ICAO

Doc 9303

机读旅行证件

第八版，2021年

第 1 部分：引言

经秘书长批准并授权出版

国际民用航空组织

ICAO

Doc 9303

机读旅行证件

第八版，2021年

第 1 部分：引言

经秘书长批准并授权出版

国际民用航空组织

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

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

Doc 9303 号文件 —《机读旅行证件》
第 1 部分 — 引言
ISBN 978-92-9265-352-1

修订

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

修订和更正记录

修订		
编号	日期	换页人

更正		
编号	日期	换页人

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

目录

1. 前言

国际民航组织机读旅行证件的工作始于 1968 年，当时理事会航空运输委员会成立了护照卡专家组。该专家组负责就标准化的机读护照本或护照卡提出建议，以加快旅客在护照检查点的通关速度。该专家组提出了一些建议，其中包括采用光学字符识别（OCR）作为选定的机读技术，因为该技术成熟、经济、可靠。1980 年，该专家组编写的规范和指导材料作为 Doc 9303 号文件第一版出版，标题为《具有机读能力的护照》，该文件成为澳大利亚、加拿大和美国最初签发机读护照的基础。

1984 年，国际民航组织成立了现称为机读旅行证件技术咨询组（TAG/MRTD）的小组，由专门从事护照和其他旅行证件签发和边检的政府官员组成，以便对专家组编写的规范进行增补更新。后来，咨询组的职权范围先被扩大到编写机读签证的规范，继而又被扩大到编写可用作官方旅行证件的机读卡的规范。

1998 年，机读旅行证件技术咨询组下的新技术工作组特别结合证件签发和移民方面的考虑，开始其建立在机读旅行证件应用中使用的最有效的生物特征识别系统及相关数据存储手段的工作。2001 年 9 月 11 日发生的事件促使各国更加重视旅行证件的安全性及其持有人的身份识别，截至此时，绝大部分工作业已完成。后来，全部工作迅速完成并得到机读旅行证件技术咨询组和航空运输委员会的认可。

后来，将关于生物特征和非接触式芯片技术的利用、逻辑数据结构（LDS）和公共密钥基础结构（PKI）的技术报告纳入了 2006 年的 Doc 9303 号文件第 1 部分（机读护照）第六版第 2 卷和 2008 年的 Doc 9303 号文件第 3 部分（机读官方旅行证件）第三版第 2 卷。

2. 范围

Doc 9303 号文件由多个不同文件组成，其中对一般规范（适用于所有机读旅行证件）以及与特定尺寸的机读旅行证件相关的规范做了分类。关于这些规范的概述，见第 5.1 节“Doc 9303 号文件的构成”。

这些规范并非旨在作为国民身份证件的标准。但是，一国颁发的身份证件被其他国家确认为有效旅行证件的，须使其身份证件的设计符合 Doc 9303 号文件第 3 部分、第 4 部分、第 5 部分或第 6 部分的规范。

虽然 Doc 9303 号文件第 4 部分中的规范旨在专门用于护照，但这些规范同样适用于其他 TD3 型身份证件，例如，通行证、航海人员的身份证件和难民旅行证件。

手头这份文件是第 1 部分。该部分介绍了 Doc 9303 号文件中的规范。它描述了 Doc 9303 号文件的十三个部分的结构、提供了关于国际民航组织的一般信息以及关于整个规范中所使用的术语和缩略语的指导。

3. 总论

3.1 国际民航组织的领导作用

国际民航组织牵头制定护照和其他旅行证件标准规范的做法，遵循了 20 世纪 20 年代国际联盟护照会议和国联的接替者联合国组织的工作所确立的传统。国际民航组织继续发挥领导作用的使命源于《国际民用航空公约》（《芝加哥公约》），该公约对高效、有序的民航运营提出了全面要求，其中包括关于人员通关的规定，即：

a) 航空旅行人员和机组遵守移民、海关和护照规章的要求（第十三条）；

b) 各国简化边境通关手续和防止不必要延误的要求（第二十二条）；

c) 各国在这些事项中相互协作的要求（第二十三条）；和

d) 各国制定和采取移民和通关国际标准程序的要求（第三十七条 j)）。

根据此项使命，国际民航组织制定和维持了供各成员国执行的附件9 —《简化手续》中的国际标准。在制定这些标准的过程中，一个基本的指导原则是，如果政府当局要简化对绝大多数航空旅行者的查验手续，它们必须对旅行证件的可靠性和查验手续的有效性胸有成竹，制定关于旅行证件及证件中所含数据的标准化规范，目的正是要建立这种信心。

国际民航组织大会在2004年申明，本组织应该作为一个高度优先的事项，开展加强旅行证件的安全性和完整性方面的合作。除了国际标准化组织以外，机读旅行证件技术咨询组的顾问还包括国际航空运输协会（IATA）、国际机场协会（ACI）和国际刑事警察组织（INTERPOL）。

2005 年，国际民航组织当时的 188 个成员国批准了一项新标准，即所有国家必须最晚在 2010 年根据 Doc 9303 号文件的规定，开始签发机读护照。最晚在 2015 年，所有非机读旅行证件必须失效。这一标准发布在附件 9 —《简化手续》第 13 版（2011 年）中。

3.2 机读旅行证件的相对成本和效益

根据Doc 9303号文件中规定的规范签发机读护照的经验表明，制作机读旅行证件的成本可能不会高于制作常规证件的成本，尽管实行生物特征识别和电子旅行证件后，成本会有所提高。随着交通流量的增加和更多的国家关注如何能够理顺利用计算机数据库和电子数据交换的通关程序，机读旅行证件将在增强的现代化监察系

统中起到关键作用。阅读证件和访问数据库的设备可能需要大量的资金投入，但是，可以预计，这种投入可以从此种系统所导致的安全性、通关速度和验证的精确性等方面的改进中得到回报。在自动通关系统中使用机读旅行证件，还可以使各国有可能取消对纸质证件如旅客舱单和登机/下机卡等的要求，以及节省与有关手工程序相关的行政费用。

3.3　运作

具有光学字符识别可读性的基本机读旅行证件是为了兼顾视读和机读而设计的。

国际民航组织各成员国认识到，标准化是必不可少的，护照和其他旅行证件采用Doc 9303号文件规定的标准格式的益处，不仅限于对装有自动通关系统中使用的机读设备和数据库的国家具有明显的好处。实际上，这种证件本身的物理特征和数据安全特性可强有力地防止篡改、伪造或假冒。不仅如此，在机读旅行证件的视读区采用标准化格式还可便于航空公司人员和政府官员进行查验，其结果是，低危旅客的通关速度会加快，有问题的情况更易于鉴别，执法会更加有力。选择性地采用生物特征识别技术并将数据存储在非接触式集成电路中，将会增强安全性和更有力地预防诈骗，使合法证件持有人更容易获得旅行签证，更容易通过边检系统。

注：确实，将会发生边检时电子机读旅行证件不能与阅读器正确对接的情况。可能发生这种情况的原因有几个，而电子机读旅行证件故障仅为其一。国际民航组织强调，发生阅读故障的电子机读旅行证件仍然是有效证件。但是，阅读故障也可能是伪冒攻击的结果，接受国应该建立本国处理这种可能性的程序，其中应该包括更加严格地检验证件和证件持有人，但是，也应考虑到故障不涉及伪冒故意的情况。

3.4　国际标准化组织的认可

Doc 9303号文件中涉及技术规范的各节已经得到国际标准化组织的认可，被定为ISO标准7501。使这种认可成为可能的是一种联络机制，在国际标准化组织的主持下，旅行证件、阅读器及其他技术的制造商通过这一联络机制将技术和工程意见提供给旅行者身份识别方案技术咨询组。依托这种工作关系，国际民航组织制定的规范通过国际标准化组织内的一种简化程序已经获得，预计将会继续获得全球标准的地位。

与国际标准化组织的联络机制不仅被成功地用于将新的旅行证件规范认定为ISO标准，而且也被成功地用于批准对这些规范的修订。因此，Doc 9303号文件随后的修订将以和以前同样的方式处理，以获得国际标准化组织的认可。

4. 定义和参考资料

4.1 缩略语

缩略语	全称
3DES	三重数据加密标准
AA	主动认证
ABC	自动化边境管制
AFS	反欺骗专家
AES	高级加密标准
AID	应用标识符
APDU	应用协议数据单元
AO	审批官员
BAC	基本访问控制
BER	基本编码规则
BLOB	二进制大对象
BSC	条形码签名证书
CA	认证机构—亦是—芯片验证
CAM	芯片认证映射
CAN	卡访问号
CAR	认证当局编号
CBC	密码组块链接
CBEFF	生物特征通用交换格式框架
CCD	电荷耦合装置
C_{DS}	证件签名证书
CIC	无接触集成电路芯片
CID	卡标识符
CMAC	基于密码的消息验证码
CMOS	互补式金属氧化物半导体
CRL	证书撤销列表
CSCA	国家签署证书当局
CSD	相机到拍摄对象的距离; 人眼平面与相机镜头光学中心之间的距离
CVCA	国家验证认证机构
DER	唯一编码规则

缩略语	全称
DES	数据加密标准
DF	专用文件
DG	数据组
DH	DH 密钥交换协议
DN	唯一甄别名
DO	数据对象
DOVID	衍射光可变图像装置（具有衍射光可变效果的特征，例如：全息效果）
DS	证件签名人
DSA	数字签名算法
DTA	电子旅行批准
DTBS	待签名的数据
DV	证件核验人
EAL	评估保证级别
ECDH	椭圆曲线密钥交换协议
ECDSA	椭圆曲线数字签名算法
ECKA	椭圆曲线密钥协商
EEPROM	电可擦可编程只读存储器
EF	基本文件
EM	口眼间距
eMRP	电子机读护照
eMROTD	电子机读官方旅行证件
eMRTD	电子机读旅行证件
eRP	电子居留证
ERZ	有效阅读区
ETS	电子旅行系统
EVZ	眼睛可见区；覆盖一个矩形的区域，其距离 V 至少为眼间距与可见眼球任何部分的 5%
FAR	错误接受率
FIPS	联邦信息处理标准
FRR	错误拒绝率
GM	通用映射
HD	水平偏角；人的鼻子与相机镜头之间假想线水平的最大允许偏差
IC	集成电路

缩略语	全称
ICAO	国际民用航空组织
ICC	集成电路卡
IED	眼间距
IFD	接口设备
IM	合成映射
IR	红外光
IS	查验系统
IV	初步引导
LDS	逻辑数据结构
MAC	消息验证码
MF	主文件
MRP	机读护照
MROTD	卡式机读官方旅行证件
MRTD	机读旅行证件
MRV-A	全尺寸 A 型机读签证
MRV-B	小尺寸 B 型机读签证
MRZ	机读区
MTF	调制传递函数
MTF20	调制传递函数为 20％或更高的最高空间频率
NAD	节点地址
NIST	国家标准技术研究所
NTWG	新技术工作组
OCR	光学字符识别
OCR-B	ISO 1073-2 定义的光学字符识别字体
OID	客体标识符
OVD	光学可变装置
OVF	光学可变特征
OVI	光学可变油墨
PACE	口令认证连接确立协议
PCD	接触式耦合装置
PICC	接触式集成电路卡
PIX	专有识别符扩展

缩略语	全称
PKD	公钥目录
PKI	公钥基础设施
RID	注册标识符
RFID	射频识别
RGB	红绿蓝
ROI	相关地区
ROM	只读存储器
RSA	RSA 公钥算法
SFR	空间频率响应
SHA	安全散列算法
SM	安全通讯
SNR	信噪比无线电
SO_D	证件安全对象
SPOC	单一联络点
sRGP	利用 ITU-R BT.709 三原色为用于显示器、打印机和互联网而创建的标准红绿蓝色彩空间
SSC	发送序列计数器
TA	终端验证
TAG/MRTD	机读旅行证件技术咨询组
TAG/TRIP	旅行者身份识别方案技术咨询组
TD1	1 型机读官方旅行证件
TD2	2 型机读官方旅行证件
TD3	3 型机读旅行证件
TLV	标志长度值
TR	技术报告
UID	唯一标识符
UV	紫外光
VDS	可见数字印章
VIS	欧盟签证信息系统
VIZ	视读区
VS	签证签名人
VVA	签证验证当局
WSQ	小波标量量化

4.2 术语和定义

术语	定义
1:1 应用案例	将样本照片与所声称身份的登记样本进行比较的生物识别过程（算法），也称作验证。
1:N 应用案例	在数据库中未登记的样板中搜索先验未知样本照片的生物识别过程（算法），也称作身份识别。
自动化边境管制门	用于电子机读旅行证件的自动化边境管制门。
奥多比系统公司（Adobe）红绿蓝	红绿蓝色彩空间旨在囊括四分色彩色打印机可实现、但在计算机显示器等装置上使用红绿蓝三原色却无法实现的大多数色彩。
算法	运算用的特定数学过程；如遵守会给出规定结果的一整套规则。
防扫描图案	一种通常由变化的角位移细线构成、嵌在安全底纹中的图像。在正常观察时，该图像不能与安全底纹的其余部分区分开来。但是当原件被扫描或复印时，这种嵌入的图像就变得可见了。
应用标识符（AID）	识别一项应用的数据元素。电子机读旅行证件应用使用四种类型的应用标识符中的一种，即标准应用标识符。由一个注册的应用提供者标识符（RID）和一个专有应用识别符扩展（PIX）组成。
非对称	通信链各终端需要不同密钥。
非对称算法	这种类型的加密操作使用一个密钥对明文进行加密，而用另一个密钥对相关密文进行解密。这两个密钥相互关联，称为一个密钥对。
非对称密钥	一个分离但相互关联的用户秘钥对，由一个公钥和一个私钥组成。每一密钥都是单向的，意味着用于信息加密的密钥，不能用来对同一信息进行解密。
认证	验证电子事项参与者所称身份的过程。
验证数据库	在此数据库中，为每个证件模型实施检查程序的验证算法。
验证数据集	验证数据库之内一套具体的证件模型的检查程序。
真实性	确认逻辑数据结构及其组成部分是由签发国或签发机构创建的能力。
授权	决定是否可给予一项服务的安全过程。
旅行批准	接收国签发的批准旅行者开始旅行的非实物和/或实物批准。
经授权的接收组织	受权受理官方旅行证件，并因此今后可能被允许记录可选扩容技术细节的组织（例如，航空器运营人）。

条形码	一维或二维光学可机读的表示形式，用于表示与其所附物体有关的数据。
条形码签名人	条形码签名人对条形码中编码的数据（标题和消息）进行数字签名。 签名也存储在条形码当中。
条形码签名证书（BSC）	条形码签名证书是包含条形码签名公钥的证书。条形码签名证书用于核验采用条形码签名私钥的数据有效性。
条形码符号表示法	消息与条形码之间的映射称为符号表示法。此类映射的定义载于条形码规范，并且包含单个数字或字符的编码、条形码周围所谓分割区的尺寸，以及用于纠错的对校验和的计算。
个人资料	证件持有人的详细个人化信息，它以文字形式显现于机读旅行证件的视读和机读区，或机读证件的芯片上（若有）。
生物特征	用于识别登记者身份或验证其宣称身份的、可测量的、唯一的生理特征或个人行为特征。
生物特征数据	从生物特征抽取而来的信息，可用来建立参考模板（模板数据）或与先前已建立的参考模板相比对（比对数据）。
生物特征识别	通过测量机读旅行证件持有人的一项或多项个人特征来识别或确认其身份的一种手段。
生物特征匹配	用一种算法将生物特征参考模板与取自现场的生物特征样本进行比对，以确定其匹配或不匹配的过程。
生物特征参考模板	界定一个人的生物特征测量的数据集，作为与以后交验的生物特征样本进行比对的基础。
生物特征样本	所采集到的离散、明确、唯一且语言中性的原始数据，代表生物特征系统所采集的某一登记者的生物特征（例如，生物特征样本可包括用于认证目的的指纹图像及其派生物）。
生物特征系统	一个具有下列功能的自动系统： 1. 从机读护照的终端用户身上采集生物特征样本； 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与一个或多个参考模板中所含的生物特征数据相比对； 4. 确定数据的匹配度，即按照所涉事项对登记者进行明确识别和个人认证的要求，执行基于规则的匹配过程；和 5. 指明是否已取得身份识别或验证。
生物特征模板	从生物特征样本中提取并压缩的数据。
生物特征验证	通过测量和验证机读旅行证件持有人的一项或多项唯一的个人特征，识别或确认其身份的一种手段。

位	二进制位数字。数字编码中不能再小的信息单元。
黑白线设计	通常以扭索纹形式表现，有时被用作安全证件边饰的、由细线组成的设计稿。该设计稿经工艺过程加载至页面时，会由阳图变为阴图。
分组	分组算法赖以操作的位串或位组。
分组算法	见分组密码。
分组密码	按位块（串或组）操作的明文加密算法。
自扩展方法	测验数据集可靠性的一种方法。
根源证件	申请旅行证件时作为身份证明的文件。
蛮力攻击	尝试各种可能的秘钥并检查所产生的明文是否有意义。
字节	通常作为一个单元操作的八位序列。
说明文字	用于识别数据域的印刷字或字句。在特殊情况下，当多个不同的官方语文不适合数据域时，可以使用数字。必须在机读护照上的另一个位置为这些数字附带解释性文字。
采集	从终端用户身上获取生物特征样本的方法。
卡	一种符合 ISO/IEC 7810，ISO/IEC 7811，ISO 7812 标准、用于传载信息的媒介。
证书	证明密钥对属于证书所标识的某个人或硬件或软件组件的电子文件。证书由认证机构签发。通过签署证书，认证机构批准个人身份或组件与密钥对之间的联系。如果证书不再证明这一联系的有效性，则可以撤销证书。证书具有有限的有效期。
证书撤销列表（CRL）	已撤销的证书列表。因此，将不再信任与证书撤销列表所载证书相关联（由其签名）的证件。
证书认证机构（CA）	为公钥基础设施签发数字证书的可信机构。
检查算法	启用具体实施检查程序的软件组件（例如：模式搜索）。
检查程序	对功能具体属性的测试程序（例如：利用红外灯检查照片呈现的情况）。
化学防涂改剂	用来防止通过化学擦除的方法篡改证件的安全试剂。如果用此方法篡改证件，漂白剂和溶剂与证件接触时，会在证件上出现不可涂改的颜色。
下巴	下颌中央前部。
国际照明委员会标准光源 D65	国际照明委员会（CIE）界定的 D 系列照明光源之一部分的常用标准光源，旨在描绘世界不同地区的露天标准照明条件。
密文	基于密钥或预定规则或符号集的隐秘书写。

排序标记	见索引标记。
变色油墨	根据观察角度和/或刺激（光）源的质量而改变其视觉特性的油墨。
比对	将生物特征样本与之前存储的参考模板或多个模板进行比较的过程。另见“一对多”和“一对一”。
非接触式集成电路	根据ISO/IEC 14443标准，用于存储机读旅行证件数据并通过射频能量与阅读器沟通的一种半导体装置。
通用生物特征交换格式框架（CBEFF）	便于生物特征数据交换和互操作性的通用文档格式。
控制号	为记录和安全目的，在制造时为证件指定的序号。
伪造品	真实的安全证件未经授权的副本或复制品，不管它是采用什么手段制作的。
国家代码	根据ISO 3166-1规定，用于标示证件签发机构或证件持有人国籍的二字或三字代码。
裁切系数	全画幅相机（43.3 mm）对角线与所选相机图像传感器对角线的比率。通过斟酌裁切系数，可以确定与全画幅相机等效视角的适当焦距镜头。
头顶	除去毛发，头的顶部。
密码学	使用算法和密钥将信息转换为密码书写、不易理解的形式的科学。
数据加密标准（DES）	联邦信息处理标准 46-3 中规定的数据加密方法。
数据特征	在证件数据或图像结构中纳入的编码信息，其通常是纳入到个人化数据，特别是肖像中。
数据组	归类于逻辑数据结构的一系列相关数据要素。
数据页	包含证件持有人个人资料的护照页，最好是第二页或倒数第二页。见“个人资料”。
待签名的数据（DTBS）	作为签名方案的签名生成算法之输入提供的消息。
解密	通过使用密钥将加密文件恢复原状的行为。
偏差列表	由签发国签发的、说明旅行证件和/或秘钥和证书方面的不合规情况的已签名列表。
偏差列表签名人	使用电子化方式在偏差列表上签名的实体。偏差列表签名人由其国家签署证书当局授权，通过签发偏差列表签名人证书来履行这一职能。

衍射光可变装置	在其结构内载有全息图或同等图像的安全特征，图像的外观随着视角或光源入射角度的不同而变化。
衍射光可变图像装置（DOVID）压层膜或涂层保护膜	内含衍射光可变图像装置的压层膜或涂层保护膜，覆盖住证件所有部分或放置在关键数据位置以对其加以保护。
数字（密码）签名	一种通过电子方式对信息进行验证的密码操作的结果。这不是以数字形式显示的机读旅行证件持有人的数字签名。
数字签名算法（DSA）	美国国家标准与技术研究院在联邦信息处理标准 186 中颁布的不对称算法。该算法仅提供数字签名函数。
数字（加密）签名方案	三种算法的元组。 钥匙生成算法将安保参数作为输入，并输出由私钥和公钥组成的钥匙对。 签名算法将私钥和消息作为输入，输出由私钥和公钥组成的钥匙对，并输出加密签名。验证算法将公钥、消息和签名作为输入，如果对钥匙对的私钥和消息使用了签名生成算法作为输入生成了签名，则输出“有效”，否则输出“无效”。
（数字）证件特征	可用于验证证件内容的证件属性。 例如：持有人的姓名、或签发日期、或证件持有人的打印图像等文本资料。数字证件的特征是证件特征的数字化版本。
数字印章	可见数字印章的简称。
电子旅行批准	在签发国国内发行和保持的电子签证。
数字水印	见信息隐藏。
目录/公钥目录（PKD）	信息存储库。一般来说，公钥基础设施的公钥簿，即是该公钥基础设施认证机构签发的公钥加密证书连同其他客户信息的存储库。公钥簿还保存交叉证书、证书撤销表和授权撤销表。
显示签名	原始的手写签名或使用数字印刷复制的原始签名。
空白证件	空白证件即为未载有个人化信息的旅行证件。一般来说，空白证件是创建个人化旅行证件所用的基本材料。
证件模型	证件模型涵盖具有相同光学外观的一个国家的证件系列（例如：（D，P，1，2005）、（D，P，2，2007）和（D，P，3，2010）。一个国家可以在特定的时间流通多个有效的证件模型（例如：（GBR，P，1，2008）和（GBR，P，2，2010）。
证件号	证件的独特识别号。建议证件号与控制号相同。
证件签名人	签发生物特征证件并以可以检测伪造情况的方式证明存储在该证件中的数据是真实的机关。

复式图案	一种由细小不规则互锁形状构成的图案，以两种或多种颜色印刷，为保持图案的完整性，需要非常紧凑的套准印刷技术。
窃听	未经授权截取数据通信。
有效阅读区（ERZ）	所有机读旅行证件通用的固定尺寸的机读区，证件阅读器能借此阅读其中的机读数据。
电可擦可编程只读存储器（EEPROM）	数据可以电擦除和改写的非易失性存储技术。
电子机读护照（eMRP）	附加内置非接触式集成电路，可以识别证件持有人的生物特征的、符合 Doc 9303 号文件第 4 部分规范的 TD3 型机读旅行证件。通常称为“电子护照”。
电子机读官方旅行证件（eMROTD）	附加内置非接触式集成电路，可以识别证件持有人的生物特征、符合 Doc 9303 号文件第 5 部分或 Doc 9303 号文件第 6 号部分规范的 TD1 型或 TD2 型机读旅行证件。
电子机读旅行证件（eMRTD）	内置非接触式集成电路、符合国际民航组织 Doc 9303 号文件《机读旅行证件》相关部分规定的标准，能对机读旅行证件持有人进行生物特征识别的机读旅行证件（护照、签证或卡）。
嵌入图像	经过编码处理的或隐藏在主要视觉图像内的图像或信息。另见信息隐藏。
加密	通过密钥来伪装信息，使未经授权者无法解读的做法。
终端用户	与生物特征系统进行交互以便登记或使其身份得到验证的人。
登记者	由签发国或签发机构为其签发机读旅行证件的人，即自然人。
登记	从一个人身上收集生物特征样本，经处理并储存代表该人身份的生物特征参考模板的过程。
电子护照	电子机读护照的通用名称。见电子机读护照（eMRP）。
曝光值（EV）	代表照相机快门速度与孔径焦距比的综合数字，因此，产生相同曝光的所有组合都具有相同的曝光值。
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。

眼的中心	眼的内、外角连接线的中心。 注 1：根据 ISO / IEC 14496. -2 的定义，眼的中心是特征点 12.1 和 12.2。 注 2：ISO / IEC 14496-2 界定了眼的内、外角。其特征点是右眼 3.12 和 3.8；左眼特征点是 3.11 和 3.7。
口眼间距	面部中心 M 与嘴的中点之间的距离（ISO / IEC 14496-2 所载的特征点是 2.3）。
面部中心	两只眼睛中心连接线的中点。
获取失败	生物特征系统未能获得为某人登记所需的生物特征。
登记失败	生物特征系统未能为某人登记。
错误接受	生物特征系统错误地识别了某人，或者根据所声称的身份错误地验证了某位冒名顶替者。
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名顶替者的概率。给定的错误接受率通常对被动冒名顶替者进行的尝试做出假定。错误接受率可估算为：FAR = NFA/NIIA 或 FAR = NFA/NIVA，其中 FAR 是错误接受率、NFA 是错误接受次数、NIIA 是冒名顶替者尝试身份识别的次数、NIVA 是冒名顶替者尝试验证的次数。
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记者的数据不匹配时反而被接受时出现的混淆。在这种应用中，接受和拒绝这两个概念被颠倒了，因此，就颠倒了“错误接受”和“错误拒绝”的意思。
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记者的数据相匹配时反而被拒绝时出现的混淆。在这种应用中，接受和拒绝这两个概念被颠倒了，因此，就颠倒了“错误接受”和“错误拒绝”的意思。
错误拒绝	生物特征系统未能识别登记者或未能验证登记者声称的合法身份的情况。
错误拒绝率（FRR）	生物特征系统未能识别登记者或者验证登记者声称的合法身份的概率。错误接受率可估算如下：FRR = NFR/NEIA 或 FRR = NFA/NEVA，其中 FRR 是错误拒绝率、NFR 是错误拒绝次数、NEIA 是登记者尝试身份识别的次数、NEVA 是登记者尝试验证的次数。这一估算假定登记者的身份识别/验证尝试代表了所有登记者的身份识别/验证尝试。错误拒绝率通常不包括“获取失败”错误。
特征	适于证明真实性的证件要素（例如：吸收红外的照片）。
纤维	在制造过程中嵌入基材中的细小线状微粒。
域	一个区内用于登记单个数据元素的特定空间。
指纹	证件持有人指尖表面构造的一个（或多个）可视化复现。

荧光油墨	含有在特定波长的光（一般为紫外线）照射下能发光的材料的油墨。
伪造	对真实证件的任何部分进行伪造。
变造	是指变造真实证件，以便使未经授权者能够使用该证件进行旅行、或者前往未经授权的目的地。真实证件持有人的个人详细资料，特别是肖像，是此种变造的主要对象。
正背（透视）对印技术	印刷在证件内页两面上的一种图案，在透射光下观察该页，构成一个连锁的图像。
完整面部图像	持有根据 Doc 9303 号文件中制定的规范而制作的机读旅行证件的人的肖像。
全尺寸（A 板式）机读签证（MRV-A）	符合Doc 9303号文件第7部分中所载尺寸规范的机读签证，其大小覆盖整个护照签证页。
库藏集	以前登记的个人生物特征模板数据库，可对其进行搜索以查找试样。
鬼像	见阴影图像。
全球互操作性	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。全球互操作性是用于在所有电子机读旅行证件中放置视读和机读数据的标准化规范的主要目标。
全球互操作生物特征	参见 Doc 9303 号文件第 9 部分中所述的人脸图像。
扭索纹图案	通常由计算机生成的一种由连续细线形成的图案，它构成一种独特图像，只能通过创建原图案使用的设备、软件和参数才能准确复原。
散列	一种数学公式，用以将任何长度的报文转换成代表原始报文即所谓“报文摘要”的唯一固定长度数据串。散列是一个单向函数，也就是说，通过逆转过程来确定原始报文是不可行的。散列函数也无法从两个不同的输入值中得出相同的报文摘要。
热封层压膜	通过加热加压，黏合在护照个人资料页上的一种层压膜。

持有人	拥有机读旅行证件，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记或者核实自身身份的人。
国际民航组织公钥簿	用作参与者签发的证件签名证书、国家签署证书当局主列表，国家签署证书当局链接证书和证书撤销列表存储库的中央数据库，以及为促进对电子机读旅行证件所载数据进行验证，由国际民航组织代表参与者进行维护的其世界范围分发系统。
识别	这是一个一对多过程，即将交验的生物特征样本与在档的所有生物特征参考模板进行比对，以确定它是否与其中任一模板匹配，如果匹配，进而再确定与模板匹配的电子机读旅行证件持有人的身份。使用一对多方法的生物特征系统谋求在数据库中找到一个身份，而不是去验证一个声称的身份。对照“验证”。
识别卡（ID-card）	当作身份证件使用的一种卡。
标识符	独一无二的数据串，在生物特征系统中用作为一个人的身份及其相关属性命名的关键字，机读旅行证件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身体特征、数据及基本属性的集合。在生物特征系统中，身份通常在个人通过使用所谓的“根源证件”如出生证，公民证书等在该系统中登记时确定。
身份证件	用来识别其持有人和签发者的证件，其中可载有该证件设计用途所必需的数据。
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现形式。它以生物特征识别为目的，以数字形式保存。
冒名顶替者	通过采用虚假身份来申请并获得证件的人，或为使用另一个人的证件而改变本人外表以使自己看上去像该人的人。
序号	按照连续的顺序印在每页外缘的符号，从首页顶部开始到下一页较低位置。最后一页的注册号出现在底部。这种印刷方法可让连续的条纹出现在护照边缘。任何已被去除的页将被登记为缺页。当使用紫外线颜色印刷时，这种条纹只有在紫外光下才变得可见。也被称为校对号。
红外隐形油墨	在可见光谱部分光的照射下，能够形成可见图像，而在红外线区域内不能被探测到的一种油墨。
红外油墨	在红外光光谱下可见的油墨。
初始化（智能卡）	将大批量卡的通用数据置入持久性存储器（如电可擦可编程只读存储器等），同时包括最低量的卡唯一项目（如集成电路卡序号和个人化密钥）的过程。
查验	国家或机构检查旅行者（机读旅行证件持有人）呈递的机读旅行证件并且验证其真实性的行为。

查验系统	任何需要对机读旅行证件进行认证，并将其用于身份验证的公、私实体，如边境管制当局、航空公司及其他运输运营人，金融机构等所使用的机读旅行证件检查系统。
凹版印刷	制作安全证件使用的一种印刷工艺，在印刷时使用高印刷压力和特种油墨在证件表面产生一种具有触感的浮雕图像。
集成电路（IC）	用于进行处理和/或存储的一种电子组件。
集成电路卡（IC card, ICC）	嵌入了一个或多个集成电路的卡。
完整性	确认逻辑数据结构及其组件与签发国或签发机构创建的逻辑数据结构相比没有发生改变的能力。
眼间距	左眼与右眼眼睛中心连接线的长度。
接口	两组件间联接的标准化技术定义。
接口设备	集成电路卡运行时与之联接的任何终端、通信设备或机器。
互操作性	几个独立的系统或子系统组件一起工作的能力。
虹膜（印刷）	见彩虹印刷。
签发人	签发机读旅行证件的机构。
签发人数据块	签发国或签发机构写入可选扩容技术的一系列数据组。
签发机关	经官方认可的向正当持有人签发机读旅行证件的实体。
签发国	签发机读旅行证件的国家。
签发机构	被授权签发官方旅行证件的组织（如作为通行证签发人的联合国组织）。
JPEG 和 JPEG2000	图像数据压缩的标准，特别用于人脸图像的存储。
密钥交换	将会话密钥发送至会话方手中的过程。
密钥管理	将密钥提供给经授权的通信方之间使用的过程。
密钥对	一个公钥和一个私钥组成的一对数字密钥，用于数字信息的加密和签名。
标签	用作护照内数据页的自粘贴纸。这不是通常推荐的做法，尤其不是针对有效期更长的证件的做法。
通行证	由超国家实体（例如联合国）签发的、一般类似于护照的证件。
层压膜	具有安全特征的透明材料，用于牢固地黏合在证件上以保护证件上的个人资料或证件其他页。

激光刻蚀	采用激光将个人化数据“刻录”进基材的一种工艺过程。数据包括文本、肖像和其他安全特征。
激光穿孔	采用激光在基材上穿孔创建数字、字母或图像的一种工艺过程。
潜像	在浮雕图像中形成的一种隐蔽图像，该图像由不同方向和外形的线结构组成，从而使该隐蔽图像只能在预定的角度才能看到，这由凹版印刷来实现。
透镜特征	将镜头结构置入证件表面或用作验证装置的一种安全特征。
一级查验	在使用站点进行粗略的检查以快速查验（容易目视识别的特征或触觉特征）。
二级查验	经过培训的查验员使用简单设备进行的检查。
三级查验	法医专家进行的查验。
现场采集	通过机读旅行证件持有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。
锁定（芯片）	实行个性化之后，必须将芯片锁定。这意味着不能继续执行个性化命令，并且不能继续将个性化数据写入芯片。只有成功执行认证机制（TA）后，才能将数据写入芯片。被锁定的芯片不能被“解锁”。
逻辑数据结构（LDS）	逻辑数据结构描述在电子机读旅行证件的非接触式集成电路中如何存储数据和格式化数据。
机器辅助证件验证	使用某种装置从数据和/或安全的角度辅助验证证件真实性的程序。
机读官方旅行证件（MROTD）	这种证件的通常形式是类似于TD1或TD2尺寸的卡，符合Doc 9303号文件第5部分和第6部分所载规范，经有关国家协议可以此通行国际边境。
机读护照（MRP）	符合 Doc 9303 号文件第 4 部分中所载规范的护照。通常制作成 TD3 尺寸大小，包含关于证件持有人信息和签发国或签发机构信息的页和用于签证和其他签注的页。机读信息载于两行由 ISO 1073-2 定义的光学字符识别字体书写的文字中，每行 44 个字符。
机读旅行证件（MRTD）	由某一国家或签发机构签发供证件持有人用于国际旅行的、符合Doc 9303号文件中所载规范的官方证件（如机读护照、机读签证、机读官方旅行证件），该证件载有强制性视读（肉眼可读）数据和一个以可机读格式存储的单独的强制性数据概要。
机读签证（MRV）	符合Doc 9303号文件第7部分所载规范的签证。机读签证通常附于护照签证页上。
机读区（MRZ）	位于机读旅行证件上的一个固定尺寸的区域，所载的强制性和选择性数据是为了使用光学字符识别方法进行机读而加以格式化的。

机器可验证的生物特征	以电子化方式存储在电子机读旅行证件芯片中的一种独特的个人身份识别人体特征（例如人脸图像、指纹或虹膜）。
放大失真	放大倍率随距离相机的间距以及面部景深而变化的图像瑕疵。
主密钥	密钥衍生链的根。
主列表	主列表是发布主列表的接收国“信任”的以数字形式签署的国家签署证书当局之证书的列表（参见 Doc 9303 号文件第 12 部分）。
国家证书列表签名人	对国家签署证书当局证书的国家证书列表进行数字签名的实体。国家证书列表签名人由其国家签署证书当局授权，通过签发国家证书列表签名人证书来履行这一职能。
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。
消息	发报人传送给收报人的最小有效信息的集合。这种信息可以包含一项或多项卡查验或有关卡查验的信息。
消息认证码（MAC）	消息认证码是附在消息内的消息摘要。除非知道秘密，否则无法对消息认证码进行计算或验证。它由发报人附加，收报人验证，从而得以发现消息伪造。
金属油墨	外观呈现金属质感的油墨。
同色异谱油墨	两种油墨经过配制，在特定条件，通常是日光照射下，呈现出同样的颜色，但在其他波长的照明下则显示不同颜色。
缩微印刷	小于 0.25 毫米/0.7 派卡的印刷文字或符号。
摩尔纹	由于拍摄场景或物体所包含的重复性细节（例如：线、点等）超出了相机传感器的分辨率而导致的类似于波状图案的假影。
变形	将两个或多个拍摄对象的脸部变形或融合在一起，从而在照片中形成单个脸部的图像处理技术。
测量模式	测量图案的边长：强度测量区域为正方形，尺寸为眼间距的 30%； 它们用于测量脸颊、额头和下巴的照明强度。
机读护照数据页	机读护照内包含有视读和机读数据标准化显示的固定尺寸页。
多生物特征	使用一种以上的生物特征。
非易失性存储器	断电后仍能保存其内容的半导体存储器（如只读存储器、电可擦可编程只读存储器等）。
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	管理电脑所用各种应用程序的程序。
光可变装置（OVD）	所显示的颜色和/或外观图像随着观察角度或验证条件不同而变化的安全特征。
光可变特征（OVF）	外观的颜色和/或图案随着观察或照射角度不同而变化的图像或特征。这样的例子有：包括具有高分辨率的衍射结构（衍射光可变图像装置）的特征、全息图、变色油墨（例如具有光可变特性的油墨）和其他衍射性或反射性材料。
带外传输	指在之前确定的传输方法或通道之外进行的传输。
涂层保护膜	可以加到证件表面上以代替层压膜的一种超薄型薄膜或保护涂层。
填充	在数据串任一边附加额外的二进制位直到预定长度。
视差	沿两条不同的视线看到、由这两条线之间的倾斜角或半角进行测量的物体表观位置的位移或差异。
渗透性编号油墨	含有颜料成分并能渗透到基材深处的油墨。
个人身份识别码（PIN）	用作本地一对一核对机制的数字安全码，其目的在于确定持卡人是否的确是经授权可以获得或使用某一具体服务的自然人，如打开卡上所存的某些信息的权利等。
个人化	把肖像、签名和个人资料加到证件上的过程。
磷光油墨	含有一种颜料的油墨，该颜料在特定波长的光照射下会发光；在去除光源后，这种活性光仍然可见，但随后会变暗。
照相亭	用于在公共场所或办公环境中以数字形式拍摄身份照片的自动系统；它将拍摄对象封闭在高度受控的照明环境中，其中包括照相机、照明装置和打印机等外围装置；它的一侧或两侧设有入口，并带有反射帘幕以遮挡环境光线。
光致变色油墨	在特定波长的光照射下，颜色发生可逆变化的油墨。
摄影棚	用于在柜台式环境中以数字形式拍摄身份照片的半自动系统；其中包括照相机和照明，并且通常在拍摄对象的后面放置一块单独的面板，以便提供所需背景，但除此之外则是开放形式。
照片替换	证件签发后将证件上的肖像换成他人肖像的一种伪造。
实际签证	贴在旅行者护照上的箔纸型旅行证件。

物理安全	在制作和个人化过程中实施的一系列安全措施，以防止盗窃和非授权进入该过程。
PKD参与者	遵循国际民航组织公钥目录参与协议的、签发或意图签发电子机读旅行证件的国际民航组织成员国或其他实体。
肖像	印刷及电子存储方式的机读旅行证件持有人面部图像的直观显示。
展示攻击	以可能干扰生物识别系统预期策略的方式向生物识别捕获子系统呈现人工制品或人类特征。
展示攻击检测	自动确定的展示攻击。
私钥	公钥密码技术中用以解密或签署信息的集成非对称钥匙对的私钥部分（只有用户知道）。
试样	身份有待确定的登记者的生物特征样本。
公钥	集成不对称密钥对中的公用成分，用于加密或验证信息。
公钥证书	经认证机构签名从而不会被遗忘的某一实体的公钥信息。
公钥密码学	一种不对称加密的形式，其中所涉各方都拥有由一个私钥和一个公钥组成的密钥对，用于数据的加密和数字签名。
公钥基础设施（PKI）	用以验证、登记和认证安全应用用户的一套政策、流程和技术。公钥基础设施应用公钥密码学和密钥认证措施，确保通信安全。
公钥系统	一种应用密钥对的密码方法，其中一为私钥，一为公钥。如果加密用公钥，解密就必须用相应的私钥，反之亦然。
径向畸变	图像瑕疵，其中放大倍数随距离光轴的间距而变化。
彩虹印刷（虹膜或隔色印刷）	这种技术是在印刷机上同时使用两种或多种颜色的油墨进行印刷，让这几种颜色进行融合，从而使其产生与彩虹类似的效果。也被称为棱镜印刷或虹膜印刷。
随机访问	一种数据存储方法，可以检索到特定的数据项而不需要依次访问所有的存储数据。
随机访问存储器（RAM）	集成电路中使用的一种可以随机访问、有电才能保存数据的易失性存储器。
反应油墨	含有安全试剂的油墨，用来防范通过化学擦除（删除）来试图对证件进行篡改，这样，当漂白剂和溶剂与证件接触时就会发生可察觉的反应。
只读存储器（ROM）	通常在集成电路制作过程中一次写成的非易失性存储器。用以存储查验中的操作系统和集成电路卡中半导体使用的算法。

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。
接收者数据组	签发国或经授权的组织写入可选扩容技术的一系列数据组。
接收国	查验证件持有人的机读旅行证件的国家。
参考数据集	参考证件的可见、红外和紫外线图片，定义了对应证件模型的检查程序。
参考证件集	其参考数据集被用来定义检查程序的一组证件。
注册	使一个人的身份被生物特征系统获知的过程，该过程将独特的标识符与该身份相关联，收集与该人相关的属性并将其记录到生物特征系统中。
注册机构（RA）	负责数字证书申请人的识别和认证的人或机构。注册机构不签发或签署证书。
浮雕（3-D）设计（团花图案）	一种加入了图像的安全背景图案，这种图像的生成方式给人一种错觉，使人觉得它在基材表面是凸起或凹陷的。
响应	从属方处理完收到的命令后向主方返回的报文。
RSA 公钥算法（RSA）	Ron Rivest,、Adi Shamir 和 Len Adleman 发明的一种非对称算法。用于公钥加密，其依据的事实是将两个大的质数相乘容易，将乘积除净则难。
匹配分值	一个从低到高的数值范围内的某个值，用于衡量生物特征试样模板记录（被搜索的人）与某个特定的模板库记录（先前登记者）之间成功匹配的程度。
副像	通过任何手段在证件他处复制的证件持有人肖像的重复图像。
安全散列算法（SHA）	美国国家标准和技术研究院规定的哈希函数，并被颁布为联邦信息处理标准 180。
安全消息	受到保护免遭非法变造或发送的消息。
安全线	在造纸过程中嵌入或部分嵌入基材的塑料或其他材料的细条。可使这种细条金属化或部分地去金属化。
透视对印技术（正背对印）	见正背对印技术。
敏感数据	这些数据被认为比非敏感数据更具隐私敏感性。对敏感性数据的访问**应该**设置更多限制。Doc 9303-11 号文件规定了终端认证作为访问敏感性数据的可互用机制。如果不要求可互用性，则可以使用其他机制。
阴影图像	为用作“鬼影”的同义词：将证件持有人肖像的色彩对比和/或饱和度和/或尺寸缩小，在证件上复制的肖像的副像。

页	包含一张以上护照页的护照中的单独一片基材。
1型机读官方旅行证件（TD1）	符合ID-1型卡规定的尺寸（ISO/IEC 7810）（不包括厚度）的卡。
2型机读官方旅行证件（TD2）	符合ID-2型卡规定的尺寸（ISO/IEC 7810）（不包括厚度）的卡或标签。
非法浏览	未经准许通过电子方式阅读存储在证件中非接触式集成电路内的数据。
小尺寸（B型）机读签证（MRV-B）	符合Doc 9303号文件第7部分中所载尺寸规范的机读签证，其尺寸可供在护照签证页上留出一个空白区。
电子欺骗	伪造传输的发送地址以便非法进入保密系统。 注：冒充、伪装、捎带和模仿都属于欺骗形式。
信息藏匿术	在主要视觉图像内对图像或信息进行编码或隐藏。
结构特征	结构特征涉及将可测定的结构加在机读旅行证件之内或之上。通过探测设备可以探测和测定出这种结构的存在。
拍摄对象	肖像显示之人；此人应为机读旅行证件的持有人。
物质特征	物质特征涉及在机读旅行证件中加入一种材料，它一般不会显现，在目视查验中不会明显显现出来。可根据这种添加物质的适当特性的存在和量级，探测出这种材料的存在。
对称算法	对明文加密和相关密文解密使用同一密钥或密钥集的一种密码操作。
合成材料	基于非纸质的、用于个人资料页或卡的材料。术语“合成材料”用作“塑料”的同义词，它包括诸如聚碳酸酯、聚对苯二甲酸乙二醇酯等材料和类似材料以及这些物质的结合体。
系统	有特定目的和操作环境的具体信息技术装置。
系统一体化	各种面向卡持有人、面向内部和伙伴方的系统以及应用程序相互之间实现一体化的过程。

系统安全政策	在一具体系统内规范如何对敏感信息及其他资源进行管理、保护和分发的一套法律、规则和措施。
触感特性	使证件有独特“触感”的表面特性。
（特征）标签	独特标识证件特征的字节。特征标签与特征之间的映射必须在配置文件中明确说明。
示踪物	可加入到机读旅行证件的物理组成部分的、无法自然产生的物质，通常具有 3 级特征，且需要特殊设备才能探测到。
示踪油墨	这种油墨中含有的化合物是无法自然产生的物质，可用特殊设备探测出来。
防篡改	证件组成部分的防变造能力。
模板/参考模板	生物特征系统使用的代表登记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。
模板尺寸	生物特征数据占用的电脑内存量。
热致变色油墨	当印制的图像经受特定温度变化时，这种油墨的颜色会发生可逆变化。
阈值	一个“基准”分值。将检查程序的结果值与对应的阈值进行比较会得出通过/未通过的决定。
标记图像	机读旅行证件持有人的肖像，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。
信任锚	在具有分层结构的密码系统中，这是一个权威实体，对其信任是假定的，不是衍生的。
常用标记	在证件持有人无法在证件上签字时代替其手写签名的符号。
对紫外线反应迟钝的基材	在紫外光照射下，不显示可见荧光的基材。
验证	证明正在考虑的系统各个方面都满足该系统规范的过程。
可变激光图像	这种特征由激光刻蚀或激光穿孔而产生，随观察角度的变化而显示不同信息或图像。
核证	生物识别:将交验的生物特征样本与被声称其身份的某一登记者的生物特征参考模板进行比对，以确定它与该登记者的模板是否匹配的过程。对照“识别”。 机器认证：验证阐述对证件模型的实时数据集适用的检查程序。验证结果通常通过数字结果值提供。
签证签名人（VS）	从签证个性化系统接收数据、使用签证签名人证书和对应的私钥进行编码，并对可见数字印章进行签名的机构。

签证签名证书	所包含信息能够查明在签证上签署可见数字印章的实体信息的证书，并包含与所创建签名的私钥相对应的公钥。
签证验证当局（VVA）	根据验证政策对可见数字印章进行验证的机构。
可见数字印章（VDS）	包含证件特征、被编码为二维条形码并打印在证件之上的加密签名数据结构。
视读区（VIZ）	机读旅行证件（机读护照的资料页）中那些未被界定为机读区的部分，即正面和背面（如适用），旨在对其进行视读检查。
水印	一般包括色调层次变化的一种定制图案，在制造过程中在纸张或其他基材中形成，通过其中的材料位移而产生，通常通过透射光可以看到。
小波标量量化（WSQ）	一种特别用于指纹图像存储的数据压缩方法。
窗口化或透明特征	通过基材的构造所产生的安全特征，在基材的构造中，基材的一部分被移除或被透明材料所代替，从而可增加诸如透镜或触觉元素等的更多安全特征。
X.509v3 证书	用于在通信网络上证明身份和公钥所有权的、国际认可的电子化证件。它包含签发人的名称、用户的身份识别信息和签发人的数字签名。
区	机读旅行证件上包含一个数据元素逻辑分组的区域。机读旅行证件被划出七（7）个区。

4.3　关键词

为表明各项要求使用了一些关键词。

Doc9303 号文件中用英文大写字母书写的“必须”、“不得”、“必要的”、“应”、“不应”、“应该”、“不应该”、“建议的”、“可以”和“选择性的”等关键词，其解释与 RFC 2119 中所述相同。

必须	这个词，或**“必要的”**或**“应”**一词，表示有关规定是规范中的一项绝对要求。
不得	这个用语，或**“不应”**一语，表示有关规定是规范中的一项绝对禁止规定。
应该	这个词，或**“建议的”**这个形容词，表示在特定情况下可能存在忽略某个特定项目的合理理由，但必须了解全部的影响，并在采取不同方针前仔细予以衡量。
不应该	这个用语，或**“不建议”**一语，表示在特定情况下可能有合理的理由认为特定行为是可以接受的，甚至是有用的，但在实施带有这一标记用语的任何行为之前，必须了解全部的影响并对情况仔细加以衡量。

可以	这个词，或**“选择性的”**这个形容词，表示一个项目是真正可以选择的。一个用户可能选择纳入一个项目因为某项具体应用需要该项目或因为用户认为它可以加强应用，而另一个用户则可能省略同一个项目。不包括某个选项的一项实施，必须具备与包括了该选项的另一项实施进行互操作的能力，尽管其功能度可能减少。同理，一项包括了某个选项的实施，也**必须**具备与不包括该选项的另一项实施进行互操作的能力（当然，该选项所提供的特征除外）。
有条件的	一个项目的使用依赖于其他项目的使用。因此，对它有进一步的限制，即在什么条件下该项目是**要求的**或**建议的**。这是 Doc 9303 号文件中使用的一个附加关键词（不是 RFC 2119 的一部分）。

使用指导 这里界定的祈使语气动词，必须慎用少用。具体而言，这些词必须仅在实际要求进行互操作时或者为了限制可能造成危害的行为（如限制转发）时使用。例如，不得在不要求互操作性时，只是为了将某一特定方法强加给实施者而使用这类用词。

安全考虑 上述用语经常用来规范具有安全影响的行为。不落实必须做的或应该做的事情，或者做了规范中规定不得做或不应该做的事情，其对安全的影响可能是非常微妙的。文件起草者应该花时间详细说明不遵循建议或要求会带来的安全影响，因为大多数实施者并不了解制定规范时发生的情况和进行的讨论。

凡实施**选择性**特征的，**必须**按 Doc9303 号文件所述加以实施。

Doc 9303 号文件中的附录属于资料性附录。 如果有人声称遵守某一（资料性）附录，便**必须**依照规定遵守该附录中使用的关键词。

4.4 客体标识符

在 Doc 9303 号文件第 10、11 和 12 部分中规定了国际民航组织客体标识符。本段列出了这些实际的国际民航组织标识符：

— **国际民航组织安全框架**

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

id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}

id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
```

— **逻辑数据结构安全对象**

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

— **国家签署证书当局国家证书列表**

```
id-icao-mrtd-security-cscaMasterList OBJECT IDENTIFIER ::= {id-icao-mrtdsecurity 2}

id-icao-mrtd-security-cscaMasterListSigningKey OBJECT IDENTIFIER ::= {id-icaomrtd-
security 3}
```

— 主动认证协议

```
id-icao-aaProtocolObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 5}
```

— 国家签署证书当局名称变更

```
id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-mrtd-security 6}

id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::= {id-icaomrtd-security-
extensions 1}
```

— 证件类型列表，见**TR**“逻辑数据结构和公钥基础设施维护”

```
id-icao-mrtd-security-extensions-documentTypeList OBJECT IDENTIFIER ::= {idicao-mrtd-
security-extensions 2}
```

— 偏差列表基础客体标识符

```
id-icao-mrtd-security-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtdsecurity 7}

id-icao-mrtd-security-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icaomrtd-
security 8}

id-Deviation-CertOrKey OBJECT IDENTIFIER ::= {id-icao-DeviationList 1}

id-Deviation-CertOrKey-DSSignature OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 1}

id-Deviation-CertOrKey-DSEncoding OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 2}

id-Deviation-CertOrKey-CSCAEncoding OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 3}

id-Deviation-CertOrKey-AAKeyCompromised OBJECT IDENTIFIER ::= {id-Deviation-CertOrKey 4}

id-Deviation-LDS OBJECT IDENTIFIER ::= {id-icao-DeviationList 2}

id-Deviation-LDS-DGMalformed OBJECT IDENTIFIER ::= {id-Deviation-LDS 1}

id-Deviation-LDS-SODSignatureWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS 3}

id-Deviation-LDS-COMInconsistent OBJECT IDENTIFIER ::= {id-Deviation-LDS 4}

id-Deviation-MRZ OBJECT IDENTIFIER ::= {id-icao-DeviationList 3}

id-Deviation-MRZ-WrongData OBJECT IDENTIFIER ::= {id-Deviation-MRZ 1}

id-Deviation-MRZ-WrongCheckDigit OBJECT IDENTIFIER ::= {id-Deviation-MRZ 2}

id-Deviation-Chip OBJECT IDENTIFIER ::= {id-icao-DeviationList 4}

id-Deviation-NationalUse OBJECT IDENTIFIER ::= {id-icao-DeviationList 5}
```

— 逻辑数据结构2客体标识符

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

id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-mrtd-security-lds2 8}

id-icao-tsSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 1}

id-icao-vSigner OBJECT IDENTIFIER ::= {id-icao-lds2Signer 2}

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

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

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

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

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

id-icao-lds2-visaRecords-application OBJECT IDENTIFIER ::= { id-icao-lds2-visaRecords 1}

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

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

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

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

— **SPOC客体标识符**

```
id-icao-spoc OBJECT IDENTIFIER ::= {id-icao-mrtd-security 10}

id-icao-spocClient OBJECT IDENTIFIER ::= {id-icao-spoc 1}

id-icao-spocServer OBJECT IDENTIFIER ::= {id-icao-spoc 2}
```

— 可见数字印章客体标识符

```
id-icao-vds OBJECT IDENTIFIER ::= { id-icao-mrtd-security 11}
```

— **DTC** 客体标识符

```
id-icao-dtc OBJECT IDENTIFIER ::= { id-icao-mrtd-security 12}

id-icao-dtcSigner OBJECT IDENTIFIER ::= {id-icao-dtc 1}

id-icao-dtcAttributes OBJECT IDENTIFIER ::= {id-icao-dtc 2}

id-icao-dtcCapabilitiesInfo OBJECT IDENTIFIER ::= {id-icao-dtcAttributes 1}
```

— EF.DIR客体标识符

```
id-EFDIR OBJECT IDENTIFIER ::= { id-icao-mrtd-security 13}
```

4.5　注的使用

在ISO/IEC标准中，注的作用是提供信息，而在Doc 9303号文件中，注是规范性文本的一部分，用来强调要求或附加信息。

5.　关于DOC 9303号文件使用的指导

5.1　Doc 9303号文件的构成

Doc 9303号文件由13个部分组成。每一部分描述机读旅行证件的一个具体方面。以这样的方式来编写Doc 9303号文件的各部分，机读旅行证件的签发人就能够针对机读旅行证件的特定类型（尺寸）来编写一套完整的相关规范。第1部分的第5.2节描述了这些尺寸与Doc 9303号文件各部分之间的关系。

以下各部分构成Doc 9303号文件中关于机读旅行证件的完整规范。

第1部分　引言

手头这份文件是第1部分。

第2部分　机读旅行证件的设计、制作和签发的安全性规范

第2部分针对旅行证件签发机关为确保其所签发的机读旅行证件以及对合法持有人的机读旅行证件进行个人化处理和签发的手段免遭欺骗性攻击需要采取的防范措施，制定了强制性和选择性规范。同时，对机读旅行证件制作、个人化处理和签发场所的物理安全，以及对从事这些工作的人员的审查也制定了强制性和选择性规范。

第3部分　所有机读旅行证件的通用规范

第3部分明确了通用于TD1型、TD2型和TD3型机读旅行证件（MRTDs）的规范，包括为确保通过视读和机读（光学字符识别）手段实现全球互操作性所需遵守的规范。适用于每种证件类型的详细规范，见Doc 9303号文件第4部分至第7部分。

第4部分　机读护照（MRPs）和其他TD3型机读旅行证件规范

第4部分明确了针对TD3型机读护照（MRPs）和其他TD3型机读旅行证件（MRTDs）的规范。为简洁起见，整个第4部分使用了机读护照这一术语；除有说明的地方外，本部分中的所有规范应同样适用于所有其他TD3型机读旅行证件。

第5部分　TD1型机读官方旅行证件（MROTDs）规范

第5部分明确了针对TD1型机读官方旅行证件（MROTDs）的规范。

第6部分　TD2型机读官方旅行证件（MROTDs）规范

第6部分明确了针对TD2型机读官方旅行证件（MROTDs）的规范。

第 7 部分　机读签证

第 7 部分明确了机读签证（MRVs）的规范，从而可通过视读（肉眼可读）和机读方式，使数据的兼容性和全球互换性得以实现。关于由一个国家签发并由接收国接受的签证的规范可用作旅行目的。机读签证应至少包含所规定的数据，且这些数据应像本部分所述的那样，既可通过视读也可通过光学字符识别方法加以辨识。

第 7 部分是以 Doc 9303 号文件第 2 部分《机读签证》第三版（2005 年）为基础编制的，其中载有关于 A 型和 B 型签证的规范。

第 8 部分　紧急旅行证件

第 8 部分提供了关于紧急旅行证件（ETD）的指导和规范。本指导材料的目的是推动在签发紧急旅行证件方面采取一致的做法，以便加强证件安保、保护个人、提高边检工作人员在口岸处理紧急旅行证件时的信心，并处理因做法与安保特征不一而产生的脆弱性。第 8 部分还明确了紧急旅行证件中使用可见数字印章的规范。

第 9 部分　生物特征识别技术的运用和机读旅行证件的电子数据存储

除那些关于 9303 号文件第 3、4、5、6 和 7 部分阐明的基本机读旅行证件的规范外，第 9 部分还明确了可供希望签发电子机读旅行证件（eMRTD）的国家使用的规范。任何安装有合适设备的接收国家可使用电子机读旅行证件从中读取与电子机读旅行证件本身及其持有人相关的、数量大大增加的数据。这包括可用作人脸识别系统的输入信息的、以及可选择性地用作指纹或虹膜识别系统的输入信息的全球可互操作的生物特征数据。这些规范要求以高清晰图像的形式存储全球可互操作的生物特征数据。

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

第 10 部分明确了电子机读旅行证件实现全球可互操作性所需要的逻辑数据结构（LDS）。签发国或签发机构所选定的电子机读旅行证件内包含的非接触式集成电路扩容技术，应使接收国能够访问数据。本部分明确了对这些数据进行标准化编排的规范。这需要确定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，要实现全球互操作性，就应遵循这种排序和/或编组，以便读取选择性地包含在电子机读旅行证件（eMRTD）中的扩容技术所记录的详细信息（数据元素）。

第 11 部分　机读旅行证件的安全机制

第 11 部分明确了使各国和各供应商能够实施可提供集成电路卡只读访问的机读旅行证件（eMRTDs）密码安全特征的规范。

第 11 部分规定了密码协议以：

- 防止非法浏览非接触式集成电路中的数据；
- 防止窃听集成电路和阅读器之间的通信；
- 根据第 12 部分中描述的公钥基础设施，对存储在集成电路中的数据提供认证，并提供对集成电路本身的认证。

第 12 部分　机读旅行证件的公钥基础设施

第 12 部分规定了关于电子机读旅行证件应用的公钥基础设施（PKI）。规定了对于签发国或签发机构的要求，包括签发证书和证书撤销列表的认证机构（CA）的运作。同时也规定了对于接收国及其验证这些证书和证书撤销列表的查验系统的要求。

第 13 部分 — 非电子证件可见数字印章

第 13 部分明确了利用非对称加密法的数字印章规范，以相对低廉但高度可靠的方式确保非电子证件的真实性和完整性。对非电子证件的信息进行加密签署，并将签名编成二维条形码编码且打印在证件原件之上。

5.2 机读旅行证件尺寸和 Doc 9303 号文件中相关部分之间的关系

表 1-1 说明了 Doc 9303 号文件中的哪些部分与机读旅行证件的特定类型（尺寸）相关。

表 1-1. 尺寸交叉参考表

	Doc 9303 号文件部分												
	1	2	3	4	5	6	7	8	9	10	11	12	13
TD3 型机读旅行证件（MRP）	√	√	√	√									
TD3 型电子机读旅行证件（eMRP）	√	√	√	√					√	√	√	√	
TD1 型机读官方旅行证件	√	√	√		√								
TD1 型电子机读官方旅行证件	√	√	√		√				√	√	√	√	
TD2 型机读官方旅行证件	√	√	√			√							
TD2 型电子机读官方旅行证件	√	√	√			√			√	√	√	√	
机读签证	√	√	√				√						√
紧急旅行证件	√	√	√					√					√

6. 参考资料（规范性）

本文参照的国际标准中的某些规定，构成 Doc 9303 号文件中的规定。Doc 9303 号文件中所载的规范凡与参照标准存在差异的，应以本文件所载规范为准，以兼顾机读旅行证件，包括机读签证的具体制作要求。

附件 9　　《国际民用航空公约》（《芝加哥公约》），附件 9 —《简化手续》

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

—完—

ISBN 978-92-9265-352-1