OACI

Doc 9303

Documentos de viaje de lectura mecánica

Octava edición, 2021

Parte 13: Sellos digitales visibles

Aprobado por la Secretaria General y publicado bajo su responsabilidad

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

OACI

Doc 9303

Documentos de viaje de lectura mecánica

Octava edición, 2021

Parte 13: Sellos digitales visibles

Aprobado por la Secretaria General y publicado bajo su responsabilidad

ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL

Publicado por separado en español, árabe, chino, francés, inglés y ruso
por la ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL
999 Robert-Bourassa Boulevard, Montréal, Québec, Canada H3C 5H7

En el sitio web www.icao.int/security/mrtd pueden obtenerse descargas
e información adicional

Doc 9303, *Documentos de viaje de lectura mecánica*
Parte 13 — *Sellos digitales visibles*
ISBN 978-92-9265-269-2 (versión impresa)
ISBN 978-92-9275-547-8 (versión electrónica)

ENMIENDAS

La publicación de enmiendas se anuncia periódicamente en los suplementos del *Catálogo de productos y servicios* de la OACI; el Catálogo y sus suplementos pueden consultarse en el sitio web de la OACI: www.icao.int. Las casillas en blanco facilitan la anotación de estas enmiendas.

REGISTRO DE ENMIENDAS Y CORRIGENDA

ENMIENDAS		
Núm.	Fecha	Anotada por
1	14/6/24	OACI

CORRIGENDA		
Núm.	Fecha	Anotado por

ÍNDICE

1. ALCANCE

En esta Parte 13 del Doc 9303 se especifica un sello digital para garantizar la autenticidad y la integridad de los documentos no electrónicos de manera comparativamente económica, pero altamente segura, mediante el uso de criptografía asimétrica. La información contenida en el documento no electrónico está firmada criptográficamente y la firma está codificada como código de barras bidimensional e impresa en el propio documento. Este método de *sello digital visible* presenta las ventajas siguientes:

- *Asimetría*. Como se utiliza criptografía asimétrica, el costo de incorporar un sello digital es considerablemente mayor que el de expedir un documento protegido con un sello digital. Por eso, aunque el costo de expedir un documento es muy reducido, resulta extremadamente costoso falsificar o adulterar los datos de personalización del documento en cuestión.

- *Personalización.* Cada sello digital verifica la información impresa en el documento físico y, en consecuencia, está ligado al titular del documento. No hay equivalente directo de un documento en blanco, por lo tanto, no hay documentos en blanco que puedan perderse o ser objeto de robo.

- *Verificación fácil*. Los documentos protegidos con sello digital pueden ser verificados incluso por personas sin instrucción al respecto utilizando equipo de bajo costo, por ejemplo, mediante aplicaciones de teléfono inteligente. Más aún, gracias al carácter binario de la firma digital, es fácil distinguir entre un documento auténtico y uno adulterado.

Si bien el sello digital mejora significativamente la seguridad de los documentos (normalmente en papel) que no tienen microplaqueta, sus limitaciones son considerables en comparación con los documentos que incluyen microplaquetas. Los sellos digitales tienen, en general, una capacidad de almacenamiento limitada, de unos pocos kBytes, y ni los datos ni las claves o esquemas criptográficos de ellos pueden actualizarse en los documentos ya existentes. Es decir, no permiten tener agilidad criptográfica. El sello digital no proporciona protección contra clonación, no cuenta con funcionalidad de protección de privacidad, y es más propenso a generar errores de lectura debido a uso y desgaste que los documentos con microplaqueta. Es más, la versatilidad de la criptoplaqueta permite incorporar elementos adicionales como esquemas de firma, autenticación de terminal, métodos de autenticación de dos factores basados en secretos compartidos, i.e., un número de identificación personal (PIN), o protocolos criptográficos seguros basados en esquemas simétricos. Dado que los códigos de barras bidimensionales no pueden sustituir los elementos funcionales o de seguridad de las microplaquetas, siempre que sea posible deben emplearse microplaquetas en los documentos de viaje.

2. CODIFICACIÓN DEL SELLO DIGITAL

Un sello digital visible es una estructura de datos con firma criptográfica que contiene elementos del documento, está codificado como código de barras bidimensional y va impreso en el documento. En esta sección se describe la codificación y la estructura del sello digital visible.

2.1 Requisitos de formato e impresión de códigos de barras

En esta especificación se define la forma en que los datos se codifican en un flujo de bytes. SE UTILIZARÁN únicamente códigos de barras bidimensionales cuya simbología está especificada como norma ISO. Entre las simbologías de códigos de barras bidimensionales normalizadas conforme a la ISO están, por ejemplo, DataMatrix [ISO/IEC 16022], Códigos Aztec [ISO/IEC 24778], y Códigos QR [ISO/IEC 18004].

El código de barras DEBERÍA imprimirse de manera tal que el equipo de lectura (i.e., teléfonos inteligentes o escáner de venta al público) pueda decodificar fiablemente el código de barras, en particular, DEBERÍA considerarse [ISO/IEC 15415] para evaluar la calidad de la impresión. Los requisitos relativos a la calidad de impresión y escaneo resultantes dependen del documento; los detalles de cada escenario de aplicación PUEDEN especificarse en un perfil. Debido al hecho de que la calidad de la impresión y escaneo incide en la proporción de errores e influye en la solidez de la verificación del sello digital, estos requisitos de calidad DEBERÍAN garantizar que el código de barras que contiene el sello digital y todos los elementos obligatorios del documento pueda verificarse de manera confiable. Otro requisito importante es aquel relacionado con el contraste del símbolo del código de barras, porque el sello digital puede estar impreso en papel de seguridad con fondo en color (p. ej., verde).

Cuando se utilicen impresoras de inyección de tinta corrientes, se RECOMIENDA imprimir con un tamaño de módulo (tamaño de un bloque del código de barras bidimensional) de por lo menos 0,3386 mm de longitud lateral por módulo, lo que corresponde a 4 puntos por longitud lateral de módulo (i.e., 16 puntos por módulo) en una impresora de 300 dpi, u 8 puntos por módulo de longitud lateral (i.e., 64 puntos por módulo) en una impresora de 600 dpi. Cuando se utilicen impresoras de alta resolución o láser, PUEDEN aceptarse tamaños de impresión más pequeños. En relación con el emplazamiento del código de barras en el documento, véanse las partes pertinentes del Doc 9303.

El código de barras codificado consta de un encabezamiento (véase la sección 2.2, una zona de mensaje (véase la sección 2.3) y una zona de firma (véase la sección 2.4). En la Figura 1, se ilustra la estructura.

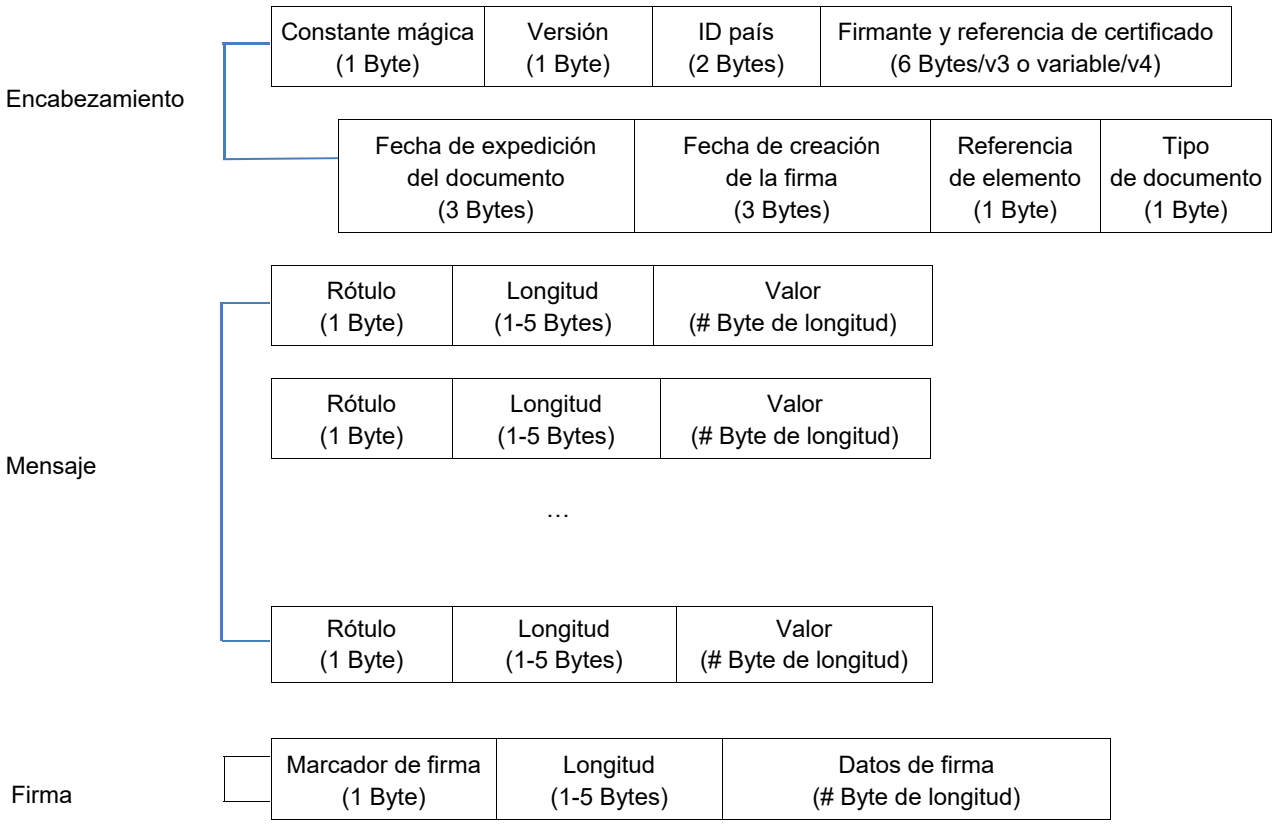

Figura 1. Estructura del sello digital

2.2 Encabezamiento

El encabezamiento contiene metadatos acerca del documento y la codificación, como el número de versión, y las fechas de expedición y de creación de la firma.

Esta especificación define dos versiones del encabezamiento, marcadas con el identificador de versión “3” y “4”, respectivamente. Las versiones difieren en la definición de la referencia de certificado (véase a continuación) y la codificación de longitud de los elementos del documento (véase la sección 2.3).

La longitud total del encabezamiento es 18 bytes para la versión 3 y variable para la versión 4. En la Tabla 1 figura una definición de encabezamiento.

Tabla 1. Formato del encabezamiento

Posición inicial	***Longitud (Byte)***	***Contenido***
`0x00`	1	*Constante mágica*. La constante mágica tiene un valor fijo de `0xDC` que identifica un código de barras conforme a esta especificación.
`0x01`	1	*Versión*. Valor de byte que identifica la versión de esta especificación. Las versiones definidas en esta especificación se identifican con el valor de byte `0x02 / 0x03`, respectivamente. El número `n` indica la versión `n+1`, p.ej., un valor 0 indica la versión 1.
`0x02`	2	*País expedidor*. Código de tres letras que identifica el Estado expedidor o la organización expedidora. El código de tres letras se ajusta al Doc 9303-3. Si el código de tres letras tiene menos de tres letras, DEBE rellenarse con caracteres de relleno (‘<’), p.ej. ‘D’ se rellena con ‘D<<’. El código se codifica conforme a C40 (véase la sección 2.6) como secuencia de dos bytes.
`0x04`	6 / v	*Identificador de firmante y Referencia de certificado*. Versión 3: código de nueve letras con identificación del firmante (código de barras) y del certificado. Versión 4: código de letras de longitud variable con identificación del firmante (código de barras) y del certificado (‘v’ indica la longitud total de este campo). Este código está codificado con C40 (véase la sección 2.6). Para la codificación de longitud variable, véase la sección 2.2.1.
`0x0A / 0x04+v`	3	*Fecha de expedición del documento*. Fecha en que se expidió el documento. Codificada según se define en la sección 2.3.1.
`0x0D / 0x07+v`	3	*Fecha de creación de la firma*. Fecha en que se creó la firma. Codificada según se define en la sección 2.3.1.
`0x10 / 0x0A+v`	1	*Referencia a la definición de elementos del documento*. Código de referencia a un documento que define el número y la codificación de los elementos del documento. Esta definición es independiente para cada categoría de tipo de documento, i.e., el mismo código de referencia a la definición de elementos del documento puede tener distintos significados para diferentes categorías de tipo de documento. Los valores DEBEN estar en el intervalo de 01dic a 254dic.
`.x11 / 0x0B+v`	1	*Categoría de tipo de documento*. Categoría del documento, p.ej., visado, documento de viaje de emergencia, certificado de nacimiento. Para las categorías de tipo de documento especificadas conforme a la OACI se UTILIZARÁN números impares en el intervalo de 01dic a 253dec.
Suma	18 / 12 + v	

2.2.1 Identificador de firmante y Referencia de certificado

Debido al tamaño reducido del código de barras, es imposible almacenar en él los certificados que contienen la clave pública correspondiente a la firma. En consecuencia, el certificado DEBE adquirirse por una vía diferente. Para identificar inequívocamente el certificado y el firmante que es la entidad del certificado, y para vincular el certificado al código de barras, se almacena en el encabezamiento una cadena que contiene el identificador del firmante y una referencia al certificado. La cadena consta de:

a) *Identificador de firmante*: Combinación del código de país de dos letras, conforme al Doc 9303-3, del país del firmante y dos caracteres alfanuméricos para identificar al firmante en el país en cuestión. El identificador de firmante DEBE ser exclusivo para un firmante de un país determinado.

b) *Referencia de certificado*:

1) Para la versión 3 del encabezamiento: cadena hexadecimal exactamente de cinco caracteres que DEBE identificar exclusivamente un certificado para un firmante determinado

2) Para la versión 4 del encabezamiento: cadena hexadecimal que comprende la concatenación de:

i) exactamente dos caracteres que denotan el número de los caracteres siguientes; y

ii) los caracteres que DEBEN identificar exclusivamente un certificado para un firmante determinado.

Nótese que para el uso específico de visados (véase el Doc 9303-7), el firmante es el *firmante del visado*.

La referencia de certificado `0 ... 0` se reserva para fines de pruebas y NO DEBE utilizarse en la producción.

El identificador de firmante (código de barras) y la referencia de certificado DEBEN corresponder al nombre distinguido (DN) de la entidad y el número de serie, respectivamente, de un certificado de firmante. Por lo tanto, el certificado de firmante puede identificarse exclusivamente al decodificar el encabezamiento.

2.2.2 Referencia de la definición de elementos del documento y categoría del tipo de documento

La combinación de la *referencia de la definición de elementos del documento* y la *Categoría del tipo de documento* identifica un conjunto específico de reglas, como esta especificación. En caso de usos futuros, puede reutilizarse el mismo formato de código de barras y encabezamiento, pero con referencia a diferentes definiciones de elementos (i.e., una referencia que define la lista de información incluida en el código de barras) o categorías del tipo de documento. Esto permite reutilizar las bases de códigos existentes, simplificar la implementación e incrementar la interoperabilidad.

Las referencias de la definición de elementos del documento y la categoría del tipo de documento para visados y documentos de viaje de emergencia se definen en el Doc 9303-7 y el Doc 9303-8, respectivamente.

2.3 Zona de mensaje

Después del encabezamiento está la zona de mensaje. La zona de mensaje consta de los elementos del documento codificados digitalmente, según se especifica en esta sección. Cualquier orden de los elementos del documento es válido, siempre que todos los elementos obligatorios del documento estén presentes.

Cada elemento del documento va precedido de:

- un rótulo que identifica el tipo de elemento (un byte)
- la longitud del elemento (de uno byte a cinco bytes)

Dependiendo del identificador de versión (en la posición inicial `0x01` en el encabezamiento, véase la Tabla 1), tienen que distinguirse dos tipos de codificación de longitud:

- Para la versión número 3 e inferior, la longitud DEBE codificarse directamente en 1 byte (este "byte de longitud" es el 2º byte directamente después del "rótulo" del mensaje).

- Para la versión número 4 y superior, la longitud DEBE codificarse con DER-TLV conforme a [X.690].

Para documentos de visado, se RECOMIENDA utilizar la versión número 4 (o superior) y, por ende, la codificación de longitud DER-TLV. La utilización de la versión número 3 (o inferior) y, por tanto, la codificación directa de la longitud, es válida, pero se desaconseja.

Para documentos de viaje de emergencia (ETD), DEBE utilizarse la versión número 4 (o superior) y, por ende, la codificación de longitud DER-TLV.

2.3.1 Codificación digital de elementos del documento (Codificación binaria)

Los elementos del documento se codifican de la manera siguiente. Como componentes esenciales, se consideran los tipos básicos siguientes:

a) *Alfanúm*: cadenas de caracteres alfanuméricos en mayúsculas[1] (i.e., A-Z, 0-9 y espacio);

b) *Binario*: secuencias de bytes;

c) *Ent*: enteros positivos; y

d) *Fecha*: fechas.

Estos tipos básicos se convierten en secuencias de bytes, de la manera siguiente:

a) Las cadenas de caracteres alfanuméricos de codifican como bytes con codificación C40 (véase la sección 2.6).

b) Las secuencias de bytes se toman tal como están.

c) Para los enteros positivos, se toma su representación de número entero sin firma.

d) Primero, una fecha se convierte en un entero positivo concatenando el mes, los días y el año (cuatro dígitos). Este entero positivo se concatena, entonces, en una secuencia de tres bytes según se define en c).

Ejemplo: marzo 25, 1957. En este caso, la concatenación del mes, día y año genera el número entero `03251957`, que resulta en estos tres bytes `0x31 0x9E 0xF5`.

Un elemento de documento digital es una secuencia de bytes con la estructura siguiente:

rótulo | longitud | valor

Aquí *rótulo* es un entero en el intervalo `0-254dec` que actúa como identificador único del elemento del documento.

1. La restricción a letras en mayúsculas se debe a que la capacidad de datos de los códigos de barras es limitada.

Nótese que el rótulo `255dec` se reserva para denotar el inicio de la firma. *longitud* consta de uno a cinco bytes conforme a la codificación de campos de longitud DER-TLV. l*ongitud* denota la longitud del valor siguiente. *valor* es un tipo básico convertido a una secuencia de bytes.

Ejemplo: Se considera un elemento de documento que codifica la cadena “VISA01” con el rótulo asignado 0x0A. La secuencia de byte codificada en C40 (véase la sección 2.6) de longitud 4 es `0xDE515826`. El elemento del documento es, por tanto, la secuencia de byte `0x0A04DE515826`.

Un caso de uso específico debe por tanto aumentar esta definición enumerando los elementos del documento que deben estar presentes y los que pueden estar opcionalmente presentes, definir los valores del rótulo y los intervalos de longitud permitidos.

PUEDE haber elementos adicionales, i.e., elementos con rótulos desconocidos, por ejemplo, para uso opcional de la entidad expedidora. Estos elementos adicionales NO DEBEN utilizar el rótulo del campo del elemento adicional, o el rótulo de cualquier otro elemento opcional u obligatorio. La presencia de elementos con rótulos desconocidos NO AFECTARÁ a la validez del código de barras, si la firma se reconoce como válida.

2.4 Zona de firma

El principio de la zona de firma está indicado por el marcador de firma que tiene el valor `0xFF`, codificado como un byte, seguido de uno byte a cinco bytes que denotan la longitud (el número de bytes) de la firma, conforme al esquema de codificación de campos de longitud DER-TLV.

La entrada del algoritmo de firma DEBE ser (la condensación de) la concatenación del encabezamiento y la zona de mensaje completa, con exclusión del rótulo que denota el inicio de la zona de firma o la longitud de la firma. La zona de firma contiene la firma resultante.

SE UTILIZARÁN únicamente los algoritmos de condensación y firma definidos en el Doc 9303-12. Debido al tamaño de la firma resultante, se RECOMIENDA (en el momento en que se preparó este documento) el Algoritmo de firma digital de curva elíptica (ECDSA) con una longitud de clave de por lo menos 256 bit en combinación con SHA-256.

Cuando se aplica el algoritmo de firma ECDSA resulta un par de enteros positivos (`r,s`). Esta firma debe almacenarse en formato en bruto en el sello. La longitud de bit de `r` y `s` respectivamente corresponde a la longitud de clave. Por lo tanto, para ECDSA-256, por ejemplo, la longitud de `r` y `s` es como máximo 256 bit = 32 byte cada uno. La firma DEBE almacenarse calculando la representación del entero sin firma de `r` y `s`, potencialmente añadiendo ceros iniciales para ajustar `r` y `s` a sus longitudes previstas (i.e., la longitud de clave), y agregando el valor resultante de `s` al de `r`. En el Apéndice B figura una conversión entre la ASN.1 y el formato en bruto de (`r,s`).

El algoritmo de condensación empleado en la firma no está codificado en la estructura. El algoritmo de condensación debe deducirse de la longitud de bits del orden del punto de base generador de la curva que se emplea para crear la firma, tanto para la firma como para la verificación.

Para deducir el algoritmo de condensación, deberían seguirse los siguientes pasos:

- Sea τ la longitud de bits del orden del punto de base o generador G. El orden η se puede recuperar de los ECParameters del certificado del firmante y da el valor de τ.

- τ DEBE ser menor o igual que la longitud de salida 'l' del algoritmo de condensación ($\tau <= l$)

Algoritmo de condensación	Si cumple
SHA-224	τ <=224
SHA-256	(τ <=256) AND (τ >224)
SHA-384	(τ <=384) AND (τ >256)
SHA-512	(τ <=512) AND (τ >384)

2.5 Relleno

Si el encabezamiento, el mensaje y la firma conjuntamente no llenan el espacio disponible del código de barras, se AGREGARÁN caracteres de relleno después de la firma. En todas las normas pertinentes de todas las simbologías de códigos de barras bidimensionales se definen métodos para rellenar, y el relleno DEBE ajustarse a esas definiciones.

2.6 Codificación C40 de cadenas

A fin de usar menos espacio en la codificación de los caracteres alfanuméricos y el símbolo de relleno <, se emplea el esquema de codificación C40, según se define en [ISO/IEC 16022]. A continuación, se describe la forma en que se utilizan estas definiciones en el entorno actual. Las dos definiciones siguientes se aplican para los elementos del documento y su codificación digital:

a) Las cadenas constan únicamente de letras mayúsculas, números, <SPACE>, y el símbolo '<'. Este último se usa como símbolo de relleno para la zona de lectura mecánica (ZLM) de los documentos de viaje. Si '<' figura en la cadena, todos los casos de '<' se sustituyen por <SPACE> antes de la codificación. Las cadenas NO DEBEN contener ningún otro símbolo.

b) En la cadena de longitud L, la longitud (i.e., el número de bytes) de la codificación digital correspondiente es el número par menor que es mayor o igual a L.

En los cálculos siguientes, el valor de byte y el equivalente entero sin firma correspondiente se convierten implícitamente. Por ejemplo, el valor de un byte se define mediante una fórmula con aritmética de enteros en valores enteros.

2.6.1 Codificación

La codificación de una cadena de caracteres en una secuencia de bytes funciona de la manera siguiente: primero, la cadena se agrupa en tuplas de tres caracteres y cada carácter se sustituye por el valor C40 correspondiente conforme a la Tabla 2, lo cual genera una tripla `(U1,U2,U3)`. Seguidamente, para cada tripla, se calcula el valor

```
U = (1600 * U1) + (40 * U2) + U3 + 1
```

El resultado se encuentra en el intervalo de 1 a 64 000, obteniéndose un valor entero de 16-bit sin firma. Este valor de 16-bit `I16` se agrupa en dos bytes:

```
Byte 1 = (I16) div 256

Byte 2 = (I16) mod 256
```

donde `div` denota la división de enteros (sin resto), y `mod` denota la operación de módulo. Nótese que estas operaciones pueden implementarse mediante el desplazamiento de bits.

Tabla 2. Cuadro de codificación C40 y correspondencia a ASCII

Valor C40	*Carácter*	*Valor ASCII*	*Valor C40*	*Carácter*	*Valor ASCII*
0	Shift 1	n/a	20	G	71
1	Shift 2	n/a	21	H	72
2	Shift 3	n/a	22	I	73
3	<SPACE>	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 Decodificación

La codificación puede invertirse fácilmente. En un par dado de bytes, `(I1,I2)` denotan sus valores enteros sin firma. El valor de 16-bit `I16` se recalcula como

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

La tripla `(U1,U2,U3)` puede recalcularse usando:

```
U1 = (V16 – 1) div 1600

U2 = (V16 - (U1*1600) - 1) div 40

U3 = V16 - (U1*1600) – (U2*40) - 1
```

Aquí nuevamente, `div` denota división de enteros. Los caracteres pueden decodificarse a partir de la tripla `(U1, U2, U3)` buscando simplemente en la Tabla 2 los valores correspondientes.

2.6.3 Relleno

La definición anterior estará bien definida solamente si la longitud de la cadena que debe codificarse es múltiplo de tres. Al igual que en las definiciones de relleno de [ISO/IEC 16022], se aplican las reglas de relleno siguientes:

a) Si quedan dos valores C40 (=dos caracteres) al final de una cadena, estos dos valores C40 se completan en una tripla con el valor C40 0 (Shift 1). La tripla se codifica conforme a la definición anterior.

b) Si queda un valor C40 (=un carácter), entonces el primer byte tiene el valor `254dec (0xFE)`. El segundo byte es el valor del esquema de codificación ASCII de DataMatrix del carácter correspondiente al valor C40. Nótese que el esquema de codificación ASCII en DataMatrix para un carácter ASCII en el intervalo 0-127 es el carácter ASCII más 1.

3. USO DEL SELLO DIGITAL

En esta sección se proporciona una descripción genérica del uso del sello digital, que se aplica a visados y documentos de viajes de emergencia. Los requisitos específicos se definen en los perfiles correspondientes.

3.1 Reglas sobre contenido y codificación

3.1.1 Encabezamiento

La codificación del encabezamiento de los sellos digitales se ajusta a la sección 2.2. El valor de los últimos 2 bytes para la referencia de la definición de los elementos del documento y la categoría del tipo de documento depende del perfil del documento específico. La categoría del tipo de documento debe ser un número impar para los perfiles de la OACI. PUEDEN utilizarse números pares para perfiles nacionales no especificados por la OACI.

3.1.2 Elementos del documento codificados en el sello digital

El elemento del documento que DEBE almacenarse en el sello es la zona de lectura mecánica (ZLM):

El sello digital CODIFICARÁ la ZLM del documento. La ZLM puede ser de cualquiera de los tipos especificados en el Doc 9303. No obstante, los perfiles de documentos específicos PUEDEN restringir los tipos de ZLM admisibles.

Cada perfil de documento PUEDE definir campos REQUERIDOS y campos OPCIONALES.

3.1.3 Reglas de codificación para los elementos del documento

La codificación de los elementos del documento depende de la referencia de la definición de los elementos del documento en combinación con la categoría del tipo de documento. Los valores específicos se definen en los correspondientes perfiles del documento.

3.2 Firmante del código de barras y creación del sello

A fin de facilitar la verificación de los sellos digitales, en esta especificación se utiliza la Infraestructura de clave pública (PKI) de la Autoridad de certificación de firma de país (CSCA) para expedir y distribuir certificados y listas de revocación de certificados (CRL). En el Doc 9303-12, se proporciona información detallada sobre perfiles de certificados.

3.2.1 Arquitectura del sistema de firmante del código de barras

El firmante del código de barras recibe datos de un sistema de personalización del documento para codificar el sello digital, y utiliza una clave de firma para firmarlo. En la Figura 2 se ilustra un posible escenario de implementación con firmante del código y su cliente, el sistema de personalización del documento.

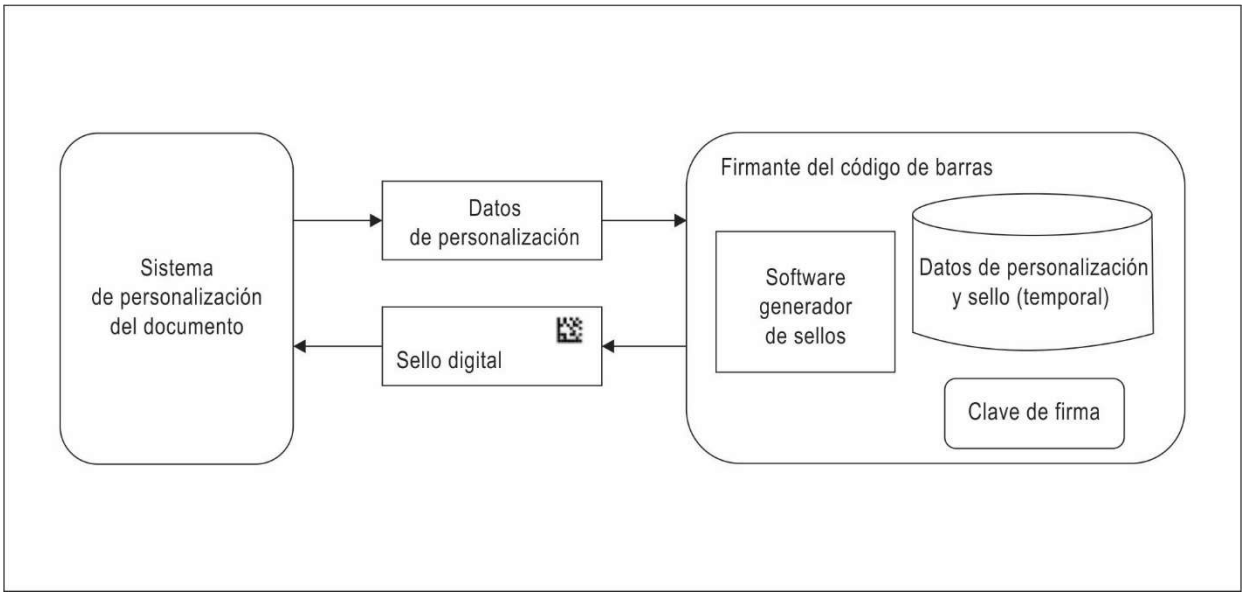

Figura 2. Personalización del documento: escenario con firmante del código de barras centralizado

El software y los datos siguientes constituyen la base del firmante del código de barras:

- El *software generador de sellos* produce sellos digitales conforme a la norma presente. Recibe los datos de personalización enviados por el cliente, firma dichos datos con una clave de firma privada y codifica los datos de personalización y la firma en un código de barras. Los datos de personalización y el sello digital son los datos de entrada y de salida, respectivamente, del software generador de sellos. Estos datos deben almacenarse temporalmente en el firmante del código de barras mientras se está generando el sello.

- Las *claves de firma* (clave privada y pública) se usan para firmar y verificar el sello digital. La clave de firma privada es el dato más crítico del firmante del código de barras.

Dependiendo del escenario de implementación, no siempre es estricta la distinción entre el sistema de personalización del documento y el firmante del código de barras. Por ejemplo, el firmante del código de barras puede ser parte del sistema de personalización en una embajada. Una posibilidad es ampliar el sistema de personalización para incluir la generación de la firma y almacenar las claves de firma en una tarjeta inteligente dentro de la embajada. Otra posibilidad es crear un firmante del código de barras central en el país de origen y permitir su conexión con las embajadas mediante un canal seguro. Por último, está la posibilidad de que en algunas embajadas no se personalicen documentos y, en este caso, el sistema de personalización podría establecerse también en el país de origen e integrarse con el firmante del código de barras.

El firmante del código de barras es un componente altamente crítico ya que produce la firma. La firma permite verificar la integridad de los datos del código de barras, i.e., si se han manipulado los datos, y su autenticidad, i.e., si los ha expedido una entidad autorizada.

Para alcanzar un nivel de seguridad suficientemente elevado, se RECOMIENDA, que el firmante del código de barras sea un servicio central y no uno que deba implementarse en cada embajada, salvo en los casos en que, por motivos operacionales, técnicos o logísticos, sea imposible instaurar un servicio centralizado. De este modo las medidas de seguridad se concentran en un perímetro limitado, teniendo en cuenta al mismo tiempo las mejores prácticas para garantizar la capacidad de recuperación y la continuidad de las operaciones. El firmante del código de barras ALMACENARÁ de manera segura las claves de firma privadas.

3.2.2 Seguridad del sistema de firma del código de barras

El alojamiento y la gestión del sistema de firma del código de barras DEBERÍAN ajustarse a las mejores prácticas de seguridad en las áreas siguientes: seguridad física; infraestructura de servidor y de red; procesos de desarrollo y apoyo del sistema; control de acceso; y seguridad de las operaciones. Si el firmante del código de barras es un sistema central, se RECOMIENDA que el perímetro del firmante del código de barras se ajuste a [ISO/IEC 27002], para así garantizar el cumplimiento de estas mejores prácticas de seguridad.

4. REFERENCIAS (NORMATIVAS)

[ISO/IEC 16022] ISO/IEC 16022 Tecnología de la información — Técnicas automáticas de identificación y de captura de datos — Especificación de simbología de código de barras, Data Matrix, 2006

[ISO/IEC 18004] ISO/IEC 18004:2006: Tecnología de la información — Técnicas automáticas de identificación y de captura de datos — Especificación de simbología de código de barras, Código QR, 2015

[ISO/IEC 24778] ISO/IEC 24778:2008: Tecnología de la información — Técnicas automáticas de identificación y de captura de datos — Especificación de simbología de código de barras, Código Aztec, 2008

[ISO/IEC 27002] ISO/IEC 27002: Tecnología de la información — Técnicas de seguridad — Código de buenas prácticas para la gestión de la seguridad de la información, 2013

[ISO/IEC 15415] ISO/IEC 15415:2011: Tecnología de la información — Técnicas automáticas de identificación y de captura de datos — Especificación de prueba de calidad de impresión de los símbolos del código de barras — Símbolos bidimensionales, 2011

[X.690] ITU-T X.690 2008, REDES DE DATOS Y COMUNICACIONES DE SISTEMAS ABIERTOS – Aspectos de redes y sistemas OSI — Notación de Sintaxis Abstracta Uno (ASN.1) – Tecnología de la información — Reglas de codificación de ASN.1

— — — — — — — —

Apéndice A de la Parte 13

EJEMPLO DE CASO DE USO (INFORMATIVO)

En esta sección se describe en términos generales el uso del sello digital para proteger documentos no electrónicos. El caso de uso específico que se considera aquí es la protección de un documento de visado, según se ilustra en la Figura A.1. Aunque para otros casos de uso los detalles técnicos pueden ser diferentes, siempre se aplican los mismos principios generales.

El flujo general del proceso puede dividirse en tres etapas. Como prerrequisito, deben generarse los Certificados de firmante de visados (VSC). Seguidamente, se generan los sellos digitales que, más adelante, se validan.

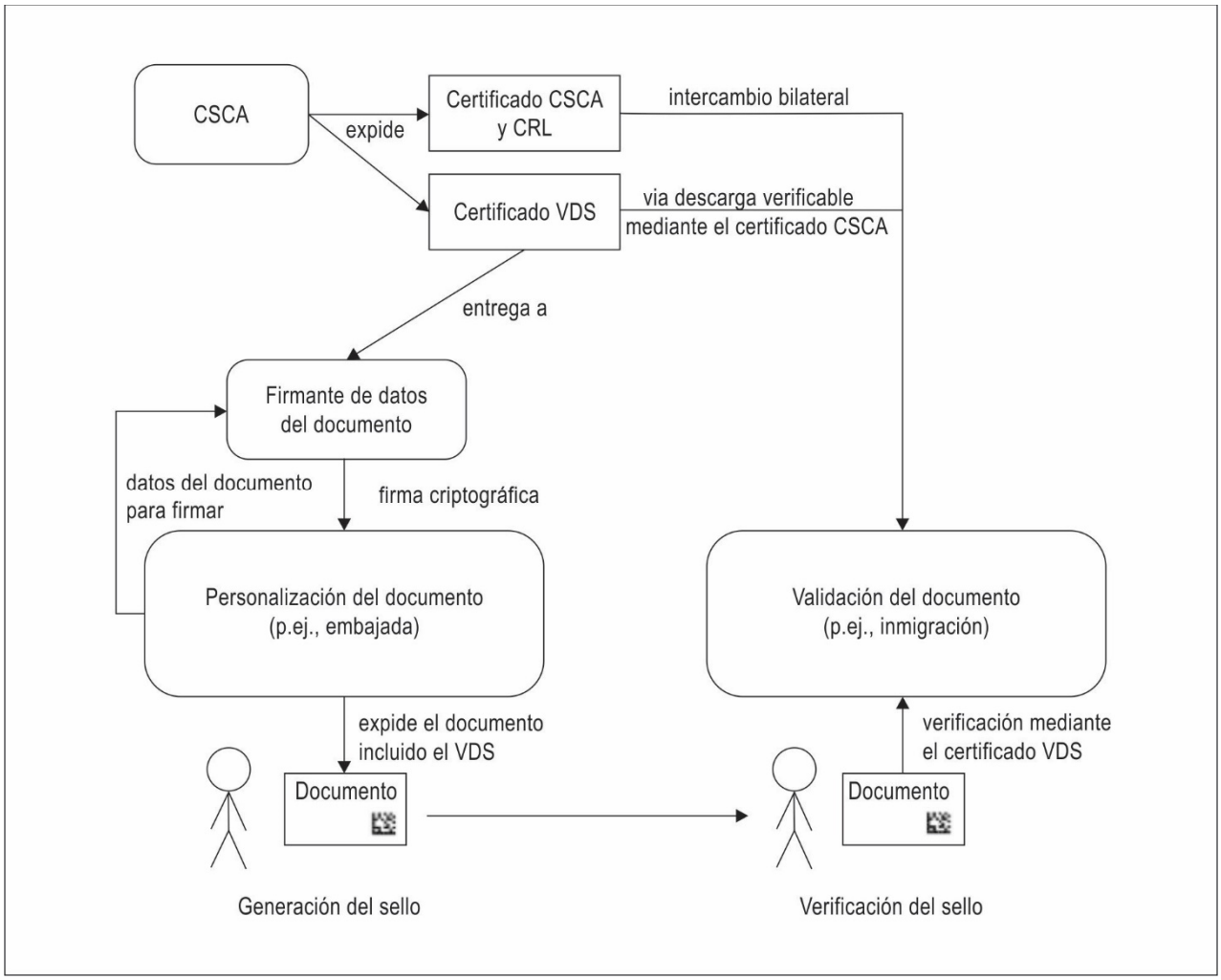

Figura A.1. Ejemplo de caso de uso de VDS

A.1 PRERREQUISITO: GENERACIÓN DEL CERTIFICADO DE FIRMANTE DE VISADO

La PKI de firma de visados se basa en la PKI establecida para pasaportes electrónicos que define la OACI. Primero está la Autoridad de certificación firmante del país (CSCA). La CSCA publica un certificado CSCA con la clave pública de la CSCA. Para establecer confianza entre los países, este certificado CSCA se distribuye de manera fiable mediante intercambio bilateral o por medio de listas maestras.

El firmante de visados es la entidad que efectivamente firma los sellos digitales. La CSCA expide los VSC y, por ende, pueden verificarse mediante el certificado CSCA.

A.2 GENERACIÓN DEL SELLO DIGITAL

El sello digital se genera en dos etapas:

a) Los interesados solicitan un visado en la embajada del lugar donde residen. La embajada registra los datos del solicitante y verifica si cumple los requisitos para recibir un visado. Si cumple los requisitos, la embajada envía al firmante de visados (VS) una representación digital de los datos registrados. El VS puede ser (1) una entidad central situada en el país que expide el visado, en este caso la embajada se conecta con el VS mediante un canal seguro, o (2) distintas entidades descentralizadas situadas en cada embajada y, en este caso, se utilizan, por ejemplo, tarjetas inteligentes con claves criptográficas que se adjuntan directamente al sistema de personalización. En ambos casos, el VS firma criptográficamente los datos registrados.

b) Para firmar, el firmante de visados usa un par de claves de una clave privada y una clave pública. La firma efectiva se realiza con la clave privada, en tanto de la clave pública se almacena en un certificado de firmante de visados. La firma resultante se envía de vuelta al sistema de personalización de visados si el firmante de visados no es una parte local del sistema de personalización, se imprime en el adhesivo del visado y se adjunta y se adhiere al pasaporte del solicitante.

A.3 VALIDACIÓN DEL SELLO DIGITAL

Cuando los solicitantes ingresan al país expedidor, presentan sus visados a la Autoridad de validación de visados (VVA), p.ej., la autoridad de control de inmigración del país expedidor. La VVA verifica la autenticidad y la integridad del sello digital en el visado mediante la validación de la firma del sello, y compara la información impresa en el adhesivo del visado y en el pasaporte con la información digital almacenada en el sello. Para verificar la firma del sello, se identifica el Certificado-VS correspondiente utilizando el identificador almacenado en el encabezamiento del sello digital y, seguidamente, la clave pública del Certificado-VS. Como se describe en los párrafos precedentes, la validez del Certificado-VS propiamente tal puede verificarse mediante el Certificado-CSCA.

Observación

Dado que todos los certificados están públicamente disponibles, la validez del visado puede ser verificada por cualquier otra entidad pertinente, no solamente el Estado expedidor. De este modo, se consideran los casos de uso por asociaciones de países en que un país expide visados para otro país (como en el caso de la Unión Europea). Otro caso de uso es el de la verificación de visados por las líneas aéreas antes de abordar un avión.

Observación

Los criterios para determinar si un documento de visado es de confianza o no, basándose en el sello digital y las ZLM del visado y el pasaporte, se definen en una política de validación.

— — — — — — — —

Apéndice B de la Parte 13

CONVERSIÓN DE FORMATOS DE FIRMA ECDSA (INFORMATIVO)

B.1 CODIFICACIÓN DE ENTEROS EN BER/DER

Los enteros se codifican en concordancia con las Reglas de codificación básica (BER) y las Reglas de codificación distinguida (DER), en el formato de codificación *big endian* con firma de longitud mínima, después de lo cual se aplica el esquema Rótulo-Longitud-Valor (TLV). Se distinguen los casos siguientes:

a) Si el valor entero es positivo, y el bit más significativo (MSB) es cero en la representación de enteros sin firma mínima, entonces la representación de enteros sin firma tendrá la forma siguiente, que corresponde al valor BER/DER:

`|0bbbbbbb| ...`

b) Si el valor entero es positivo, y el MSB es uno en la representación de enteros sin firma mínima, i.e., tienen la forma `|1bbbbbbb|` ... , entonces se pone un byte con ceros en frente y el valor BER/DER es:

`|00000000|1bbbbbbb| ...`

c) Si el valor entero es negativo, entonces ese valor se codifica como el complemento a dos, por ejemplo, con la representación de enteros mínima sin firma, invirtiendo y agregando uno. Seguidamente, el MSB se pone a uno. Por ejemplo, para -25357, la representación de enteros mínima sin firma es:

`|0110 0011|0000 1101|`

Esto se invierte como sigue:

`|1001 1100|1111 0010|`

Se añade uno:

`|1001 1100|1111 0011|`

para obtener como resultado el valor BER/DER. Nótese que el hecho de que el número sea negativo puede inferirse directamente porque el MSB (aquí totalmente a la izquierda) es uno.

Finalmente, uno da un valor TLV al poner dos bytes frente a los valores BER/DER codificados más arriba. El primer byte corresponde al rótulo con la constante `0x02`. El segundo byte contiene la longitud (i.e., el número de bytes) del valor BER/DER codificado siguiente. La decodificación puede realizarse simplemente, por ejemplo, distinguiendo conforme al MSB, si hay un entero negativo o positivo codificado y aplicando los pasos anteriores en orden inverso.

B.2 EJEMPLO

En la Tabla B.1 figuran ejemplos de enteros codificados en BER/DER.

Tabla B.1. Ejemplos de codificación BER/DER para algunos valores enteros

Valor (dec)	*´Rótulo (hex)*	*Longitud (hex)*	*Valor (hex)*	*Valor (binario)*
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 FIRMAS ECDSA EN ASN.1/DER

La descripción ASN.1 de una firma ECDSA es

```
Signature ::= SEQUENCE {
         r INTEGER, s INTEGER
}
```

Esta secuencia se codifica conforme a DER como una tripla TLV con el rótulo `0x30`, la longitud como el número de bytes del valor siguiente, y el valor como la concatenación de las triplas TLV de la codificación `r` añadida a la codificación de `s`.

En la Tabla B.2 figuran dos secuencias, a modo de ejemplo. Obviamente, los enteros `r y s` de una firma ECDSA son considerablemente mayores en la práctica.

Tabla B.2. Secuencias de dos enteros codificadas en DER

Enteros		*Secuencia de TLV*		
R	***S***	***Rótulo***	***Longitud***	***Valor***
127	1	0x30	0x06	0x02 0x01 0x7F 0x02 0x01 0x01
128	127	0x30	0x07	0x02 0x02 0x00 0x80 0x02 0x01 0x7F

Nótese que `r` y `s` son siempre enteros positivos para las firmas ECDSA. Por lo tanto, para la conversión de firma en bruto a DER, primero debe dividirse la firma en bruto por la mitad para obtener `r` y `s` individualmente y luego, codificarse como una secuencia ASN.1 codificada en DER, conforme a la definición precedente. Por el contrario, para la decodificación de firma ECDSA a DER, primero debe decodificarse la secuencia, extraer la representación de enteros sin firma de `r` y `s` y dar a `r` y `s` una representación de longitud fija (= longitud de tamaño de clave), quitando o agregando bytes cero iniciales (por ejemplo, en el caso de ECDSA-256, tanto `r` como `s` deben tener una longitud de 256 bit = 32 byte) y añadiendo el valor resultante `s` al valor resultante `r`.

— — — — — — — —

Apéndice C de la Parte 13

EJEMPLOS PARA CODIFICACIÓN C40 (INFORMATIVO)

C.1 EJEMPLO 1

Se supone que debe codificarse la cadena “XK<CD”. Por definición, todos los casos de '<' se sustituyen por <SPACE> antes de la codificación. La cadena resultante es entonces “XK CD”, i.e. “XK<SPACE>CD” (un espacio insertado). La codificación/decodificación C40 de la cadena “XK<SPACE>CD” figura en la Tabla C.1.

Tabla C.1. Ejemplo de codificación/decodificación de la cadena “XK<SPACE>CD”

Operación	***Resultado***			
cadena original	“XK<SPACE>CD”			
agrupamiento en triplas	(X, K, <SPACE>)		(C, D,)	
sustitución por valores C40 y relleno	(37, 24, 3)		(16, 17, relleno)	
cálculo del valor entero de 16 bit	60164		26281	
	Byte 1 (div)	**Byte 2 (mod)**	**Byte 1 (div)**	**Byte 2 (mod)**
secuencia de byte resultante (decimal)	235	4	102	169
secuencia de byte resultante (hex)	0xEB	0x04	0x66	0xA9

C.2 EJEMPLO 2

Se supone que debe codificarse la cadena “XKCD”. La cadena consta únicamente de letras mayúsculas. Su codificación/decodificación figura en la Tabla C.2.

Tabla C.2. Ejemplo de codificación/decodificación de la cadena "XKCD"

Operación	***Resultado***			
cadena original	“XKCD”			
agrupamiento en triplas	(X, K, C)		(D, ,)	
sustitución por valores C40 y relleno	(37, 24, 16)		(liberar C40 y codificar en ASCII)	
cálculo del valor entero de 16 bit	60177			
	Byte 1 (div)	***Byte 2 (mod)***	***Byte 1***	***Byte 2***
secuencia de byte resultante (decimal)	235	11	254	69
secuencia de byte resultante (hex)	0xEB	0x11	0xFE	0x45

— — — — — — — —

Apéndice D de la Parte 13

REGLAS DE LA POLÍTICA DE VALIDACIÓN (INFORMATIVO)

La política de validación es un conjunto de reglas de validación que permiten determinar la validez del sello en un documento. La aplicación de esta política de validación genera una indicación del estado con uno de los valores siguientes:

a) VÁLIDO (VALID). Se han confirmado la autenticidad y la integridad del sello. En este caso, autenticidad significa que los datos del sello fueron efectivamente firmados por un firmante de códigos de barras del país expedidor del documento, y que el certificado del firmante del código de barras correspondiente es válido. Integridad significa que los datos de la ZLM del documento sellado no han sido modificados y que el sello digital no se traspasó desde el documento al que se adjuntó originalmente.

b) INVÁLIDO (INVALID). El sello no se reconoce como válido y se requiere investigar más a fondo. La invalidación puede deberse a las tres razones siguientes:

   1) *Fraude/Falsificación*. Incluye personalización no autorizada de un documento, con un autoadhesivo en blanco robado, cambios en los datos de personalización de un documento basándose en un autoadhesivo original, o traspasando un autoadhesivo de código de barras desde un documento robado (por ejemplo, pasaporte) a otro documento, u otras falsificaciones

   2) *Daños/Deterioro*. El código de barras no puede decodificarse debido a desgaste, deterioro o manchas.

   3) *Errores desconocidos y/o imprevistos*. Esto incluye errores imprevisibles, por ejemplo, debido a fallas en la implementación del software utilizado para decodificar, o codificación errónea durante la personalización.

A la indicación de estado INVALID, se añaden subindicaciones del estado que señalan las razones de la invalidación del sello. Como la posibilidad de fraude depende de estas razones, se recomienda vincular las indicaciones y subindicaciones del estado con los tres niveles de confianza: “confiable”, “posibilidad mediana de fraude”, y “posibilidad alta de fraude”. La correspondencia recomendada se ilustra en la Tabla D.1.

En esta política de validación genérica se consideran siempre las preguntas siguientes:

a) ¿Es válido el sello digital visible?

b) ¿Es válida la ZLM del documento?

c) ¿La ZLM del documento coincide con el sello digital visible?

A continuación, figuran las reglas de validación para cada tipo de control, una lista de criterios de validación, los resultados previstos para cada criterio, y las subindicaciones del estado resultantes.

Validación del sello digital visible

1. Validación del formato

    - si el formato de codificación físico no se ajusta a la especificación, o si hay errores debido a ruido físico que no pueden corregirse, el estado es INVALID con la subindicación de error de lectura READ_ERROR,

    - si el formato de codificación (i.e, las estructuras del sello que constan de encabezamiento, zona de mensaje y zona de firma, o la codificación binaria/C40) no se ajusta a la especificación, o

    - si se desconocen los valores previstos en el encabezamiento, o

    - si falta un campo obligatorio en la zona de mensaje, o

    - si el formato de un campo en la zona de mensaje no se ajusta a la especificación de la versión definida en el encabezamiento, entonces el estado es INVALID con la subindicación de formato incorrecto WRONG_FORMAT, en cualquier otro caso, continuar, o

    - si en la zona de mensaje hay un campo desconocido, entonces debería ponerse una subindicación de elemento desconocido UKNOWN_FEATURE. La indicación del estado será VALID o INVALID dependiendo de la validez de la firma verificada conforme a los pasos siguientes. Nótese que, si la firma es válida, la presencia de un solo elemento desconocido no debe violar la validez del sello.

2. Validación de la firma

    - si el certificado de firmante del código de barras al que se hace referencia en el encabezamiento del sello no está presente, el estado indica INVALID con la subindicación de certificado desconocido UNKNOWN_CERTIFICATE,

    - si el certificado de firmante del código de barras al que se hace referencia en el encabezamiento del sello no tiene la firma de la CSCA, o falla la verificación de la firma, el estado es INVALID con la subindicación de certificado no confiable UNTRUSTED_CERTIFICATE,

    - si el certificado de firmante del código de barras contiene una extensión del tipo de documento y el contenido del código de barras incluye una ZLM, y el tipo de documento de la ZLM no está contenido en la extensión del tipo de documento, el estado es INVALID con la subindicación de tipo de documento inválido INVALID_DOCUMENTTYPE,

    - si el certificado de firmante del código de barras al que se hace referencia en el encabezamiento del sello está expirado, el estado es INVALID con la subindicación de certificado expirado EXPIRED_CERTIFICATE,

    - si el certificado de firmante del código de barras al que se hace referencia en el encabezamiento del sello está revocado, el estado es INVALID con la subindicación de certificado revocado REVOKED_CERTIFICATE,

    - si la verificación de la firma del encabezamiento y la zona de mensaje que usa el certificado del firmante del código de barras al que se hace referencia en el encabezamiento del sello falla, el estado es INVALID con la subindicación de firma inválida INVALID_SIGNATURE,

    - en cualquier otro caso, continuar.

3. Validación del expedidor

    - si la CSCA no es de confianza para el Sistema de validación de códigos de barras en su dominio de confianza, el estado es INVALID con la subindicación de certificado no confiable UNTRUSTED_CERTIFICATE, en cualquier otro caso, continuar.

Las reglas de validación precedentes permiten una comparación entre los datos almacenados en el sello y los datos almacenados en la ZLM del documento. Además, podría llevarse a cabo una inspección manual de los datos que están almacenados en el sello e impresos en el documento, pero que no están presentes en la ZLM del documento.

Tabla D.1. Niveles de confianza recomendados de la Política de documentos

Indicación de estado	***Subindicación de estado***	***Nivel de confianza***
VALID	-	*confiable*
	UNKNOWN_FEATURE	
INVALID	READ_ERROR EXPIRED_CERTIFICATE	*posibilidad mediana de fraude*
	WRONG_FORMAT	*posibilidad elevada de fraude*
	UNKNOWN_CERTIFICATE	
	UNTRUSTED_CERTIFICATE	
	INVALID_DOCUMENTTYPE REVOKED_CERTIFICATE	
	INVALID_SIGNATURE	

— FIN —

ISBN 978-92-9275-547-8