Doc 9303

机读旅行证件

第 1 部分
机读护照
第 2 卷
具有生物特征识别
能力的电子护照规范

经秘书长批准并由其授权出版

第六版 —— 2006 年

国际民用航空组织

国际民航组织分别用中文、英文、阿拉伯文、法文、俄文和西班牙文出版本出版物，除订单与订购款外，所有信函都应写给秘书长。

订单应与美元汇款或下单国货币的汇款一起寄往下列地址之一。鼓励客户使用信用卡(MasterCard、Visa或American Express)，以免交货延误。有关使用信用卡或以其他方法付款的信息，见于国际民航组织出版物和视听培训教材目录的订货信息部分。

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

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

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

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

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

India. Oxford Book and Stationery Co., 57, Medha Apartments, Mayur Vihar, Phase-1, New Delhi - 110 091
Telephone: +91 11 65659897; Facsimile: +91 11 22743532

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

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

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

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

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

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

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

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

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

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

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

Spain. A.E.N.A. — Aeropuertos Españoles y Navegación Aérea, Calle Juan Ignacio Luca de Tena, 14, Planta Tercera, Despacho 3. 11,
28027 Madrid / Teléfono: +34 91 321-3148; Facsímile: +34 91 321-3157; Correo-e: sscc.ventasoaci@aena.es

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

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

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

国际民航组织出版物
和视听培训教材目录

目录每年出版一次，开列所有现行出版物和视听培训教材。目录的补编公布新的出版物和视听培训教材，以及修订、增补和再版物等。

由国际民航组织文件销售部免费提供。

Doc 9303

机读旅行证件

第 1 部分
机读护照
第 2 卷
具有生物特征识别
能力的电子护照规范

经秘书长批准并由其授权出版

第六版 —— 2006 年

国际民用航空组织

修订

各项修订都定期地在《国际民航组织月刊》和每月出版的《国际民航组织出版物和视听培训教材目录增补》中公布，本出版物持有者应进行核查。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

页码

第 I 节

绪　论

Doc 9303 号文件第 1 部分第 2 卷中所载的规范是自 1998 年以来若干年工作的结晶。这项工作前期是对生物特征以及利用生物特征增强护照和其他旅行证件身份确认能力的可能性进行系统研究，后期是为将生物特征识别纳入机读旅行证件编制技术规范。其中的大部分工作是由机读旅行证件技术咨询组 (TAG/MRTD) 下的新技术工作组 (NTWG) 完成的。

第一步是确定可用于旅行证件的“适当的生物特征”。而要做到这点，首先是要确定旅行证件的签发和查验的特殊要求，再估量每一种生物特征与这些要求的兼容性。简言之，所确定的要求是：与旅行证件的签发和更新的兼容性；与签发和查验过程中的机器辅助身份验证要求的兼容性；冗余度；全球公众对生物特征及其采集流程的认可程度；存储要求；以及性能。根据上面提到的所有这些因素进行评估，人脸获得最高的兼容等级，而指纹和虹膜并列第二。因此，人脸被推荐为主要生物特征，为保证护照查验系统的全球互用性,它被确定为强制性的，而指纹和虹膜则被推荐为次要的生物特征，由签发国自行决定是否使用。

下一步是确定一个合适的媒体将电子数据存储到证件中。选择的媒体必须为人脸图像和其他可能的生物特征信息提供足够的数据存储空间，因为由于模板及其阅读器没有一个统一的国际标准，运用模板的概念被放弃了。采用的技术必须是非私有的，在全世界的公共范围内都可获得，以利于全球互用，并且必须可用在用纸和布料做成的本式证件上。使用方便，无须将证件放入或插入读取装置中，也是一个考虑因素。非接触式集成电路 (IC) 是满足所有这些要求的技术，经过深入研究决定，在两个可选择的 ISO 标准中，应指定采用“紧耦合”型技术 (ISO/IEC 14443)。

接下来，一种用于芯片编程的标准化“逻辑数据结构”被确定下来，以确保在任何一个国家编程的芯片都能被其他国家阅读。最后，因为写入芯片的数据能被覆盖，需要一套公钥基础设施 (PKI) 方案，使芯片阅读者确信，数据是由经授权的证件签发者存储在那里的，并且没有以任何方式被篡改。因此，新技术工作组内的一个专家小组编制了用于旅行证件签发和查验的专用公钥基础设施规范。

2003 年，机读旅行证件技术咨询组正式向国际民航组织提出了一项由四个部分组成的建议：建议将以高分辨率标准照的形式存储在符合 ISO/IEC 14443 标准的非接触式集成电路 (IC) 中的人脸图像，作为全球通用的生物特征标准。同时支持将以图像形式存储的指纹和虹膜作为次要生物特征。生物特征信息，机读区数据的副本，以及各种其他可选的数据信息应该按照逻辑数据结构被存储到集成电路中，并用专门设计的公钥基础设施加以保护以防止被擅自改动。这项建议作为国际民航组织的行动计划得到接受和认可。

本卷使此项决定以正式形式确定下来，它在后面各节中提供了详细的规范。第 II 节 —— *生物特征的利用*，确定了生物特征数据的采集和使用方法以及用来存储数据的非接触式集成电路的要求。第 III 节 —— *逻辑数据结构*，阐述了数据如何存储到集成电路中。第 IV 节 —— *公/私钥基础设施*，介绍了用于保护集成电路中数据的系统和流程，并包括一项关于基本访问控制的建议以便使数据访问受到适当的限制。

第 II 节

生物特征识别技术的利用和机读护照中数据的电子存储

1. 范围

1.1 第 II 节确定的规范是 Doc 9303 号文件第 1 部分第 1 卷中提出的基本机读护照规范的补充，以供决定签发电子机读护照 (电子护照) 的国家使用。只要拥有适当的设备，接受国就可以从这种证件中读取关于机读护照本身及其持证人的大量增加的数据。这包括强制性的全球互用生物特征数据，这些数据可用来作为人脸识别系统和在自选的基础上作为指纹或虹膜识别系统的输入。规范要求全球互用生物特征数据以高分辨率图像的形式存储在高容量的非接触式集成电路 (IC) 中，机读区数据的副本也要编码后写入集成电路。这些规范也允许签发国自行决定存储选择性数据。

补编说明:

针对这一标准的 Doc 9303 号文件，国际民航组织将随时发布“Doc 9303 号文件第 1 部分补编”，补编将包含旨在对旅行证件标准问题进行澄清、补充说明或详细阐述，以及对实施过程中发现的错误加以纠正的资料。希望补编中含有的资料将使 Doc 9303 号文件及国际民航组织发布的技术报告中所载的现有指导材料更加丰富。补编将连续不断地发布。

应该始终结合最新发布的补编中提供的补充资料阅读理解 Doc 9303 号文件中的规范，最新发布的补编可在国际民航组织网站 (http://www.icao.int/mrtd) 上找到。

2. 电子护照

2.1 *与 Doc 9303 号文件第 1 部分第 1 卷的规范的符合性* 电子机读护照 (电子护照) 不但要符合本卷中所载的规范，还要在所有方面符合 Doc 9303 号文件第 1 部分第 1 卷中提出的规范。

2.2 *电子护照的有效期* 电子护照的有效期由签发国自行决定；然而，考虑到证件有限的耐久性和护照持证人的外貌随时间而变化，建议有效期不超过 10 年。各国似宜考虑采用更短的有效期，使电子护照能随着技术的发展而逐步升级。

2.3 Doc 9303 号文件第 1 部分第 2 卷把重点放在与机读护照相关的生物特征上，并为了简便使用了术语“电子护照”来表示具有生物特征识别性能的可全球互用的护照。任何不符合本卷规范的机读护照不能叫做电子护照，不得使用电子护照的标识。

3. 机读护照为电子护照的直观显示

3.1 所有的电子护照都须带有下面这种标识 (图 II-1)：

图 II-1

该标识的电子版可在国际民航组织的网站上获得。这个标识只能用在这样一种机读护照上：含有一个非接触式微芯片，数据存储容量至少为 32 kB，该芯片根据逻辑数据结构 (本卷第 III 节) 编码，数据组 1 中至少存有机读区数据，数据组 2 中至少存有本节所规定的人脸图像，所有输入数据的安全都用本卷第 IV 节所规定的数字签名加以保护。只有符合上述的这些最基本要求，才能被叫做电子护照，使用电子护照的标识。标识须显示在电子护照的封面上，可靠近封面顶端或底端。上面所显示的图像是正片，即图像中暗的部分须被印制出来或以其他方式显现出来。标识须包括在封面的烫金或其他图案中。建议将标识以一种合适的颜色也印在资料页不影响读取其他数据的地方。签发国也可以将标识印在内置非接触式集成电路的电子护照内页或封皮上，或者该国自行选定的电子护照的其他位置。

3.2　图 II-2 显示了标识在电子护照本的封皮或资料页上的建议尺寸。

下面是对应的尺寸 (英寸)：9.0 毫米 (0.35 英寸)，5.25 毫米 (0.21 英寸)，3.75 毫米 (0.15 英寸)，2.25 毫米 (0.09 英寸)，0.75 毫米 (0.03 英寸)。

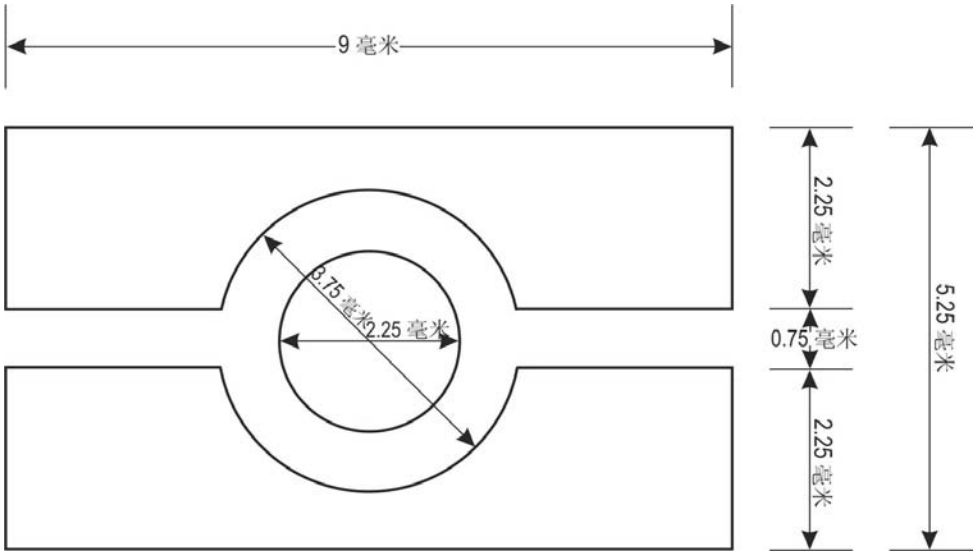


图 II-2

3.3　建议在 ID1 尺寸的电子护照卡上使用按比例缩小的 4.2×7.2 毫米 (0.17×0.28 英寸) 的尺寸。

3.4　标识可以按比例进行缩放，以便用于 (例如) 电子护照页或方向标志的背景图案中。

3.5　*关于妥善保管电子护照的警示*　建议在护照本的显眼位置添加警示，要求电子护照持证人保管好证件。建议的措辞如下：

“此护照内置敏感电子元件，为保持最佳性能，请不要将护照弯折、打孔或者暴露在高温或极为潮湿的环境中”。

另外，签发国可以在内置集成电路的页面位置上和几个相临页的相应位置上标上警告语：

“非盖章区”

4.　生物特征识别

4.1　“生物特征识别”是一个专业术语，用来描述通过对不同的生理和行为特征进行测定自动识别活体人的方法。

4.2　“生物特征模板”是对计算机软件算法所产生特征的机器编码表示法，能够通过比对 (匹配) 为单独记录的特征识别 (或者不识别) 同一个人的置信度打分。生物特征模板数据量一般较小；然而，每一个生物特征系统的制造商都使用一种独一无二的模板格式，而且模板在不同系统之间不能互换。

4.3　Doc 9303 号文件中仅仅考虑三种类型的生物特征识别系统，它们都是与生理相关的系统，即：

- 人脸识别 (强制性的)
- 指纹识别 (选择性的)
- 虹膜识别 (选择性的)

一项国际标准即由几部分组成的 ISO/IEC 19794 为这几种生物特征识别提供了规范。签发国须遵守这些规范。

4.4　*生物特征测定学术语*　以下术语将同生物特征识别一起使用：

- “验证”是指将所提供的现时从机读护照持证人身上获得的生物特征数据与持证人在系统登录时产生的生物特征模板进行一对一的匹配；
- “识别”是指将所提供的生物特征数据与在系统中登录的所有个体的模板进行一对多的搜索比对。

4.5　生物特征测定学可在身份识别中用于提高护照，签证或其他旅行证件申请过程中背景核查工作的质量。它可在身份验证中用于确定旅行证件与出示该证件的人是否确实匹配。

5.　关键注意事项

5.1　在规范生物特征评估在机读护照中的应用时，应注意如下几个关键事项：

- *全球互用性* —— 迫切需要规定一个可普遍互用的生物特征应用系统；
- *一致性* —— 需要通过制定具体的标准，实际可能地尽量减小各成员国可能应用的各种不同解决方案之间的差异；

- 技术可靠性 —— 需要提供指导方针和参数，保证成员国所利用的技术已经证明从身份确认的角度讲具有高度的可信性，而且在读取其他国家编码的数据时能够确信，提供给它们的数据具有足够高的质量和完整性，使其能够在其自己的系统中进行准确的身份验证；

- 实用性 —— 需要保证各国能够贯彻执行所制定的规范，而无需为了应付所有可能出现的变化和对标准的各种解释而引入多余的系统和设备；

- 耐久性 —— 要求引入的系统的使用寿命与旅行证件的有效期相同，最多达到 10 年，并且未来的升级能够向下兼容。

6. 定义和术语

6.1 与生物特征测定学相关的术语定义如下：

生物特征 一种用于识别登录者的身份或验证其声称的身份的可测定的生理特征或个人行为特点。

生物特征数据 从生物特征样本中提取的，用于建立参考模板 (模板数据) 或用于与以前创建的参考模板进行比对 (比对数据) 的信息。

生物特征样本 作为一种确切的、唯一的和语言中性的离散值采集的原始数据，该离散值代表着生物特征识别系统所采集的某一登录者的生物特征 (例如，生物特征样本可包括指纹图像及其用于鉴别目的的派生物)。

生物特征系统 一个具有下列功能的自动系统：

1. 为制作机读护照，采集最终用户的生物特征样本；
2. 从该生物特征样本中提取生物特征数据；
3. 将该特定的生物特征数据值与一个或多个参考模板中所含的生物特征数据值相比对；
4. 确定数据匹配度，即根据相关业务对登录者进行明确识别和个体鉴别的要求，执行一个基于规则的匹配过程；
5. 指示是否已完成身份识别或验证。

采集 从最终用户身上收集生物特征样本的方法。

认证机构 签发生物特征证件并以可检测篡改的方法核证该证件中存储数据的真实性的机构。

比对 将生物特征样本与以前存储的一个或多个参考模板进行比对的过程。另见“一对多”和“一对一”。

非接触式集成电路 一种与天线进行耦合的电子微芯片，它使数据能够在该芯片与编码/阅读设备之间进行传递，而无需进行直接的电气连接。

数据库 对生物特征模板和相关的最终用户信息的任何存储。

数据存储 一种在如机读护照之类的证件上存储数据的手段。Doc 9303 号文件第 1 部分第 2 卷规定，电子护照上的数据将存储在非接触式集成电路上。

最终用户　与生物特征系统发生交互作用以便登录或使其[1]身份得到验证的人。

登录　从一个人身上收集生物样本，随后生成与存储代表该人身份的生物特征参考模板的过程。

登录者　由签发国或签发机构发予机读旅行证件的人，即自然人。

电子护照　一种内置非接触式集成电路芯片的机读护照 (MRP)，该芯片储存有机读护照资料页的数据，即持证人的生物特征测定数值和一个用公钥基础设施 (PKI) 密码技术保护数据的安全对象，并符合 Doc 9303 号文件第 1 部分的规范。

提取　将采集的生物特征样本转成生物特征数据，以便能够将其与参考模板进行比对的过程。

获取失败　生物特征系统未能获得为某人登录所必需的生物特征。

登录失败　生物特征识别系统未能为某人登录。

错误接受　生物特征系统错误地识别了某人或者错误地根据所声称的身份验证了某位冒充者。

错误接受率/*FAR*　生物特征系统错误识别某人或者未能拒绝一个冒充者的概率。给定的比率通常采用被动冒充者的尝试次数。错误接受率可被估计为 *FAR = NFA / NIIA* 或者 *FAR = NFA / NIVA*，其中 *FAR* 表示错误接受率，*NFA* 表示错误接受的次数，*NIIA* 表示冒充者企图通过识别的次数，*NIVA* 表示冒充者企图通过验证的次数。

错误匹配率　“错误接受率”的替代形式；用以避免当声称者的生物特征数据同登录者的数据相匹配时反而被拒绝的应用时混乱的情况。在这种应用中，接受和拒绝的概念被颠倒，从而颠倒了“错误接受”和“错误拒绝”的含义。

错误不匹配率　“错误拒绝率”的替代形式；用以避免当声称者的生物特征数据同登录者的数据相匹配时反而被拒绝的应用时混乱的情况。在这种应用中，接受和拒绝的概念被颠倒，从而颠倒了“错误接受”和“错误拒绝”的含义。

错误拒绝　生物特征系统未能识别出某个登录者或者未能验证登录者声称的合法身份。

错误拒绝率/*FRR*　生物特征系统未能识别登录者或者验证登录者声称的合法身份的概率。错误拒绝率可被估计为：*FRR = NFR / NEIA* 或者 *FRR = NFR / NEVA*，其中 *FRR* 表示错误拒绝率，*NFR* 表示错误拒绝的次数，*NEIA* 表示登录者试图通过识别的次数，NEVA 表示登录者试图通过认证的次数。这种估计采用登录者试图通过识别或验证的次数代表所有的登录者试图通过识别或验证的次数。错误拒绝率通常排除“获取失败”的差错。

完整正面 (人脸) 图像　根据 Doc 9303 号文件第 1 部分第 1 卷第 IV 节 7 中的规范制作的机读护照持证人的标准照。

[1] 本文件中通篇使用英文的男性代词应被理解为包括男女两性。

模板库　可用来查找探测模板的，以前登录的个人生物特征模板数据库。

全球互用性　全世界不同国家的检查系统 (人工或者自动) 获得和交换数据，处理从其他国家的系统接收的数据，以及在各自国家运用该数据进行查验操作的能力。全球互用性是为在所有电子护照中加载视读和机读数据制定标准化规范的主要目标。

持证人　拥有电子护照，并在声称具有合法或伪造身份时提交生物特征样本进行身份验证或识别的人。与生物特征系统交互作用以进行登录或者核实身份的人。

标识符　独一无二的数据串，在生物特征系统中用作一个人的身份及其相关属性命名的关键字，护照号码便是标识符的一个例子。

身份　可将一个人与他人明显区分开的独特的个人和生理特征、数据及基本属性的集合。在生物特征系统中，身份通常是在个人通过使用所谓的“源证件”如出生证，公民证书等在该系统中登录时确定的。

识别　一对多的比对过程，即将一个提交的生物特征样本同档案内的所有生物特征参考模板进行比对，确定是否与其中任一个模板相匹配，如果相匹配，将该样本与其模板实现匹配的电子护照持证人的身份进行比对。生物特征系统使用一对多的方法是在一个数据库中找到某种身份，而不是验证一个声称的身份。它与验证形成对照。

图像　通常通过摄像机、照相机或扫描仪等采集的生物特征的表示形式。为了生物特征识别的目的，它以数字形式存储。

冒充者　为故意或无意地充作他人而提交生物特征样本的人。

查验　国家检查旅行者 (电子护照持证人) 呈递的电子护照并且验证其真实性的行为。

签发国　在电子护照旅行证件上写入生物特征以使接受国 (也可能是其本身) 能够对其加以验证的国家。

JPEG 和 JPEG2000　图像数据压缩的标准，特别用于人脸图像的存储。

LDS　描述生物特征数据如何写入电子护照和格式化的逻辑数据结构。

现场采集　通过电子护照持证人和生物特征系统之间的交互作用来采集生物特征样本的过程。

匹配　将生物特征样本和以前存储的模板进行比对并为相似度评分的过程。然后根据相似度得分是否超过设定的阈值，做出接受或者拒绝的决定。

MRTD　机读旅行证件，例如护照、签证或者其他被认可的旅行用官方身份证件。

多生物特征　使用一种以上的生物特征。

一对少　一对多识别和一对一验证的结合。一对少的过程通常包括将一个提交的生物特征样本和档案中少量的生物特征参考模板相比对。当与被列入监控名单的需要进行详细身份调查的人或者一些已知的犯罪分子、恐怖主义分子等进行比对时，常运用这种方法。

一对多　与“识别”同义。

一对一　与“验证”同义。

操作系统　一种对计算机使用的各种应用程序加以管理的程序。

PKI　能够检测电子护照中的数据是否被篡改的公钥基础设施方法。

探针模板　待确定身份的登录者的生物特征模板。

随机访问　一种数据存储方法，可以不需要依次访问所有的存储数据而得到特定的数据项。

读取范围　带有天线的非接触式集成电路同读取设备之间的最大实际距离。

接受国　读取生物特征信息并要对其进行验证的国家。

注册　使生物特征系统了解某个人的身份，将唯一的标识符与该身份相关联，并采集该人的相关属性和将其记录到系统中的过程。

得分　一个从低到高的数值范围内的某个值，用于衡量生物特征探针模板记录 (被搜索的人) 与某个特定的模板库记录 (先前登录者) 之间成功匹配的程度。

模板/参考模板　生物特征系统使用的代表登录者生物特征测量结果的数据，用来与随后提交的生物特征样本相比对。

模板大小　生物特征数据占用的计算机内存量。

阈值　一个“基准”得分，所存储的生物特征与某一个人之间的匹配得分高于这个基准被认为是可接受的，反之，被认为是不可接受的。

特征图像　机读护照持证人的人脸图像，一般是一个完整的正面图像，该图像的尺寸已被调整以确保两眼之间的距离是固定的。如果在拍摄或采集原始头像时没有使两眼中心的连线与长方形头像的上边缘平行，还可以稍微旋转图像以确保二者平行 (见 Doc 9303 号文件第 1 部分本卷第 II 节 13)。

确认　证明正在考虑的系统各个方面都满足该系统规范的过程。

验证　将一个提交的生物特征样本同一个声称具有其身份的登录者的生物特征参考模板相比对，以确定它是否同该登录者的模板相匹配的过程。它与“识别”形成对照。

WSQ 小波标量量化　一种特别用于指纹图像存储的数据压缩方法。

7. 与生物特征识别相关的关键过程

7.1　生物特征系统的主要组成部分是：

采集 —— 原始生物特征样本的获取
提取 —— 原始生物特征样本数据到中间形式的转换
生成模板 —— 中间数据到存储模板的转换
比对 —— 与存储在参考模板中的信息相比较

7.2 这些过程包括：

- 登录过程，该过程就是采集原始生物特征样本。它用来给每个提取生物特征样本的新个体 (潜在的机读护照持证人) 建立一个新的模板。这个采集过程是通过采集设备，例如指纹扫描仪、照片扫描仪、现场采集数字图像照相机或者现场采集虹膜变焦相机等自动获取生物特征。每种采集设备需要有为采集过程确定的某些标准和程序 —— 例如，人脸识别图像采集的标准姿态是正面面对照相机；指纹是平面采集或者是滚动采集；虹膜采集要求眼睛要完全睁开等。

- 模板生成过程，该过程是将采集的生物特征样本中不同的和可重复的生物特征保存下来，这一过程一般通过专有软件算法来完成，以便从采集的图像中提取模板，模板对该图像的处理方式能使该图像随后同另一幅采集的图像相比对并确定比对得分。这种算法具有内在的质量控制功能，通过某种机制对样本进行质量评定。质量标准需尽量的高，因为所有以后的核实都要依靠原始采集的图像质量。如果质量不合格，采集的过程就应该重来一次。

- 识别过程，该过程是将新的样本同已登录的最终用户的已存模板相比对，来决定此最终用户先前是否已经在系统中登录过，如果是，是否是同一个身份。

- 验证过程，该过程是为一个电子护照持证人采集新样本，并将该样本同先前保存的该持证人的样本相比对，来决定持证人是否显示同一个身份。

8. 生物特征方案的应用

8.1 生物特征方案的关键应用是，通过将机读护照持证人和他所持有的机读护照相关联进行身份验证。

8.2 生物特征在申请机读护照的登录过程中有一些典型的应用。

8.2.1 可以在搜索一个或者多个的生物特征库 (识别) 时利用登录过程产生的最终用户的生物特征数据，以确定该最终用户是否能够被相应系统识别出来 (例如：持有一本不同身份的护照，有犯罪记录，持有另一国家的护照等)。

8.2.2 当最终用户来取护照或者签证 (或者在完成了初始申请程序并且采集了生物特征数据后前来进行签发过程的任一步骤时)，可以再次采集他的生物特征数据，并与初始采集的生物特征数据进行比对。

8.2.3 可以对从事登录工作的工作人员的身份进行验证，确认他们有权从事所分配的工作。这可能包括通过对护照签发过程的各个步骤中的审计日志实行数字签名来进行生物特征鉴定，让生物特征把工作人员与他们负责的工作联系起来。

8.3 在边境也有不少生物特征的典型应用。

8.3.1　每当旅行者 (即机读护照持证人) 进出一个国家时，其身份可比照为他签发旅行证件时生成的图像进行验证。这样可以确保持证人是被发予证件的合法人，并且可以提高任何旅客信息预报 (API) 系统的效力。生物特征模板最好和图像一起存储在旅行证件中，这样在无法连接到中央数据库的地方，或者在永久性集中存储生物特征数据是不可接受的管辖区，旅行者的身份也可以得到验证。

8.3.2　双向检测 —— 可将旅行者现场采集的生物特征图像数据与其旅行证件上的 (或者中央数据库中的) 生物特征模板进行匹配，来确认旅行证件未被改动。

8.3.3　三向检测 —— 可将旅行者的现时生物特征图像数据，其旅行证件上面的图像，以及存储在中央数据库的图像进行比对 (通过为每一种信息建立生物特征模板)，确认旅行证件未被改动。这项技术是将本人与其护照以及与将签发该护照时存储在护照中的数据记录下来的数据库进行比对。

8.3.4　四向检测 —— 第四种确认性检测 (并不是电子化的) 实际上是将三向检测的结果与旅行者护照资料页上的数字照片进行目视比对。

8.4　除了生物特征正如在一对一或者一对多的匹配中所体现的在登录和边境安全中的各种应用之外，各国还应考虑到下列因素，并为其制定各自的标准：

—— 系统生物特征匹配功能的精确性。签发国必须按照逻辑数据结构规范对机读护照的一个或多个人脸，指纹，或者虹膜等生物特征进行编码。(这些信息也可存储到接受国可访问的数据库中)。考虑到国际民航组织规定的标准化生物特征图像，接受国必须选择自己的生物特征验证软件并为身份验证接受率 —— 因而也为剔除冒充者确定自己的生物特征得分阈值。

—— 生物特征系统或整个边检系统的通关量 (如每分钟的旅行者流量)。

—— 特定生物特征技术 (人脸，指纹或者虹膜) 在边检应用的适用性。

9.　对生物特征方案的限制

9.1　众所周知，大多数的生物特征技术的实施都要服从于未来科技的高速发展。由于技术革新比较快，任何规范 (包括本文件中的规范) 都必须考虑到并且承认技术进步带来的变革。

9.2　旅行证件中存储的生物特征信息必须符合签发国的国家信息保护法或隐私保护法。

10.　国际民航组织关于生物特征技术的设想

10.1　国际民航组织对应用生物特征技术的设想包括：

—— 为在边检中使用的 (用于验证、黑名单) 以及供承运人和证件签发方使用的生物特征技术的主要互用形式制定规范，以及对已达成共识的补充性生物特征技术制定规范；

—— 为证件签发方使用的 (用于识别，验证和黑名单) 生物特征识别技术制定规范；

—— 数据检索能力按 Doc 9303 号文件中的规定最长达到 10 年；

—— 不涉及所有权问题，确保在生物特征技术方面投资的任何国家得到保护，使其免受基础设施变化或提供商变化的影响。

11. 对适用于电子护照的生物特征的选择

11.1 仅凭姓名和名誉不足以保证持有某签发国签发的身份证件 (机读护照) 的人，就是在接受国宣称自己与发予证件的那个人是同一个人的人，这一点早已得到共识。

11.2 将该人与其旅行证件不可改变地联系在一起的唯一方法，是用一种防篡改的方法将该人的生理特征与其旅行证件相结合。这种生理特征便是一种生物特征。

11.3 在就各国对既适用于机读证件签发手续，又适用于过境旅行中不同程序，且符合各国隐私保护法的生物特征识别符的实际需求进行了五年调查研究后，国际民航组织明确规定，人脸识别须成为全球互用的生物特征技术。一个国家也可以自行选用指纹和/或虹膜识别辅助人脸识别。

11.4 在作出这一结论时，国际民航组织指出，对大多数国家而言，人脸图像具有如下优点：

11.4.1 人脸照片不会泄露该人一般不向公众公开的信息。

11.4.2 从社会和文化角度讲，照片 (人脸图像) 已经被全世界所接受。

11.4.3 为制作符合 Doc 9303 号文件标准的护照，在办理机读护照申请表时已经按常规采集和验证了人脸图像。

11.4.4 公众已经熟知人脸图像的采集及其在身份验证方面的应用。

11.4.5 人脸图像的采集是非干扰性的。最终用户无需为了登录而在较长时间内接触物理装置或与之相互作用。

11.4.6 人脸图像采集不需引进新的、成本高的登录程序。

11.4.7 人脸图像采集工作可以比较及时地布置进行，并还可能采集以前的人脸图像。

11.4.8 许多国家都有一个遗留下来的人脸图像数据库，这些图像是在对护照照片进行数字化制作时采集的，可为身份比对目的将这些照片编码成人脸模板和进行比对验证。

11.4.9 在签发国确定的适当情况下，人脸图像可从被认可的照片上采集，而无需本人在场。

11.4.10 就黑名单而言，人脸照片通常是可用于比对的唯一的生物特征。

11.4.11 与照片/本人比照进行人的生物特征验证的过程相对简单，也被边检机构所熟知。

11.5 *人脸生物特征的存储* 人脸识别技术供应商全部使用专有算法来生成他们的生物特征模板。供应商们将这些算法作为其知识产权加以保密，而且这些算法不能反向设计来生成可识别的人脸图像。因此，人脸识别模板在供

应商之间是不能互用的，而使人脸图像具有互用性的唯一途径是将“原始”采集的照片传至接受国。然后接受国使用其本国供应商的算法 (其供应商/版本可能与签发国所使用的相同，也可能不同) 将实时采集的机读护照持证人的人脸图像与该国利用机读护照数据存储技术读取的人脸图像进行对比。

12. 选择性额外生物特征

12.1　各国可以选择性地为其自己 (及其他国家) 的身份验证过程提供额外数据输入，在其旅行证件中包括多种生物特征，即把人脸和/或指纹和/或虹膜结合起来。当国家有现成的指纹或虹膜数据库，因而可以以此为依据验证，例如作为身份卡系统的一部分提供给他们的生物特征时，这样做就特别适宜。

12.2　*选择性指纹生物特征存储*　指纹生物特征技术分为三类：基于指纹图像的系统、基于指纹特征点的系统和基于指纹式样的系统。虽然这些类别的标准已经制定出来，以便使大部分系统在同类中可以互用，但这些标准在各类别之间是不能互用的。因而也就出现了三种指纹互用性标准：图像数据存储、特征点数据存储和式样数据存储。当签发国决定在所签发的电子护照中加载指纹数据时，就必须存储指纹图像以实现各类别之间的互用性。是否存储相关模板由签发国自定。

12.3　*选择性虹膜生物特征存储*　因缺乏经过实践检验的供应商，使虹膜生物特征识别变得复杂化。因此，一个事实上的虹膜生物特征识别标准根据某个被认可的供应商的方法形成了。其他供应商将来可能会提供虹膜技术，但是作为出发点，他们很可能首先需要虹膜图像，而不是现有供应商生成的模板。如果签发国决定在所签发的电子护照中加载虹膜数据，就必须存储虹膜图像以实现全球互用性。是否存储相关模板由签发国自定。

13. 图像存储、压缩及裁切

13.1　在逻辑数据结构中，对逻辑数据结构影响最大的大小可变的数据项当属显示的图像。接下来的问题是，在不影响接受国对生物特征的比对效果的情况下，“签发国可将图像压缩到什么程度”。

13.2　生物特征系统将获取的原始图像 (人脸，指纹和/或虹膜) 压缩到一个用于进行匹配的特征空间，因此，只要不对这个特征空间造成影响，就可以尽量进行压缩，以减少对所保留图像的存储要求。

13.3　*人脸图像数据尺寸*　符合国际民航组织标准尺寸的 300 dpi 彩色扫描标准照所产生的人脸图像是，两眼间像素单位约为 90，图像尺寸约为 643 K (千字节)，稍压缩即减为 112 K。

13.4　使用标准照片图像，但利用不同的供应商算法和 JPEG 和/或 JPEG 2000 压缩方式进行的研究表明，符合国际民航组织护照照片图像标准的最小可用图像数据大小约为 12 K。研究表明，超过这个大小的高度压缩会大大影响人脸识别结果的可靠性。即使是 12 千字节也不是总能够达到，因为以同样的压缩比，有些图像压缩得要比其他的多，而这取决于服装、色彩和发型等因素。实际上，最适于电子护照的人脸图像平均压缩尺寸在 15 K～20 K 之间。

13.4.1　*裁切*：尽管为了节省存储空间，图像可以裁切到只保留眼睛、鼻子和嘴，但是这会严重影响一个人能否轻而易举地验证图像上的人是否就是站在面前的这个人，或者是否就是护照资料页照片上的那个人。

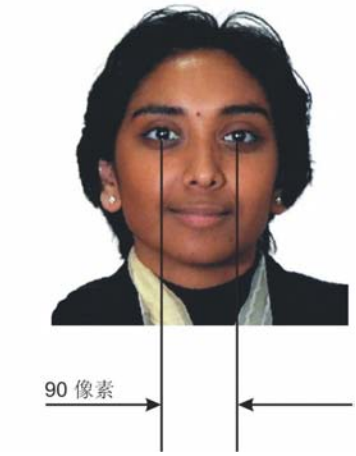
例如，左侧的图像比右侧的图像更难辨认。

因此，建议在数据逻辑结构中存储的图像采取如下两种办法中的一种：

- 不裁切，即与资料页上的标准照保持一致；
- 裁切成下图所示的样子，至少保留从下巴到头顶和从左边缘到右边缘部分。

13.4.2 为了便于人脸识别，人脸图像须存储为符合 ISO/IEC 19794-5 中确定的规范的完整正面图像或者特征图像。特征图像是一种人脸图像，如果需要可以旋转，以确保两眼中心之间的假想连线与照片上边缘及经调整的尺寸相平行。国际民航组织建议两眼中心距约为 90 像素，如下图所示：

原始图像



特征图像 (调整了角度和尺寸)

逻辑数据结构 (参见第 III 节) 可以包括眼睛坐标的存储。(关于在逻辑数据结构中记录人脸图像的详细内容，见本卷第 III 节 10.3.1。)

13.4.3　*人脸装饰物*　签发国须决定在多大程度上允许人脸装饰物出现在存储的 (和显示的) 标准照中。一般来说，如果这种装饰物是永远佩带的，就应允许出现在存储的图像中。

13.5　*选择性指纹图像尺寸*　如果一个国家决定将指纹图像存入集成电路中，最理想的图像大小是每个手指的数据量约为 10 K (例如采用典型的 WSQ 压缩技术) 。

13.6　*选择性虹膜图像尺寸*　如果一个国家决定将虹膜图像存入集成电路，最理想的图像大小是每只眼的数据量约为 30 K。

14.　生物特征及其他数据以逻辑格式在非接触式集成电路中的存储

14.1　这些规范还要求采用数字图像，并且这些图像必须“机载”，即以电子手段存储在旅行证件中。

14.2　这些图像应标准化。

14.3　大容量非接触式集成电路是一种电子存储媒体，国际民航组织规定将其作为运用生物特征的电子护照所使用的扩容技术。

14.3.1　*非接触式集成电路数据存储容量*　集成电路的数据存储容量由各签发国自行决定，最小不低于 32 千字节。这种最小容量是存储强制存储的人脸图像 (通常是 15～20 千字节)、机读区数据副本以及保证数据安全的必要元素所必需的。存储额外的人脸、指纹和/或虹膜图像可能需要大大增加数据存储容量。对集成电路的最大数据容量没有规定。

14.4　*其他数据存储*　有些国家会希望利用电子护照中集成电路的存储容量来扩大机读护照的机读数据容量，使之超过为全球互换所规定的容量。这样做的目的可能是为了提供对源证件信息 (如出生证细节)、存储的个人身份证明 (生物特征) 和/或证件真实性验证细节等的机读访问。

14.5　*逻辑数据结构*　为了保证全球互用性，使各国都能对存储的详细信息进行机读，“逻辑数据结构”或者简称为“LDS”规定了在非接触式集成电路中记录详细信息的格式。本卷第 III 节有对 LDS 的详细说明。

14.6　*所存储数据的安全性及保密性*　签发国和接受国都需要确信，集成电路中存储的数据自证件签发时被写入后未被修改过。此外，签发国的隐私保护法或惯例也可能要求，只有经授权的人员或机构才可以访问这些数据。因此，国际民航组织在第 IV 节中就各国将在其根据 Doc 9303 号文件所载的规范制作的机读旅行证件中使用的现代加密技术，特别是可互用的公钥基础设施 (PKI) 方案的应用和使用方法制定了规范。意图主要是想在国际上采用机读护照及其合法持证人的自动认证方法，从而加强安全性。此外，国际民航组织还为实施国际电子护照认证，以及利用电子护照方便生物特征或电子商务的应用提出了一些方式方法。第 IV 节中的规范准许签发国利用访问控制保护所存储的数据不被未经授权的人员访问。规定了两种访问控制：基本访问控制和扩展访问控制。

14.7　现有规范只允许在机读护照签发时向集成电路中写入数据。

14.8 *公钥基础设施* 公钥基础设施方案的目的，正如所描述的那样，主要是使电子护照查验机构 (接受国) 能够验证电子护照中所存储数据的真实性和完整性。规范并不是要对复杂的公钥基础设施结构的全部实施作出规定，而只是想为各国提供一种实施办法，使其能够在若干领域 (如主动或被动认证、防不当读取和访问控制、自助通关等) 做出选择，从而可能分阶段增加额外特征，而不会与整个架构不相容。

14.8.1 证书用于安全目的，同时还提供了一个向成员国传递公钥 (证书) 的方法，而基础设施是为国际民航组织定制的。

14.8.2 关于公钥基础设施的规范详见本卷第 IV 节。

14.9 *公钥基础设施和逻辑数据结构* 有关逻辑数据结构和公钥基础设施的章节规定了在将生物特征运用于机读护照的过程中如何实现数据的完整性和保密性。

14.10 *非接触式集成电路和编码* 机读护照所使用的非接触式集成电路应符合 ISO/IEC 14443 Type A 或 Type B 的规定。片上操作系统须符合 ISO/IEC 7816-4 标准。逻辑数据结构将按照随机访问方法编码。读取距离 (电子护照和阅读器之间的) 应像 ISO/IEC 14443 所注明的那样达到 10 厘米。

14.11 *逻辑数据结构存储的最少数据项* 非接触式集成电路上的逻辑数据结构所存储的最少强制性数据项须是数据组 1 中机读区数据及数据组 2 中持证人人脸图像的副本。此外，一个兼容的电子护照中的集成电路须包含验证签发国创建数据的完整性所需的安全数据 (EF.SOD)。这种数据存储在为逻辑数据结构规定的 1 号 DF (专用文件) 中 (见第 III 节)。安全数据 (EF.SOD) 由所用的数据组的散列数据组成，详细内容参见第 IV 节。

14.12 *存储数据的结构* 第 III 节中规定的逻辑数据结构详细描述了逻辑数据结构内特定生物特征数据区中应包括的强制性和选择性信息。

15. 非接触式集成电路在机读护照中的放置

15.1 *机读护照中非接触式集成电路及相关天线的位置* 机读护照非接触式集成电路及相关天线的位置由签发国自行决定。各国都应意识到保护非接触式集成电路，使之免遭物理篡改和包括因不小心造成的弯折在内的损坏的重要性。

15.2 *非接触式集成电路及相关天线的选择性位置* 已确定的位置如下：

资料页 —— 将 IC 及其天线放置在资料页结构内，构成护照本的一个内页。

中间页 —— 将 IC 及其天线放置在护照本的中间页。

封皮 —— 将 IC 及其天线放置在护照封皮结构内。

单独的缝入页 —— 将 IC 及其天线纳入一个单独页中，该页可以是和 ID3 一样大小的塑料卡，在制作护照时缝进去。

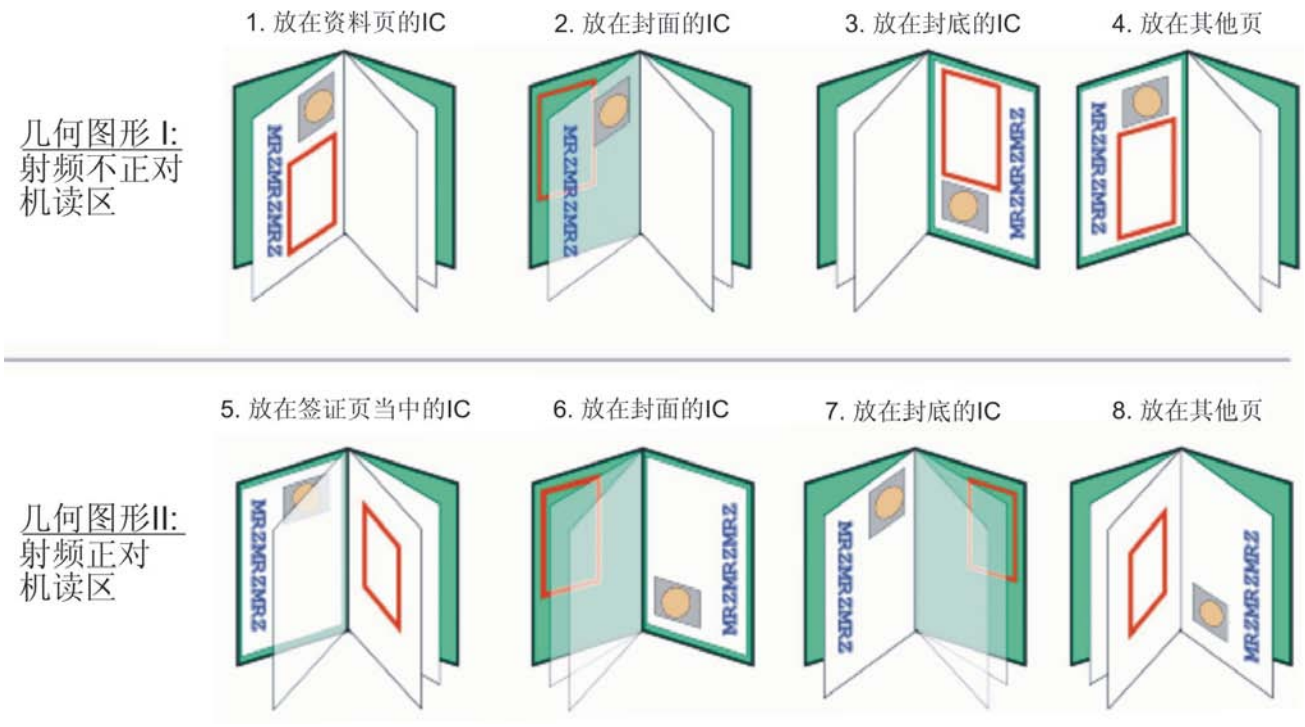


图 II-3

图 II-3 为上述几种选择的示意图。

注：以上示图中带轮廓的长方形代表 IC 及其天线，资料页上的 MRZMRZMRZ 字样代表机读区，长方形里边划一个圆圈代表标准照。

15.3　*电子护照制作注意事项*　需要确保各国电子护照本的制作过程和个人化过程不会对 IC 及其天线造成意外损坏。例如，塑封膜层压时温度过热或在 IC 及其天线区做图像打孔都可能会损坏 IC 装置。同样，当 IC 放置在封面时，如果在 IC 装好后再在封皮外烫金也可能会损坏 IC 或与其天线的连接。

15.4　*既读取 OCR 数据也读取 IC 数据*　极力建议接受国既读取 OCR 数据也读取 IC 上存储的数据。当一个国家为防窃听而将 IC 锁定时，要想访问 IC 数据，就必须读取 OCR。最好只用一个阅读器进行两种操作，即安装的阅读器能够读取两种数据。如果机读护照在资料页上被打开并被放在一个全资料页阅读器上，有些机读护照就将 IC 放在资料页的背面，而其他的则将 IC 放置在护照本中没有全资料页阅读器的部分。

15.5　*阅读器的结构*　因此，各国须安装能够同时处理两种几何结构机读护照的阅读装置，最好能够同时读取 OCR 和集成电路。图 II-4 展示了可能的阅读器结构，每种结构都能够同时读取 OCR 和 IC。护照本是半敞的，两个天线能够确保 IC 被正常读取，不管 IC 是否正对机读区。同时展示的还有一种不那么理想的结构，这里的电子护照先要放在 OCR 阅读器上或划过 OCR 阅读器进行机读区阅读，然后再放在一个阅读器上读取 IC 数据。这种安排将给移民局工作人员带来不便。

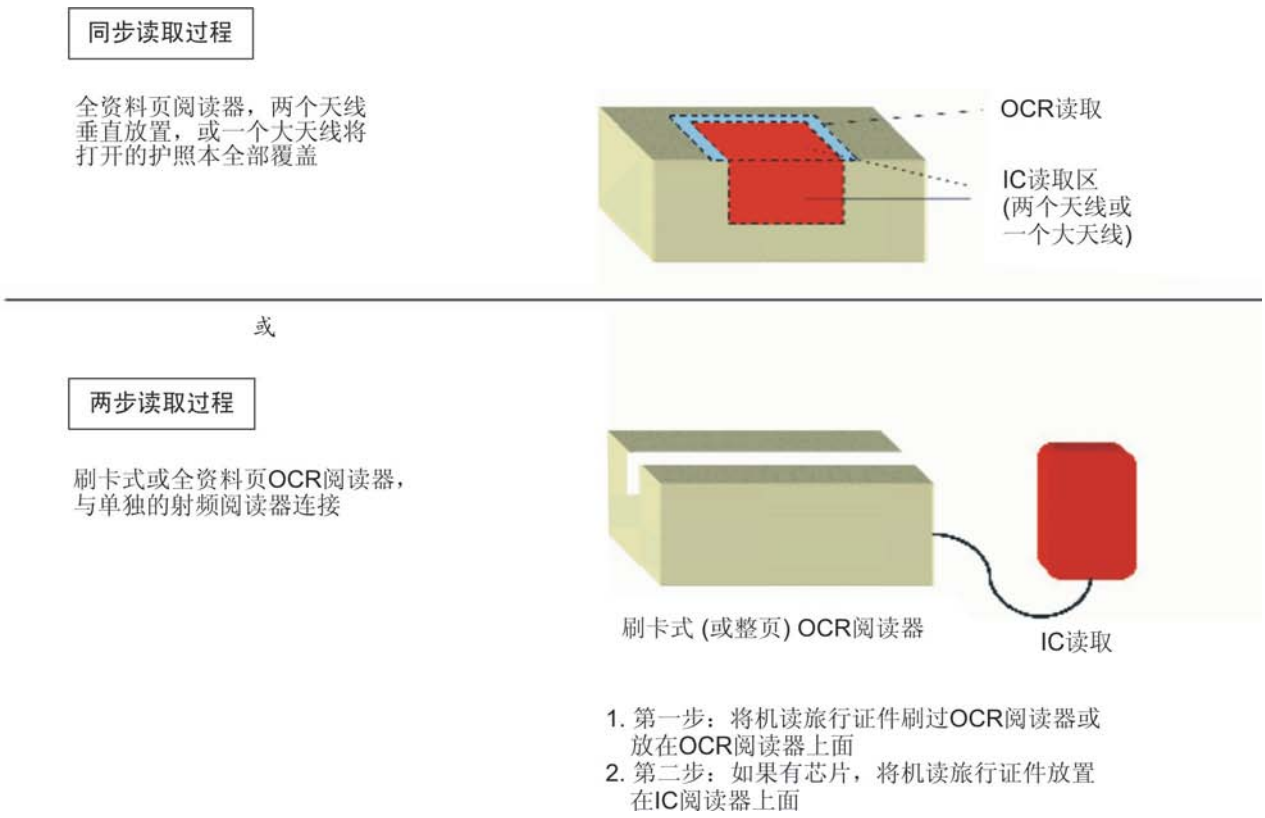


图 II-4

15.6 *阅读几何* 阅读器制造商需考虑如何设计机读解决方案，使之考虑到各种可能的方位，最好能够同时阅读机读区和非接触式集成电路。

16. 电子护照读取过程

16.1 图 II-5 展示了在对电子护照持证人进行生物特征验证前所涉及的过程。

17. 对非接触式集成电路中所存储数据的保护

17.1 非接触式集成电路所存储的数据需要防止被修改。这意味着必须对这些数据加以保护、加密和鉴别。有关这些概念的解释详见第 III 节中的逻辑数据结构和第 IV 节中的公钥基础设施。

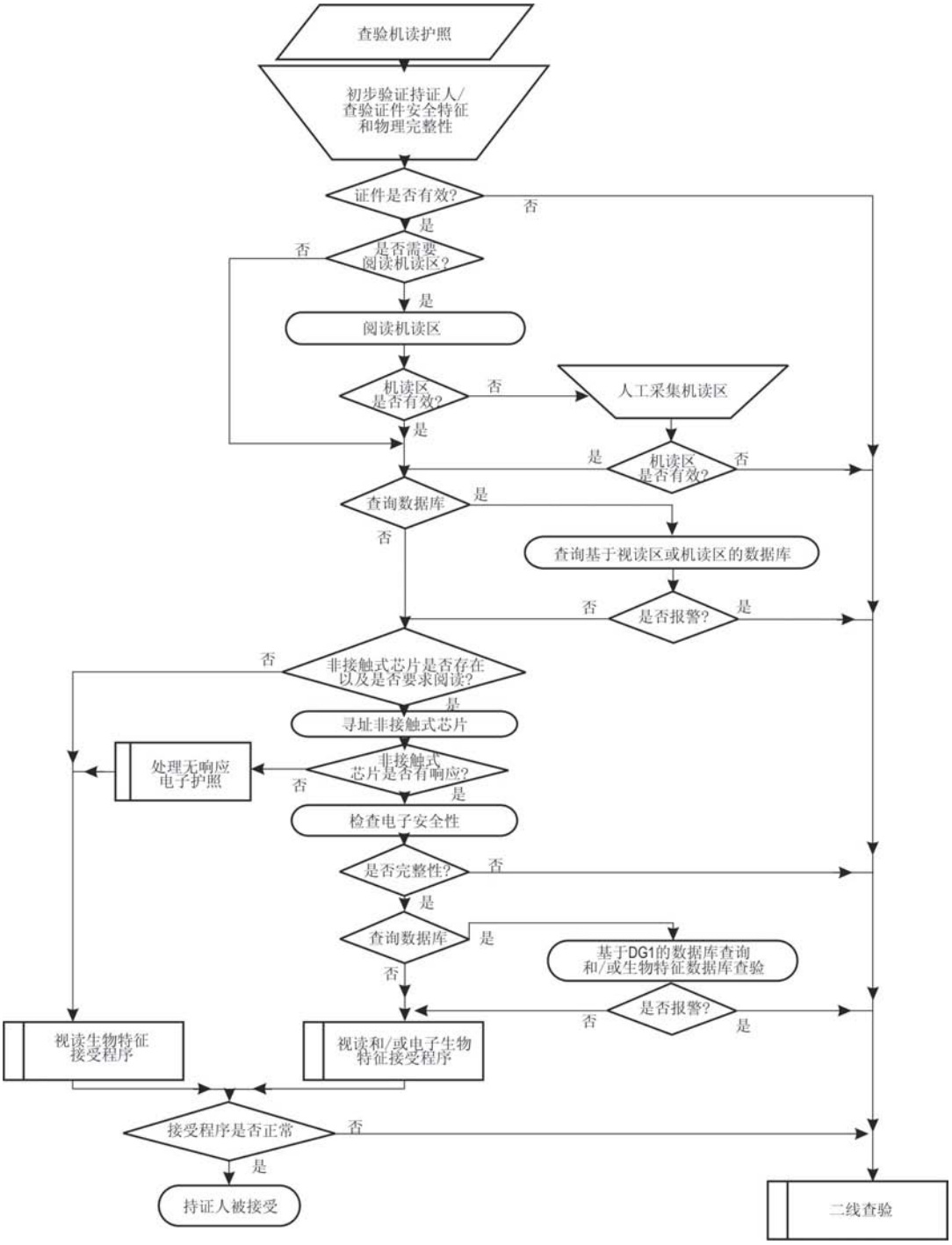

查验机读护照
初步验证持证人/
查验证件安全特征
和物理完整性
证件是否有效?
否
是
是否需要
阅读机读区?
否
是
阅读机读区
机读区
是否有效?
否
人工采集机读区
是
是
机读区
是否有效?
否
查询数据库
是
否
查询基于视读区或机读区的数据库
否
是否报警?
是
非接触式芯片是否存在
以及是否要求阅读?
否
是
寻址非接触式芯片
处理无响应
电子护照
非接触式
芯片是否有响应?
否
是
检查电子安全性
是否完整性?
否
是
查询数据库
是
基于DG1的数据库查询
和/或生物特征数据库查验
否
否
是否报警?
是
视读生物特征
接受程序
视读和/或电子生物
特征接受程序
接受程序是否正常
否
是
持证人被接受
二线查验

图 II-5

第 III 节

非接触式集成电路数据存储技术的逻辑数据结构

1. 范围

1.1 本节定义了电子护照实现全球互用性所需要的逻辑数据结构 (LDS)。它为在签发国或签发机构选择了机读护照非接触式集成电路扩容技术后将记录在该技术中的数据进行标准化组织，使接受国能够访问该数据确定了规范。这需要识别所有的强制性和选择性数据元素，并对数据元素进行规定性的排序和/或编组，要实现全球互用性，就必须遵循这种排序和/或编组，以便读取选择性地包含在机读护照 (电子护照) 中的扩容技术所记录的详细信息 (数据元素)。

2. 规范性参考资料

2.1 本文中参考的下列国际标准的某些规定，构成本节的规定。为了兼顾对包括机读护照在内的机读旅行证件的具体结构要求，当本节中所载的新规范与所参考的标准之间存在差异时，须以本节中所载的规范为准。

ISO 3166-1: 1997 代表国家及其下属行政区名称的代码 —— 第 1 部分：国家代码

ISO 3166-2: 1998 代表国家及其下属行政区名称的代码 —— 第 2 部分：国家下属行政区代码

ISO 3166-3: 1999 代表国家及其下属行政区名称的代码 —— 第 3 部分：国家曾用名称代码

ISO/IEC 7816-1: 1998 识别卡 —— 接触式集成电路卡 —— 第 1 部分：物理特性

ISO/IEC 7816-2: 1998 识别卡 —— 接触式集成电路卡 —— 第 2 部分：触点尺寸和位置

ISO/IEC 7816-3: 1997 识别卡 —— 接触式集成电路卡 —— 第 3 部分：电气接口和传输协议

ISO/IEC 7816-4: 2005 识别卡 —— 接触式集成电路卡 —— 第 4 部分：组织、安全和交换命令

ISO/IEC 7816-5: 2003 识别卡 —— 接触式集成电路卡 —— 第 5 部分：应用供应商注册

ISO/IEC 7816-6: 2003 识别卡 —— 接触式集成电路卡 —— 第 6 部分：行业间互交换数据元素 (包括缺陷报告在内)

ISO/IEC 7816-7: 1998 识别卡 —— 接触式集成电路卡 —— 第 7 部分：结构化卡查询语言 (SCQL) 的命令

ISO/IEC 7816-8: 2003 识别卡 —— 接触式集成电路卡 —— 第 8 部分：安全操作命令

ISO/IEC 7816-9: 1999 识别卡 —— 接触式集成电路卡 —— 第 9 部分：卡和文件管理命令

ISO/IEC 7816-10: 1999 识别卡 —— 接触式集成电路卡 —— 第 10 部分：同步卡的电气接口

ISO/IEC 7816-11: 2003 识别卡 —— 接触式集成电路卡 —— 第 11 部分：使用生物特征方法的个人身份验证

ISO/IEC 7816-15: 2003 识别卡 —— 接触式集成电路卡 —— 第 15 部分：密码信息应用

ISO 8601:2000 数据元素和交换格式 —— 信息交换 —— 日期和时间的表达方法

ISO/IEC 8824-2: 1998 ITU-T 建议 X.681 (1997)，信息技术 —— 第一种抽象语法表示法 (ASN.1)：信息对象规范

ISO/IEC 8824-3: 1998 ITU-T 建议 X.682 (1997)，信息技术 —— ISO/IEC 8824-1: 1998

ISO/IEC 8824-4: 1998 ITU-T 建议 X.683 (1997)，信息技术 —— 第一种抽象语法表示法 (ASN.1)：ASN.1 规范的参数化

ISO/IEC 8825-1: 2003 信息技术 —— ASN.1 编码规则：基本编码规则 (BER)、标准编码规则 (CER) 和特异编码规则 (DER) 规范

ISO/IEC 8825-2: 2003 信息技术 —— ASN.1 编码规则：压缩编码规则 (PER) 规范

ISO/IEC 8825-3: 2003 信息技术 —— ASN.1 编码规则：编码控制表示法规范

ISO/IEC 8825-4: 2003 信息技术 —— ASN.1 编码规则：XML 编码规则 (XER)

ISO/IEC 10373-6:2001 紧耦合卡测试方法

ISO/IEC 10373-6: 2001/FDAM1 紧耦合卡的测试方法 (修订 1：紧耦合卡的协议测试方法)

ISO/IEC 10373-6: 2001/AM2: 2003 紧耦合卡的测试方法 (修订 2：改进后的射频测试方法)

ISO/IEC 10373-6: 2001/FDAM4 紧耦合卡的测试方法 (修订 4：PCD 射频接口和 PICC 交变磁场暴露的补充测试方法)

ISO/IEC 10373-6: 2001/FDAM5 紧耦合卡的测试方法 (修订 5：fc/64、fc/32 和 fc/16 的比特率)

ISO/IEC 10918 信息技术 —— 数字压缩和连续色调静止图像的编码

ISO/IEC 14443-1: 2000 识别卡 —— 非接触式集成电路卡 —— 紧耦合卡 —— 第 1 部分：物理特性

ISO/IEC 14443-2: 2001 识别卡 —— 非接触式集成电路卡 —— 紧耦合卡 —— 第 2 部分：射频功率和信号接口

ISO/IEC 14443-2: 2001/AM1: 2005 紧耦合卡：射频功率和信号接口 (修订 2：fc/64、fc/32 和 fc/16 的比特率)

ISO/IEC 14443-3 识别卡 —— 非接触式集成电路卡 —— 紧耦合卡 —— 第 3 部分：初始化和防冲突

ISO/IEC 14443-3: 2001/AM1:2005 紧耦合卡：初始化和防冲突 (修订 1：fc/64、fc/32 和 fc/16 的比特率)

ISO/IEC 14443-4	识别卡 —— 非接触式集成电路卡 —— 紧耦合卡 —— 第 4 部分：传输协议
ISO/IEC15444	JPEG 2000
ISO/IEC 19785-1	信息技术 —— 通用生物特征交换格式框架 —— 第 1 部分：数据元素规范
ISO/IEC 19794-4	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	信息技术 —— 生物特征数据交换格式 —— 第 5 部分：人脸图像数据
ISO/IEC 19794-6	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 9797-1:1999	信息技术 —— 安全技术 —— 报文认证码 —— 第 1 部分：使用分组密码的机制
Unicode 4.0.0	Unicode 协会。Unicode 标准，4.0.0 版，定义源自：*The Unicode Standard, Version 4.0* (Boston, MA, Addison-Wesley, 2003. ISBN 0-321-18578-1) (与 ISO/IEC 10646-1 标准一致)

3. 定义

就本节而言，须适用如下定义。

(注：与基本的机读护照、签证和官方旅行证件有关的定义见 Doc 9303 号文件第 1 部分第 1 卷第 II 节。)

ASN.1　第一种抽象语法表示法

CBEFF　通用生物特征交换格式框架。这是一种便于生物特征数据交换和互用的通用文件格式。ISO/IEC JTC1/SC37 目前正在作为一项国际标准草案推介这一文档。

受权接受机构　获得授权处理官方旅行证件的机构 (如航空器运营人)，此类机构因而可能在未来被允许在选择性容量扩展技术中记录详细信息。

逻辑数据结构 (*LDS*)　在选择性容量扩展技术中存储的数据元素分组的集合。

数据组　逻辑数据结构中构成组群的一系列相关数据元素。

签发方数据块　一系列由签发国或签发机构写入选择性容量扩展技术的数据组。

接受方数据块　一系列由接受国或受权接受机构写入选择性容量扩展技术的数据组。

真实性　确认逻辑数据结构及其组成要素是由签发国或签发机构所创建的能力。

完整性　确认逻辑数据结构及其组成要素与签发国或签发机构创建的逻辑数据结构及其组成要素相比未经任何修改的能力。

4. 对逻辑数据结构的需要

4.1 要想实现全球互用性，使机器能够读取存储在签发国或签发机构自行决定加入到机读旅行证件内的某种扩容技术中的详细记录信息，则标准化的逻辑数据结构是必不可少的。

4.2 在开发逻辑数据结构的过程中，国际民航组织最初作为一项重要的要求提出，需要为使用任何一种正在考虑的选择性扩容技术的所有机读旅行证件提供一个单一的逻辑数据结构。随着讨论的深入，非接触式集成电路明显成为唯一能够满足国际民航组织所有需求的技术。

注：随着愿意使用该逻辑数据结构的国际民航组织成员国及其他机构对扩容的需求得到进一步确认，逻辑数据结构会得到不断发展。而随着对数据完整性和保密性需要的进一步了解，数据安全要求的发展尤其会对该逻辑数据结构产生影响。

5. 逻辑数据结构的要求

5.1 国际民航组织已确定，预定义的标准化逻辑数据结构必须满足以下强制性要求：

- 确保合法持证人的使用效率和最优化的使用便利；
- 确保记录在选择性扩容技术中的详细信息能够得到保护；
- 通过使用通用于所有机读旅行证件的单一逻辑数据结构，实现扩容数据在全球范围内的交流；
- 满足签发国和签发机构对不同选择性扩容的需求；
- 随着用户需求和可用技术的发展，提供进一步的扩容；
- 支持各类数据保护选项；
- 支持签发国或签发机构所选择的对详细信息的更新；
- 在保证签发国或签发机构所创建数据的真实性[2]和完整性[3]的同时，支持接受国或经批准的接受机构添加详细信息；
- 最大限度地利用现有的国际标准，尤其是全球可互用的生物特征方面的新兴国际标准。

6. 强制性和选择性数据元素

6.1 如图 III-1 所示，为满足对出示机读旅行证件者进行检查放行的全球性要求，已经为该逻辑数据结构（LDS）确定了一系列强制性和选择性数据元素。

---

[2] 真实性 —— 确认逻辑数据结构及其组成要素是由签发国或签发机构所创建的能力。
[3] 完整性 —— 确认逻辑数据结构及其组成要素与签发国或签发机构创建的逻辑数据结构及其组成要素相比未被修改的能力。

7. 数据元素的排序和编组

7.1　如图 III-1 所示，已经为上述一系列强制性和选择性数据元素建立了一个由相关数据元素排序编组支持的逻辑顺序[4]。

7.2　根据数据元素的排序编组是由 1) 一个签发国或签发机构记录的，还是由 2) 一个接受国或经批准的接受机构记录的，数据元素的排序编组又被进一步分组。

注：在本版本的 Doc 9303 号文件第 1 部分所定义的逻辑数据结构不支持接受国或经批准的接受机构向该逻辑数据结构添加数据的能力。

7.3　如果某个逻辑数据结构被记录在选择性扩容技术 (非接触式集成电路) 中，那么有四个组别的数据元素将是强制性的：

- 界定电子护照机读区 (MRZ) 内容的数据元素 (数据组 1)；
- Doc 9303 号文件第 1 部分第 1 卷和第 2 卷第 II 节中所定义的电子护照持证人脸部编码图像；
- EF.COM，包含版本信息和标签表；
- EF.SOD，包含数据完整性和真实性信息。

7.4　所有其他已经确定可由签发国或签发机构记录的数据元素都是选择性的。

7.5　由接受国或经批准的接受机构添加的数据元素编组可以在，也可以不在逻辑数据结构中出现。在逻辑数据结构中可以出现一个以上的由接受国或经批准的接受机构添加的数据元素编组记录。

注：本版本的 Doc 9303 号文件中第 1 部分不支持接受国或经批准的接受机构向该逻辑数据结构添加数据的能力。

7.6　该逻辑数据结构被认为是一个单一的内聚性实体，内含机读时记录在选择性扩容技术中的数据元素编组号码。

注：根据设计，该逻辑数据结构具有足够的灵活性，可以应用于所有类型的机读旅行证件。在下面的图和表中，部分数据项目只适用于机读签证和机读官方身份证件，或者对这些证件需要采取不同的表示方法。就电子护照而言，这些项目应当被忽略。

7.7　在该逻辑数据结构中，有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。

7.8　每个数据组都被分配了一个参考编号。图 III-2 显示的是每个数据组的参考编号。例如，“DG2”表示数据组 2，机读旅行证件合法持证人的脸部编码识别特性 (即人脸生物特征详细信息)。

注：本版本的 Doc 9303 号文件第 1 部分不支持接受国数据组 (数据组 17 ~ 19)。

---

[4] 为了满足对出示机读旅行证件者进行检查放行时加强便利性和改善安全性的全球性要求，数据元素的逻辑顺序已经实现了标准化。编组数据元素在记录时的实际顺序根据为确保非接触式集成电路扩展技术高效性能而制定的规范加以确定。这些规范见附件 1。

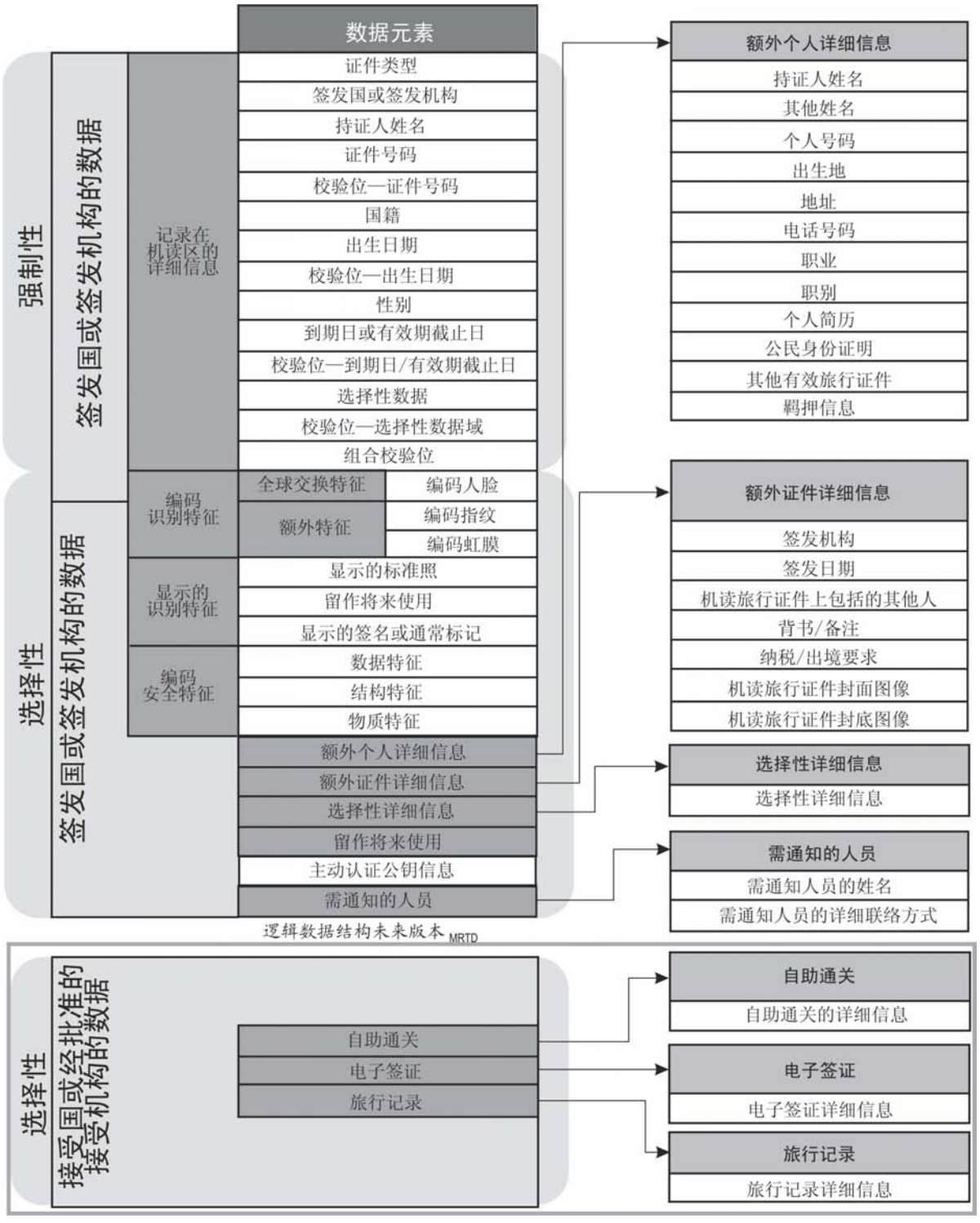


图 III-1　为逻辑数据结构规定的强制性和选择性数据元素

8. 用于确认数据真实性和完整性的编码数据组

8.1　为了能够对所记录的详细信息的真实性和完整性加以确认，真实性/完整性对象被包括在内。每个数据组都将在该真实性/完整性对象中体现出来，且该对象会被记录在一个独立的基本文件 (EF.SOD) 中。(细节请参见第 IV 节 —— 公钥基础设施)。利用编码识别特征数据组 2-4 所使用的 CBEFF 结构和第 IV 节 —— 公钥基础设施中所定义的选择性“额外生物特征安全”特征，签发国或签发机构也可以自行决定对身份确认详细信息 (如生物特征模板) 提供单独的保护。

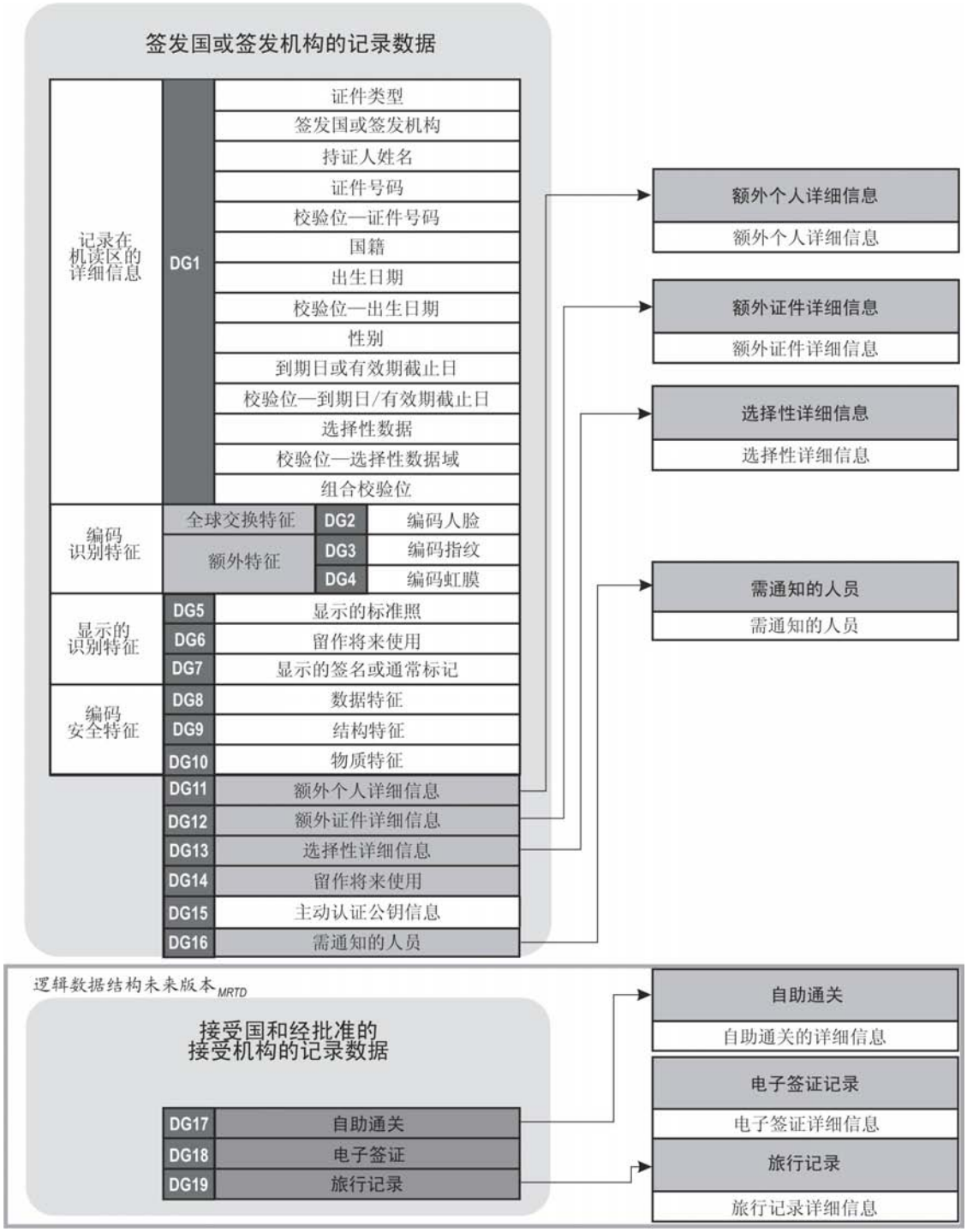


图 III-2　指定给逻辑数据结构的数据组参考编号

图 III-2 注：现在还不允许接受国选择添加关于通关、电子签证和旅行记录的数据，但列入该选项是为了表明未来的发展方向。

9.　签发国或签发机构记录的数据组

下表确定了强制性和选择性数据组，两者的结合将构成由签发国或签发机构记录的逻辑数据结构部分。

数据组	强制性 (M)/ 选择性 (O)	数据项	
机读旅行证件机读区记录的详细信息			
1	M	机读区 (MRZ) 数据	
机器辅助身份确认详细信息 —— 编码识别特征			
2	M	**全球交换特征**	编码人脸
3	O	额外特征	编码指纹
4	O	额外特征	编码虹膜
机器辅助身份确认详细信息 —— 显示的识别特征			
5	O	显示的标准照 [见 10.3]	
6	O	留作将来使用	
7	O	显示的签名或通常标记	
机器辅助安全特征验证 —— 编码安全特征			
8	O	数据特征	
9	O	结构特征	
10	O	物质特征	
额外个人详细信息			
11	O	额外个人数据元素	
额外证件详细信息			
12	O	额外证件数据元素	
选择性详细信息			
13	O	由签发国或签发机构确定的自由选定数据元素	
留作将来使用			
14	O	留作将来使用	
15	O	主动认证公钥信息	
需通知的人员			
16	O	需通知人员的数据元素	

10.　构成数据组 1 至数据组 16 的数据元素

10.1　数据组 1 (DG1) 至数据组 16 (DG16) 均各自包含一定数量的强制性和选择性数据元素。数据组中的数据

元素顺序为标准化顺序。

10.2 如下各表定义了强制性和选择性数据元素，两者的结合将构成数据组 1 (DG1) 至数据组 16 (DG16) 的结构。

10.2.1 机读旅行证件机读区记录的详细信息。分配给数据组 1 (DG1) 的数据元素如下所示。数据组 1 中的数据元素旨在反映机读区中的全部内容，无论机读区中包含的是实际数据，还是填充字符。关于机读区执行的详细内容在 Doc 9303 号文件第 1 部分第 1 卷中有具体规定。

数据组	数据元素	固定/ 可变	强制性/ 选择性	数据项
DG1			**M**	**机读区 (记录在机读旅行证件上的详细信息摘要，参见 Doc 9303 号文件)**
	01	F	M	证件类型
	02	F	M	签发国或签发机构
	03	F	M	持证人姓名
	04	F	M	证件号码 (9 个最高有效字符)
	05	F	M	校验位 —— 证件号码或填充字符 (<) 表示证件号码超过 9 个字符。[见 10.2.2]
	06	F	M	国籍
	07	F	M	出生日期
	08	F	M	校验位 —— 出生日期
	09	F	M	性别
	10	F	M	到期日 (对于机读护照而言为 TD-1 和 TD-2)
	11	F	M	校验位 —— 到期日或有效期截止日
	12	F	M	选择性数据和/或就 TD-1 而言证件号码中最低有效字符，加上证件号码校验位，再加上填充字符
	13	F	M	校验位 —— 选择性数据域
	14	F	M	组合校验位

10.2.2 关于校验位计算的详细内容，参见 Doc 9303 号文件第 1 部分第 1 卷。

10.3　机器辅助身份确认详细信息 —— 编码识别特征　分配给数据组 2 (DG2) 至数据组 4 (DG4) 的数据元素如下所示：

数据组	数据元素	强制性/ 选择性	数据项
DG2		**M**	**全球交换识别特征 —— 人脸** [见 10.3.1]
	01	M	已记录的人脸生物特征编码数量
	02[5]	M	报头 [见 A.13.3]
	03[6]	M	人脸生物特征数据编码 [见 A.13.3]
额外识别特征 [见10.3.2]			
DG3		**O**	**额外识别特征 —— 指纹** [见 10.3.2]
	01	M (如编码指纹特征已记录)	已记录的指纹生物特征编码数量
	02[6]	M (如编码指纹特征已记录)	报头 [见 A.13.3]
	03[6]	M (如编码指纹特征已记录)	指纹生物特征数据编码 [见 A.13.3]
DG4		**O**	**额外识别特征 —— 虹膜** [见 10.3.2]
	01	M (如编码虹膜特征已记录)	已记录的虹膜生物特征编码数量
	02[6]	M (如编码虹膜特征已记录)	报头 [见 A.13.3]
	03[6]	M (如编码虹膜特征已记录)	虹膜生物特征数据编码 [见 A.13.3]

10.3.1　数据组 2 (DG2) 表示的是利用机读旅行证件进行机器辅助身份确认的全球互用生物特征，这一特征须是将被输入到人脸识别系统中的持证人的人脸图像。如果有一项以上的记录，最新的国际互用编码须是第一项输入。使用芯片技术的首要目的是能够采集旅行证件的生物特征信息。记录在数据组 2 中的人脸生物特征数据交换图像须取自用于创建打印在电子护照资料页上的显示标准照的，并且须根据最新版本的 ISO/IEC 19794-5 中规定的完整正面或特征性正面图像类型格式进行编码。数据组 2 须根据签发国自行作出的决定，包含完整正面或特征性正面人脸生物特征数据交换格式图像或两者兼备。如果包含的是完整正面图像，也可以使用 ISO/IEC 19794-5 中确定的选择性特

[5] 当存在一个以上生物特征记录时，数据元素将在数据组中重复出现，如数据元素 01 所定义的那样。具体的执行方法请参见技术映射附件 1。
[6] 当存在一个以上显示的签名或通常标记/编码安全特征时，数据元素将在数据组中重复出现，如数据元素 01 所定义的那样。

征点数据块，在完整正面图像中包含眼部位置。如签发国希望记录显示的标准照，即当人脸生物特征数据交换格式图像与显示的标准照存在较大差异时，须将该图像记录在数据组 5 (DG5) 中。

10.3.2 国际民航组织认为，各成员国可选择使用指纹和/或虹膜识别作为支持机器辅助身份确认的额外的生物特征技术，它们须被分别编码为数据组 3 (DG3) 和数据组 4 (DG4)。

10.4 *机器辅助身份确认详细信息 —— 显示的识别特征* 分配给数据组 5 (DG5) 至数据组 7 (DG7) 的数据元素如下所示：

数据组	数据元素	强制性/选择性	数据项
DG5		**O**	**显示的标准照**
	01	M (如显示的标准照已记录)	已记录的显示的标准照数量
	02[7]	M (如显示的标准照已记录)	显示的标准照的表示法 [见 10.4.1]
DG6		**O**	**留作将来使用**
DG7		**O**	**显示的签名或通常标记**
	01	M (如显示的签名或通常标记已记录)	显示的签名或通常标记数量
	02[6]	M (如显示的签名或通常标记已记录)	显示的签名或通常标记的表示法 [见 10.4.1]

10.4.1 数据组 5 (DG5) 和数据组 7 (DG7) 的数据元素须根据 ISO/IEC 10918-1 的规定使用 JFIF 选项或 ISO/IEC 15444 (JPEG2000) 编码。

10.5 *机器辅助安全特征验证 —— 编码的详细信息* 组合构成数据组 8 (DG8) 至数据组 10 (DG10) 的数据元素如下所示：

数据组	数据元素	强制性/选择性	数据项
DG8		**O**	**数据特征**
	01	M (如该编码特征已使用)	数据特征的数量
	02[6]	M (如该编码特征已使用)	报头 (待定)

[7] 当存在一个以上显示的特征记录时，数据元素将在数据组中重复出现，如数据元素 01 所定义的那样。

数据组	数据元素	强制性/选择性	数据项
	03	M (如该编码特征已使用)	数据特征数据
DG9		**O**	**结构特征**
	01	M (如该编码特征已使用)	结构特征的数量
	02	M (如该编码特征已使用)	报头 (待定)
	03	M (如该编码特征已使用)	结构特征数据
DG10		**O**	**物质特征**
	01	M (如该编码特征已使用)	已记录的物质特征数量
	02	M (如该编码特征已使用)	报头 (待定)
	03	M (如该编码特征已使用)	物质特征数据

10.6　额外个人详细信息　组合构成数据组 11 (DG11) 的数据元素如下所示：

数据组	数据元素	强制性/选择性	数据项
DG11		**O**	**额外个人详细信息**
	01	O	持证人姓名 (主要和次要标识符，完整的)
	02	O	其他姓名
	03	O	个人编号
	04	O	出生地
	05	O	出生日期 (完整的)
	06	O	地址
	07	O	电话号码
	08	O	职业
	09	O	职别
	10	O	个人简历

数据组	数据元素	强制性/选择性	数据项
	11	O	公民身份证明 [见 10.6.1]
	12	M* *如数据元素 13 已记录。	其他有效旅行证件的数量
	13	O	其他旅行证件的数量
	14	O	羁押信息

10.6.1 数据元素 11 须根据 ISO/IEC 10918-1 或 ISO/IEC 15444 (JPEG2000) 的规定编码。

10.7 额外证件详细信息 组合构成数据组 12 (DG12) 的数据元素如下所示：

数据组	数据元素	强制性/选择性	数据项
DG12			**额外证件详细信息**
	01	O	签发机构 (适用于机读旅行证件)
	02	O	签发日期 (适用于机读旅行证件)
	03	M* *如其他人也包含在机读旅行证件上	机读旅行证件上包含的其他人的数量 (仅适用于机读签证)
	04	O	机读旅行证件上包含的其他人 (仅适用于机读签证)
	05	O	背书/备注 (与机读旅行证件有关)
	06	O	纳税/出境要求
	07	O	机读旅行证件封面图像 [见 10.7.1]
	08	O	机读旅行证件封底图像 [见 10.7.1]
	09	O	机读旅行证件个人化的时间
	10	O	用于为机读旅行证件进行个人化处理的设备

10.7.1 数据元素 07 和 08 须根据 ISO/IEC 10918-1 或 ISO/IEC 15444 (JPEG2000) 的规定编码。

10.8 选择性详细信息 组合构成数据组 13 (DG13) 的数据元素如下所示：

数据组	数据元素	强制性/选择性	数据项
DG13		**O**	**选择性详细信息**
	01	M (如数据组 13 已记录)	由签发国或签发机构确定的详细信息

10.9　数据组 14：未分配的数据组。留作将来使用。

数据组	数据元素	强制性/选择性	数据项
DG14		**O**	**留作将来使用**

10.10　数据组 15 (DG15)：主动认证公钥信息。该数据组中包含选择性的主动认证公钥 (参见第 IV 节 —— 公钥基础设施)。

数据组	数据元素	强制性/选择性	数据项
DG15		**O**	**主动认证公钥信息**

10.11　需通知的人员　组合构成数据组 16 (DG16) 的数据元素如下所示：

数据组	数据元素	强制性/选择性	数据项
DG16		**O**	**需通知的人员**
	01	M (如数据组 16 已记录)	识别的人员数量
	02	M (如数据组 16 已记录)	已记录的详细日期
	03	M (如数据组 16 已记录)	需通知人员的姓名
	04	M (如数据组 16 已记录)	需通知人员的电话号码
	05	O	需通知人员的地址

11.　接受国或经批准的接受机构记录的数据组

11.1　下表确定了组合后构成逻辑数据结构一部分的选择性数据组，逻辑数据结构的这一部分将来可能会提供给接受国或经批准的接受机构用于记录数据。

注：根据这一版本的 Doc 9303 号文件第 1 部分的规定，不允许接受国或经批准的接受机构记录数据。因此，数据组 17 至数据组 19 是无效的，而且目前在逻辑数据结构中也不支持这两个数据组。此处包含这两个数据组是要表明规划的未来发展方向。

数据组	强制性 (M)/选择性 (O)	数据项
自助通关的详细信息		
DG17	O	自助通关

数据组	强制性 (M)/选择性 (O)	数据项
电子签证		
DG18	O	电子签证
旅行记录详细信息		
DG19	O	旅行记录

12. 数据元素的格式

12.1 数据元素目录

本节描述的是可能在每个数据组中出现的数据元素。

12.1.1 签发国或经批准的签发机构的数据元素

数据组 1 (DG1) 至数据组 16 (DG16): 数据元素及其在每个数据组区中的格式如下：

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 外的任何字符)、F = 固定长度域、Var = 可变长度域

数据元素	选择性 (O)/强制性 (M)	数据元素名称	字节数	固定或可变	编码类型	编码要求
数据组 1：机读区内记录的数据						
01	M	证件类型	2	F	A、S	证件类型 (按照 Doc 9303 号文件中所定义的机读区)
02	M	签发国或签发机构	3	F	A、S	签发国或签发机构 (按照 Doc 9303 号文件中所定义的机读区)
03	M	持证人姓名				
	M	主要和次要标识符	39	F	A、S	按照 Doc 9303 号文件中所定义的机读区插入的单字或双字填充字符 (<)。
04	M	证件号码	9	F	A、N、S	证件号码 (按照机读区) 注： 根据 Doc 9303 号文件第 3 部分为 TD-1 确定的规范，如果证件号码长度超过 9 个字符，须在证件校验位位置 (DE 05) 插入一个填充字符 (<) 。组成证件号码的其余字符须记录在 DE 12 开头的位置，后面紧跟证件号码校验位和一个填充符 (<)。

数据元素	选择性 (O)/强制性 (M)	数据元素名称	字节数	固定或可变	编码类型	编码要求
05	M	校验位 —— 证件号码	1	F	N、S	数据元素 04 的校验位 (按照 Doc 9303 号文件中所定义的机读区)。
06	M	国籍	3	F	A、S	三字母代码 (根据机读区)。
07	M	出生日期	6	F	N、S	格式 = YYMMDD (按照 Doc 9303 号文件中所定义的机读区)。 完整的出生日期可以存储在 DG11 中，格式为 CCYYMMDD，以避免年编码发生混淆。
08	M	校验位 —— 出生日期	1	F	N	数据元素 07 的校验位 (按照 Doc 9303 号文件中所定义的机读区)。
09	M	性别	1	F	A、S	按照 Doc 9303 号文件中所定义的机读区。
10	M 如果是 TD-1 型、TD-2 型机读护照	到期日	6	F	N	格式 = YYMMDD (按照机读区)。
	M 如果是 A 型、B 型机读签证	有效期截止日	6	F	N	格式 = YYMMDD (按照机读区)。
11	M	校验位 —— 到期日或有效期截止日	1	F	N	数据元素 10 的校验位 (按照 Doc 9303 号文件中所定义的机读区)。
12	M 如果是机读区内的选择性数据	选择性数据				
	M 如果是机读区内的选择性数据	选择性数据	14	F	A、N、S	按照机读区。
13	M	校验位 —— 选择性数据域	1	F	N	数据元素 12 的校验位 (按照 Doc 9303 号文件中所定义的机读区)。
14	M	校验位 —— 组合校验位	1	F	N	按照 Doc 9303 号文件中所定义的机读区。

数据元素	选择性 (O)/ 强制性 (M)	数据元素名称	字节数	固定或 可变	编码类型	编码要求
数据组2：编码识别特征 —— 人脸						
01	M 如果包括编码人脸特征	已记录的人脸生物特征编码数量	1	F	N	1至9表明唯一的人脸数据编码数量。
02	M 如果包括编码人脸特征	报头		F		编码的详细信息见规范性附录 1，A13.3。 根据 DE 01 的规定，数据元素可重复出现。
03	M 如果包括编码人脸特征	人脸生物特征数据编码	最大 99999	Var	A、N、S、B	编码的详细信息见规范性附录 1，A13.3。 根据 DE 01 的规定，数据元素可重复出现。
数据组3：编码识别特征 —— 指纹						
01	M 如果包括编码指纹特征	已记录的指纹生物特征编码数量	1	F	N	1至9表明唯一的指纹数据编码数量。
02	M 如果包括编码指纹特征	报头		F		编码的详细信息见规范性附录 1，A13.3。 根据 DE 01 的规定，数据元素可重复出现。
03	M 如果包括编码指纹特征	指纹生物特征数据编码	最大 99999	Var	A、N、S、B	编码的详细信息见规范性附录 1。 根据 DE 01 的规定，数据元素可重复出现。
数据组 4：编码识别特征 —— 虹膜						
01	M 如果包括编码虹膜特征	已记录的虹膜生物特征编码数量	1	F	N	1至9表明唯一的虹膜数据编码数量。
02	M 如果包括编码虹膜特征	报头		F		编码的详细信息见规范性附录 1。 根据 DE 01 的规定，数据元素可重复出现。
03	M 如果包括编码虹膜特征	虹膜生物特征数据编码	最大 99999	Var	A、N、S、B	编码的详细信息见规范性附录 1。 根据 DE 01 的规定，数据元素可重复出现。
数据组5：显示的识别特征 —— 标准照						
01	M 如果包括显示的标准照	条目的数量：显示的标准照	1	F	N	1至9表明唯一的显示标准照记录的数量。
02	M 如果包括显示的标准照	显示的标准照数据		F		根据 DE 01 的规定，数据元素可重复出现。

数据元素	选择性 (O)/强制性 (M)	数据元素名称	字节数	固定或可变	编码类型	编码要求
	M 如果包括显示的标准照	用于表现显示的标准照的字节数	5	F	N	00001 至 99999，表明用于表现紧接其后的显示的标准照的字节数。
	M 如果包括显示的标准照	显示标准照的表现	最大 99999	Var	A、N、S、B	根据 ISO/IEC 10918-1 或 ISO/IEC 15444 格式化。
数据组6：留作将来使用						
数据组 7：显示的识别特征 —— 签名或通常标记						
01	M 如果包括显示的签名或通常标记	条目的数量：显示的签名或通常标记	1	F	N	1至9表明唯一的显示签名或通常标记记录的数量。
02	M 如果包括显示的签名或通常标记	显示的签名或通常标记数据		Var		根据 DE 01 的规定，数据元素可重复出现。
	M 如果包括显示的签名或通常标记	显示签名或通常标记的表现	最大 99999	Var	A、N、S、B	根据 ISO/IEC 10918-1 或 ISO/IEC 15444 格式化。
数据组 8：编码安全特征 —— 数据特征						
01	M 如果包括编码数据特征	数据特征的数量	1	F	N	1至9表明唯一的数据特征编码数量 (包括 DE 02 至 DE 04)。
02	M 如果包括编码数据特征	报头信息	1	待定		待定报头详细信息。
03	M 如果包括编码数据特性	数据特征数据		Var		
	M 如果包括编码数据特征	编码数据特征	最大 999	Var	B	由签发国或签发机构自行确定的格式。
数据组 9：编码安全特征 —— 结构特征						
01	M 如果包括编码结构特征	结构特征的数量	1	F	N	1至9表明唯一的结构特征编码数量 (包括 DE 02 至 DE 04)。
02	M 如果包括编码结构特征	报头信息	待定	待定	N	待定的报头详细信息。

数据元素	选择性 (O)/强制性 (M)	数据元素名称	字节数	固定或可变	编码类型	编码要求
03	M 如果包括编码结构特征	结构特征数据		Var		
	M 如果包括编码结构特征	编码结构特征	最大 999	Var	B	由签发国或签发机构自行确定格式。
数据组 10：编码安全特征 —— 特征						
01	M 如果包括编码物质特征	物质特征的数量	1	F	N	1至9表明唯一的结构特征编码数量 (包括 DE 02 至 DE 04)。
02	M 如果包括编码物质特征	标题信息	待定	待定	N	待定的报头详细信息。
03	M 如果包括编码物质特征	物质特征数据		Var		
	M 如果包括编码物质特征	编码物质特征	最大 999	Var	B	由签发国或签发机构自行确定格式。
数据组11：额外个人详细信息						
见数据元素目录 —— 额外个人详细信息 [见 12.1.2]						
数据组12：额外证件详细信息						
见数据元素目录 —— 额外证件详细信息 [见 12.1.3]						
数据组 13：选择性详细信息						
见数据元素目录 —— 选择性详细信息 [见 12.1.4]						
数据组 14：留作将来使用						
保留						
数据组 15：主动认证公钥信息						
本卷第 IV 节“提供 ICC 只读访问的机读旅行证件公钥基础设施”中所规定的主动认证公钥信息						
数据组 16：需通知的人员						
见数据元素目录 —— 需通知人员的详细信息 [见 12.1.5]						

12.1.2 数据组 11 (DG11) **数据组 11：额外个人详细信息**中的数据元素及其格式如下所示：

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 外的任何字符)、F = 固定长度域、Var = 可变长度域

数据组 11：额外个人详细信息						
数据元素	选择性 (O)/ 强制性 (M)	数据元素名称	字节数	固定或 可变	编码类型	编码要求
01	O	持证人姓名 (全名)				
	M 如果 DE 01 包括在内	主要和次要标识符	最大 99	Var	A、S	按照机读区插入填充符 (<)。在行尾不插入填充符。不允许截取。
02	O	其他姓名				
		主要和次要标识符	最大 99	Var	A、S	按照机读区插入填充符 (<)。在行尾不插入填充符。不允许截取。
03	O	个人编号				
		个人编号	最大 99	Var	A、N、S	自由形式的文本。
04	O	出生地				
		出生地	最大 99	Var	A、N、S	自由形式的文本。
05	O	地址				
		地址	最大 99	Var	A、N、S	自由形式的文本。
06	O	完整的 出生日期				
		出生日期	8	F	N	CCYYMMDD
07	O	电话				
	M 如 DE 07 包 括在内	电话	最大 99	Var	N、S	自由形式的文本。
08	O	职业				
	M 如 DE 08 包 括在内	职业	最大 99	Var	A、N、S	自由形式的文本。
09	O	职别				
	M 如 DE 09 包 括在内	职别	最大 99	Var	A、N、S	自由形式的文本。
10	O	个人简历				
	M 如 DE 10 包 括在内	个人简历	最大 99	Var	A、N、S	自由形式的文本。
11	O	公民身份证明		Var		
	M 如 DE 11 包	公民身份详细信息	最大 9999999	Var	B	根据 ISO/IEC 10918-1 格式化的公民证件图像。

数据组 **11**：额外个人详细信息						
数据元素	**选择性 (O)/ 强制性 (M)**	**数据元素名称**	**字节数**	**固定或可变**	**编码类型**	**编码要求**
	括在内					
12	O	其他有效旅行证件		Var		
	M 如 DE 12 包括在内	旅行证件号码	最大 99		A、N、S	自由形式的文本，由<分隔。
13	O	羁押信息		Var		
	M 如 DE 13 包括在内	羁押信息	最大 999	Var	A、N、S	自由形式的文本。

12.1.3 数据组 12 (DG12) **数据组 12 —— 额外证件详细信息**中的数据元素及其格式如下所示：

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 外的任何字符)、F = 固定长度域、Var = 可变长度域

数据组 **12**：额外证件详细信息						
数据元素	**选择性 (O) / 强制性 (M)**	**数据元素名称**	**字节数**	**固定或可变**	**编码类型**	**编码要求**
01	O	签发机构				
		签发机构	最大 99	Var	A、N、S	自由形式的文本。
02	O	签发日期	8	F	N	发证日期：即 YYYYMMDD
03	O	包含的其他人员				** 仅在有机读签证时有效 **。
		其他人员的详细信息	最大 99	Var	A、N、S	自由形式的文本。
04	O	背书/备注				
		背书/备注	最大 99	Var	A、N、S	自由形式的文本。
05	O	纳税/出境要求				
		纳税/出境要求	最大 99	Var	A、N、S	自由形式的文本。
06	O	机读旅行证件封面图像				
		机读旅行证件的图像	最大 9999999	Var	B	根据 ISO/IEC 10918-1 格式化。

数据组 12：额外证件详细信息						
数据元素	选择性 (O) / 强制性 (M)	数据元素名称	字节数	固定或可变	编码类型	编码要求
		(封面)				
07	O	机读旅行证件封底图像				
		机读旅行证件的图像 (封底)	最大 9999999	Var	B	根据 ISO/IEC 10918-1 格式化。
08	O	个人化时间				
		证件个人化的时间		F	F 14N	ccyymmddhhmmss
09	O	个人化序列号				
		个人化设备的序列号		Var	V 99ANS	自由格式。

12.1.4　数据组 13 (DG13)　**数据组 13 —— 选择性详细信息**中的数据元素及其格式如下所示：

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 外的任何字符)、F = 固定长度域、Var = 可变长度域

数据组 13：选择性详细信息						
数据元素	选择性 (O) / 强制性 (M)	数据元素名称	字节数	固定或可变	编码类型	编码要求
待定	O	选择性详细信息		Var		由签发国或签发机构自行决定。

12.1.5　数据组 16 (DG16)　**数据组 16 —— 需通知的人员**中的数据元素及其格式如下所示：

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 外的任何字符)、F = 固定长度域、Var = 可变长度域

数据组16：需通知的人员						
数据元素	选择性 (O) / 强制性 (M)	数据元素名称	字节数	固定或可变	编码类型	编码要求
01	M 如 DG 16 包括在内	识别的人员数量	2	F	N	表明包含在该数据组中的人员数量。
02	M	记录的日期详	8	F	N	记录通知日期的日期；格式

数据组16：需通知的人员						
数据元素	选择性 (O) / 强制性 (M)	数据元素名称	字节数	固定或可变	编码类型	编码要求
	如 DG 16 包括在内	细信息				= CCYYMMDD
03	M 如 DG 16 包括在内	需通知人员的姓名 主要和次要标识符		Var	A、S	根据机读区插入填充字符(<)。不允许截取。
04	M 如 DE 03 包括在内	需通知人员的电话号码		Var	N、S	国际格式的电话号码 (国家代码和地区区号码)。
05	M	需通知人员的地址		Var	A、N、S	自由形式的文本。

13. 安全原则

13.1 安全原则用于保护记录的逻辑数据结构 (LDS) 并确保接受国或经批准的接受机构能够确认从选择性扩容技术中读取的数据的真实性和完整性。关于安全原则的进一步论述，参见第 IV 节 —— 公钥基础设施。

图 III-3 强制性报头和数据组存在信息

14. 非接触式集成电路数据扩展技术的映射原则

14.1 *逻辑数据结构的排序* 为实现国际互用性，只允许使用随机排序方案。逻辑数据结构排序的具体描述请参见本节的规范性附录1。

14.2 *随机排序方案* 随机排序方案允许按照随机排序方式对数据组和数据元素加以记录，而且这种排序方式与选择性扩容技术即使在数据元素采用无序记录方式时也允许直接检索具体数据元素的能力相符合。可变长度数据元素被编码为长度/值 (Length/Value)，长度见 ASN.1 记数法中的规定。

强制性报头和数据组存在图被包括在内。这一信息存储在EF.COM文件中。请参见附录1。

14.2.1　*报头*　报头中包含的下列信息可以使接受国或经批准的接受机构对签发国或签发机构记录的数据块中所包含的各个数据组和数据元素进行定位和解码。

应用标识符 (AID)
逻辑数据结构版本号
UNICODE 版本号

14.2.2　*逻辑数据结构版本号*　逻辑数据结构版本号决定了逻辑数据结构的格式版本 [8]。用于存储该值的确切格式将在技术映射附录中确定。逻辑数据结构版本号标准化格式为“aabb”，其中：

“aa”= 用于表明逻辑数据结构版本的 (即逻辑数据结构的重要增补内容的) 编号 (01–99)；

“bb”= 用于表明逻辑数据结构更新的编号 (01–99)。

14.2.3　*Unicode 版本号* [9]　Unicode 版本号表明记录字母字符、数字字符和特殊字符，包括国家字符时所使用的编码方法。用于存储该值的确切格式将在技术映射附录中确定。Unicode 版本号的标准格式为“aabbcc”，其中：

“aa”= 用于表明 Unicode 标准**主要版本** (即以书的形式公布的该标准的重要增补内容) 的编号；

“bb”=用于表明 Unicode 标准**次要版本** (即以**技术**报告形式公布的新增的字符或更加重要的规范修改) 的编号；

“cc”=用于表明 Unicode 标准**更新版本** (即该标准中任何有可能改变程序行为的规范部分或重要资料部分的修改。这些修改都反映在新的 Unicode 字符数据库文件和更新页中) 的编号。

注：由于历史的原因，在每一个域 (即 a、b、c) 中的编号并不一定是连续的。

14.3　*数据组存在图*　数据组存在图 (DGPM) 中包含的信息能够使接受国或经批准的接受机构确定哪些数据组存在于签发国或签发机构记录的数据块中。

14.3.1　集成电路执行程序中使用的数据组存在图由一个“标签”表组成，该表符合识别接触式和非接触式集成电路中记录的数据组的约定，在集成电路中每个标签都可以分辨某一特定的数据组是否被记录在签发国或签发机构记录的数据块中。这种数据组存在图在 EF.COM 中以标签表的形式执行，其中 Tag = ‘5C’。请参见附录 1。

数据组“n”标签
•
•
数据组“m”标签

[8] 国际民航组织已经预计对逻辑数据结构标准组织的未来更新，并将通过公布对有关规范的修订跟上这些更新。每次更新都会有一个版本号，确保接受国和经批准的接受机构能够精确地对逻辑数据结构的所有版本进行解码。

[9] *Unicode* 以 ISO/IEC 10646 为基础。如欲了解 *Unicode* 的详细信息，请访问 www.unicode.org。

标签存在 = 数据组存在
标签不存在 = 数据组不存在

14.4 *数据元素存在图* 有一些数据组使用一种类似的存在图概念，这些数据组中包含作出记录的国家或机构可能自行决定包括的一系列从属数据元素。这些被称为数据元素存在图 (DEPM) 的存在图位于这些具体数据组的起始位置，可以像图 III-4 表明的那样进行选择性的扩展。

需要使用数据元素存在图的数据组见附录 1。

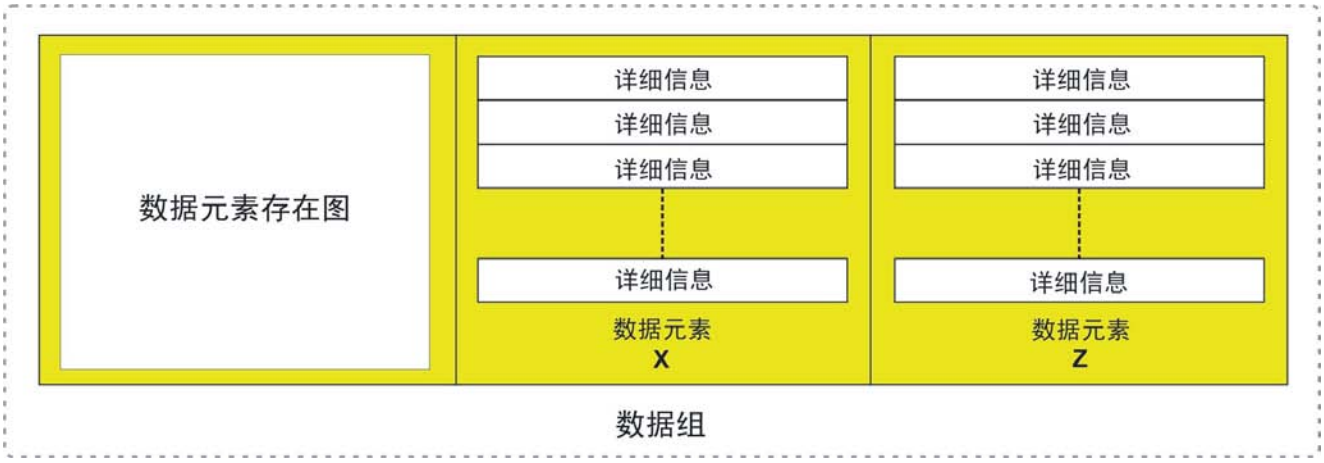


图 III-4 数据元素存在图

14.4.1 数据元素存在图中包含的信息能够使接受国或经批准的接受机构确定哪些数据元素存在于数据组中。

14.4.2 数据元素存在图由一个“标签”表组成，该表符合识别接触式和非接触式集成电路中记录的数据元素的约定，在集成电路中，每个标签都可以分辨某一特定的数据元素是否被记录在数据组中。数据元素存在图的这种形式在相关数据组中被编码为标签表。

数据元素“n”标签
•
•
数据元素“m”标签

标签存在 = 数据元素存在
标签不存在 = 数据元素不存在

注：第 III 节的规范性附录 1 对分配给数据元素存在图的字节数做了规定。

第III节规范性附录1

使用随机存取表示法的逻辑数据结构
向非接触式集成电路 (IC) 的映射

A.1　范围　附录 1 定义的是关于将使用随机存取表示法的逻辑数据结构 —— (LDS) [1.7 版] 映射至机读旅行证件的集成电路 (IC) 上，从而使签发国或签发机构能够自行决定对机读数据容量加以扩展的现行规范。

注：附录 1 中提供的规范仅适用于支持“离卡”生物特征鉴别的逻辑数据结构，即机读旅行证件为机器辅助身份确认提供的逻辑数据结构只将机读旅行证件作为数据载体使用。

A.2　规范性参考资料　参见第 III 节 2。

A.3　随机存取文件表示法　随机存取文件表示法是在做了下列考虑和假设的情况下确定的。

- 支持各种各样执行程序。逻辑数据结构包括各种各样的选择性数据元素。包含这些数据元素是为了便于机读旅行证件的认证、合法持证人的验证，并且可以加快证件/人员查验点的处理速度。
- 该数据结构必须支持：

  —— 有限的或广泛的数据元素集；
  —— 特定数据元素的重复出现；
  —— 特定执行程序的不断改进。

- 支持至少一种应用数据集。
- 支持各国其他的特定应用。
- 支持使用存储的非对称密钥对和芯片上的非对称加密技术进行的选择性证件主动认证。有关此类主动认证的详细内容载于第 IV 节 —— 公钥基础设施。
- 支持对选定的数据元素的快速访问，以便于对持证人的快速处理：

  —— 立即访问必要的数据元；
  —— 直接访问数据模板，尤其是生物特征数据。

A.3.1　为了提供互用性，附录 1 对如下各项进行了界定：

- 初始化、防冲突和传输协议；
- 命令集；
- 包括安全参考在内的命令的使用；

- 国际民航组织机读旅行证件逻辑数据结构应用的文件结构；
- 数据元素向文件的映射；
- 字符集。[10]

A.4 *安全要求* 数据的完整性和真实性对进行可信的国际交换是必不可少的。详细规范请参见第 IV 节 —— *公钥基础设施*。

A.5 *与现有国际标准的兼容性* 为了便于实施和确保互用性，与现有标准兼容是至关重要的。因此，这项规范将最大限度地与第 III 节 2 所提到的标准保持兼容。

A.6 *定义* 请参见第 III 节 3。

A.7 *物理特性* 证件的物理特性须符合第 1 卷中所定义的物理特性。

A.8 *耦合区的位置和尺寸*

A.8.1 耦合区的尺寸须符合 ISO/IEC 14443。

A.8.2 TD-1 尺寸证件耦合区的位置须符合 ISO/IEC 14443，TD-3 证件耦合区的位置由签发方自行决定。

A.9 *电信号* 射频功率和信号接口的规定见 ISO/IEC 14443。

A.10 *传输协议和请求应答*

A.10.1 *传输协议* 机读旅行证件将支持 ISO/IEC 14443-4 中规定的半双工传输协议。机读旅行证件可以支持 Type A 或 Type B 传输协议。

A.10.2 *命令请求* 集成电路须使用请求应答 —— Type A (ATQA) 或请求应答 —— Type B (ATQB) 对命令请求 —— Type A (REQA) 或命令请求 —— Type B (REQB) 做出响应。

A.10.3 *应用选择* IC 卡须支持至少一种符合下述要求的机读旅行证件 (MRTD) 应用：

- 一种应用须包含由签发国或签发机构记录的数据 (数据组1～16) 和证实签发者所创建的并存储在DF 1中的数据完整性所需要的安全数据 (EF.SOD)。安全数据 (EF.SOD) 包含在用的数据组散列。详细信息请参见第IV节 —— *公钥基础设施*。
- 第二种应用是本版本的Doc 9303号文件第1部分所不支持的，它将包含接受国或经批准的接受机构所添加的数据 (数据组17～19)。

[10] 字符集中使用的是 UTF-8 编码。逻辑数据结构中使用的多数数据元素都是基本拉丁语 (ASCII) 字符或二进制码。有一小部分数据元素，例如“以本国字符书写的姓名”、“出生地”等，不可能全部使用基本拉丁语代码集来实现编码。因此，字符编码所使用的是 Unicode 标准：UTF-8。这是一种能够保留 ASCII 透明性的可变长度的编码。UTF-8 完全符合 Unicode 标准和 ISO/IEC 10646。UTF-8 使用一个字节来编码标准的 ASCII 字符 (代码值 0…127)。许多非表意文字则以两个字节来表达。剩余的字符则以三个或四个字节来表达。使用 UTF-8 可以很容易地编入非 ASCII 字符，而无需用两个、三个或四个字节去表达所有的字符。

此外，签发国或签发机构可能希望添加其他应用。文件结构须有能力容纳此类额外应用，但此类应用的具体细节并不属于本规范性附录所涉及的范围。

机读旅行证件应用须通过作为保留的专用文件 (DF) 名使用应用识别 (AID) 加以选择。应用识别须包含 ISO 根据 ISO/IEC 7816-5 分配的注册应用标识符 (RID)，以及本文件中所规定的专有应用标识符扩展 (PIX)。

应用标识符为‘A0 00 00 02 47’。

签发者存储的数据应用须使用PIX = ‘1001’。

A.10.4　安全性

数据组1～15须具备写保护　每个数据组的在用散列须存储在安全数据 (EF.SOD) 中。安全数据还须包含在用散列的数字签名。参见第IV节 —— 公钥基础设施。

只有签发国或签发机构对这些数据组拥有写访问权。因此，没有交换要求，而且实现写保护所使用的手段不属于本规范所涉及的内容。

数据组 16 须具备写保护。只有签发国或签发机构对该数据组中的数据元拥有写访问权。

数据组 17、18 和 19 将在逻辑数据结构第 2 版中规定。

A.11　文件结构　IC 卡中的信息存储在一个 ISO/IEC 7816-4 定义的文件系统中。IC 卡的文件系统以层级方式组织成专用文件 (DF) 和基本文件 (EF)。专用文件包含基本文件或其他专用文件。文件系统的根可以是一个选择性[11]的主文件 (MF)。

本规范所定义的 DF1 (强制性) 包含签发者的数据元素。该专用文件在应用 (注册 RID 和 PIX) 中的名称为‘A0 00 00 02 47 10 01’，并使用该名称进行选择。如果 IC 卡有一个主文件，则该主文件可以放置在附属于 IC 卡主文件的专用文件树上的任意位置。

在每一项应用中都可能包含数个“数据组”。签发国或签发机构的应用可以包含最多 16 个数据组。数据组 1 [DG1] (机读区) 和数据组 2 (编码人脸) 是强制性的。所有其他数据组都是选择性的。接受国或经批准的接受机构的应用可以包含三个数据组 (DG17～19)。这三个数据组都是选择性的。所有数据组都采取数据模板的形式，并且拥有各自的 ASN.1 标签。

A.11.1　DF1

DF1 拥有一个包含应用通用信息的文件 (文件名为 EF.COM)。该文件的短文件标识符为 30 (‘1E’)。该文件包含逻辑数据结构版本信息、Unicode 版本信息和一个用于应用的数据组列表。每个数据组须存储在一个透明的基本文件 (EF) 中。基本文件须以表 III-A1 中所显示的短文件标识符寻址。基本文件须具有这些文件的文件名，这些文件名须符合 EF.DGn 的命名规则，其中 n 表示数据组的编号。包含安全数据的基本文件的名称为 EF.SOD。文件结构的图示见图 IIIA-1。

[11] 是否需要主文件，根据操作系统的选择而定。

每个数据组包含一个模板内的一系列数据对象。每个数据组须存储在一个独立的基本文件 (EF) 中。当单个数据对象在透明文件中的相对位置确定之后，数据组中的单个数据对象便可以直接检索。

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规定见 ISO/IEC 7816-4 和 7816-6。每个数据对象有一个按十六进制编码的识别标签 (例如‘5A’)。本附录中定义的标签采用共存编码选项。每个数据对象都有一个独一无二的标签、长度和值。可能出现在一个文件中的数据对象标明强制性 (M) 和选择性 (O) 两种。这些定义包含对第 13 节所定义的数据元编号的具体参照。在一切可能的情况下都使用了跨行业标签。请注意，某些标签的具体定义和格式已经改变以使其与机读旅行证件应用相关联。例如：

标签 5A 被定义为证件号码，而不是主账户号码，其格式也从 V19N 变为 F9N。

标签 5F20 原为持卡人姓名，现已被重新定义为“持证人姓名”，长度最大为 39 个字符，按照 Doc 9303 号文件格式编码。

标签 65 被定义为显示的标准照，而不是持卡人相关数据。

根据需要，还定义了范围从 5F01 至 5F7F 的一些额外标签。

表III-A1　强制性签发国或签发机构应用

数据组	基本文件名	短基本文件标识符	文件标识符	标签
通用	EF.COM	‘1E’	‘01 1E’	‘60’
DG1	EF.DG1	‘01’	‘01 01’	‘61’
DG2	EF.DG2	‘02’	‘01 02’	‘75’
DG3	EF.DG3	‘03’	‘01 03’	‘63’
DG4	EF.DG4	‘04’	‘01 04’	‘76’
DG5	EF.DG5	‘05’	‘01 05’	‘65’
DG6	EF.DG6	‘06’	‘01 06’	‘66’
DG7	EF.DG7	‘07’	‘01 07’	‘67’
DG8	EF.DG8	‘08’	‘01 08’	‘68’
DG9	EF.DG9	‘09’	‘01 09’	‘69’
DG10	EF.DG10	‘0A’	‘01 0A’	‘6A’
DG11	EF.DG11	‘0B’	‘01 0B’	‘6B’
DG12	EF.DG12	‘0C’	‘01 0C’	‘6C’
DG13	EF.DG13	‘0D’	‘01 0D’	‘6D’
DG14	EF.DG14	‘0E’	‘01 0E’	‘6E’
DG15	EF.DG15	‘0F’	‘01 0F’	‘6F’
DG16	EF.DG16	‘10’	‘01 10’	‘70’
安全数据	$EF.SO_D$	‘1D’	‘01 1D’	‘77’

A.12　命令集　机读旅行证件所支持的最小命令集如下所示：

—— SELECT
—— READ BINARY

强制性和选择性的命令参数的规定见本附录的 A.17。A.23 段描述了对长度超过 32 767 字节的文件进行访问所使用的命令选项。

所有的命令、格式及其返回码的定义见 ISO/IEC 7816-4。请参见本附录 A.22。

为了安全地加载和更新数据，建立正确的安全环境，并实施第 IV 节 —— 公钥基础设施中所确定的选择性安全条款，还需要一些额外的命令，这一点已得到共识。这些命令不属于本互用性规范的范畴，但它们可以包括：

—— GET CHALLENGE
—— EXTERNAL AUTHENTICATE
—— VERIFY CERTIFICATE

A.13　签发者数据应用

签发者数据应用，AID = ‘A0 00 00 02 47 10 01’。签发者应用包含两个强制性的数据组和 14 个选择性的数据组。各数据组的通用信息存储在应用模板‘60’中。该模板则存储在强制性文件 EF.COM 中。

A.13.1　EF.COM　通用数据元素 (短文件标识符 = 30 (‘1E’))

应用模板标签 ‘60’ —— 应用层信息

注：该模板目前只包含修改层和标签表‘5C’。所定义的模板结构支持未来的发展，如动态签名和生物特征信息模板 (BIT)。可能出现在该模板中的数据元素包括：

标签	长度	值
‘5F01’	04	逻辑数据结构版本号，格式为 aabb，其中 aa 用于定义逻辑数据结构的版本，bb 用于定义升级级别。
‘5F36’	06	Unicode 版本号，格式为 aabbcc，其中 aa 用于定义主要版本，bb 用于定义次要版本，而 cc 用于定义发布级别。
‘5C’	X	标签表。所有存在的数据组表。

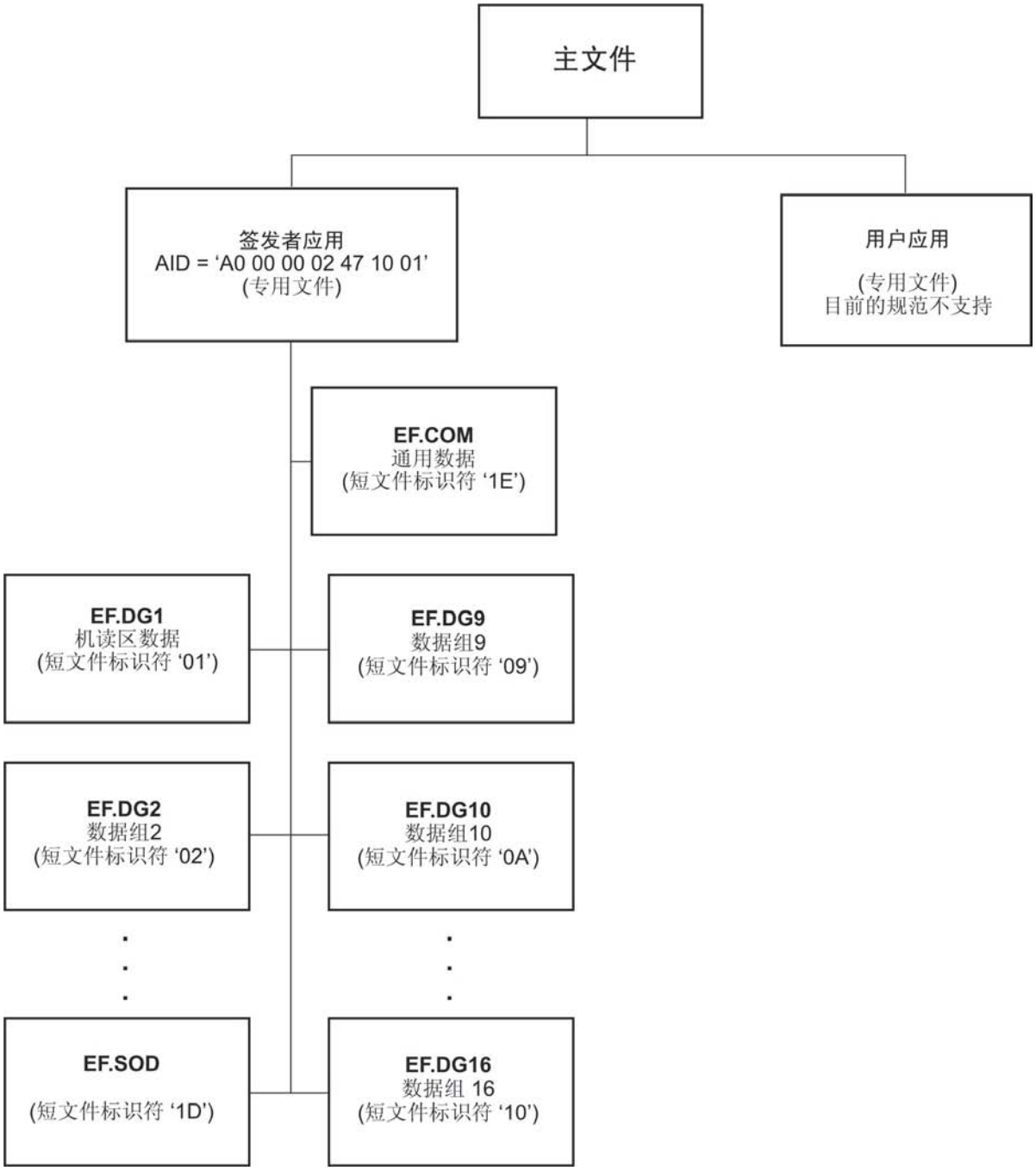

主文件
签发者应用
AID = 'A0 00 00 02 47 10 01'
(专用文件)
用户应用
(专用文件)
目前的规范不支持
EF.COM
通用数据
(短文件标识符 '1E')
EF.DG1
机读区数据
(短文件标识符 '01')
EF.DG9
数据组9
(短文件标识符 '09')
EF.DG2
数据组2
(短文件标识符 '02')
EF.DG10
数据组10
(短文件标识符 '0A')
EF.SOD
(短文件标识符 '1D')
EF.DG16
数据组 16
(短文件标识符 '10')

图 IIIA-1

下面的示例表示的是一个使用 Unicode 4.0.0 版，含有数据组 1 (标签‘61’)、数据组 2 (标签‘75’)、数据组 4 (标签‘76’) 和数据组 12 (标签‘6C’) 的 1.7 版逻辑数据结构的实施。

在本示例和其他示例中，标签均以**黑体**印刷，长度以斜体表示，值则以罗马体表示。十六进制标签、长度和值均在引号内表示 (‘xx’) 。

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

该示例将完全以十六进制表达：

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

假设的逻辑数据版本 15.99 将编码为：

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

或使用十六进制：

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

A.13.2　EF.DG1 机读区信息标签 = ‘61’ 强制性

该数据元素在模板‘61’中包含证件的强制性机读区 (MRZ) 信息。该模板包含一个数据对象，即数据对象‘5F1F’中的机读区。该机读区数据对象是一个复合数据元素，与证件上打印的 OCR-B 机读区信息相同。

标签	长度	值
‘5F1F’	F	作为复合数据元素的机读区数据对象。(强制性) (该数据元素包含从证件类型到复合 —— 校验位的 13 个原始域。)

机读区数据元素的构成如下所示：

请注意，复合数据元素中并没有使用标签。这些标签仅起到参考的作用。数据对象被解析为单个的数据元素后，这些标签便可使用。

域	内容	强制性/ 选择性	格式	示例	标签 (仅供参考)
1	证件类型	M	F 2A,S	P<	5F03
2	签发国或签发机构	M	F 3A,S	ATA	5F28
3	持证人姓名 [12]	M	F 39ANS	Smith<<John<T	5B
4	证件号码	M	F 9ANS[13]	123456789	5A
5	校验位 —— 证件号码	M	F 1N,S	1 或<	5F04
6	国籍	M	F 3A,S	HMD	5F2C
7	出生日期	M	F 6N,S	740622 (yymmdd)	5F57
8	校验位 —— 出生日期	M	F 1N	2	5F05
9	性别	M	F 1A,S	F、M、或 <	5F35
10	到期日或有效期截止日	M	F 6N	101231 (yymmdd)	59
11	校验位 —— 到期日	M	F 1N	3	5F06
12	选择性数据	M	F14ANS	0121	53
13	校验位 —— 选择性数据 (仅适用于 ID-3 证件)	M	F 1N	5	5F02
14	校验位 —— 复合	M	F 1N	4	5F07

使用这一信息的 DG1 例子如下所示。机读区数据元素的长度为 88 字节 (‘58’)。

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

另一个例子：

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

[12] 关于长度超过 39 个字符的名称进行截取的规则，参见第 1 卷。

[13] 如果证件编号长度超过 9 个字符，在接下来的校验位域 (域 5) 中添加一个 ‘<‘ 字符，剩余的证件编号数位将被置于选择性数据域中，后面紧跟着证件号码的校验位。在上面的例子中，总的文件号码长度为 12 (值=123456789012)，校验位 = 1。

A.13.3　EF.DG2— EF.DG4 (每个数据组都有一个基本文件) 生物特征模板标签 = ‘’75’ ‘63’ ‘76’

DG2—DG4 使用 ISO/IEC 7816-11, 表 C-10 所定义的嵌套式离卡选择，以便有可能存储多个属于同一类的，而且与通用生物特征交换文件格式 (CBEFF) NISTR 6529a 协调一致的生物特征模板。生物特征子报头定义了所出现的生物特征的类型和具体的生物特征。

每个嵌套模板都具有下列结构。

注:

ISO/IEC 7816-11, 表 C-10 的嵌套选择自始至终都要使用，甚至用于单个生物特征模板的编码。后一种情况以编号 n=1 表示。

通用生物特征交换文件格式的默认 OID 被使用。ISO/IEC 7816-11 中所规定的数据元素‘06’并不包含在本结构中。同样，该结构中也没有规定标签的分配权限。

为了实现互用性，每个数据组中记录的第一条生物特征记录须是 ISO/IEC JTC1/SC37 中规定的国际上互用的生物特征数据块。参见第 II 节。

为了保护隐私，可使用 7816-11 附件 D 中定义的安全通信模板对生物特征数据块进行加密。但此类实施已超出了本规范的范畴。

标签	**长度**	**值**				
‘7F61’	**X**	**生物特征信息组模板**				
		标签	**长度**	**值**		
		‘02’	1	整数 —— 本类型生物特征实例数量		
		‘7F60’	X	第 1 个生物特征信息模板		
			标签	**长度**		
			‘A1’	X	生物特征报头模板 (BHT)	
				标签	**长度**	**值**
				‘80’	‘02’	国际民航组织报头版本‘0101’(选择性) —— 通用生物特征交换文件格式赞助方报头格式的版本
				‘81’	‘01-03’	生物特征类型 (选择性)
				‘82’	‘01’	生物特征子类型 (DG2 为选择性，DG3 和 DG4 为强制性)
				‘83’	‘07’	创建日期及时间 (选择性)
				‘84’	‘08’	有效期 (起止时间) (选择性)
				‘86’	‘02’	生物特征参考数据的创建者 (产品标识符) (选择性)
				‘87’	‘02’	格式所有者 (强制性)
				‘88’	‘02’	格式类型 (强制性)
			‘5F2E’ 或 ‘7F2E’	x	生物特征数据 (根据格式所有者编码) 也被称为生物特征数据块 (BDB)。	
		标签	**长度**			
		‘7F60’	X	第 2 个生物特征信息模板		
			标签	**长度**		
			‘A1’	X	生物特征报头模板 (BHT)	

标签	长度	值				
				标签	长度	值
				‘80’	‘02’	国际民航组织报头版本‘0101’(选择性) ——通用生物特征交换文件格式赞助方报头格式的版本
				‘81’	‘01’	生物特征类型 (选择性)
				‘82’	‘01’	生物特征子类型 (DG2 为选择性，DG3 和 DG4 为强制性)
				‘83’	‘07’	创建日期及时间 (选择性)
				‘85’	‘08’	有效期 (起止时间) (选择性)
				‘86’	‘04’	生物特征参考数据的创建者 (产品标识符) (选择性)
				‘87’	‘02’	格式所有者 (强制性)
				‘88’	‘02’	格式类型 (强制性)
			‘5F2E’ 或 ‘7F2E’	x	生物特征数据 (根据格式所有者编码) 也被称为生物特征数据块 (BDB)。	

每个单独的生物特征信息模板结构如下。所给出的生物特征报头模板标签及其值是每项实施必须支持的最低要求。

示例：

一个带签名的人脸生物特征，其生物特征数据块的长度为 12 642 字节 (‘3162’ 字节)，使用 PID 为‘00 01 00 01’的设备编码，使用由模板提供商‘00 0A’所拥有的‘00 04’格式类型，采集于 2002 年 3 月 15 日 (无世界标准时间 (UTC) 偏移)，有效期为 2002 年 4 月 1 日至 2007 年 3 月 31 日。使用 1.0 版的国际民航组织赞助方模板。

模板的总长度为 12 704 字节。模板从 EF.DG2 (SFID 02) 的起始处开始保存。

‘75’ *‘82319EC’*
‘7F61’ *‘823199’*
‘02’ *‘01’* ‘01’
‘7F60’ *‘823191’*
‘A1’ *‘26’*
‘80’ *‘02’* ‘0101’
‘81’ *‘01’* ‘02’
‘83’ *‘07’* ‘20020315133000’
‘85’ *‘08’* ‘2002040120070331’
‘86’ *‘04’* ‘00010001’
‘87’ *‘02’* ‘000A’
‘88’ *‘02’* ‘0004’
‘5F2E’ *‘823162’* ‘……12642 字节的生物特征数据……’

A.13.4 EF.DG5—EF.DG7 (每个数据组都有一个基本文件) 显示的图像模板

标签 = ‘65’ 显示的标准照　　标签 = ‘67’ 显示的签名或通常标记

标签	长度	值
‘02’	1	整数 —— 本类显示图像的实例数量 (在第一个模板中为强制性的，不用于后续的模板中。)
‘5F40’ 或 ‘5F43’	X	显示的标准照 显示的签名或标记

示例：显示的图像数据长度为 2 000 字节的图像模板。模板的长度为 2 008 字节 (‘07D8’) 。

‘65’ *‘8207D8’*

‘02’ *‘01’* 1

‘5F40’ *‘8207D0’* ‘……2000 字节的图像数据……’

特定类型显示图像的如下格式所有者已得到认可。

显示的图像	格式所有者
显示的人脸图像	ISO/IEC 10918，JFIF 选项
显示的指纹	ANSI/NIST-ITL 1-2000
显示的签名/通常标记	ISO/IEC 10918，JFIF 选项

A.13.5　EF.DG8-EF.DG10 机器辅助安全特征，标签 ‘68’ ‘69’ ‘6A’

这三个数据组仍有待于定义。在定义之前，这些数据组可用于临时的专有用途。这些数据元素可使用类似生物特征模板的结构。

标签	长度	值
‘02’	1	整数 —— 该类型模板中的实例数量 (在第一个模板中为强制性的，不用于后续的模板中。)
	x	报头模板。细节待定。

A.13.6　EF. DG11 额外个人详细信息，标签 = 6B

该数据组用于存储有关持证人的额外详细信息。由于该数据组中所有的数据元素都是选择性的，因此要使用一个标签表来定义所出现的数据元素。说明：该模板可包含非拉丁语字符。

标签	长度	值
‘5C’	X	模板中含有数据元素表的标签表
‘5F0E’	X	以持证人本国语言字符书写的持证人完整姓名。根据 Doc 9303 号文件的规则编码。
‘A0’	‘X’	针对特定内容构建的姓名数据对象
‘02’	01	其他姓名的数量
‘5F0F’	X	按 Doc 9303 号文件的规定格式化的其他姓名。该数据对象根据‘02’元素的规定的次数重复出现。
‘5F10’	X	个人号码
‘5F2B’	04	完整的出生日期 yyyymmdd (BCD 编码)
‘5F11’	X	出生地。各个域以‘<’分隔
‘5F42’	X	永久性地址。各个域以‘<’分隔

‘5F12’	X	电话
‘5F13’	X	职业
‘5F14’	X	职别
‘5F15’	X	个人简历
‘5F16’	X	公民身份证明。按照 ISO/IEC 10918 格式压缩的图像
‘5F17’	X	其他有效旅行证件号码。以‘<’分隔
‘5F18’	X	羁押信息

下面的例子显示如下个人详细信息：完整姓名 (John J Smith)、出生地 (Anytown, MN)、永久性地址 (123 Maple Rd, Anytown, MN)、电话号码 1-612-555-1212 和职业 (Travel Agent)。模板的长度为 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’* 1-612-555-1212

‘5F13’ *‘0C’* TRAVEL<AGENT

A.13.7 EF.DG12 额外证件详细信息，标签 = 6C

该数据组用于存储有关证件的额外信息。该数据组中所有的数据元素都是选择性的。

标签	长度	值
‘5C’	X	附带模板中数据元素列表的标签列表
‘5F19’	X	签发机构
‘5F26’	‘04’	签发日期，yyyymmdd (BCD 编码)
‘A0’	X	针对特定内容构建的其他人员数据对象
‘02’	‘01’	其他人员的数量
‘5F1A’	X	根据 Doc 9303 号文件的规则格式化的其他人员的姓名
‘5F1B’	X	背书、备注
‘5F1C’	X	纳税/出境要求
‘5F1D’	X	证件封面的图像。图像符合 ISO/IEC 10918 的规定
‘5F1E’	X	证件封底的图像。图像符合 ISO/IEC 10918 的规定
‘5F55’	‘07’	证件个人化的日期和时间 yyyymmddhhmmss
‘5F56’	X	个人化系统的序列号

下面的例子包含签发机构 (美国)、签发日期 (2002 年 5 月 31 日)、证件上包含的另外一位人员 (Brenda P Smith)。模板的长度为 64 字节 (‘40’)。

‘6C’ *‘40’*

‘5C’ *‘06’* **‘5F19’ ‘5F26’ ‘5F1A’**

‘5F19’ *‘18’* UNITED STATES OF AMERICA

‘5F26’ *‘08’* 20020531

‘5F1A’ *‘0F’* SMITH<<BRENDA<P

A.13.8　EF.DG13 选择性详细信息

该数据组是为存储各国特定数据而保留的。其格式由各国自行确定。

A.13.9　EF.DG15 主动认证公钥信息，标签 = ‘6F’

该数据组包含符合 RFC3280 的主动认证公钥信息。

标签	长度	值
‘6F’	X	参见第 IV 节 —— 公钥基础设施

A.13.10　EF.DG16 需通知的人员，标签 ‘70’

该数据组列出了紧急情况下的通知信息。这个数据组以一系列模板编码，使用的标签‘Ax’。数据不带签名，允许持证人对其进行更新。

标签	长度	值
‘02’	01	模板的数量 (只出现在第 1 个模板中)
‘Ax’	X	模板的起始点，其中 x (x=1, 2, 3……) 每次发生时递增
‘5F50’	‘04’	已记录的日期数据
‘5F51’	X	人员姓名
‘5F52’	X	电话
‘5F53’	X	地址

本例子中包含两个条目：Charles R Smith，Anytown, MN 和 Mary J Brown，Ocean Breeze, CA。模板的长度为 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

A.13.11　EF.SOD 逻辑数据结构安全数据，标签 = ‘77’

该基本文件包含一个符合 RFC3369 的带签名的数据结构。

标签	长度	值
‘77’	X	参见第 IV 节 —— 公钥基础设施

A.14 接受国的应用

Doc 9303 号文件第 1 部分本版中所描述的逻辑数据结构不支持接受国的应用。

A.15 所用标签

15.1 逻辑数据结构中所使用的规范性标签

标签	定义	使用的地方
‘02’	整数	生物特征和显示模板
‘5C’	标签表	EF.COM 和其他多处
‘5F01’	逻辑数据结构版本号	EF.COM
‘5F08’	出生日期 (截取的)	机读区
‘5F09’	压缩图像 (ANSI/NIST-ITL 1-2000)	显示指纹
‘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’	完整姓名，以本国文字字符表示	额外个人详细信息
‘5F0F’	其他名称	额外个人详细信息
‘5F10’	个人号码	额外个人详细信息
‘5F11’	出生地	额外个人详细信息
‘5F12’	电话	额外个人详细信息
‘5F13’	职业	额外个人详细信息
‘5F14’	职位	额外个人详细信息
‘5F15’	个人简历	额外个人详细信息
‘5F16’	公民身份证明 (10918 图像)	额外个人详细信息
‘5F17’	其他有效旅行证件号码	额外个人详细信息
‘5F18’	羁押信息	额外个人详细信息
‘5F19’	发证机构	额外证件详细信息
‘5F1A’	证件上包含的其他人员	额外证件详细信息
‘5F1B’	背书/备注	额外证件详细信息
‘5F1C’	纳税/出境要求	额外证件详细信息
‘5F1D’	证件封面图像	额外证件详细信息
‘5F1E’	证件封底图像	额外证件详细信息
‘5F1F’	机读区数据元素	机读区数据对象

标签	定义	使用的地方
‘5F26’	发证日期	额外证件详细信息
‘5F2B’	出生日期 (8 位)	额外个人详细信息
‘5F2E’	生物特征数据块	生物特征数据
‘5F36’	Unicode 版本级别	EF.COM
‘5F40’	压缩图像模板	显示的标准照
‘5F42’	地址	额外个人详细信息
‘5F43’	压缩图像模板	显示的签名或标记
‘5F50’	已记录的日期数据	需通知的人员
‘5F51’	人员姓名	需通知人员的姓名
‘5F52’	电话	需通知人员的电话号码
‘5F53’	地址	需通知人员的地址
‘5F55’	证件个人化的日期和时间	额外证件详细信息
‘5F56’	个人化系统的序列号	额外证件详细信息
‘60’	通用数据元素	EF.COM
‘61’	机读区数据组模板	
‘63’	指纹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’	额外个人详细信息模板	
‘6C’	额外个人详细信息模板	
‘6D’	选择性详细信息	
‘6E’	留作未来使用	
‘70’	需通知的人员	
‘75’	人脸生物特征数据组模板	
‘76’	虹膜 (眼睛) 生物特征模板	
‘77’	EF.SOD (安全数据的基本文件)	
‘7F2E’	生物特征数据块 (加密的)	
‘7F60’	生物特征信息模板	
‘7F61’	生物特征信息组模板	
‘8x’	针对上下文的标签	通用生物特征交换文件格式 (CBEFF)

标签	定义	使用的地方
‘90’	加密散列码	真实性/完整性代码
‘A0’	针对上下文的结构数据对象	额外个人详细信息 额外证件详细信息
‘Ax’或‘Bx’	重复模板，其中“x”定义重复发生次数	生物特征报头

15.2 对中间处理有用的标签 (资料性)

标签	定义	使用的地方
‘53’	选择性数据	机读区的一部分
‘59’	到期日或有效期截止日	机读区的一部分
‘5A’	证件号码	机读区的一部分
‘5F02’	校验位 —— 选择性数据 (仅适用于 ID-3)	机读区的一部分
‘5F03’	证件类型	机读区的一部分
‘5F04’	校验位 —— 证件号码	机读区的一部分
‘5F05’	校验位 —— 出生日期	机读区的一部分
‘5F06’	校验位 —— 到期日	机读区的一部分
‘5F07’	校验位 —— 复合	机读区的一部分
‘5B’	持证人姓名	机读区的一部分
‘5F28’	签发国或签发机构	机读区的一部分
‘5F2B’	出生日期	机读区的一部分
‘5F2C’	国籍	机读区的一部分
‘5F35’	性别	机读区的一部分
‘5F57’	出生日期 (6 位数字)	机读区的一部分

15.3 留作未来使用的标签 (规范性)

标签	定义	使用的地方
‘5F44’	入境/出境国	旅行记录

标签	定义	使用的地方
‘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/出境指示标记	旅行记录
‘5F48’	停留期长度	旅行记录
‘5F49’	类别 (分类)	旅行记录
‘5F4A’	检查员参考	旅行记录
‘5F4B’	入境/出境指示标记	旅行记录
‘71’	电子签证模板	
‘72’	通关方案模板	
‘73’	旅行记录数据组模板	

A.16　互用性的最低要求　以下是基于非接触式集成电路的紧耦合 (ISO/IEC 14443) 机读旅行证件的最低互用性要求：

- 符合 ISO/IEC 14443 第 1～4 部分和 ISO/IEC 10373-6 的规定，并且考虑到两个标准系列的各个修订版；
- 采用 Type A 或 Type B 信号接口；[14]
- 支持 ISO/IEC 7816-4 所定义的变长记录文件结构；
- 支持 ISO/IEC 7816-4、5 所定义的一种或多种应用及适当命令。

更详细的信息，请参见第 II 节。

A.17　接口设备可使用的命令和命令参数

A.17.1　下面是选择 DF1 应用和从基本文件中检索数据的典型处理顺序。同样的检索 (读取) 过程也用于该专用文件中的所有基本文件。这样一来，便可通过计算数据组的散列值，并且将其与安全数据 EF.SO_D 中检索得到的散列值进行比对，验证 DF1 中数据组的有效性。

典型的动作顺序如下所示：

- 证件进入紧耦合设备 (PCD) 的操作域
- 集成电路酌情使用请求应答-Type A (ATQA) 或请求应答-Type B (ATQB) 对命令请求-Type A (REQA) 或命令请求-Type B (REQB) 做出适当的响应。
- 如果操作域内有多个证件，则紧耦合设备须探测和解决任何可能发生的冲突。
- 与 7816 命令相符合须以如下方式表示：

  —— Type A: SAK (选择确认) bit 6 = 1, bit 3 = 0

[14] 请注意，这表示阅读器 (紧耦合设备) 必须具备读取 Type A 和 B 的能力。

—— Type B: Protocol_Type = “0001”

- 须选择国际民航组织机读旅行证件签发国应用。
- 然后根据需要对基本文件进行选择和读取。将同样的选择和读取过程用于所有的基本文件。命令格式的具体描述见本附录结尾部分。

  —— 在选择基本文件时，可以使用 SELECT 命令。从基本文件读取数据的过程是由一系列基本的 READ BINARY 命令来执行的，每个命令会指定将要读取的后续数据区。该命令是强制性的。

  —— 作为另外一种选择，也可以通过指定第一个 READ BINARY 命令（最初的数据区）中基本文件的短文件标识符来选择基本文件。剩余的数据便可以通过一系列基本的 READ BINARY 命令来读取，每个命令会指定将要读取的后续数据区。注：对这种选择方法的支持是选择性的。

- 首先，读取通用数据文件 EF.COM（短文件标识符 = ‘1E’），该文件包含应用标识符、版本级别和‘60’模板中的标签表。
- EF.COM 中的标签表列出了出现在 DF1 中的数据组（基本文件）。接口设备会确定要读取和使用哪个数据组（EF）。然后对每个基本文件进行访问，以从基本文件中获得该数据组。
- 机读区（MRZ）通常是第一个读取的基本文件（EF）。
- 根据需要，还要对其他基本文件进行读取以获得相应的数据组。
- 接下来要读取 $EF.SO_D$ 来确认从 DF1 中读取的数据组的完整性。请注意，也可以首先读取 $EF.SO_D$ 。

A.18 关于根据 ISO/IEC 14443 Type A 进行 ISO/IEC 14443 Type A 初始化和防冲突操作的细节。

A.18.1 REQA 和 WUPA（(Wake-UP Type A） 紧耦合集成电路卡（PICC）在上电后应处于空闲（IDLE）状态。此时卡片会监听命令并须识别 REQA 和 WUPA 命令。两种命令都在一个（7 位的）短帧内传输。

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

兼容的紧耦合集成电路卡必须对这些命令做出响应；在此环境中，所有其他的值都是禁止使用的。

A.18.2 ATQA 当紧耦合设备（PCD）传送 REQA 命令后，所有处于空闲（IDLE）状态下的紧耦合集成电路卡都须对 ATQA 做出同步响应。

当紧耦合设备（PCD）传送 WUPA 命令后，所有处于空闲（IDLE）或停止（HALT）状态下的紧耦合集成电路卡都须对 ATQA 做出同步响应。

ATQA 响应（ATQA Response）包含两个字节。根据 ISO/IEC 14443-3 的规定，最高有效位（MSB）只包含留作

将来使用和专有位，因此任何兼容的软件都必须忽略这些字节。

最低有效位 (LSB) 的 7 位和 8 位根据下表规定紧耦合集成电路卡的唯一标识符 (UID) 长度：

b8	**b7**	**含义**
0	0	UID 长度：单字节
0	1	UID 长度：双字节
1	0	UID 长度：三字节
1	1	RFU

符合规格的紧耦合集成电路卡必须返回三个有效唯一标识符长度中的任何一个。

最低有效位 1 至 5 表示的是位帧防冲突。必须设定这些位中的一个，而且只能设置一个。第 6 位为留作将来使用，而且不允许任何软件求取其数值。

A.18.3　*防冲突和选择*　根据 ATQA 响应 (ATQA Response) 所确定的唯一标识符的长度，必须为每个级联层发送一个选择命令。如果发生冲突，则须执行防冲突循环。

A.18.3.1　对选择命令，只允许使用‘93’ (级联层 1)、‘95’ (级联层 2) 和‘97’ (级联层 3) 这三个值。

A.18.3.2　在防冲突循环完成后，单个紧耦合集成电路卡将被选择并返回 SAK 响应 (SAK Response)。SAK 包含一个单个字节，该字节中只有两个位是有效的。第 3 位表示唯一标识符还没有完全传输，这意味着必须在下一个级联层上再执行一次选择/防冲突循环。

A.18.3.3　如果第 3 位没有设置，则第 6 位将确定该紧耦合集成电路卡是否符合 ISO/IEC 14443-4。所有用于存储逻辑数据结构数据的紧耦合集成电路卡都必须支持 14443-4，因此该位必须设置。

A.18.4　*选择应答请求* (Request for Answer To Select – RATS)　在防冲突和选择循环执行后，必须向紧耦合集成电路卡发送选择应答请求 (RATS)。RATS 包含一个固定的起始字节‘E0’和一个规定紧耦合设备和 CID 最大帧长度的参数字节。CID 在最低有效半字节中规定；它被用于识别处于激活状态的紧耦合集成电路卡。

最高有效半字节 (FDSI) 根据如下转换方案包含最大帧长度 (FSD)。

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

为了进行逻辑数据结构数据的传输，符合规格的阅读器必须支持 256 字节的帧长度，因此参数数字中最高有效半字节必须是‘8’。

A.18.5　*选择应答*　选择应答规定有关紧耦合集成电路卡能力的信息。它包含最多 3 个接口字节。第一个接口字节 TA (1) 包含紧耦合集成电路卡的位速率能力。第 2 个接口字节 TB (1) 传达用于定义帧的等待时间和起始帧的保护

时间的信息。第 3 个接口字节 TC (1) 规定协议参数。如果紧耦合集成电路卡支持 NAD，则最低有效字节必须是 1。如果紧耦合集成电路卡支持 CID，则第 2 个字节必须是 1。

所有其他的位都是 RFU，而且任何符合规格的软件都必须忽略它们。

紧跟接口字节的是历史字节。它们包含有关紧耦合集成电路卡的一般性信息，而且任何符合规格的软件都不应求取其数值。

A.19 关于 ISO/IEC 7816 命令格式和参数选项的详细信息

A.19.1 应用选择

应用必须根据其文件标识符或其应用名来选择。当选择一项应用后，即可对该应用中的文件进行访问。

注：应用名必须是唯一的。因此，每当需要时便可使用应用名对应用加以选择。

A.19.2 选择主文件:

CLA	**INS**	**P1**	**P2**	**Lc**	**Data**	**Le**
‘00’	‘A4’	‘00’	‘00’	—	Empty	—

A.19.3 根据应用标识符选择应用

须使用专用文件名来选择一项应用。APDU 命令的参数如下所示。

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

A.20 使用 SELECT 命令选择基本文件

文件必须根据其文件标识符进行选择。当使用文件标识符对文件进行选择时，必须确保在其内部保存这些文件的应用此前已经被选择过。

CLA	**INS**	**P1**	**P2**	**Lc**	**Data**	**Le**
‘00’	‘A4’	‘02’	‘0C’	‘02’	FileID	—

A.21 从基本文件中读取数据

读取数据的方法主要有两种：第一种是通过选择文件，然后读取数据 (建议使用该方法)；而第二种方法是使用短文件标识符直接读取数据。

A21.1.1　读取选择文件 (透明文件) 的数据

CLA	INS	P1	P2	Lc	Data	Le
‘00’	‘B0’	偏移理的最高有效字节 (Offset MSB)	偏移量的最低有效字节 (Offset LSB)	—	—	最大返回长度

P1 和 P2 的定义：

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

A21.1.2　使用短文件标识符 (透明文件) 读取数据

CLA	INS	P1	P2	Lc	Data	LE
‘00’	‘B0’	SFI	偏移量的最低有效字节 (Offset LSB)	—	—	最大返回长度

P1 和 P2 的定义：

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

A.22　ISO/IEC 7816 在逻辑数据结构中的用法示例

A.22.1　使用文件选择 (File Selection) 读取机读区

下面的顺序可用于读取数据组 1 (机读区) 的数据。

CLA	INS	P1	P2	Lc	数据	Le	说明
‘00’	‘A4’	‘04’	‘0C’	‘07’	‘A0 00 00 02 47 10 01’	—	选择签发方的应用
‘00’	‘A4’	‘02’	‘0C’	‘02’	‘01 01’	—	选择 DG1
‘00’	‘B0’	‘00’	‘00’	—	—	‘00’	读取最多 256 个字节

A.22.2 读取数据组 2

A.22.2.1 下面的顺序可用于读取数据组 2 (编码人脸) 中的数据。模板的长度设定为 12 543 字节。整个数据区的长度为 12 547 字节 (模板标签增加一个字节，长度域增加三个字节)。这样就需要 49 个字块，每个字块 256 个字节，外加由 3 个字节组成的最后一个字块。

A22.2.2 模板中接下来的部分是通过逐步递增偏移量读取的，每次递增的偏移量为 256 字节 ('01 00')。需要读取的数据总量由模板的长度决定。建议最后的 READ BINARY 命令只为剩余的数据量发出。因此，最后的偏移量为 '31 00'。

CLA	**INS**	**P1**	**P2**	**Lc**	**Data**	**Le**	**说明**
'00'	'A4'	'04'	'0C'	'07'	'A0 00 00 02 47 10 01'	—	选择签发方的应用
'00'	'A4'	'02'	'0C'	'02'	'01 02'	—	选择 DG2
'00'	'B0'	'00'	'00'	—	—	'00'	读取第一个 256 字节
'00'	'B0'	'01'	'00'	—	—	'00'	读取下一个 256 字节
'00'	'B0'	'02'	'00'	—	—	'00'	读取下一个 256 字节
'00'	'B0'	'03'	'00'	—	—	'00'	:

A22.3 当连续读取一个以上数据组时，签发者应用只能被选择一次 (在读取第一个文件之前)。

A.22.4 使用全局 SFI 读取机读区数据

CLA	**INS**	**P1**	**P2**	**Lc**	**Data**	**Le**	**说明**
'00'	'B0'	'81'	'00'	—	—	'00'	直接读取 256 字节

A22.5 使用全局 SFI 读取数据组 2

可与 SFI 结合在一起使用 READ BINARY 命令来读取文件中的第一个 256 字节。后续的字节只能使用“标准”的 READ BINARY 命令来读取。

CLA	**INS**	**P1**	**P2**	**Lc**	**Data**	**Le**	**说明**
'00'	'B0'	'82'	'00'	—	—	'00'	直接读取 256 字节
'00'	'B0'	'01'	'00'	—	—	'00'	读取下一个 256 字节
'00'	'B0'	'02'	'00'	—	—	'00'	读取下一个 256 字节
'00'	'B0'	'03'	'00'	—	—	'00'	:

A.23 长度大于 32 767 字节的基本文件 (EF)

A.23.1 基本文件的最大长度通常是 32 767 字节，但一些集成电路支持更大的文件。当偏移量超过 32 767 时，要想访问数据区就需要使用不同的 READ BINARY 参数选项和命令格式。这种命令格式应当在模板的长度和是否需要访问扩展数据区的数据确定之后再使用。例如，如果数据区包含多个生物特征数据对象，可能就不需要读取整个数据区。当数据区的偏移量大于 32 767 字节时，则须使用该命令格式。偏移量被放在命令域中，而不是在参数 P1 和 P2 中。

CLA	**INS**	**P1**	**P2**	**Lc**	**Data**	**Le**	**说明**
‘00’	‘B1’	‘00’	‘00’	Var.	编码的偏移量 TLV 格式	‘00’	读取长度大于 32 767 字节的文件

数据域中编码的偏移示例：

偏移：‘FF FF’被编码为‘54 02 ff ff’

A23.2　后续的 READ BINARY 命令须在数据域中规定偏移量。最后一个 READ BINARY 命令应请求剩余的数据区。

A.24　ASN.1 BER 长度编码规则

范围	字节编号	第 1 个字节	第 2 个字节	第 3 个字节
0 至 127	1	二进制值	无	无
128 至 255	2	‘81’	二进制值	无
256 至 65 535	3	‘82’	二进制值 MS 字节　　LS 字节	
MS = 最高有效的字节；LS = 最低有效的字节				

注：引号 (‘ ’) 用于以目视方式分隔十六进制字符。这些符号不在逻辑数据结构中编码。

A.24.1　以上文定义的规则为基础的示例：

示例 1：长度三十九 (39) 在十六进制表达方法中被编码为‘27’。

示例 2：长度一百九十九 (199) 在十六进制表达方法中被编码为‘81C7’。

示例 3：长度一千 (1 000) 在十六进制表达方法中被编码为‘8203E8’。

A.25　生物特征子特征编码：下表显示的是子特征的编码方案：

b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**生物特征子类型**
0	0	0	0	0	0	0	0	无信息
						0	1	右
						1	0	左
			0	0	0			无意义
			0	0	1			拇指
			0	1	0			食指
			0	1	1			中指
			1	0	0			无名指
			1	0	1			小指
x	x	x						留作未来使用

第IV节

提供ICC只读访问的机读旅行证件的公钥基础设施

1. 范围

1.1 本节所提供的规范是为了使各国和供应商能够实施一种基于专用基础设施的证件认证方案，该基础设施为应用现代公钥基础设施(PKI)方案而构建，目的在于在提供 ICC 只读访问的机读旅行证件 ("MRTD") 中实现和使用数字签名。

1.2 以必须在 2006 年有可能得到有效实施为前提，这些规范并不试图规定在每个国家全面实施复杂的公钥基础设施结构，而是试图提供一种实施的方法，以便各国能够在几个方面 (例如主动或被动认证、防不当读取和访问控制或自助通关) 进行选择，从而有可能在不与整体框架发生冲突的情况下，逐步地实施额外特征。

2. 假定条件

2.1 假定读者熟悉公钥密码技术和公钥基础设施所提供的概念和机制。

2.2 虽然使用公钥密码技术增加了实施使用集成电路的护照的复杂性，但这项技术是有附加价值的，即：它为一线的边境控制点提供了确定护照证件真伪的另一种措施。如果使用这种技术是确定真伪的唯一措施，则**不应该**将其作为一个单一的决定因素来依赖。

2.3 假定以数字形式存储的人脸图像不属于隐私敏感信息。机读旅行证件持有人的脸部图像也打印在机读旅行证件上，并且可以一目了然地看到。

2.4 以数字形式存储的指纹和/或虹膜图像是额外的生物特征，各国**可以**选择用于国内。它们一般被认为是隐私敏感信息，因此需要根据签发国的国家法律得到保护。

2.5 由国际民航组织或任何其他单一的中心性组织为任何国家分配、保存或管理安全私钥都是不可行的。尽管参加国之间有很多战略联盟，这样做仍不能被认为是一个可信赖的解决方案。

2.6 如果由于诸如证书被撤销或无效的签名验证等造成芯片上的数据不能使用，或者如果芯片被有意留作空白(如本节 7.1.1 中所述)，机读护照未必就失效。在这种情况下，接受国**可以**依赖证件的其他安全特征达到确认的目的。

2.7 证书撤销表 (CRL) 的使用仅限于国家签名 CA 证书和证件签名者证书。证书撤销表不适用于单独的证件安全对象和针对具体证件的主动认证密钥对。

3. 术语

3.1 本节中的"**须**"、"**要求**"、"**应该**"、"**建议**"和"**可以**"等关键词的解释与参考文件 4 (RFC 2119，S. Bradner, "*Key Words for Use in RFCs to Indicate Requirement Levels*" *BCP 14, RFC 2119, March 1997.)* 中的描述相同。

3.2 当实施**选择性**特征时，它们**须**按照本节的描述予以执行。

3.1 认证机构、密钥和证书

下述密钥和证书与本节内容密切相关：

名称	缩写	注释
国家签名 CA	CSCA	
国家签名 CA 证书	C_{CSCA}	由国家签名 CA 颁发 (自签)。 附有国家签名 CA 公钥 (KPu_{CSCA})。 存储在查验系统中。
国家签名 CA 私钥	KPr_{CSCA}	签署证件签名者证书 (C_{DS})。 存储在签发国 (高度) 安全的环境中。
国家签名 CA 公钥	KPu_{CSCA}	用于验证证件签名者证书 (C_{DS}) 的真实性。
证件签名者	DS	
证件签名者证书	C_{DS}	由国家签名 CA (CSCA) 颁发。 附有证件签名者公钥 (KPu_{DS})。 存储在查验系统和/或机读旅行证件的芯片中。
证件签名者私钥	KPr_{DS}	签署证件安全对象 (SO_D)。 存储在签发国 (高度) 安全的环境中。
证件签名者公钥	KPu_{DS}	用于验证证件安全对象 (SO_D) 的真实性。
证件安全对象	SO_D	一种 RFC3369 CMS 签名的数据结构，由证件签名者 (DS) 签署。 附有逻辑数据结构数据组的散列值。 存储在机读旅行证件的芯片上。 **可以**附有证件签名者证书 (C_{DS})。
主动认证 私钥	KPr_{AA}	**选择性**。 以机读旅行证件芯片的主动认证机制进行签名计算。 存储在芯片的安全存储器内。
主动认证 公钥	KPu_{AA}	**选择性**。 以机读旅行证件芯片的主动认证机制进行签名验证。

名称	缩写	注释
证件的基本访问密钥	K_{ENC} 和 K_{MAC}	**选择性**。 获得访问机读旅行证件公开数据的权利并实现机读旅行证件芯片与查验系统之间的安全通信。

3.2　缩写

缩写	
APDU	应用协议数据单元
BLOB	二进制大型对象
CA	认证机构
CRL	证书撤销表
DO	数据对象
ICAO	国际民航组织
ICC	集成电路卡
IFD	接口装置
LDS	逻辑数据结构
MRTD	机读旅行证件
MRZ	机读区
NTWG	新技术工作组
PICC	紧耦合集成电路卡
PCD	紧耦合装置
PKI	公钥基础设施
PKD	公钥簿
SM	安全通信
TAG	技术咨询组

4.　参考文件

下述文件用作本节的参考：

公钥基础设施威胁评估，ICAO-NTWG, 9 月　日，最终版，2003 年 10 月 3 日。

技术报告：机读旅行证件公钥基础设施数字签名，第 4 版。

技术报告：逻辑数据结构开发 —— 用于选择性扩容技术的逻辑数据结构。

RFC 2119, S. Bradner: “在 RFC 中使用的表明要求等级的关键词”，BCP 14, RFC 2119, 1997 年 3 月。

RFC 3279, W. Polk R. Housley, 和 L. Bassham: “因特网 X.509 公钥基础设施证书和证书撤销表 (CRL) 概要中使用的算法和标识符”, 2002 年 4 月。

RFC 3280, R. Housley, W. Polk, W. Ford, 和 D. Solo: “因特网 X.509 公钥基础设施证书和证书撤销表 (CRL) 概要”, RFC 3280, 2002 年 4 月。

RFC 3447, J. Jonsson 和 B. Kaliski: “公钥加密标准 (PKCS) #1: RSA 加密规范 2.1 版”, 2003 年 2 月。

FIPS 180-2, 联邦信息处理标准出版物 (FIPS PUB) 180-2, 安全散列标准, 2002 年 8 月。

FIPS 186-2, 联邦信息处理标准出版物 (FIPS PUB) 186-2 (+ 变更通知), 数字签名标准, 2000 年 1 月 27 日 (代替 1998 年 12 月 15 日的 FIPS PUB 186-1。)

FIPS 186-3, 联邦信息处理标准出版物 (FIPS PUB) 186-3, 数字签名标准。

X9.62, “金融服务业的公钥加密: 椭圆曲线数字签名算法 (ECDSA)”, 1999 年 1 月 7 日。

ISO/IEC 7816-4:2005 识别卡 —— 集成电路卡 —— 第 4 部分: 互换的组织、安全和命令。

ISO/IEC 7816-8, 识别卡 —— 集成电路卡 —— 第 8 部分: 安全操作的命令。

RFC 3369, 密码信息的句法, 2002 年 8 月。

ICAODoc 9303 号文件, 机读旅行证件，第 5 版 —— 2003 年。

ISO/IEC 3166, 代表国家及其下属行政区名称的代码 —— 1997 年。

ISO/IEC 9796-2, 信息技术 —— 安全技术 —— 提供报文恢复的数字签名方案 —— 第 2 部分: 基于整数因数分解的机制，2002 年。

ISO 11568-2:2005 —— 银行业 —— 密钥管理 (零售) —— 第 2 部分: 对称密码、其密钥管理和寿命周期 (只有英文版本)。

5. 概述

5.1 公钥基础设施方案的原则在其使用中获得了不断发展，当应用于现代环境中时已经变得十分复杂。它们主要用在因特网事务处理中。在因特网事务处理中，密钥在广泛的用户和代理商之间必须是可信的，这就导致形成了复杂的密钥证书系统。在此系统中，公钥以“证书”的形式颁发，“证书”由被称为认证机构(CA)的可信签发机构进行数字签名。对这些 CA 机构的信任再由信任分级结构中的上一级进一步验证，分级结构中的每一级为其下一级颁发密钥和签署证书。这种分级结构中的最高层被称之为“根 CA”。不同的分级结构相互交叉认证，以确立对彼此颁发的密钥的信任。

5.2 一个复杂的因素就是需要有一个证书撤销表 (CRL)，用以表明密钥 (证书) 不管是出于何种原因已经失效的情况。事实上，通过撤销某个证书并在证书撤销表中公布这一撤销信息，该证书的颁发者向接受方通报该证书的内容不再可信。每进行一项事务的处理都需要对证书进行验证，这常常意味着要多次访问不同数据库中的认证机构记录和证书撤销表记录。这是一个复杂的要求。

5.3　符合国际民航组织标准的机读旅行证件的操作环境不同于上述的商业环境。在机读旅行证件的操作环境中，公钥撤销问题是以不同的方式表现的 (与单个用户相比较)，因为万一出现在某段时间里用来为很多机读旅行证件签名的任何国家的私钥被泄漏的情况，也不能否认这些证件确实是使用该密钥签署的。这些 (有效) 证件依然由持证人在旅行时使用。所使用的数字签名是打算在机读旅行证件的整个有效期内持续使用的，而不只是用于每天的事务处理。如果出现密钥泄漏的情况，**须**使用告警机制，提醒各国更严密地检查这些证件。

5.4　因此，Doc 9303 号文件的本卷提出了一个定制方法，它将使机读旅行证件的广大用户群体能够快速跟踪这一应用在 ICC 只读机读旅行证件上的实施情况，并在不试图涉及更大的公钥基础设施政策问题和复杂的分级结构的情况下利用它的好处。证书向各成员国分发公钥 (证书) 的建议方法，都用于安全目的，并且基础设施是按照国际民航组织的需要而定制的。

5.5　责任

国际民航组织的公钥基础设施的应用程序在完全对等的用户环境下运作，各国在机读旅行证件和安全事宜上是独立自主的。然而，应该有一个共同接受的高效手段，使所有参加国在任何时候都能够对现有的所有未到期机读旅行证件的有效公钥集进行共享和更新，这是这一方案必不可少的一部分。

5.5.1　签发国

每一参加国**须**建立自己的安全设施，为不同时期生成密钥集；这种密钥集**须**被用来计算用于签署证书的数字签名。这些系统或设施**须**通过固有的设计和硬件安全设施得到妥善的保护，防止外部或未经授权的访问。

国家签名 CA

将被嵌入密钥生成功能的 CA 分级结构只有在涉及到分发给接受国的证书时才与本节相关。被分发的最顶层证书**须**作为接受国的信任点。在本节中，这个证书被称为国家签名 CA 证书 (C_{CSCA})。国家签名 CA 证书 (C_{CSCA})**须**由国家签名 CA(CSCA)自签和颁发。

建议国家签名 CA 密钥对 (KPu_{CSCA}, KPr_{CSCA}) 应由签发国在受到高度保护的离线 CA 基础设施上生成和存储。

国家签名 CA 证书 (C_{CSCA}) **须**通过严格保密的外交手段进行分发 (带外分发)。

由每一国家生成的每一个国家签名 CA 证书 (C_{CSCA}) 还**须**提交给国际民航组织 (用于确认证件签名者证书 (C_{DS}))。

国家签名 CA 私钥 (KPr_{CSCA}) 被用来签署证件签名者证书 (C_{DS})。

附录 1 规定了证书概要。

证件签名者

建议证件签名者密钥对 (KPu_{DS}, KPr_{DS}) 应由签发国在受到高度保护的 CA 基础设施上生成和存储。

每一国家生成的每一个证件签名者证书 (C_{DS}) **须**提交给国际民航组织，并且**可以**存储在机读旅行证件的芯片中。

证件签名者私钥被用来签署证件安全对象 (SO_D)。

每一国家生成的每一个证件安全对象**须**存储在相应的机读旅行证件的芯片中。

附录 1 规定了证书概要。

证书撤销

在发生意外事件 (例如密钥泄漏) 时，签发国可以撤销证书。这类撤销**须**在 48 小时之内以双边形式通告所有其他的参加国和国际民航组织的公钥簿。

在没有意外事件发生的情况下，签发国**应该**至少每 90 天以双边形式向其他参加国和国际民航组织的公钥簿分发“例行”的证书撤销表。

5.5.2 国际民航组织公钥簿 (PKD)

为了有效地共享所有国家的证件签名者证书 (C_{DS})，国际民航组织将开发并向所有参加国提供公钥簿服务。该服务**须**接收来自各国的有关公钥的信息，将其储存在公钥簿中，并允许所有其他国家访问。

对储存在公钥簿中的证书表进行更新的访问**须**限制在参加国的范围之内。

对阅读公钥簿 (例如为下载公钥簿信息) **不得**设置访问控制。

国家签名 CA 证书

国家签名 CA 证书 (C_{CSCA}) 不是国际民航组织公钥簿服务的一部分。但是，公钥簿在发布参加国提交的证件签名者证书之前，**须**使用国家签名 CA 证书 (C_{CSCA}) 验证其真实性和完整性。

国际民航组织不允许访问国家签名 CA 证书 (C_{CSCA})。

证件签名者证书

国际民航组织公钥簿旨在作为一个存储库，存储所有参加国在任何时候使用的证件签名者证书 (C_{DS})。这包括任何时候用来签名的正在使用的证书和已经不再使用但对已签发的机读旅行证件依然有效的证书。

国际民航组织公钥簿将是所有这些证件签名者证书 (C_{DS}) 的主要分发机制，因此所有参加国**须**对其进行补充并随时加以更新。

当其他当事方 (除参加国以外) 需要使用存储在公钥簿中的某个签发国的公钥信息去验证数字存储的机读旅行证件数据的真实性时，也**须**向他们提供。

证书撤销表

公钥簿也是每一参加国发布的所有证书撤销表 (CRL) 的存储库。尽管各国**须**主要以双边方式分发证书撤销表，但它们也**须**向公钥簿传送证书撤销表。因此，国际民航组织公钥簿将成为证书撤销表的辅助分发机制。

5.5.3　接受国

公钥簿服务的用户**须**定期访问国际民航组织的公钥簿，下载新的密钥证书信息，供其内部边检系统存储和使用。

同样，在高速缓冲存储器内保存一个当前证书撤销表，即一套当前的证书撤销表是接受国的责任。该表**须是**从国际民航组织公钥簿下载信息的一部分。

每一接受国**须**负责国家签名 CA 证书 (C_{CSCA})、证件签名者证书 (C_{DS}) 和证书撤销表向其查验系统的内部分发。

作为信任点在其边检系统中安全存储国家签名 CA 证书 (C_{CSCA}) 是国家的责任。

5.5.4　其他当事方

凡配有适当设备者，都能读取机读旅行证件上的芯片内容，但只有配备了适当的公钥证书和证书撤销表的当事方才能验证芯片内容的真实性和完整性。这些当事方**可以**从国际民航组织的公钥簿中获取这方面的信息，但是他们需要通过其他途径获取国家签名 CA 证书 (C_{CSCA}) 集，因为这些证书不由国际民航组织公钥簿发布。

5.6　数据认证

5.6.1　被动认证

除了逻辑数据结构数据组外，芯片上还包含一个证件安全对象 (SO_D)。该对象由签发国数字签名，并包括逻辑数据结构内容的散列表示 (见本节第 7 段)。

配备有每一国证件签名者公钥 (KPu_{DS}) 的查验系统，或者已从机读旅行证件上读取了证件签名者证书 (C_{DS}) 的查验系统将能验证证件安全对象 (SO_D)。这样，通过证件安全对象 (SO_D) 的内容，逻辑数据结构内容就会得到认证。

这种验证机制不需要机读旅行证件中芯片的处理能力。因此，它被称作对芯片内容的“被动认证”。

被动认证能证明证件安全对象 (SO_D) 和逻辑数据结构的内容是真实的和没有被修改的。它不能防止对芯片内容的精确复制或对芯片的替换。

因此，被动认证系统**应该**辅之以对机读旅行证件的附加物理查验。

被动认证在 7.2.2 中有具体规定。

5.6.2　主动认证

签发国**可以**选择保护其机读旅行证件的芯片不被替换。通过采用主动认证机制能够做到这一点。

如果得到支持，主动认证机制**须**能通过查验系统和机读旅行证件芯片之间的询问—响应协议，确保芯片没有被替换。

为此，芯片包含有其自身的主动认证密钥对 (KPr_{AA} 和 KPu_{AA})。数据组 15 (公钥 (KPu_{AA}) 信息) 的散列表示被

存储在证件安全对象 (SO_D) 中，因此可由签发者的数字签名进行认证。相应的私钥 (KPr_{AA}) 被储存在芯片的安全存储器中。

通过使用机读旅行证件的主动认证密钥对 (KPr_{AA} 和 KPu_{AA})，结合询问—响应对视读机读区进行认证 (利用证件安全对象 (SO_D) 中的散列的机读区)，查验系统能够验证出所读取的证件安全对象 (SD_D) 来自存储在真实机读旅行证件中的真实芯片。

主动认证需要机读旅行证件芯片的处理能力。

主动认证在 7.2.2 中有具体规定。

5.7 访问控制

将配备有无触点芯片的机读旅行证件与传统的机读旅行证件相比较，显现出两个不同：

- 无需打开文件就能对存储在芯片中的数据进行电子阅读 (不当读取)。
- 在芯片和阅读器之间的未加密通信在几米之内能被窃听到。

虽然有物理措施能够应对不当读取行为，但解决不了窃听的问题。因此，各国理所当然地**可以**选择实施一种基本访问控制机制，这种访问控制机制实际上需要持证人知道他的机读旅行证件上储存在芯片中的数据正在通过一种安全的方式被读取。这种基本访问控制机制能够防止不当读取，也能够防止窃听。

这种推荐的最佳做法旨在通过防止不当读取和窃听，保护隐私和承认旅行者的这种受保护的权利。

这个访问控制机制是**选择性**的。本节中关于基本访问控制和安全通信的描述和规范只适用于支持该项选择的机读旅行证件和查验系统。如果得到支持，该机制**须**确保芯片上的内容只有当持证人在知情的情况下提供机读旅行证件的时候才能被读取。

受基本访问控制机制保护的芯片拒绝对其内容的访问，除非查验系统能够证明对芯片的访问是被授权的。这种证明在询问—响应协议中给出，查验系统要证明它知道根据机读区的信息推导出的芯片所专有的证件基本访问密钥 (K_{ENC} 和 K_{MAC})。

查验系统**须**首先得到这方面的信息才能够阅读芯片。信息需要从机读旅行证件 (例如从机读区) 中以光学/目视的方式获得。在机读区不能进行机器阅读时，检查员还**须**以人工方式将该信息输入到查验系统中。

另外，在成功地认证了查验系统之后，**要求**芯片采用安全通信技术，为查验系统和机读旅行证件的芯片之间的通信信道加密。

假定证件基本访问密钥 (K_{ENC} 和 K_{MAC}) 不能从合上的证件上得到 (因为它们要通过以光学方式阅读机读区获得)，可以被认为护照是在知情的情况下送交查验的。由于信道加密，要对通信进行窃听需要付出巨大的努力。

访问控制机制在 7.2.2 中有具体规定。

5.8　额外生物特征的安全性

存储在芯片上的被确定为全球互用的强制性最低限度的个人资料，是机读区和数字存储的持证人的人脸图像。当机读旅行证件被打开供查验时，这两项内容都可以直观地看到 (阅读)。

除了数字存储的人脸图像是全球互用的主要生物特征外，国际民航组织已经认可使用数字存储的指纹和/或虹膜图像。为供本国或双边使用，各国**可以**选择存储模板和/或选择限制访问或加密该资料，具体由各国自定。

对访问这些比较敏感的个人资料**应该**施加更多的限制。这可以通过两种途径实现：扩展访问控制或数据加密。尽管在本节提到了这些选择，但国际民航组织现在没有在这些领域提出或规定任何标准或做法。

5.8.1　扩展访问控制

选择性扩展访问控制机制与已经描述过的基本访问控制机制相类似，但是，对于扩展访问控制，使用的是证件扩展访问密钥集，而不是证件基本访问密钥 (K_{ENC} 和 K_{MAC})。

对 (芯片专用的) 证件扩展访问密钥集的界定由执行国自己做。证件扩展访问密钥集**可以**由例如源自机读区和国家主控密钥的对称密钥构成，或者由附带相应的卡验证证书的非对称密钥对构成。

扩展访问控制需要机读旅行证件芯片的处理能力。

5.8.2　加密

为限制访问额外生物特征，还**可以**对它们进行加密。为能够解密加密的数据，查验系统**须**配备解密密钥。对加密/解密算法和将要使用的密钥的界定由执行国自己做，不在本文件的范围之内。

6.　保护机读旅行证件电子数据的安全 (摘要)

除了通过数字签名进行被动认证外，各国**可以**选择提供额外的安全保障，采用更加复杂的方法保护芯片及其数据的安全。可以适当地结合表 IV-1 给出的选择，根据现有的 ISO/IEC 标准实现额外的安全保障。

表 IV-1　基线安全方法

方法	签发者	查验系统	优点	缺点
被动认证 （5.6.1）	**M**	**M**	证明证件安全对象和逻辑数据结构的内容是真实的和没有被改变的。	不能防止精确的复制或芯片替换。 不能防止未经授权的访问。 不能防止不当读取。
高级安全方法				
常规机读区（OCR-B）和基于芯片的机读区（LDS）之间比对	N/A	O	证明芯片内容和实际的机读旅行证件是一体的。	增加（少许的）复杂性。 不能防止对芯片和常规的证件进行精确的复制。

方法	签发者	查验系统	优点	缺点
主动认证 (5.6.2)	O	O	防止复制证件安全对象，并能证明它是从真实的芯片上读取的。 证明芯片没有被替换。	增加复杂性。 需要处理器-芯片。
基本访问控制 (5.7)	O	O	防止不当读取和滥用。 防止窃听机读旅行证件和查验系统之间的通信 (当被用来建立加密的会话信道时)。	不能防止精确的复制或芯片替换 (还需要复制常规证件)。 增加复杂性。 需要处理器-芯片。
扩展访问控制 (5.8.1)	O	O	防止对额外生物特征进行非授权的访问。 防止不当读取额外生物特征。	需要附加的密钥管理。 不能防止精确的复制或芯片替换 (还需要复制常规证件)。 增加复杂性。 需要处理器-芯片。
数据加密 (5.8.2)	O	O	保护额外生物特征的安全。 不需要处理器-芯片。	需要复杂的解密密钥管理。 不能防止精确的复制或芯片替换。 增加复杂性。

选择使用先进的安全方法的国家所签发的机读旅行证件将完全符合国际民航组织的要求，并被认为达到了全球互用性标准。

7. 规范

7.1 机读旅行证件的制作和个人化

7.1.1 机读旅行证件的制作和个人化是签发国的责任。

然而，**建议**各国采取措施保护芯片运输和存储的安全、机读旅行证件芯片嵌入的安全，以及个人化过程的安全。

本版的 Doc 9303 号文件第 1 部分第 2 卷基于这样的假设，即在个人化之后，不再向机读旅行证件上写入内容。因此，个人化过程**应该**把锁定芯片作为最后一个步骤。

如果一个国家不具备作为个人化的一部分为机读旅行证件的数据进行签名的公钥基础设施，而证件的签发又不能耽搁，**建议**将机读旅行证件的芯片留作空白并锁定。为此，护照上**应该**有一个打印的适当说明。这可能是一种特殊情况。

7.1.2　存储在芯片上的信息

机读旅行证件芯片上的内容图示如下：

MF
|
|---------DF — LD_S　　要求的
　　|
　　|---------K_{ENC}　　选择性的
　　|
　　|---------K_{MAC}　　选择性的
　　|
　　|---------KPr_{AA}　　选择性的
　　|
　　|---------EF — COM　　要求的
　　|
　　|---------EF — SO_D　　要求的
　　|
　　|---------EF — Datagroup-1 (MRZ)　　要求的
　　|
　　|---------EF — Datagroup-2 (编码人脸)　　要求的
　　//
　　|---------EF — Datagroup-n　　选择性的

K_{ENC} , K_{MAC}

(选择性) 证件基本访问密钥 (K_{ENC} 和 K_{MAC}) 存储在专用文件中。 根据机读区的信息对这些密钥进行的推导在 7.2.2 中有描述。

KPr_{AA}

(选择性) 主动认证私钥 (KPr_{AA}) 存储在专用文件中。

EF-COM

见第 III 节，*逻辑数据结构*。

EF-数据组 1-n

见第 III 节，*逻辑数据结构*。

EF-SO_D

EF-SO_D 包含证件安全对象(SO_D)。证件安全对象 (SO_D) 包含正在使用的逻辑数据结构数据组的散列值。(这个结构被称作逻辑数据结构安全对象 (SO_{LDS}.))。证件安全对象 (SO_D) 的规范，包括逻辑数据结构安全对象 (SO_{LDS}) 的 ASN.1 格式化例子，见附录 3。

7.2 查验

7.2.1 查验系统

为了支持所需要的功能和能在出示的机读旅行证件上实现的规定选择，查验系统需要满足某些先决条件。

用于机读旅行证件基本访问控制

尽管所述的基本访问控制是选择性的，但支持它的查验系统**须**满足下述先决条件：

1. 查验系统要配备机读区阅读器或某种类型的人工输入装置 (例如键盘)，以便根据机读旅行证件上的信息推导出证件基本访问密钥 (K_{ENC} 和 K_{MAC})。

2. 当向包含用安全通信进行的通信信道加密的系统提供带有基本访问控制的机读旅行证件时，安全查验系统软件要支持 7.2.2 中描述的协议。

用于被动认证

为了对存储在机读旅行证件芯片上的数据进行被动认证，查验系统需要了解签发国的密钥信息：

1. 每个参加的签发国的国家签名CA证书(C_{CSCA})**须**存储在查验系统中。

2. 每个参加的签发国的证件签名者证书(C_{DS}) **须**存储在查验系统中。

用于主动认证

查验系统对主动认证的支持是**选择性的**。

如果查验系统支持**选择性的**主动认证，**要求**查验系统具有阅读直观机读区的能力。

如果查验系统支持**选择性的**主动认证，查验系统软件**须**支持 7.2.2 中描述的主动认证协议。

用于对额外生物特征的扩展访问控制

对**选择性**额外生物特征实施保护取决于一个国家的内部规范或国与国之间就共享该信息商定的双边规范。

用于对额外生物特征的解密

对**选择性**额外生物特征实施保护取决于一个国家的内部规范或国与国之间就共享该信息商定的双边规范。

7.2.2 查验流程

本段按照事件发生的顺序描述查验工序的的流程。对**选择性的**和**要求的**步骤都作出了描述。

机读旅行证件的基本访问控制（选择性）

当带有**选择性**基本访问控制机制的机读旅行证件提供给查验系统时，使用以光学或目视方式读取的信息导出证件基本访问密钥 (K_{ENC} 和 K_{MAC})，以便访问芯片和在机读旅行证件芯片与查验系统之间建立安全通信信道。

支持基本访问控制的机读旅行证件芯片**须**对非授权的阅读企图 (包括对逻辑数据结构中的(被保护的)文件的选择) 作出“没有满足安全状态”(0x6982) 的响应。为认证查验系统，**须**进行下述步骤：

1. 查验系统按照Doc 9303号文件第1部分第1卷中第9段和15段的描述，使用OCR-B阅读器从机读区读取“MRZ_information”，该信息由并置的证件号码、出生日期和到期日构成，并包括它们各自的校验位。或者可以将所需的信息敲上去。在这种情况下，所需的信息**须**随机读区内的显示打入。这一“MRZ_information”SHA-1散列中的最高有效16字节被用作密钥种子，通过附录5.1描述的密钥衍生机制导出证件基本访问密钥。

2. 查验系统和机读旅行证件芯片相互认证和推导会话密钥。须使用附录5.2中描述的认证和密钥建立协议。

3. 在成功地完成认证后，随后的通信**须**通过附录5.3中描述的安全通信加以保护。

被动认证（要求的）

查验系统执行下列步骤：

1. 从芯片上读取证件安全对象 (SO_D) (选择性地包括证件签名者证书 (C_{DS}))。

2. 从证件安全对象 (SO_D) 上读取证件签名者 (DS)。

3. 查验系统使用证件签名者公钥 (KPu_{DS}) 验证证件安全对象 (SO_D) 的数字签名。从国际民航组织的公钥簿下载的该密钥的证件签名者证书 (C_{DS}) 存储在查验系统中，也**可以**存储在机读旅行证件芯片上。这样可以确保证件安全对象 (SO_D) 是真实的，是由证书安全对象 (SO_D) 提及的机关签发的，而且没有被修改。这样证件安全对象 (SO_D) 的内容就可以被信任，并**应该**在查验系统中使用。

4. 查验系统从逻辑数据结构中读取相关的数据组。

5. 通过将内容散列并将结果与证件安全对象 (SO_D) 中相对应的散列值进行比较，查验系统能确保数据组的内容是真实的，且没有被改变。

生物特征信息现在可以被用来对提供机读旅行证件的人进行生物特征验证。

主动认证（选择性）

当把带有选择性数据组 15 的机读旅行证件提供给查验系统时，**可以**使用主动认证机制确保数据是从真实的芯片上读取的，而且芯片和资料页是一致的。

查验系统和芯片执行下列步骤：

1. 从机读旅行证件的资料页视读整个机读区 (如果还没有作为基本访问控制程序的一部分被阅读的话)，

并与数据组1中的机读区数值相比对。因为数据组1的真实性和完整性已经通过被动认证被查验，相似性能确保视读机读区是真实的，没有被改变。

2. 被动认证还证明了数据组15的真实性和完整性。这可以确保主动认证公钥 (KPu_{AA}) 是真实的，没有被改变。

3. 为确保证件安全对象 (SO_D) 不是复制品，查验系统使用机读旅行证件主动认证密钥对(KPr_{AA}和KPu_{AA})按照附录4中A4.2的描述，利用机读旅行证件芯片的询问—响应协议进行查验。

在成功地执行询问—响应协议后，就可以证明证件安全对象是属于资料页的，芯片是真实的，而且芯片和资料页是一致的。

对额外生物特征的扩展访问控制 (选择性)

对**选择性**附加生物特征实施保护取决于一个国家的内部规范或国与国之间就共享该信息商定的双边规范。

额外生物特征的解密 (选择性)

对**选择性**额外生物特征实施保护取决于一个国家的内部规范或国与国之间就共享该信息商定的双边规范。

7.2.3 附加的命令集

最小的命令集**须**至少包括下列命令：

SELECT（见 ISO/IEC 7816-4）
READ BINARY（见 ISO/IEC 7816-4）

执行在本节中被定义为**选择性的**建议，需要下述附加命令的支持：

EXTERNAL AUTHENTICATE（见 ISO/IEC 7816-4）
INTERNAL AUTHENTICATE（见 ISO/IEC 7816-4）
GET CHALLENGE（见 ISO/IEC 7816-4）。

8. 算法

8.1 概述

各国**须**在它们的国家签名 CA、证件签名密钥和主动认证密钥对 (如适用) 中使用相同的算法，尽管根据所选择的算法可能需要不同的密钥长度。

各国**须**在希望确认护照证件上的签名和与其他国家交换密钥管理的点上支持所有的算法。

关于密钥长度的建议在此假设建议使用最长的密钥颁发期和最长 10 年的证件有效期。

对于主动认证机制的签名生成，各国**须**使用 ISO/IEC 9796-2 数字签名方案 1 ([R17]，*ISO/IEC 9796-2, Information Technology—Security Techniques—Digital Signature Schemes giving message recovery—Part 2: Integer factorisation based mechanisms, 2002.)*。

对于自己国家在国家签名 CA、证件签名密钥和证件安全对象 (如果适用) 中使用的算法，各国**须**支持下述算法中的一种：

8.2　公钥算法 (RSA)

在签名生成以及证件和证件安全对象(SO_D)验证中应用 RSA 算法的国家**须**使用 RFC3447 ([R7]，*RFC 3447, J.Jonsson, B. Kaliski, "Public-key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003*)。RFC 3447 规定两种签名机制：RSASSA-PSS 和 RSASSA-PKCS1_v15。**建议**根据 RSASSA-PSS 生成签名，但接受国还**须**准备验证根据 RSASSA-PKCS1_v15 生成的签名。

建议使用 RSA 公钥算法的国家签名 CA 密钥的最小长度模数 n 为 3 072 位。

建议使用 RSA 公钥算法的证件签名者密钥的最小长度模数 n 为 2 048 位。

建议使用 RSA 公钥算法的主动认证密钥的最小长度模数 n 为 1 024 位。

8.3　数字签名算法 (DSA)

在签名生成或验证中应用 DSA 算法的国家**须**使用 FIPS (联邦信息处理标准出版物) 186-2 ([R9], *Federal Information Processing Standards Publication (FIPS PUB) 186-2 (+ Change Notice), Digital Signature Standard, 27 January 2000. (Supersedes FIPS PUB 186-1 dated 15 December 1998))*。

数字签名算法 FIPS186-2 的目前规范只支持 1 024 密钥长度。新版本的标准 FIPS186-3 正在试用，但何时可用现在尚不能确定。

建议使用数字签名算法的国家签名 CA 密钥的最小长度模数 p 和 q 分别为 *3 072 和256 位*。

建议使用数字签名算法的证件签名者密钥的最小长度模数 p 和 q 分别为 *2 048 和224 位*。

建议使用数字签名算法的主动认证密钥的最小长度模数 p 和 q 分别为 *1 024 和160 位*。

8.4　椭圆曲线 DSA

在签名生成或验证中应用椭圆曲线 DSA 算法的国家**须**使用 X 9.62 ([R11], *X9.62, "Public key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", 7 January 1999)*。用来生成椭圆曲线 DSA 密钥对的椭圆曲线域参数**须**在公钥参数中作出明确的描述，即：参数**须**为 ECParameters 型 (无命名曲线，无隐含参数) ，并**须**包括选择性余因子。ECPoints 须为未压缩格式。

建议使用椭圆曲线数字签名算法的国家签名 CA 密钥的基点指令最小长度为 *256 位*。

建议使用椭圆曲线数字签名算法的证件签名者密钥的基点指令最小长度为 *224 位*。

建议使用椭圆曲线数字签名算法的主动认证密钥的基点指令最小长度为 *160 位*。

8.5 散列法算法

SHA-1、SHA-224 (草案)、SHA-256、SHA-384 和 SHA-512 都是被允许的散列算法。见[R8], *FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard, August 2002*。

对于选定的签名算法，**应该**选择适当长度的散列法算法。例如：

- SHA-1，使用RSA 1024;
- SHA-224，使用ECDSA 224。

9. 密钥管理

9.1 概述

签发国**须**至少具有两种密钥类型，称为：

- 国家签名CA密钥
- 证件签名者密钥

签发国**可以**拥有额外的密钥类型：

- 主动认证密钥

国家签名 CA 密钥和证件签名者密钥使用 X.509 证书颁发 (RFC3280，见[R6], *RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo*：*"Internet X. 509 Public key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002*)。包括在证书中的公钥用来确认由该国颁发的证件签名者密钥 (就国家签名 CA 密钥而言) 或证件安全对象 (SO_D) (就证件签名者密钥而言) 的有效性。

各国颁发的所有证书**须**符合附录 1 中的证书概要。

各国应定期发布证书撤销表，见关于撤销的 9.5。

9.2 主动认证密钥

选择性主动认证密钥对 (KPr_{AA} 和 KPu_{AA}) 须以安全方式生成。

主动认证公钥 (KPu_{AA}) 和主动认证私钥 (KPr_{AA}) 都被存储在机读旅行证件的芯片中。此后，任何密钥管理都不适用于这些密钥。

9.3　证件签名者密钥

证件签名者证书 (C_{DS}) 被用来验证证件安全对象 (SO_D) 的有效性。因此，为接受来自另外一个国家的电子护照，接受国**须**已经将起源国的证件签名者证书 (C_{DS}) 的复制件存放在某种形式的信任存储中。

建议将证件签名者证书 (C_{DS}) 存储在证件安全对象 (SO_D) 中。详细论述请见附录3。

如果签发国支持将该证书存储在芯片中，证件签名者证书 (C_{DS}) 可以从机读旅行证件的芯片上读取。

证件签名者密钥的使用期

证件签名者密钥的使用期，即证件的有效期，是将下述两个时间段联系在一起来确定的：

- 密钥被用来签发护照的持续时间；
- 使用该密钥签发的护照的 (最长) 有效期。[15]

证件签名者证书 (C_{DS}) **须**在这个整个期间内有效，以便使护照的真实性能够得到验证。然而，密钥**应该**只能在有限的期间内用来签发证件；一旦用该密钥签发的最后一份证件本身到期了，该公钥也就不再需要了。

建议各国在最后一份证件制作完成后，立即将私钥以可审计和可问责的方式清除。

证件签名者密钥的颁发周期

各国在配置系统时，似宜将每个证件签名者密钥将要签署的证件数量考虑在内。每天签发大量证件，但只使用一个证件签名者密钥的国家似宜使用较短的颁发周期，以便在证件签名者密钥被撤销 (见 9.5) 的情况下将连续维持业务的成本降到最低。或者，一个国家也可以选择使用大量的签名密钥，以降低单一密钥的间接费用。

但是，如果一个国家只颁发少量的证书，证件签名者密钥的颁发周期就没有必要定得那么短，**可以**定得长一些。

因此，**建议**用于签署护照证件的证件签名者密钥的最长期限为三个月。对于产生大量机读旅行证件的国家，可以在任何给定的时间里同时颁发几个在用的证件签名密钥。

9.4　国家签名 CA 密钥

国家签名 CA 证书 (C_{CSCA}) 被用来验证证件签名者密钥的有效性。因此，为接受来自另外一个国家的电子护照，接受国**须**已经将该起源国的国家签名 CA 证书 (C_{CSCA}) 的复制件存放在边境控制系统可以访问的某种形式的信任存储中。

国家签名 CA 密钥的使用期

国家签名 CA 密钥的使用期，即证件的有效期，是将下述时间段联系在一起来确定的：

[15] 一些国家可能会在护照生效前先将其签发，例如在婚后更改姓名时。这样做的效果是将预先签发的护照的有效期延长尽可能长的时间。

- 国家签名CA密钥将被用来颁发证件签名者证书(C_{DS})的持续时间；
- 证件签名者密钥的密钥使用期，它包括：

  —— 该密钥将被用来签发护照的持续时间；
  —— 使用该密钥签发的护照的最长有效期。

国家签名 CA 密钥的颁发周期

国家签名 CA 密钥的颁发周期是下述三项考虑的微妙平衡：

- 如果万一一个国家的国家签名CA密钥被泄密，那么使用根据该密钥颁发的证件签名者密钥所签发的所有护照的有效性就会遭到质疑。所以，各国似宜将颁发周期保持相当短的时间；
- 然而，将颁发周期保持很短的时间会导致在任何一个时间点上都会有大量的国家签名CA密钥存在。这可能使边境处理系统内的证书管理复杂化；
- 如果国家签名CA密钥很少进行延期，由于缺乏知识或设施，这可能会给各国带来更多的困难。

因此，**建议**一个国家的国家签名 CA 密钥每隔三到五年更换一次。

国家签名 CA 密钥的重发

国家签名 CA 密钥在整个系统中提供信任点，没有这些信任点，该系统会崩溃。因此，各国**应该**对其国家签名 CA 密钥的更换作出认真的安排。初始签名期一旦过去，一个国家将在任何一个时间里始终保持有至少两个有效的国家签名 CA 证书 (C_{CSCA})。

各国**须**提前 90 天发出它将更改国家签名 CA 证书的通知，然后以双边方式分发其新的国家签名 CA 证书。为了认证新的证书，各国还应该使用带外方法确认其新的国家签名 CA 证书。

各国还**可以**生成链接证书，支持同先前颁发的国家签名 CA 证书的反向兼容。选择颁发链接证书的国家，不一定要使用带外方法颁发国家签名 CA 证书。

各国应该避免在颁发后的前两天使用国家签名 CA 证书。

9.5 证书撤销

颁发证件签名者证书 (C_{DS}) 的所有国家机构**须**以证书撤销表 (CRL) 的形式定期发出证书撤销信息。发布的证书撤销表**须**符合附录 2 中确定的概要。

各国须每隔 90 天至少发布一份证书撤销表。各国**可以**选择以相隔时间不多于 90 天但不少于 48 小时的频度发布证书撤销表。

证书撤销通知

当一个国家想撤销某一证件签名者密钥时，它不需要等到当前证书撤销表的下一个更新周期开始后再发布新的证书撤销表。**建议**新的证书撤销表在发出证书撤销通知后的 48 小时之内发布。

国家签名 CA 密钥的撤销

撤销国家签名 CA 密钥既严厉又复杂。在通知信赖国国家签名 CA 密钥已被撤销的同时，使用该密钥颁发的所有其他密钥实际上也被撤销了。

如果一个国家一直使用老的国家签名 CA 密钥认证新的国家签名 CA 密钥 (见 9.4 中的“国家签名密钥的重发”)，撤销老的国家签名 CA 密钥**须**被视为也是对新的国家签名 CA 密钥的撤销。

为签发新的证件，签发国基本上**须**返回到原来的程序中，即通过以双边的方式对它使用带外方法颁发的新的国家签名 CA 证书 (C_{CSCA}) 进行认可，重新引导其认证程序。

10. 证书和证书撤销表的分发

各国需要为国家签名 CA 密钥和证件签名者密钥制定证书延期策略，以便能够使证书和证书撤销表及时传送到接受国的边防控制系统中。传送最好在 48 小时之内发生，但是一些接受国的边防检查哨所比较偏远，联络不畅，可能需要更多的时间才能将证书和证书撤销表传送出去。接受国**应该**竭尽全力将这些证书和证书撤销表在 48 小时之内分发到所有的边防检查站。

国家签名 CA 证书的分发

签发国应该要求接受国将在 48 小时之内传送国家签名 CA 证书 (C_{CSCA})。

证件签名者证书的分发

签发国应该要求在 48 小时之内传送证件签名者证书 (C_{DS})。

通过将证件签名者证书 (C_{DS}) 包括在证件安全对象 (SO_D) 中，签发国能够确保证件签名者证书的及时传送。

证书撤销表的分发

各国**应该**尽力通过电子或其他手段执行那些在特殊情况下发布的证书撤销表。

关于证书撤销表的分发，另见 5.5.2。

10.1 通过国际民航组织公钥簿进行的分发

对于证件签名者证书 (C_{DS})，其主要分发渠道将是国际民航组织的公钥簿。对于证书撤销表，公钥簿是辅助分发渠道。国家签名 CA 证书 (C_{CSCA}) 并不公布，在公钥簿中也不能访问，但公钥簿使用它们对提供给它公布的证书签名者证书 (C_{DS}) 进行验证。

通信

与国际民航组织公钥簿的所有通信**须**基于服务器端认证的安全套接层协议。为此，国际民航组织**须**从商业方获取一个单一的服务器密钥 (每个站点一个)。

公钥簿更新

公钥**须**作为签发国使用该国国家签名 CA 密钥签名的 X.509—格式证书发送给公钥簿。这些证书**须**满足附录 1 中的要求。

当公钥簿根据提交的变更进行修改时，其更新**须**采用简易目录访问协议进行。因为国际民航组织有必要对更新过程给予应有的注意，所以公钥簿**须**包括一个“书写簿”，拟议的证书和证书撤销表更新将发送到那里，还**须**包括一个“阅读簿”，它用来在给予应有注意之后将新的证书包括进去，机读旅行证件的广大用户群体可以访问它，并下载这些信息。

就其性质而言，证书和证书撤销表是由签发国签名的。 这个签名**须**由国际民航组织先进行验证，然后再将证书或证书撤销表公布在“阅读簿”上。

公钥簿的下载

公钥簿将做成一个 X.500 的簿。公钥簿的估计大小将为 15—20 MB。

因为公钥簿比较小，**建议**各国每天下载整个公钥簿。

对公钥簿的读访问不得只限制在参加国的范围内。公钥簿将是完全公开的和通过因特网就能使用的资源，航空公司等单位还可以对其服务进行只读访问 (下载)。

10.2 通过双边手段进行分发

对于证书撤销表和国家签名 CA 证书 (C_{CSCA})，主要的分发渠道将是在参加国和用户国之间进行双边互换。

各国一般都有双边协议和双边交换信息的途径 (例如电子邮件或简易目标访问协议服务)。各国应该使用这些已有的渠道互相交换证书和证书撤销表。

目前没有双边协议或双边交换信息途径的国家**应该**同其他参加国签订这种协议和建立这种通信渠道。

规范性附录1

证书概要

与该规范保持一致的国家须颁发符合本概要的证书。所有的安全对象须以特异编码规则 (DER) 格式产生，以保持其中签名的完整性。

下述概要在 X.509 证书的每个域中使用如下术语：

m　强制性 —— 该域须存在。
x　不使用 —— 该域不应该被填充。
o　选择性 —— 该域可以存在。
c　关键的 —— 该扩展被标示为关键的，接受应用程序须能够处理这个扩展。

A.1.1　证书主体部分

证书组成部分	在 RFC 3280 中的章节	国家签名 CA 证书	证件签名者证书	注释
Certificate	4.1.1	m	m	
TBSCertificate	4.1.1.1	m	m	见本表的下一部分。
SignatureAlgorithm	4.1.1.2	m	m	这里插入的值取决于所选择的算法。
SignatureValue	4.1.1.3	m	m	这里插入的值取决于所选择的算法。
TBSCertificate	4.1.2			
version	4.1.2.1	m	m	须为 v3。
serialNumber	4.1.2.2	m	m	
signature	4.1.2.3	m	m	这里插入的值须与签名算法中的 OID 匹配。
issuer	4.1.2.4	m	m	见 A1.5
validity	4.1.2.5	m	m	执行程序须规定在 2049 年之前使用 UTC 时间，从那以后使用通用时间。
subject	4.1.2.6	m	m	见 A1.5
subjectPublicKeyInfo	4.1.2.7	m	m	
issuerUniqueID	4.1.2.8	x	x	
subjectUniqueID	4.1.2.8	x	x	
extensions	4.1.2.9	m	m	见下表。在下表中扩展应该存在。

A1.2 扩展名

扩展名称	在 RFC 3280 中的段落	国家签名 CA 证书	证件签名者证书	注释
AuthorityKeyIdentifier	4.2.1.1	o	m	在所有证书中都是强制性的，但自签的国家签名 CA 证书除外。
SubjectKeyIdentifier	4.2.1.2	m	o	
KeyUsage	4.2.1.3	mc	mc	这个扩展须标示为关键的。
PrivateKeyUsagePeriod	4.2.1.4	o	o	这将是私钥的颁发周期。
CertificatePolicies	4.2.1.5	o	o	
PolicyMappings	4.2.1.6	x	x	
SubjectAltName	4.2.1.7	x	x	
IssuerAltName	4.2.1.8	x	x	
SubjectDirectoryAttributes	4.2.1.9	x	x	
BasicConstraints	4.2.1.10	mc	x	这个扩展名须标示为关键的。
NameConstraints	4.2.1.11	x	x	
PolicyConstraints	4.2.1.12	x	x	
ExtKeyUsage	4.2.1.13	x	x	
CRLDistributionPoints	4.2.1.14	o	o	如果有些国家选择使用这个扩展，它们须将国际民航组织的公钥簿作为一个分布点包括在内。执行程序也可以包括相关的 CRL 分布点，供本地使用。这些可以被其他国家忽略。
InhibitAnyPolicy	4.2.1.15	x	x	
FreshestCRL	4.2.1.16	x	x	
privateInternetExtensions	4.2.2	x	x	
other private extensions	N/A	o	o	如果为国内使用目的包括任何扩展，这些扩展不得标示为关键的。不提倡各国包括任何私有扩展。
AuthorityKeyIdentifier	**4.2.1.1**			
keyIdentifier		m	m	如果使用这个扩展，该域至少须得到支持。
authorityCertIssuer		o	o	见 A1.5
authorityCertSerialNumber		o	o	
SubjectKeyIdentifier	**4.2.1.2**			
subjectKeyIdentifier		m	m	
KeyUsage	**4.2.1.3**			
digitalSignature		x	m	
nonRepudiation		x	x	
keyEncipherment		x	x	
dataEncipherment		x	x	
keyAgreement		x	x	

扩展名称	在 RFC 3280 中的段落	国家签名 CA 证书	证件签名者证书	注释
keyCertSign		m	x	
cRLSign		m	x	
encipherOnly		x	x	
decipherOnly		x	x	
BasicConstraints	**4.2.1.10**			
cA		m	x	对 CA 证书来说，此值为 TRUE。
pathLenConstraint		m	x	0 代表新的国家签名 CA 证书，1 代表链接的国家签名 CA 证书。
CRLDistributionPoints	**4.2.1.14**			
distributionPoint		m	x	
reasons		m	x	
cRLIssuer		m	x	
CertificatePolicies	**4.2.1.5**			
PolicyInformation				
policyIdentifier		m	m	
policyQualifiers		o	o	

A1.3　签名算法

在参考文件 5 (*RFC 3279, W. Polk, R. Housley, L.Bassham, "Algorithms and Identifiers for the Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002*) 第 2.2 节和参考文件 7 (*RFC 3447, J. Jonsson, B. Kaliski, "Public-key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003*) 第 A.2 节中规定的客体标识符须被用在第 IV 节第 8 段确定的那些算法中。

A1.4　签名值

在"签名值"域存储的签名结构须像参考文件 5 (*RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002*) 第 2.2 节规定的那样，用在第 IV 节第 8 段确定的那些算法中。

A1.4　主体公钥信息

用在第 IV 节第 8 段规定的算法中的主体公钥信息域须根据参考文件 5 (*RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002*) 第 2.3 节进行填充。

A1.5 证书和命名惯例

在国家签名 CA 证书和证件签名者证书的颁发者和主体域以及证书撤销表的颁发者域中，**建议**使用下列命名和寻址惯例。

应该使用下述属性：

- 国家 (国家代码须遵循在参考文件 16 (*ISO/IEC 3166, Codes for the representation of names of countries and their subdivisions—1997*.) 中规定的两字母国家代码的格式。)；
- 组织；
- 组织单位；
- 通用名称。

另外，一些国家**可以**使用：

- 序号。

想使用现有公钥基础设施支持其护照签发系统的国家可能受到现行命名惯例的约束。

规范性附录2

证书撤销表概要

下述概要在 X.509 证书撤销表的每个域中使用如下术语：

m　强制性 —— 该域**须**存在。
x　不使用 —— 该域**不应该**被填充。
o　选择性 —— 该域**可以**存在。
c　关键的 —— 该扩展被标示为关键的，接收应用程序**须**能够处理这个扩展。

证书表组成部分	在 **RFC 3280** 中的章节	国家签名 **CA** 证书撤销表	注释
CertificateList	5.1.1	m	
tBSCertList	5.1.1.1	m	见该表的下一部分。
signatureAlgorithm	5.1.1.2	m	这里插入的值取决于所选择的算法。
signatureValue	5.1.1.3	m	这里插入的值取决于所选择的算法。
tBSCertList	5.1.2		
version	5.1.2.1	m	**须**为 v2。
signature	5.1.2.2	m	这里插入的值取决于所选择的算法。
issuer	5.1.2.3	m	**要求** UTF8 编码。
thisUpdate	5.1.2.4	m	执行程序**须**规定在 2049 年之前使用 UTC 时间，从那以后使用通用时间。
nextUpdate	5.1.2.5	m	执行程序**须**规定在 2049 年之前使用 UTC 时间，从那以后使用通用时间。
revokedCertificates	5.1.2.6	m	
crlExtensions	5.1.2.7	m	

扩展名称	在 **RFC 3280** 中的章节	国家签名 **CA** 证书撤销表	注释
authorityKeyIdentifier	5.2.1	m	这须与 CRL 颁发者证书中的‘主体密钥标识符’域的值相同。
issuerAltName	5.2.2	x	
cRLNumber	5.2.3	m	
deltaCRLIndicator	5.2.4	x	
issuingDistributionPoint	5.2.5	x	
freshestCRL	5.2.6	x	
CRL Entry Extensions			
reasonCode	5.3.1	x	
holdInstructionCode	5.3.2	x	

扩展名称	在 **RFC 3280** 中的章节	国家签名 **CA** 证书撤销表	注释
invalidityDate	5.3.3	x	
certificateIssuer	5.3.4	x	

注：证书撤销表中可能会包括其他撤销信息，例如关于系统操作员或注册权限证书的撤销信息。

规范性附录3

证件安全对象

证件安全对象是作为参考文件 14 (*RFC 3369, Cryptographic Message Syntax, August 2002*) 中所规定的已签名数据类型来执行的。所有的安全对象须采用特异编码规则 (DER) 格式生成，以保持其中签名的完整性。

A3.1　已签名数据类型

适用 RFC3369 中的处理规则。

m　强制性 —— 该域**须**存在。
x　不使用 —— 该域**不应该**被填充。
o　选择性 —— 该域**可以**存在。
c　选择 —— 该域的内容是备选方案中一种选择。

值		注释
SignedDate		
version	m	值 = v3
digestAlgorithms	m	
encapContentinfo	m	
eContentType	m	id-icao-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	各国可选择包含证件签名者证书 (C_{DS})，它可以用来验证签名者信息域中的签名。
Crls	x	建议各国不要使用该域。
signerInfos	m	建议各国在该域中只提供 1 个签名者信息。
SignerInfo	m	
version	m	该域中的值受 sid 域的控制。有关该域的规则，见 RFC3369 第 5.3 节。
Sid	m	
issuerandSerialNumber	c	建议各国支持关于主体密钥标识符的该域。
subjectKeyIdentifier	c	
digestAlgorithm	m	该算法的算法标识符被用来生成关于封装内容和已签名属性的散列值。
signedAttrs	m	生成国可能希望在签名中包括额外属性，但是，除了验证签名值外，这些额外属性不一定需要接受国进行处理。
signatureAlgorithm	m	该算法的算法标识符被用来生成签名值和任何相关的参数。
signature	m	签名生成过程的结果。
unsignedAttrs	o	生成国可能希望使用该域，但不建议使用，而且接受国可以选择忽略它们。

A3.2 ASN.1 概要逻辑数据安全对象

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

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

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

-- Constants

ub-DataGroups INTEGER ::= 16

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

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {V0(0)}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

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

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

DataGroupNumber ::= INTEGER {
     dataGroup1      (1),
     dataGroup2      (2),
     dataGroup3      (3),
```

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

END
```

注：

dataGroupValue 域包含数据组编号规定的关于数据组 EF 全部内容的计算散列。

规范性附录4

主动认证公钥信息4

A4.1 主动认证公钥信息

选择性主动认证公钥存储在逻辑数据结构数据组 15 中。结构的格式 (主体公钥信息) 在参考文件 6 规定 (*R. Housley, W. Polk, W. Ford, D. Solo, "Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280", April 2002.)* 中有规定。所有的安全对象**须**根据特异编码规则 (DER) 格式产生，以保持其中签名的完整性。

ActiveAuthenticationPublicKeyInfo ::= SubjectPublicKeyInfo

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

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

A4.2 主动认证机制

主动认证是使用 ISO/IEC 7816 INTERNAL AUTHENTICATE 命令进行的。输入是一个随机数(RND.IFD)，须为 8 个字节。当使用基于整数周数分解的机制计算签名时，ICC 根据 ISO/IEC 9796-2 数字签名方案 1 ([R17]，*ISO/IEC 9796-2, Information Technology—Security Techniques—Digital Signature Schemes giving message recovery—Part 2: Integer factorisation based mechanisms 2002.*) 计算签名。

M **须**包括 M1 和 M2，其中 M1 **须**为一个长度 c —— 4 位的随机数， M2 为 RND.IFD。如果是 SHA-1，**须**使用包尾选项 1；如果不是 SHA-1，则**须**使用选项 2。

签名计算的结果**须**为签名 σ，没有不可恢复的报文部分 M2。

更详细的过程是，IFD（查验系统）和 ICC（机读旅行证件的芯片）执行下列步骤：

1) IFD生成一个随机数RND.IFD，并使用INTERNAL AUTHENTICATE命令将其发送到ICC。

2) ICC执行下列操作：

   a) 创建报头
   b) 生成M1
   c) 计算h (M)
   d) 创建包尾
   e) 计算报文代表F
   f) 计算签名σ，并将响应发送到IFD。

3) IFD根据发送INTERNAL AUTHENTICATE命令验证该响应，并检查ICC是否返回了正确值。

规范性附录5

基本访问控制和安全通信

A5.1　密钥衍生机制

证件基本访问密钥 (K_{ENC} 与 K_{MAC}) 和安全通信会话密钥都是通过对一个密钥种子 (K_{seed}) 产生的两个主要的3DES 密钥进行计算来建立的。

使用一个 32 位的计数器 c，以便能够从一个单一的种子密钥中衍生出多个密钥。根据密钥是被用来加密的，还是用来进行 MAC 计算的，须分别选用下列值：

— c = 1 (i.e. ‘0x 00 00 00 01’)，用于加密。
— c = 2 (i.e. ‘0x 00 00 00 02’)，用于MAC计算。

执行下列步骤，以便从密钥种子 K_{seed} 和 c 中衍生出两个主要的 3DES 密钥：

1. 假定D为K_{seed} 和 c的并置 ($D = K_{seed} \| c$)。
2. 计算H = SHA-1(D)，即：D的SHA-1散列。
3. H的字节1..8 形成密钥K_a ，H的字节9..16形成密钥K_b。
4. 调整密钥K_a 和 K_b的奇偶校验位形成正确的DES密钥。

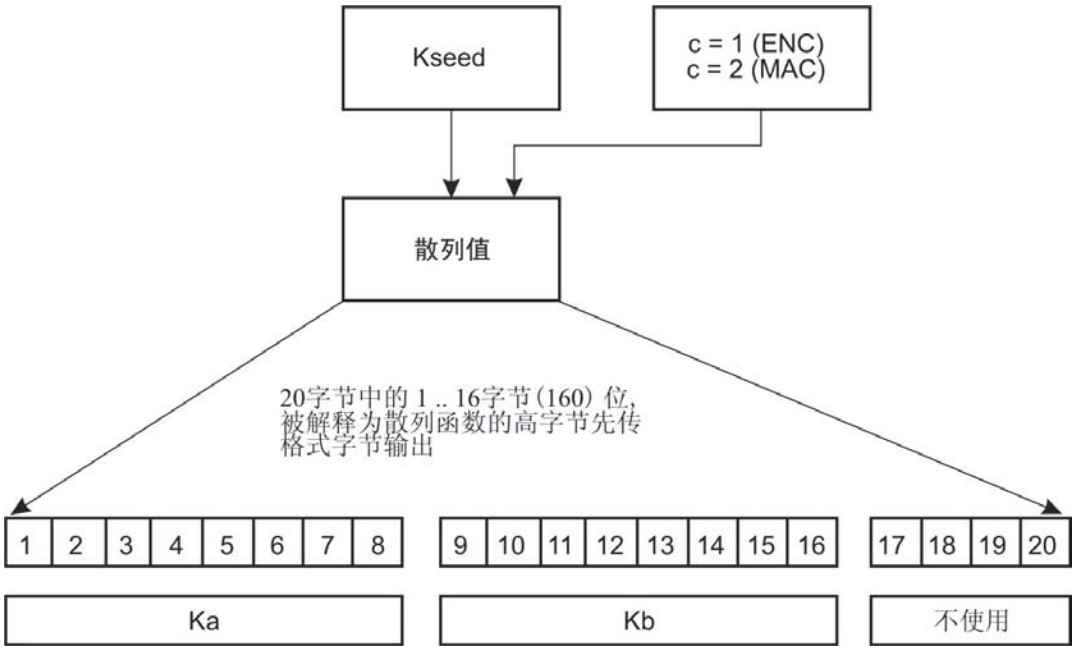


图 IV-5-1　根据密钥种子方案计算密钥

A5.2 认证和密钥建立

认证和密钥建立是根据 ISO/IEC 11770-2 密钥建立机制 6，把 3DES 用作分组密码，通过三次询问—响应协议实现的。符合 ISO/IEC 9797-1 报文认证码算法 3 的密码校验和经过计算，并被附加到加密报文上。须使用附录 5.4 中描述的运算方式。被交换的随机数须为 8 个字节，被交换的密钥材料须为 16 个字节。不得使用特异标识符。

更详细的过程是， IFD 和 ICC 执行下列步骤：

1) IFD通过发出GET CHALLENGE命令的方式，请求询问RND.ICC。ICC用随机数RND.ICC进行生成和作出响应。

2) IFD 执行下列操作：
   a) 生成一个随机数RND.IFD 和密钥材料K.IFD。
   b) 生成并置S = RND.IFD || RND.ICC || K.IFD。
   c) 计算密报E_IFD = E[K_ENC](S)。
   d) 计算校验和M_IFD = MAC[K_MAC](E_IFD)。
   e) 使用数据E_IFD || M_IFD，发送MUTUAL AUTHENTICATE命令。

3) ICC执行下列操作：
   a) 检查密码E_IFD 的校验和 M_IFD。
   b) 破译密码E_IFD。
   c) 从S中提取RND.ICC，并检查IFD是否返回了正确值。
   d) 生成密钥材料K.ICC。
   e) 生成并置 R = RND.ICC || RND.IFD || K.ICC。
   f) 计算密码 E_ICC = E[K_ENC](R)。
   g) 计算校验和 M_ICC = MAC[K_MAC](E_ICC)。
   h) 使用数据E_ICC || M_ICC发送响应。

4) IFD执行下列操作：
   a) 检查密码E_ICC 的校验和 M_ICC。
   b) 破译密码E_ICC。
   c) 从R中提取RND.IFD，并检查ICC是否返回了正确值。

A5.3 安全通信

在成功地执行了认证协议之后，IFD 和 ICC 以 (K.ICC 异或 K.IFD) 作为密钥种子，使用附录 5.1 描述的密钥衍生机制计算会话密钥 KS_ENC 和 KS_MAC 。所有进一步的通信都须以 MAC_ENC 模式的安全通信进行保护。

A5.3.1 SM APDU 的报文结构

须按照下列顺序根据表 IV-1 使用 SM 数据对象：

- 命令APDU: [DO‘87’] [DO‘97’] DO‘8E’。
- 响应APDU: [DO‘87’] DO‘99’ DO‘8E’。

所有的 SM 数据对象都**须**按照 ISO/IEC 7816-4 的规定以 BER TLV 的格式编码。命令报头**须**被包括在报文认证码计算中，因此**须**使用分类字节 CLA = 0x0c。

在应用安全通信后，Lc 的实际值将被修改成 Lc'。如果需要，一个适当的数据对象可以有选择地被包括在 APDU 数据部分中，以便传送 Lc 的原始值。在保护命令 APDU 中，新 Le 字节须被设定为'00'。

表 IV-1　SM 数据对象的使用

	DO'87'	**DO'97'**	**DO'99'**	**DO'8E'**
含义	填充—内容指示字节('01'代表 ISO—填充)，后面跟有密报。	Le (需要由 CC 保护)	处理状态 (SW1-SW2, 受MAC 的保护)	密码校验和(MAC)
命令 APDU	强制性的，如果发送数据。否则，不存在。	强制性的，如果请求数据。否则，不存在。	不使用。	强制性的。
响应 APDU	强制性的，如果返回数据。否则，不存在。	不使用。	强制性的。只有在发生 SM 错误时才不存在。	强制性的，如果 DO'87'和/或 DO'99'存在。

图 IV-5-2 显示的是在数据和 *Le* 可用的情况下，不受保护的命令 APDU 向受保护的命令 APDU 的转换。如果没有数据可用，不考虑构建 DO ‘87’。如果 *Le* 不可用，不考虑构建 DO ‘97’。

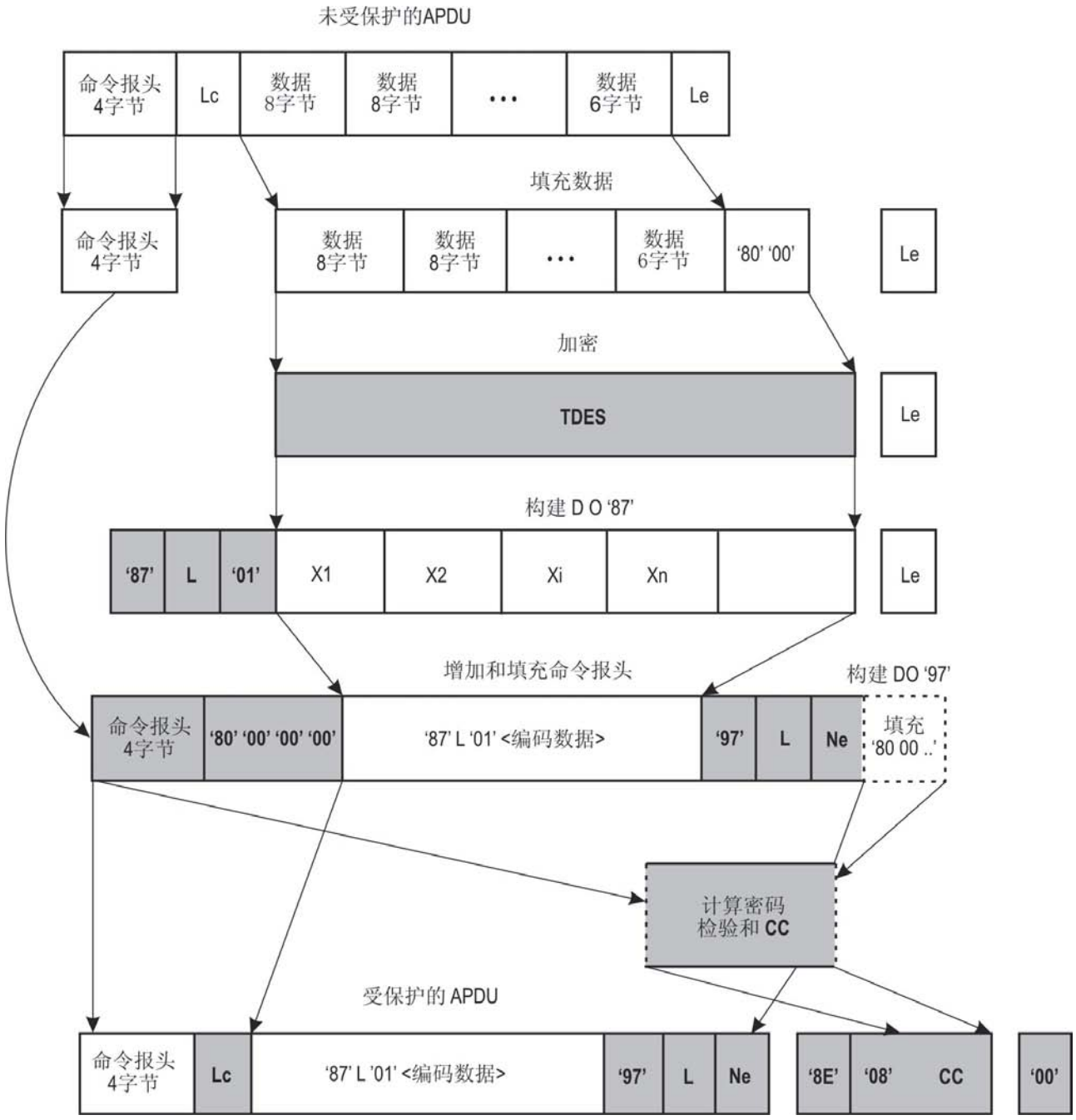


图 IV-5-2　计算 SM 命令 APDU

图 IV-5-3 显示的是在数据可用的情况下，不受保护的响应 APDU 向受保护的响应 APDU 的转换。如果没有数据可用，不考虑构建 DO ‘87’。

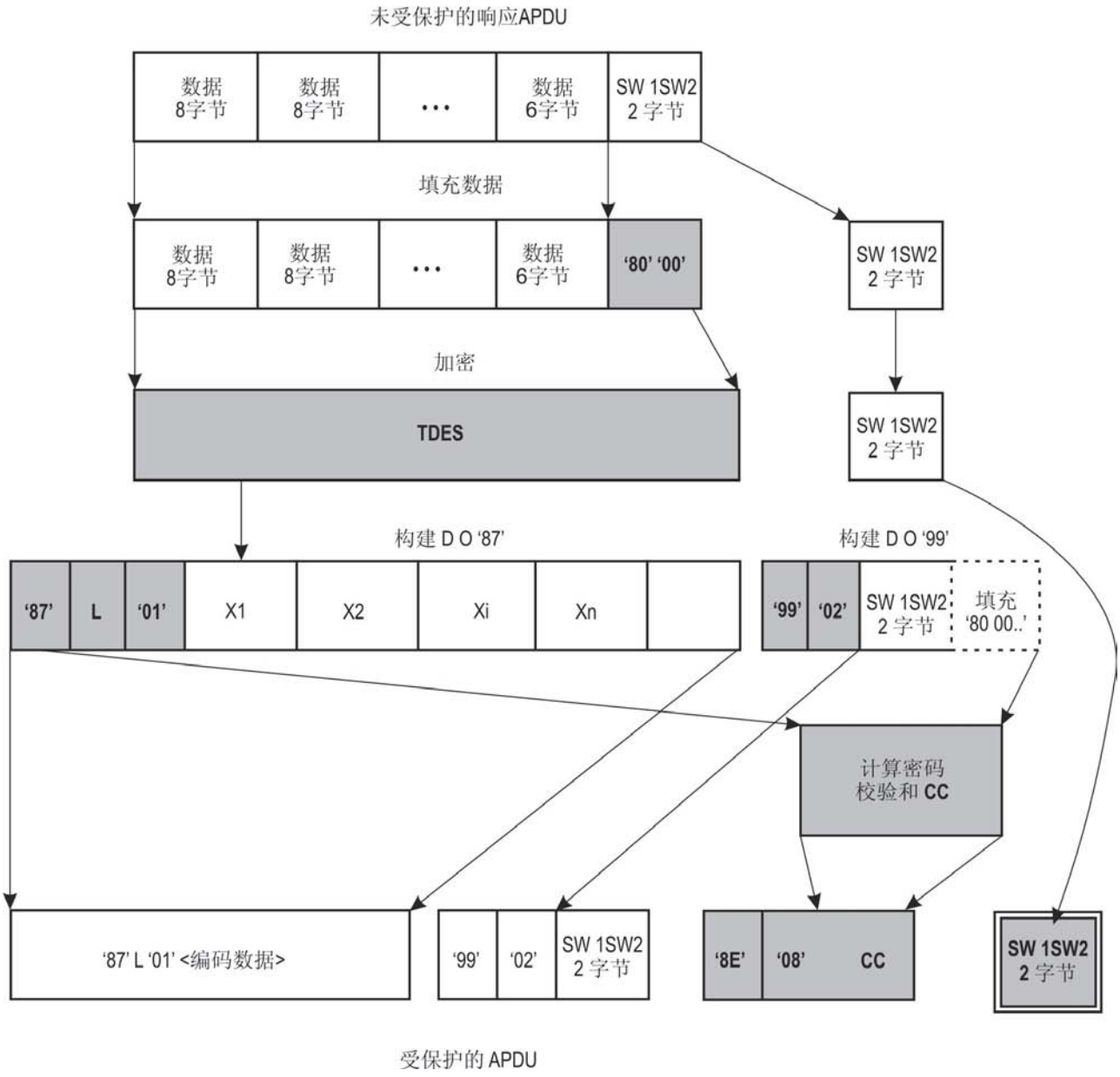


图 IV-5-3　计算 SM 响应 APDU

A5.3.2 SM 错误

当 ICC 在解释一条命令时发现有 SM 错误后，状态字节必须在不带 SM 的情况下被返回。在 ISO/IEC 7816-4 中确定了下述状态字节，用以表明 SM 错误：

- ‘6987’: 预计缺少 SM 数据对象
- ‘6988’: SM数据对象不正确

注: 在专用上下文中，可能出现更多的 SM 状态字节。当 ICC 返回的状态字节不带 SM DO 或带有错误的 SM DO 时，安全会话被中止。如果错误得到正确处理，会话将不被中止。

A5.4 3DES 操作模式

A5.4.1 加密

根据 ISO 11568-2，在带有零 IV (即：0x00 00 00 00 00 00 00 00)的 CBC 模式中，使用两个主要的 3DES (见图 IV-5-4)。在执行 MUTUAL AUTHENTICATE 命令时，对输入数据不使用填充。在对 SM APDU 进行计算时，使用符合 ISO/IEC 9797-1 填充方法 2 的填充。

A5.4.2 报文认证

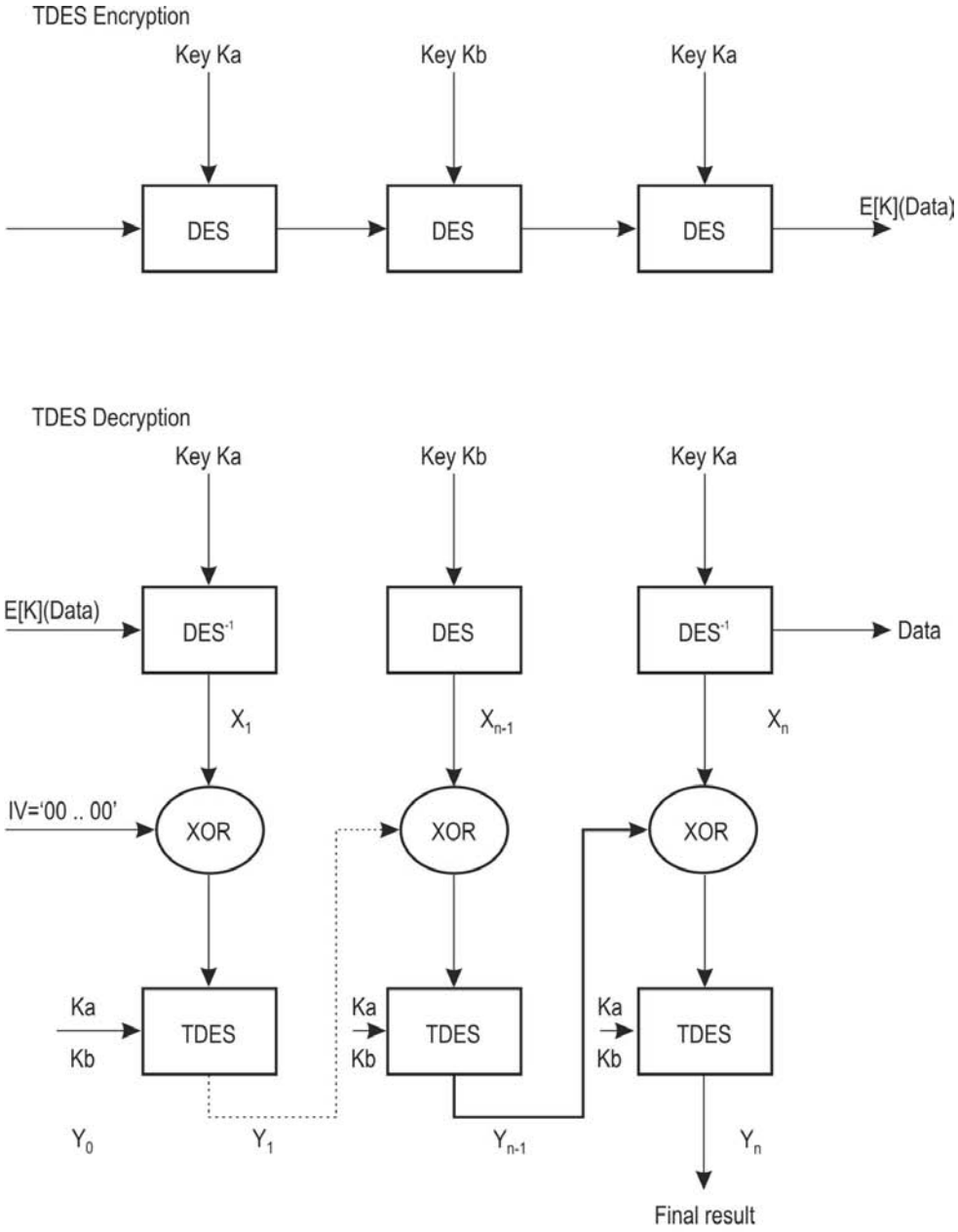
使用带有分组密码 DES、零 IV (8 字节) 的 ISO/IEC 9797-1 MAC 算法 3 和 ISO/IEC 9797-1 填充方法 2，计算密码校验和。报文认证码长度**须**为 8 字节 (见图 IV-5-5)。

经过成功的认证后，将被编上报文认证码的数据图**须**被发送序列计数器预先考虑。通过分别并置连接 RND.ICC 和 RND.IFD 的四个最低有效字节，对发送序列计数器进行计算：

SSC = RND.ICC (4 个最低有效字节) || RND.IFD (4 个最低有效字节)。

发送序列计数器在每次报文认证码被计算之前都要增加，也就是说，如果起始值是 x，在下一个命令中 SSC 值即是 x+1。那么，第一次响应的值则为 x+2。

对于 MUTUAL AUTHENTICATE，初始校验块 Y_0 **须**被设置为零 ‘0000000000000000’。



IV = 零初始化向量
'X_1ll ... ll$^{X}_{n}$' = 明文(待加密的报文)，每个 X_1 块为 64位长。
'Y_1ll ... ll$^{Y}_{n}$' = 结果密报(加密报文)，每个 Y_1 块为 64位长。

图 IV-5-4　在 CBC 模式下的 DES 加密/解密

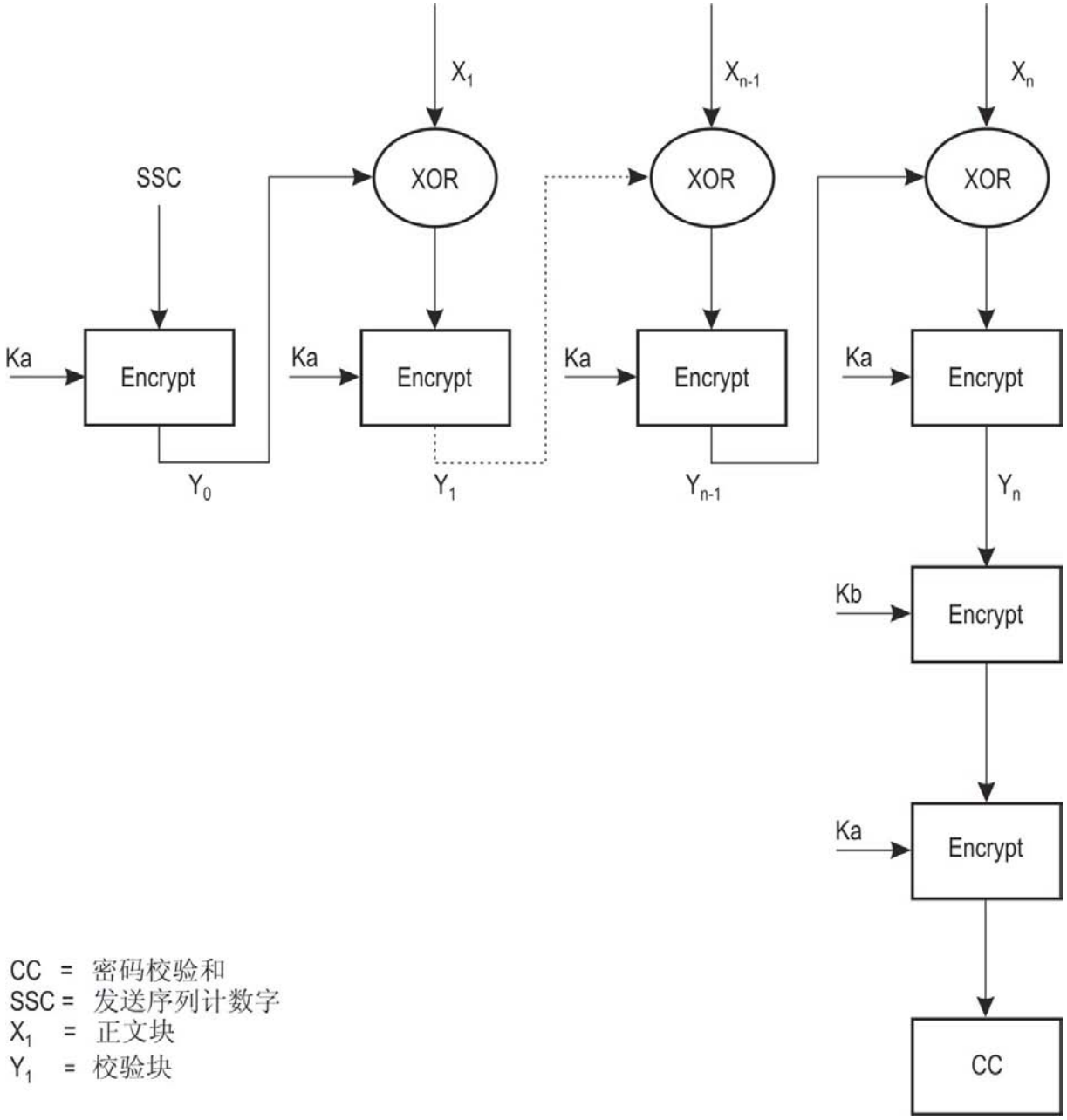


图 IV-5-5　零售版 MAC 计算

资料性附录6

处理过程实例

A6.1　命令序列

A6.1.1　基于机读区的基本访问控制和安全通信

根据密钥种子 (K_{seed}) 计算密钥

输入:

K_{seed} = ‘239AB9CB282DAF66231DC5A4DF6BFBAE’

计算加密密钥 (c = ‘00000001’):

1. 并置 K_{seed}和c：
   D = ‘239AB9CB282DAF66231DC5A4DF6BFBAE00000001’
2. 计算D的SHA-1散列：
   H_{SHA-1}(D) = ‘AB94FCEDF2664EDFB9B291F85D7F77F27F2F4A9D’
3. 形成密钥 K_a和K_b：
   K_a = ‘AB94FCEDF2664EDF’
   K_b = ‘B9B291F85D7F77F2’
4. 调整奇偶校验位：
   K_a = ‘AB94FDECF2674FDF’
   K_b = ‘B9B391F85D7F76F2’

一个特殊的奇校验

改变每个byte中8位中的最后1位
使每个byte满足 奇个1

计算 MAC 计算密钥 (c = ‘00000002’):

1. 并置K_{seed}和c：
   D = ‘239AB9CB282DAF66231DC5A4DF6BFBAE00000002’
2. 计算D的SHA-1散列：
   H_{SHA-1}(D) = ‘7862D9ECE03C1BCD4D77089DCF131442814EA70A’
3. 形成密钥K_a和K_b：
   K_a = ‘7862D9ECE03C1BCD’
   K_b = ‘4D77089DCF131442’
4. 调整奇偶校验位：

K_a = ‘7962D9ECE03D1ACD’
K_b = ‘4C76089DCE131543’

衍生证件基本访问密钥 (K_{ENC} 和 K_{MAC})

1. 阅读机读区：
   机读区 = P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<<
   L898902C<3UTO6908061F9406236ZE184226B<<<<<14

2. 根据机读区构建MRZ_information:
   证件号码 = L898902C<，校验位 = 3
   出生日期 = 690806，校验位 = 1
   到期日 = 940623，校验位 = 6
   机读区_信息 = L898902C<369080619406236

3. 计算MRZ_information的SHA-1散列：
   H_{SHA-1}(机读区_信息) = ‘239AB9CB282DAF66231D
   C5A4DF6BFBAEDF477565’

4. 找出最高有效的16个字节形成K_{seed}：
   K_{seed} = ‘239AB9CB282DAF66231DC5A4DF6BFBAE’

5. 运用附录5.1计算基本访问密钥(K_{ENC} 和 K_{MAC})：
   K_{ENC} = ‘AB94FDECF2674FDFB9B391F85D7F76F2’
   K_{MAC} = ‘7962D9ECE03D1ACD4C76089DCE131543’

会话密钥的认证和建立

查验系统：

1. 向机读旅行证件芯片请求一个8字节的随机数：

   命令APDU：

CLA	**INS**	**P1**	**P2**	**LE**
00h	84h	00h	00h	08h

   响应 APDU：

响应数据域	**SW1SW2**
RND.ICC	9000h

   RND.ICC = ‘4608F91988702212’

2. 生成一个随机8字节和一个随机16字节：
   RND.IFD = ‘781723860C06C226’
   K_{IFD} = ‘0B795240CB7049B01C19B33E32804F0B’

3. 并置RND.IFD、RND.ICC 和 K_{IFD}：
   S = ‘781723860C06C2264608F91988702212
   0B795240CB7049B01C19B33E32804F0B’

4. 根据附录5.2的计算，用TDES密钥K_{ENC} 为S加密：
   E_{IFD} = ‘72C29C2371CC9BDB65B779B8E8D37B29
   ECC154AA56A8799FAE2F498F76ED92F2’

5. 根据附录5.2中的计算，用TDES密钥 K_{MAC} 计算E_{IFD}的MAC：
   M_{IFD} = ‘5F1448EEA8AD90A7’

6. 构建MUTUAL AUTHENTICATE命令数据，并将命令APDU发送给机读旅行证件芯片：
   cmd_数据 = ‘72C29C2371CC9BDB65B779B8E8D37B29ECC154AA
   56A8799FAE2F498F76ED92F25F1448EEA8AD90A7’

命令 APDU：

CLA	INS	P1	P2	LC	命令数据域	LE
00h	82h	00h	00h	28h	cmd_数据	28h

机读旅行证件芯片：

7. 破译和验证接收的数据，并将RND.ICC与对GET CHALLENGE命令的响应作比较。

8. 生成一个随机16字节：
   K_{ICC} = ‘0B4F80323EB3191CB04970CB4052790B’

9. 计算K_{IFD} 和 K_{ICC}:的“异—或”逻辑：
   K_{seed} = ‘0036D272F5C350ACAC50C3F572D23600’

10. 使用附录5.1, 计算会话密钥 (KS_{ENC} 和 KS_{MAC})：
    KS_{ENC} = ‘979EC13B1CBFE9DCD01AB0FED307EAE5’
    KS_{MAC} = ‘F1CB1F1FB5ADF208806B89DC579DC1F8’

11. 计算发送序列计数字：
    SSC = ‘887022120C06C226’

12. 并置RND.ICC、RND.IFD 和 K_{ICC}：
    R = ‘4608F919887022127817238 60C06C226
    0B4F80323EB3191CB04970CB4052790B’

13. 根据附录5.2的计算，用TDES 密钥K_{ENC} 为R加密：

E_{ICC} = ‘46B9342A41396CD7386BF5803104D7CE
DC122B9132139BAF2EEDC94EE178534F’

14. 根据附录5.2中的计算，用TDES密钥K_{MAC}计算E_{ICC}的MAC：

M_{ICC} = ‘2F2D235D074D7449’

15. 构建MUTUAL AUTHENTICATE响应数据，并将响应APDU发送到查验系统：

响应_数据 = ‘46B9342A41396CD7386BF5803104D7CEDC122B91
32139BAF2EEDC94EE178534F2F2D235D074D7449’

响应 APDU：

响应数据域	SW1SW2
响应数据 (resp_data)	9000h

查验系统：

16. 破译和验证接收的数据，并将接收到的 RND.IFD与生成的RND.IFD作比较。

17. 计算K_{IFD} 和 K_{ICC} 的异或值：

K_{seed} = ‘0036D272F5C350ACAC50C3F572D23600’

18. 使用附录5.1，计算会话密钥 (KS_{ENC}和KS_{MAC})：

KS_{ENC} = ‘979EC13B1CBFE9DCD01AB0FED307EAE5’
KS_{MAC} = ‘F1CB1F1FB5ADF208806B89DC579DC1F8’

19. 计算发送序列计数器：

SSC = ‘887022120C06C226’

安全通信

在认证和建立会话密钥后，查验系统选择 EF.COM (文件 ID = ‘011E’)，并使用安全通信阅读数据。计算出的KS_{ENC}, KS_{MAC} 和 SSC (前面的步骤 18 和 19) 将被使用。

首先选择 EF.COM，然后阅读该文件的前 4 个字节，这样就能确定该文件的结构长度。此后，再阅读剩下的字节。

1. 选择EF.COM

未受保护的命令APDU:

CLA	INS	P1	P2	LC	命令数据域
00h	A4h	02h	0Ch	02h	01h 1Eh

a. 覆盖分类字节和填充命令报头：

CmdHeader (命令报头) = ‘0CA4020C80000000’

b. 填充数据：

数据 = ‘011E800000000000’

c. 用 KS_{ENC} 加密数据:

加密数据= ‘6375432908C044F6’

d. 构建 DO‘87’：

DO87 = ‘8709016375432908C044F6’

e. 并置 CmdHeader (命令报头) 和 DO87：

M = ‘0CA4020C800000008709016375432908C044F6’

f. 计算 M 的 MAC：

i. 用 1 为 SSC 增值：

SSC = ‘887022120C06C227’

ii. 并置 SSC 和 M，并增加填充:

N = ‘887022120C06C2270CA4020C80000000
8709016375432908C044F68000000000’

iii. 用 KS_{MAC} 计算 N 的 MAC：

CC = ‘BF8B92D635FF24F8’

g. 建立 DO‘8E’：

DO8E = ‘8E08BF8B92D635FF24F8’

h. 构建并发送受保护的 APDU：

受保护的 APDU = ‘0CA4020C158709016375432908C0
44F68E08BF8B92D635FF24F800’

i. 接收机读旅行证件芯片的响应 APDU：

RAPDU = ‘990290008E08FA855A5D4C50A8ED9000’

j. 通过计算 DO’99’的 MAC，验证 RAPDU CC：

i. 用 1 为 SSC 增值：

SSC = ‘887022120C06C228’

ii. 并置 SSC 和 DO‘99’，并增加填充：

K = ‘887022120C06C2289902900080000000’

iii. 用 KS_{MAC} 计算 MAC：

CC’ = ‘FA855A5D4C50A8ED’

iv. 将 CC’与 RAPDU 的 DO‘8E’数据作比较。

‘FA855A5D4C50A8ED’ == ‘FA855A5D4C50A8ED’? YES (是)。

2. “Read Binary”命令的前四个字节：

受保护的命令APDU:

CLA	INS	P1	P2	LE
00h	B0h	00h	00h	04h

a. 覆盖分类字节，并填充命令报头:

CmdHeader (命令报头) = ‘0CB0000080000000’

b. 建立 DO‘97’:

DO97 = ‘970104’

c. 并置 CmdHeader 和 DO97:

M = ‘0CB0000080000000970104’

d. 计算 M 的 MAC:

i. 用 1 为 SSC 增值:

SSC = ‘887022120C06C229’

ii. 并置 SSC 和 M，并增加填充:

N = ‘887022120C06C2290CB00000
8000000097010480000000000’

iii. 用 KS_{MAC} 计算 N 的 MAC:

CC = ‘ED6705417E96BA55’

e. 建立 DO‘8E’:

DO8E = ‘8E08ED6705417E96BA55’

f. 构建并发送受保护的 APDU:

受保护的 APDU = ‘0CB000000D9701048E08ED6705417E96BA5500’

g. 接收机读旅行证件芯片的响应 APDU:

RAPDU = ‘8709019FF0EC34F992265199029000
8E08AD55CC17140B2DED9000’

h. 通过计算 DO‘87’ 和 DO‘99’并置的 MAC，验证 RAPDU CC:

i. 用 1 为 SSC 增值:

SSC = ‘887022120C06C22A’

ii. 并置 SSC、DO‘87’ 和 DO‘99’，并增加填充:

K = ‘887022120C06C22A8709019F
F0EC34F99226519902900080’

iii. 用 KS_{MAC} 计算 MAC:

CC’ = ‘AD55CC17140B2DED’

iv. 将 CC’与 RAPDU 的 DO‘8E’数据作比较:

‘AD55CC17140B2DED’ == ‘AD55CC17140B2DED’？YES(是).

i. 用 KS_{ENC} 解密 DO‘87’数据:

解密数据= ‘60145F01’

j. 确定结构长度:

L = ‘14’ + 2 = 22 字节

3. “Read Binary”命令从偏移 4 开始剩下的 18 字节：

未受保护的命令 APDU：

CLA	**INS**	**P1**	**P2**	**LE**
00h	B0h	00h	04h	12h

a. 覆盖分类字节，并填充命令报头：

CmdHeader (命令报头) = ‘0CB0000480000000’

b. 建立 DO‘97’：

DO97 = ‘970112’

c. 并置 CmdHeader 和 DO97：

M = ‘0CB00004800000009701128’

d. 计算 M 的 MAC：

i. 用 1 为 SSC 增值：

SSC = ‘887022120C06C22B’

ii. 并置 SSC 和 M，并增加填充：

N = ‘887022120C06C22B0CB00004
800000009701128000000000’

iii. 用 KS_{MAC} 计算 N 的 MAC：

CC = ‘2EA28A70F3C7B535’

e. 建立 DO‘8E’：

DO8E = ‘8E082EA28A70F3C7B535’

f. 构建并发送受保护的 APDU：

受保护的 APDU = ‘0CB000040D9701128E082EA28A70F3C7B53500’

g. 接收机读旅行证件芯片的响应 APDU：

RAPDU = ‘871901FB9235F4E4037F2327DCC8964F1F9B8C30F42
C8E2FFF224A990290008E08C8B2787EAEA07D749000’

h. 通过计算 DO‘87’ 和 DO‘99’并置的 MAC，验证 RAPDU CC：

i. 用 1 为 SSC 增值：

SSC = ‘887022120C06C22C’

ii. 并置 SSC、DO‘87’和 DO‘99’，并增加填充：

K = ‘887022120C06C22C871901FB9235F4E4037F232
7DCC8964F1F9B8C30F42C8E2FFF224A99029000’

iii. 用 KS_{MAC} 计算 MAC：

CC’ = ‘C8B2787EAEA07D74’

i.v 将 CC’与 RAPDU 的 DO‘8E’数据作比较：

‘C8B2787EAEA07D74’ == ‘C8B2787EAEA07D74’？YES(是)

i. 用 KS_{ENC} 解密 DO‘87’数据：

加密数据 = ‘04303130365F360630343030305C026175’

结果：

EF.COM 数据 = ‘60145F0104303130365F360630343030305C026175’

A6.1.2 被动认证

步骤 1：从芯片上读取证件安全对象 (SO_D) (选择性地包含证件签名者证书 (C_{DS}))。

步骤 2：从证书安全对象 (SO_D) 上读取证书签名者 (DS)。

步骤 3：查验系统使用证件签名者公钥 (KPu_{DS}) 验证 SO_D。

步骤 4：查验系统使用国家签名 CA 公钥 (KPu_{CSCA}) 验证 C_{DS}。

如果步骤 3 和 4 中的两次验证都是正确的，这就确保 SO_D 的内容是可信的，并**应该**在查验过程中使用。

步骤 5：从逻辑数据结构中读取相关的数据组。
步骤 6：计算相关数据组的散列。
步骤 7：将计算出的散列值与 SO_D 中的相应散列值作比较。

如果步骤 7 中的散列值是相同的，这就确保数据组的内容是真实的，没有被改变。

A6.1.3 主动认证

这个处理过的例子使用下列设置：

1. 基于整数因数分解的机制: RSA

2. 模数长度: 1 024 比特 (128 字节)

3. 散列算法: SHA1

查验系统:

1. 生成一个8字节随机数：
   RND.IFD = ‘F173589974BF40C6’

2. 构建内部识别命令，并将命令APDU发送到机读旅行证件的芯片：

   命令APDU

CLA	INS	P1	P2	LC	命令数据域	LE
0xh	88h	00h	00h	08h	RND.IFD	00h

机读旅行证件芯片：

3. 根据进来的APDU，确定M_2：
   M_2 = ‘F173589974BF40C6’

4. 创建包尾：
   T = ‘BC’ (即：SHA1)

5. 确定长度:
   a. $c = k – L_h – 8t – 4 = 1024 – 160 – 8 – 4 = 852$ 比特
   b. $L_{M1} = c – 4 = 848$ 比特

6. 生成长度L_{M1}的随机数M_1：

M_1 = ‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8’

7. 创建M：

M = M_1 | M_2 = ‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8F173589974BF
40C6’

8. 计算M的SHA1摘要：

H = SHA1(M) =‘C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127’

9. 构建报文代表：

F = ‘6A’ | M_1 | H | T =
‘6A9D2784A67F8E7C659973EA1AEA25D9
5B6C8F91E5002F369F0FBDCE8A3CEC19
91B543F1696546C5524CF23A5303CD6C
98599F40B79F377B5F3A1406B3B4D8F9
6784D23AA88DB7E1032A405E69325FA9
1A6E86F5C71AEA978264C4A207446DAD
4E7292E2DCDA3024B47DA8C063AA1E6D
22FBD976AB0FE73D94D2D9C6D88127BC’

10. 用主动认证私钥为F加密，形成签名：

S = ‘756B683B036A6368F4A2EB29EA700F96
E26100AFC0809F60A91733BA29CAB362
8CB1A017190A85DADE83F0B977BB513F
C9C672E5C93EFEBBE250FE1B722C7CEE
F35D26FC8F19219C92D362758FA8CB0F
F68CEF320A8753913ED25F69F7CEE772
6923B2C43437800BBC9BC028C49806CF

2E47D16AE2B2CC1678F2A4456EF98FC9’

11. 为INTERNAL AUTHENTICATE构建响应数据，并将响应APDU 发送到查验系统：

响应APDU：

响应数据域	**SW1SW2**
S	9000h

查验系统：

12. 用公钥破译签名：

F = ‘6A9D2784A67F8E7C659973EA1AEA25D9
5B6C8F91E5002F369F0FBDCE8A3CEC19
91B543F1696546C5524CF23A5303CD6C
98599F40B79F377B5F3A1406B3B4D8F9
6784D23AA88DB7E1032A405E69325FA9
1A6E86F5C71AEA978264C4A207446DAD
4E7292E2DCDA3024B47DA8C063AA1E6D
22FBD976AB0FE73D94D2D9C6D88127BC’

13. 通过包尾T*，确定散列算法：

T = ‘BC’ (即：SHA1)

14. 提取摘要：

D = ‘C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127’

15. 提取M_1：

M1 = ‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8’

16. 包头表明部分恢复，但签名具有模数长度，所以将M_1 与已知的M_2 并置(即：RND.IFD)：

M* = ‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A

```
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8F173589974BF
40C6'
```

17. 计算M*的SHA1摘要：

```
D* = 'C063AA1E6D22FBD976AB0FE73D94D2D9
     C6D88127'
```

18. 比较D和D*：

D等于D*，所以验证是成功的

A6.2　使用期限

下面的例子演示了对如何计算第 9 段中描述的密钥使用期限的解释。

A6.2.1　例 1

第一个例子演示的是国家希望将其全部证书的使用期限保持最短的系统。该国的护照有效期为五年，由于该国每年签发比较多的护照，因此决定将其密钥的颁发期限保持最短。

期限	经过时间	
证件签名者密钥颁发		1 个月
护照有效期	5 年	—
证件签名者证书有效期	5 年	1 个月
国家签名 CA 密钥颁发	3 年	—
国家签名 CA 证书有效期	8 年	1 个月

该例的结果是，到第一份国家签名 CA 证书失效时，至少颁发了 36 个证件签名者密钥 (每个月一个)，在该国家签名 CA 密钥的最后几个月里，至少还会有另外两个国家签名 CA 密钥对签名验证有效。

A6.2.2　例 2

第二个例子演示的是国家采用一种略微宽松的做法的系统。护照的有效期为十年；该国决定对全部密钥保持平均的颁发期限。

期限	经过时间	
证件签名者密钥颁发		2 个月
护照有效期	10 年	—
证件签名者证书有效期	10 年	2 个月
国家签名 CA 密钥颁发	4 年	—
国家签名 CA 证书有效期	14 年	2 个月

该例的结果是，到第一份国家签名 CA 证书失效时，至少颁发了 24 个证件签名者密钥，在该国家签名 CA 密钥的最后几个月里，至少还会有另外三个国家签名 CA 密钥对签名验证有效。

A6.2.3 例 3

最后的例子演示的是国家决定使用本框架建议的最长极限。护照有效期为十年，国家签名 CA 密钥每五年更换一次，证件签名者密钥每三个月更换一次。

期限	经过时间	
证件签名者密钥颁发		3 个月
护照有效期	10 年	—
证件签名者证书有效期	10 年	3 个月
国家签名 CA 密钥颁发	5 年	—
国家签名 CA 证书有效期	15 年	3 个月

该例的结果是，到第一份国家签名 CA 证书失效时，至少颁发了 20 个证件签名者密钥，在该国家签名 CA 密钥的最后几个月里，至少还会有另外三个国家签名 CA 密钥对签名验证有效。

资料性附录7

公钥基础设施和安全威胁

A7.1　密钥管理

A7.1.1　国家签名 CA 和证件签名者密钥

为保护私钥，**建议**使用安全硬件装置生成签名 (安全签名生成装置—SSCD)，也就是说，由安全签名生成装置安全地生成新的密钥对、存储和销毁 (到期后) 相应的私钥。为防止对签名生成装置的攻击，包括临信道攻击 (例如定时、功耗、EM 辐射、故障注入) 以及对随机数发生器的攻击，**建议**所使用的签名生成装置要顺利通过符合 CCRA 标准的认证机构根据适当的，具有 EAL 4 和高级功能强度的通用标准保护框架进行的认证/确认。

当通过外交手段分发自签的国家签名 CA 证书时，必须格外小心，防止插入凶猛的国家签名 CA 证书。另外，**建议**各国安全地保存收到的国家签名 CA 证书，阅读装置要以安全的方式阅读这些证书。为防止对卡接收器的攻击，**建议**所使用的卡接收器要顺利通过符合 CCRA 标准的认证机构根据适当的，具有 EAL 4 和高级功能强度的通用标准保护框架进行的认证/确认。

A7.1.2　主动认证密钥

建议采用安全方式生成主动认证密钥对。由于私钥存储在芯片的安全存储器中，而芯片硬件必须在机读旅行证件的整个有效期内能抵御攻击，因此**建议**所使用的芯片要顺利通过符合 CCRA 标准的认证机构根据适当的，具有 EAL 4 和高级功能强度的通用标准保护框架进行的认证/确认。

可用的芯片技术影响着芯片中使用的主动认证密钥的最大密钥长度。很多芯片目前不支持超过 80 位安全等级的密钥长度，这就是选择该值作为建议的最低值的原因所在。与机读旅行证件有效期相比，这是一个比较低的安全等级。因此，**建议**如果芯片支持的话，使用长一些的密钥。

使用主动认证机制验证外国的机读旅行证件的国家还应认识到，对于泄密的主动认证密钥，一直还没有规定撤销机制。

A7.1.3　拒绝服务攻击

依赖公钥簿分发证件签名者证书和证书撤销表的国家必须考虑到拒绝服务攻击。这种攻击是防不胜防的。因此，**建议**验证证书安全对象所需的证件签名者证书也包括在证件安全对象本身中。接受国**应该**利用所提供的证件签名者证书。

为双边分发证书撤销表，**建议**与其他国家建立多种渠道 (例如：因特网、电话、传真和邮件等)，并在收到证书撤销表时应予以确认。

A7.2 克隆威胁

与纸基机读旅行证件相比，复制存储在射频芯片中的签名数据一般来说更容易做到。担心自己国家的公民的数据可能会被复制到另外一个芯片上的国家，**应该**实施在一定程度上可防止这种情况发生的主动认证。

A7.2.1 被动认证

被动认证不能防止对存储在芯片上的数据的复制。因而，一本机读旅行证件上的芯片有可能被存有从其他机读旅行证件上复制下来的数据的假芯片替换。接受国**应该**验证从该芯片上读取的数据是否确实属于所提交的机读旅行证件。将存储在芯片上的数据组 1 与打印在机读旅行证件资料页上的机读区作比较，就能完成上述的验证。如果将数据组 1 和机读区相比较，证书安全对象是有效的，而且提交的机读旅行证件没有被篡改 (没有被伪造)，那么，机读旅行证件和存储在芯片上的数据就可以被认为是一体的。

A7.2.2 主动认证

主动认证使芯片替换变得更加困难，但并不是不可能的。攻击者提交给查验系统的机读旅行证件可以装有专用芯片。这个芯片是作为远处的一个真正芯片的代理而工作：该芯片与该攻击者通信，该攻击者再与另一个攻击者通信，后者可以 (临时) 访问这个真正的芯片。查验系统不可能发现它所认证的是一个远距的芯片，而不是所提交的芯片。这种攻击被称作“国际象棋大师”攻击。

A7.3 保密性威胁

A7.3.1 无访问控制

采用紧耦合芯片已经将保密性风险降到最低程度，因为阅读装置必须要非常靠近芯片，所以不把不正当读取作为严重威胁。但是从较远的距离上窃听芯片与阅读器之间正在进行的通信是可能的。希望解决这种威胁的国家**应该**实施基本访问控制。

A7.3.2 基本访问控制

用来认证阅读器和为芯片与阅读器之间的通信进行加密建立会话密钥的基本访问密钥，是根据 9 位数的证件号码、出生日期和到期日期生成的。因此，该密钥的熵比较低。对于一本 10 年有效期的机读旅行证件，平均信息量最多是 56 位。如果再加上额外的信息 (例如持证人的大约年龄，或文件号码与到期日期之间的关系)，该平均信息量就会降得更多。由于平均信息量比较低，攻击者从理论上讲有可能记录加密的会话，通过“强力攻击”技术根据认证计算基本访问密钥，推导会话密钥和解密记录的会话。但这与从其他渠道获取数据相比还是需要相当大的努力。

A7.3.3 主动认证 (数据追踪)

在主动认证中使用的询问—响应协议中，芯片签署一个由查验系统或多或少随机选择的位串。如果接受国使用当前日期、时间和地点以不可预知，但可验证的方式 (例如使用安全硬件) 生成该位串，第三方事后便可确信该签名者在某个日期和时间在某个地点。

A7.4　密码威胁

由于已经选定了建议的最小密钥长度，所以破坏那些密钥需要一定的 (假定) 努力，不管选择的是什么签名算法：

密钥类型	安全等级
国家签名 CA	128 位
证件签名者	112 位
主动认证	80 位

A7.4.1　数学的进步和非标准计算

根据摩耳定律，计算能力每 18 个月翻一番。然而，签名算法的安全不仅仅受计算能力的影响，数学的进步 (密码分析学) 和可用的新型非标准计算法 (例如量子计算机) 也需要考虑在内。

由于密钥的有效期长，很难预测数学的进步和可用的非标准计算装置的发展情况。因此，关于密钥长度的建议主要基于外推的计算能力。各国**应该**出于上述原因经常审查其自己的但也要审查所接收的机读旅行证件的密钥长度。

生成特殊形式的密钥对可以提高签名算法的总体性能，但将来也可能被密码分析学所利用。因此，**应该**避免使用这种特殊的密钥对。

A7.4.2　散列值冲突

尽管要找到能够生成与指定报文具有相同散列值的另一份报文从计算的角度来说是不可行的，但是要找到能够生成相同散列值的两份报文却容易得多。这被称作生日悖论。

一般来说，需要签名的所有报文都是由证件签名者本身产生的。因此，找出散列值冲突帮不了攻击者多少忙。然而，如果申请人以数字形式提供的照片在没有做额外的随机修改的情况下被证书签名者接受，则有可能受到下列攻击：

- 两个人共享他们的数字照片。然后他们随机反复地快速转动每张照片中的少量数位，直到两幅照片产生相同的散列值。
- 两个人使用伪造的照片申请一本新的机读旅行证件。只要能更换芯片中的数字照片（例如通过替换芯片），两个人中的任何一个人现在就能够使用另外一个人的机读旅行证件。

散列函数 SHA-1 对于散列值冲突只提供 80 位的安全。因此，要找出散列值冲突比破坏证件签名者密钥要容易得多，因为证件签名者密钥提供 112 位的安全。因此，每当散列值冲突变得令人担心的时候（例如，如上面所述的情况），**建议**不要将 SHA-1 用作散列函数。

— 完 —

国际民航组织在航空运输领域的出版物和相关出品

下文简要介绍国际民用航空组织在航空运输领域的各项出版物和相关出品。

- 国际标准和建议措施（SARPs），是理事会根据《国际民用航空公约》第三十七、五十四和九十条予以通过的，并为方便起见而定为公约的各附件。附件9《简化手续》载有与国际空中航行有关的涉及海关、卫生检疫、移民和健康事项的国际标准和建议措施。附件17《保安》是由与保护民用航空免遭非法干扰行为有关的所有事项的国际标准和建议措施组成的。各国的国家规章和措施与一项国际标准的规定之间的任何差异，必须根据《公约》第三十八条通知理事会。理事会还请各缔约国通知其与建议措施的规定之间的差异。

- 国际民航组织的政策，内容涉及国际航空运输的管理、机场和空中航行服务的收费以及在国际航空运输领域的税收。

- 技术规范的内容涉及机读旅行证件（MARTDs）。

- 费率涉及机场和空中航行服务，包括在180多个国家对用户适用的收费。

- 手册向各缔约国提供信息或指导，涉及诸如国际航空运输的管理、机场和空中航行服务的财务管理、空中交通预测方法和对附件17各项规定的遵守情况等事项。

- 通告提供各缔约国感兴趣的专门信息，包括关于航空运输业在全球和地区一级的中期和长期趋势的研究，以及世界性的专题研究，涵盖诸如通信、导航、监视/空中交通管理（CNS/ATM）系统实施的经济和财务问题、航空公司运营经济的地区差异、民用航空的经济贡献、机场和空中航行服务的私有化和分配起降时刻的管理方面的影响等事项。

- 航空保安配套培训资料（ASTPs）和课程，内容涉及一系列题目，旨在协助保安专业人员、管理人员和工作人员更全面地理解国际标准和建议措施，以及根据当地方案，在各项措施和规定的实施和监控方面提供专门和实用的专业知识。如欲了解进一步情况，请与avsec@icao.int联系，或访问国际民航组织航空保安网站www.icao.int/avsec的培训网页。

- 电子形式的出版物是数据库或互动形式的，例如世界各种航空运输协定和国际民航组织的航空运输协定范本。民用航空统计资料可通过付费，年度订阅使用由国际民航组织商业网站www.icaodata.com发布的一个或多个数据系列。关于国际民航组织统计资料或特殊订购统计数据的问题应向sta@icao.int提出。

- 航空运输领域的会议报告包括关于简化手续和统计的专业类型会议的报告，以及与航空保安、国际航空运输的管理、机场和空中航行服务经济会议有关的报告。

ICAO 2007
8/07, C/P1/35

Order No. 9303P1-2
Printed in ICAO

ISBN 92-9194-944-2