ICAO

Doc 9303

机读旅行证件

第八版, 2021年

第13部分：可见数字印章

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13部分：可见数字印章

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

下载及补充信息载于： www.icao.int/security/mrtd

Doc 9303 号文件 —《机读旅行证件》
第 13 部分 — 可见数字印章
ISBN 978-92-9265-324-8（印刷版）
ISBN 978-92-9275-541-6（电子版）

修订

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

修订和更正记录

修订		
编号	日期	换页人
1	14/6/24	ICAO

更正		
编号	日期	换页人

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

目录

1. 范围

Doc 9303 号文件的这一第 13 部分，利用非对称加密法，以相对低廉但高度安全的方式，明确了数字印章规范，以确保非电子证件的真实性和完好性。对非电子证件的信息进行加密签署，对签名进行二维条形码编码并打印在证件原件之上。这种做法 — 可见电子印章 — 具备以下优势：

- 非对称　由于使用非对称加密法，加附数字印章的费用显著高于签发具有数字印章保护的证件。这样做，即使签发证件的费用很低，但是假冒或伪造证件个性化数据的费用却极高。

- 个性化　每个数字印章核实实际证件上打印的信息，并因此与持证人绑定。没有直接等效的空白证件，因此，不存在遗失或被盗的空白证件。

- 易于核实　即使未经训练的人员也可以通过智能手机安装的应用程序等低成本设备，核实采用数字印章保护的证件。此外，由于数字签名具有二元性，因此真实证件与伪造证件的区别一目了然。

尽管数字印章为没有微芯片（通常纸版）的证件提供了显著的安保改进，但与基于芯片的证件相比仍具有很大局限性。数字印章的存储容量通常限于最多几千字节，并且无论是数据还是密钥或者是数字印章方案，都无法在现有证件上进行更新。换言之，不支持加密灵活性。数字印章无法防止克隆，没有实施隐私保护特征，并且比基于芯片的证件更容易出现磨损导致的读取错误。此外，加密芯片的通用性允许实施额外的特征，如：签名方案、终端认证、基于共享秘密的双重验证法，即：个人身份识别号码，或者基于对称方案的安全密码协议。由于二维条形码不能取代微芯片的特征和安保特征，因此，在可行的情况下，旅行证件必须采用微芯片。

2. 数字印章编码

可见数字印章是一种内含证件特征、被编码为二维条形码并打印在证件上的加密签名数据结构。本节阐述了可见数字印章的编码和结构。

2.1 条形码的格式和打印要求

这项规范界定了对数据进行编码使其成为字节流的方式。**必须**只使用其符号被确定为国际标准化组织标准的二维条形码。国际标准化组织的标准化二维条形码符号包括，例如：数据矩阵[ISO/IEC 16022]、阿兹特克码[ISO/IEC 24778]和二维码[ISO/IEC 18004]。

条形码的打印方式，**应当**允许读取设备（即：现成的智能手机或扫描仪）对条形码进行可靠解码；尤其是，**应当**虑及[ISO/IEC 15415]评估打印质量。最终的打印和扫描质量要求取决于证件; 与应用场景具体相关的细节**可以**在配置文件中明确说明。由于打印和扫描质量会影响差错率并影响数字印章验证的可靠性，因此，这些质量要求**应当**确保可以可靠地验证包含数字印章和所有强制性证件特征的条形码。另外一项重要要求涉及条形码的符号对比，因为数字印章可以被打印在具有彩色背景（如：绿色）的防伪纸上。

当使用标准喷墨打印机时，**建议**采用每个模块边长至少 0.3386 毫米的模块（二维条形码一个组块的尺寸），对应模块的每个边长 4 点（即每个模块 16 点），在每英寸 300 点的打印机上进行打印，或者模块的每个边长 8 点（即：每个模块 64 点）在每英寸 600 点的打印机上进行打印。如果使用高分辨率打印机或激光打印机，则**可以**接受较小的打印尺寸。有关在证件上放置条形码的情况，请参见 Doc 9303 号文件的相关部分。

经编码的条形码包括标头（见第 2.2 节）、信息区（见第 2.3 节）和签名区（见第 2.4 节）。图 1 载有关于该结构的概述。

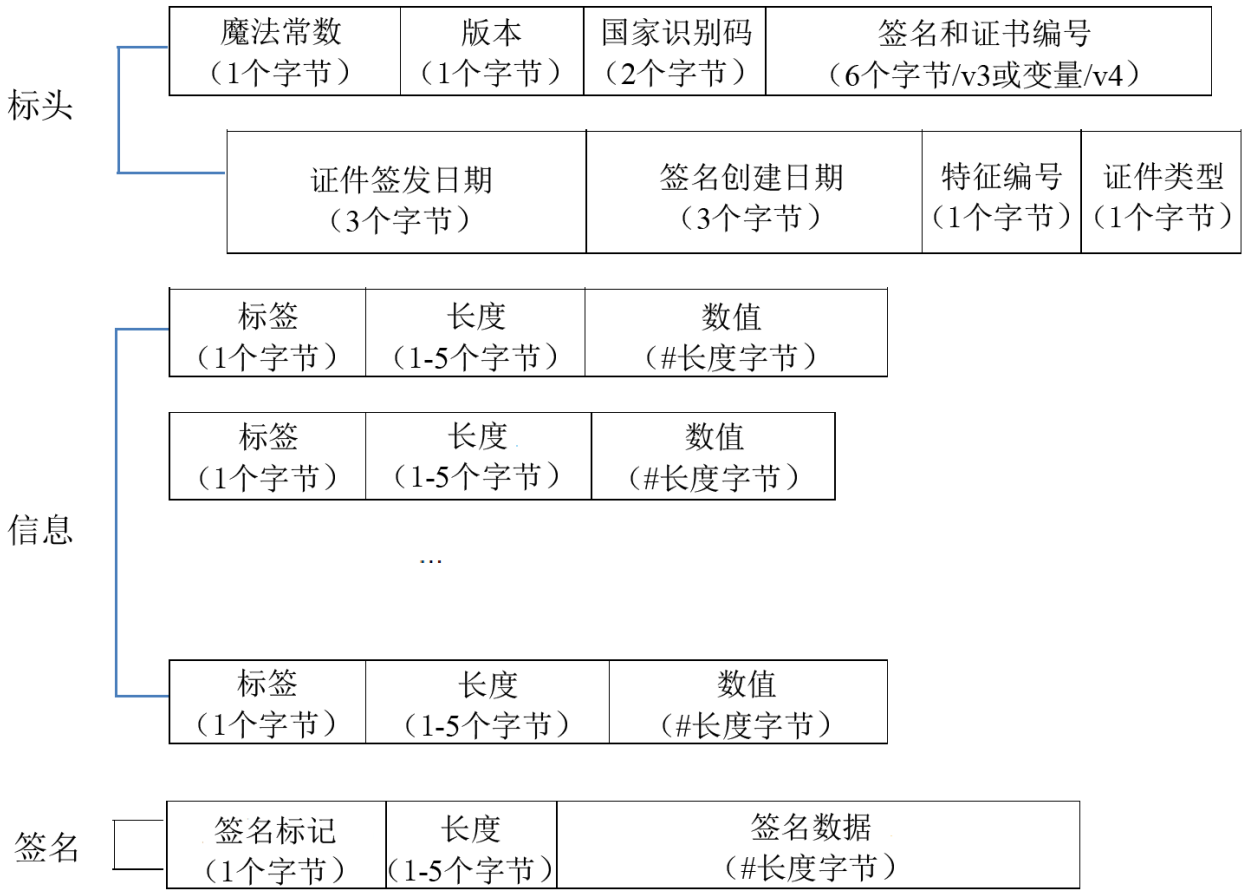

图 1　数字印章结构

2.2　标头

标头包含证件和编码的元数据，例如：版本号、证件签发日期和签三 fi 名创建日期等。

此规范界定了标头的两个版本，分别由版本标识符“3”和“4”表示。版本的不同之处在于证书编号的定义（见下文）和证件特征的长度编码（见第 2.3 节）。

版本 3 的标头总长是 18 个字节，而版本 4 的标头长度是个变量。标头的定义载于表 1。

表 1　标头格式

开始位置	长度（字节）	内容
0x00	1	*魔法常数*　魔法常数的固定值为 0xDC，用于标识符合此规范的条形码。
0x01	1	*版本*　标识此规范版本的字节数。此规范界定的版本分别由字节数 0x02 / 0x03 标识。数字 n 表示版本 n + 1，例如：数值 0 表示版本 1。
0x02	2	*签发国*　识别签发国或签发组织的 3 字代码。3 字代码是根据 9303-3 号文件编制的。如果 3 字代码的构成不足三个字母，该代码**必须**用填充符（‘<’）补足，例如‘D’被填充为‘D<<’。代码由 C40 进行编码（见 2.6 节）作为一个两字节序列。
0x04	6 / v	*签名标识符和证书编号* 版本 3：标识（条形码）签名和证书的 9 字代码。 版本 4：标识（条形码）签名和证书的可变长度字母代码（“ v”表示这一字段的总长度）。 代码由 C40 进行编码（见 2.6 节）。关于可变长度的编码，见第 2.2.1 节。
0x0A/0x04 + v	3	*证件签发日期*　签发证件的日期。 根据 2.3.1 节的定义进行编码。
0x0D/0x07 + v	3	*签名创建日期*　创建签名的日期。根据 2.3.1 节的定义进行编码。
0x10 / 0x0A + v	1	*证件特征定义编号*　证件编号代码，定义证件特征的数字和编码。此定义对于每个证件类型的类别都是独立的，即：相同的证件特征的定义编号代码，对于不同的证件类型的类别可能具有不同的含义。数值**必须**在 01（十进制）与 254（十进制）之间。
0x11 / 0x0B + v	1	*证件类别*　证件类别，例如：签证、紧急旅行证件、出生证。01（十进制）与 253（十进制）之间的奇数，**必须**用于国际民航组织规定的证件类别。
和	18/12 + v	

2.2.1 签名标识符和证书编号

由于尺寸限制，无法在条形码中存储包含与签名对应的公钥证书。因此，**必须**通过不同渠道获取证书。为了独特地标识证书和作为证书题目的签名，并将证书与条形码联系在一起，在标头中存储了包含签名标识符及证书编号的字符串。此字符串包括：

a) 签名标识符：根据关于签名国的 Doc 9303-3 号文件，将两字国家代码与两字组成的字母数字字符合并，以标识上述界定国家内签名人的身份。对于特定国家内的签名人，签名标识符**必须**具有独特性。

b) 证书编号：

1) 对于标头版本 3：正好是**必须**独特标识特定签名证书的五个字符组成的十六进制字符串。

2) 对于标头版本 4：包含以下级联内容的十六进制字符串：

i) 正好两个字符，表示后续字符的数量，和

ii) **必须**独特地标识特定的签名证书。

请注意签证的具体使用情况（见 Doc 9303-7 号文件），签名人即签证签名人。

证书编号 0 ... 0 留作测试，**不得**用于证件制作。

（条形码）签名标识符和证书编号，**必须**分别对应签名证书的题目标识名（DN）和序列号。因此，可以在解码标头时对签名证书进行独特的标识。

2.2.2 证件特征定义编号和证件类型的类别

证件特征定义编号和证件类型的类别组合标明了一组具体规则，如本规范。因此，未来使用时，可以重复使用相同的条形码和标头格式，但参照不同的特征定义（即：定义条形码所含信息列表的参照）或证件类型的类别。这允许重复使用现有的代码库，简化实施并提高可互用性。

签证和紧急旅行证件的证件特征定义编号及证件类型的类别，分别在 Doc 9303-7 号文件和 Doc 9303-8 号文件中做了界定。

2.3 信息区

标头之后是信息区。根据本节的规定，信息区包括数字编码的证件特征。只要具备所有强制性的证件特征，证件特征的所有顺序便是有效的。

每项证件特征之前：

- 有标识特征类型的标签（1 个字节）
- 有该特征的长度（1 个字节到 5 个字节）

根据版本标识符（在标头的开始位置 0x01，见表 1），必须区分两种长度编码：

- 对于 3 号及其之下的版本，其长度**必须**直接采用 1 个字节进行编码（此“长度字节”是紧随信息“标签”之后的第二个字节）。
- 对于 4 号及其之上的版本，其长度**必须**根据[X.690]采用特异编码规则 — 标签长度值进行编码。

对于签证证件，**建议**使用 4 号版本（或更高版本），并因此使用特异编码规则 — 标签长度值的长度编码。使用 3 号版本（或更低版本）并因此直接进行长度编码是有效的，但建议避免这种做法。

对于 ETD 证件，**必须**使用 4 号版本（或更高版本），因此**必须**使用特异编码规则-标签长度值的长度编码。

2.3.1　证件特征的数字编码（二进制编码）

证件特征按以下方式编码。我们审议以下基本类型作为构建组块：

a) *字母数字*：大写[1]字母数字字符串（即：A-Z、0-9 和空格）；

b) *二进制*：字节序列；

c) Int（*整数*）：正整数；和

d) *日期*：日期。

这些基本类型被转换为以下字节序列：

a) 按照 C40 编码的字节对字母数字字符串进行编码（见 2.6 节）。

b) 字节序列原样不动。

c) 对于正整数，采用其无符号整数的表示形式。

d) 首先按照将月、日和（4 位数）年的级联将日期转换为正整数。然后，将这个正整数级联到上述 c) 所界定的三个字节的序列中。

示例：以 1957 年 3 月 25 日为例。将月、日和年进行级联，产生整数 03251957，结果是三个字节 0x31 0x9E 0xF5。

数字证件特征是字节序列。它具有以下结构：

标签 | 长度 | 数值

此处标签是 0-254（十进制）范围内的整数，用作证件特征的独特标识符。请注意，标签 255（十进制）被保留用以表示签名的开始。根据特异编码规则 — 标签长度值长度字段编码，长度由一到五个字节组成。长度表示后续数值的长度。数值是转换为字节序列的基本类型。

1. 对大写字母的限制是条形码的数据容量有限所致。

示例：以指定的标签 0x0A 对字符串“VISA01”进行编码的证件特征为例。长度 4 的 C40 编码字节序列（见 2.6 节）是 0xDE515826。因此，证件特征的字节序列是 0x0A04DE515826。

因此，具体使用时必须通过例举须具备和可以任选具备的证件特征、界定其标签数值和允许的长度范围来加强此定义。

可能出现额外特征，即：附不详标签的特征，例如：供签发实体选择使用。此类额外特征**不得**使用附加特征字段的标签或任何其他可选或强制特征的标签。如果承认签名有效，则所出现的附带不详标签的特征，**不得**影响条形码的有效性。

2.4 签名区

签名区的开始处由数值为 0xFF 的签名标记予以标明，被编码为一个字节，其后是使用特异编码规则 — 标签长度值长度字段的编码方案来表示签名长度（字节数）的 1 到 5 个字节。

签名算法的输入**必须**是标头与完整信息区的级联（散列），不包括表示签名区开始处或签名长度的标签。签名区包含产生的签名。

必须只使用 Doc 9303-12 号文件界定的散列和签名算法。由于产生的签名大小所致，**建议**与 SHA-256 结合使用至少 256 位密钥长度（在创建本文件时）的椭圆曲线数字签名算法（ECDSA）。

适用椭圆曲线数字签名算法可得到一对正整数（r、s）。此签名**必须**以原始格式存储在印章中。r 和 s 的位长分别对应密钥的长度。因此，例如：对于椭圆曲线数字签名算法-256，r 和 s 各项的长度最多是 256 位= 32 个字节。**必须**通过计算 r 和 s 的无符号整数表示存储签名，并且可能添加前导零以使 r 和 s 符合其预期长度（即密钥长度），并将 s 的结果值加到其中的一个 r 当中。参见附录 B 关于抽象语法标记 1 与（r、s）原始格式之间的转换。

签名中使用的散列算法不在结构中编码。散列算法需要从用于创建签名的曲线基点生成器的阶次位长中推导出来，用于签名和验证。

推导散列算法的步骤如下：

- 令**τ**表示基点生成器 G 的阶次位长。阶次**η**可以从签名者证书的 EC 参数中获取，并给出**τ**的值
- **τ**必须小于或等于散列算法（**τ**<=l）的输出长度“l”

散列算法	如果条件满足
SHA-224	**τ** <=224
SHA-256	(**τ** <=256) 和 (**τ** >224)

散列算法	如果条件满足
SHA-384	(**τ** <=384) 和 (**τ** >256)
SHA-512	(**τ** <=512) 和 (**τ** >384)

2.5　填充

如果标头、信息和签名未一起填满条形码的可用空间，则**必须**在签名后面添加填充字符。所有相关的二维条形码符号，界定其各自标准中的填充方法，填充**必须**遵循该界定。

2.6　字符串 C40 编码

为了节省编码字母数字字符和填充符号<的空间，根据[ISO/IEC 16022]的界定，使用了编码方案 C40。以下界定了在当前设置中对这些定义的使用方式。后面两项定义适用于证件特征及其数字编码：

a) 字符串仅包括大写字母、数字、<**空格**>和符号'<'。后者被当做旅行证件机读区（MRZ）的填充符。如果字符串中出现'<'，则将在编码之前用<**空格**>替换所出现的所有'<'。字符串**不得**包含任何其他符号。

b) 已知一个字符串的长度为 L，对应数字编码的长度（即：字节数）即大于或等于 L 的最小偶数。

在以下运算中，对一个字节数值和对应的无符号整数等价进行了隐式转换。例如：我们通过对整数数值进行整数运算的公式来界定字节的数值。

2.6.1　编码

将字符串编入字节序列的方式如下：首先，将字符串分为由三个字符组成的元组，然后根据表 2，用对应的 C40 的数值替换每个字符，得出三元组（U1、U2、U3）。然后，计算每个三元组的数值。

U =（1600 * U1）+（40 * U2）+ U3 + 1

其结果介于 1 到 64 000 之间，并给出一个无符号 16 位整数的数值。这一 16 位的数值 I16 被打包成两个字节

字节 1 =（I16）div 256

字节 2 =（I16）mod 256

此处 div 表示整除（无余数），而 mod 表示取余运算。请注意，这些运算可以通过位元移位进行。

表 2　C40 编码图及与美国信息交换标准代码的对应

C40 数值	字符	美国信息交换标准代码数值	C40 数值	字符	美国信息交换标准代码数值
0	移位 1	不适用	20	G	71
1	移位 2	不适用	21	H	72
2	移位 3	不适用	22	I	73
3	<空格>	32	23	J	74
4	0	48	24	K	75
5	1	49	25	L	76
6	2	50	26	M	77
7	3	51	27	N	78
8	4	52	28	O	79
9	5	53	29	P	80
10	6	54	30	Q	81
11	7	55	31	R	82
12	8	56	32	S	83
13	9	57	33	T	84
14	A	65	34	U	85
15	B	66	35	V	86
16	C	67	36	W	87
17	D	68	37	X	88
18	E	69	38	Y	89
19	F	70	39	Z	90

2.6.2　解码

编码很容易倒置。已知一对字节，设其（I1、I2）表示无符号整数值。16 位的数值 I16 被重新计算为

$$V16 = (I1 * 256) + I2$$

可以通过以下公式重新计算三元组（U1、U2、U3）

U1 =（V16 – 1）div 1600

U2 =（V16 –（U1 * 1600）-1）div 40

U3 = V16 –（U1 * 1600）–（U2 * 40）-1

此处 div 依然表示整除。只需查找表 2 中的对应数值，即可通过三元组（U1、U2、U3）对字符进行解码。

2.6.3　填充

如拟编码的字符串长度是三的倍数，上述定义便只是良定义。类似于[ISO/IEC 16022]所载的已知填充定义，以下填充规则适用：

a) 当两个 C40（=两个字符）的数值保留在字符串的末尾，则这两个 C40 的数值将被补全成为 C40 数值为 0（移位 1）的三元组。该三元组根据上述定义进行编码。

b) 如果一个 C40 的数值（= 一个字符）不变，则第一个字节的数值为 254（十进制）（0xFE）。第二个字节是对应 C40 数值的字符数据矩阵的美国信息交换标准代码编码方案的数值。请注意，0-127 范围内的美国信息交换标准代码数据矩阵内的美国信息交换标准代码的编码方案，即是美国信息交换标准代码的字符加 1。

3.　数字印章的用法

本节给出了对适用于签证和紧急旅行证件的数字印章用法的通用描述。具体要求在对应的配置文件中进行了界定。

3.1　内容和编码规则

3.1.1　标头

根据第 2.2 节对数字印章的标头进行编码。证件特征定义编号和证件类型类别的最后 2 个字节的数值取决于具体的证件配置文件。对于国际民航组织的配置文件，证件类型的类别必须是奇数。偶数**可以**用于国际民航组织未指定的国家配置文件。

3.1.2　在数字印章中进行编码的证件特征

印章中**必须**存储的证件特征是机读区（MRZ）：

数字印章**必须**对证件机读区进行编码。机读区可以是 Doc 9303 号文件规定的任何类型。但是，证件的具体配置文件**可能会**限制机读区的允许类型。

每个证件的配置文件都**可能会**界定其他**必填**字段和**选填**字段。

3.1.3 证件特征的编码规则

证件特征的编码取决于证件特征定义的编号以及证件类型的类别。对应的证件配置文件界定了具体的数值。

3.2 条形码签名和印章的创建

为了便于对数字印章进行核实，本规范利用现有的国家签署证书机构（CSCA）公钥基础结构（PKI），签发和发布证书以及证书吊销名单（CRLs）。有关详细信息和证书配置文件，请参见 Doc 9303-12 号文件。

3.2.1 条形码签名系统的结构

条形码签名从证件个性化系统接收数据以便对数字印章进行编码，然后使用签名密钥对其进行签名。图 2 描述了条形码签名及其客户、证件个性化系统的可能实施。

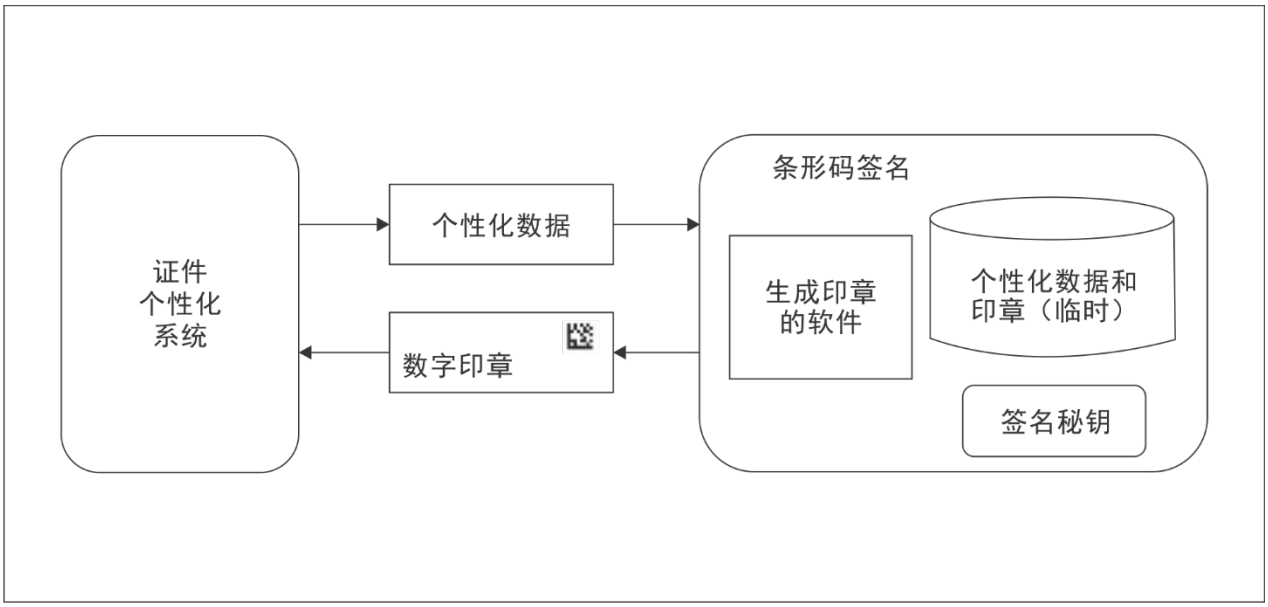

图 2. 证件个性化：采用集中化条形码签名的情景

条形码签名依赖以下软件和数据：

- 生成印章的软件产生符合当前标准的数字印章。它接收客户端发送的个性化数据，使用专用签名密钥对这些数据进行签名，并将个性化数据和签名编为条形码。个性化数据和数字印章分别是生成印章的软件输入和输出数据。在生成印章的过程中，必须将这方面的数据临时存储在条形码签名当中。

- 签名密钥（私钥和公钥）被用于核实签名和数字印章。签名私钥是条形码签名的最关键数据。

根据部署情况，证件个性化系统与条形码签名之间的区别并不总是绝对的。例如：条形码签名可以是使馆个性化系统的一部分。一种可能的情况就是扩展个性化系统以包含生成签名，并将签名密钥存储在使馆内的智能卡上。另一种做法是在母国设置一个中央条形码签名，然后使使馆通过安全通道与其连接。最后，有些使馆可能自己不对证件进行个性化设置；这样的话，也可以在母国建立个性化系统并与条形码签名进行集成。

在生成签名时，条形码签名是非常关键的组成部分。签名允许对条形码数据的完好性进行核实，即：数据是否已被篡改，及其真实性，即：它们是否由经授权的实体签发。

为了实现足够高的安保水平，**建议**条形码签名成为一项中央服务，不要在使馆进行部署，除非运行、技术或后勤方面的原因妨碍进行集中部署。这是为了将安保措施集中在有限的边界上，同时虑及确保可恢复性和业务连续性的最佳做法。签名私钥**必须**由条形码签名人予以妥善保存。

3.2.2　条形码签名系统的安保

条形码签名系统**应当**根据以下方面的最佳安保做法进行托管和运行：实际安保；服务器和网络基础设施；系统开发和支持过程；访问控制；以及运行安保。如果条形码签名被设置成中央服务，**建议**确保遵守[ISO/IEC 27002]条形码签名人的界限，以确保遵守这些最佳安保做法。

4.　编号资料（规范说明）

［ISO/IEC 16022］　ISO/IEC 16022 信息技术 — 自动识别和数据捕获技术 — 数据矩阵条形码符号规范，2006 年

［ISO/IEC 18004］　ISO/IEC 18004：2006：信息技术 — 自动识别和数据捕获技术 — 二维码条形码符号规范，2015 年

［ISO/IEC 24778］　ISO/IEC 24778：2008：信息技术 — 自动识别和数据捕获技术 — 阿兹特克码条形码符号规范，2008 年

［ISO/IEC 27002］　ISO/IEC 27002：信息技术 — 安保技术 — 信息安保管理做法守则，2013 年

［ISO/IEC 15415］　ISO/IEC 15415：2011：信息技术 — 自动识别和数据捕获技术 — 条形码符号打印质量测试规范 — 二维符号，2011 年

［X.690］　ITU-T X.690 2008，数据网络和开放系统通信 OSI 网络和系统方面 — 抽象语法标记 1（ASN.1）信息技术 — 抽象语法标记 1 的编码规则

— — — — — — — —

第 13 部分附录 A

示例使用案例（信息说明）

本节概述了使用数字印章保护非电子证件的概况。这里审议的具体使用案例是对签证证件的保护，如图 A.1 所示。尽管其他使用案例的技术细节可能有所不同，但适用的一般原则相同。

一般工作流程可以分为三个步骤。作为前提条件，必须生成签证签名证书（VSCs）。而后，生成数字印章，然后进行验证。

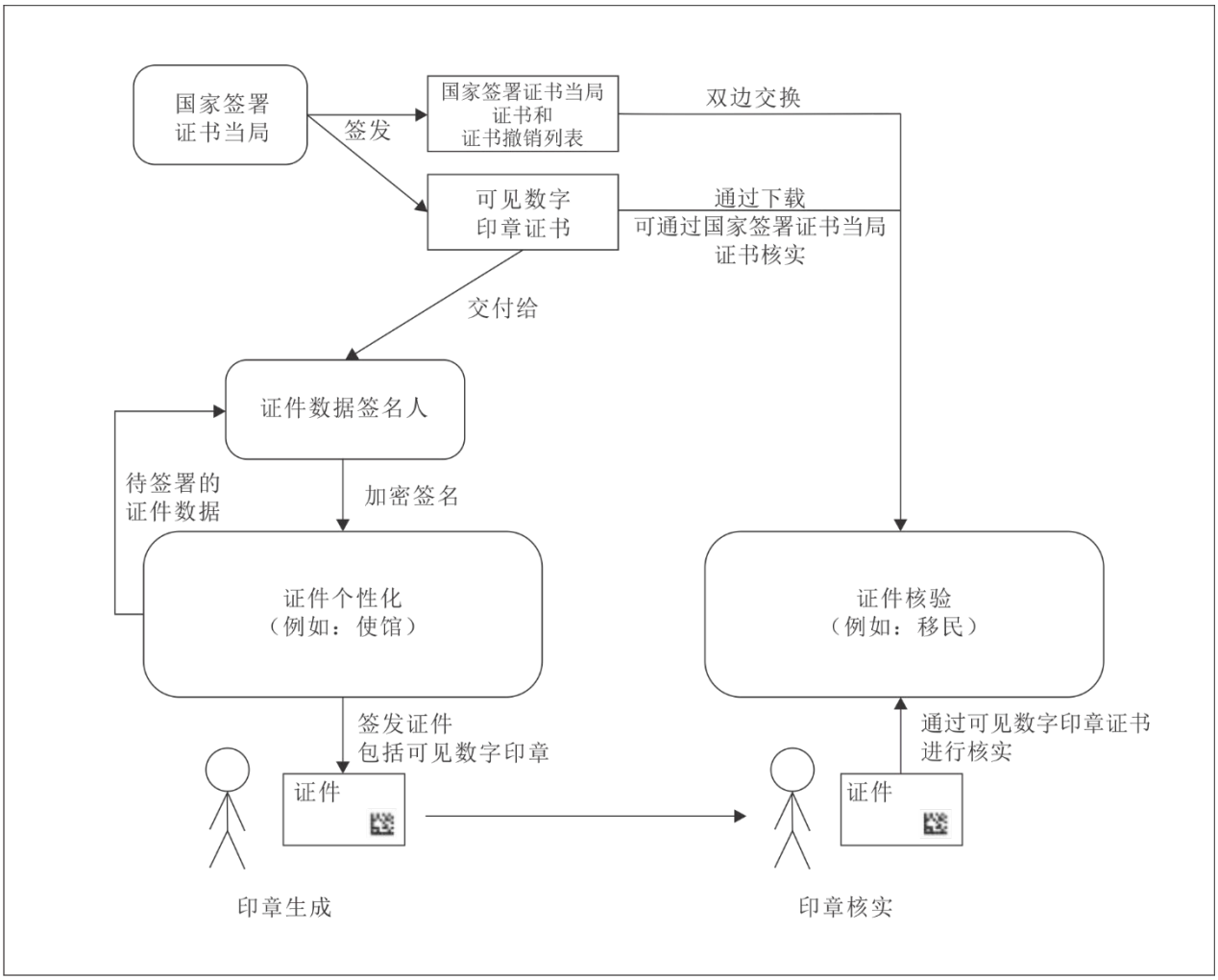

图 A.1.　示例性 VDS 使用案例

A.1 先决条件：签证签名证书的生成

签证签名公钥基础结构的基础是国际民航组织为电子护照界定的公钥基础结构设置。根本上就是每个国家的国家签署证书机构（CSCA）。国家签署证书机构发布包含国家签署证书机构公钥的国家签署证书机构证书。为了实现国家之间的信任，可以通过双边交换或主列表以可信赖的方式分发此国家签署证书机构证书。

签证签名人是实际签署数字印章的实体。签证签名证书由国家签署证书机构颁发，因此可以通过国家签署证书机构证书进行核实。

A.2 数字印章的生成

数字印章分两步生成：

a) 申请人在使馆所在地申请签证。使馆记录申请人的数据，并检查申请人是否符合申领签证的各项要求。如果符合要求，使馆便将所记录数据的数字形式发给签证签名人（VS）。签证签名人可以是：（1）位于签发签证的国家内的中央实体，且使馆通过安全渠道与签证签名人连接在一起，或（2）签证签名人属于每个使馆下设的分散实体，例如：使用包含加密密钥、直接附在个性化系统上的智能卡。在这其中任一情况下，签证签名人均以加密方式签署所记录的数据。

b) 为进行签名，签证签名人使用私钥和公钥的密钥对。实际签名使用私钥完成，而公钥则存储在签证签名证书当中。如果签证签名人不是个性化系统的本地部分，则将生成的签名发回签证个性化系统、打印在签证贴纸上并贴在申请人的护照上。

A.3 数字印章的验证

当申请人进入签发国家时，他们向签证验证机构（VVA）如：签证签发国家的出入境管制当局出示其签证。签证验证机构通过验证印章签名，并将签证贴纸和护照上的所印信息与印章中存储的数字信息进行比对，从而核实签证数字印章的真实性和完好性。借助数字印章标头中存储的标识符来识别对应的签证签名证书，然后使用签证签名证书的公钥来核实印章的签名。如上述几段所述，签证签名证书本身的有效性可以通过国家签署证书机构的证书进行核实。

备注

由于所有证书都公开提供，因此，不只是签发国家，而且所有第三方均可对签证的有效性进行核实。因此，这一做法可以处理使用国家联盟签证的情况，其中一个国家签发另一个国家的签证（如欧盟的示例）。另一项使用案例就是航空公司在登机之前对签证进行核实。

备注

根据数字印章及签证和护照机读区，确定签证文件是否可信的准则已在验证政策中做了界定。

— — — — — — — —

第 13 部分附录 B

椭圆曲线数字签名算法签名格式的转换（信息说明）

B.1 基本编码规则/特异编码规则中的整数编码

整数编码根据基本编码规则（BER）和特异编码规则（DER）进行，作为最小长度的有符号大端编码，其后适用标签长度值（TLV）方案。通过以下情况对其进行区分：

a) 假设整数值为正数，并且最小无符号整数表示形式的最高有效位（MSB）为零。则无符号整数表示形式如下所示，即基本编码规则/特异编码规则数值：

| 0bbbbbbb | …

b) 假设整数值为正数，并且最小无符号整数表示形式的最高有效位为 1，即表示为|1bbbbbbb| …则包含零的字节前置，且基本编码规则 / 特异编码规则数值为：

| 00000000 | 1bbbbbbb | …

c) 假设整数值为负数。则该数值编码为 2 的补码，例如：采用无符号最小整数表示形式，求逆再加 1。之后，将最高有效位设为 1。例如：对于-25357，无符号最小整数表示为：

| 0110 0011 | 0000 1101 |

倒置为

| 1001 1100 | 1111 0010 |

加 1

| 1001 1100 | 1111 0011 |

得出基本编码规则/特异编码规则数值。请注意，该数字为负数的这一事实，可以通过最高有效位（此处最左侧）为 1 的事实直接推断出来。

最后，将两个字节置于上述经编码的基本编码规则/特异编码规则数值之前，得出标签长度值的数值。第一个字节是常数 0x02 的标签。第二个字节包含以下经编码的基本编码规则/特异编码规则数值的长度（即：字节数）。根据最高有效位 ，区分被编码的是负整数或正整数并采用与上述相反的步骤，即可完成解码。

B.2 示例

表 B.1 给出了基本编码规则/特异编码规则之编码整数的一些示例。

表 B.1. 一些整数值的基本编码规则/特异编码规则的编码示例

数值 （十进制）	标签 （十六进制）	长度 （十六进制）	数值 （十六进制）	数值 （二进制）
0	0x02	0x01	0x00	00000000
127	0x02	0x01	0x7F	01111111
128	0x02	0x02	0x00 0x80	00000000 10000000
-129	0x02	0x02	0xFF 0x7F	11111111 01111111

B.3 采用抽象语法标记 1/特异编码规则的椭圆曲线数字签名算法的签名

椭圆曲线数字签名算法签名的抽象语法标记 1 的描述是

签名：= 序列 {
    r 整数，s 整数
}

此序列根据特异编码规则进行编码，作为标签长度值的三倍数，标签为 0x30，长度为后续数值的字节数，该数值作为 r 编码标签长度值三倍数的级联，并附 s 的编码。

两个示例序列-整数 r 和椭圆曲线数字签名算法签名的 s 如表 B.2 所列，实际则当然大很多。

表 B.2. 特异编码规则编码的两个整数序列

整数		序列的标签长度值		
R	**S**	标签	长度	数值
127	1	0x30	0x06	0x02 0x01 0x7F 0x02 0x01 0x01
128	127	0x30	0x07	0x02 0x02 0x00 0x80 0x02 0x01 0x7F

请注意，对于椭圆曲线数字签名算法的签名，r 和 s 始终是正整数。因此，要将原始签名转换为特异编码规则，就必须首先将原始签名分拆，分别获得 r 和 s，然后根据上述定义将它们编码为特异编码规则编码的抽象语法标记 1 的序列。反之，为了将特异编码规则的椭圆曲线数字签名算法签名解码，就必须首先对该序列进行解码，提取 r 和 s 的无符号整数表示，并且如果需要，则通过去除或增加前导零的字节，将 r 和 s 同时设定一个固定长度（=关键尺寸的长度）的表示（即：以椭圆曲线数字签名算法-256 为例，r 和 s 都必须具有 256 位的长度 = 32 字节），并将通过 s 得出的数值附加到通过 r 得出的数值上。

— — — — — — — —

第 13 部分附录 C

C40 编码示例（信息说明）

C.1 示例 1

假设对字符串“XK<CD”进行编码。根据定义，在编码之前，用<空格>取代所出现的全部‘<’。因此，形成的字符串是“XK CD”，即：“XK<空格>CD”（插入一个空格）。表 C.1 描述了字符串“XK<空格>CD”的 C40 编码/解码。

表 C.1 字符串“XK<空格>CD”的编码/解码示例

运算	结果			
原始字符串	“XK <空格> CD”			
分为三元组	（X，K，<空格>）		（C，D，）	
替换为 C40 的数值和填充	（37，24，3）		（16、17，填充）	
计算 16 位整数的数值	60164		26281	
	字节 1（无余数）	**字节 2（取余运算）**	**字节 1（无余数）**	**字节 2（取余运算）**
结果字节序列（十进制）	235	4	102	169
结果字节序列（十六进制）	0xEB	0x04	0x66	0xA9

C.2 示例 2

假设对“XKCD”进行编码。该字符串仅包含大写字母。表 C.2 描述了其 C40 编码/解码。

表 C.2 字符串“XKCD”的编码/解码示例

运算	结果			
原始字符串	“XKCD”			
分为三元组	（X，K，C）		（D，，）	
替换为 C40 的数值和填充	（37、24、16）		（解锁 C40 并以美国信息交换标准代码编码）	
计算 16 位整数的数值	60177			
	字节 1（无余数）	**字节 2（取余运算）**	**字节 1**	**字节 2**
结果字节序列（十进制）	235	11	254	69
结果字节序列（十六进制）	0xEB	0x11	0xFE	0x45

第 13 部分附录 D

验证政策规则（信息说明）

验证政策是能够确定证件印章有效性的一组验证规则。执行这一验证政策，会通过以下之一项数值得出状态显示：

a) VALID（**有效**）。印章的真实性和完好性已得到确认。此处的真实性是指印章中的数据确实采用证件签发国条形码签名人签署，并且对应的条形码签名证书有效。完好性是指加封印章的证件机读区的数据没有被改动，并且原证件所附的数字印章没被调换。

b) INVALID（**无效**）。印章有效性不被承认，而且需要做进一步调查。可能由于以下三种原因导致无效：

   1) *欺诈/伪造*。这包括在被盗空白贴纸基础上对证件进行未经授权的个性化设置，在原始贴纸基础上修改证件个性化数据，或将条形码贴纸从某一被盗证件（例如：护照）调换到另一证件，或进行其他伪造。

   2) *损坏/撕裂*。由于磨损、撕裂或污渍，无法对条形码进行解码。

   3) *未知错误和/或意外错误*。这包括不可预测的错误。例如：因用于解码的软件实施中出现错误，或个性化过程中出现错误编码。

状态显示 INVALID 所附的是状态子显示。它们表明印章无效的原因。由于发生欺诈的可能性取决于这些原因，因此建议用三个信任级别来映射状态显示和子显示：“可信”、“欺诈可能性中等”和“欺诈可能性较高”。表 D.1 对所建议的映射做了说明。

此通用验证政策始终虑及了以下问题：

a) 可见数字印章是否有效？

b) 证件机读区是否有效？

c) 证件的机读区是否与可见数字印章相符？

以下是每种控制类型的验证规则、验证指标列表、每项指标的预期结果，以及得出的状态子显示。

可见数字印章的验证

1. 格式验证

- 如果实际编码格式不符合规范，或者由于实际干扰信息导致的错误无法得到纠正，则状态为 INVALID，并附子显示 READ_ERROR（读取错误），
- 如果编码格式（即：包括标头、信息区和签名区，或二进制/C40 编码的印章结构）不符合规范，或者
- 如果标头中预期数值不详，或者
- 如果信息区的必填字段缺失，或者
- 如果信息区中的字段格式不符合标头界定的版本规范，则状态为 INVALID 并附子显示 WRONG_FORMAT（错误格式），否则继续，或者
- 如果信息区出现不详字段，则应设置子显示 UKNOWN_FEATURE（不详特征）。根据以下步骤中对签名有效性的核实情况，状态显示将是“VALID”或“INVALID”。请注意，如果签名有效，仅出现不详特征，不得破坏印章的有效性。

2. 签名的验证

- 如果没有出现印章标头参照的条形码签名证书，则状态为 INVALID，并附子显示 UNKNOWN_CERTIFICATE（不详证书），
- 如果印章件标头参照的条形码签名证书未由国家签署证书机构签署，或签名核实未果，则状态为 INVALID，并附子显示为 UNTRUSTED_CERTIFICATE（非置信证书），
- 如果条形码签名证书包含一个证件类型扩展名，且条形码的内容包含一个机读区，而机读区的证件类型不包含在证件类型扩展名之内，则状态为 INVALID，并附子显示 INVALID_DOCUMENTTYPE（无效证件类型），
- 如果印章标头参照的条形码签名证书过期，则状态为 INVALID，子显示为 EXPIRED_CERTIFICATE（过期证书），
- 如果印章标头参照的条形码签名证书被撤销，则状态为 INVALID，并附子显示 REVOKED_CERTIFICATE（已吊销证书），
- 如果使用印章标头参照的条形码签名证书对标头和信息区进行的签名核实未果，则状态为 INVALID，并附子显示 INVALID_SIGNATURE（无效签名），
- 否则继续。

3. 签发人的验证

- 如果国家签署证书机构在其置信域中得不到条形码验证系统的置信，则状态为 INVALID，并附子显示为 UNTRUSTED_CERTIFICATE，否则继续。

上述验证规则涵盖将印章件中存储的数据与证件机读区存储的数据进行比较。此外，可以对存储在印章中并打印在证件上，但未出现在证件机读区的那些数据进行人工检查。

表 D.1.　所建议证件政策的置信等级

状态显示	子状态显示	置信等级
VALID	--	可信
	不详特征	
INVALID	读取错误	欺诈可能性中等
	过期证书	
	错误格式	欺诈可能性高
	不详证书	
	非置信证书	
	无效证件类型	
	已吊销证书	
	无效签名	

—完—

ISBN 978-92-9275-541-6