ICAO

Doc 9303

机读旅行证件

第八版, 2021年

第 12 部分：机读旅行证件的公钥基础设施

经秘书长批准并由其授权出版

国际民用航空组织

ICAO

Doc 9303

机读旅行证件

第八版, 2021年

第 12 部分：机读旅行证件的公钥基础设施

经秘书长批准并由其授权出版

国际民用航空组织

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

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

Doc 9303 号文件 — 《机读旅行证件》
第 12 部分 — 机读旅行证件的公钥基础设施
订购编号：9303P12
ISBN 978-92-9265-531-0（印刷版）

修订

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

修订和更正记录

修订		
编号	日期	换页人

更正		
编号	日期	换页人

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

目录

1. 范围

Doc 9303 号文件第 12 部分阐述了电子机读旅行证件应用的公钥基础设施（PKI）。其中对各签发国或签发机构的要求进行了规定，包括与签发证书和证书撤销列表（CRLs）的认证机构（CA）的运行相关的要求。还对接收国及其用于验证这些证书和证书撤销列表的查验系统的要求进行了规定。

Doc 9303 号文件第八版纳入了关于可见数字印章（称为 VDS）的规范和关于选择性的旅行记录、签证记录和附加生物特征应用（称为 LDS2）的规范，这些应用可作为强制性电子机读旅行证件应用（称为 LDS1）的扩展。

Doc 9303 号文件第 12 部分应结合下列文件进行阅读：

- Doc 9303 号文件第 10 部分 — 在非接触式集成电路（IC）中存储生物特征和其他数据的逻辑数据结构（LDS）；
- Doc 9303 号文件第 11 部分 — 机读旅行证件的安全机制；和
- Doc 9303 号文件第 13 部分 — 可见数字印章。

2. 公钥基础设施概述

电子机读旅行证件公钥基础设施（PKI）可以支持在电子机读旅行证件对象（包括证件安全对象（SO_D））上创建数字签名并随后对数字签名进行校验，以确保签署的数据是真实的且未被修改。证书被撤销、认证路径验证程序失败或电子签名校验失败本身并不能作为判断电子机读旅行证件无效的理由。这样的失败意味着无法通过电子手段校验逻辑数据结构数据的完整性和真实性，这时可以采用其他非电子机制来进行判断，并将其作为电子机读旅行证件整个查验工作的一部分。

电子机读旅行证件公钥基础设施比通用的多应用的公钥基础设施（如在[RFC 5280]中定义的因特网公钥基础设施）简单得多。在电子机读旅行证件公钥基础设施中，每一个签发国/签发机构都建立一个向终端实体（包括证件签名者）直接签发所有证书的单一认证机构（CA）。这些认证机构被称为国家签名认证机构（CSCAs）。在该基础设施中没有其他认证机构。接收国直接在每个签发国或签发机构的国家签名认证机构的密钥/证书里建立信任。

电子机读旅行证件的公钥基础设施是以通用的公钥基础设施标准为基础的，包括[X.509]和[RFC 5280]。这些基准公钥基础设施标准定义了一大套与电子机读旅行证件应用并不相关的选择性特征和认证机构之间的复杂信任关系。Doc 9303 号文件的本部分概述了为电子机读旅行证件应用专门制定的标准。电子机读旅行证件应用的一些独特方面包括：

- 每一签发国仅有一个国家签名认证机构；
- 认证路径仅包含一个证书（如证件签名者）；
- 在创立之后 5-10 年内必须能够进行签名校验；
- 支持国家签名认证机构更名；和
- 在认证路径中，国家签名认证机构链接证书不作为中间证书处理。

在大多数情况下，电子机读旅行证件的公钥基础设施与 [RFC 5280] 是一致的。然而，国家签名认证机构可以更名这一点对电子机读旅行证件公钥基础设施提出了独特要求，这些要求与 [RFC 5280] 中规定的一些证书撤销列表验证程序并不相符。已将这样的差异保持在最低限度，并对其进行了明确说明。

对于 VDS 和 LDS2，可确保数据对象完整性和真实性的数字签名公钥基础设施是 LDS1 公钥基础设施的扩展。VDS 和 LDS2 的签名者证书也由为 LDS1 签发签名者证书的国家签名认证机构签发。本文件对因这些新应用而需对证书概要做出的修改进行了说明。该基础设施合起来被称为**电子机读旅行证件公钥基础设施**。

数字签名公钥基础设施由以下实体组成：

- 国家签名认证机构（CSCA）；
- 用于签署证件安全对象（SO_D）的证件签名者证书（DSC）；
- LDS2 签名者证书，包括以下部分：
  - — LDS2-TS 签名者 — 签署 LDS2 旅行印章；
  - — LDS2-V 签名者 — 签署 LDS2 电子签证；和
  - — LDS2-B 签名者 — 签署 LDS2 附加生物特征；
- 条形码签名者证书（BCSC），本文件定义了以下两种特定类型：
  - — 签证签名者证书（VSC）；和
  - — 紧急旅行证件签名者证书（ESC）；
- 用于签署国家证书列表的国家证书列表签名者证书（MSC）；
- 用于签署偏差列表的偏差列表签名者证书（DLSC）；和
- 证书撤销列表（CRL）。

所有不同的证书类型都由同一个国家签名认证机构签署。国家签名认证机构还签署证书撤销列表，该列表包含任何已被撤销的证书，而不管被撤销的是何种证书。国家签名认证机构签发的所有证书统称为**签名者证书**。

对于 LDS2 应用，为其定义了单独的**授权公钥基础设施**。授权公钥基础设施使电子机读旅行证件签发国或签发机构能够对给予其他国家将 LDS2 数据对象写入其电子机读旅行证件并读取这些数据对象的授权进行管制和管理。其他国家如果想要读取或写入 LDS2 数据，就必须直接从电子机读旅行证件签发国或签发机构获得授权证书。

授权公钥基础设施使用的是另一种不同的证书结构（ISO 7816 卡可校验证书），因此需要额外的基础设施组件。

LDS2 要求终端向电子机读旅行证件非接触式集成电路证明其有权将 LDS2 数据对象写入非接触式集成电路或有权读取 LDS2 数据对象。这样的终端配备有至少一个私钥和相应的终端证书，该证书对终端的公钥和访问权限进行编码。在终端证明知道该私钥后，机读旅行证件芯片会授予终端访问权限，使其可以读取/写入终端证书中所示的 LDS2 数据。

LDS2 授权公钥基础设施由以下实体组成：

- 国家校验认证机构（CVCAs）；
- 证件校验者（DVs）；
- 终端；和
- 单一联络点（SPOC）。

一个国家的国家校验认证机构和其他国家的证件校验者之间授权证书的分发和管理是通过每个国家的单一联络点（SPOC）来进行处理的。

Doc 9303 号文件第 12 部分规定了电子机读旅行证件公钥基础设施的概要、授权公钥基础设施的概要以及相应的对象，其中包括：

- 基础设施中各实体的作用和责任；
- 加密算法和密钥管理；
- 证书和证书撤销列表的内容；
- 证书和证书撤销列表的分发机制；和
- 认证路径验证。

3. 作用和责任

本节详细介绍了电子机读旅行证件公钥基础设施和授权公钥基础设施的各实体及其作用和责任。

3.1 电子机读旅行证件公钥基础设施

电子机读旅行证件中所存储数据的真实性和完整性由被动认证保护。对于电子机读旅行证件公钥基础设施，这一安全机制以数字签名为依据，包含下列公钥基础设施实体：

- **国家签名认证机构（CSCA）**：每一个签发国/签发机构建立单一的一个国家签名认证机构作为其在电子机读旅行证件方面的国家信任点。该国家签名认证机构为一个或多个（国家）证件签名者签发公钥证书，以及选择性地为国家证书列表签名者和偏差列表签名者等其他终端实体签发公钥证书。国家签名认证机构还定期发布证书撤销列表（CRL），说明所签发的证书是否有被撤销的。

- **证件签名者（DS）**：证件签名者用数字方式签署要存储在电子机读旅行证件中的数据；该签名存储在电子机读旅行证件的证件安全对象中。

- **LDS2 签名者**：LDS2 签名者用数字方式签署一种或多种类型的 LDS2 数据对象。

- **条形码签名者（BCS）：**条形码签名者用数字方式签署条形码中编码的数据（标头和报文）。签名也存储在条形码中。本文件指定了使用条形码签名者的两个用例，即签证和紧急旅行证件。

- **查验系统（IS）：**查验系统用于校验数字签名，包括认证路径验证，以作为被动认证的一部分校验存储在电子机读旅行证件中的电子数据的真实性和完整性。

- **国家证书列表签名者：**国家证书列表签名者是通过电子方式签署国家签名认证机构证书（国内和国外）列表的一个选择性实体，以支持国家签名认证机构证书的双边分发机制。

- **偏差列表签名者：**偏差列表签名者用于签署偏差列表。偏差列表在 Doc 9303 号文件第 3 部分中做了规定。

用于生成密钥对的安全设施应在签发国或签发机构的控制之下。每一个密钥对包括一个“私钥”和一个“公钥”。私钥及相关系统或设施应妥善保护好，以免被任何外部人员或未经授权的人员通过固有的设计和硬件安全设施获取到。

尽管国家签名认证机构的证书是相对稳定的，但是随着时间的推移，将产生大量证件签名者证书。

每一个签发国或签发机构的国家签名认证机构充当接收国的信任点。签发国或签发机构以证书的形式将其自己的国家签名认证机构公钥分发给接收国。接收国通过带外方式确定这一证书（和经认证的密钥）为“可信的”，并为该可信的密钥/证书存储一个“信任锚”。这些国家签名认证机构证书应该是由国家签名认证机构直接签发的自签名证书。国家签名认证机构证书不得为较大公钥基础设施中的从属证书或交叉证书。还可以签发国家签名认证机构自签名链接证书，以帮助接收国在密钥更替后对国家签名认证机构的新密钥/证书建立信任。

注：一些国家要求有一个认证机构中央管控者（CCA）作为向所有应用发布自签名证书的最高机构。在此类情况下，一个可能的解决方案是由国家签名认证机构创建自签名证书（满足国际民航组织 Doc 9303 号文件的要求），并请认证机构管控者会签该证书（满足该国自己的认证机构管控者要求）。但是这种会签证书不是电子机读旅行证件公钥基础设施中的一部分，不会被分发给接收国。

3.1.1 国家签名认证机构

建议在保护严密的线下认证机构基础设施中生成和存储国家签名认证机构密钥对（KPu_{CSCA}、KPr_{CSCA}）。

国家签名认证机构私钥（KPr_{CSCA}）用于签署证件签名者证书（C_{DS}）、其他证书和证书撤销列表。

国家签名认证机构证书（C_{CSCA}）用于验证证件签名者证书、国家证书列表签名者证书、偏差列表签名者证书、证书撤销列表和国家签名认证机构签发的其他证书。

所有证书和证书撤销列表必须符合第 7 节所规定的概要，且必须使用第 5 节所规定的分发机制进行分发。

对于公钥目录参与国，每个国家签名认证机构证书（C_{CSCA}）还必须由证书签发者发送给公钥目录（用于验证证件签名者证书（C_{DS}））。

如第 4 节所述，证书撤销列表必须定期发布。

3.1.2　证件签名者

建议在保护严密的基础设施中生成和存储证件签名者密钥对（KPu_{DS}、KPr_{DS}）。

证件签名者私钥（KPr_{DS}）用于签署证件安全对象（SO_D）。

证件签名者证书（C_{DS}）用于验证证件安全对象（SO_D）。

每一个证件签名者证书（C_{DS}）均必须符合第 7 节中所规定的证书概要，且必须存储于用相应的证件签名者私钥签署的每一个电子机读旅行证件的非接触式集成电路中（详见 Doc 9303 号文件第 10 部分）。这可确保接收国获取到与每一个电子机读旅行证件相关的证件签名者证书。

公钥目录参与国的证件签名者证书还应由证书签发者发送给国际民航组织，以便公布在国际民航组织公钥目录（PKD）中。

3.1.3　LDS2 签名者

LDS2 签名者用数字方式签署一种或多种类型的 LDS2 数据对象。

如果需要将 LDS2 签名者称为签署特定 LDS2 数据对象类型的签名者，则按以下方式进行称呼：

- LDS2-TS 签名者 — 签署 LDS2 旅行印章；
- LDS2-V 签名者 — 签署 LDS2 电子签证；和
- LDS2-B 签名者 — 签署 LDS2 附加生物特征；

建议每个国家安排不超过一个 LDS2-TS 签名者、一个 LDS2-V 签名者和一个 LDS2-B 签名者。还可以由一个 LDS2 签名者承担这些角色中的部分或全部角色。

如果需要进一步区分，例如添加旅行印章的位置、哪位官员为旅行者办理了通关手续、哪位官员授予了签证或者添加附加生物特征的位置，则可以将其包含在相应 LDS2 数据对象本身的专有字段中。

3.1.4　条形码签名者

建议在保护严密的基础设施中生成和存储条形码签名者密钥对（KPu_{BCS}、KPr_{BCS}）。

条形码签名者私钥（KPr_{BCS}）用于签署条形码中编码的数据（标头和报文）。签名也存储在条形码中。

条形码签名者证书（C_{BCS}）用于验证条形码中编码的数据（标头和报文）。

每一个条形码签名者证书（C_{BCS}）均必须符合第 7 节中所规定的证书概要。条形码签名者证书并不包含在数字印章本身中。因此，签发受数字印章保护的证件的国家必须发布其所有的条形码签名者证书。条形码签名者证书的主要分发渠道是公钥目录/双边交换。其他机制，例如在网站上发布，是次要渠道。

公钥目录参与国的条形码签名者证书还应由证书签发者发送给国际民航组织，以便公布在国际民航组织公钥目录（PKD）中。

签证签名者（VS）和紧急旅行证件签名者是条形码签名者的特殊用例。

3.1.5 查验系统

查验系统用于进行被动认证，以确保存储在电子机读旅行证件非接触式集成电路中的数据的完整性和真实性。作为该过程的一部分，查验系统必须进行第 6 节所示的认证路径验证。

3.1.6 国家证书列表签名者

国家证书列表签名者私钥用于签署国家签名认证机构国家证书列表。

国家证书列表签名者证书用于验证国家签名认证机构国家证书列表。

3.1.7 偏差列表签名者

偏差列表签名者私钥用于签署偏差列表。

偏差列表签名者证书用于验证偏差列表。

3.2 授权公钥基础设施

LDS2 应用由签发国或签发机构在进行个人化设置时写入电子机读旅行证件的非接触式集成电路。

另一个国家必须获得签发国或签发机构的授权才可以将 LDS2 对象写入该非接触式集成电路。每个 LDS2 数据对象都由写入国的 LDS2 签名者进行数字签名，然后由该国经授权的终端写入非接触式集成电路。这样一个两步过程，即由签名者进行签名和由经授权的终端写入，类似于 LDS1 概念，在该概念中，证件签名者对证件安全对象进行数字签名，但随后通过个人化过程将它们写入非接触式集成电路，图 1 显示了这一过程。随后从非接触式集成电路读取 LDS2 对象是通过经授权可以进行相关 LDS2 对象类型读取工作的终端完成的。

授权公钥基础设施使电子机读旅行证件签发国或签发机构能够对其签发的电子机读旅行证件中非接触式集成电路上的 LDS2 数据的访问权限（读取和写入）进行控制。

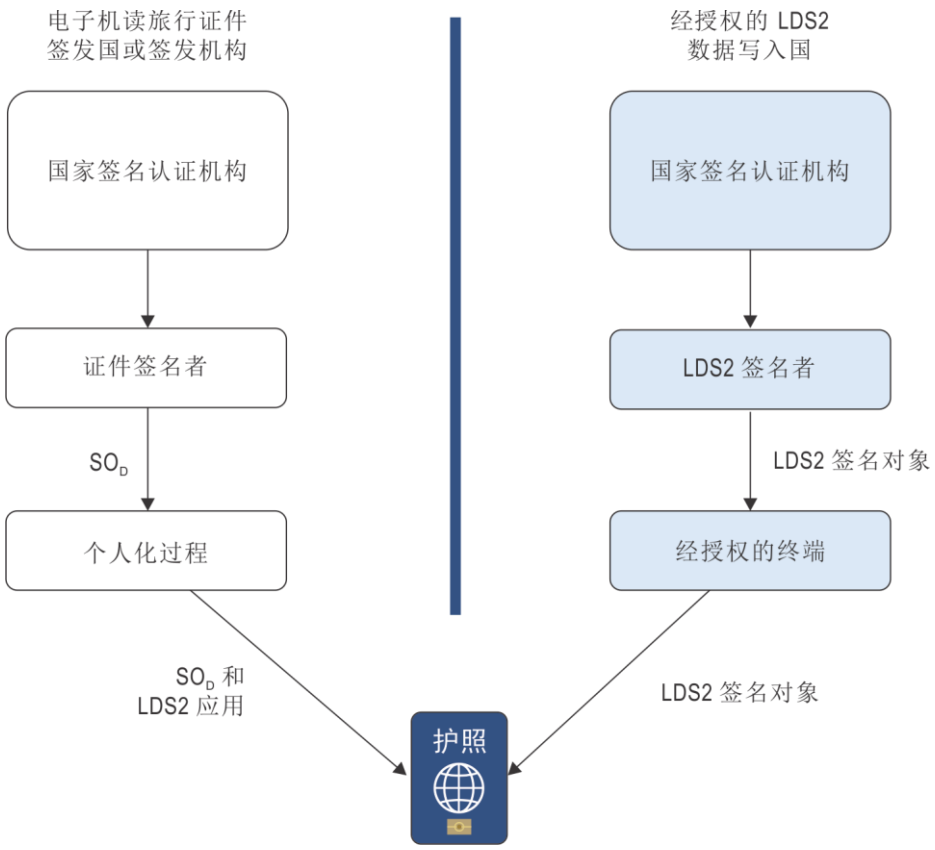

图 1　LDS2 信任模型和写入架构

3.2.1　国家校验认证机构

每个允许将 LDS2 数据添加到其电子机读旅行证件的签发国或签发机构都必须设立一个单一的国家校验认证机构（CVCA）。该国家校验认证机构是一个认证机构（CA），它是该签发国或签发机构授权公钥基础设施的信任锚，涵盖所有的 LDS2 应用。国家校验认证机构可以是一个独立的实体，也可以与该签发国或签发机构的国家签名认证机构合为一体。然而，即使是合署办公，国家校验认证机构也必须使用与国家签名认证机构不同的密钥对。国家校验认证机构确定将授予所有外国和国内证件校验者（DV）的访问权限，并向每一个证件校验者签发包含单独授权的证书。

3.2.2　证件校验者

证件校验者（DV）是一个认证机构，它是组织单位的一部分，管理着一组终端（例如：由国家边境警察运行的终端）并向这些终端签发授权证书。证件校验者必须先从负责相关工作的国家校验认证机构收到授权证书，然后才能向其终端签发相关证书。由证件校验者向终端签发的证书可以包含证件校验者本身收到的授权或该授权的一部分。这些证书所包含的授权不得超出证件校验者所获得的授权。

3.2.3 终端/查验系统

在授权公钥基础设施的情况下，终端是访问电子机读旅行证件的非接触式集成电路并将经数字签名的 LDS2 数据对象写入该集成电路或读取 LDS2 数据对象的实体。终端必须有一个由本地证件校验者签发给它的授权证书，证件校验者通过这一证书授予其所需的授权。终端也称为查验系统。

3.2.4 单一联络点（SPOC）

每个参与 LDS2 授权公钥基础设施的国家都必须设立一个单一联络点。该单一联络点是一个国家的国家校验认证机构与另一个国家的证件校验者之间所有通信的接口。证书请求和响应由每个国家的单一联络点之间通过使用第 8 节中定义的单一联络点协议进行沟通。

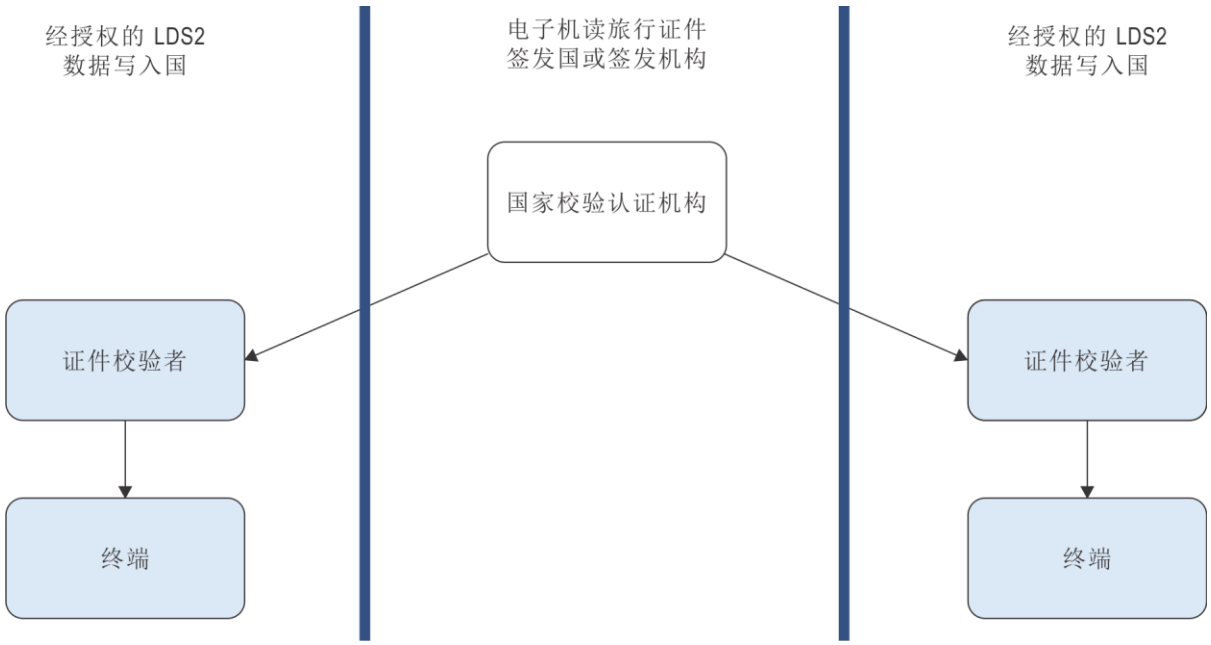

图 2 授权公钥基础设施信任模型

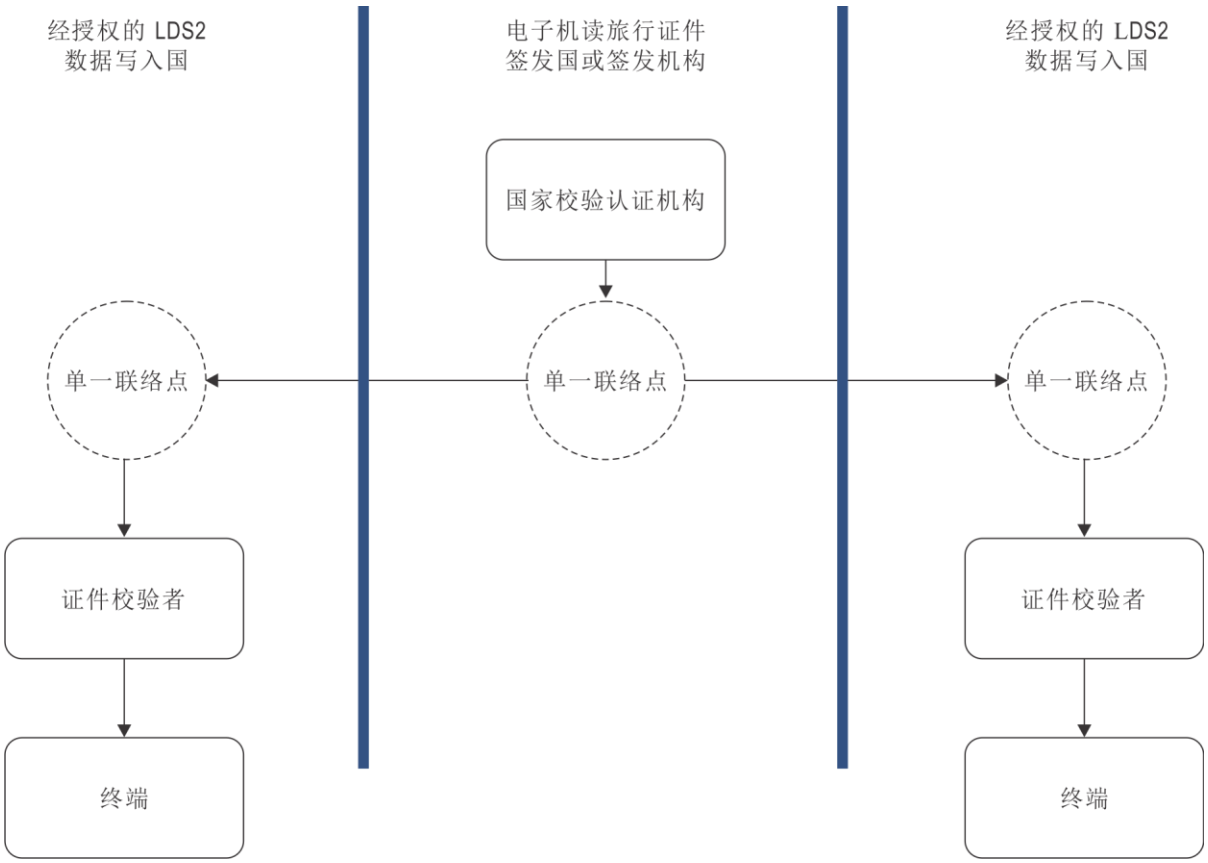

图 3　单一联络点的角色

4.　密钥管理

本节就两种公钥基础设施的密钥管理分别做了论述。

4.1　电子机读旅行证件公钥基础设施

签发国或签发机构应至少有两个密钥对类型：

- 国家签名认证机构密钥对；和
- 证件签名者密钥对。

签发国或签发机构可以有额外类型的密钥对：

- 国家证书列表签名者密钥对；
- 偏差列表签名者密钥对；
- LDS2 签名者密钥对；

- 单一联络点客户端密钥对；
- 单一联络点服务器密钥对；和
- 签证签名者密钥对/紧急旅行证件签名者密钥对（两者都是条形码签名者的一种类型）。

国家签名认证机构、签名者证书和单一联络点证书公钥用[X.509]证书进行签发。国家签名认证机构证书中所包含的公钥用于校验已签发的签名者证书、单一联络点证书、国家签名认证机构证书上的国家签名认证机构签名以及已签发的证书撤销列表上的国家签名认证机构签名。

对于国家证书列表签名者、偏差列表签名者和通信密钥与证书而言，私钥的生命周期和证书的有效期由签发国或签发机构自行确定。

国家签名认证机构证书和证件签名者证书都有相应的私钥使用期限和公钥有效期，具体如表 1 所示。

表 1　密钥的使用期限和有效期

	私钥的使用期限	**公钥的有效期 （假设护照有效期为 10 年）**
国家签名认证机构	3-5 年	13-15 年
证件签名者	最长至 3 个月[1]	约 10 年
LDS2-TS 签名者	1-2 年	10 年+3 个月
LDS2-V 签名者	1-2 年	10 年+3 个月
LDS2-B 签名者	1-2 年	10 年+3 个月
单一联络点客户端	未作规定	6-18 个月
单一联络点服务器	未作规定	6-18 个月
签证条形码签名者	1-2 年	私钥使用期限+签证有效期
紧急旅行证件条形码签名者	1 年+2 个月（2 个月是为了顺利过渡）	私钥使用期限+紧急旅行证件有效期
国家证书列表签名者	由签发国或签发机构自行确定	由签发国或签发机构自行确定
偏差列表签名者	由签发国或签发机构自行确定	由签发国或签发机构自行确定
通信	由签发国或签发机构自行确定	由签发国或签发机构自行确定

1. 应注意的是，证件签名者证书中对应的 privateKeyUsage 扩展可以稍长点，以便允许重叠或满足制证要求。

4.1.1　证件签名者密钥和证书

证件签名者私钥的使用期限比对应公钥的证件签名者证书的有效期要短很多。

4.1.1.1　证件签名者公钥有效期

证件签名者公钥的生命周期，即证书有效期，是通过将下列期限关联在一起来确定的：

- 对应的私钥用于签发电子机读旅行证件的期限长度，和；
- 根据该密钥签发的任何电子机读旅行证件的最长有效期[2]。

证件签名者证书（C_{DS}）应在该整个时期都有效，以便可以对电子机读旅行证件的真实性进行校验。然而，对应的私钥应该仅在有限的一段时间内用于签发证件；一旦用其进行签发的最后一份证件的有效期到期，将不再需要公钥。

4.1.1.2　证件签名者私钥签发期限

在部署其系统时，签发国或签发机构似宜考虑到一个证件签名者私钥将要签署的证件的数量。

签发国或签发机构可以部署一个或多个证件签名者，每个签名者都拥有自己独特的密钥对，该密钥对将在特定时间内保持有效。

为了最大程度地降低证件签名者证书被撤销时产生的业务持续成本，每天签发大量电子机读旅行证件的签发国或签发机构似宜：

- 使用一个使用期限很短的私钥；和/或
- 部署几个同时工作的并行证件签名者，每一个签名者都拥有自己的独特私钥和公钥证书。

每天签发少量电子机读旅行证件的签发国或签发机构可以选择部署单个证件签名者，还可以稍微延长一下私钥的使用期限。

无论每天签发的电子机读旅行证件的数量或同时工作的证件签名者的数量有多少，建议用于签署电子机读旅行证件的证件签名者私钥的最长有效期为三个月。

一旦使用特定私钥签署的最后一个证件制作完成，建议签发国或签发机构以可接受审计和问责的方式删除该私钥。

---

2. 一些签发国或签发机构可能会在电子机读旅行证件生效之前签发证件，如在结婚后改变姓名时。在此类情况下，“任何电子机读旅行证件的最长有效期”包括该电子机读旅行证件的实际有效期（如 10 年）加上该电子机读旅行证件签发日期与其生效日期之间的最长时间。

4.1.2 LDS2 签名者密钥和证书

与证件签名者密钥对相类似，LDS2 签名者密钥对中私钥的使用期限远短于相应证书的有效期。证书必须在电子机读旅行证件或签名的 LDS2 对象的生命周期（以较长者为准）内保持有效。由于签名的数据对象将被写入来自不同国家的电子机读旅行证件，因此这些证书必须至少在最长的电子机读旅行证件生命周期（即 10 年）内保持有效。

4.1.2.1 LDS2 签名者公钥有效期

LDS2 签名者公钥的生命周期，即证书有效期，是通过将以下两个期限关联在一起来确定的：

- 对应的私钥用于签署 LDS2 对象的期限长度，和：
- 以下各项的有效期，以较长者为准：
  - — 将存储用该密钥签名的 LDS2 对象的任何电子机读旅行证件；或
  - — 用该密钥签名的任何 LDS2 对象。请注意，对于 LDS2 电子签证，已签署的电子签证的有效期可能会超过包含该签证的电子机读旅行证件的有效期。

4.1.3 条形码签名者密钥和证书

条形码签名者是一种特定类型的签名服务器，用于签署独特的证件类型类别，例如签证、紧急旅行证件等。按照该领域的最佳做法，建议仅并行使用有限数量的签名密钥（较低的一位数）来创建数字印章签名，除非实际操作要求使得绝对有必要部署大量的密钥。为确保在发生与签名密钥相关的安全事件时条形码签名者的可用性，建议采取措施确保业务连续性（例如准备备份密钥、备份站点等）。

为了便于处理相应的证书（参见第 5 节），必须将每年发布的签名验证密钥数量限制在 5 个。

4.1.3.1 条形码签名者公钥有效期

本节适用于所有条形码签名者，包括签证签名者和紧急旅行证件签名者。

条形码签名者公钥的生命周期，即证书有效期，是通过将以下两个期限关联在一起来确定的：

- 对应的私钥用于签署签证或紧急旅行证件的期限长度，和；
- 根据该密钥签发的任何证件的最长有效期[3]

3. 一些签发国或签发机构可能会在电子机读旅行证件生效之前签发证件，如在结婚后改变姓名时。在此类情况下，“任何电子机读旅行证件的最长有效期”包括该电子机读旅行证件的实际有效期（如 10 年）加上该电子机读旅行证件签发日期与其生效日期之间的最长时间。

条形码签名者证书应在该整个期限内一直有效，以便可以对证件的真实性进行校验。然而，对应的私钥应该仅在有限的一段时间内用于签发证件；一旦用公钥进行签发的最后一份证件到期，将不再需要该公钥。

私钥使用期限：　　根据证件的概要而定
证书有效期：　　私钥使用期限+证件有效期

示例

注：本示例中用于计算的实际有效期并不意味着建议采取这样的有效期。

假设签发的证件有效期为 5 年，条形码签名者证书的私钥使用期限为 1 年。那么，条形码签名者证书的有效期为 1 + 5 = 6 年。如果国家签名认证机构证书的私钥使用期限为 3 年，则国家签名认证机构证书的有效期为 3 + 6 = 9 年。

4.1.4　国家签名认证机构密钥和证书

国家签名认证机构私钥的使用期限比对应公钥的国家签名认证机构证书的有效期要短很多。

4.1.4.1　国家签名认证机构的公钥有效期

国家签名认证机构公钥的生命周期，即证书有效期，是通过将下列期限关联在一起来确定的：

- 对应的国家签名认证机构私钥用于签署该机构签发的任何证书的期限长度；和
- 该国家签名认证机构签署的任何证书的最长密钥生命周期。

4.1.4.2　国家签名认证机构私钥的签发有效期限

用于签署证书和证书撤销列表的国家签名认证机构私钥的使用期限是在下列各种要素之间达成的一种微妙平衡：

- 万一签发国或签发机构的国家签名认证机构私钥被破坏，那么所有电子机读旅行证件只要是由遭破坏的国家签名认证机构私钥进行签署的证件签名者密钥签发的，其有效性就会遭到质疑。因此，签发国或签发机构似宜保持非常短的签发有效期。
- 然而，保持很短的签发有效期将造成任何时候都存在大量有效的国家签名认证机构公钥。这可在边防处理系统中造成更加复杂的证书管理问题。

因此建议签发国或签发机构每 3 到 5 年对其密钥对进行一次替换。

4.1.4.3 国家签名认证机构密钥重发

国家签名认证机构密钥在整个系统中提供了信任点，若没有这些信任点，系统将会崩溃。因此，签发国或签发机构应谨慎地计划其国家签名认证机构密钥对的替换事宜。一旦初始国家签名认证机构签名私钥的签发有效期已过，签发国或签发机构将在任何时候总有至少两个国家签名认证机构证书（C_{CSCA}）同时有效。

签发国或签发机构必须向接收国通报其国家签名认证机构密钥更替计划。这种通报必须在密钥更替开始前 90 天进行。在对密钥进行更替后，应将新的国家签名认证机构证书（认证新的国家签名认证机构公钥）分发给各接收国。

如果国家签名认证机构证书是一个新的自签名证书，应该使用带外方法对该证书进行验证。

在对国家签名认证机构密钥进行更替后，必须签发一个证书，用于链接新旧密钥，以便各信赖方可以进行安全的过渡。一般的做法是签发一个自签发证书，其中签发者和主体域相同，而用于校验签名的密钥是旧密钥对，经认证的公钥是新密钥对。这些国家签名认证机构链接证书无需使用带外方法进行校验，因为这些证书上的签名可通过使用该国家签名认证机构已有的可信公钥进行校验。还可以使用国家证书列表分发国家签名认证机构链接证书和国家签名认证机构自签名根证书。

在国家签名认证机构密钥更替后的头两天，签发国或签发机构应尽量不要使用国家签名认证机构新私钥，以便确保对应的国家签名认证机构新公钥证书成功分发完成。

签发国或签发机构在签署所有证书和签署证书撤销列表时必须使用最新的国家签名认证机构私钥。

4.1.5 证书撤销

如果出现事故（如密钥遭到破坏），签发国或签发机构可能需要撤销证书。

所有国家签名认证机构必须以证书撤销列表（CRL）的形式制作定期的撤销信息。

国家签名认证机构必须每 90 天至少发布一份证书撤销列表，即使自上次发布证书撤销列表之后没有撤销过任何证书也必须这么做。证书撤销列表的发布频率可以高于每 90 天一次，但是不得高于每 48 小时一次。

如果有证书被撤销，必须在 48 小时内分发一份证书撤销列表，标明被撤销的证书。

只有证书可以被撤销，证件安全对象不可被撤销。证书撤销列表的使用限于通报已撤销的由签发证书撤销列表的国家签名认证机构签发的证书（包括国家签名认证机构证书、证件签名者证书、国家证书列表签名者证书、偏差列表签名者证书和该认证机构签发的其他证书类型的撤销通知）。

电子机读旅行证件应用中不使用分区的证书撤销列表。一个国家签名认证机构撤销的所有证书，包括证件签名者证书、国家签名认证机构证书、国家证书列表签名者证书和偏差列表签名者证书，都列在同一个证书撤销列表中。尽管证书撤销列表总是由最新的（当前的）国家签名认证机构签名私钥签署，但证书撤销列表同时包括使用这一私钥签署的证书的撤销通知和使用国家签名认证机构早先签名私钥签署的证书的撤销通知。

4.1.5.1　国家签名认证机构证书的撤销

国家签名认证机构证书的撤销既极端罕见又不好处理。在告知接收国某一国家签名认证机构证书已被撤销后，使用对应的国家签名认证机构私钥签署的所有其他证书也被实际撤销。

当已经使用旧的国家签名认证机构私钥签署国家签名认证机构链接证书，以认证新的国家签名认证机构公钥时（见 4.1.4.3“国家签名认证机构密钥重发”），撤销旧的国家签名认证机构证书也应撤销新的国家签名认证机构证书。

如果需要撤销一个国家签名认证机构证书，该国家签名认证机构可以发布一份使用与要被撤销的公钥对应的私钥签署的证书撤销列表，因为这是此时证书撤销列表用户可以校验的唯一一个密钥。国家签名认证机构的这一公钥只有在用于校验该证书撤销列表的签名目的时，才应被认为是有效的。一旦证书撤销列表用户校验完证书撤销列表签名，国家签名认证机构的签名私钥便被认为已遭破坏，且证书将被撤销，未来不再用于校验目的。

为签发新的证件，签发国或签发机构必须重新从头启动认证过程，做法是：签发新的国家签名认证机构根证书，将该证书分发给各接收国，支持用带外方法确认每一个接收国所接收到的证书确实是真实的现行国家签名认证机构证书。

4.1.5.2　其他证书的撤销

当签发国或签发机构想要撤销国家签名认证机构签发的签名者证书时，无需等到当前证书撤销列表中的 nextUpdate 开始时再发布新的证书撤销列表。建议在撤销通知发出后的 48 小时内发布新的证书撤销列表。

4.1.6　加密算法

签发国或签发机构可能会支持在其国家证书签名认证机构和签名证书密钥中使用不同的算法。例如，国家签名认证机构证书可能是使用 RSA 签发的，但签名者证书使用的可能是椭圆曲线数字签名算法（ECDSA），反之亦然。

签发国或签发机构应选择适当的密钥长度，以防范遭受攻击。应该考虑采用适当的加密目录。

接收国若希望验证电子机读旅行证件上的签名，必须支持所有算法。

为了能在其国家签名认证机构、签名密钥和证件安全对象（如适用）中使用下文所述的算法，签发国或签发机构应支持其中一种算法。

4.1.6.1　RSA 公钥算法

使用 RSA 算法生成签名以及校验证书和证件安全对象（SO_D）的签发国或签发机构应使用[RFC 4055]。[RFC 4055]规定了两种签名机制：RSASSA-PSS 和 RSASSA-PKCS1_v15。建议签发国或签发机构根据 RSASSA-PSS 生成签名，但接收国还必须可以根据 RSASSA-PKCS1_v15 校验签名。

4.1.6.2 数字签名算法（DSA）

使用数字签名算法生成签名或校验签名的签发国或签发机构应使用 [FIPS 186-4]。

4.1.6.3 椭圆曲线数字签名算法（ECDSA）

使用椭圆曲线数字签名算法生成签名或校验签名的签发国或签发机构应使用 [X9.62] 或 [ISO/IEC 15946]。用来生成椭圆曲线数字签名算法密钥对的椭圆曲线域参数必须在公钥参数中作出明确说明，即：参数必须为 ECParameters 型（无命名曲线，无隐含参数），并且必须包括选择性辅因子。ECPoints 必须为非压缩格式。

建议遵循 [TR 03111] 指导原则。

4.1.6.4 散列法算法

唯有 SHA-224、SHA-256、SHA-384 和 SHA-512 是允许采用的散列算法。见[FIPS 180-2]。

4.1.7 LDS2 签名者证书加密算法

由于 LDS2 证书和签名对象存储在非接触式集成电路上，因此它们需要尽可能紧凑。所以，无论国家签名认证机构和证件签名密钥中使用的是什么算法，LDS2 签名者都必须使用 ECDSA。

4.2 授权公钥基础设施

实施 LDS2 的签发国或签发机构应具有以下几种密钥对：

- 国家校验认证机构（CVCA）密钥对；
- 证件校验者（DV）密钥对；和
- 终端密钥对。

国家校验认证机构公钥和证件校验者公钥由国家校验认证机构认证。终端公钥由证件校验者认证。国家校验认证机构、证件校验者和终端的公钥证书是卡可校验证书，必须符合第 7 节中定义的各自的证书概要。国家校验认证机构、证件校验者或终端证书没有撤销机制。因此，它们的有效期比 X.509 类型的证书短得多。

私钥使用期限没有具体规定，可由国家自行确定。然而，私钥使用期限必须至多等于公钥有效期。国家校验认证机构、证件校验者和终端密钥对的公钥有效期如表 2 所示。

表 2　卡可校验证书密钥使用期限

	公钥有效期
国家校验认证机构	6 个月至 3 年
证件校验者	2 周至 3 个月
终端	1 天至 1 个月

4.2.1　终端认证加密算法

授权公钥基础设施中用于终端认证的算法由电子机读旅行证件签发国的国家校验认证机构确定。一个证书链（即某一个给定授权的国家校验认证机构、证件校验者和终端证书）中必须使用相同的签名算法、域参数和密钥大小。因此，必须为证件校验者和终端提供几个密钥对。国家校验认证机构链接证书可以包含一个偏离当前参数的公钥，即国家校验认证机构可以切换到新的签名算法、新的域参数或密钥大小。

对于终端认证，可以使用 RSA 或 ECDSA。Doc 9303 号文件第 11 部分提供了这方面的详细信息。

4.2.2　单一联络点加密算法

表 3 列出了用于单一联络点协议的 TLS 加密套件。

表 3　TLS 加密套件

密码套件	证书和密钥交换算法
TLS_RSA_WITH_AES_128_CBC_SHA	RSA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE_RSA
TLS_RSA_WITH_AES_256_CBC_SHA	RSA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE_RSA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE_ECDSA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE_ECDSA

对于 TLS 握手协商，客户端应支持表 3 中定义的所有 TLS 密码套件。服务器和客户端均应支持基于 RSA 和 ECDSA 的认证。允许服务器向客户端请求，也允许客户端发送与服务器证书不同类型的客户端证书。

在 TLS 握手中使用 ECDHE_ECDSA 密钥协议是按照[TLSECC]、[TLS1.2]和[TLSEXT]中定义的添加做法来进行的。就 TLS 握手而言，客户端和服务器都应支持 [TLSECC] 规范中规定的适当的椭圆曲线扩展。[TLSECC] 第 5 节对受支持的椭圆曲线和椭圆曲线点格式作了定义。对于表 3 中定义的使用高级加密标准（AES）进行加密的受支持 TLS 密码套件，使用这些套件应按照 [TLSAES] 规范来进行。

5. 分发机制

对于电子机读旅行证件公钥基础设施，需要将公钥基础设施对象分发至各接收国。根据对象类型和运行要求的不同，可采用多种不同的分发机制。须注意的是，这些对象的分发并不建立对这些对象或与其相关的私钥/公钥的信任。有关建立信任的机制在第 6.1 节中进行了说明。

授权公钥基础设施的分发机制在第 8 节进行了介绍。

需要从签发国或签发机构分发到接收国的对象包括：

- 国家签名认证机构证书；
- 国家签名认证机构链接证书；
- 证件签名者证书；
- LDS2 签名者证书；
- 国家校验认证机构初始证书；
- 国家校验认证机构链接证书；
- 证件校验者证书；
- 条形码签名者证书；
- 证书撤销列表（空或非空）；
- 国家证书列表签名者证书；国家证书列表；和
- 偏差列表签名者证书；偏差列表。

在电子机读旅行证件和授权公钥基础设施中使用的分发机制包括：

- 公钥目录；
- 双边交换；
- 单一联络点；
- 国家证书列表；

- 偏差列表；和
- 电子机读旅行证件非接触式集成电路。

如表 4 所示，为每一个对象规定了主要和次要（如适用）分发机制。

表 4　公钥基础设施对象的分发

	非接触式集成电路	单一联络点	双边交换	公钥目录	偏差列表	国家证书列表	注释
国家签名认证机构证书			Y（主要）			Y（次要）	
证件签名者证书	Y（主要）			Y（次要）			在写入证件安全对象的同时将证书写入
LDS2签名者证书	Y						在写入签名对象的同时将证书写入
国家校验认证机构初始证书	Y						在电子机读旅行证件个人化时将证书写入
国家校验认证机构链接证书	Y	Y					通过单一联络点将证书分发给证件校验者，并在下一次校验时在非接触式集成电路上对国家校验认证机构信任锚进行更新
证件校验者证书		Y					仅分发给主体证件校验者
证书撤销列表（空或非空）			Y（次要）	Y（主要）			国家签名认证机构签发的证书撤销列表包含与 LDS2公钥基础设施对象相关的撤销信息
国家证书列表签名者证书						Y	
条形码签名者证书			Y（次要）	Y（主要）			条形码签名者未在条形码中进行编码，因此必须确保分发证书，以验证条形码
国家证书列表			Y	Y			
偏差列表签名者证书					Y		

从操作上讲，接收国不必非得既使用主要方法，也使用次要方法。在查验系统的每日操作中，查验机构可自行决定是使用主要方法，还是使用次要方法。如果接收国的相关机构在其日常操作中使用次要方法验证证书或证书撤销列表，则该机构也应该做好支持主要方法的准备。

签发国或签发机构需要为国家签名认证机构密钥和签名者密钥制定密钥对更替策略，以便能够使证书和证书撤销表及时传送到接收国的边防控制系统中。传送最好在 48 小时之内进行，但是一些接收国的边防检查哨所可能比较偏远，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。接收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。

签发国或签发机构应该要求接收国将在 48 小时之内将国家签名认证机构证书（C_{CSCA}）传送出去。

通过将证件签名者证书（C_{DS}）包括在证件安全对象（SO_D）中，签发国或签发机构能够确保证件签名者证书（C_{DS}）的及时传送。签发国或签发机构还应该要求在 48 小时之内将公钥目录中公布的证件签名者证书（C_{DS}）传送至边防检查站。

条形码签名者证书并不包含在数字印章本身中。因此，签发受数字印章保护的证件的国家必须发布其所有的条形码签名者证书。条形码签名者证书的主要分发渠道是公钥目录/双边交换。其他机制，例如在网站上发布，是次要渠道。

对于条形码签名者，证书的发布必须遵循以下原则：

- 新证书一经创建，必须在 48 小时之内将其发布；和
- 证书必须保持发布状态，直至到期或被撤销。

接收国应该竭尽全力通过电子或其他手段执行证书撤销列表，包括那些在特殊情况下发布的证书撤销表。

可通过将国家证书列表签名者证书包含在每次的国家证书列表中来确保其及时传送出去。

5.1 公钥目录分发机制

国际民航组织提供了一项公钥目录（PKD）服务。这一服务应接受各种公钥基础设施对象，包括来自于公钥目录参与国的证书、证书撤销列表和国家证书列表，将它们存储在一个目录中，并让所有接收国都可以获得这些对象。

国家签名认证机构证书（C_{CSCA}）并不作为国际民航组织公钥目录服务的一部分单独存储。然而，如果将它们载于国家证书列表中，它们是可以出现在公钥目录中的。

每一个证书在公钥目录中保留至其证书有效期到期，无论对应的私钥是否还在用。

所有公钥目录参与国存储在公钥目录中的证书、证书撤销列表和国家证书列表应对需要使用该信息验证通过数字方式存储的电子机读旅行证件数据、LDS2 对象和可见数字印章对象的真实性和完整性的各方（包括非公钥目录参与国）提供。

5.1.1　公钥目录的上传

仅公钥目录参与国可以将证书、证书撤销列表和国家证书列表上传至公钥目录。所有证书和证书撤销列表必须符合第 7 节中的概要。所有国家证书列表必须遵守第 9 节中的规范。

公钥目录由“写入目录”和“读取目录”组成。公钥目录参与国应使用轻量级目录访问协议（LDAP）将他们的对象上传至写入目录。一旦对一个对象进行了电子签名校验，且完成了其他例行检查，该对象便会发布在读取目录中。

5.1.2　公钥目录的下载

应该向公钥目录参与国和非参与国提供读取公钥目录中公布的所有证书、证书撤销列表和国家证书列表的权限。不得对公钥目录的读取实施访问控制。

接收国应负责将从公钥目录中下载的对象分发至其查验系统，并且应维持一个证书撤销列表当前缓存区和校验电子机读旅行证件数据上的签名所需用到的证书。

5.2　双边交换分发机制

对于证书撤销列表和国家证书签名认证机构证书（C_{CSCA}），主要分发渠道是签发国或签发机构和接收国之间的双边交换。双边交换也可用于分发国家证书列表。

用于这种双边交换的具体技术可能因每一个需要分发其证书、证书撤销列表和国家证书列表的签发国或签发机构的政策以及需要使用这些对象的每一个接收国的政策而异。可用于双边交换的技术的一些例子包括：

- 外交信使/外交邮袋；
- 电子邮件交换；
- 从与进行签发的国家签名认证机构相关的网站进行下载；和
- 从与进行签发的国家签名认证机构相关的轻量级目录访问协议服务器上进行下载。

这并非详尽的列表，还可以使用其他技术。

5.3　国家证书列表分发机制

国家证书列表是双边分发机制的一种支持技术。因此，通过国家证书列表分发国家签名认证机构证书是双边分发机制的一种方法。

国家证书列表是发布该列表的接收国或接收机构所“信任的”国家签名认证机构证书的一个经数字签名的列表。国家签名认证机构自签名根证书和国家签名认证机构链接证书可以纳入国家证书列表中。国家证书列表的结构和格式在第 8 节进行了规定。公布国家证书列表可以让其他接收国或接收机构从一个单一来源（国家证书列表发布者）获得一套国家签名认证机构证书，而不用与在该列表上出现的每一个签发机关或签发机构达成直接双边交换协议。

国家签名认证机构授权国家证书列表签名者编制、通过数字方式签署和发布国家证书列表。国家证书列表不得由国家签名认证机构自己直接签名和发布。国家证书列表签名者证书必须符合第 7 节中所规定的证书概要。

在发布国家证书列表之前，负责发布的国家证书列表签名者应该广泛地验证将要被会签的国家证书签名认证机构的证书，包括确保这些证书确实属于所确定的国家签名认证机构。用于这种带外验证的程序应该在签发该国家证书列表签名者证书的国家签名认证机构的公布的证书政策中予以反映。

每一个国家证书列表必须包括国家证书列表签名者证书，该证书将被用于校验该国家证书列表上的签名以及签发该国家证书列表签名者证书的国家签名认证机构的证书。

如果接收国收到新的国家签名认证机构证书，且已经完成验证程序，则建议编制和发布新的国家证书列表。

对于一些接收国而言，使用国家证书列表确实可以使国家签名认证机构证书的分发变得更为高效。然而，使用国家证书列表的接收国仍旧必须确定关于对该列表内所载证书建立信任的相关政策（详见第 6 节）。

6. 公钥基础设施的信任和验证

电子机读旅行证件公钥基础设施和授权公钥基础设施有着不同的公钥基础设施信任和验证做法。

6.1 电子机读旅行证件公钥基础设施

在电子机读旅行证件公钥基础设施的环境中，接收国的查验系统扮演公钥基础设施信赖方的角色。对电子机读旅行证件的证件安全对象上电子签名的成功校验可确保存储于该电子机读旅行证件的非接触式集成电路中的数据的真实性和完整性。签名校验过程要求信赖方确定用于校验签名的证件签名者公钥本身是“可信的”。

通过第 5 节中界定的各种分发机制，接收国可以获得校验所涉数字签名所需的证书和证书撤销列表。然而，这些分发机制不对这些证书、证书撤销列表或用于校验这些证书和证书撤销列表上签名的公钥建立信任。

国家签名认证机构证书（C_{CSCA}）中所载的公钥用于校验证书和证书撤销列表上的数字签名。因此，在接受另一个签发国的电子机读旅行证件时，接收国必须已经将签发国或签发机构的国家签名认证机构证书（C_{CSCA}）的一个受信任副本或者从该证书获得的关于该国家签名认证机构公钥的其他形式的信任锚信息放入某种形式的信任库，其边防管制系统应可以使用该信任库。

接收国有责任以安全的方式对国家签名认证机构证书（C_{CSCA}）建立信任并将该证书（或来自该证书的信息）存储为信任锚，供其边防查验系统使用。

6.1.1 信任锚的管理

正如 [RFC 5280] 所规定的，必须建立一个信任锚，用于确定一特定证件签名者、国家证书列表签名者、偏差列表签名者或其他类型证书的验证程序。

每一个信任锚由一个可信的公钥和相关的元数据组成。信任锚必须至少包括下列内容：

- 可信的公钥和任何相关的密钥参数；
- 公钥算法；
- 密钥所有者的名称；和
- 国家签名认证机构证书包含国际民航组织分配的签发机关或机构三字代码的“SubjectAltName”扩展的值。尽管这方面的信息不用于认证路径或证书撤销列表验证程序中，但是用于 Doc 9303 号文件第 11 部分中定义的被动验证。

在电子机读旅行证件应用中，对特定国家签名认证机构的每一个公钥都建立一个单独的信任锚。对于从国家签名认证机构获得的初始公钥，必须通过带外机制建立信任。例如，如果从与国家签名认证机构相关的服务器上下载一个国家签名认证机构证书，可采用带外通信（如电话或电子邮件）来校验所下载的证书实际上是该国家签名认证机构的真实证书。另外，信赖方可以分析进行签发的国家签名认证机构的政策、程序和做法，以确定其是否足够安全，可以满足使用证书的当地要求。一旦为特定国家签名认证机构建立了初始信任锚，便可对该国家签名认证机构后续密钥的处理过程进行简化。如果该国家签名认证机构签发了一个国家签名认证机构链接证书，那么可以省去通过带外方式与该国家签名认证机构进行通信以校验新证书的真实性，因为可以使用该国家签名认证机构的已经获得信任的公钥来校验该链接证书上的签名。

信任锚信息可以为国家签名认证机构证书的一个可信副本，或其他一种可信格式。

由于国家签名认证机构所签发证书上的签名需要在该国家签名认证机构更新其密钥对后的很长时间内可以验证，因此，接收国通常会在同一时间有多个针对同一国家签名认证机构的信任锚。如果国家签名认证机构已经更名，这些信任锚中有一些将包含旧的国家签名认证机构名称，其他信任锚则将包含新的名称。

6.1.2　证书/证书撤销列表验证和撤销检查

作为校验电子机读旅行证件应用中数据对象（如证件安全对象、国家证书列表、偏差列表等）的真实性和完整性的过程的一部分，接收国应：

- 验证用于校验数据对象（如证件签名者证书、国家证书列表签名者证书、偏差列表签名者证书）上签名的证书；
- 验证用于检查所涉证书的撤销状态的证书撤销列表；和
- 处理证书撤销列表，以便校验所涉证书的撤销状态。

现在已有可用于这些过程的示范算法，如 [RFC 5280] 中规定的算法。接收国无需采用 RFC 5280 中定义的具体算法，但是所提供的功能必须与这一程序的外部性能相当。在具体操作时，可以采用任何算法，只要该算法可以推导出正确的结果。

附录 D 为选择 [RFC 5280] 中规定的算法作为自己算法的依据的接收国提供了指导。

6.1.3 条形码验证机构

条形码验证机构通过应用验证策略来验证数字印章。Doc 9303 号文件第 13 部分详细规定了用于生成验证状态的验证标准和算法。

图 4 图解说明了条形码验证机构的功能架构。条形码验证机构依赖于验证软件开展工作，该软件可以部署在边防管制机构使用的任何计算机上。

该验证软件与一个阅读器相连。这一阅读器读取条形码的图像以检索证件的条形码和机读区，并读取该证件的图像以检索其机读区。为了校验数字印章签名的有效性，验证软件应至少每 24 小时与公钥基础设施发布点进行同步，以检索最新的条形码签名者证书和证书撤销列表。

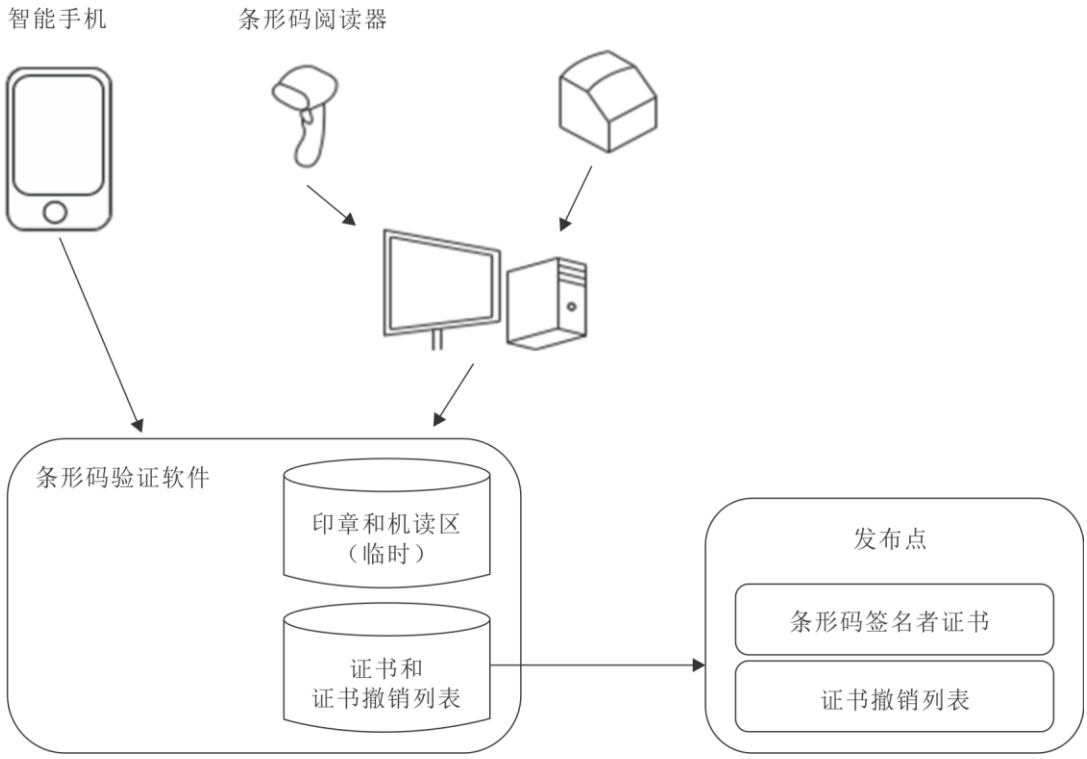

图 4 条形码的验证

条形码验证软件对任何相关证件（如签证或护照）的数字印章和机读区进行解码，验证数字印章的签名，并应用验证策略（参见 Doc 9303 号文件第 13 部分）以生成证件的验证状态。

在移动场景中，验证软件也可以直接在智能手机上运行。虽然印章的有效性可以通过智能手机上的软件进行验证，但印章内的（签名）数据与打印的机读区（如签证或护照的机读区）之间的比较必须手动完成，或者通过光学字符识别方法从捕获的图像中识别机读区，后者实践起来往往具有挑战性。

条形码验证软件可处理以下数据：

- 阅读器提供的输入数据，例如签证或护照的图像；和
- 证书和证书撤销列表。

6.2　授权公钥基础设施

对于授权公钥基础设施，在信任锚和验证的处理方面，采取的是另一种不同的做法。

6.2.1　卡可校验证书的验证

对于授权公钥基础设施中的证件校验者和终端证书，信任锚是签发电子机读旅行证件的国家所设立的国家校验认证机构的最新公钥。初始信任锚应在制作或（预）个人化阶段安全存储在电子机读旅行证件非接触式集成电路中。当国家校验认证机构使用的密钥对随时间发生变化时，会生成国家校验认证机构链接证书。电子机读旅行证件非接触式集成电路必须根据收到的有效链接证书自行更新其信任锚。由于国家校验认证机构链接证书的时间安排，一次最多将有两个国家校验认证机构信任锚存储在非接触式集成电路上。

为了验证终端证书，必须为电子机读旅行证件非接触式集成电路提供一个证书链，证书链的起始端为存储在该电子机读旅行证件非接触式集成电路上的信任锚。

证件校验者和终端证书的验证程序取决于具体的 LDS2 终端认证协议，Doc 9303 号文件第 11 部分对该验证程序进行了规定。

7.　证书和证书撤销列表概要

本节分别对电子机读旅行证件公钥基础设施和授权公钥基础设施的证书概要进行了规定。

7.1　电子机读旅行证件公钥基础设施

签发国或签发机构必须签发符合下文所规定概要的证书和证书撤销列表。所有证书和证书撤销列表必须使用唯一编码规则（DER）格式制作，以保护其中签名的完整性。本规范第六版中所载的关于国家签名认证机构和证件签名者证书的概要在一些地方与当前概要存在不同。查验系统必须能够处理根据早先概要（见附录 C）以及当前概要签发的证书。

这些概要是基于这样的要求制定的：每一个签发国或签发机构或实体应建立单一的一个国家签名认证机构负责签署符合 Doc 9303 号文件规定的所有机读旅行证件。

本节针对下列证书类型规定了证书概要：

- 国家签名认证机构；
- 证件签名者；

- 国家签名认证机构国家证书列表签名者；
- 偏差列表签名者；和
- 通信 — 即使严格来讲其并不是现在所需的。这是未来用于验证的一个步骤。这些证书可用于访问公钥目录或用于各国之间的 LDAP/EMAIL/HTTP 通信。建议由国家签名认证机构签发这类证书。

国家签名认证机构、证件签名者、偏差列表签名者和国家签名认证机构国家证书列表签名者对象在第 3 节中进行了规定。

证书撤销列表概要在第 7.1.4 节中进行了规定。

对于每一个组成部分/扩展的存在要求，这些概要使用下列术语进行表示：

m 强制性 — 该域必须存在；
x 不使用 — 该域不得存在；
o 选择性 — 该域可以存在；
c 条件性 — 该域应在特定条件下存在。

对于可以/必须包括在内的扩展的关键性要求，这些概要使用下列术语进行表示：

c 关键的 — 接收应用必须能够处理该扩展；
nc 非关键的 — 接收应用若不理解该扩展，可将其忽略。

这些概要中确定的一些要求是从所参考的基准概要（如 RFC 5280）中沿用而来的。为方便起见，附录 B 中的表格对涉及具体要求的基准概要中的相关文字进行了抄录。

7.1.1 证书概要

表 5 规定了证书正文部分各个域的证书概要要求，这些要求对于所有证书是通用的。表 6 规定了证书扩展要求。

表 5 证书各域概要

证书组成部分	是否应存在	注释
Certificate	m	
TBSCertificate	m	见表 6
signatureAlgorithm	m	这里插入的值取决于所选择的算法
signatureValue	m	这里插入的值取决于所选择的算法
TBSCertificate		
version	m	**必须**为 v3
serialNumber	m	必须为正整数且最大为 20 个八位位组 必须使用二进制补码且以最少的八位位组表示

证书组成部分	是否应存在	注释
signature	m	这里插入的值必须和 Certificate 序列的 signatureAlgorithm 组成部分的值相同
issuer	m	如果存在 countryName 和 serialNumber，必须为 PrintableString 有 DirectoryString 句法的其他属性必须为 PrintableString 或 UTF8String countryName 必须为大写字母 见第 7.1.1.1 节的命名规则
validity	m	必须以 Z 结束 必须存在秒元素 2049 年及以前的日期必须为 UTCTime UTCTime 必须以 YYMMDDHHMMSSZ 表示 2050 年及以后的时间必须为 GeneralizedTime GeneralizedTime 不得有小数秒 GeneralizedTime 必须以 YYYYMMDDHHMMSSZ 表示
subject	m	如果存在 countryName 和 serialNumber，必须为 PrintableString 有 DirectoryString 句法的其他属性必须为 PrintableString 或 UTF8String countryName 必须为大写字母 issuer 域和 subject 域中的 countryName 必须匹配 见第 7.1.1.1 节的命名规则
subjectPublicKeyInfo	m	
issuerUniqueID	x	
subjectUniqueID	x	
extensions	m	见关于应该存在哪些扩展的表 6 扩展的缺省值不得编码

表 6　证书扩展概要

扩展名称	国家签名认证机构自签名根		国家签名认证机构链接		证件签名者		国家证书列表签名者和偏差列表签名者		通信		注释
	是否应存在	关键性	是否应存在	关键性	是否应存在	关键性	是否应存在	关键性	是否应存在	关键性	
AuthorityKeyIdentifier	**o**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	
keyIdentifier	m		m		m		m		m		
authorityCertIssuer	o		o		o		o		o		
authorityCertSerialNumber	o		o		o		o		o		
SubjectKeyIdentifier	**m**	**nc**	**m**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	
subjectKeyIdentifier	m		m		m		m		m		
KeyUsage	**m**	**c**	**m**	**c**	**m**	**c**	**m**	**c**	**m**	**c**	
digitalSignature	x		x		m		m		o		一些通信证书（如传输层安全证书）要求按照所使用的特定加密套件来设置 keyUsage 位。一些加密套件要求设置 digitalSignature 位，一些则不要求。
nonRepudiation	x		x		x		x		x		
keyEncipherment	x		x		x		x		o		
dataEncipherment	x		x		x		x		x		
keyAgreement	x		x		x		x		o		
keyCertSign	m		m		x		x		x		
cRLSign	m		m		x		x		x		
encipherOnly	x		x		x		x		x		
decipherOnly	x		x		x		x		x		
PrivateKeyUsagePeriod	**m**	**nc**	**m**	**nc**	**m**	**nc**	**o**	**nc**	**o**	**nc**	
notBefore	o		o		o		o		o		notBefore 和 notAfter 中必须至少出现一个
notAfter	o		o		o		o		o		必须编码为 generalizedTime

扩展名称	国家签名认证机构自签名根		国家签名认证机构链接		证件签名者		国家证书列表签名者和偏差列表签名者		通信		注释
CertificatePolicies	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	
PolicyInformation	m		m		m		m		m		
policyIdentifier	m		m		m		m		m		
policyQualifiers	o		o		o		o		o		
PolicyMappings	**x**		**x**		**x**		**x**		**x**		见注 1
SubjectAltName	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	见第 7.1.1.2 节
IssuerAltName	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	见第 7.1.1.2 节
SubjectDirectoryAttributes	**x**		**x**		**x**		**x**		**x**		
Basic Constraints	**m**	**c**	**m**	**c**	**x**		**x**		**x**		
cA	m		m		x		x		x		
PathLenConstraint	m		m		x		x		x		必须始终为“0”
NameConstraints	**x**		**x**		**x**		**x**		**x**		见注 1
PolicyConstraints	**x**		**x**		**x**		**x**		**x**		见注 1
ExtKeyUsage	**x**		**x**		**x**		**m**	**c**	**m**	**c**	见第 7.1.1.3 节
CRLDistributionPoints	**m**	**nc**	**m**	**nc**	**m**	**nc**	**m**	**nc**	**o**	**nc**	
distributionPoint	m		m		m		m		m		必须为 ldap、http 或 https 见第 7.1.1.4 节
reasons	x		x		x		x		x		
cRLIssuer	x		x		x		x		x		
InhibitAnyPolicy	**x**		**x**		**x**		**x**		**x**		见注 1
FreshestCRL	**x**		**x**		**x**		**x**		**x**		见注 2
privateInternetExtensions	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	见注 3
NameChange	**o**	**nc**	**o**	**nc**	**x**		**x**		**x**		见第 7.1.1.5 节
DocumentType	**x**		**x**		**m**	**nc**	**x**		**x**		见第 7.1.1.6 节
Netscape Certificate Type	**x**		**x**		**x**		**x**		**x**		见注 4
other private extensions	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	**o**	**nc**	

注 1：按照定义，扩展只可以出现在中间认证机构证书上（一个认证机构向另外一个认证机构签发的证书）。中间认证机构证书不用在电子机读旅行证件的公钥基础设施中。因此电子机读旅行证件证书中禁用这种扩展。

注 2：使用最新的证书撤销列表扩展指向增量证书撤销列表。电子机读旅行证件的公钥基础设施不支持增量证书撤销列表。因此禁用这种扩展。

注 3：RFC 5280 中规定了两种专用因特网扩展（机构信息访问和主体信息访问），用于指向与证书签发者或证书主体相关的信息。这些扩展不要求出现在电子机读旅行证件的公钥基础设施中。然而，由于它们不影响互操作性，且是非关键的，因此可以选择性地将其包括进电子机读旅行证件证书当中。

注 4：网景证书类型扩展可用来限制一个证书的使用用途。extKeyUsage 和 basicConstraints 扩展是当前用于表示这种用途的标准扩展，且用在电子机读旅行证件应用中。由于标准扩展和网景专用扩展的值之间存在潜在冲突，因此禁用网景扩展。

7.1.1.1 关于签发者和主体域的要求

签发者和主体域对所有证书都是通用的，但 LDS2 签名者证书有特定的限制。

7.1.1.1.1 一般要求

要求遵守关于 Issuer 和 Subject 域的下列命名和寻址规则。

- countryName 必须存在。该值包含一个国家代码，该代码必须遵守 Doc 9303 号文件第 3 部分中所规定的两字国家代码格式
- commonName 必须存在。

签发国或签发机构还可自行决定纳入其他属性。

7.1.1.1.2 关于 LDS2 签名者证书的要求

LDS2 签名者证书必须符合上文规定的证件签名者证书概要，但 7.1.2 规定了一些例外情况。

7.1.1.2 关于签发者和主体替代名称的要求

由于电子机读旅行证件应用中的替代名称所发挥的功能是专门针对这种应用且不同于[RFC 5280]中为因特网公钥基础设施所规定的功能，因此电子机读旅行证件证书的主体替代名称扩展通常不会清楚地表明证书主体。

在电子机读旅行证件应用中，替代名称发挥下列两种功能。

第一种功能是提供证书的主体和/或签发者的联系信息。为此，它应该至少包括下列内容：

- rfc822Name；
- dNSName；或
- uniformResourceIdentifier.

第二种功能是提供一个由国际民航组织所分配的国家代码组成的目录字符串。为此，使用该概要签发的证书必须额外地包括一个按如下方式构成的目录名称：

- 包含国际民航组织国家代码的 localityName，该代码应与机读区中所示的一样；和

- 如果这一国家代码无法作为签发国或签发机构的唯一识别信息，则应该使用 stateOrProvinceName 这一属性来表示国际民航组织分配的该签发国或签发机构三字代码。
- 不允许使用其他属性。

在国家签名认证机构的自签名根证书中，IssuerAltName 和 SubjectAltName 扩展必须是相同的。在国家签名认证机构链接证书中，这些值可以不同。例如，如果国家签名认证机构的 rfc822Name 在快要签发国家签名认证机构链接证书之前发生了变化，则 IssuerAltName 扩展将包含旧的 rfc822Name，而 SubjectAltName 扩展将包含新的 rfc822Name。任何后续的国家签名认证机构链接证书将在两个扩展中包含新的 rfc822Name。

7.1.1.3　关于扩展密钥用途扩展的要求

国家证书列表签名者证书的 extendedKeyUsage 扩展中必须包括的对象标识符（OID）为 2.23.136.1.1.3。

偏差列表签名者证书的 extendedKeyUsage 扩展中必须包括的对象标识符（OID）为 2.23.136.1.1.8。

对于通信证书而言，这一扩展的值取决于所使用的通信协议（见 RFC 5280 第 4.2.1.12 节）。

7.1.1.4　关于证书撤销列表分发点扩展的要求

国家签名认证机构可以在多个地方公布其证书撤销列表，包括公钥目录、自己的网站等。

对于在公钥目录以外地方（例如网站或本地轻量目录访问协议服务器）公布的证书撤销列表，这一扩展中要包括的值受签发相关证书和证书撤销列表的国家签名认证机构的控制。

对于提交给公钥目录的证书撤销列表，公钥目录参与国可以使用下列模板针对其证书撤销列表纳入两个 URL 值（用国际民航组织分配的签发国或签发机构三字代码代替“CountryCode”）。如果该国家代码无法作为签发国或签发机构的唯一识别信息，则通过下列方式输入内容：在机读区中的三字国家代码上附加“_”符号，接着输入可作为该签发国或签发机构唯一识别信息的国际民航组织分配的该签发国或签发机构三字代码。

https://pkddownload1.icao.int/CRLs/CountryCode.crl
https://pkddownload2.icao.int/CRLs/CountryCode.crl

这是一种强制扩展，并且撤销状态检查是验证程序的一个强制部分。因此必须至少填写其中的一个值：

- 公钥目录的值可能是扩展中仅有的值；
- 可能会有额外的值（例如，国家签名认证机构可能也会选择在网站上公布其证书撤销列表并包括一个指向该来源的指示标）；或
- 即使国家签名认证机构也将其证书撤销列表提交给公钥目录，该机构也可能选择仅包括单个值（例如，指向其网站来源的指示标）。

下列示例说明了新加坡和香港签发机构所签发的证书中要填写的公钥目录的值：

新加坡公钥目录示例：
https://pkddownload1.icao.int/CRLs/SGP.crl
https://pkddownload2.icao.int/CRLs/SGP.crl

香港示例：
https://pkddownload1.icao.int/CRLs/CHN_HKG.crl
https://pkddownload2.icao.int/CRLs/CHN_HKG.crl

7.1.1.5 名称变更扩展

当对国家签名认证机构密钥进行更替时，必须签发一个将旧公钥与新公钥链接起来的证书，以便为信赖方提供安全的过渡。通常，这是通过签发自签发证书实现的，在该证书中，issuer 和 subject 这两个域是相同的，但是用于校验签名的密钥是旧的密钥对，经认证的公钥是新密钥对。

建议国家签名认证机构不要无谓地更改它们的唯一甄别名（DN），因为这会对信赖方产生负面影响（它们必须为同一签发国或签发机构保留新旧两种名称，作为有效的国家签名认证机构，直至旧名称之下的所有电子机读护照失效）。然而，如果确需更名，必须通过签发国家签名认证机构链接证书将相关情况传送给信赖方，在该证书中，issuer 域包含旧名称，subject 域包含新名称。这一国家签名认证机构链接证书也可以传送有关密钥更替的信息，其中用于校验签名的密钥是旧密钥对，而经认证的公钥是新密钥对。既用于传达国家签名认证机构名称变更又用于传达该机构的密钥更替情况的证书必须包含 NameChange 扩展，以便表明该证书的这种性质。这对 PathLengthConstraint 没有影响，它仍旧是“0”。

此外，NameChange 扩展也可以包括在国际签名认证机构唯一甄别名发生变化时创建的新的国家签名认证机构自签名证书中。在这样的自签名国家签名认证机构根证书中，issuer 和 subject 域均包含新的唯一甄别名。不同于同时包含国家签名认证机构新旧唯一甄别名的国家签名认证机构自签发链接证书，将 NameChange 包括进国家签名认证机构自签名根证书只是表明已经发生了更名，并不将新旧唯一甄别名链接起来。

国家签名认证机构不得重复使用证书序列号。国家签名认证机构所签发的每一份证书，无论该机构是否更过名，都必须是唯一的。

用于更名扩展的 ASN.1：

```
nameChange EXTENSION ::= {
    SYNTAX NULL
    IDENTIFIED BY id-icao-mrtd-security-extensions-nameChange}

id-icao-mrtd-security-extensions OBJECT IDENTIFIER ::= {id-icao-
mrtd-security 6}
id-icao-mrtd-security-extensions-nameChange OBJECT IDENTIFIER ::=
{id-icao-
mrtd-security-extensions 1}
```

7.1.1.6　证件类型扩展

必须使用 DocumentType 扩展来表示对应的证件签名者可以制作的证书类型，该类型应该与机读区上所示的信息一样。该扩展必须始终被设定为非关键的。

证件类型列表扩展的 ASN.1：

```
documentTypeList EXTENSION ::= {
    SYNTAX DocumentTypeListSyntax
    IDENTIFIED BY id-icao-mrtd-security-extensions-documentTypeList}

DocumentTypeListSyntax ::= SEQUENCE {
    version        DocumentTypeListVersion,
    docTypeList    SET OF DocumentType }

DocumentTypeListVersion ::= INTEGER {v0(0)}
```

— 证件类型和机读区所载类型一样，如其中“P”或“ID”
— 每个单一字母表示以该字母打头的所有证件类型

```
DocumentType ::= PrintableString(SIZE (1..2))

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

7.1.2　LDS2 签名者证书概要

LDS2 签名者证书必须符合 7.1.1 规定的证件签名者证书概要，但有以下例外情况：

主体域：
LDS2 签名者证书的“主体”域必须按照以下方式填写：

- countryName 必须存在。该值包含一个国家代码，该代码必须遵守 Doc 9303 号文件第 3 部分中所规定的两字国家代码格式。
- commonName 必须存在。此属性中的值长度不得超过 9 个字符。
- 不得包含其他属性。

证书扩展：
LDS2 签名者证书必须包含下表 7 中所示的证书扩展。所有其他证书扩展均不得包括在内。

表 7　LDS2 强制性证书扩展

扩展名称	LDS2签名者		注释
	是否应存在	关键性	
AuthorityKeyIdentifier	**m**	**nc**	
keyIdentifier	m		
authorityCertIssuer	o		
authorityCertSerialNumber	o		
ExtKeyUsage	**m**	**c**	见注1

注 1：每个 LDS2 签名者证书类型的 EKU 扩展必须按如下所示的方式进行填写。请注意，一个 LDS2 签名者可以被授权对多个 LDS2 数据对象类型进行签名。在这种情况下，EKU 扩展将包含该签名者的所有相关对象标识符：

```
id-icao-mrtd-security-lds2 OBJECT IDENTIFIER ::= {id-icao-mrtd-security 9}
id-icao-lds2Signer OBJECT IDENTIFIER ::= {id-icao-mrtd-security-lds2 8}
```

- LDS2旅行印章签名者（LDS2-TS）证书：
  `id-icao-tsSigner OBJECT IDENTIFIER ::= { id-icao-lds2Signer 1}`
- LDS2签证签名者（LDS2-V）证书：
  `id-icao-vSigner OBJECT IDENTIFIER ::= { id-icao-lds2Signer 2}`
- LDS2生物特征签名者（LDS2-B）证书：
  `id-icao-bSigner OBJECT IDENTIFIER ::= { id-icao-lds2Signer 3}`

注 2：LDS2 签名者证书必须符合 Doc 9303 号文件第 10 部分中 EF.Certifates 设定的大小限制。

虽然这些证书中不包括证书撤销列表分发点扩展，但作为正常验证过程的一部分，必须检查每个证书的撤销状态。在校验证书撤销状态时所用到的证书撤销列表是由签发该证书的国家签名认证机构所签发的证书撤销列表。

7.1.3　条形码签名者证书概要

条形码签名者证书必须符合 LDS2 签名者证书概要。由于条形码签名者证书的作用与 LDS2 证书不同，因此二者的概要在某些方面存在差异。特别是，对于条形码签名者证书的主体甄别名和序列号，存在具体的要求（见 Doc 9303 号文件第 13 部分）。

主体域：

条形码签名者证书的主体域必须按照以下方式填写：

- commonName 必须存在。必须由可作为一个国家内条形码签名者唯一识别信息的两个大写字母组成，该两个字母必须为 printableString 格式，并且必须按照 Doc 9303 号文件第 13 部分的规定与条形码中签名者标识符的第 3 和第 4 个字母相匹配。

- countryName 必须由条形码签名者的两字国家代码（见 Doc 9303 号文件第 3 部分）组成，该代码必须为大写字母，printableString 格式，并且必须按照 Doc 9303 号文件第 13 部分的规定与条形码中签名者标识符的第 1 和第 2 个字母相匹配。

- 不得包含其他属性。

证书扩展：

条形码签名者证书必须包含下表 8 中所示的证书扩展。所有其他证书扩展均不得包括在内。

表 8　条形码签名者证书的允许扩展

扩展名称	LDS2签名者		注释
	是否应存在	关键性	
AuthorityKeyIdentifier	**m**	**nc**	
keyIdentifier	m		
authorityCertIssuer	o		
authorityCertSerialNumber	o		
DocumentType	**o**		此扩展表示允许条形码签名者生成的证件类型
ExtKeyUsage	**m**	**c**	见下面的注

注：每个条形码签名者证书类型的 EKU 扩展必须按如下所示的方式进行填写。

```
id-icao-mrtd-security-vds OBJECT IDENTIFIER ::= {id-icao-mrtd-security 11}
id-icao-vdsSigner OBJECT IDENTIFIER ::= {id-icao-mrtd-security-vds 1}
```

7.1.4　证书撤销列表概要

表 9 规定了证书撤销列表正文部分各个域的证书撤销列表概要要求。表 10 规定了关于证书撤销列表和证书撤销列表输入扩展的证书撤销列表概要要求。

表 9　证书撤销列表各个域的概要

证书列表组成部分	国家签名认证机构 证书撤销列表	注释
CertificateList	m	
tBSCertList	m	见表 10
signatureAlgorithm	m	这里插入的值取决于所选择的算法
signatureValue	m	这里插入的值取决于所选择的算法
tBSCertList		
Version	m	必须为 v2
Signature	m	这里插入的值必须和 CertificateList 序列的 signatureAlgorithm 组成部分的值相同
Issuer	m	如果存在 countryName 和 serialNumber，必须为 PrintableString 有 DirectoryString 句法的其他属性必须为 PrintableString 或 UTF8String countryName 必须为大写字母
thisUpdate	m	必须以 Z 结束 必须存在秒元素 2049 年及以前的时间必须为 UTCTime UTCTime 必须以 YYMMDDHHMMSSZ 表示 2050 年及以后的时间必须为 GeneralizedTime GeneralizedTime 不得有小数秒 GeneralizedTime 必须以 YYYYMMDDHHMMSSZ 表示
nextUpdate	m	必须以 Z 结尾 必须存在秒元素 2049 年及以前的时间必须为 UTCTime UTCTime 必须以 YYMMDDHHMMSSZ 表示 2050 年及以后的时间必须为 GeneralizedTime GeneralizedTime 不得有小数秒 GeneralizedTime 必须以 YYYYMMDDHHMMSSZ 表示
revokedCertificates	c	如果有被撤销的证书，则应存在。如果没有被撤销的证书，则不应存在。如果存在，不得为空白

证书列表组成部分	国家签名认证机构 证书撤销列表	注释
crlExtensions	m	见关于应该存在哪些扩展的表 10 扩展的缺省值不得编码

表 10　证书撤销列表和证书撤销列表输入扩展概要

扩展名称	国家签名认证 机构证书撤销列表	关键性	注释
证书撤销列表扩展			
authorityKeyIdentifier	**m**	**nc**	该项必须与证书撤销列表签发者证书的 subjectKeyIdentifier 域中的值相同
keyIdentifier	**m**		
authorityCertIssuer	**o**		
authorityCertSerialNumber	**o**		
issuerAlternativeName	**o**	**nc**	见注 1
cRLNumber	**m**	**nc**	必须为非负整数且最大为 20 个八位位组 必须使用二进制补码且以最少的八位位组表示
deltaCRLIndicator	**x**		
issuingDistributionPoint	**x**		
freshestCRL	**x**		
CRL Entry Extensions			
reasonCode	**x**		
holdInstructionCode	**x**		
invalidityDate	**x**		
certificateIssuer	**x**		
other private extensions	**o**	**nc**	

注 1：如果一国家签名认证机构经历了更名，这一扩展可以包括进国家签名认证机构更名后签发的证书撤销列表中。如果存在这一扩展，其中的值必须与该国家签名认证机构在之前的名称下签发的证书的 issuer 域相同。一旦在国家签名认证机构之前的名称下签发的所有证书均已过期，可将该国家签名认证机构的名称从后续的证书撤销列表中剔除。不要求查验系统处理这一扩展。鉴于国际民航组织的 Doc 9303 号文件规定每个国家只能有一个国家签名认证机构，签发者域的 countryName 这一组成部分足以作为该国家签名认证机构的唯一识别信息。用该国家签名认证机构的最新公钥校验证书撤销列表上的签名。由于一个国家签名认证机构签发一份单一的证书撤销列表，因此该证书撤销列表涵盖使用该 countryName 签发的所有证书。除了这种强制检查之外，还可以进行选择性检查，检查证书的 issuer 域与证书撤销列表的 issuer 域或证书撤销列表中 issuerAltName 这一扩展的其中一个值是否相同。

注 2：证书撤销列表可能会包含其他撤销信息，例如，关于系统运营人或登记机构证书的信息。

7.2 授权公钥基础设施

授权公钥基础设施包括用于单一联络点的 X.509 证书和用于国家校验认证机构、证件校验者和终端的卡可校验证书。本节规定了单一联络点证书、国家校验认证机构证书、证件校验者证书和查验系统证书的概要。本节对包含在卡可校验证书中的数据对象进行了概述，并且还对这些对象的编码进行了说明。

7.2.1 单一联络点证书概要

可使用单独的认证机构来直接颁发单一联络点证书，但对认证机构自签名证书概要有以下限制：

- 认证机构证书必须符合[RFC 5280]；
- SHA-224、SHA-256、SHA-384 和 SHA-512 是唯一允许的散列算法；和
- countryName 必须出现在主体域中。

LDS2 单一联络点证书（客户端和服务器）必须符合第 7.1 节中规定的通信证书概要，但有以下限制。

签发者域：
单一联络点证书由国家签名认证机构或专门用于签发单一联络点证书的单独的认证机构签发。

主体域：
对于 LDS2 单一联络点证书，主体域必须按照以下方式填写：

- countryName 必须存在。该值包含一个国家代码，该代码必须遵守 Doc 9303 号文件第 3 部分中所规定的两字国家代码格式。
- commonName 必须存在。对于单一联络点 TLS 客户端证书，该值应该为“SPOC TLS client”。对于单一联络点 TLS 服务器证书，该值应该为“SPOC TLS server”。
- 签发国或签发机构还可自行决定纳入其他属性。

密钥用途扩展
对于单一联络点证书，值取决于所用的密码套件。

主体替代名称扩展

除了通信证书概要中所示的值之外，单一联络点 TLS 服务器证书还必须包含一个 dNSName 值，它是单一联络点 URL 的主机部分。

扩展密钥用途扩展

对于单一联络点客户端和服务器证书，必须包括下面列出的相关值。

- 单一联络点客户端证书：对象标识符是 2.23.136.1.1.10.1；
- 单一联络点服务器证书：对象标识符是 2.23.136.1.1.10.2。

证书撤销列表分发点扩展

单一联络点客户端和服务器证书中必须包含该扩展。

7.2.2　国家校验认证机构、证件校验者和终端证书概要

国家校验认证机构链接证书、证件校验者证书和终端证书由集成电路进行验证。由于这些芯片的计算限制，这些证书必须采用卡可校验格式（卡可校验证书）。

应使用表 11 中规定的证书格式和概要。有关编码值的详细信息，请参阅 Doc 9303 号文件第 11 部分。

表 11　卡可校验证书概要

数据对象	是否应 存在证书中
卡可校验证书	m
证书正文	m
证书概要标识符	m
认证机构编号	m
公钥	m
证书持有者编号	m
证书持有者授权模板	m
证书生效日期	m
证书到期日期	m
证书扩展	o
签名	m

7.2.2.1　证书概要标识符

概要的版本由证书概要标识符表示。应使用版本 1，该版本用值 0 进行标识。

7.2.2.2　认证机构编号和证书持有者编号

每个卡可校验证书必须包含两个公钥编号（证书持有者编号和认证机构编号）。

认证机构编号是对认证机构（国家校验认证机构或证件校验者）的（外部）公钥的指称，应使用该编号对证书的签名进行校验。

证书持有者编号是证书中提供的公钥的标识符，应使用该编号指称这一公钥。

注：因此，证书中包含的认证机构编号必须等同于签发证书的认证机构的相应证书中的证书持有者编号。

证书持有者编号应由以下串联元素组成：国家代码、持有者助记符和序列号。这些元素必须根据表 12 和以下规则进行选择：

a) 国家代码：

- 国家代码应为 Doc 9303 号文件第 3 部分中规定的证书持有者所在国两字代码。

b) 持有者助记符：

- 应指定持有者助记符作为唯一标识符，具体做法如下所示：
  - — 国家校验认证机构的持有者助记符应由该机构自己指定；
  - — 证件校验者的持有者助记符应由其所在国的国家校验认证机构指定；
  - — 查验系统的持有者助记符应由负责对其进行监督的证件校验者指定。

c) 序列号：

- 序列号应由证书持有者指定；
- 序列号必须是数字或字母数字；
  - — 数字序列号应由字符“0……9”组成。
  - — 字母数字序列号应由字符“0……9”和“A……Z”组成。
- 序列号必须以 Doc 9303 号文件第 3 部分中规定的认证机构所在国两字代码开头，其余三个字符应指定为字母数字序列号；和
- 如果所有可用的序列号都用完了，则可以重置序列号。

表 12 证书持有者编号

	编码	长度
国家代码	Doc 9303号文件第3部分	2F
持有者助记符	ISO/IEC 8859-1	9V
序列号	ISO/IEC 8859-1	5F

7.2.2.3　公钥

该域包含经认证的公钥。

国家校验认证机构自签名证书必须包含域参数。国家校验认证机构链接证书可能包含域参数，除非域参数已更改。在这种情况下，链接证书必须包含新的域参数。

证件校验者和终端证书不得包含域参数。证件校验者和终端公钥的域参数应继承自各自的国家校验认证机构公钥。

7.2.2.4　证书持有者授权模板

证书持有者的角色和授权应在证书持有者授权模板中进行编码。该模板是一个由以下数据对象组成的序列：

a)　指明终端类型和模板格式的对象标识符；和

b)　对相对授权进行编码的自主数据对象，相对授权即证书持有者相对于认证机构的角色和授权。

具体值在 Doc 9303 号文件第 10 部分中进行了规定。

7.2.2.5　证书生效日期和证书到期日期

这两个日期合起来表示证书的有效期。证书生效日期必须是证书生成的日期。证书到期日期是证书失效的日期。

7.2.2.6　证书扩展（授权扩展）

国家校验认证机构、证件校验者和终端证书中可包含授权扩展。这些扩展描述的是证书中的证书持有者授权模板所包含的授权之外的附加授权。

授权扩展是一个自主数据模板序列，其中每个自主数据模板都应包含由以下数据对象组成的一个序列，如表 13 所示：

a)　指明扩展内容和格式的对象标识符；和

b)　包含编码授权的上下文特定数据对象。

表 13　证书扩展

数据对象
证书扩展
自主数据模板
对象标识符
上下文特定数据对象
自主数据模板
对象标识符
上下文特定数据对象
……

注：Doc 9303 号文件第 11 部分中描述的证书验证程序未将证书扩展纳入考虑。因此，扩展是非关键的属性，集成电路不得因存在未知扩展而拒绝证书。

7.2.2.7 签名

证书上的签名应在编码的证书正文上创建（即包括标志和长度）。认证机构编号应可标识出将用于校验签名的公钥。

7.2.3 数据对象

表 14 概述了国家校验认证机构、证件校验者和终端证书中使用的数据对象的标志、长度和值。

表 14 数据对象概述（按标志排序）

名称	标志	长度	值	注释
对象标识符	0x06	V	对象标识符	–
认证机构编号	0x42	16V	字符串	标识证书中包含的由签发证书的认证机构提供的公钥。
自主数据	0x53	V	八位位组串	包含任意数据。
证书持有者编号	0x5F20	16V	字符串	用标识符表示证书中包含的公钥。
证书到期日期	0x5F24	6F	日期	证书失效的日期。
证书生效日期	0x5F25	6F	日期	证书生成的日期。
证书概要标识符	0x5F29	1F	无符号整数	证书版本和证书请求格式。
签名	0x5F37	V	八位位组串	由非对称密码算法产生的数字签名。
证书扩展	0x65	V	序列	嵌套证书扩展。
认证	0x67	V	序列	包含与认证相关的数据对象。
自主数据模板	0x73	V	序列	嵌套任意数据对象。

名称	标志	长度	值	注释
证件校验者证书	0x7F21	V	序列	嵌套证书正文和签名。
公钥	0x7F49	V	序列	嵌套公钥值和域参数。
证书持有者授权模板	0x7F4C	V	序列	对证书持有者的角色（即国家校验认证机构、证件校验者、终端）进行编码，并分配读取/写入访问权限。
证书正文	0x7F4E	V	序列	嵌套证书正文的数据对象。

F：固定长度（确切的八位位组数），V：可变长度（最大的八位位组数）。

7.2.3.1　值的编码

本规范中使用的基本值类型如下：（无符号）整数、椭圆曲线点、日期、字符串、八位位组串、对象标识符和序列。

7.2.3.1.1　无符号整数

本规范中使用的所有整数都是无符号整数。无符号整数应转换为以二进制整数表示并采取大端格式的八位位组串。应使用最少数量的八位位组，即如果前导八位位组的值为 0x00，则不得使用。

注：相反，ASN.1 类型的整数始终是有符号整数。

7.2.3.1.2　椭圆曲线点

椭圆曲线点到八位位组串的转换在 [TR-03111] 中进行了规定。应使用未压缩格式。

7.2.3.1.3　日期

日期以 YYMMDD 的格式以 6 位数编码，即“d1…d6”，并使用格林尼治标准时间时区。通过将每个数字 dj 编码为八位位组 oj，将其转换为八位位组串“o1…o6”，使其作为非压缩 BCD（$1 \leqslant j \leqslant 6$）。

年份 YY 以两位数编码，表示 20YY，即年份在 2000 到 2099 之间。

7.2.3.1.4　字符串

字符串“c1…cn”由 n 个字符 cj 串联而成，其中 $1 \leqslant j \leqslant n$ 。应将字符串转换为八位位组串“o1…on”，做法是使用 ISO/IEC 8859-1 字符集将每个字符 cj 转换为八位位组 oj。

字符代码 0x00-0x1F 和 0x7F-0x9F 未分配，因此不得使用。将八位位组转换为未分配的字符将导致错误。

7.2.3.1.5 八位位组串

八位位组串“o1...on”由 n 个八位位组 oj 串联而成，其中 1 ≤ j ≤ n 。每个八位位组 oj 由 8 个位组成。

7.2.3.1.6 对象标识符

对象标识符“i1.i2…in”编码为 n 个按顺序排列的无符号整数 ij ，其中 1 ≤ j ≤ n。应使用以下程序将其转换为八位位组串“o1...on-1”：

1) 将前两个整数 i1 和 i2 打包成一个整数 i，然后将其转换为八位位组串 o1。值 i 计算如下：

$$i=i1\cdot 40+i2$$

2) 剩余的整数 ij 直接转换为八位位组串 oj−1，其中 3 ≤ j ≤ n。
关于编码的更多详细信息见 [X.690]。

注：无符号整数使用 Doc 9303 号文件第 11 部分中所述的大端格式编码为八位位组串，但仅使用每个八位位组的第 1-7 位。设置为 1 的第 8 位（最左边的位）用于指示该八位位组不是八位位组串的最后一个八位位组。

7.2.3.1.7 序列

序列“D1…Dn”为 n 个按顺序排列的数据对象 Dj，其中 1 ≤ j ≤ n。应将序列转换为一组串联的八位位组串“O1…On”，做法是以唯一编码规则格式将每个数据对象 Dj 编码为八位位组串 Oj。

7.2.3.2 公钥数据对象的编码

一个公钥数据对象包含由一个对象标识符和几个上下文特定数据对象组成的一个序列：

- 对象标识符视具体应用而定，不仅指代公钥的格式（即上下文特定数据对象），还指代其用法。
- 上下文特定数据对象由对象标识符决定，包含公钥值和域参数。

本规范中使用的公钥数据对象的格式如下所述。

7.2.3.2.1 RSA 公钥

RSA 公钥中包含的数据对象如表 15 所示。数据对象的顺序是固定的。

表 15　RSA 公钥

数据对象	简写	标志	类型	卡可校验证书
对象标识符		0x06	对象标识符	m
复合模数	n	0x81	无符号整数	m
公钥指数	e	0x82	无符号整数	m

7.2.3.2.2　椭圆曲线公钥

椭圆曲线公钥中包含的数据对象如表 16 所示。数据对象的顺序是固定的，条件性域参数必须要么全部存在（除了辅因子），要么全部不存在，如下所示：

- 国家校验认证机构自签名证书应包含域参数；
- 国家校验认证机构链接证书可包含域参数；
- 证件校验者和终端证书不得包含域参数。证件校验者和终端公钥的域参数应继承自各自的国家校验认证机构公钥；和
- 证书请求必须始终包含域参数。

表 16　椭圆曲线公钥

数据对象	简写	标志	类型	卡可校验证书
对象标识符		0x06	对象标识符	m
素数模数	p	0x81	无符号整数	c
第一系数	a	0x82	无符号整数	c
第二系数	b	0x83	无符号整数	c
基点	G	0x84	椭圆曲线点	c
基点次序	r	0x85	无符号整数	c
公钥点	Y	0x86	椭圆曲线点	m
辅因子	f	0x87	无符号整数	c

8. 单一联络点协议

单一联络点（SPOC）是一个国家公开的用于在 LDS2 授权公钥基础设施方面与外国进行密钥管理操作的唯一接口。单一联络点协议是不同国家的国家校验认证机构和证件校验者之间开展操作的密钥管理协议。尽管单一联络点协议也可以用于国家校验认证机构与其国内证件校验者之间以及证件校验者与其管理的一组国内终端之间的国内通信，但并非必需这样做。可用其他密钥管理协议来开展国内的密钥管理工作。

单一联络点协议旨在用于交换密钥和证书，以便：

- 证件校验者可以向外国的国家校验认证机构发送认证请求；
- 国家校验认证机构可以将签发的证书发送给提出请求的证件校验者；
- 国家校验认证机构和证件校验者可以向外国的国家校验认证机构索取一套有效证书；和
- 证件校验者与国家校验认证机构可以在相互间交换一般消息。

在一个国家内：

- 国家校验认证机构应利用其国内的单一联络点接收由外国发来的认证请求，并将生成的证书或未能受理请求的通知发送给请求者；
- 证件校验者应利用其国内的单一联络点向外国的国家校验认证机构发送认证请求并接收生成的证书或未能受理请求的通知；
- 单一联络点必须收集来自国内的国家校验认证机构和证件校验者的请求和响应，并将它们转发给接收国的单一联络点；和
- 单一联络点必须收集来自其他国家的单一联络点的请求和响应，并将它们传送给国内相关的国家校验认证机构/证件校验者。

单一联络点 Web 服务通信应使用可以进行客户端和服务器 TLS 认证的 HTTPS。

注：单一联络点是授权公钥基础设施各实体之间的通信枢纽，因此应该全天候运行，并且外国的单一联络点应可以对其进行访问。

每个单一联络点分别向所有其他相关的单一联络点注册，并至少提供以下信息：

- 单一联络点所在国 — 单一联络点为其提供通信接口的国家；
- 单一联络点 URL — 对单一联络点接口和服务位置进行描述的 WSDL 的 URL；和
- 单一联络点认证机构证书 — 用于校验单一联络点通信证书的证书。

8.1　单一联络点相关结构

本节针对单一联络点报文定义了以下结构。

8.1.1　证书请求结构

证书请求是简化的卡可校验证书，可以包含一个额外的签名。应使用表 17 中规定的证书请求概要。

表 17　卡可校验证书请求概要

数据对象	是否应存在证书中
认证	c
卡可校验证书	m
证书正文	m
证书概要标识符	m
认证机构编号	r
公钥	m
证书持有者编号	m
签名	m
认证机构编号	c
签名	c

8.1.1.1　证书概要标识符

版本为 1，由值 0 进行标识。

8.1.1.2　认证机构编号

应使用认证机构编号通知认证机构有关申请人期望用于签署证书的私钥。如果请求中包含的认证机构编号与签发的证书中包含的认证机构编号不同（即所签发的证书不是用申请人所期望的私钥签名的），则还应该在响应中将认证机构的相应证书提供给申请人。

8.1.1.3　公钥

证书请求必须始终包含域参数。

8.1.1.4　证书持有者编号

证书持有者编号用于识别请求及生成的证书中所包含的公钥。

8.1.1.5 签名

一个证书请求最多可以有两个签名，一个内层签名和一个外层签名：

内层签名（必需的）

证书正文是自签名的，即内层签名应可以使用证书请求中包含的公钥进行验证。签名应在编码的证书正文上创建（即包括标志和长度）。

外层签名（条件性）

- 如果实体申请的是初始证书，则该签名是选择性的。在这种情况下，可以由接收请求的认证机构信任的另一个实体另外对请求进行签名（例如，国家校验认证机构可以对证件校验者发送至外国的国家校验认证机构的请求进行认证）。
- 如果实体申请的是后续证书，则该签名是必需的。在这种情况下，必须由申请人使用先前在接收请求的认证机构注册的最新密钥对另外对请求进行签名。

如果使用外层签名，则应使用认证数据对象来嵌套卡可校验证书（请求）、认证机构编号和附加签名。认证机构编号应可标识出将用于校验附加签名的公钥。签名应在并置的经编码的卡可校验证书和经编码的认证机构编号（即都包括标志和长度）上创建。

8.2 单一联络点协议报文

本节详细介绍了单一联络点协议中所使用的报文。

8.2.1 请求证书报文

使用目的：

单一联络点使用 RequestCertificate 报文向外国的国家校验认证机构请求为其某个证件校验者生成新证书。

输入参数：

callerID：（强制性）
此参数包含报文发起国的标识符。该值应为 Doc 9303 号文件第 3 部分中规定的两字国家代码。接收报文的单一联络点应根据发起报文的单一联络点在其注册期间所记录下的值对 callerID 的值进行校验。

messageID：（强制性）
此参数包含报文的标识符。它必须可从发起方的所有报文中唯一地标识出该报文。如果将针对该报文向发起方发送响应报文，则该响应报文将包含相同的 messageID。由此可以将传入的响应报文分配到正确的原始报文。messageID 的创建和分配可以由发起方决定，接收方不对其进行校验。

certReq：（强制性）
此参数包含实际的证书请求。它必须按照第 8.1.1 节的规定创建。编码必须遵循第 7.2.3.1 节中的规范。

输出参数：

CertificateSeq：（条件性）

如果接收方已成功同步处理该报文，则此参数将包含该报文经处理后的结果（一个或多个证书）。如果必须将证书与响应一起发送，则此参数是必需的。如果没有证书随响应报文一起发送，则该参数不得存在。

返回代码：

- ok_cert_available：报文已成功同步处理。输出参数 certificateSeq 包含一个或多个证书。
- ok_reception_ack：确认收到报文。尚未对该报文进行进一步校验。将以异步方式处理该报文。处理结果将使用 SendCertificates 这一报文发送到注册的 URL。
- failure_inner_signature：实际证书请求的内层签名校验失败。
- failure_outer_signature：实际证书请求的外层签名校验失败。
- failure_syntax：报文的语法不正确。
- failure_request_not_accepted：报文已正确处理，但请求未被接受。
- failure_request_syntax：证书请求不正确（例如语法或文件格式不正确）。
- failure_expired：将用于校验请求外层签名的证书已过期。
- failure_domain_parameters：请求中包含的域参数与拟用于签署证件校验者所请求的证书的国家校验认证机构证书的域参数不匹配。
- failure_internal_error：上述以外的错误。

备注：

证书请求的正文应包含认证机构编号（CAR），以通知国家校验认证机构请求者期望使用哪个私钥来签署证书。如果请求中包含的认证机构编号与签发的证书中包含的认证机构编号不同，则还应在响应中提供国家校验认证机构的相应证书。在这种情况下，如果报文是同步处理的，该国家校验认证机构证书应作为 certificateSeq 输出参数的一部分。证件校验者证书应为序列中的第一个证书。序列中的国家校验认证机构证书（根证书和/或链接证书）应按生效日期（升序）排序。

8.2.2　发送证书报文

使用目的：

单一联络点使用 SendCertificates 报文将新证书或证书链发送到发出请求的单一联络点。应针对以下情况生成此种报文：

- RequestCertificate：在签发完证书，即成功完成对请求的异步处理之后；
- GetCACertificates

此外，在创建新证书（国家校验认证机构根证书和链接证书）以将证书推送到已注册的外国单一联络点时，必须使用该报文。

输入参数：

callerID：（强制性）
此参数包含报文发起国的标识符。该值应为 Doc 9303 号文件第 3 部分中规定的两字国家代码。接收报文的单一联络点应根据发起报文的单一联络点在其注册期间所记录下的值对 callerID 的值进行校验。

messageID：（条件性）
如果此报文是为响应某个请求报文而生成的，则该参数所包含的值必须与请求报文中的 messageID 参数相同。如果此报文的生成是在没有外部干预的情况下触发的（国家核验认证机构证书的密钥更新），则 statusInfo 的值应为 new_cert_available_notification，并且 messageID 这一参数可以省略，如果存在，则忽略该参数。

statusInfo：（强制性）
此参数包含关于相应报文处理结果的状态代码。可以有以下几种状态：

- new_cert_available_notification：发起报文的单一联络点主动通知有新的国家校验认证机构证书可用。
- ok_cert_available：请求已成功处理。输入参数 certificateSeq 包含一个或多个证书。
- failure_inner_signature：实际证书请求的内层签名校验失败。
- failure_outer_signature：实际证书请求的外层签名校验失败。
- failure_syntax：相应报文的语法不正确。
- failure_request_not_accepted：相应报文已正确处理，但请求未被接受。
- failure_certificate：发送的一个或多个证书不正确（语法或签名）。
- failure_internal_error：上述 certificateSeq （条件性）之外的错误。

如果必须将证书与报文一起发送，则此参数是必需的。如果没有证书随报文一起发送，则该参数不得存在。证书应按照第 7.2.3 节中的规定以二进制 TLV DER 的格式进行编码。

如果此报文是为响应 GetCACertificates 报文而生成的，或者是因为有新的证书而生成的，则该序列应包含一系列认证机构证书。该系列证书应按顺序排列。在该序列中，国家校验认证机构证书（链接证书和/或根证书）应按生效日期排序。如果序列中有些证书的域参数不同，则针对每个域参数变体，至少应有一个含有相关变体域参数的证书。所有现行的认证机构证书都应包括在内。

如果此报文是为响应 RequestCertificate 报文而生成的，则序列的内容与针对 RequestCertificate 同步响应所述的相同。

输出参数：

无

返回代码：

- ok_received_correctly：报文已正确接收。
- failure_syntax：报文的语法不正确。
- failure_messageID_unknown：包含的 messageID 与之前发送的报文不匹配。
- failure_internal_error：上述以外的错误。

8.2.3　获取认证机构证书报文

使用目的：

单一联络点向外国的单一联络点发送此报文，以便获取该国家的所有有效的国家校验认证机构证书（链接证书和自签名证书）。

输入参数：

callerID：（强制性）
此参数包含报文发起国的标识符。该值应为 Doc 9303 号文件第 3 部分中规定的两字国家代码。接收报文的单一联络点应根据发起报文的单一联络点在其注册期间所记录下的值对 callerID 的值进行校验。

messageID：（强制性）
此参数包含报文的标识符。它必须可从发起方的所有报文中唯一地标识出该报文。如果将针对该报文向发起方发送响应报文，则该响应报文将包含相同的 messageID。由此可以将传入的响应报文分配到正确的原始报文。messageID 的创建和分配可以由发起方决定。

输出参数：

CertificateSeq：（条件性）
如果接收方已成功同步处理该报文，则此参数将包含该报文经处理后的结果（一个或多个证书）。如果必须将证书与响应一起发送，则此参数是必需的。如果没有证书随响应报文一起发送，则该参数不得存在。

返回代码：

- ok_cert_available：报文已成功同步处理。输出参数 certificateSeq 包含一个或多个认证机构证书。
- ok_reception_ack：确认收到报文。尚未对该报文进行进一步校验。将以异步方式处理该报文。处理结果将使用 SendCertificates 这一报文发送到注册的 URL。

- failure_syntax：报文的语法不正确。
- failure_internal_error：上述以外的错误。

备注：

如果报文已成功处理并被接受，国家校验认证机构必须在响应中将所有有效的国家校验认证机构证书发送出去，可将这些证书包含在输出参数 certificateSeq（同步处理）中，或是将其包含在相应的响应报文 SendCertificates（异步处理）中。

8.2.4 一般性的报文

使用目的：

单一联络点向外国的单一联络点发送此报文，以便发送通知或其他人类可读的一般文本报文。

输入参数：

callerID：（强制性）
此参数包含报文发起国的标识符。该值应为 Doc 9303 号文件第 3 部分中规定的两字国家代码。接收报文的单一联络点应根据发起报文的单一联络点在其注册期间所记录下的值，包括根据报文安全特征（每个国家都注册有数字签名证书/TLS 客户端证书），对 callerID 的值进行校验。

messageID：（强制性）
此参数包含报文的标识符。它必须可从发起方的所有报文中唯一地标识出该报文。如果将针对该报文向发起方发送响应报文，则该响应报文将包含相同的 messageID。由此可以将传入的响应报文分配到正确的原始报文。messageID 的创建和分配可以由发起方决定。

主题：（强制性）
此参数包含报文的主题。主题应简要描述报文正文的内容。主题部分必须使用英语。

正文：（强制性）
此参数包含报文的正文。正文应是人类可读的纯文本，不用于直接自动处理。正文部分必须使用英语。

返回代码：

- ok：报文已被接受，将被发送。
- failure_syntax：报文的语法不正确。
- failure_internal_error：上述以外的错误。

8.3　Web 服务

Web 服务接口是单一联络点间例行网络数据交换的接口。该接口应使用[SOAP] over [HTTPS]协议。单一联络点 Web 服务接口应符合第 8.3.3 节中规定的 WSDL。

8.3.1　SOAP 的使用

应使用纯粹的[SOAP] over [HTTPS]来实施 Web 服务接口。不得使用任何其他 SOAP 扩展（例如：WS-Addressing、WS-Security、WS-Secure Conversation、WS-Authorization、WS-Federation、WSAuthorization、WS-Policy、WS-Trust、WS-Privacy、WS-Test 和 WS 的其他扩展）。

不得使用 SOAP 中间节点类型。只应使用客户端单一联络点直连服务器单一联络点这一模式。

SOAP 故障元素应仅在发生未在本规范涵盖范围之内的传输层处理错误时使用。应用层错误应作为正常的 SOAP 响应使用针对每种报文所述的错误机制进行传递。

建议根据 [WS-IBP] 和 [WSI-SSBP] 实施 Web 服务接口。

单一联络点 SOAP 接口必须符合第 8.3.3 节中所述的 WSDL 定义。

8.3.2　安全考虑因素

单一联络点 Web 服务通信应使用安全且经过认证的通道。应使用 SOAP over HTTPS。应使用 TLS v1.2。

TLS 客户端应开展以下校验工作：

- 应根据 [RFC5280] 对服务器证书进行全面验证，包括撤销状态；
- 服务器证书 ExtKeyUsage 扩展必须存在，并且应包含第 7.2.1 节中针对单一联络点 TLS 服务器证书规定的对象标识符；和
- 服务器证书主体国家应等于 callerID 参数的值。如果出现任何故障，TLS 客户端必须关闭连接。

TLS 服务器应开展以下校验工作：

- 应使用证书对客户端进行全面认证；
- 应根据 [RFC5280] 对客户端证书进行全面验证，包括撤销状态；
- 客户端证书 ExtKeyUsage 扩展必须存在，并且应包含第 7.2.1 节中针对单一联络点 TLS 服务器证书规定的对象标识符；和
- 客户端证书主体国家应与预期的国家一致。

如果其中某些项目校验失败，应使用 HTTP 401 未授权响应代码拒绝请求。

对于 TLS 握手协商，客户端应支持第 4.2.2 节中规定的所有 TLS 密码套件。服务器和客户端均应支持基于 RSA 和 ECDSA 的认证。允许服务器向客户端请求，也允许客户端发送与服务器证书不同类型的客户端证书。

在 TLS 握手中使用 ECDHE_ECDSA 密钥协议是按照 [TLSECC]、[TLS1.2] 和 [TLSEXT] 中定义的添加做法来进行的。就 TLS 握手而言，客户端和服务器都应支持 [TLSECC] 规范中规定的适当的椭圆曲线扩展。[TLSECC] 第 5 节对受支持的椭圆曲线和椭圆曲线点格式作了定义。对于第 4.2.2 节中规定的使用高级加密标准（AES）进行加密的受支持 TLS 密码套件，使用这些套件应按照 [TLSAES] 规范来进行。

8.3.3 用于单一联络点 Web 服务接口的 WSDL

单一联络点 SOAP 接口必须符合以下 WSDL 定义：

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/
  " xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:SPOC="http://namespaces.icao.int/lds2"
  targetNamespace="http://namespaces.
  icao.int/lds2">

  <wsdl:types>
    <xs:schema xmlns="http://namespaces.icao.int/lds2"
      targetNamespace="http://namespaces."
      elementFormDefault="qualified" attributeFormDefault="unqualified">
      <xs:element name="certificateSequence">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="certificate" type="xs:base64Binary" minOccurs="1"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
      </xs:element>
      <xs:element name="RequestCertificateRequest">
    <xs:complexType>
      <xs:sequence>
            <xs:element name="callerID" type="xs:string"/>
            <xs:element name="messageID" type="xs:string"/>
            <xs:element name="certificateRequest" type="xs:base64Binary"/>
      </xs:sequence>
    </xs:complexType>
      </xs:element>
      <xs:element name="RequestCertificateResponse">
    <xs:complexType>
      <xs:sequence>
            <xs:element ref="certificateSequence" minOccurs="0" maxOccurs="1"/>
            <xs:element name="result">
          <xs:simpleType>
```

```
            <xs:restriction base="xs:string">
              <xs:enumeration value="ok_cert_available"/>
              <xs:enumeration value="ok_reception_ack"/>
              <xs:enumeration value="failure_inner_signature"/>
              <xs:enumeration value="failure_outer_signature"/>
              <xs:enumeration value="failure_syntax"/>
              <xs:enumeration value="failure_request_not_accepted"/>
              <xs:enumeration value="failure_request_syntax"/>
              <xs:enumeration value="failure_expired"/>
              <xs:enumeration value="failure_domain_parameters"/>
              <xs:enumeration value="failure_internal_error"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
    </xs:element>
    <xs:element name="SendCertificatesRequest">
  <xs:complexType>
    <xs:sequence>
          <xs:element name="callerID" type="xs:string"/>
          <xs:element name="messageID" type="xs:string" minOccurs="0" maxOccurs="1"/>
          <xs:element ref="certificateSequence" minOccurs="0" maxOccurs="1"/>
          <xs:element name="statusInfo">
        <xs:simpleType>
            <xs:restriction base="xs:string">
              <xs:enumeration value="new_cert_available_notification"/>
              <xs:enumeration value="ok_cert_available"/>
              <xs:enumeration value="failure_inner_signature"/>
              <xs:enumeration value="failure_outer_signature"/>
              <xs:enumeration value="failure_syntax"/>
              <xs:enumeration value="failure_request_not_accepted"/>
              <xs:enumeration value="failure_certificate"/>
              <xs:enumeration value="failure_internal_error"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
    </xs:element>
    <xs:element name="SendCertificatesResponse">
  <xs:complexType>
        <xs:sequence>
          <xs:element name="result">
        <xs:simpleType>
            <xs:restriction base="xs:string">
              <xs:enumeration value="ok_received_correctly"/>
              <xs:enumeration value="failure_syntax"/>
              <xs:enumeration value="failure_messageID_unknown"/>
              <xs:enumeration value="failure_internal_error"/>
          </xs:restriction>
        </xs:simpleType>
```

```
    </xs:element>
  </xs:sequence>
</xs:complexType>
  </xs:element>
  <xs:element name="GetCACertificatesRequest">
<xs:complexType>
  <xs:sequence>
        <xs:element name="callerID" type="xs:string"/>
        <xs:element name="messageID" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
  </xs:element>
  <xs:element name="GetCACertificatesResponse">
<xs:complexType>
  <xs:sequence>
        <xs:element ref="certificateSequence" minOccurs="0" maxOccurs="1"/>
        <xs:element name="result">
      <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="ok_cert_available"/>
            <xs:enumeration value="ok_reception_ack"/>
            <xs:enumeration value="failure_syntax"/>
            <xs:enumeration value="failure_internal_error"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
  </xs:element>
  <xs:element name="GeneralMessageRequest">
<xs:complexType>
  <xs:sequence>
        <xs:element name="callerID" type="xs:string"/>
        <xs:element name="messageID" type="xs:string"/>
        <xs:element name="subject" type="xs:string"/>
        <xs:element name="body" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
  </xs:element>
  <xs:element name="GeneralMessageResponse">
<xs:complexType>
  <xs:sequence>
        <xs:element name="result">
      <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="ok"/>
            <xs:enumeration value="failure_syntax"/>
            <xs:enumeration value="failure_internal_error"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
  </xs:sequence>
```

```
  </xs:complexType>
</xs:element>
  </xs:schema>
</wsdl:types>

<wsdl:message name="RequestCertificateRequest">
  <wsdl:part name="RequestCertificateRequest" element="SPOC:RequestCertificateRequest"/>
</wsdl:message>
<wsdl:message name="RequestCertificateResponse">
  <wsdl:part name="RequestCertificateResponse" element="SPOC:RequestCertificateResponse"/>
</wsdl:message>

<wsdl:message name="SendCertificatesRequest">
  <wsdl:part name="SendCertificatesRequest" element="SPOC:SendCertificatesRequest"/>
</wsdl:message>
<wsdl:message name="SendCertificatesResponse">
  <wsdl:part name="SendCertificatesResponse" element="SPOC:SendCertificatesResponse"/>
</wsdl:message>

<wsdl:message name="GetCACertificatesRequest">
  <wsdl:part name="GetCACertificatesRequest" element="SPOC:GetCACertificatesRequest"/>
</wsdl:message>
<wsdl:message name="GetCACertificatesResponse">
  <wsdl:part name="GetCACertificatesResponse" element="SPOC:GetCACertificatesResponse"/>
</wsdl:message>

<wsdl:message name="GeneralMessageRequest">
  <wsdl:part name="GeneralMessageRequest" element="SPOC:GeneralMessageRequest"/>
</wsdl:message>
<wsdl:message name="GeneralMessageResponse">
  <wsdl:part name="GeneralMessageResponse" element="SPOC:GeneralMessageResponse"/>
</wsdl:message>

<wsdl:portType name="SPOCPortType">
  <wsdl:operation name="RequestCertificate">
    <wsdl:input message="SPOC:RequestCertificateRequest"/>
    <wsdl:output message="SPOC:RequestCertificateResponse"/>
  </wsdl:operation>
  <wsdl:operation name="SendCertificates">
    <wsdl:input message="SPOC:SendCertificatesRequest"/>
    <wsdl:output message="SPOC:SendCertificatesResponse"/>
  </wsdl:operation>
  <wsdl:operation name="GetCACertificates">
    <wsdl:input message="SPOC:GetCACertificatesRequest"/>
    <wsdl:output message="SPOC:GetCACertificatesResponse"/>
  </wsdl:operation>
  <wsdl:operation name="GeneralMessage">
    <wsdl:input message="SPOC:GeneralMessageRequest"/>
    <wsdl:output message="SPOC:GeneralMessageResponse"/>
  </wsdl:operation>
</wsdl:portType>
```

```
  <wsdl:binding name="SPOCSOAPBinding" type="SPOC:SPOCPortType">
    <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="RequestCertificate">
      <soap:operation soapAction="RequestCertificate"/>
  <wsdl:input>
        <soap:body parts="RequestCertificateRequest" use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap:body parts="RequestCertificateResponse" use="literal"/>
      </wsdl:output>
</wsdl:operation>
    <wsdl:operation name="SendCertificates">
      <soap:operation soapAction="SendCertificates"/>
      <wsdl:input>
        <soap:body parts="SendCertificatesRequest" use="literal"/>
  </wsdl:input>
      <wsdl:output>
        <soap:body parts="SendCertificatesResponse" use="literal"/>
      </wsdl:output>
</wsdl:operation>
    <wsdl:operation name="GetCACertificates">
      <soap:operation soapAction="GetCACertificates"/>
      <wsdl:input>
        <soap:body parts="GetCACertificatesRequest" use="literal"/>
  </wsdl:input>
      <wsdl:output>
        <soap:body parts="GetCACertificatesResponse" use="literal"/>
      </wsdl:output>
</wsdl:operation>
    <wsdl:operation name="GeneralMessage">
      <soap:operation soapAction="GeneralMessage"/>
      <wsdl:input>
        <soap:body parts="GeneralMessageRequest" use="literal"/>
  </wsdl:input>
      <wsdl:output>
        <soap:body parts="GeneralMessageResponse" use="literal"/>
      </wsdl:output>
</wsdl:operation>
  </wsdl:binding>

  <wsdl:service name="SPOC">
    <wsdl:port name="SPOCPort" binding="SPOC:SPOCSOAPBinding">
      <soap:address location="http://spoc-server/SPOC"/>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

9. 国家签名认证机构国家证书列表结构

如 [RFC 5652] 中所规定的那样，国家证书列表是作为 ContentInfo 类型的示例来加以实施的。ContentInfo 必须包含如下所述的 SignedData 类型的单一示例。该 ContentInfo 中不包含其他数据类型。所有国家证书列表必须按唯一编码规则格式进行制作，以便保留其所含签名的完整性。

9.1 SignedData 类型

[RFC 5652]中的处理规则适用。

国家证书列表结构的规范使用下列术语表示每个域的存在要求。

m　　强制性 — 该域必须存在；
r　　建议的 — 该域应该存在；
x　　不使用 — 该域不得存在；
o　　选择性 — 该域可以存在。

表 18　国家证书列表

值		注释
SignedData		
Version	m	值= v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-cscaMasterList
eContent	m	一份 cscaMasterList 的编码内容
Certificates	m	必须包含国家证书列表签名者证书，且应该包含可用于校验 signerInfos 域中签名的国家签名认证机构证书。
Crls	x	
signerInfos	m	建议各国在该域中只提供 1 个 signerinfo。

值		注释
SignerInfo	m	
Version	m	该域的值由 sid 域决定。见[RFC 5652]中关于该域的规则。
Sid	m	
subjectKeyIdentifier	r	建议支持该域，而非 issuerandSerialNumber。
digestAlgorithm	m	用于得出 encapsulatedContent 和 SignedAttrs 哈希值的算法的算法标识符。 见下面的注。
signedAttrs	m	可能包含额外的属性。但是接收国不必处理这些属性，除了为校验签名值之外。 signedAttrs 必须包括签名时间（见[PKCS #9]）。
signatureAlgorithm	m	用于得出签名值的算法的算法标识符，及任何相关参数。 见下面的注。
signature	m	签名生成过程的结果。
unsignedAttrs	o	尽管可能包含该域，但是接收国可选择将它忽略。

注：DigestAlgorithmIdentifiers 必须省略“零”参数，而对于 SignatureAlgorithmIdentifier（如 RFC 3447 所规定），如果没有参数，则必须包括“零”作为参数，即使在按照 RFC 5754 使用 SHA2 算法时也是如此。具体实施时，必须接受两种条件（参数缺失或有“零”参数）下的 DigestAlgorithmIdentifiers。

9.2 ASN.1 国家证书列表规范

```
CscaMasterList
{ joint-iso-itu-t(2) international-organization(23) icao(136) mrtd(1)
security(1) masterlist(2)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

 -- Imports from RFC 5280 [PROFILE], Appendix A.1
     Certificate
       FROM PKIX1Explicit88
```

```
          { iso(1) identified-organization(3) dod(6)
            internet(1) security(5) mechanisms(5) pkix(7)
              mod(0) pkix1-explicit(18) };
-- CSCA Master List

CscaMasterListVersion ::= INTEGER {v0(0)}

CscaMasterList ::= SEQUENCE {
  version            CscaMasterListVersion,
  certList           SET OF Certificate }

-- Object Identifiers

id-icao-cscaMasterList OBJECT IDENTIFIER ::=
                                     {id-icao-mrtd-security 2}
id-icao-cscaMasterListSigningKey OBJECT IDENTIFIER ::=
                                     {id-icao-mrtd-security 3}
END
```

10.　偏差列表结构

如 [RFC 3852] 中所规定的那样，偏差列表是作为 SignedData 类型加以实施的。所有偏差列表必须按唯一编码规则格式进行制作，以便保留其所含签名的完整性。

偏差的范围将由以下各项界定：

- 日期范围（包括签发日期和到期日期）；
- 签发者名称和序列号；
- 证件签名者证书的主体密钥标识符；
- 电子机读旅行证件编号列表。

将通过这些值的适当组合来准确限定受影响的机读旅行证件的范围。在对这些值进行组合时，所用的处理方式是用“AND”将其连接起来。不能用“OR”对这些值进行连接处理。

10.1　SignedData 类型

采用了[RFC 3852]中的处理规则：

m　强制性 — 该域必须存在；
r　建议的 — 该域应该存在；
x　不使用 — 该域不得填充；
o　选择性 — 该域可以存在。

表 19　偏差列表

值		注释
SignedData		
version	m	值 = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-DeviationList
eContent	m	DeviationList 的编码内容
certificates	m	各国必须纳入偏差列表签名者证书，且应该纳入可用于校验 signerInfos 域中签名的国家签名认证机构证书。
crls	x	
signerInfos	m	建议各国在该域中只提供 1 个 signerInfo。
SignerInfo	m	
version	m	该域的值由 sid 域决定。见 [RFC 3852] 第 5.3 节中关于该域的规则。
sid	m	
subjectKeyIdentifier	r	建议各国支持该域，而非 issuerandSerialNumber。
digestAlgorithm	m	用于得出 encapsulatedContent 和 SignedAttrs 哈希值的算法的算法标识符。
signedAttrs	m	制作国或可在签名中纳入额外的属性，但是接收国不必处理这些属性，除了为校验签名值之外。 signedAttrs 必须包括签名时间（见 PKCS #9）。
signatureAlgorithm	m	用于得出签名值的算法的算法标识符，及任何相关参数。
signature	m	签名生成过程的结果。
unsignedAttrs	x	

10.2　ASN.1 规范

```
DeviationList
{ joint-iso-itu-t (2) international-organization(23) icao(136) mrtd(1) security(1)
deviationlist(7)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

  -- 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)
                   mod(0) pkix1-explicit(18) }

  -- Imports from RFC 3852
       SubjectKeyIdentifier, Digest, IssuerAndSerialNumber
          FROM CryptographicMessageSyntax2004
                 { iso(1) member-body(2) us(840) rsadsi(113549)
                   pkcs(1) pkcs-9(9) smime(16) modules(0)
                   cms-2004(24) };

DeviationListVersion ::= INTEGER {v0(0)}

DeviationList ::= SEQUENCE {
 version      DeviationListVersion,
 digestAlgorithm AlgorithmIdentifier OPTIONAL,
 deviations   SET OF Deviation
}

Deviation ::= SEQUENCE{
 documents       DeviationDocuments,
 descriptions SET OF DeviationDescription
}

DeviationDescription ::= SEQUENCE{
 description     PrintableString OPTIONAL,
 deviationType   OBJECT IDENTIFIER,
 parameters   [0] ANY DEFINED BY deviationType OPTIONAL,
 nationalUse     [1] ANY OPTIONAL

 -- The nationalUse field is for internal State use, and is not governed
 -- by an ICAO specification.
}

DeviationDocuments ::= SEQUENCE {
 documentType    [0] PrintableString (SIZE(2)) OPTIONAL,
          -- per MRZ, e.g. 'P'
 dscIdentifier   DocumentSignerIdentifier OPTIONAL,
```

```
 issuingDate     [4] IssuancePeriod OPTIONAL,
 documentNumbers    [5] SET OF PrintableString OPTIONAL
}

DocumentSignerIdentifier ::= CHOICE{
 issuerAndSerialNumber [1] IssuerAndSerialNumber,
 subjectKeyIdentifier [2] SubjectKeyIdentifier,
 certificateDigest  [3] Digest   --  if  used,  digestAlgorithm  must  be  present  in
DeviationList
}

IssuancePeriod ::= SEQUENCE {
 firstIssued   GeneralizedTime,
 lastIssued   GeneralizedTime
}

-- CertField is used to define which part of a certificate is
  affected by a coding error. Parts of the Body are identified by
  the corresponding value of CertificateBodyField, extensions
  by the corresponding OID identifying the extension.

CertField ::= CHOICE {
 body  CertificateBodyField,
 extension OBJECT IDENTIFIER
}
CertificateBodyField ::= INTEGER {
 generic(0), version(1), serialNumber(2), signature(3), issuer(4),
 validity(5), subject(6), subjectPublicKeyInfo(7),
 issuerUniqueID(8), subjectUniqueID(9)
}

Datagroup ::= INTEGER
              {dg1(1), dg2(2), dg3(3), dg4(4), dg5(5), dg6(6),
               dg7(7), dg8(8), dg9(9), dg10(10), dg11(11),
               dg12(12), dg13(13), dg14(14), dg15(15), dg16(16),
               sod(20), com(21)}

MRZField ::= INTEGER
              {generic(0), documentCode(1), issuingState(2), personName(3),
               documentNumber(4), nationality(5), dateOfBirth(6),
               sex(7), dateOfExpiry(8), optionalData(9)}

-- Base 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-DeviationList OBJECT IDENTIFIER ::= {id-icao-mrtd-security 7}
id-icao-DeviationListSigningKey OBJECT IDENTIFIER ::= {id-icao-mrtd-security 8}

-- Deviation Object Identifiers and Parameter Definitions
```

```
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-DGHashWrong OBJECT IDENTIFIER ::= {id-Deviation-LDS 2}
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}

END
```

11. 参考材料（规范性）

FIPS 180-2	FIPS 180-2，联邦信息处理标准出版物（FIPS PUB）180-2，《安全哈希标准》，2002 年 8 月。
FIPS 186-4	FIPS 186-4，联邦信息处理标准出版物（FIPS PUB）186-4，《数字签名标准（DSS）》，2013 年 7 月（替换 2009 年 6 月的 FIPS PUB 186-3）。
ISO 3166-1	ISO/IEC 3166-1: 2006，国家及其地区名称代码 — 第 1 部分：国家代码。
ISO/IEC 15946	ISO/IEC 15946: 2002，信息技术 — 安全技术 — 基于椭圆曲线的加密技术。
RFC 3280	RFC 3280，R. Housley，W. Polk，W. Ford，D. Solo，因特网 X.509 公钥基础设施证书和证书撤销列表（CRL）概要，2002 年 4 月。
RFC 4055	RFC 4055，J. Schaad， B. Kaliski，R. Housley，在因特网 X.509 公钥基础设施证书和证书撤销列表（CRL）概要中使用的 RSA 加密额外算法和标识符，2005 年 6 月。
RFC 5652	RFC 5652，R. Housley，加密电文句法，2009 年 9 月。
RFC 5280	RFC 5280，D. Cooper，S. Santesson，S. Farrell，S. Boeyen，R. Housley，W. Polk，因特网 X.509 公钥基础设施证书和证书撤销列表（CRL）概要，2008 年 5 月。

TR 03111	BSI TR-03111：椭圆曲线加密技术 2.0 版本，2012 年。
X9.62	X9.62，用于金融服务业的公钥加密技术：椭圆曲线数字签名算法（ECDSA），1999 年 1 月 7 日。
X.509	ITU-T X.509 | ISO/IEC 9594-8，2008 年：信息技术 — 开放系统互联 — 目录：公钥和属性证书框架。
X.690	ITU-T X.690 2008：信息技术 — ASN.1 编码规则：基本编码规则（BER）、规范编码规则（CER）和唯一编码规则（DER）规范。
RFC-RSA	Jakob Jonsson 和 Burt Kaliski，RFC 3447，公钥密码学标准（PKCS）#1：RSA 密码学规范，2.1 版，2003 年。
PKCS#1	RSA Laboratories，RSA Laboratories 技术说明，PKCS#1 v2.2：RSA 加密标准，2012 年。
TLSAES	P. Chown，“用于传输层安全 （TLS）的高级加密标准（AES）密码套件”，RFC 3268，2002 年 6 月。
TLSECC	S. Blake-Wilson，N. Bolyard，V. Gupta，C. Hawk 和 B. Moeller，“用于传输层安全（TLS） 的椭圆曲线加密 （ECC）密码套件”，RFC 4492，2006 年 5 月。
TLS1.2	T. Dierks 和 E. Rescorla，“传输层安全（TLS）协议 1.2 版”，RFC 5246，2008 年 8 月。
TLSEXT	S. Blake-Wilson，M. Nystrom，D. Hopwood，J. Mikkelsen 和 T. Wright，“传输层安全（TLS）扩展”，RFC 4366，2006 年 4 月。
SOAP	SOAP 1.2 版第 1 部分：报文传送框架（第二版），W3C 建议，2007 年 4 月 27 日。
HTTPS	E. Rescorla，“HTTP Over TLS”，RFC 2818，2000 年 5 月。
WSI-BP	WS-I 基本概要，见 http://www.ws-i.org/Profiles/BasicProfile-1.1.html 。
WSI-SSBP	WS-I 基本绑定，见 http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html 。

— — — — — — — —

第 12 部分附录 A

有效期（资料性）

下列示例描述了第 4 部分所述的各种情景下私钥使用期限和公钥证书有效期的计算方法。

A.1　示例 1

第一个示例描述了电子机读旅行证件有效期为五年的情景。由于每天都签发大量的电子机读旅行证件，这一政策旨在将私钥使用期限和公钥证书有效期保持在最小值。在本示例中，证件签名者证书的最短私钥使用期限是 1 个月。

项目	使用/有效期
电子机读旅行证件有效性	5 年
证件签名者私钥使用期限	1 个月
证件签名者证书有效期	5 年+1 个月
国家签名认证机构私钥使用期限	3 年
国家签名认证机构证书有效期	8 年+1 个月

本示例的结果是当第一个国家签名认证机构证书失效时，将有至少 36 个已经签发的证件签名者证书（每个证书对应一个使用期限为一个月的私钥）。在第一个国家签名认证机构证书失效前的几个月，将有至少其他两个已经签发的国家签名认证机构证书（每个证书对应一个使用期限为三年的私钥）。

A.2　示例 2

第二个示例描述了电子机读旅行证件有效期为十年的情景。该政策旨在将私钥使用期限和公钥证书有效期保持在平均长度。

项目	使用/有效期
电子机读旅行证件有效期	10 年
证件签名者私钥使用期限	2 个月
证件签名者证书有效期	10 年+2 个月

项目	使用/有效期
国家签名认证机构私钥使用期限	4 年
国家签名认证机构证书有效期	14 年+2 个月

本示例的结果是当第一个国家签名认证机构证书失效时，将有至少 24 个已经签发的证件签名者证书（每个证书对应一个使用期限为两个月的私钥）。在第一个国家签名认证机构证书失效前的几个月，将有至少其他三个已经签发的国家签名认证机构证书（每个证书对应一个使用期限为四年的私钥）。

A.3 示例 3

最后一个示例描述了电子机读旅行证件有效期为十年的情景。该政策旨在使用最长的私钥使用期限和公钥证书有效期。

项目	使用/有效期
电子机读旅行证件有效期	10 年
证件签名者私钥使用期限	3 个月
证件签名者证书有效期	10 年+3 个月
国家签名认证机构私钥使用期限	5 年
国家签名认证机构证书有效期	15 年+3 个月

本示例的结果是当第一个国家签名认证机构证书失效时，将有至少 20 个已经签发的证件签名者证书（每个证书对应一个使用期限为三个月的私钥）。在第一个国家签名认证机构证书失效前的几个月，将有至少其他三个已经签发的国家签名认证机构证书（每个证书对应一个使用期限为五年的私钥）。

— — — — — — — —

第 12 部分附录 B

证书和证书撤销列表概要参考文本
（资料性）

第 7 节所规定的证书和证书撤销列表概要的依据是所参考的文件中规定的定义和基本概要要求。以下表格复制了这些源文件（截至编制本文件之时）一些相关部分的简短摘录。提供这些摘录是为了帮助读者理解电子机读旅行证件证书以及证书撤销列表概要中规定的一些要求的背景。这些摘录并非为了取代参考文件作为参考的依据。在任何情况下，要获取所提到的组成部分/扩展的完整规范以及获取最新规范，必须使用实际的参考文件。

表 B-1　证书的域和扩展

组成部分/扩展	参考	相关摘录
Certificate	RFC 5280 – 4.1.1	
TBSCertificate	RFC 5280 – 4.1.1.1	
signatureAlgorithm	RFC 5280 – 4.1.1.2	
signatureValue	RFC 5280 – 4.1.1.3	
TBSCertificate	RFC 5280 – 4.1.2	
version	RFC 5280 – 4.1.2.1	当按照本概要的预期使用扩展时，版本必须是 3（值为 2）。
serialNumber	RFC 5280 – 4.1.2.2	序列号必须是认证机构为各证书分配的一个正整数。该序列号对于给定认证机构签发的每个证书来说必须是唯一的（即，签发者名称和序列号能够确定证书的唯一性）。认证机构必须要求 serialNumber 为一个非负整数。 鉴于上文提到的唯一性要求，序列号可以包含长整数。证书使用者必须能够处理长达 20 个八位位组的 serialNumber 值。遵守相关规则的认证机构不得使用长度超过 20 个八位位组的 serialNumber 值。

组成部分/扩展	参考	相关摘录
	X.690 – 8.3.2	如果整数值编码的内容八位位组包括一个以上的八位位组，则第一个八位位组的所有位和第二个八位位组的第 8 位： a) 不应都为 1；和 b) 不应都为零。 注：这些规则确保了在对整数值进行编码时总是使用可能最少的八位位组。
	X.690 – 8.3.3	内容八位位组应为等于整数值的一个二进制补码数值，包括第一个八位位组的第 8 位至第 1 位，后面接着第二个八位位组的第 8 位至第 1 位，再后面依次接着各个八位位组的第 8 位至第 1 位，直至并包括内容八位位组的最后一个八位位组。
signature	RFC 5280 – 4.1.1.2	该域必须包括与序列 Certificate 内的 signatureAlgorithm 域相同的算法标识符。
issuer	RFC 5280 – 附录 A.1	X520countryName ::= PrintableString (SIZE (2)) X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))
	RFC 5280 – 4.1.2.4	遵守本概要的认证机构必须使用 DirectoryString 的 PrintableString 编码或者 UTF8String 编码。
	ISO 3166-1	
validity	RFC 5280 – 4.1.2.5	notBefore 和 notAfter 均可编码为 UTCTime 或者 GeneralizedTime。 遵守本概要的认证机构必须总是将直至 2049 年的证书有效期编码为 UTCTime。2050 年或者之后的证书有效期必须编码为 GeneralizedTime。
(if encoded as UTCTime)	X.690 – 11.8.1	按照 ITU-T X.680 | ISO/IEC 8824-1 关于 UTCTime 的条款所述，编码应以“Z”结尾。
	X.690 – 11.8.2	秒元素应始终存在。
(if encoded as GeneralizedTime)	X.690 – 11.7.1	按照 ITU-T Rec. X.680 | ISO/IEC 8824-1 关于 GeneralizedTime 的条款所述，编码应以“Z”结尾。
	X.690 – 11.7.2	秒元素应始终存在。

组成部分/扩展	参考	相关摘录
	RFC 5280 – 4.1.2.5.2	GeneralizedTime 的值不得包括小数秒。 对于本概要，GeneralizedTime 的值必须表述为格林尼治标准时间（Zulu），并且必须包括秒（即，时间是 YYYYMMDDHHMMSSZ），即使秒数为零。
subject	RFC 5280 – 附录 A.1	X520countryName ::= PrintableString (SIZE (2)) X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))
	RFC 5280 – 4.1.2.6	遵守本概要的认证机构必须使用 DirectoryString 的 PrintableString 编码或者 UTF8String 编码。
subjectPublicKeyInfo	RFC 5280 – 4.1.2.7	
issuerUniqueID	RFC 5280 – 4.1.2.8	遵守本概要的认证机构不得生成带有唯一标识符的证书。
subjectUniqueID	RFC 5280 – 4.1.2.8	遵守本概要的认证机构不得生成带有唯一标识符的证书。
extensions	X.690 – 11.5	在对 set 值或者 sequence 值进行编码时不应包括对等于其默认值的任何组成部分的值进行编码。
AuthorityKeyIdentifier	RFC 5280 – 4.2.1.1	由遵守相关规则的认证机构生成的所有证书都必须包括 authorityKeyIdentifier 扩展中的 keyIdentifier 域，以促进认证路径的构建。有一个例外情况。如果认证机构分发的是“自签名”证书形式的公钥，则可以省去机构密钥标识符。
keyIdentifier		
authorityCertIssuer		
authorityCertSerialNumber		

组成部分/扩展	参考	相关摘录
SubjectKeyIdentifier	RFC 5280 – 4.2.1.2	为促进认证路径的构建，该扩展必须出现在遵守相关规则的认证机构的所有证书上，即包括 cA 值为 TRUE 的基本限制扩展（第 4.2.1.9 节）在内的所有证书。
subjectKeyIdentifier		
KeyUsage	RFC 5280 – 4.2.1.3	当要限制可用于一次以上操作的密钥时，可采取使用管制。
digitalSignature		当通过数字签名机制使用主体公钥以支持证书签名（第 5 位）或者证书撤销列表签名（第 6 位）之外的安全服务时，digitalSignature 位将被确认。
nonRepudiation		
keyEncipherment		
dataEncipherment		
keyAgreement		
keyCertSign		当使用主体公钥来校验公钥证书的签名时，keyCertSign 位将被确认。
cRLSign		当使用主体公钥来校验证书撤销列表（例如证书撤销列表、增量证书撤销列表或机构撤销列表）上的签名时，cRLSign 位将被确认。该位必须在用于校验证书撤销列表上签名的证书内被确认。
encipherOnly		
decipherOnly		
PrivateKeyUsagePeriod	RFC 3280 – 4.2.1.4	遵守本概要的认证机构不得生成带有私钥使用期限扩展的证书，除非这两个组成部分中至少存在一个，并且扩展是非关键性的。
notBefore		notBefore 和 notAfter 在使用时表示为 GeneralizedTime，并且必须按照第 4.1.2.5.2 节中的规定进行说明和解读。
notAfter		

组成部分/扩展	参考	相关摘录
CertificatePolicies	RFC 5280 – 4.2.1.4	如果该扩展是关键性的，路径验证软件必须能够解读该扩展（包括可选限定符），或者必须拒绝该证书。
PolicyInformation		
policyIdentifier		
policyQualifiers		
PolicyMappings	RFC 5280 – 4.2.1.5	
SubjectAltName	RFC 5280 – 4.2.1.6	
IssuerAltName	RFC 5280 – 4.2.1.7	
SubjectDirectoryAttributes	RFC 5280 – 4.2.1.8	
Basic Constraints	RFC 5280 – 4.2.1.9	基本限制扩展可确定证书主体是否为认证机构以及确定包含该证书的有效认证路径的最大深度。遵守相关规则的认证机构必须将该扩展纳入包含用来验证证书数字签名的公钥的所有认证机构证书，并且必须在这些证书中将该扩展标记为关键性的。
cA		cA 布尔表明经认证的公钥是否属于认证机构。如果 cA 布尔未被确认，则密钥用途扩展中的 keyCertSign 位不得被确认。
PathLenConstraint		
NameConstraints	RFC 5280 – 4.2.1.10	
PolicyConstraints	RFC 5280 – 4.2.1.11	
ExtKeyUsage	RFC 5280 – 4.2.1.12	该扩展表明在密钥用途扩展所示的基本用途之外或作为这些用途的替代，经认证的公钥可用作的一个或多个用途。

组成部分/扩展	参考	相关摘录
CRLDistributionPoints	RFC 5280 – 4.2.1.13	
distributionPoint		
reasons		
cRLIssuer		
InhibitAnyPolicy	RFC 5280 – 4.2.1.14	
FreshestCRL	RFC 5280 – 4.2.1.15	
privateInternetExtensions	RFC 5280 – 4.2.2	
NameChange		
DocumentType		
Netscape Certificate Type		
other private extensions		

表 B-2　证书撤销列表的域和扩展

组成部分/扩展	参考	有关摘录
CertificateList	RFC 5280 – 5.1.1	
tBSCertList	RFC 5280 – 5.1.1.1	
signatureAlgorithm	RFC 5280 – 5.1.1.2	
signatureValue	RFC 5280 – 5.1.1.3	
	RFC 5280 – 5.1.2	
version	RFC 5280 – 5.1.2.1	该可选域描述了经编码的证书撤销列表的版本。当按照本概要的要求使用扩展时，该域必须存在，并且必须指定版本 2（整数值为 1）。
signature	RFC 5280 – 5.1.2.2	该域必须包括与序列 CertificateList 内的签名域相同的算法标识符。

组成部分/扩展	参考	有关摘录
issuer	RFC 5280 – Appendix A.1	X520countryName ::= PrintableString (SIZE (2)) X520SerialNumber ::= PrintableString (SIZE 1..ub-serial-number))
	RFC 5280 – 5.1.2.3 and 4.1.2.4	遵守本概要的认证机构必须使用 DirectoryString 的 PrintableString 编码或者 UTF8String 编码。
thisUpdate	RFC 5280 – 5.1.2.4	遵守本概要的证书撤销列表签发者必须将直至 2049 年的 thisUpdate 编码为 UTCTime。遵守本概要的证书撤销列表签发者必须将 2050 年或者之后的 thisUpdate 编码为 GeneralizedTime。
(if encoded as UTCTime)	X.690 – 11.8.1	按照 ITU-T X.680 | ISO/IEC 8824-1 关于 UTCTime 的条款所述，编码应以“Z”结尾。
	X.690 – 11.8.2	秒元素应始终存在。
(if encoded as GeneralizedTime)	X.690 – 11.7.1	按照 ITU-T X.680 | ISO/IEC 8824-1 关于 GeneralizedTime 的条款所述，编码应以“Z”结尾。
	X.690 – 11.7.2	秒元素应始终存在。
	RFC 5280 – 4.1.2.5.2	GeneralizedTime 的值不得包括小数秒。 对于本概要，GeneralizedTime 的值必须表述为格林尼治标准时间（Zulu），并且必须包括秒（即，时间是 YYYYMMDDHHMMSSZ），即使秒数为零。
nextUpdate	5.1.2.5	遵守本概要的证书撤销列表签发者必须将直至 2049 年的 nextUpdate 编码为 UTCTime。遵守本概要的证书撤销列表签发者必须将 2050 年或者之后的 nextUpdate 编码为 GeneralizedTime。
(if encoded at UTCTime)	X.690 – 11.8.1	按照 ITU-T X.680 | ISO/IEC 8824-1 关于 UTCTime 的条款所述，编码应以“Z”结尾。
	X.690 – 11.8.2	秒元素应始终存在。
(if encoded at GeneralizedTime)	X.690 – 11.7.1	按照 ITU-T X.680 | ISO/IEC 8824-1 关于 GeneralizedTime 的条款所述，编码应以“Z”结尾。
	X.690 – 11.7.2	秒元素应始终存在。

组成部分/扩展	参考	有关摘录
	RFC 5280 – 4.1.2.5.2	GeneralizedTime 的值不得包括小数秒。 对于本概要，GeneralizedTime 的值必须表述为格林尼治标准时间（Zulu），并且必须包括秒（即，时间是 YYYYMMDDHHMMSSZ），即使秒数为零。
revokedCertificates	RFC 5280 – 5.1.2.6	如果没有已撤销的证书，则不得有撤销证书列表。否则，要根据序列号列出已撤销的证书。
crlExtensions	RFC 5280 – 5.2	遵守相关规则的证书撤销列表签发者需要在签发的所有证书撤销列表内包含机构密钥标识符（第 5.2.1 节）以及证书撤销列表号码（第 5.2.3 节）扩展。
	X.690 – 11.5	在对 set 值或者 sequence 值进行编码时不应包括对等于其默认值的任何组成部分的值进行编码。
authorityKeyIdentifier	RFC 5280 – 5.2.1	遵守相关规则的证书撤销列表签发者必须使用密钥标识符方法，并且必须在签发的所有证书撤销列表内包含该扩展。
issuerAlternativeName	RFC 5280 – 5.2.2	
cRLNumber	RFC 5280 – 5.2.3	遵守本概要的证书撤销列表签发者必须在所有的证书撤销列表内包含该扩展，并且必须将该扩展标记为非关键性的。 CRLNumber ::= INTEGER (0..MAX) 鉴于上述要求，证书撤销列表号码可以包含长整数。证书撤销列表校验者必须能够处理长达 20 个八位位组的 CRLNumber 值。遵守相关规则的证书撤销列表签发者不得使用长度超过 20 个八位位组的 CRLNumber 值。
	X.690 – 8.3.2	如果整数值编码的内容八位位组包括一个以上的八位位组，则第一个八位位组的所有位和第二个八位位组的第 8 位： a) 不应都为 1；和 b) 不应都为零。 注：这些规则确保了在对整数值进行编码时总是使用可能最少的八位位组。

组成部分/扩展	参考	有关摘录
	X.690 – 8.3.3	内容八位位组应为等于整数值的一个二进制补码数值，包括第一个八位位组的第 8 位至第 1 位，后面接着第二个八位位组的第 8 位至第 1 位，再后面依次接着各个八位位组的第 8 位至第 1 位，直至并包括内容八位位组的最后一个八位位组。
deltaCRLIndicator	RFC 5280 – 5.2.4	
issuingDistribution Point	RFC 5280 – 5.2.5	
freshestCRL	RFC 5280 – 5.2.6	
reasonCode	RFC 5280 – 5.3.1	
holdInstructionCode	RFC 5280 – 5.3.2	
invalidityDate	RFC 5280 – 5.3.3	
certificateIssuer	RFC 5280 – 5.3.4	

— — — — — — — —

第 12 部分附录 C

较早的证书概要
（资料性）

本附录中的证书概要为国际民航组织 Doc 9303 号文件第六版中所规定的。尽管国家签名认证机构必须签发符合第 7 节所述最新概要的证书，但在此处提供了较早的概要，这些概要仅作参考之用，原因是按照较早概要签发的证件将在数年内保持流通，并由查验系统进行处理。

表 C-1　证书正文

证书组成部分	**RFC 3280** 中的章节	国家签名认证机构证书	证件签名者证书	注释
Certificate	4.1.1	m	m	
TBSCertificate	4.1.1.1	m	m	见表 C-2
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	应为 v3
serialNumber	4.1.2.2	m	m	
signature	4.1.2.3	m	m	这里插入的值应与 signatureAlgorithm 的对象标识符相匹配
issuer	4.1.2.4	m	m	
validity	4.1.2.5	m	m	实施时应指明 2049 年之前使用世界协调时间，2049 年之后使用 GeneralizedTime
subject	4.1.2.6	m	m	
subjectPublicKeyInfo	4.1.2.7	m	m	
issuerUniqueID	4.1.2.8	x	x	

证书组成部分	**RFC 3280** 中的章节	国家签名认证机构证书	证件签名者证书	注释
subjectUniqueID	4.1.2.8	x	x	
extensions	4.1.2.9	m	m	见关于应该存在哪些扩展的表 C-2

表 C-2 扩展

扩展名称	**RFC 3280** 中的段落	国家签名认证机构证书	证件签名者证书	注释
AuthorityKeyIdentifier	4.2.1.1	o	m	所有证书都必需具备，自签名的国家签名认证机构证书除外
SubjectKeyIdentifier	4.2.1.2	m	o	
KeyUsage	4.2.1.3	mc	mc	应将该扩展标记为关键性的
PrivateKeyUsagePeriod	4.2.1.4	o	o	这将是私钥的签发周期
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	应将该扩展标记为关键性的
NameConstraints	4.2.1.11	x	x	
PolicyConstraints	4.2.1.12	x	x	
ExtKeyUsage	4.2.1.13	x	x	

扩展名称	**RFC 3280** 中的段落	国家签名认证机构证书	证件签名者证书	注释
CRLDistributionPoints	4.2.1.14	o	o	如果签发国或签发机构选择使用该扩展，则应将国际民航组织公钥目录包含在内，作为一种分发点。在实施时还可出于本地目的，包含相关的证书撤销列表分发点；其他接收国可对其予以忽略。
InhibitAnyPolicy	4.2.1.15	x	x	
FreshestCRL	4.2.1.16	x	x	
privateInternetExtensions	4.2.2	x	x	
other private extensions	不适用	o	o	如果出于本国目的，包含任何专用扩展，则不应对其进行标记。不主张签发国或签发机构包含任何专用扩展。
AuthorityKeyIdentifier	4.2.1.1			
keyIdentifier		m	m	如果使用该扩展，应支持该域采取最小的值
authorityCertIssuer		o	o	
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	
keyCertSign		m	x	

扩展名称	**RFC 3280** 中的段落	国家签名认证机构证书	证件签名者证书	注释
cRLSign		m	x	
encipherOnly		x	x	
decipherOnly		x	x	
BasicConstraints	4.2.1.10			
cA		m	x	对于认证机构证书，该扩展为 TRUE
PathLenConstraint		m	x	对于新的国家签名认证机构证书，该扩展为 0；对于国家签名认证机构链接证书，该扩展为 1
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	

— — — — — — — —

第 12 部分附录 D

RFC 5280 验证的兼容性
（资料性）

本附录为想要使用采用 [RFC 5280] 认证路径和证书撤销列表验证算法的系统的接收国提供了指导。

电子机读旅行证件公钥基础设施信任模型是 [RFC 5280] 中所规定的验证程序所涵盖的模型的一个部分。第 D.1 节确定了 [RFC 5280] 所规定步骤中为电子机读旅行证件应用所必需的部分，并提供了认证路径验证、证书撤销列表验证和撤销检查所需要的输入值和初始化值以及过程。

第 D.2 节涵盖了 [RFC 52180] 中所规定的与电子机读旅行证件应用无关的其余步骤。提供了认证路径验证和证书撤销列表验证的输入值和初始化值。本节中的指导用于相关工具采用的是完整的 [RFC 5280] 算法而不仅仅是 D.1 中所述的子集的情况。

第 D.3 节为支持在国家签名认证机构改名之后将基于[RFC 5280]的证书撤销列表处理工作加以扩展以涵盖撤销检查提供了指导。

D.1 与电子机读旅行证件相关的步骤

此处规定的电子机读旅行证件认证路径验证程序是以 [RFC 5280] 中所述的程序为依据的。使用了相同的术语和过程说明。电子机读旅行证件证书概要将认证路径限制为一个单一的证书，并禁止使用其他应用中使用的很多可选特征，例如 [RFC 5280] 中规定的互联网公钥基础设施。电子机读旅行证件认证路径验证程序省去了与这些特征相关的路径验证步骤。

D.1.1 认证路径验证程序

D.1.1.1 输入

[RFC 5280] 规定了路径验证算法的一组（共九项）输入值。仅下列三项与电子机读旅行证件应用相关：

- 认证路径：一个单一的证书（例如，证件签名者证书）；
- 当前日期/时间；和
- 信任锚信息，包括：
    - 可信的签发者名称：如果信任锚采取的是国家签名认证机构证书的形式，则可信的签发者名称是该证书 subject 域的值；

- 可信的公钥算法：如果信任锚采取的是国家签名认证机构证书的形式，则可信的公钥算法取自该证书的 SubjectPublicKeyInfo 域；
- 可信的公钥：如果信任锚采取的是国家签名认证机构证书的形式，则可信的公钥取自该证书的 SubjectPublicKeyInfo 域；和
- 可信的公钥参数：这是一个选择性输入值，只有在可信的公钥算法需要参数时才将其包括在内。如果信任锚采取的是国家签名认证机构证书的形式，则这些参数取自该证书的 SubjectPublicKeyInfo 域。

如果在实施时需要提供另外六个输入值，D.2 提供了这方面的建议。

对于签发正在接受验证的证书的国家签名认证机构，可能存在多个信任锚。在这些信任锚中，必须使用所包含的公钥与正在接受验证的证书中的机构密钥标识符扩展值相匹配的那个信任锚。

D.1.1.2 初始化

[RFC 5280]中规定了 11 个国家变量。仅下列五个与电子机读旅行证件应用相关：

- 应用：max_path_length：初始化为“0”；
- working_issuer_name：初始化为可信的签发者名称的值；
- working_public_key_algorithm：初始化为可信的公钥算法的值；
- working_public_key：初始化为可信的公钥的值；和
- working_public_key_parameters：初始化为可信的公钥参数的值。

如果在实施时需要初始化另外六个变量，D.2 提供了这方面的建议。

D.1.1.3 证书处理

电子机读旅行证件证书的处理步骤是[RFC 5280]中所规定的步骤的一部分。使用这一简化过程处理电子机读旅行证件证书的结果将与使用完整的 RFC 5280 算法的结果一致。如果按 D.2 所述设置了其他输入值和国家变量：

a) 核实基本证书信息。证书必须满足下列各项：
   - 可通过 working_public_key_algorithm、working_public_key 和 working_public_key_parameters 核实证书上的签名；
   - 证书有效期包括当前时间；
   - 在当前时间，证书没有被撤销（详细介绍见 6.3）；和
   - 证书签发者名称是 working_issuer_name。

b) 将证书的 subjectPublicKey 赋给 working_public_key。

c) 如果证书的 subjectPublicKeyInfo 域包含一个参数为非空的算法域，将参数赋给 working_public_key_parameters 变量。如果证书的 subjectPublicKeyInfo 域包含一个参数为空或省去参数的算法域，将证书的 subjectPublicKey 算法与 working_public_key_algorithm 作比较。如果证书的 subjectPublicKey 算法与 working_public_key_algorithm 不同，则将 working_public_key_parameters 设为空值。

d) 将证书的 subjectPublicKey 算法赋给 working_public_key_algorithm 变量。

e) 查明并处理证书中存在的任何其他关键扩展。

f) 处理证书中存在的其他任何经查明的非关键性扩展。

如果步骤 a) 中的任一检查失败或者证书中有任何未被查明从而未能被处理的关键性扩展，路径验证程序失败。否则该程序成功。

D.1.1.4　输出

如果路径验证成功，程序终止，返回成功指示以及 working_public_key、working_public_key_algorithm 和 working_public_key_parameters。

如果路径验证失败，程序终止，返回失败指示和相关原因。

D.1.2　证书撤销列表验证和撤销检查

[REC 5280]中的证书撤销列表验证算法涵盖了各种类型的证书撤销列表，包括增量证书撤销列表、分组证书撤销列表、间接证书撤销列表等等。电子机读旅行证件应用中的证书撤销列表概要极具限制性，禁止使用这些特征。同样还禁止使用 issuingDistributionPoint 扩展以及所有标准化的证书撤销列表记录扩展。因此，电子机读旅行证件应用的证书撤销列表验证和撤销检查相对简单。

D.1.2.1　输入

[RFC 5280]规定了证书撤销列表验证算法的两个输入值。仅下列一个与电子机读旅行证件应用相关。如果在实施时需要提供另外一个输入值，D.2 提供了这方面的建议。

- 证书：证书序列号和签发者名称

D.1.2.2　初始化

[RFC 5280]中规定了三个国家变量。仅下列一个与电子机读旅行证件应用相关。如果在实施时需要初始化另外两个变量，D.2 提供了这方面的建议。

- cert_status：初始化为值 UNREVOKED。

D.1.2.3 证书撤销列表处理

电子机读旅行证件应用中的所有证书撤销列表都是完整的证书撤销列表，涵盖由签发证书撤销列表的国家签名认证机构所签发的所有当前证书。无分组、增量或间接证书撤销列表。电子机读旅行证件应用的证书撤销列表处理算法步骤为：

a) 获取签发证书的国家签名认证机构的当前证书撤销列表。如果不能获取证书撤销列表，则将 cert_status 变量设为 UNDETERMINED，并停止处理。

b) 核实证书撤销列表签发者与签发所涉证书的国家签名认证机构为同一实体。因为每一国家仅有一个国家签名认证机构，并且电子机读旅行证件应用是封闭性的，由查验系统保存该应用所特有的证书撤销列表缓存，所以，核实证书撤销列表的签发者域中的国家名称与证书签发者域中的国家名称是相同的就足够了。

- 如果自签发证书后，国家签名认证机构并未更改名称，那么，证书撤销列表中的签发者域和证书中的签发者域将是相同的。
- 如果自签发证书后，国家签名认证机构更改了名称，那么，证书签发者域名称和证书撤销列表签发者域中的国家属性将是相同的，但其他一些属性可能不同。
- 如果信赖方希望核实并未对一些非电子机读旅行证件证书撤销列表进行过替换，信赖方可以选择性地核实其拥有关于国家签名认证机构两个名称的信任锚并且这些信任锚是针对同一国家签名认证机构的。如果国家签名认证机构更改了名称，并且将可选的 issuerAltName 扩展放入了证书撤销列表中，则信赖方可以选择性地核实证书中的签发者域与该扩展的其中一个值是相同的。

如果证书撤销列表签发者并非签发证书的国家签名认证机构，则将 cert_status 变量设为 UNDETERMINED，并停止处理。

c) 验证证书撤销列表签发者的认证路径。注意在电子机读旅行证件应用中，所有证书撤销列表都是由作为针对各自路径的信任锚的国家签名认证机构签发的。与[RFC 5280]中的算法不同，电子机读旅行证件应用不要求用来验证证书撤销列表认证路径的信任锚与用来验证目标证书的信任锚为同一个。但是，如果信任锚不同，它们必须都是针对同一国家签名认证机构的信任锚。与[RFC 5280]不同，在电子机读旅行证件应用中，一个既定的国家签名认证机构有多个同时有效的信任锚。如果不能成功验证认证路径，则将 cert_status 变量设为 UNDETERMINED，并停止处理。

d) 核实证书撤销列表上的签名。如果不能成功核实该签名，则将 cert_status 变量设为 UNDETERMINED，并停止处理。

e) 搜索证书撤销列表上的证书。如果发现与证书签发者和序列号相匹配的某条记录，则将 cert_status 变量设为 UNSPECIFIED。

D.1.2.4 输出

返回 cert_status。如果步骤 a)、b)、c) 或 d) 失败，状态将为 UNDETERMINED。如果证书在证书撤销列表中被列为已撤销，则状态为 UNSPECIFIED。如果证书撤销列表验证成功，但证书未列在证书撤销列表上，则状态为 UNREVOKED。

D.2　电子机读旅行证件不需要采取的步骤

D.2.1　认证路径验证

与电子机读旅行证件验证不相关的其他输入值的设定包括：

- initial-policy-mapping-inhibit：设定为禁止策略映射；
- initial-any-policy-inhibit：设定为禁止处理 any-policy 值；
- initial-permitted-subtrees：设定为允许所有子树；
- initial-excluded-subtrees：设定为不排除子树；
- initial-explicit-policy：不应设定；和
- user-initial-policy-set：设定为特殊值“any-policy”。

与电子机读旅行证件不相关的国家变量的初始化包括：

- permitted_subtrees：初始化为允许所有子树；
- excluded_subtrees：初始化为不排除子树；
- inhibit_any_policy：如果设定了 initial-any-policy-inhibit，则初始化为“0”。否则，将其设定为 1 或者大于 1 的任何值；
- policy_mapping：初始化为“0”；
- explicit_policy：初始化为“2”；和
- valid_policy_tree：将 valid_policy 元素初始化为“anyPolicy”，将 qualifier_set 元素初始化为空，以及将 expected_policy_set 初始化为“anyPolicy”。

D.2.2　证书撤销列表验证

与电子机读旅行证件验证不相关的其他输入值的设定包括：

- use-deltas：设定为禁止使用增量。

与电子机读旅行证件应用不相关的国家变量的初始化包括：

- reasons_mask：初始化为空集；和
- Interim_reasons_mask：初始化为特殊值“all-reasons”。

D.3 为处理证书撤销列表需要做出的改动

按照 [RFC 5280] 中的证书撤销列表验证程序运行的证书撤销列表验证系统并不支持认证机构进行过更名的环境，如电子机读旅行证件应用环境。因此，需对这些系统做一些改动，以应对这一特殊情况，具体如下所述：

a) 在 [RFC 5280] 证书撤销列表验证程序第 6.3.3 条的步骤 a) 中，使用所涉证书的证书撤销列表分发点扩展分发点域的名称来更新相关证书撤销列表的本地缓存。对于电子机读旅行证件应用，需要对这一步骤进行修改，仅应使用分布点域的 countryName 属性来确定和获取相关的证书撤销列表。

b) 在 [RFC 5280] 证书撤销列表验证程序第 6.3.3 条的步骤 f) 中，要求使用与用于验证目标证书相同的信任锚来验证证书撤销列表签发者的认证路径。对于电子机读旅行证件应用来说无此要求，因为国家签名认证机构的每个公钥都设有独立的信任锚。

用于验证证书撤销列表签发者的信任锚将为用来签署证书撤销列表的私钥所对应的国家签名认证机构公钥的信任锚。用来验证目标证书认证路径的信任锚可能是国家签名认证机构较早的一个密钥对的信任锚。

— — — — — — — —

第 12 部分附录 E

LDS2 示例
（资料性）

以下示例展示了 LDS2 签名公钥基础设施和 LDS2 授权公钥基础设施的不同组件之间的交互。

为了说明典型业务场景所需的交互和预备条件，请考虑这样一个场景：敌托邦国想要在乌托邦国公民的护照上写入旅行印章。随后，亚特兰蒂斯国想要读取敌托邦国写入乌托邦国护照的旅行印章。

预备条件如下：

- 乌托邦国在其护照上安装了 LDS2 旅行印章应用程序。
- 敌托邦国和乌托邦国都建立了各自的 LDS2 授权公钥基础设施。
- 敌托邦国已建立了本国的 LDS1 签名公钥基础设施来签发 LDS2 签名者证书。
- 乌托邦国和敌托邦国已在某个时候以受信任的方式交换了国家校验认证机构证书以及单一联络点客户端和服务器证书（随后，可以通过单一联络点直接交换新的国家校验认证机构和单一联络点证书）。
- 乌托邦国和亚特兰蒂斯国已在某个时候以受信任的方式交换了国家校验认证机构证书以及单一联络点客户端和服务器证书（随后，可以通过单一联络点直接交换新的国家校验认证机构和单一联络点证书）。如果 LDS2 旅行印章应用程序是开放供读取的，即任何国家都可以读取 LDS2 旅行印章（只有写入才需要许可），则可以省略此步骤。
- 敌托邦国和亚特兰蒂斯国已在某个时候以受信任的方式交换了国家校验认证机构证书。

敌托邦国在乌托邦国的电子机读旅行证件上加盖电子印章的循环过程如下：

- 敌托邦国向乌托邦国申请证件校验者证书。
- 敌托邦国的单一联络点使用其单一联络点客户端证书和乌托邦国的单一联络点服务器证书来发起单一联络点连接。然后，由敌托邦国的证件校验者生成请求，并通过单一联络点将该请求发送至对方的单一联络点。根据请求，乌托邦国会为敌托邦国生成具有读/写访问权限的针对外国证件校验者的证书，该证书将通过单一联络点传回对方的单一联络点。
- 敌托邦国的证件校验者在从其本国的单一联络点收到证件校验者证书后，为其边界的终端生成终端证书。连接到护照，乌托邦国护照上的集成电路用敌托邦国的证件校验者证书校验敌托邦国的终端证书，并用乌托邦国的国家校验认证机构证书校验敌托邦国的证件校验者证书。然后，集成电路授予敌托邦国终端对 LDS2 旅行印章应用程序的读/写访问权限。

在电子机读旅行证件上加盖电子印章的过程如下：

- 敌托邦国创建一个电子旅行印章，并使用与存储在敌托邦国 LDS2 签名公钥基础设施的 LDS2（旅行印章）签名者证书中的公钥对应的私钥对其进行签名。LDS2 签名者证书存储在乌托邦国护照的非接触式集成电路上。

在亚特兰蒂斯国边境遇到乌托邦国护照时：

- 如果从乌托邦国护照上读取旅行印章需要具有读取权限的终端证书，则亚特兰蒂斯国将通过其单一联络点将证书请求发送至乌托邦国的单一联络点。根据请求，乌托邦国为亚特兰蒂斯国生成具有读取访问权限的针对外国证件校验者的证书，并通过其单一联络点将该证书发送给亚特兰蒂斯国的单一联络点。亚特兰蒂斯国使用该证件校验者证书为其本国终端生成具有对乌托邦国护照读取访问权限的终端证书。如果任一终端都可以读取乌托邦国护照上的旅行印章，则可以省略此步骤。

- 为了校验敌托邦国写入护照的旅行印章，亚特兰蒂斯国使用敌托邦国的 LDS1 签名公钥基础设施：用存储在护照中的敌托邦国 LDS2 签名者证书校验旅行印章。一条链条由此就建立起来了，即用前期收到的敌托邦国的国家签名认证机构证书对敌托邦国的 LDS2 签名者证书进行校验。

—完—

ISBN 978-92-9265-531-0