OACI

Doc 9303

Documents de voyage lisibles à la machine

Huitième édition (Révision), 2021

Partie 13 : Cachets numériques visibles

Approuvé par la Secrétaire générale et publié sous son autorité

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

OACI

Doc 9303

Documents de voyage lisibles à la machine

Huitième édition (Révision), 2021

Partie 13 : Cachets numériques visibles

Approuvé par la Secrétaire générale et publié sous son autorité

ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

Publié séparément en français, en anglais, en arabe, en chinois, en espagnol
et en russe par l'ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE
999, boul. Robert-Bourassa, Montréal (Québec) H3C 5H7 Canada

Le site www.icao.int/security/mrtd permet de télécharger les documents et d'obtenir des renseignements supplémentaires.

Huitième édition (Révision), 2021

Doc 9303, *Documents de voyage lisibles à la machine*
Partie 13 — *Cachets numériques visibles*

Commande nº : 9303P13
ISBN 978-92-9265-529-7

AMENDEMENTS

La parution des amendements est annoncée dans les suppléments au *Catalogue des produits et services*. Le Catalogue et ses suppléments sont disponibles sur le site web de l'Organisation (www.icao.int). Le tableau ci-dessous est destiné à rappeler les divers amendements.

RELEVÉ DES AMENDEMENTS ET DES RECTIFICATIFS

AMENDEMENTS		
N°	Date	Inséré par

RECTIFICATIFS		
N°	Date	Inséré par

TABLE DES MATIÈRES

1. PORTÉE

La présente Partie 13 du Doc 9303 fournit les spécifications applicables au cachet numérique, qui permet de garantir l'authenticité et l'intégrité de documents non électroniques de façon relativement peu coûteuse mais hautement sécurisée à l'aide de la cryptographie asymétrique. Les renseignements figurant sur le document non électronique sont signés selon un procédé cryptographique, puis la signature est codée sous la forme d'un code à barres bidimensionnel et imprimée sur le document lui-même. Cette méthode – le *cachet numérique visible* – apporte les avantages suivants :

- *Asymétrie*. Étant donné qu'on utilise la cryptographie asymétrique, l'apposition d'un cachet numérique est bien plus onéreuse que la délivrance d'un document protégé par un cachet numérique. Ainsi, bien que le coût de la délivrance d'un document reste très bas, contrefaire ou falsifier les données de personnalisation de ce même document coûte extrêmement cher.

- *Personnalisation*. Chaque cachet numérique vérifie les renseignements imprimés sur le document physique, et se rattache par conséquent au titulaire du document. Il n'existe pas à proprement parler de cachet numérique « vierge », qui pourrait être perdu ou volé.

- *Vérification facilitée*. Il n'est pas nécessaire d'avoir suivi une formation pour être en mesure de vérifier un document protégé par un cachet numérique à l'aide d'un dispositif peu coûteux, par exemple une application installée sur un téléphone intelligent. En outre, étant donné qu'une signature numérique est de nature binaire, on peut aisément distinguer le document authentique d'une version falsifiée.

S'il représente une nette amélioration sur le plan de la sécurité pour les documents (habituellement sur support papier) dépourvus de puce, le cachet numérique a ses limites par rapport aux documents à puce. Sa capacité de stockage n'excède pas quelques kilo-octets, et ni les données, ni les clés ou schémas cryptographiques du cachet numérique ne peuvent être actualisés sur des documents existants. Autrement dit, on ne peut pas tirer parti de l'agilité cryptographique. Le cachet numérique ne protège pas du clonage, ne comprend pas de fonction de protection de la confidentialité, et peut, davantage que les documents à puce, faire l'objet d'erreurs de lecture due à l'usure. En outre, la polyvalence des puces cryptographiques permet la mise en œuvre de fonctionnalités supplémentaires, telles que les schémas de signature, l'authentification du terminal, les méthodes de double authentification sur la base des secrets partagés, soit un NIP, ou des protocoles cryptographiques sécurisés fondés sur des schémas symétriques. Étant donné que les codes à barres bidimensionnels ne peuvent pas remplacer les caractéristiques fonctionnelles et les éléments de sécurité des puces, il faut que, dans la mesure du possible, les documents de voyage soient dotés de puces.

2. CODAGE DU CACHET NUMÉRIQUE

Un cachet numérique visible (VDS) est une structure de données signée selon un procédé cryptographique qui contient les caractéristiques du document, codée sous la forme d'un code à barres bidimensionnel et imprimée sur un document. La présente section décrit le codage et la structure d'un cachet numérique visible.

2.1 Format du code à barres et critères d'impression

La présente spécification définit la méthode de codage des données en un flux d'octets. Seuls les codes à barres bidimensionnels dont la symbologie répond aux spécifications d'une norme ISO DEVRONT être utilisés, par exemple les codes Data Matrix [ISO/IEC 16022], les codes Aztec [ISO/IEC 24778] et les codes QR [ISO/IEC 18004].

Le code à barres DEVRAIT être imprimé de sorte à permettre aux appareils de lecture (c'est-à-dire aux téléphones intelligents et lecteurs du commerce) de décoder le code à barres avec des résultats fiables ; il FAUDRAIT notamment prendre en considération la norme [ISO/IEC 15415] au moment d'évaluer la qualité d'impression. Les critères de qualité de l'impression et de la lecture qui en découlent dépendent du document ; des détails propres à certains scénarios d'application PEUVENT être indiqués dans un profil. Étant donné que la qualité de l'impression et de la lecture a une incidence sur les taux d'erreur et sur la fiabilité de la vérification du cachet numérique, ces critères de qualité DEVRAIENT garantir qu'on puisse vérifier de manière fiable le code à barres contenant le cachet et toutes les caractéristiques obligatoires du document. Le contraste du symbole du code à barres est un autre critère crucial, car il arrive que le cachet numérique soit imprimé sur un papier de sécurité coloré (vert, par exemple).

Dans le cas où l'on utilise des imprimantes à jet d'encre classique, il est RECOMMANDÉ que la longueur du côté d'un module (bloc de code à barres bidimensionnel) soit d'au moins 0,3386 mm, ce qui correspond à 4 points par côté du module (soit 16 points par module) sur une imprimante dont la résolution est de 300 ppp, ou 8 points par côté (soit 64 points par module) sur une imprimante à 600 ppp de résolution. Une taille d'impression moindre PEUT être acceptable, si on utilise des imprimantes à haute résolution ou à des imprimantes à laser. Pour ce qui est de la position du code à barres sur le document, voir les parties du Doc 9303 sur le sujet.

Une fois codé, le code à barres se compose d'un en-tête (voir la section 2.2), d'une zone de message (voir la section 2.3) et d'une zone de signature (voir la section 2.4). On trouvera une synthèse de la structure dans la Figure 1.

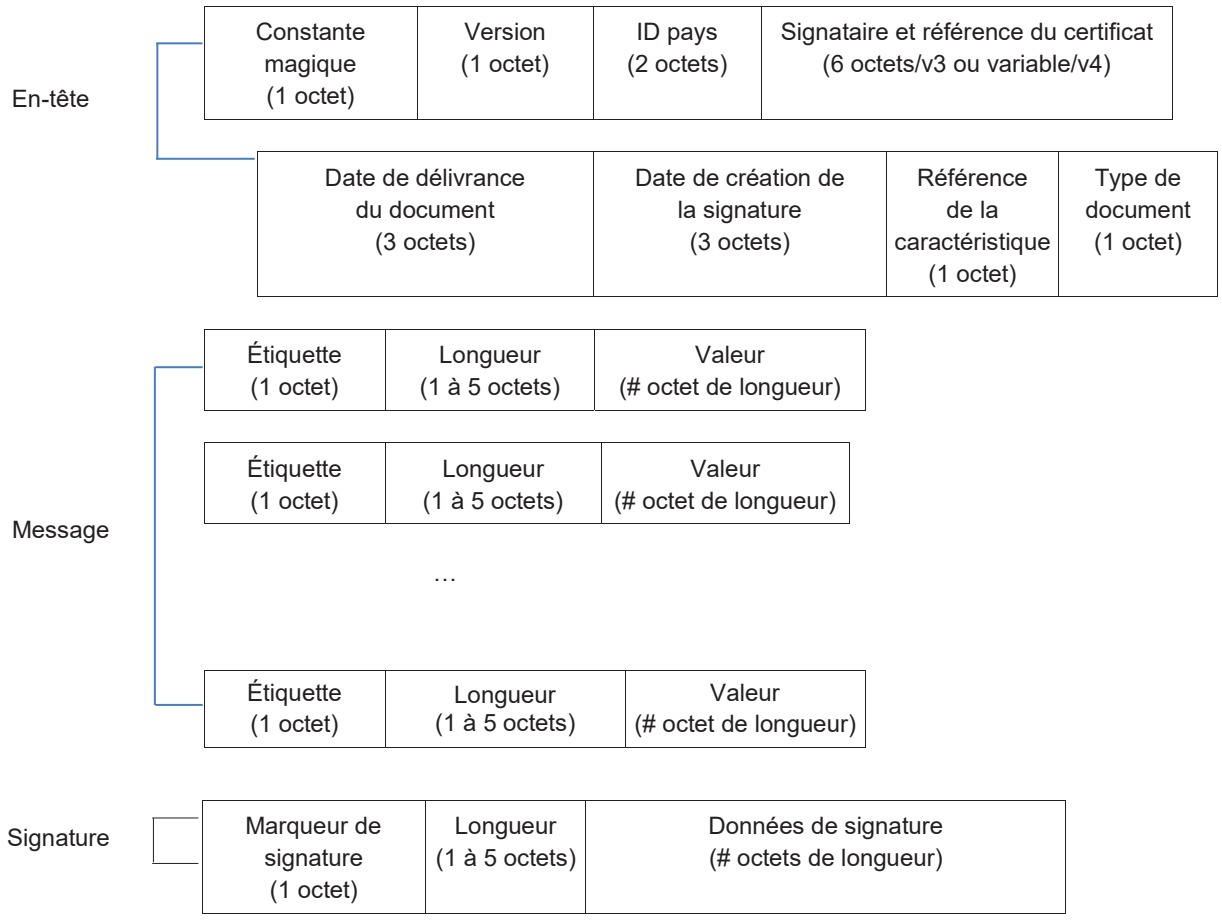

Figure 1. Structure d'un cachet numérique

2.2 En-tête

L'en-tête contient des métadonnées sur le document et le codage, comme le numéro de la version, la date de délivrance du document et la date de création de la signature.

La présente spécification définit deux versions de l'en-tête, marquées respectivement des identifiants « 3 » et « 4 ». Les versions divergent sur le plan de la définition de la référence de certificat (voir ci-après) et du codage de la longueur des caractéristiques du document (voir la section 2.3).

L'en-tête fait 18 octets de long dans la version 3 et un nombre variable d'octets dans la version 4. Le Tableau 1 donne une définition des différents éléments contenus dans l'en-tête.

Tableau 1. Format de l'en-tête

Position de départ	***Longueur (en octets)***	***Contenu***
`0x00`	1	*Constante magique*. La constante magique a une valeur fixe de `0xDC` qui indique que le code à barres se conforme à la présente spécification.
`0x01`	1	*Version*. Valeur en octet indiquant la version de la présente spécification qui est utilisée. Les versions définies dans la présente spécification sont marquées par la valeur en octet `0x02 / 0x03`, respectivement. Un nombre `n` indique qu'il s'agit de la version `n+1`, par exemple la valeur 0 correspond à la version 1.
`0x02`	2	*Pays de délivrance.* Code de trois lettres indiquant l'État ou l'organisation de délivrance. Ce code est établi dans la Partie 3 du Doc 9303. Si le code comporte moins de trois lettres, il DOIT être complété par des caractères de remplissage (« < »), par exemple le code « D » devient « D<< ». Il est codé en C40 (voir la section 2.6) sous la forme d'une séquence de deux octets.
`0x04`	6 / v	*Identifiant du signataire et référence du certificat.* Version 3 : Code de neuf lettres identifiant le signataire (du code à barres) et le certificat. Version 4 : Code à lettres de longueur variable identifiant le signataire (du code à barres) et le certificat (« v » indique la longueur totale de ce champ). Le code est codé en C40 (voir la section 2.6). En ce qui concerne le codage d'une longueur variable, voir la section 2.2.1.
`0x0A / 0x04+v`	3	*Date de délivrance du document.* Date à laquelle le document a été délivré. Codée conformément aux indications données dans la section 2.3.1.
`0x0D / 0x07+v`	3	*Date de création de la signature*. Date à laquelle la signature a été créée. Codée conformément aux indications données dans la section 2.3.1.
`0x10 / 0x0A+v`	1	*Référence de la définition des caractéristiques du document.* Code de référence renvoyant à un document qui définit le nombre et le codage des caractéristiques du document. Cette définition est indépendante pour chaque catégorie de type de document, c'est-à-dire que le même code de référence de la définition des caractéristiques du document peut avoir différentes significations en fonction des catégories. Les valeurs DOIVENT être comprises entre 01dec et 254dec.
`0x11 / 0x0B+v`	1	*Catégorie du type de document.* Catégorie du document, par exemple visa, document de voyage d'urgence, acte de naissance. Il FAUT utiliser des nombres impairs compris entre 01dec et 253dec pour les catégories de type de documents spécifiés par l'OACI.
Total	18 / 12 + v	

2.2.1 Identifiant du signataire et référence du certificat

La taille du code à barres étant limitée, il est impossible d'y stocker les certificats qui contiennent la clé publique correspondant à la signature. Par conséquent, le certificat DOIT être obtenu par une autre voie. Afin de donner au certificat et au signataire qui en fait l'objet un identifiant unique, et de lier le certificat au code à barres, une chaîne contenant l'identifiant du signataire et une référence au certificat est stockée dans l'en-tête. La chaîne est composée de deux éléments :

a) *L'identifiant du signataire* : combinaison des deux lettres du code de pays établi dans la Partie 3 du Doc 9303 du pays du signataire et de deux caractères alphanumériques qui identifient un signataire dans ledit pays. Cet identifiant DOIT être unique au signataire d'un pays donné ;

b) *La référence du certificat* :

1) pour l'en-tête version 3 : chaîne hexadécimale de cinq caractères exactement qui DOIT identifier un certificat pour un signataire donné de façon unique.

2) pour l'en-tête version 4 : chaîne hexadécimale qui consiste à concaténer :

i) deux caractères exactement qui indiquent le nombre de caractères suivants ;

ii) des caractères qui DOIVENT identifier un certificat pour un signataire donné de façon unique.

Veuillez noter que dans le cas d'utilisation spécifique des visas (voir la Partie 7 du Doc 9303), le signataire désigne le *signataire du visa*.

La référence de certificat `0 ... 0` est réservée aux mises à l'essai et NE DOIT PAS être utilisée en production.

L'identifiant du signataire (du code à barres) et la référence du certificat DOIVENT correspondre au nom distinctif (DN) et au numéro de série, respectivement, du certificat d'un signataire. Ainsi, le certificat en question bénéficie d'une identification unique, décodable dans l'en-tête.

2.2.2 Référence de la définition des caractéristiques du document et Catégorie du type de document

La combinaison de la *Référence de la définition des caractéristiques du document* et de la *Catégorie du type de document* renvoie à un ensemble de règles particulier, à l'image de la présente spécification. Le même code à barres et le même format d'en-tête peuvent être réutilisés ultérieurement dans d'autres cas de figure, mais ils renverront alors à différentes définitions des caractéristiques (c'est-à-dire à une référence qui établit la liste des renseignements contenus dans le code à barres) ou à différentes catégories de type de document. Il est ainsi possible de réutiliser les bases de codes existantes, ce qui simplifie la mise en œuvre et améliore l'interopérabilité.

Les références de définition des caractéristiques du document et les catégories du type de document pour les visas et les documents de voyage d'urgence sont définies dans les Parties 7 et 8 du Doc 9303, respectivement.

2.3 Zone de message

L'en-tête est suivi de la zone de message. On y trouve les caractéristiques du document codées selon des procédés numériques, conformément aux indications de la présente section. Peu importe leur ordre, tant que toutes les caractéristiques du document obligatoires y figurent.

Chaque caractéristique du document est précédée des éléments suivants :

- une étiquette qui indique le type de caractéristique (un octet) ;
- la longueur de la caractéristique (entre un et cinq octets).

En fonction de l'identifiant de version (dont la position de départ dans l'en-tête est `0x01`, voir le Tableau 1), il convient de distinguer deux types de codage de la longueur :

- Pour la version 3 et en-deçà, la longueur DOIT être directement codée sur un octet (cet « octet de longueur » est le deuxième octet et se situe directement à la suite de l'étiquette du message).
- Pour la version 4 et au-delà, la longueur DOIT être codée en DER-TLV conformément à la recommandation [X.690].

En ce qui concerne les visas, il est RECOMMANDÉ d'utiliser la version 4 (ou une version supérieure) et donc le codage de longueur en DER-TLV. Si l'utilisation de la version 3 (ou d'une version inférieure) et donc le codage direct de la longueur est valide, elle n'est pas encouragée.

Pour les documents de voyage d'urgence, seule la version 4 (ou une version supérieure) et donc le codage de la longueur en DER-TLV DOIT être utilisée.

2.3.1 Codage numérique des caractéristiques du document (codage binaire)

Les caractéristiques du document sont codées comme suit. On prend en compte les types fondamentaux ci-après comme blocs fonctionnels :

a) *Alphanum* : chaînes de caractères alphanumériques en haut de casse[1] (soit les lettres de A à Z, les chiffres de 0 à 9 et les espaces) ;

b) *Binaire* : séquences d'octets ;

c) *Int* : nombres entiers positifs ;

d) *Date* : dates.

Les types de base sont convertis en séquences d'octets, comme suit :

a) Les chaînes de caractères alphanumériques sont codées sous forme d'octets en codage C40 (voir la section 2.6) ;

b) Les séquences d'octets sont prises telles quelles ;

1. La restriction aux hauts de casse est due à la capacité limitée du code à barres en matière de données.

c) Pour les nombres entiers positifs, on utilise leur représentation sans signe ;

d) Une date est d'abord convertie en nombre entier positif par la concaténation du mois, du jour et de l'année (en 4 chiffres). Ce nombre entier positif est ensuite concaténé en une séquence de trois octets définis à l'alinéa c) ci-dessus.

Exemple : Prenons le 25 mars 1957. En concaténant le mois, le jour et l'année, on obtient le nombre entier `03251957`, ce qui donne les trois octets `0x31 0x9E 0xF5`.

Une caractéristique de document sous forme numérique est une séquence d'octets, organisée selon la structure suivante :

étiquette | longueur | valeur

Dans le cas présent, l'*étiquette* est un nombre entier compris entre `0 et 254dec` qui sert d'identifiant propre à la caractéristique en question. Veuillez noter que l'étiquette `255dec` sert exclusivement pour indiquer le début de la signature. La *longueur* est constituée d'un à cinq octets, conformément au codage des champs de longueur DER-TLV. Elle signale la longueur de la valeur qui va suivre. La *valeur* est un type de base converti en une séquence d'octets.

Exemple : Prenons une caractéristique de document qui code la chaîne « VISA01 », à laquelle on attribue l'étiquette 0x0A. La séquence d'octets codée en C40 (voir la section 2.6) de longueur 4 est `0xDE515826`. La caractéristique du document est ainsi la séquence d'octets `0x0A04DE515826`.

Dans le cas d'une utilisation spécifique, il faut par conséquent compléter cette définition en énumérant les caractéristiques du document qui doivent être présentes et celles qui sont facultatives et en définissant la valeur de leurs étiquettes et les dimensions de longueur autorisées.

D'autres caractéristiques, soit des caractéristiques dont les étiquettes ne sont pas connues, PEUVENT être présentes, comme celles qui sont réservées à l'entité de délivrance. Ces caractéristiques supplémentaires NE DOIVENT PAS utiliser l'étiquette du champ des caractéristiques supplémentaires, ni celle de toute autre caractéristique facultative ou obligatoire. La présence de caractéristiques aux étiquettes inconnues NE DOIT PAS affecter la validité du code à barres, si la signature est reconnue comme étant valide.

2.4 Zone de signature

Le début de la zone de signature est indiqué par le marqueur de signature dont la valeur est `0xFF`, codé sur un octet, suivi d'un à cinq octets signalant la longueur (le nombre d'octets) de la signature, conformément au système de codage des champs de longueur DER-TLV.

L'entrée de l'algorithme de la signature DOIT être (le hachage de) la concaténation de l'en-tête et de la zone de message entière, à l'exception de l'étiquette qui marque le début de la zone de signature ou la longueur de la signature. La zone de signature contient la signature qui en découle.

Seuls les algorithmes de hachage et de signature définis dans la Partie 12 du Doc 9303 DOIVENT être utilisés. En raison de la taille de la signature qui en découle, il est RECOMMANDÉ (au moment de l'établissement du présent document) d'utiliser l'algorithme de signature numérique à courbe elliptique (ECDSA, *Elliptic Curve Signature Algorithm*) avec une longueur de clé d'au moins 256 bits, combiné à l'algorithme SHA-256.

L'application de l'algorithme de signature ECDSA donne une paire de nombres entiers positifs (`r, s`). Cette signature DOIT être stockée sous forme brute dans le cachet. La longueur en bits de `r` et de `s`, respectivement, correspond à la longueur de la clé. Ainsi, pour donner un exemple, pour l'algorithme ECDSA-256, la longueur de de `r` et de `s` est au plus de 256 bits = 32 octets chacun. La signature DOIT être stockée en additionnant les représentations sans signe des nombres entiers `r` et `s`, éventuellement en ajoutant des successions de zéros afin de faire tenir `r` et `s` dans la longueur

attendue (soit la longueur de la clé) et en y ajoutant la valeur obtenue pour `s` à celle de `r`. Voir l'Appendice B pour en savoir davantage sur la conversion entre ASN.1 et le format brut de (`r,s`).

2.5 Remplissage

Si l'en-tête, le message et la signature ne remplissent pas l'espace disponible du code à barres, des caractères de remplissage DOIVENT être ajoutés à la suite de la signature. Toutes les symbologies pertinentes des codes à barres bidimensionnels définissent des méthodes de remplissage applicables à leur norme respective, et le remplissage DOIT suivre cette définition.

2.6 Codage C40 des chaînes

Afin d'économiser de l'espace dans le codage des caractères alphanumériques et le symbole de remplissage <, on utilise le schéma de codage C40, comme le définit la norme [ISO/IEC 16022]. La manière d'utiliser ces définitions dans la configuration actuelle est décrite ci-dessous. Les deux définitions suivantes s'appliquent aux caractéristiques du document et à leur codage numérique :

a) Les chaînes sont uniquement composées de lettres majuscules, de chiffres, <SPACE>, et du symbole '<'. Ce dernier est utilisé comme symbole de remplissage pour la zone de lecture automatique (ZLA) des documents de voyage. Si le symbole '<' se trouve dans la chaîne, toutes les occurrences de '<' sont remplacées par <SPACE> avant le codage. Une chaîne NE DOIT contenir aucun autre symbole.

b) Pour une chaîne de longueur L, la longueur (c'est-à-dire le nombre d'octets) du codage numérique correspondant est le nombre pair le plus petit qui est supérieur ou égal à L.

Dans les calculs suivants, une valeur en octet et l'équivalent en nombre entier non signé correspondant sont implicitement convertis. Par exemple, nous définissons la valeur d'un octet par une formule contenant des opérations arithmétiques sur des valeurs entières.

2.6.1 Codage

Le codage d'une chaîne de caractères en une séquence d'octets se présente comme suit : tout d'abord, la chaîne est groupée en tuples de trois caractères, et chaque caractère est remplacé par la valeur correspondante du codage C40 selon le Tableau 2, donnant ainsi un triplet `(U1,U2,U3)`. Pour chaque triplet, la valeur

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

est calculée. Le résultat se situe entre 1 et 64 000, ce qui donne une valeur entière non signée de 16 bits. Cette valeur de 16 bits `I16` est groupée en deux octets :

```
Octet 1 = (I16) div 256

Octet 2 = (I16) mod 256
```

où `div` désigne la division entière (sans reste), et mod désigne l'opération modulo. Il est à noter que ces opérations peuvent être implémentées par décalage de bit.

Tableau 2. Table de codage C40 et correspondance en ASCII

Valeur C40	*Caractère*	*Valeur ASCII*	*Valeur C40*	*Caractère*	*Valeur ASCII*
0	Shift 1	s. o.	20	G	71
1	Shift 2	s. o.	21	H	72
2	Shift 3	s. o.	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 Décodage

Le codage peut être facilement inversé. Dans une paire donnée d'octets, `(I1,I2)` désigne leurs valeurs entières non signées La valeur de 16 bits `I16` est recalculée comme suit

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

Le triplet `(U1,U2,U3)` peut être recalculé comme suit :

```
U1 = (V16 – 1) div 1600

U2 = (V16 – (U1*1600) – 1) div 40

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

Ici encore, `div` désigne la division entière. Les caractères peuvent être décodés à partir du triplet `(U1, U2, U3)` simplement en repérant les valeurs correspondantes au tableau 2.

2.6.3 Remplissage

La formule ci-dessus n'est bien définie que si la longueur de la chaîne à coder est un multiple de trois. Tout comme les formules de remplissage de la norme [ISO/IEC 16022], les règles suivantes en matière de remplissage s'appliquent :

a) Si deux valeurs C40 (=deux caractères) restent à la fin d'une chaîne, ces deux valeurs C40 sont complétées par la valeur C40 0 (Shift 1) pour former un triplet. Le triplet est codé selon la formule présentée plus haut.

b) S'il reste une valeur C40 (=un caractère), alors le premier octet a la valeur `254dec (0xFE)`. Le second octet est la valeur du système de codage ASCII de Data Matrix du caractère correspondant à la valeur C40. Il est à noter que le système de codage ASCII en Data Matrix pour un caractère ASCII dans le bloc 0-127 est le code ASCII du caractère plus 1.

3. UTILISATION DU CACHET NUMÉRIQUE

La présente section donne une description générale de l'utilisateur du cachet numérique, qui s'applique aux visas et aux documents de voyage d'urgence. Des exigences particulières sont définies dans les profils correspondants.

3.1 Contenu et règles de codage

3.1.1 En-tête

Le codage de l'en-tête des cachets numériques correspond à ce qui est présenté dans la Section 2.2. La valeur des deux derniers octets pour la Référence de la définition des caractéristiques du document et la Catégorie du type de document dépend du profil spécifique du document. La catégorie du type de document doit être un nombre impair pour les profils de l'OACI. Les nombres pairs PEUVENT être utilisés pour des profils nationaux qui ne sont pas spécifiés par l'OACI.

3.1.2 Caractéristiques du document codées dans le cachet numérique

La caractéristique du document qui DOIT être stockée dans le cachet est la zone de lecture automatique (ZLA) :

Le cachet numérique DOIT coder la ZLA d'un document. Le type de ZLA peut correspondre à tous ceux qui sont spécifiés dans le Doc 9303. Toutefois, les profils particuliers du document PEUVENT limiter les types de ZLA autorisés.

Chaque profil de document PEUT définir des champs supplémentaires REQUIS et FACULTATIFS.

3.1.3 Règles de codage pour les caractéristiques du document

Le codage des caractéristiques du document dépend de la Référence de la définition des caractéristiques du document et de la Catégorie du type de document. Des valeurs précises sont définies dans les profils correspondants du document.

3.2 Signataire de code à barres et création du cachet

Pour faciliter la vérification des cachets numériques, la présente spécification s'appuie sur l'infrastructure de clé publique (PKI) de l'autorité de certification signataire nationale existante du pays afin de délivrer et de distribuer des certificats ainsi que des listes de révocation de certificats (LRC). La Partie 12 du Doc 9303 contient plus de détails et présente les profils de certificats.

3.2.1 Architecture du système du signataire de code à barres

Le signataire de code à barres reçoit des données d'un système de personnalisation des documents afin de coder un cachet numérique et utilise une clé de signature pour le signer. La Figure 2 décrit une mise en œuvre possible du signataire de code à barres et de son client, le système de personnalisation du document.

Le signataire de code à barres s'appuie sur les logiciels et les données suivants :

- Le *Logiciel de génération de cachets* produit des cachets numériques qui se conforment à la présente norme. Il reçoit les données de personnalisation envoyées par le client, signe ces données à l'aide d'une clé privée de signataire et code les données de personnalisation et la signature dans un code à barres. Les données de personnalisation et le code à barres sont les données d'entrée et de sortie, respectivement, du logiciel de génération de cachets. Ces données doivent être stockées temporairement dans le signataire de code à barres pendant que le cachet est généré.

- Les *clés de signature* (clé privée et clé publique) servent à signer et à vérifier un cachet numérique. La clé de signature privée constitue les données les plus critiques du signataire de code à barres.

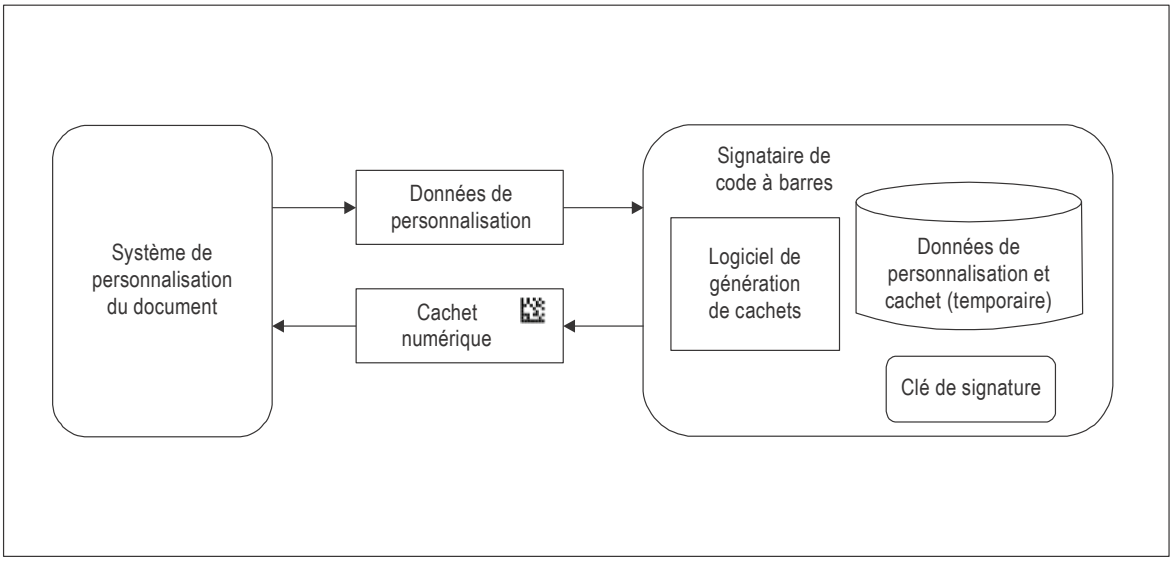

Figure 2. Personnalisation du document : Scénario comprenant un signataire de code à barres centralisé

Selon le scénario d'implantation, la distinction entre le système de personnalisation du document et le signataire de code à barres n'est pas toujours stricte. Par exemple, le signataire de code à barres peut faire partie du système de personnalisation dans une ambassade. L'un des scénarios est d'élargir le système de personnalisation pour y inclure la génération de signature et stocker les clés de signature sur une carte à puce dans l'ambassade. Une autre stratégie consisterait à établir un signataire de code à barres central dans le pays de résidence et permettre aux ambassades de s'y connecter de manière sécurisée. Enfin, certaines ambassades ne personnaliseraient pas les documents elles-mêmes ; le système de personnalisation pourrait donc aussi être établi dans le pays de résidence et intégré au signataire de code à barres.

Le signataire de code à barres est un élément très critique puisqu'il produit la signature. La signature permet de vérifier l'intégrité des données du code à barres, c'est-à-dire de vérifier si les données ont été manipulées, et leur authenticité, c'est-à-dire si elles ont été émises par une entité autorisée.

Afin d'atteindre un niveau de sécurité suffisamment élevé, il est RECOMMANDÉ que le signataire de code à barres soit un service central, qui n'est pas implanté dans les ambassades, sauf si des raisons opérationnelles, techniques ou logistiques empêchent un déploiement centralisé, afin de concentrer les mesures de sécurité dans un périmètre limité, tout en tenant compte des meilleures pratiques pour assurer la capacité de récupération et la continuité des activités. Les clés privées de signature DOIVENT être stockées de manière sécurisée par le signataire de code à barres.

3.2.2 Sécurité du système de signataire de code à barres

Le système de signataire de code à barres DEVRAIT être hébergé et exploité selon les meilleures pratiques de sécurité dans les domaines suivants : sécurité physique ; infrastructure serveur et réseau ; processus de développement et de soutien des systèmes ; contrôle d'accès ; et sécurité opérationnelle. Si le signataire de code à barres est configuré comme service central, il est RECOMMANDÉ d'assurer la conformité avec la norme [ISO/IEC 27002] au périmètre du signataire de code à barres afin de veiller à la conformité avec ces meilleures pratiques de sécurité.

4. RÉFÉRENCES (NORMATIVES)

[ISO/IEC 16022] ISO/IEC 16022 : Technologies de l'information — Techniques automatiques d'identification et de capture des données – Spécification de symbologie de code à barres Data Matrix, 2006

[ISO/IEC 18004] ISO/IEC 18004:2006 : Techniques automatiques d'identification et de capture des données – Spécification de symbologie de code à barres QR, 2015

[ISO/IEC 24778] ISO/IEC 24778:2008 : Techniques automatiques d'identification et de capture des données – Spécification de symbologie de code à barres Aztec, 2008

[ISO/IEC 27002] ISO/IEC 27002 : Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information, 2013

[ISO/IEC 15415] ISO/IEC 15415:2011 : Technologies de l'information — Techniques automatiques d'identification et de capture des données — Spécification de test de qualité d'impression des symboles de codes à barres — Symboles bidimensionnels, 2011

[X.690] ITU-T X.690 2008, RÉSEAUX POUR DONNÉES, COMMUNICATIONS ENTRE SYSTÈMES OUVERTS – réseautage OSI et aspects systèmes – Notation de syntaxe abstraite numéro un (ASN.1) Technologies de l'information – Règles de codage ASN.1

– – – – – – – – – – – –

APPENDICE A À LA PARTIE 13
(INFORMATIF)

EXEMPLE DE CAS D'USAGE

La présente section donne un aperçu général de l'utilisation d'un cachet numérique pour protéger un document non électronique. L'exemple de cas précis examiné ici est la protection d'un document de visa décrit à la Figure A.1. Bien que les détails techniques puissent varier dans d'autres cas d'usage, les mêmes principes généraux s'appliquent.

Le flux de travail peut être divisé en trois étapes. Comme condition préalable, des certificats de signataire de visa (CSV) doivent être générés. Ensuite, les cachets numériques sont générés, puis validés ultérieurement.

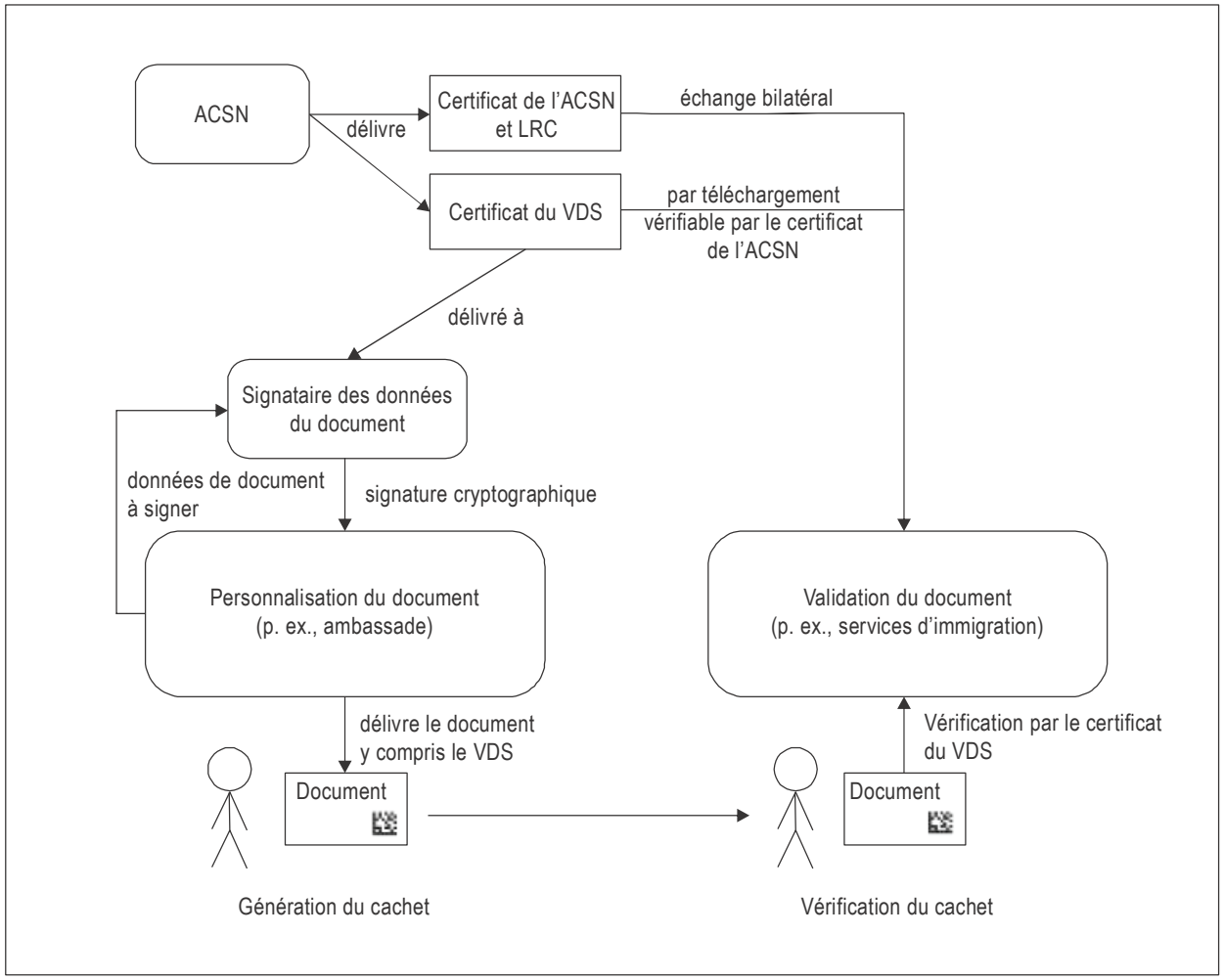

Figure A.1. Exemple de cas d'utilisation d'un cachet numérique visible (VDS)

A.1 CONDITION PRÉALABLE : GÉNÉRATION D'UN CERTIFICAT DE SIGNATAIRE DE VISA

L'ICP du signataire de visa est basée sur l'ICP configurée pour les passeports électroniques définie par l'OACI. À la base on trouve l'autorité de certification signataire nationale (ACSN) de chaque pays. L'ACSN publie un certificat de l'Autorité de certification signataire nationale qui contient sa clé publique. Pour favoriser la confiance entre les pays, le certificat de l'ACSN est distribué par échange bilatéral ou au moyen de listes de contrôle.

Le signataire de visa est l'entité qui signe véritablement les cachets numériques. Les CSV sont délivrés par l'ACSN et peuvent donc être vérifiés au moyen du certificat de l'ACSN.

A.2 GÉNÉRATION DU CACHET NUMÉRIQUE

Un cachet numérique est généré en deux étapes :

a) Les demandeurs de visa présentent une demande à l'ambassade de leur pays de résidence. L'ambassade enregistre les données du demandeur et vérifie si la demande est conforme aux exigences relatives à l'obtention d'un visa. Si c'est le cas, l'ambassade envoie une représentation numérique des données enregistrées au signataire de visa (VS). Le VS peut être soit 1) une entité centrale située dans le pays qui délivre le visa, et l'ambassade se connecte au VS de manière sécurisée, soit 2) les VS sont des entités décentralisées placées dans chaque ambassade, par exemple, au moyen de cartes à puce contenant des clés cryptographiques qui sont directement connectées au système de personnalisation. Dans tous les cas de figure, le VS signe les données enregistrées selon un procédé cryptographique.

b) Pour les besoins de la signature, le signataire de visa utilise une paire de clés constituée d'une clé privée et d'une clé publique. La signature se fait au moyen de la clé privée alors que la clé publique est stockée dans un certificat de signataire de visa. La signature produite est renvoyée au système de personnalisation de visa si le signataire de visa ne constitue pas une partie locale du système de personnalisation, imprimée sur l'autocollant du visa et jointe au passeport du demandeur.

A.3 VALIDATION DU CACHET NUMÉRIQUE

Lorsque les demandeurs entrent dans le pays de délivrance, ils présentent leur visa à une Autorité de validation des visas (AVV), c'est-à-dire l'autorité de contrôle de l'immigration du pays de délivrance. L'AVV vérifie l'authenticité et l'intégrité du cachet numérique sur le visa en validant la signature du cachet et en comparant les informations imprimées sur l'étiquette du visa et sur le passeport avec les informations numériques stockées dans le cachet. La signature du cachet est vérifiée en identifiant le certificat du signataire de visa correspondant à l'aide de l'identifiant stocké dans l'en-tête du cachet numérique et en utilisant ensuite la clé publique du certificat. Comme indiqué précédemment, la validité du certificat du signataire de visa lui-même peut être vérifiée au moyen du certificat de l'ACSN.

Observation

Puisque tous les certificats sont publics, la validité du visa peut être vérifiée par *n'importe quel* tiers et non pas seulement par l'État de délivrance. Ce processus permet de régler le cas d'unions entre pays, dans lesquels un pays délivre un visa pour un autre pays (comme dans l'Union européenne). Un autre cas est la vérification des visas par les compagnies aériennes avant l'embarquement.

Observation

Les critères permettant de déterminer si un document de visa est fiable ou non, en fonction du cachet numérique et de la ZLA du visa et du passeport, sont définis dans une politique de validation.

– – – – – – – – – – – –

APPENDICE B À LA PARTIE 13
(INFORMATIF)

CONVERSION DES FORMATS DE SIGNATURE ECDSA

B.1 CODAGE DES ENTIERS EN BER/DER

Les entiers sont codés selon les règles de codage de base (BER) et les règles de codage distinctives (DER) comme le codage signé en mode gros-boutiste de longueur minimale, à la suite de quoi le schéma Étiquette-Longueur-Valeur (TLV) est appliqué. On distingue les cas suivants :

a) En supposant que la valeur entière est positive, et que le bit le plus significatif (MSB) est zéro dans la représentation minimale de l'entier non signé, alors la représentation de l'entier non signé a la forme ci-dessous, qui correspond à la valeur BER/DER :

`|0bbbbbbb| ...`

b) En supposant que la valeur entière est positive, et que le MSB est 1 dans la représentation minimale de l'entier non signé, c'est-à-dire qu'il a la forme `|1bbbbbbb| ...` alors un octet contenant des zéros est placé devant et la valeur BER/DER est

`|00000000|1bbbbbbb| ...`

c) En supposant que la valeur entière est négative, alors cette valeur est codée comme le complément à deux, par exemple en prenant la représentation minimale de l'entier non signé, en l'inversant, et en ajoutant 1. Par la suite, le MSB est réglé à 1. Par exemple, pour -25357, la représentation minimale de l'entier non signé est

`|0110 0011|0000 1101|`

Inversé comme suit :

`|1001 1100|1111 0010|`

Auquel 1 est ajouté :

`|1001 1100|1111 0011|`

ce qui donne la valeur BER/DER. Il est à noter que le fait que le nombre soit négatif peut être directement déduit du fait que le MSB (à l'extrême gauche) est 1.

Enfin, on génère une valeur TLV en ajoutant deux octets devant les valeurs BER/DER codées précédemment. Le premier octet est l'étiquette avec la constante `0x02`. Le second octet contient la longueur (c'est-à-dire le nombre d'octets) de la valeur BER/DER codée suivante. Le décodage peut se faire simplement, par exemple en distinguant, selon le MSB, si un entier négatif ou positif est codé, et en appliquant les étapes précédentes en ordre inverse.

B.2 EXEMPLE

Le Tableau B.1 donne des exemples d'entiers codés en BER/DER.

Tableau B.1 Exemples de codage BER/DER de quelques valeurs entières

Valeur (déc.)	*Étiquette (hex)*	*Longueur (hex)*	*Valeur (hex)*	*Valeur (binaire)*
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 SIGNATURES ECDSA DANS ASN.1/DER

La description ASN.1 d'une signature ECDSA est

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

La séquence est codée en DER comme un triplet TLV avec l'étiquette `0x30`, la longueur comme le nombre d'octets de la valeur suivante, et la valeur comme la concaténation des triplets TLV du codage de `r` suivie par le codage de `s`.

Deux exemples de séquences sont présentés dans le Tableau B.2. Bien entendu, les entiers `r` et `s` d'une signature ECDSA sont considérablement plus grands en pratique.

Tableau B.2 Séquences de deux entiers codés en DER

Entiers		*Séquence de TLV*		
R	***S***	***Étiquette***	***Longueur***	***Valeur***
127	1	0x30	0x06	0x02 0x01 0x7F 0x02 0x01 0x01
128	127	0x30	0x07	0x02 0x02 0x00 0x80 0x02 0x01 0x7F

Il est à noter que `r` et `s` sont toujours des entiers positifs pour une signature ECDSA. Par conséquent, pour la conversion de la signature brute en DER, il faut d'abord diviser la signature brute en deux pour obtenir `r` et `s` individuellement, puis les coder comme une séquence ASN.1 codée en DER selon la définition ci-dessus. À l'inverse, pour le décodage de la signature ECDSA en DER, il faut tout d'abord décoder la séquence, extraire la représentation entière non signée de `r` et `s` et donner à `r` et `s` une représentation de longueur fixe (= longueur de la taille de la clé), en enlevant ou en ajoutant des octets zéros à gauche au besoin (par exemple dans le cas de ECDSA-256, tant `r` que `s` doit avoir une longueur de 256 bits = 32 octets), et en concaténant la valeur résultante `s` à la valeur résultante `r`.

– – – – – – – – – – – –

APPENDICE C À LA PARTIE 13
(INFORMATIF)

EXEMPLES DE CODAGE C40

C.1 EXEMPLE 1

Supposons que la chaîne « XK<CD » doit être codée. Par définition, toutes les occurrences de '<' sont remplacées par <SPACE> avant le codage. La chaîne qui en résulte est par conséquent « XK CD », c'est-à-dire « XK<SPACE>CD » (un espace inséré). Le codage/décodage C40 de la chaîne « XK<SPACE>CD » est décrit dans le Tableau C.1.

Tableau C.1 Exemple de codage/décodage de la chaîne « XK<SPACE>CD »

Opération	***Résultat***			
chaîne originale	« XK<SPACE>CD »			
groupement en triplets	(X, K, <SPACE>)		(C, D,)	
remplacement par les valeurs C40 et remplissage	(37, 24, 3)		(16, 17, remplissage)	
calcul de la valeur entière de 16 bits	60164		26281	
	Octet 1 (div)	**Octet 2 (mod)**	**Octet 1 (div)**	**Octet 2 (mod)**
séquence d'octet résultante (décimale)	235	4	102	169
séquence d'octet résultante (hexadécimale)	0xEB	0x04	0x66	0xA9

C.2 EXEMPLE 2

Supposons que la chaîne « XKCD » doit être codée. La chaîne est composée uniquement de majuscules. Son codage/décodage C40 est décrit dans le Tableau C.2.

Tableau C.2 Exemple de codage/décodage de la chaîne « XKCD »

Opération	***Résultat***			
chaîne originale	« XKCD »			
groupement en triplets	(X, K, C)		(D, ,)	
remplacement par les valeurs C40 et remplissage	(37, 24, 16)		(décoder C40 et coder en ASCII)	
calcul de la valeur entière de 16 bits	60177			
	Octet 1 (div)	***Octet 2 (mod)***	***Octet 1***	***Octet 2***
séquence d'octet résultante (décimale)	235	11	254	69
séquence d'octet résultante (hexadécimale)	0xEB	0x11	0xFE	0x45

– – – – – – – – – – – –

APPENDICE D À LA PARTIE 13
(INFORMATIF)

RÈGLES DE LA POLITIQUE DE VALIDATION

La Politique de validation est un ensemble de règles de validation qui permettent de déterminer la validité du cachet sur le document. En appliquant cette politique de validation, on obtient une indication de statut avec l'une des valeurs suivantes :

a) VALID. L'authenticité et l'intégrité du cachet ont été confirmées. Ici l'authenticité signifie que les données dans le cachet ont été effectivement signées par un Signataire de code à barres du pays de délivrance du document, et le Certificat du Signataire du code à barres correspondant est valide. L'intégrité signifie que les données de la ZLA du document portant le cachet n'ont pas été modifiées, et que le cachet numérique n'a pas été transféré du document auquel il était originalement attaché.

b) INVALID. Le cachet n'est pas reconnu comme valide et un complément d'enquête est nécessaire. La non-validité peut être attribuable aux trois raisons suivantes :

   1) *Fraude/Contrefaçon*. Cela inclut la personnalisation non autorisée d'un document, au moyen d'une étiquette vierge volée, des modifications des données de personnalisation d'un document fondées sur une étiquette originale, ou le remplacement d'une étiquette de code à barres d'un document par celle prise sur un document volé (p. ex., un passeport), ou d'autres falsifications.

   2) *Dommage/Détérioration*. Le code à barres ne peut être décodé du fait de l'usure, de la détérioration ou de taches.

   3) *Erreurs inconnues et/ou inattendues*. Cela comprend des erreurs imprévisibles. Par exemple, du fait de bogues dans l'implantation du logiciel utilisé pour le décodage, ou un codage erroné pendant la personnalisation.

L'indication de statut INVALID s'accompagne de sous-indications, qui indiquent les raisons pour lesquelles un cachet n'est pas valide. Étant donné que le risque d'une fraude dépend de ces raisons, il est recommandé de mettre en correspondance les indications et les sous-indications de statut avec les trois niveaux de confiance « fiable », « possibilité moyenne de fraude » et « possibilité élevée de fraude ». Le mappage recommandé est illustré au Tableau D.1.

La politique de validation générique examine toujours les questions suivantes :

a) Le cachet numérique visible est-il valide ?

b) La ZLA du document est-elle valide ?

c) La ZLA du document correspond-elle au cachet numérique visible ?

Sont présentés ci-dessous les règles de validation pour chaque type de contrôle, une liste de critères de validation, les résultats attendus pour chaque critère et les sous-indications de statut qui en découlent.

Validation du cachet numérique visible

1. Validation du format

    - si le format physique de codage n'est pas conforme à la spécification ou si des erreurs attribuables à du bruit physique ne peuvent être corrigées, le statut est INVALID avec la sous-indication READ_ERROR, ou

    - si le format de codage (c'est-à-dire les structures du cachet qui comprennent l'en-tête, la zone de message et la zone de signature, ou le codage binaire/C40) n'est pas conforme à la spécification, ou

    - si les valeurs attendues dans l'en-tête sont inconnues, ou

    - si un champ obligatoire dans la zone de message est manquant, ou

    - si le format d'un champ dans la zone de message n'est pas conforme à la spécification de la version définie dans l'en-tête, alors le statut est INVALID avec la sous-indication WRONG_FORMAT, autrement continuer, ou

    - si un champ inconnu est présent dans la zone de message, alors la sous-indication UKNOWN_FEATURE devrait être activée. L'indication de statut sera VALID ou INVALID selon la validité de la signature vérifiée dans les étapes ci-dessous. Il faut noter que si la signature est valide, la seule présence d'une caractéristique inconnue ne doit pas violer l'intégrité du cachet.

2. Validation de la signature

    - si le certificat du signataire de code à barres auquel il est fait référence dans l'en-tête du cachet n'est pas présent, le statut est INVALID avec la sous-indication UNKNOWN_CERTIFICATE,

    - si le certificat du signataire de code à barres auquel il est fait référence dans l'en-tête du cachet n'a pas été signé par l'ACSN, ou si la vérification de la signature échoue, le statut est INVALID avec la sous-indication UNTRUSTED_CERTIFICATE,

    - si le certificat du signataire de code à barres contient une extension de type de document et que le contenu du code à barres contient une ZLA, et que le type de document de la ZLA n'est pas contenu dans l'extension de type de document, le statut est INVALID avec la sous-indication INVALID_DOCUMENTTYPE,

    - si le certificat du signataire de code à barres auquel il est fait référence dans l'en-tête du cachet a expiré, le statut est INVALID avec la sous-indication EXPIRED_CERTIFICATE,

    - si le certificat du signataire de code à barres auquel il est fait référence dans l'en-tête du cachet est révoqué, le statut est INVALID avec la sous-indication REVOKED_CERTIFICATE,

    - si la vérification de la signature de l'en-tête et de la zone de message à l'aide du certificat du signataire de code à barres auquel il est fait référence dans l'en-tête du cachet échoue, le statut est INVALID avec la sous-indication INVALID_SIGNATURE,

    - autrement, continuer.

3. Validation de l'émetteur

    - si le système de validation du code à barres considère que l'ACSN n'est pas fiable dans son domaine de confiance, le statut est INVALID avec la sous-indication UNTRUSTED_CERTIFICATE, autrement, continuer.

Les règles de validation ci-dessus couvrent une comparaison des données stockées sur le cachet avec les données stockées sur la ZLA du document. De plus, une inspection manuelle des données stockées sur le cachet et imprimées sur le document, mais non présentes dans la ZLA des documents, pourrait être effectuée.

Tableau D.1. Niveaux de confiance recommandés pour les règles du document

Indication de statut	***Indication de sous-statut***	***Niveau de confiance***
VALID	-	*Fiable*
	UNKNOWN_FEATURE	
INVALID	READ_ERROR	*Possibilité moyenne de fraude*
	EXPIRED_CERTIFICATE	
	WRONG_FORMAT	*Possibilité élevée de fraude*
	UNKNOWN_CERTIFICATE	
	UNTRUSTED_CERTIFICATE	
	INVALID_DOCUMENTTYPE	
	REVOKED_CERTIFICATE	
	INVALID_SIGNATURE	

— FIN —

ISBN 978-92-9265-529-7