
				‘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组块（BDB）。见 4.5.6。	
		标志	**长度**			
		‘7F60’	Var	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
				‘83’	‘07’	创建日期和时间（选择性的）
				‘85’	‘08’	有效期（从___至___）（选择性的）

标志	长度	值				
				‘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组块（BDB）。见 4.5.6。	

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‘7F60’）下面的对象标识符数据对象（标志‘06’）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 / IEC19794-4]的规定进行编码。

注：ISO/IEC 39794 将接替 ISO/IEC 19794:2005 成为生物特征编码的国际标准。见第 4.5.6 节。

4.7.3.2　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=二进制数据，F = 固定长度域，Var = 可变长度域。

表 48　EF.DG3 的数据元素

数据元素	选择性的或强制性的	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	数据元素可按数据元素 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	B	数据元素可按数据元素 01 的规定重现。

4.7.3.2.1 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 49 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

4.7.3.2.2 零样品的编码

没有签发带指纹的逻辑数据结构 1 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逻辑数据结构 1 电子机读旅行证件的证件安保对象中一个静态的数据组 3 散列，其中生物特征在签发逻辑数据结构 1 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，那些支持在其逻辑数据结构 1 电子机读旅行证件中使用指纹的国家，在签发逻辑数据结构 1 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‘00’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‘53’。

表 50　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）。		

4.7.3.2.3　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 51　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’	Var	生物特征信息组模板。				
			‘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’	Var	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’	Var	生物特征首标模板。		
					‘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’	Var	生物特征数据。该生物特征数据组块必须确切包含一个指纹图像。		

注：ISO/IEC 39794 将接替 ISO/IEC 19794:2005 成为生物特征编码的国际标准。见第 4.5.6 节。

4.7.3.2.4 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 52 对一个以上样品编码

标志	长度	值						
‘63’	Var	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’	Var	生物特征信息组模板。				
			‘02’	‘01’	‘02’	界定作为随后的生物特征信息模板存储的指纹总数。		
			‘7F 60’	Var	第一个生物特征信息模板。			
				‘A1’	Var	生物特征首标模板。		
					‘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。也有可能指纹的次序（左/右）是不同的。			
				‘5F 2E’	Var	生物特征数据组块。生物特征数据组块必须确切包含一个指纹图像。		
			‘7F 60’	Var	第二个生物特征信息模板。			
				‘A1’	Var	生物特征首标模板。		
					‘81’	‘01’	‘08’	生物特征类型“指纹”
					‘82’	‘01’	‘0A’	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’	Var	生物特征数据组块。生物特征数据组块必须确切包含一个指纹图像。		

注：ISO/IEC 39794 将接替 ISO/IEC 19794:2005 成为生物特征编码的国际标准。见第 4.5.6 节。

4.7.4 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 53　数据组 4 标志

标志	长度	值
‘76’	Var	见 EF.DG4 的生物特征编码

4.7.4.1　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 54　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		
			‘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’	‘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）

标志	长度	值				
			‘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组块（BDB）。见 4.5.6。	
		标志	长度	值		
		‘7F60’	Var	第 2 个生物特征信息模板		
			标志	长度	值	
			‘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’	‘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组块（BDB）。见 4.5.6。	

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‘7F60’）下面的对象标识符数据对象（标志‘06’）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 / IEC19794-6]的规定进行编码。

注：ISO/IEC 39794 将接替 ISO/IEC 19794:2005 成为生物特征编码的国际标准。 见第 4.5.6 节。

4.7.4.2 数据组 4 — EF.DG4 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= 二进制数据，F = 固定长度域，Var = 可变长度域。

表 55　数据组 4 的数据元素

数据元素	选择性的或强制性的	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	数据元素可按数据元素 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	B	数据元素可按数据元素 01 的规定重现。

4.7.4.2.1　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 56　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

4.7.4.2.2 零样品的编码

没有签发带虹膜的逻辑数据结构 1 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逻辑数据结构 1 电子机读旅行证件的证件安保对象中一个静态的数据组 4 散列，其中生物特征在签发逻辑数据结构 1 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，那些支持在其逻辑数据结构 1 电子机读旅行证件中使用虹膜的国家，在签发逻辑数据结构 1 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‘00’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‘53’。

表 57 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’	生物特征信息模板组模板		
			‘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）。		

4.7.4.2.3 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。

4.7.4.2.4 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。

4.7.5 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 58 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 59　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

4.7.5.1　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= 二进制数据，F = 固定长度域，Var = 可变长度域。

表 60　数据组 5 的数据元素

数据元素	选择性的或强制性的	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	数据元素可按数据元素 01 的规定重现。
03	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	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。

4.7.6 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 61 数据组 6 标志

标志	长度	值
‘66’	Var	

4.7.6.1 数据组 6 — EF.DG6 数据元素

数据组 6 的数据元素留作将来使用。

4.7.7 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（DG7）的数据元素应如下：

表 62 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 63 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

4.7.7.1 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= 二进制数据，F = 固定长度域，Var = 可变长度域。

表 64　数据组 7 的数据元素

数据要素	选择性的或强制性的	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	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。

4.7.8　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、机器辅助安保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 65　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。

4.7.8.1　数据组 8 — EF.DG 8 数据元素

本节描述数据组 8 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= 二进制数据，F = 固定长度域，Var = 可变长度域。

表 66　数据组 8 的数据元素

数据元素	选择性的或强制性的	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（包括数据元素 02 至数据元素 04）。
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, U, B	格式由签发国或签发机构自行确定。

4.7.9　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（DG9）的数据元素应如下：

表 67　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。

4.7.9.1　数据组 9 — EF.DG9 数据元素

每个数据组区域内的数据组 9 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= 二进制数据，F = 固定长度域，Var = 可变长度域。

表 68　数据组 9 的数据元素

数据元素	选择性的或强制性的	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（包括数据元素 02 至数据元素 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	B	

4.7.10　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 69　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。

4.7.10.1　数据组 10 — EF.DG 10 数据元素

本节描述数据组 10 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= 二进制数据，F = 固定长度域，Var = 可变长度域。

表 70　数据组 10 的数据元素

数据要素	选择性的或强制性的	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（包括数据元素 02 至数据元素 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, U,B	格式由签发国或签发机构自行确定。

4.7.11　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 71　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

4.7.11.1　数据组 11 – EF.DG 11 数据元素

本节描述数据组 11 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 = 二进制数据，F = 固定长度域，Var = 可变长度域。

表 72 数据组 11 的数据元素

数据要素	选择性的或强制性的	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	U	自由格式文本。
04	O	出生年月日	8	F	N	YYYYMMDD
05	O	出生地	99 最大	Var	U	自由格式文本。
06	O	地址	99 最大	Var	U	自由格式文本。
07	O	电话	99 最大	Var	N,S	自由格式文本。按照 ITU-T E.164 的建议编码。
08	O	职业	99 最大	Var	U	自由格式文本。
09	M, 如果包括数据元素 08	职衔	99 最大	Var	U	自由格式文本。
10	M, 如果包括数据元素 09	个人简历	99 最大	Var	U	自由格式文本。
11	M, 如果包括数据元素 10	公民资格证明		Var	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	U	自由格式文本，用<隔开。
13	O	监护信息	999 最大	Var	U	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。

4.7.12　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 73　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数据元素 02（带标志‘02’的数据对象）中所指示的重复多次。
		‘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。

4.7.12.1　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 = 二进制数据，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 74　数据组 12 的数据元素

数据元素	选择性的或强制性的	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	U	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	U	自由格式文本。
04	O	签注/意见	99 最大	Var	U	自由格式文本。
05	O	税收/出境要求	99 最大	Var	U	自由格式文本。
06	O	电子机读旅行证件的正面图像		Var	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	B	按照 [ISO/IEC 10918-1]进行格式化
08	O	个人化时间	14	F	N	yyyymmddhhmmss
09	O	个人化设备序列号	99 最大	Var	U	自由格式。

4.7.13　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 75　数据组 13 标志

标志	长度	值
‘6D’	Var	

4.7.14　数据组 14 — 安保选项（有条件的）

数据组 14(DG14)包含附加安保机制的安保选项。详情见 Doc 9303 号文件第 11 部分。电子机读旅行证件应用中包含的文件数据组 14 是必要的，如果芯片认证或利用通用映射/集成映射的口令认证连接确立（PACE - GM/-IM）得到电子机读旅行证件芯片支持的话。

表 76　数据组 14 标志

标志	长度	值
‘6E’	Var	参考 Doc 9303 号文件第 10 部分的数据组 14 安保信息

4.7.14.1　数据组 14 — EF.DG14 数据元素

本节描述数据组 14 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= 二进制数据，F = 固定长度域，Var = 可变长度域。

表 77　数据组 14 的数据元素

数据元素	选择性的或强制性的	数据元素名称	字节数	固定或可变的	编码类型	编码要求
	O	安保信息		Var	B	参考 Doc 9303 号文件第 10 部分。第 4.7.14.2 中所界定的数据组 14 安保信息

4.7.14.2　数据组 14 安保信息

下面一般性的 ASN.1 数据结构 SecurityInfos（安保信息）允许次要生物特征安保选项的各种实施。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保协议。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
}
```

安保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。

4.7.15 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 78 数据组 15 标志

标志	长度	值
‘6F’	Var	参考 Doc 9303 号文件第 11 部分

4.7.15.1 数据组 15 — EF.DG15 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= 二进制数据，F = 固定长度域，Var = 可变长度域。

表 79 数据组 15 的数据元素

数据要素	选择性的或强制性的	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

4.7.16 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（DG16）（如所有其他数据组一样）在签发后不应更新；数据组 16 由证件安保对象中的一个散列值表示，证件安保对象仅在签发时签名一次。

表 80　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’	‘08’			记录的日期数据
‘5F51’	Var			人的姓名
‘5F52’	Var			电话
‘5F53’	Var			地址

4.7.16.1　*数据组 16 — EF.DG16 数据元素*

本节描述数据组 16 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 = 二进制数据，F = 固定长度域，Var = 可变长度域。

表 81　数据组 16 的数据元素

数据元素	选择性的或强制性的	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	1	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 = YYYYMMDD。
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	A, N, S	按照机读区插入填充符（<）。不允许截取。
04	M, 如果包括 数据元素 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）。按照 ITU-T E.164 的建议编码。
05	M	被通知人地址		Var	U	自由格式文本。

5. 逻辑数据结构 2 应用（选择性的）

逻辑数据结构 2（LDS2）是逻辑数据结构 1 电子机读旅行证件芯片的一个选择性的和向后兼容的扩展，允许在证件签发后对旅行信息进行数字安全存储。逻辑数据结构 2 通过增加可以数字存储旅行数据（签证和旅行印章）及其他有助于持证人旅行信息的应用（附加生物特征），扩展电子机读旅行证件有效期内的使用范围。通过将证件中包含的其余数据“数字化”提供一系列简化手续效益，更好地发挥电子机读旅行证件的全部潜力，同时进一步保护证件免受伪造、复制和未经授权的阅读或书写等漏洞的侵害。

被描述为逻辑数据结构 2 的附加选择性应用是：

- 旅行记录（印章）；
- 电子签证；和
- 附加生物特征。

在宣布任何选择性 逻辑数据结构 2 应用之前，必须提交 逻辑数据结构 1 电子机读旅行证件应用。

5.1 旅行记录应用（有条件的）

旅行记录应用**可以**由签发国或签发机构实施。如果已调用选择性的旅行记录应用，则以下内容在一定条件下便是必需的。

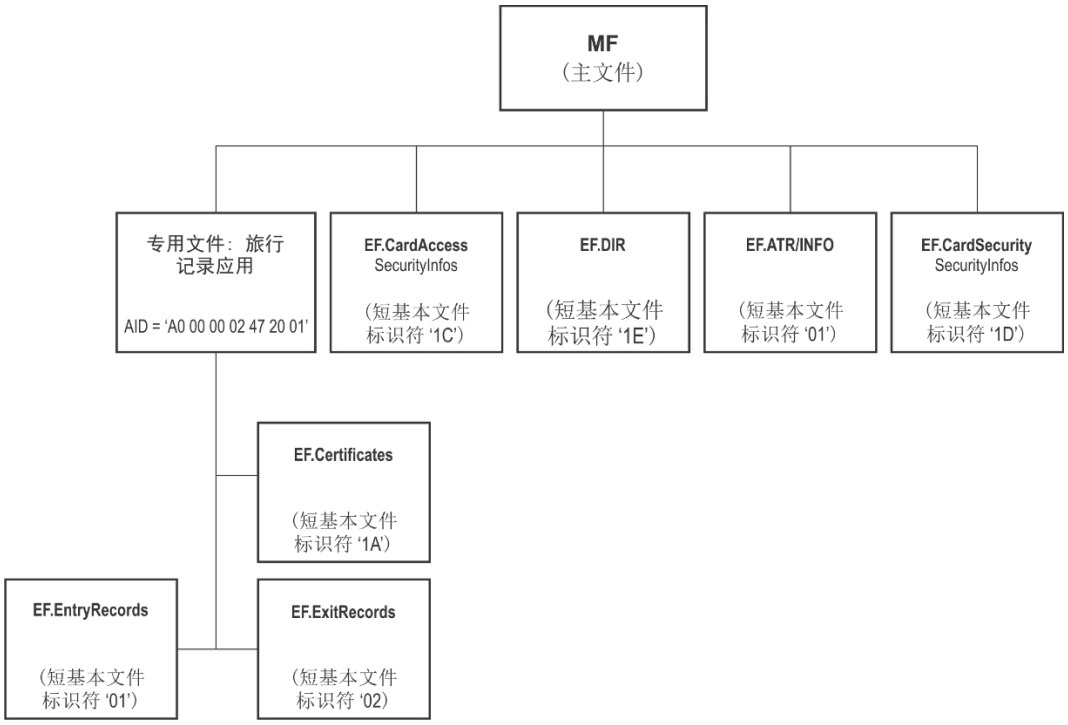

图 4. 旅行记录结构

根据 [ISO/IEC 7816-4]，入境和出境旅行记录存储在两个单独的基本文件 EF.EntryRecords 和 EF.ExitRecords 中，在旅行记录应用专用文件下，两者都具有线性结构，记录大小可变。旅行记录签名者证书存储在单独的基本文件 EF.Certificates 中，具有线性结构且记录大小可变。

5.1.1　应用选择 — 专用文件

旅行记录应用**必须**通过使用作为预留专用文件名的应用标识符（AID）来选择。应用标识符**必须**包括国际标准化组织根据 [ISO/IEC7816-5] 分配的注册应用标识符，后接旅行记录应用的专有应用标识符扩展（PIX）：

- 注册应用标识符是‘A0 00 00 02 47’;
- 旅行记录应用必须使用专有应用标识符扩展= ‘20 01’; 和
- 旅行记录应用的全部应用标识符必须是‘A0 00 00 02 47 20 01’。

如果有效授权不授予对逻辑数据结构 2 应用中任何数据的访问权限，则集成电路**必须**拒绝选择此应用。

5.1.2　EF.Certificates（强制性）

旅行记录签名者证书存储在应用专用文件内的 基本文件 中，具有线性结构，记录大小可变。这些证书旨在供 查验系统用于进一步离线验证 EF.ExitRecords 和 EF.EntryRecords 文件中每项记录的数字签名。

表82.　EF.Certificates

文件名	EF.Certificates
文件标识	‘011A’
短基本文件标识符	‘1A’
选择/FMM访问	PACE+TA（根据表 96，旅行记录授权b3位）
读记录/搜索记录访问	PACE+TA（根据表 96，旅行记录授权b3位）
附加记录访问	PACE+TA（根据表 96，旅行记录授权b4位）
写/更新记录访问	永不
擦除记录访问	永不
文件结构	线性结构，记录大小可变
大小	可变

证书记录包含单个 逻辑数据结构2-TS签名人X.509证书数据对象。一个证书记录**可以**被一个或多个出入境旅行记录编号。

表 83. EF.Certificates 记录格式

标志	内容	强制性/选择性的	格式	示例
‘5F3A’	证书序号	M	V(22)B	‘5F3A’ ‘Len’ {国家代号|| SerialNumber }
‘72’	X.509证书	M	V (900) B	‘72’ ‘Len’ { X.509 证书 }

注：本表规定的行业间标志用于逻辑数据结构环境，因此不需要共存标志分配方案。

根据Doc 9303第3部分，DO‘5F3A’**必须**包含两个字母的国家代号（与X.509题目证书上签发的countryName相同的编码和数值），后接证书序号。

每个X.509证书都包含一组表84所示的ASN.1编码的数据元素。有关X.509证书的详细要求可参见Doc 9303号文件第12部分的证书配置文件规范。

表 84. X.509 证书结构示例

域			说明	示例值
证书				
	版本		必须是第3版	2
	serialNumber		独特正整数	最多20个字节
	签名		签名算法	ecdsa-with-SHA256
	签发者			
		countryName	签发国名	‘US’
		commonName	签发者名(最多9个字符)	‘DHSCA0001’
	有效性			
		notBefore	证书生效日期	‘131225000000Z’
		notAfter	证书失效日期	‘230824235959Z’
	题目			
		countryName	查验系统 国家名	‘US’
		commonName	查验系统 名(最多9个字符)	‘SFO000001’

subjectPublicKeyInfo			
	公钥算法	ecPublicKey	
	题目公钥	查验系统 公钥	ECC256 公钥
扩展			
	AuthorityKeyIdentifier		
	ExtKeyUsage		
签名算法		ecdsa-with-SHA256	
签名		签发者签名	ECDSA256签名

注：此表仅为举例说明。使用APPEND RECORD命令将证书记录写入旅行记录应用专用文件下的EF.Certificates。可以使用READ RECORD命令从EF.Certificates读取证书记录。不得更新或删除证书记录。旅行记录应用专用文件下EF.Certificates的最大记录数必须是254。

5.1.3　EF.ExitRecords（强制性的）

出境记录必须在登机时即由经授权的查验系统添加。

表 85.　EF.ExitRecords

文件名	EF.ExitRecords
文件标识	’0102’
短基本文件标识符	’02’
选择/FMM 访问	PACE+TA（根据表 96，旅行记录授权 b1 位）
读记录/ 搜索记录访问	PACE+TA（根据表 96，旅行记录授权 b1 位）
附加记录访问	PACE+TA（根据表 96，旅行记录授权 b2 位）
写/更新记录访问	永不
擦除记录访问	永不
文件结构	线性结构，记录大小可变
大小	可变

出境记录的内容如表 86 所示。

注：下表规定的行业间标志用于逻辑数据结构环境，因此不需要共存标志分配方案。

表 86. 入境/出境记录格式

标志	标志	内容	强制性/选择性的	格式	示例
‘5F44’		登机/下机的国家（搜索记录副本）	M	F (3) A	USA
‘73’	入境/出境旅行记录（签名信息）				
	‘5F44’	登机/下机的国家	M	F (3) A	USA
	‘5F4C’	签证批准、拒绝和撤销	O	V (50) A,N,S,U	自由格式文本
	‘5F45’	旅行日期（入境/出境日期）	M	F (8) N	20120814 (yyyymmdd)
	‘5F4B’	检查当局	M	V (10) A,N,S	CBP
	‘5F46’	检查地点（入境/出境口岸）	M	V (10) A,N,S	SFO
	‘5F4A’	检查员编号	M	V (20) A,N,S	SFO00001234
	‘5F4D’	检查结果	O	V (50) A,N,S,U	自由格式文本
	‘5F49’	旅行方式	O	F (1) A	A（航空），S（航海），L（陆地）
	‘5F48’	滞留时间（天）	O	V (2) B	‘00FF’ (255 days)
	‘5F4E’	持有人需要在签发国遵守的条件	O	V(50) A,N,S,U	自由格式文本
‘5F37’	真实性标记（签名）		M	V (140) B	‘5F’ ‘37’ Len {签名}
‘5F38’	证书储备中的逻辑数据结构 2-TS 签名者证书编号（记录号）		M	F (1) B	‘01’ …’FE’

注 1：A = 字母字符 [a-z, A-Z]，N = 数字字符 [0-9]，S = 特殊字符 [‘<’]，B = 二进制数据，F = 固定长度域，V = 可变长度域。

注 2：由于逻辑数据结构 2-TS 签名者证书在多个旅行记录中可能相同（例如，当通过只有一个 逻辑数据结构 2-TS 签名者的同一机场进出一个国家时），在将新证书写入/附加到 EF.Certificates 之前，查验系统应在 EF.Certificates 中查找同一证书的副本，并参考现有证书。这将减少 EF.Certificates 的大小并实现更快的查找。

注 3：逻辑数据结构 2 电子机读旅行证件不强制要求 查验系统 只将入境记录写入 EF.EntryRecords，而不写入 EF.ExitRecords，反之亦然。

注 4：根据 Doc 9303 号文件第 3 部分的登机/下机国家三字代码。

数据对象在记录中的顺序是固定的。查验系统 **必须**按照表中规定的顺序使用数据对象构建记录内容。

每项记录**必须**包含通过 DO’73’计算的数字签名（真实性标记），包括标志 73 和长度。签名由 逻辑数据结构 2-TS 签名者生成。

核实旅行记录签名所需的逻辑数据结构 2-TS 签名者证书**必须**存储在旅行记录应用专用文件下的 EF.Certificates 中（如果同一文件中尚未提供）。

旅行记录使用 APPEND RECORD 写入（附加）到 基本文件。旅行记录**不得**更改（更新）或删除。每项基本文件中允许的最大记录数**必须**是 254。

5.1.4　EF.EntryRecords（强制性）

下机时**必须**由经授权的查验系统附加入境记录。

表 87.　EF.EntryRecords

文件名	EF.EntryRecords
文件标识	‘0101’
短基本文件标识符	‘01’
选择/FMM 访问	PACE+TA（根据表 96，旅行记录授权 b1 位）
读记录/ 搜索记录访问	PACE+TA（根据表 96，旅行记录授权 b1 位）
附加记录访问	PACE+TA（根据表 96，旅行记录授权 b2 位）
写/更新记录访问	永不
擦除记录访问	永不
文件结构	线性结构，记录大小可变
大小	可变

入境记录的结构与表 86 所规定的出境记录的结构相同。

5.2　签证记录应用（有条件的）

签证记录应用**可以**由签发国或签发机构实施。如果调用了任选的签证记录应用，则以下便成为有条件限制的必要内容。

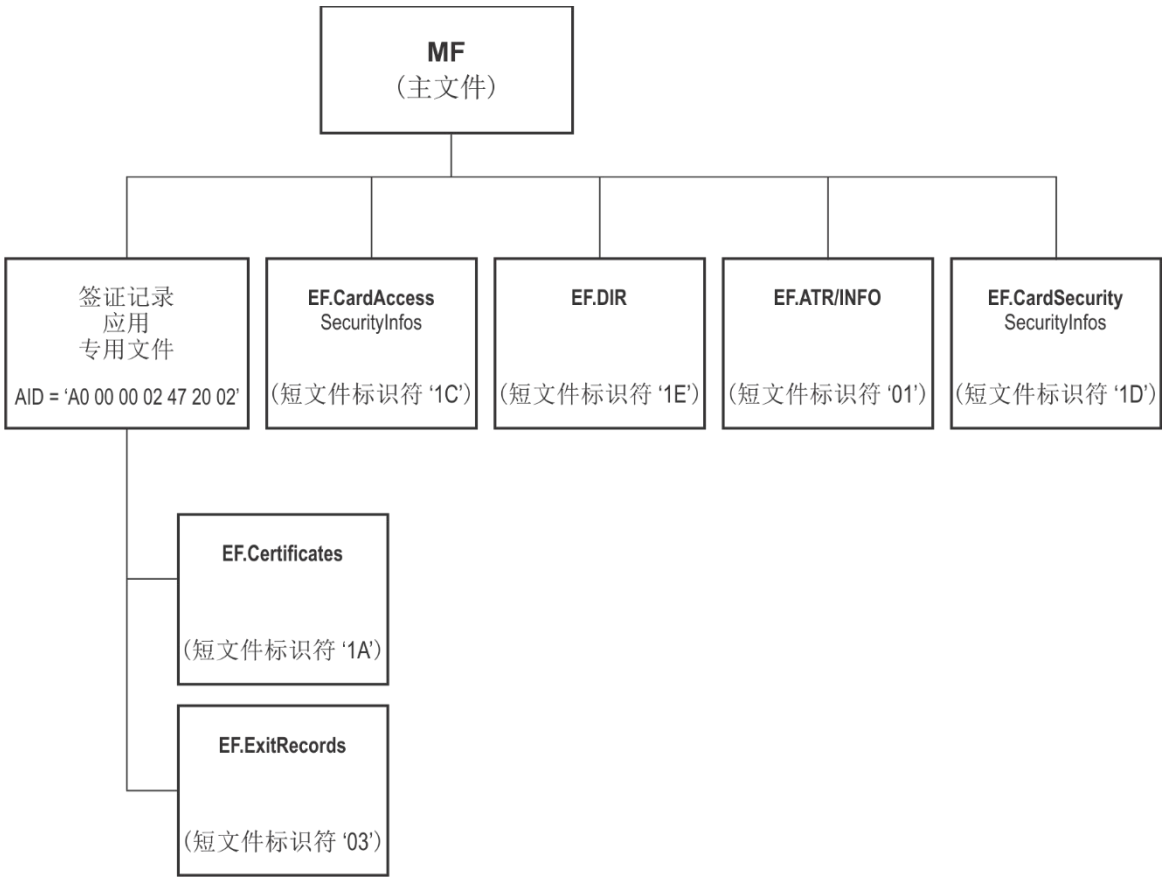

图 5. 签证记录结构

签证记录保存在签证记录应用专用文件下的基本文件 EF.VisaRecords 中。根据[ISO/IEC 7816-4]，基本文件**必须**具有记录大小可变的线性结构。签证记录签名者证书存储在单独的基本文件 EF.Certificates 中，具有线性结构，记录大小可变。

5.2.1 应用选择 — 专用文件

签证记录应用**必须**使用应用标识符（AID）作为预留专用文件名进行选择。应用标识符必须包括 ISO 根据 [ISO/IEC 7816-5] 分配的注册应用标识符，后接签证记录应用的专有应用标识符扩展（PIX）：

- 注册应用标识符是'A0 00 00 02 47'；
- 签证记录应用必须使用专有应用标识符扩展='2002'；和
- 签证记录应用的完整应用标识符是'A0 00 00 02 47 20 02'。

如果有效授权未授予对逻辑数据结构 2 应用中任何数据的访问权限，则 IC **必须**拒绝选择此应用。

5.2.2　EF.Certificates（强制性）

签证记录签名者证书存储在应用专用文件内的EF.Certificates中，呈线性结构，记录大小可变。这些证书旨在供 查验系统 进一步离线验证EF.VisaRecords中每项记录的数字签名。

表88.　EF.Certificates

文件名	EF.Certificates
文件标识	‘011A’
短基本文件标识符	‘1A’
选择/FMM访问	PACE+TA（根据表97，签证记录授权b3位）
读记录/ 搜索记录访问	PACE+TA（根据表97，签证记录授权b3位）
附加记录访问	PACE+TA（根据表97，签证记录授权b4位）
写/更新记录访问	永不
擦除记录访问	永不
文件结构	线性结构，记录大小可变
大小	可变

证书记录包含单个 逻辑数据结构 2-V 签名者 X.509 证书数据对象。一个证书记录**可以**被一个或多个签证记录编号。

签证应用中的证书记录的结构与表 83 所规定的旅行记录应用中的证书记录的结构相同。

证书记录使用 APPEND RECORD 命令写入签证记录应用专用文件下的 EF.Certificates。可以使用 READ RECORD 命令从 EF.Certificates 读取证书记录。**不得**更新或删除证书记录。签证记录应用专用文件下 EF.Certificates 的最大记录数为 254。

5.2.3　EF.VisaRecords（强制性的）

签证记录**必须**存储在具有记录大小可变的线性结构的 EF.VisaRecords 中。

表 89. EF.VisaRecords

文件名	EF.VisaRecords
文件标识	‘0103’
短基本文件标识符	‘03’
选择/FMM访问	PACE+TA（根据表97，签证记录授权b1位）
读记录/搜索记录访问	PACE+TA（根据表97，签证记录授权b1位）
附加记录访问	PACE+TA（根据表97，签证记录授权b2位）
写/更新记录访问	永不
擦除记录访问	永不
文件结构	线性结构，记录大小可变
大小	可变

每项签证记录**必须**包含一系列 BER-TLV 数据对象（DO‘5F28’和 DO‘71’），后接真实性标记（签名）DO，以及包含对 EF.Certificates 中逻辑数据结构 2-V 签名者证书编号的 DO。DO‘71’包含下表中列出的一组 DOs（域）。

注：下表规定的行业间标志用于逻辑数据结构环境，因此不需要共存标志分配方案。

表 90. EF.VisaRecords 格式

标志	标志	内容	强制性/选择性的/有条件的	格式	示例
‘5F28’		签发国或机构（搜索记录副本）	M	F (3) A	NLD
‘71’	签证记录（签名信息）				
	‘5F28’	签发国或机构	M	F (3) A	NLD
	‘43’	证件类型	M	F (2) A,N,S	VS
	‘5F71’	A类机读签证	O	F (48) A,N,S	
	‘5F72’	B类机读签证	O	F (44) A,N,S	VCD<<DENT<<ARTHUR<PHILIP<<<<<<<<<<<<
	‘5F73’	入境次数	O	V (1) B	‘01’ – ‘FF’

标志	标志	内容	强制性/选择性的/有条件的	格式	示例
	‘5F74’	滞留时间（日月年）	O	F (3) B	‘010000’ – ‘FFFFFF’
	‘5F75’	护照号	O	F (9) A,N,S	XI85935F8
	‘5F76’	签证类型/类别/种类	O	V (4) B	
	‘5F77’	领土信息	O	V (8) B	
	‘49’	签发地（签发机关）	M	V (50) A, Sp	纽约
	‘5F25’	生效日期（签发日期）	M	F (8) N	20120826 (yyyymmdd)
	‘5F24’	失效日期	M	F (8) N	20130826 (yyyymmdd)
	‘5A’	证件号	M	F (9) A,N,S	XI85935F8
	‘5F32’	补充信息（签注：持续时间、限制和付费情况）	O	V (50) A,N,S,U	自由格式文本
	‘5B’	持有人姓名（全名）	M	V (50) A, Sp	VAN DER STEEN MARIANNE LOUISE
	‘5F33’	主要标识符（姓）	M	V (50) A, Sp	VAN DER STEEN
	‘5F34’	次要标识符（名）	M	V (50) A, Sp	MARIANNE LOUISE
	‘5F35’	性别	M	F (1) A,S	F, M, or <
	‘5F2B’	出生日期	M	F (8) N,S	19870814 (yyyymmdd)
	‘5F2C’	国籍	M	F (3) A	NLD
	‘5F1F’	机读区	M	V (50) A,N,S	VAN<DER<STEEN<< MARIANNE<LOUISE
	‘5F40’	附加的生物特征基本文件编号	O	F (2) B	’0201’
‘5F37’	真实性标记（签名）		M	V (140), B	‘5F’ ‘37’ Len {签名}
‘5F38’	逻辑数据结构2-V证书储备签名者证书编号（记录号）		M	F (1) B	‘01’ …’FE’

注 1：A = 字母字符[a-z, A-Z]，N = 数字字符[0-9]，S = 特殊字符[‘<’]，B=二进制数据，F = 固定长度域，V = 可变长度域，Sp=空格。

注 2：根据 Doc 9303 号文件第 3 部分的签发国三字代码。

注 3：任选的 DO'5F40'，如填写，则必须在包含生物特征数据的附加生物特征应用中包含基本文件的两个字节标识符。只有当电子机读旅行证件上填写附加生物特征应用时，才能使用这一 DO。

记录中数据对象的顺序是固定的。查验系统**必须**按照表中规定的顺序使用数据对象构建记录内容。

每项签证记录**必须**包含一个通过 DO'71'计算的数字签名（真实性标记），包括标志 71 和长度。签名由 逻辑数据结构 2-V 签名者生成。

核实签证记录签名所需的逻辑数据结构 2-V 签名者证书存储在签证记录应用专用文件下的单独 EF.Certificates 储备中。

每项签证记录**必须**使用 APPEND RECORD 附加到 EF.VisaRecords。签证记录**不得**涂改（更新）或擦除。EF.VisaRecords 中允许的最大记录数**必须**是 254。

5.3 附加生物特征应用（有条件的）

附加生物特征应用**可以**由签发国或签发机构实施。如果已调用任选的附加生物特征应用或任何签证记录已对其进行引用，则以下便是有条件限制的必要内容。

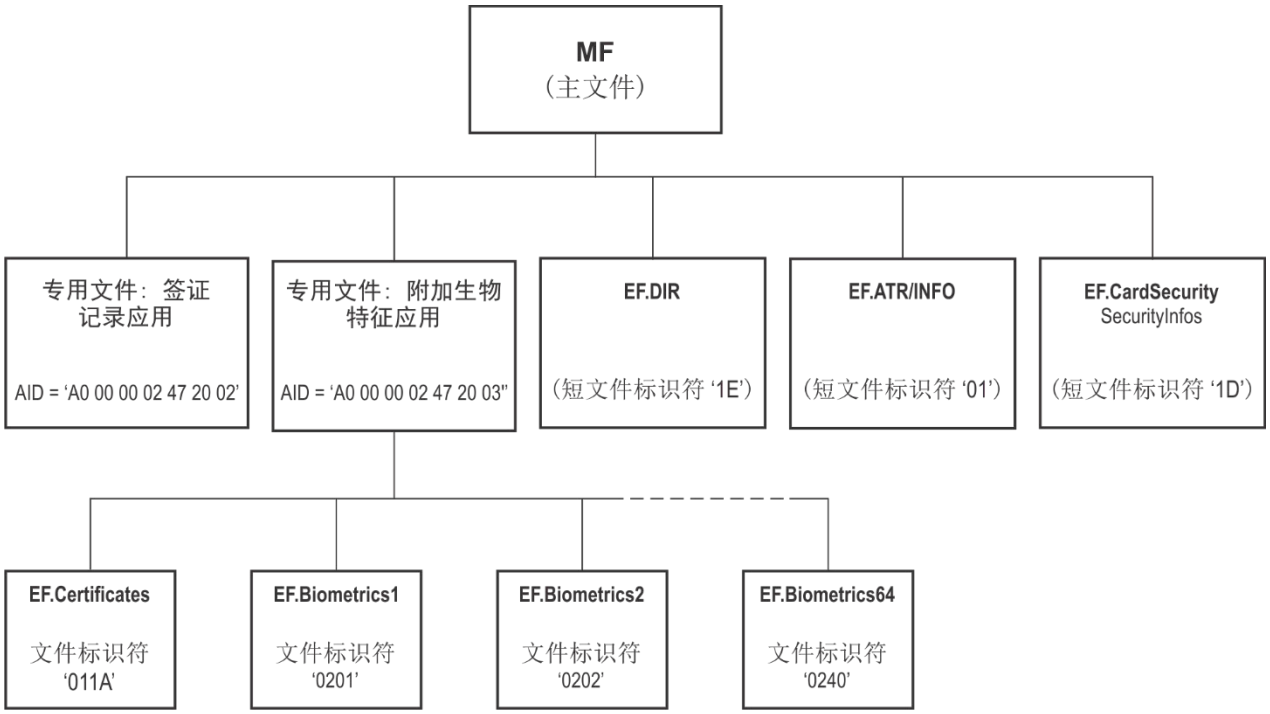

图 6. 附加生物特征应用结构

5.3.1　应用选择 — 专用文件

必须利用应用标识符（AID）来选择附加生物特征应用作为预留专用文件名。应用标识符**必须**包含 ISO 根据 [ISO/IEC 7816-5] 分配的注册应用标识符，后接附加生物特征应用的专有应用标识符扩展 (PIX)：

- 注册应用标识符是‘A0 00 00 02 47’;
- 附加生物特征应用**必须**使用专有应用标识符扩展 = ‘20 03’；和
- 附加生物特征应用的完整应用标识符是‘A0 00 00 02 47 20 03’。

如果有效授权未授予对逻辑数据结构 2 应用中任何数据的访问权限，则 IC **必须**拒绝选择此应用。

5.3.2　EF.Certificates（强制性的）

附加生物特征的签名者证书存储在应用专用文件内的 EF.Certificates 中，具有线性结构，记录大小可变。这些证书旨在供 查验系统 用于进一步离线验证 EF.Biometrics 中的数字签名。

表 91.　EF.Certificates

文件名	EF.Certificates
文件标识	‘011A’
短基本文件标识符	‘1A’
选择/FMM访问	PACE+TA［附加生物特征授权字节1b1位（见表98）］
读记录/搜索记录访问	PACE+TA［附加生物特征授权字节1b1位（见表98）］
附加记录访问	PACE+TA［附加生物特征授权字节1b2位（见表98）］
写/更新记录访问	永不
擦除记录访问	永不
文件结构	线性结构，记录大小可变
大小	可变

证书记录包含单个附加生物特征签名者 X.509 证书数据对象。一个证书记录**可以**被一个或多个附加生物特征基本文件编号。

附加生物特征应用中的证书记录的结构与表 83 所规定的旅行记录应用中的证书记录结构相同。

使用 APPEND RECORD 命令将证书记录写入附加生物特征应用专用文件下的 EF.Certificates。可以使用 READ RECORD 命令从 EF.Certificates 读取证书记录。**不得**更新或删除证书记录。附加生物特征应用专用文件下的 EF.Certificates 中的最大记录数**必须**是 64。

5.3.3 EF.Biometrics

根据[ISO/IEC 7816-4]，附加生物特征**必须**存储在基本文件中的附加生物特征应用下，并具有透明结构。

每项附加生物特征的基本文件**可以**使用附加生物特征基本文件标识符，链接到签证记录应用（或其他基本文件和应用）中的 EF.VisaRecords 的一个或多个记录。

表 92. EF.Biometrics1 直到 EF.Biometrics64

文件名	EF.Biometrics1直到EF.Biometrics64
文件标识	‘0201’直到‘0240’
短基本文件标识符	不适用
在停用状态下选择/FMM/读访问	PACE+TA（根据表 98字节2至17的 b2位、b4位、b6位、b8位，AdditionalBiometrics授权）
在停用状态下写访问	PACE+TA（根据表98字节2至17的b2位、b4位、b6位、b8位，AdditionalBiometrics授权）
在停用状态下激活访问	PACE+TA（根据表98字节2至17的b2位、b4位、b6位、b8位，AdditionalBiometrics授权）
在激活状态下选择/FMM/读访问	PACE+TA（根据表98字节2至17的b1位、b3位、b5位、b7位，AdditionalBiometrics授权）
在激活状态下写访问	永不
在激活状态下激活访问	永不
擦除访问	永不
文件结构	透明结构
大小	可变

每个附加生物特征基本文件**必须**包含一个 BER-TLV 数据对象 DO'7F2E'，封装三个数据对象：生物特征数据 DO'5F2E'，后接真实性标记（签名）DO'5F37'和 DO'5F38'，其中包含对 EF.Certificates 中附加生物特征签名者证书的编号，如下表所示。

DO’5F2E’的内容由附加生物特征发行人决定，不在本规范范围内。

附加生物特征基本文件的创建机制不在本规范范围内。发行人**应该**预先创建一些附加的生物特征基本文件。

注：下表中指定的行业间标志用于逻辑数据结构环境，因此不需要共存标志分配方案。

表 93.　EF.Biometrics 格式

标志	标志	内容	强制性的/选择性的/有条件的	格式	示例
‘7F2E’		生物特征数据模板	M		‘7F’ ‘2E’ Len {DO’5F2E’ || DO’5F37’ || DO’5F38’}
	‘5F2E’	附加生物特征数据	M	V, B	‘5F’ ‘2E’ Len {生物特征数据}
	‘5F37’	真实性标记（签名）	M	V (140), B	‘5F’ ‘37’ Len {签名}
	‘5F38’	证书储备中的附加生物特征签名者证书编号（记录号）	M	F (1) B	‘01’ …’40’

注：B=二进制数据，F = 固定长度域，Var = 可变长度域。

基本文件中数据对象的顺序是固定的。

每个附加生物特征的基本文件**必须**包含一个通过 DO'5F2E'计算的数字签名（真实性标记），包括标志和长度。签名由附加生物特征签名者生成。

核实附加生物特征签名所需的附加生物特征签名者证书存储在一个附加生物特征应用专用文件下的单独 EF.Certificates 储备中。

每个附加生物特征的基本文件**必须**使用 UPDATE BINARY 命令编写。

附加生物特征的基本文件不得更改（更新）或擦除。附加生物特征基本文件的最大数量为 64。

表 94 列出了所有可能的附加生物特征基本文件名称、标识符和短标识符。

表 94. EF.Biometrics 标识符

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

5.4　逻辑数据结构 2 应用文件访问条件（有条件的）

5.4.1　作用与默认授权级别（强制性的）

每个 CV 证书都包含一个证书持有者授权模板（CHAT），用于标识证书持有者的作用（查验系统、DV、CVCA）并包含对所需逻辑数据结构 2 电子机读旅行证件应用的访问权（出于传统原因或国家其他用途）。

证书持有者授权模板包含两个对象的序列：

a) 规定终端类型和模板格式的对象标识符 [TR-03110]:

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

b) 根据下表包含证书持有者的位编码作用和只读访问权的自定义数据对象（标志 '53'）：

表 95.　证书持有者授权模板默认授权

	描述	字节 1							
		b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**
Role	CVCA	1	1						
	DV（国内）	1	0						
	DV（国外）	0	1						
	查验系统	0	0						
读取权限	预留								
	预留								
	预留								
	预留								
	DG4（虹膜）							1	
	DG3（手指）								1

注：逻辑数据结构 2 电子机读旅行证件**必须**忽略证书持有者授权中的预留位的值。

5.4.2　应用授权级别（强制性的）

每个逻辑数据结构2应用的证书持有者授权都编码在CV证书扩展当中（每项应用都有一个扩展）。证书扩展是一个自定义模板（标志“73”），包括两个数据对象：一个用于特定应用的授权对象标识符（标志“06”），和一个包含证书持有人对指定应用的位编码访问权限的自定义数据对象（标志“53”）。

为确定证书持有人的有效授权，逻辑数据结构2电子机读旅行证件芯片对查验系统证书和编号的DV和CVCA证书的证书扩展中包含的访问权限进行逐位布尔“和”计算。

对于旅行记录应用，授权对象标识符和访问权限编码为：

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

表 96. 旅行记录应用授权

	描述	字节 1							
		b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**
访问权	预留								
	预留								
	预留								
	预留								
	附加 EF.Certificates					1			
	读/搜索/选择/FMM EF.Certificates						1		
	附加 EF.EntryRecords/ExitRecords							1	
	读/搜索/选择/FMM EF.EntryRecords/ExitRecords								1

对于签证记录应用，授权对象标识符和访问权编码是：

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

表 97. 签证记录应用授权

	描述	字节 1							
		b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**
访问权	预留								
	预留								
	预留								
	预留								
	附加EF.Certificates					1			
	读/搜索/选择/FMM EF.Certificates						1		
	附加 EF.VisaRecords							1	
	读/搜索/选择/FMM EF.VisaRecords								1

对于附加生物特征应用，授权对象标识符和访问权编码为：

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

表 98.　附加生物特征应用授权

	描述	基本文件标识符	授权							
			b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**
字节1	预留									
	预留									
	预留									
	预留									
	预留									
	预留									
	附加EF.Certificates	‘011A’							1	
	选择/FMM/读/搜索EF.Certificates	‘011A’								1
字节 2	在停用状态下选择/FMM/写/激活/读 EF.Biometrics1	‘0201’	1							
	在激活状态下选择/FMM/读EF.Biometrics1	‘0201’		1						
	在停用状态下选择/FMM/写/激活/读EF.Biometrics2	‘0202’			1					
	在激活状态下选择/FMM/读EF.Biometrics2	‘0202’				1				
	在停用状态下选择t/FMM/写/激活/读EF.Biometrics3	‘0203’					1			
	在激活状态下选择/FMM/读 EF.Biometrics3	‘0203’						1		
	在停用状态下选择/FMM/写/激活/读EF.Biometrics4	‘0204’							1	
	在激活状态下选择/FMM/读EF.Biometrics4	‘0204’								1
…										
Byte 17	在停用状态下选择/FMM/写/激活/读EF.Biometrics61	‘023D’	1							
	在激活状态下选择/FMM/读EF.Biometrics61	‘023D’		1						
	在停用状态下选择/FMM/写/激活/读EF.Biometrics62	‘023E’			1					
	在激活状态下选择/FMM/读EF.Biometrics62	‘023E’				1				
	在停用状态下选择/FMM/写/激活/读EF.Biometrics63	‘023F’					1			
	在激活状态下选择/FMM/读EF.Biometrics63	‘023F’						1		
	在停用状态下选择/FMM/写/激活/读EF.Biometrics64	‘0240’							1	
	在激活状态下选择/FMM/读EF.Biometrics64	‘0240’								1

注 1：逻辑数据结构 2 电子机读旅行证件**必须**忽略证书持有人授权中预留的位的值。

注 2：如果签发国或机构只有附加生物特征的读取授权，则签发国或签发机构**不得**向查验系统签发具有写/激活授权的终端证书。

6. 对象标识符

6.1 逻辑数据结构 1 和逻辑数据结构 2 应用对象标识符摘要

表 99. 逻辑数据结构 1.7、逻辑数据结构 1.8 和逻辑数据结构 2 对象标识符

对象标识符	值	说明
id-icao	joint-iso-itu-t(2) international-organizations(23) icao(136)	国际民航组织对象标识符
id-icao-mrtd	id-icao 1	电子机读旅行证件对象标识符
id-icao-mrtd-security	id-icao-mrtd 1	
id-icao-ldsSecurityObject	id-icao-mrtd-security 1	逻辑数据结构安保对象
id-icao-mrtd-security-cscaMasterList	id-icao-mrtd-security 2	国家签署证书当局主列表
id-icao-mrtd-security-cscaMasterListSigningKey	id-icao-mrtd-security 3	
id-icao-mrtd-security-documentTypeList	id-icao-mrtd-security 4	证件类型列表
id-icao-mrtd-security-aaProtocolObject	id-icao-mrtd-security 5	激活授权协议
id-icao-mrtd-security-extensions	id-icao-mrtd-security 6	国家签署证书当局更名
id-icao-mrtd-security-extensions-nameChange	id-icao-mrtd-security-extensions 1	
id-icao-mrtd-security-extensions-documentTypeList	id-icao-mrtd-security-extensions 2	证件签名照者 证件类型
id-icao-mrtd-security-DeviationList	id-icao-mrtd-security 7	缺陷清单数据库对象标识符
id-icao-mrtd-security-DeviationListSigningKey	id-icao-mrtd-security 8	
id-icao-lds2	id-icao-mrtd-security 9	逻辑数据结构 2 对象标识符
id-icao-lds2-travelRecords	id-icao-lds2 1	旅行记录应用数据库对象标识符
id-icao-lds2-travelRecords-application	id-icao-lds2-travelRecords 1	旅行记录 AID
id-icao-lds2-travelRecords-access	id-icao-lds2-travelRecords 3	授权证扩展
id-icao-lds2-visaRecords	id-icao-lds2 2	签证记录应用数据库对象标识符
id-icao-lds2-visaRecords-application	id-icao-lds2-visaRecords 1	签证记录 AID
id-icao-lds2-visaRecords-access	id-icao-lds2-visaRecords 3	授权证扩展
id-icao-lds2-additionalBiometrics	id-icao-lds2 3	附加的生物特征数据库对象标识符
id-icao-lds2-additionalBiometrics-application	id-icao-lds2-additionalBiometrics 1	附加的生物特征 AID
id-icao-lds2-additionalBiometrics-access	id-icao-lds2-additionalBiometrics 3	授权证扩展
id-icao-lds2Signer	id-icao-lds2 8	逻辑数据结构 2 签名者对象标识符
id-icao-tsSigner	id-icao-lds2Signer 1	逻辑数据结构 2 旅行印章签名者证书
id-icao-vSigner	id-icao-lds2Signer 2	逻辑数据结构 2 签证签名者证书
id-icao-bSigner	id-icao-lds2Signer 3	逻辑数据结构 2 生物特征签名者证书
id-icao-spoc	id-icao-mrtd-security 10	SPOC 对象标识符
id-icao-spocClient	id-icao-spoc 1	客户
id-icao-spocServer	id-icao-spoc 2	服务器

7. ASN.1 规范

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

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

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

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

逻辑数据结构 **2** 旅行记录应用对象标识符
id-icao-lds2-travelRecords OBJECT IDENTIFIER ::= {id-icao-lds2 1}
id-icao-lds2-travelRecords-application OBJECT IDENTIFIER ::= {id-icao-lds2-travelRecords 1}
id-icao-lds2-travelRecords-access OBJECT IDENTIFIER ::= {id-icao-lds2-travelRecords 3}

逻辑数据结构 **2** 签证记录应用对象标识符
id-icao-lds2-visaRecords OBJECT IDENTIFIER ::= {id-icao-lds2 2}
id-icao-lds2-visaRecords-application OBJECT IDENTIFIER ::= {id-icao-lds2-visaRecords 1}
id-icao-lds2-visaRecords-access OBJECT IDENTIFIER ::= {id-icao-lds2-visaRecords 3}

逻辑数据结构 **2** 附加的生物特征应用对象标识符
id-icao-lds2-additionalBiometrics OBJECT IDENTIFIER ::= {id-icao-lds2 3}
id-icao-lds2-additionalBiometrics-application OBJECT IDENTIFIER ::= {id-icao-lds2-additionalBiometrics 1}
id-icao-lds2-additionalBiometrics-access OBJECT IDENTIFIER ::= {id-icao-lds2-additionalBiometrics 3}

id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-lds2 8}
id-icao-tsSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 1}
id-icao-vSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 2}
id-icao-bSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 3}

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

8. 参考文献（规范性）

ISO/IEC 14443-1	ISO/IEC 14443-1:2016，识别卡 — 非接触式集成电路卡 — 感应卡 — 第 1 部分：物理特性
ISO/IEC 14443-2	ISO/IEC 14443-2:2016，识别卡 — 非接触式集成电路卡 — 感应卡 — 第 2 部分：射频功率和信号接口
ISO/IEC 14443- 3	ISO/IEC 14443-3:2016，识别卡 — 非接触式集成电路卡 — 感应卡 — 第 3 部分：初始化和防冲突
ISO/IEC 14443-4	ISO/IEC 14443-4:2016，识别卡 — 非接触式集成电路卡 — 感应卡 — 第 4 部分：传输协议
ISO/IEC 10373-6	ISO/IEC 10373-6: 2016, 识别卡 — 测试方法 — 第 6 部分：感应卡
ISO/IEC 18745-2	ISO/IEC 18745-2:2016 信息技术 — 机读旅行证件（MRTD）和相关设备的测试方法 — 第 2 部分：无接触界面的测试方法
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、安保及交换命令
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: 2016，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: 2017，识别卡 — 集成电路卡 — 第 11 部分：通过生物特征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 19794-6	ISO/IEC 19794-6:2011, 信息技术 — 生物特征数据交换格式 — 第 6 部分：虹膜图像数据

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
ISO/IEC 19795-6	ISO/IEC 19795-6:2012, 信息技术 — 生物特征性能测试和报告 — 第 6 部分：运行评估的检测方法
ISO/IEC 39794-4	ISO/IEC 39794-4:2019, 信息技术 — 可扩展的生物特征数据交换格式 — 第 4 部分：指纹图像数据
ISO/IEC 39794-5	ISO/IEC 39794-5:2019, 信息技术 — 可扩展的生物特征数据交换格式 — 第 5 部分：面部图像数据
ISO/IEC 39794-6	ISO/IEC 39794-6:2021, 信息技术 — 可扩展的生物特征数据交换格式 — 第 6 部分：虹膜图像数据

— — — — — — — —

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** 型逻辑数据结构 1 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** 型逻辑数据结构 1 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，其生物特征数据组块长度为 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’* ‘20020401200703 31’
    - **‘86’** *‘04’* ‘00010001’
    - **‘87’** *‘02’* ‘0101’
    - **‘88’** *‘02’* ‘0008’
  - **‘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.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

— — — — — — — —

第 10 部分附录 B

电子机读护照中的非接触式集成电路
（资料性）

B.1 电子机读旅行证件的天线大小和等级

天线大小由签发国自行决定。除天线大小例外， 逻辑数据结构 1 及逻辑数据结构 2 电子机读旅行证件须满足[ISO/IEC 18745-2]中规定的适用第 1 类规范的所有测试。

建议电子机读旅行证件也符合第 1 类规范。

对于集成电路没有强制性位置，可以放在任意位置。非接触式天线的位置由签发国自行决定，只要它位于以下位置之一：

数据页 — 集成电路和天线位于构成内部页面的数据页结构内部，
证件本中心 — 将集成电路及其天线放在本子的中心页之间，
封面 — 放在封面的结构或构造内，
单独的装订页 — 将集成电路及其天线合并到一个单独的页面中，此页面可以是 ID3 尺寸塑料卡的形式，在制造过程中装订入证件本中；或
封底 — 放置在封底的结构或构造内。

B.2 启动和轮询

被带入根据[ISO/IEC 18745-2]测量为 1.5 A/m 的交变磁场的电子机读旅行证件在放入 10ms 的未调交变磁场后，须对任何适合其类型的请求/唤醒（REQ/WUP）做出响应。**建议**在放入 5 ms 的未调交变磁场后，能够对任何适合其类型的请求/唤醒（REQ/WUP）做出响应。

B.3 防冲突和类型

电子机读旅行证件可以声明符合[ISO/IEC 14443-2]中定义的 A 型或 B 型。除非已经由电子机读旅行证件相关查验系统重新设置，否则不得更改其类型。

B.4 强制性比特率

电子机读旅行证件须强制性至少提供以下比特率，如[ISO/IEC 14443-2]所界定：106 kbit/s 和 424 kbit/s 电子机读旅行证件和电子机读旅行证件相关查验系统之间双向。

下列比特率是选择性的：212 kbit/s 的比特率、从 848 kbit/s 到 6.78 Mbit/s 双向所有比特率、和从电子机读旅行证件相关查验系统到电子机读旅行证件从 10.17 Mbit/s 到 27.12 Mbit/s 的比特率，如[ISO/IEC 14443-2]所界定。

B.5 电磁干扰（EMD）

支持电磁干扰为非强制性。

注：电磁干扰功能增强了电子机读旅行证件和电子机读旅行证件相关查验系统之间非接触式通信对电子机读旅行证件产生的电磁干扰的抗干扰能力。电子机读旅行证件在执行命令期间的动态电流消耗可能导致对磁场的任意负载调制效应（此效应可能不是纯电阻性的）。在某些情况下，电子机读旅行证件相关查验系统可能会将电磁干扰错误理解为电子机读旅行证件发送的数据，从而可能会对正确接收电子机读旅行证件的响应产生负面影响。

B.6 （选择性）支持附加参数交换

电子机读旅行证件可支持[ISO / IEC 14443-4]中定义的附加参数交换，以便能兼容高于 106 kbit / s 的比特率。它也可以使用同样的附加参数来兼容带有纠错的帧，如[ISO / IEC 14443-4]所界定。

B.7 屏蔽

建议不要屏蔽电子机读旅行证件的任何页面。

B.8 （建议性）唯一标识符（UID）和伪唯一接触式集成电路卡标识符（PUPI）

电子机读旅行证件可以提供随机或固定的 UID/PUPI，如[ISO/IEC 14443-3]所界定。

建议使用随机 UID/PUPI 来加强电子机读旅行证件持有人的隐私并减少跟踪的可能性。

B.9 （建议性）共振频率范围

对电子机读旅行证件申请人的共振频率没有要求，但可以将其共振频率默认限制在一定范围内以增加互操作性。

B.10 （建议性）帧大小

根据[ISO/IEC 14443]，电子机读旅行证件可以支持不超过 4 千字节的帧。但是，建议支持至少 1 千字节大小的帧。如果支持超过 1 千字节的帧，则建议使用带有纠错的帧，如[ISO/IEC 14443-4]中所界定。

注：字节数较高的帧会显著减少电子机读旅行证件应用的总处理时间。

B.11　（建议性）帧等待时间整数（FWI）和等待时间扩展 S 组块请求[S(WTX)]

建议将电子机读旅行证件帧等待时间整数值设置为小于或等于 11，以提高性能。建议对于每个需要附加时间的特定命令使用 S（WTX）命令来延长帧等待时间,所使用的 S（WTX）命令其 WTXM 不大于 10。

如果电子机读旅行证件发送多个 S（WTX）请求，则建议当前 I-Block 的总处理时间不超过 5 秒。

注：这里推荐的较低 FWI 值会大大减少传输错误的时间损失，而 S（WTX）是在必要情况下提供更多时间的理想方法。

— — — — — — — —

第 10 部分附录 C

查验系统
（资料性）

C.1 操作量和测试位置

电子机读旅行证件相关查验系统须按照[ISO/IEC 18745-2]中规定的查验系统类型之一完成操作量。操作量是满足本技术报告所有要求的量。

注：每个查验系统类型的测试位置在[ISO/IEC 18745-2]中就电子机读旅行证件相关检测系统的（设备）0 mm 表面做了进一步规定。

C.2 特定的波形和射频要求

用于通信的交变磁场的波形须完全符合[ISO/IEC 14443-2]。一般而言，除场强外，对于基本标准不得有例外或不同。

对于 1 型、2 型和 3 型电子机读旅行证件相关查验系统，建议对于第 1 类在所有位置的场强至少为 2A/m。对于 M 型电子机读旅行证件相关查验系统，对于第一类在所有位置的场强须至少为 1.5A/ m。

注：电子旅行证件最好也能与其他非接触式查验系统和移动设备（例如使用 1.5A/m 的 NFC 智能手机）通信。

C.3 轮询序列和电子机读旅行证件检测时间

电子机读旅行证件相关检测系统的轮询序列须在任何 A 类请求/A 类唤醒（REQA/WUPA）或 B 类请求/B 类唤醒(REQB/WUPB)之前提供 10 ms 的未调制载波。

为加快检测和处理，电子机读旅行证件查验系统：

- 须对 A 型和 B 型以两个类型相等的请求次数进行轮询
- 对于1,2和3型查验系统，应在同一类型的请求/唤醒（REQ/WUP）之间发生一次射频重置
- 对于根据[ISO/IEC 18745-2]最小强制型操作量中存在的位于任何位置的电子机读旅行证件，须保证在150ms 内对于 A 型和 B 型均至少有一个轮询命令。

电子机读旅行证件查验系统可以在 13.56 MHz 载波上轮询任何其他调制类型的非接触式产品，前提是满足上述所有要求。

注：要求有 10 ms 的未调制载波以检测域中的所有电子机读旅行证件，这是基于以前的规范。

C.4 强制性比特率

电子机读旅行证件相关查验系统须强制性提供以下：106 kbit/s 和 424 kbit/s 从电子机读旅行证件到电子机读旅行证件相关查验系统和反之双向。

以下比特率为选择性：212 kbit/s 比特率、所有从 848 kbit/s 到 6.78 Mbit/s 双向的比特率、和自电子机读旅行证件相关查验系统到电子机读旅行证件的 10.17 Mbit/s 到 27.12 Mbit/s 的比特率，如[ISO/IEC 14443-2]中所界定。

C.5 电磁干扰（EMD）

支持电磁干扰为非强制性。

注：电磁干扰功能增强了电子机读旅行证件和电子机读旅行证件相关查验系统之间非接触式通信对电子机读旅行证件产生的电磁干扰的抗干扰能力。电子机读旅行证件在执行命令期间的动态电流消耗可能导致对磁场的任意负载调制效应（此效应可能不是纯电阻性的）。在某些情况下，电子机读旅行证件相关查验系统可能会将电磁干扰错误理解为电子机读旅行证件发送的数据，这可能会对正确接收电子机读旅行证件的响应产生负面影响。

C.6 支持的天线类别

1 型和 2 型电子机读旅行证件相关查验系统须至少支持操作量中的第 1 类电子机读旅行证件。

在 ISO/IEC 14443 中，第 2 类和第 3 类是强制性的，但是对于电子机读旅行证件查验系统是选择性的。

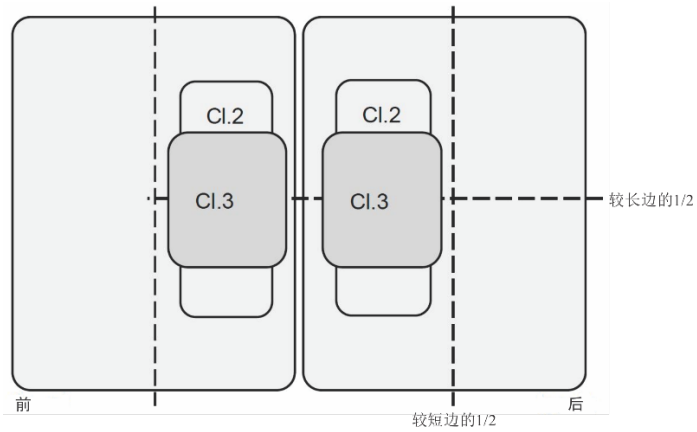

图 C-1：在每个 ID-3 表面上第 2 类和第 3 类天线须由 1 型和 2 型电子机读旅行证件相关查验系统读取的强制性位置。

C.7　（选择性）帧大小和纠错

电子机读旅行证件相关查验系统可选择支持不超过 4 千字节的所有帧大小，如[ISO/IEC 14443-3]中所界定。建议对于所支持的所有大于 1 千字节的帧大小使用带有纠错的帧，如[ISO / IEC 14443-3]中所界定。

注：对于 M 型电子机读旅行证件相关查验系统，目前没有设想高于 256 字节的帧大小。

C.8　（选择性）支持附加类型

所有类型的电子机读旅行证件相关查验系统可额外支持第 4 类、第 5 类和第 6 类，以便与例如与电子机读旅行证件相关查验系统天线线圈的耦合较少的移动设备可互操作。

C.9　（建议性）工作温度

建议电子机读旅行证件相关查验系统在-10°至 50°C 的温度下工作。

C.10　（建议性）支持多个电子机读旅行证件和其他卡或对象或多个主机

强烈建议将电子机读旅行证件相关查验系统设计为可处理一个以上电子机读旅行证件，或一个电子机读旅行证件和符合[ISO/IEC 14443]的任何其他卡或对象。

除其他外，可应用以下规则之一或组合：

- 运用[ISO/IEC 14443-3]中定义的完整防冲突算法；
- 检查是否支持[ISO/IEC 14443-4]并弃用所有不支持的卡；
- 检查是否有电子机读旅行证件应用；和
- 使用卡标识符（CID）和节点地址（NAD）。

注：NAD 也可用于具有多个主机的移动设备。

C.11　（建议性）帧大小

根据[ISO/IEC 14443-3]，电子机读旅行证件相关查验系统可支持不超过 4 千字节的帧大小。但是，建议支持至少 1 千字节的帧。若支持等于或大于 1 千字节的帧，则建议使用带有纠错的帧，如[ISO/IEC 14443-4]中所界定。

建议对应用层面有效载荷进行任何分解，应采用所支持的最大帧的有效长度（最后一帧除外），分解至最小的帧数量。

C.12 （建议性）错误修复

在传输错误或电子机读旅行证件无响应之后，建议电子机读旅行证件相关查验系统根据[ISO/IEC 14443-4]的查验系统规则 4，发送第二个包含否定确认的 R 组块（R（NAK））。

C.13 （建议性）发现错误和修复机制

当使用可选的比特率以及高于 256 字节的可选帧大小时，如果传输错误的数量高于通常的数量，则建议降低比特率和有效帧大小。

— — — — — — — —

第 10 部分附录 D

证件安保对象 EF.SOD 版本 V0 LDS v1.7（传统）（资料性的）

逻辑数据结构 V1.7 的证件安保对象 V0 不包含逻辑数据结构和 Unicode 版本信息：

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

D.1 SO_D V0 的 SIGNEDDATA 类型

证件安保对象根据[RFC 3369]的规定实施为 SignedData 类型。所有安保对象均**必须**以唯一编码规则（DER）格式编制，以保持其中签名的完整性。

注 1：m=强制性的 — 该域**必须**填写。

注 2：x=不使用 — 该域**不应**被填充。

注 3：o=选择性的 — 该域**可以**填写。

注 4：c=选择 — 该域内容是从备选内容中选出的。

表 D-1 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 — 安保 — 逻辑数据结构安保对象
eContent	m	逻辑数据结构安保对象的编码内容。
Certificates	o	各国可选择包括证件签名者证书（C_{DS}），它可以用来核实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	制作国家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，除非是为了核实签名值。
signatureAlgorithm	m	该算法的算法标识符用于编制签名值和任何相关参数。
Signature	m	签名生成过程的结果。
unsignedAttrs	o	制作国家可能希望使用该域，但不建议使用，接收国可以选择予以忽略。

D.2 SO_D V0 的 ASN.1 配置文件逻辑数据结构证件安保对象

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

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
IMPORTS

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

-- Constants

ub-DataGroups INTEGER ::= 16

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

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {v0(0)}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

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

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

注 1：dataGroupHashValue（数据组哈希值）的域，包含由 dataGroupNumber（数据组号）规定的通过数据组基本文件完整内容计算的散列值。

注 2：DigestAlgorithmIdentifiers（摘要算法标识符）**必须**省略 NULL 参数，而如果没有填写参数的话，即使在按照 RFC 5754 使用 SHA2 算法时，SignatureAlgorithmIdentifier（签名算法标识符）（如 RFC 3447 的定义）必须包括 NULL 作为参数。检查系统必须接受两个条件的 DigestAlgorithmIdentifiers（摘要算法标识符），即：没有参数或有 NULL 参数。

— — — — — — — —

第 10 部分附录 E

文件结构摘要（资料性）

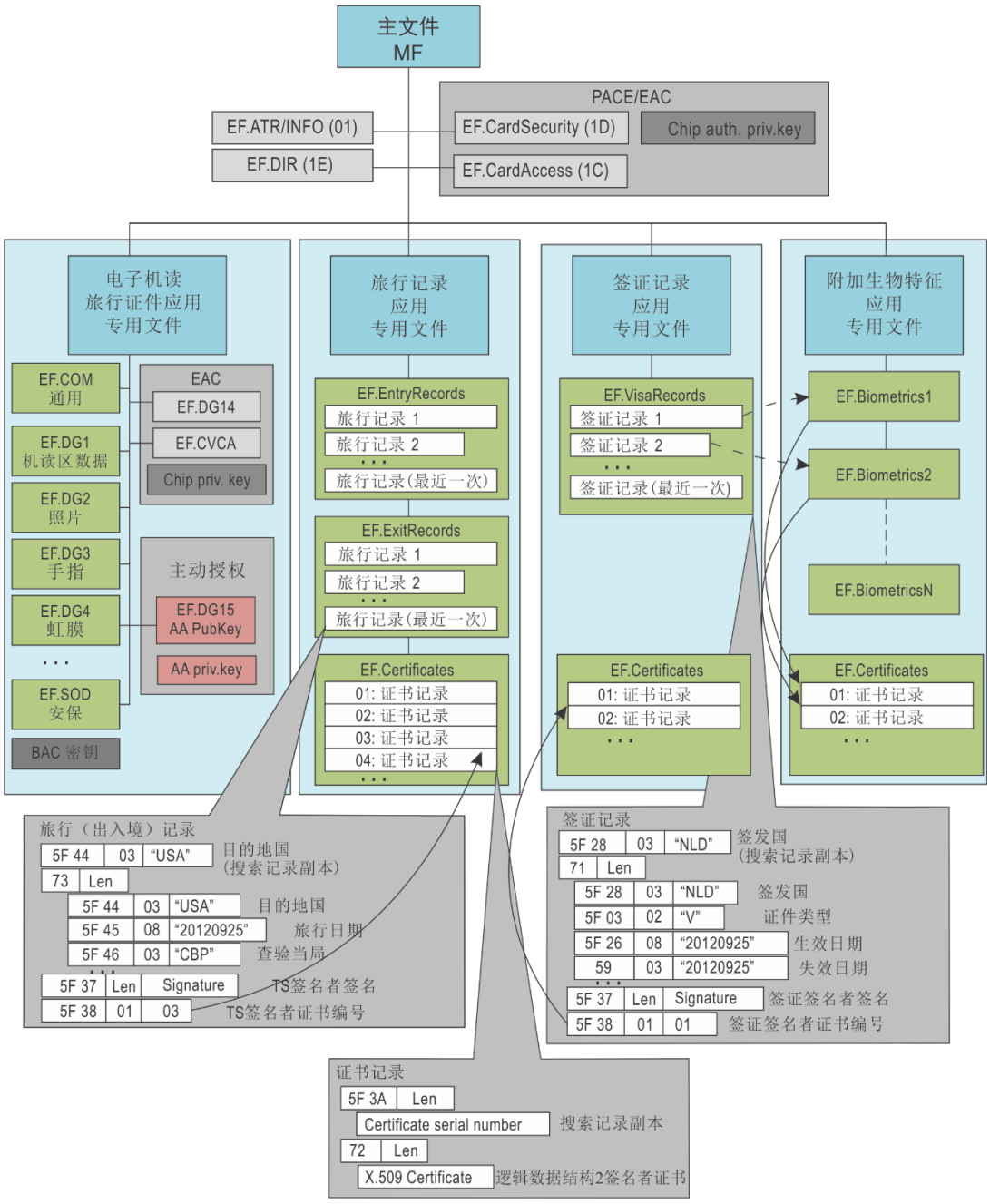

图 E-1.　文件结构摘要

第 10 部分附录 F

逻辑数据结构授权摘要
（资料性）

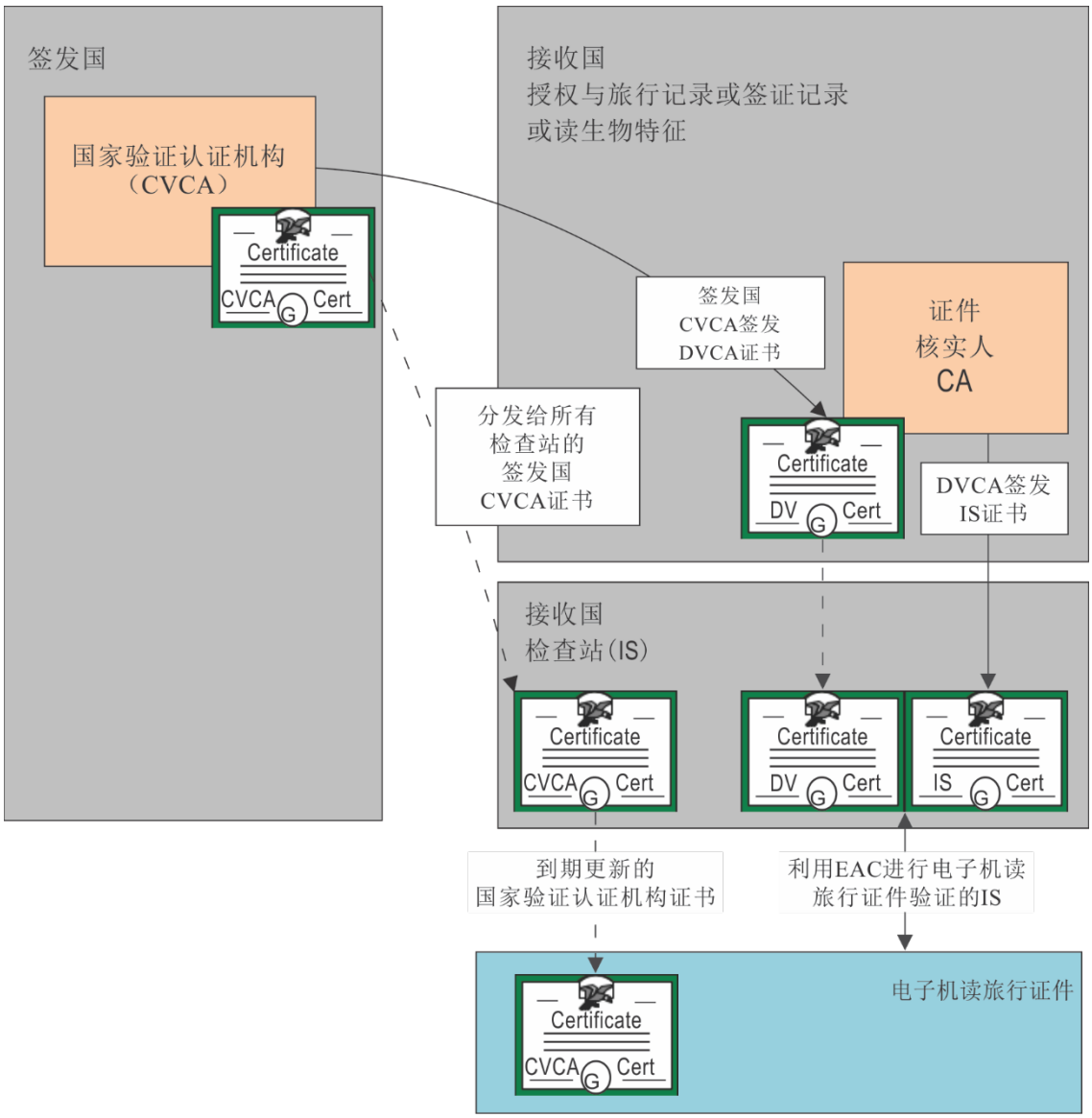

图 F-1.　逻辑数据结构授权摘要

第 10 部分附录 G

逻辑数据结构数字签名摘要
（资料性）

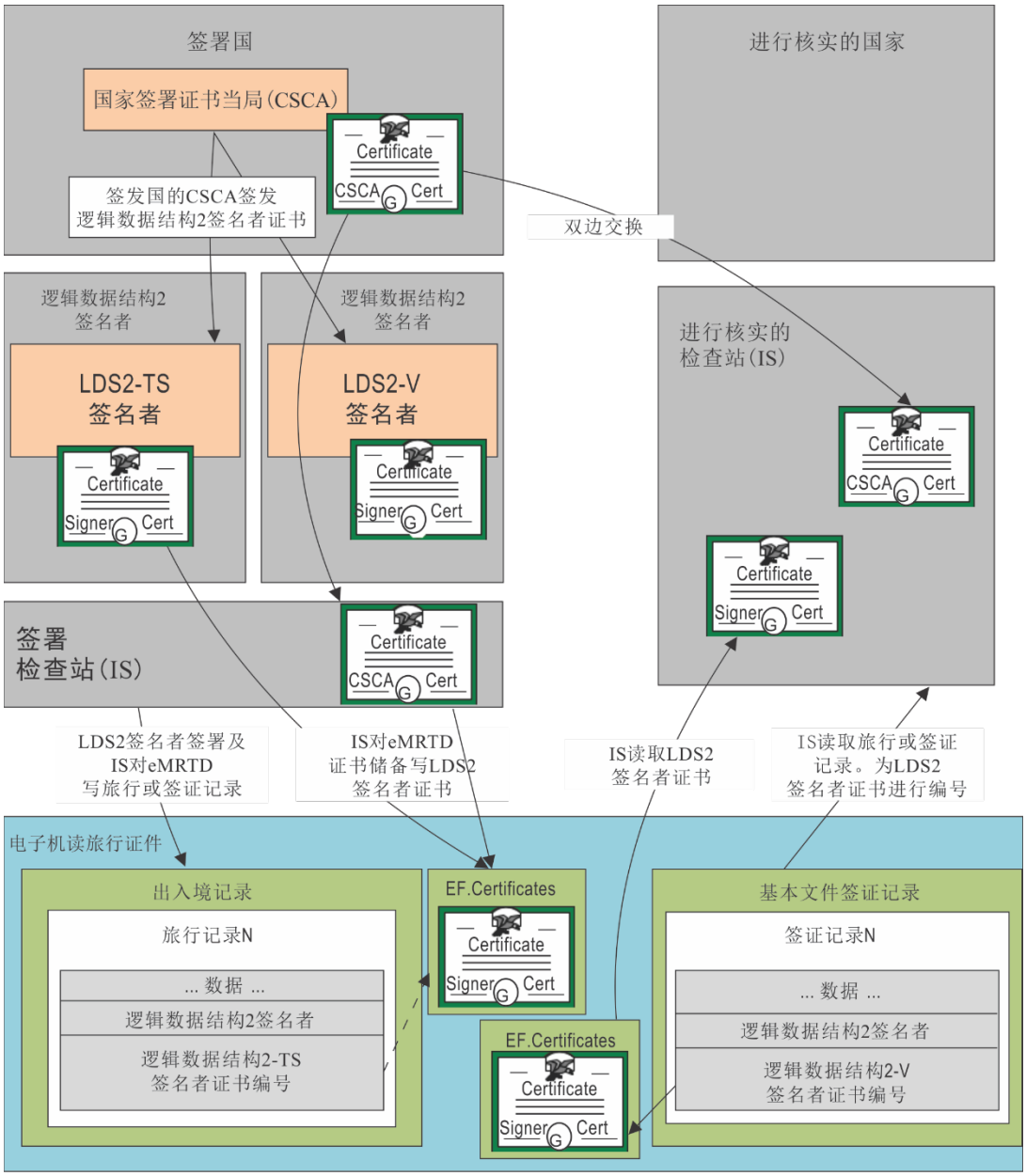

图 G-1.　逻辑数据结构数字签名

— — — — — — — —

第 10 部分附录 H

读取旅行记录的示例
（资料性）

H.1　FMM 命令检索入境记录号

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

CLA：　专有类/无可靠消息传递
INS：　FMM
P1：　‘01’ — 命令数据域的基本文件标识符
P2：　‘04’ — 返回记录基本文件的现有记录编号
LC：　‘04’
DATA：　包含入境记录基本文件标识符‘0101’的 DO’51’
LE：　‘00’（短 LE）

响应：表示基本文件所载记录号的 FILE AND MEMORY MANAGEMENT DO。

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

响应数据中的 DO 包含可用于下一个 READ RECORD 命令（P1）的最后一个记录号。

例如：最后一个记录号‘00’表示这一文件中没有记录，响应‘FD’表示记录数是 253（最大记录数为 254）。

H.2　从检索列表检索最后一条旅行记录的 READ RECORD 命令

以下命令可用于使用 FMM 命令返回的记录号检索单个记录：

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

CLA： 行业间类/无可靠信息传递
INS： READ RECORD(S)
P1： 来自此前命令响应的记录号
P2： P1 中的记录号/读记录 P1
LE： ‘00 00 00’（扩展的 LE），读完整记录

响应：记录号是 253（‘FD’）。

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

H.3 从检索列表检索最后两项旅行记录的 READ RECORD 命令

以下命令可用于从 FMM 命令返回的列表中检索两项（或更多）记录。在一次应用协议数据单元（APDU）交换中读取多项记录可提高效绩。单项命令可以检索的记录号，可根据 EF.ATR/INFO 中的扩展长度信息和旅行记录的最大长度来确定。

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

CLA： 行业间类/无可靠信息传递
INS： READ RECORD(S)
P1： 来自 FMM 响应的递减记录号（253 - 1 = 252 = ‘FC’）
P2： P1 中的记录号/读 P1 的所有记录直到最后一项记录
LE： ‘00 00 00’（扩展的 LE），读完整记录

响应：返回最后两项记录 252（‘FC’）和 253（‘FD’）。

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

— — — — — — — —

第 10 部分附录 I

国家搜索记录示例
（资料性）

I.1 按目的地国搜索旅行记录的 SEARCH RECORD 命令

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

CLA： 行业间类/无可靠信息传递

INS： SEARCH RECORD(S)

P1： 记录号 = ‘00’

P2： 通过多个基本文件进行搜索

LC： 命令数据域的长度

数据： DO’7F76’ — 记录处理 DO

DO’51’ — 文件编号 DO（EF.EntryRecords 短标识符‘01’）

DO’A1’ — 搜索设置模板

DO’80’ — 搜索设置参数：‘00’（搜索所有记录）

DO’B0’ — 搜索窗口模板

DO’02’ — 偏移：‘03’

DO’02’ — 字节号：‘03’

DO’A3’ — 搜索串模板

DO’B1’ — 搜索串DO

DO’81’ — 搜索串（国家代码）：xx xx xx

Le: ‘00’（短Le）

响应：DO’7F76’ — 记录处理DO

DO’51’ — EF.EntryRecords 短标识符‘01’

包含匹配记录号的一个或多个DO’02’

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

— — — — — — — — —

第 10 部分附录 J

写旅行记录和证书的示例
（资料性）

J.1 按证书序号搜索 EF.CERTIFICATES 的 SEARCH RECORD 命令

查验系统检查 EF.Certificates 中是否存在具有所需序号的逻辑数据结构 2-TS 签名者证书。以下命令可用于搜索证书：

CLA	INS	P1	P2	Lc	数据	Le
'00'	'A2'	'00'	'F8'	Var	'7F 76' 'Len' '51 01 1A' 'A1 0B' '80 01 30' 'B0 06' '02 01 03' '02 01' {搜索串的大小} 'A3' 'Len' 'B1' 'Len' '81' 'Len' xx xx .. xx xx	'00'

CLA： 行业间类/无可靠信息传递 INS: SEARCH RECORD(S)
P1： 记录号 = '00'
P2： 通过多个基本文件进行搜索
LC： 命令数据域的长度
DATA： DO'7F76' — 记录处理 DO
DO'51' — 文件编号DO（EF.Certificates短标识符'1A'）
DO'A1' — 搜索设置模板
DO'80' — 搜索设置参数：'30'（找到记录即停止）
DO'B0' — 搜索窗口模板
DO'02' — 偏移：'03'
DO'02' — 字节号：搜索串大小
DO'A3' — 搜索串模板
DO'B1' — 搜索串DO
DO'81' — 国家代码和证书序号搜索级联：xx xx .. xx xx

Le: '00'（短Le）

响应：DO'7F76' — 记录处理 DO
DO'51' — EF.Certificates 短标识符'1A'
DO'02' — 包含匹配记录号

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

或警告代码“62 82”，如果没有匹配搜索指标的记录：

SW1-SW2
‘62 82’

如果 EF.Certificate 记录与搜索指标匹配，查验系统可以选择在 READ RECORD 命令中使用返回的记录号（‘01’）来检查证书是否正确。如果 EF.Certificate 记录与搜索指标不匹配，则查验系统使用 J.2 节中的 APPEND RECORD 命令将证书写入 EF.Certificates，最后使用 J.3 节中的 APPEND RECORD 命令写条目记录。

J.2 写证书的 APPEND RECORD 命令

查验系统将逻辑数据结构 2-TS 签名者证书写入 EF.Certificates。以下命令可用于写证书：

CLA	INS	P1	P2	Lc	数据	Le
‘00’	‘E2’	‘00’	‘D0’	‘00’ XX XX	‘5F3A’ ‘Len’ {证书序号} ‖ ‘72’ ‘Len’ {X.509 证书}”	空

CLA： 行业间类/无可靠信息传递
INS： APPEND RECORD
P1： ‘00’（任何其他值均无效）
P2： 短基本文件标识符（= ‘1A’）
LC： 记录长度（扩展的 LC）
数据： 记录数据

响应：成功或错误代码

SW1-SW2
‘90 00’

J.3　写旅行记录的 APPEND RECORD 命令

查验系统使用逻辑数据结构 2-TS 签名者证书的编号生成旅行记录，并使用以下命令将其写入 EF.EntryRecords:

CLA	INS	P1	P2	Lc	数据	Le
‘00’	‘E2’	‘00’	‘08’	‘00’ XX XX	‘5F44’ ‘Len’ {目的地国} ‖ ‘73’ ‘Len’ {入境旅行记录} ‖ ‘5F37’ ‘Len’ {签名} ‖ ‘5F38’ ‘Len’ {证书编号}	空

CLA：　行业间类/无可靠信息传递
INS：　APPEND RECORD
P1：　‘00’（任何其他值均无效）
P2：　短基本文件标识符（= ‘01’）
LC：　记录长度（扩展的 LC）
数据：　记录数据

响应：成功或错误代码

SW1-SW2
‘90 00’

—完—

ISBN 978-92-9275-542-3