**AIGCEV / VDSIC**

**Association Internationale de Gouvernance du Cachet Electronique Visible**

**Visible Digital Seal International Council**

**Spécifications relatives à la mise en œuvre du Cachet Electronique Visible (CEV) aux fins d’authentification, vérification et saisie automatique des données véhiculées par un document.**

**Cas d’usage :**

**« Courrier Permis à points »**

#### Spécime de CEV « Permis à poits » :



#### Historique des versions

AIGCEV ANTS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Version* | *Date* |  | *Version* | *Date* |
|  |  |  | 3.0.0 | 14 février 2017 |
| 1.0 | 04 octobre 2017 |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table des matières

[1 Introduction 3](#_Toc480974337)

[2 Documents de type « Courrier permis à points » 3](#_Toc480974338)

[2.1 Format, type de document et périmètre 5](#_Toc480974339)

[2.2 Représentation graphique et position du CEV 7](#_Toc480974340)

[2.3 Dimension 8](#_Toc480974341)

[2.4 Message 9](#_Toc480974342)

[2.4.1 Identifiants de données non spécifiques au « Courrier permis à points » 9](#_Toc480974343)

[2.4.2 Identifiants de données propres au type de document « Courrier permis à points » 11](#_Toc480974344)

[2.4.3 Données obligatoires et facultatives du Courrier permis à points 13](#_Toc480974345)

[2.5 Signature des données et type de sécurité 13](#_Toc480974346)

[3 Traitements sur les données 14](#_Toc480974347)

[3.1 Troncature des champs 14](#_Toc480974348)

[3.2 Retrait de la ponctuation 14](#_Toc480974349)

[4 Exemple complet d’encodage : « Courrier permis à points » 15](#_Toc480974350)

# Introduction

Cette introduction n’est pas spécifique à ce cas d’usage. Elle a pour objet de présenter les différentes structures possibles d’un CEV définies dans la partie 1 de la norme expérimentale CEV de l’AFNOR.

Ces structures correspondent à des versions opérationnelles gérées par l’AIGCEV dénommées V2, V3 et V4.

**Structures et codage du CEV :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Entête** | **Message** | **Signature** | **Annexe** |
|  |  |  |  |  |
| **V2** | C40 | C40 | C40 |  |
|  |  |  |  |  |
| **V3** | C40 | C40 | C40 |  |
|  |  |  |  |  |
|  |  |  |  |  |
| **V4** | C40 | C40 | C40 |  |
|  | C40 | C40 | C40 | C40 |
|  | C40 | C40/Binaire | Binaire |  |
|  | C40 | C40/Binaire | Binaire | Binaire |
|  | C40 | Binaire | Binaire |  |
|  | C40 | Binaire | Binaire | Binaire |
|  | Binaire | Binaire | Binaire |  |
|  | Binaire | Binaire | Binaire | Binaire |
|  |  |  |  |  |

Combiner du C40 et du Binaire est possible, mais il est recommandé de faire soit tout en C40, soit tout en binaire.

**Structures de l’Entête et Nombre de caractères enC40 :**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **Identifiant** | **Identifiant** | **Date** | **Date de** | **Type de** |  |  | **Nombre de** |
|  | **Marqueur** | **Version** | **de l’AC** | **du certificat** | **d’émission** | **signature** | **document** | **Périmètre** | **Pays** | **caractères** |
|  |  |  |  |  |  |  |  |  |  |  |
| **V2** | X | X | X | X | X | X | X |  |  | **22** |
|  |  |  |  |  |  |  |  |  |  |  |
| **V3** | X | X | X | X | X | X | X | **X** |  | **24** |
|  |  |  |  |  |  |  |  |  |  |  |
| **V4** | X | X | X | X | X | X | X | X | **X** | **26** |
|  |  |  |  |  |  |  |  |  |  |  |

**Structures de l’Entête et Nombre de caractères en binaire :**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **Identifiant** | **Identifiant** | **Date** | **Date de** | **Type de** |  |  | **Nombre** |
|  | **Marqueur** | **Version** | **de l’AC** | **du certificat** | **d’émission** | **signature** | **document** | **Périmètre** | **Pays** | **d’octets** |
|  |  |  |  |  |  |  |  |  |  |  |
| **V4** | X | X | X | X | X | X | X | X | **X** | **19** |
|  |  |  |  |  |  |  |  |  |  |  |

**Encodages du Marqueur CEV suivant les Versions :**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Entête** | **Marqueur** |  |  |  |
|  |  |  |  |  |  |
| **V2** | C40 | DC |  |  |  |
|  |  |  |  |  |  |
| **V3** | C40 | DC |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| **V4** | C40 | DC | tables de caractères C40 uniquement | | |
|  | C40 | **DD** | toutes tables de caractères | | |
|  | Binaire | DC | usages régaliens | |  |
|  | Binaire | **DD** | réservé |  |  |
|  |  |  |  |  |  |

En synthèse :

* Le passage de la V2 à la V3 est dû à l’introduction du champ « Périmètre » dans l’Entête qui de ce fait passe de 22 caractères à 24 caractères.
* Le passage de la V3 à la V4 permet l’utilisation d’un encodage Binaire. Du fait de l’introduction du champ « Pays », l’Entête passe de 24 caractères à 26 caractères.

Pour la génération de nouveaux CEV, l’utilisation de la V3 est recommandée.

# Documents de type « Courrier permis à points »

## Format, type de document et périmètre

### Entête en version 3 (V3)

Le champ « Marqueur » CEV prend la valeur ’**DC**’ (cf. tableau supra).

Le champ « Version » en V3 prend la valeur ’**03**’.

Le champ « Identifiant de l’AC » qui a émis le certificat utilisé pour le type « Bulletin de salaire » par l’émetteur, contient 4 caractères alphanumériques [A-Z][0-9]. Pour l’exemple ci-après, il prend la valeur ‘**FR03**’.

Le champ « Identification du certificat » (du certificat utilisé pour signer les données de ce Type de document) est composé de 4 caractères alphanumériques [A-Z][0- 9]. Ici, il prend la valeur ‘**AIG0**’ qui correspond au certificat utilisé par l’AIGCEV pour éditer des Spécimens

Les champs « Date d’émission du document » et « Dates de signature du CEV » ont une date exprimée par le nombre de jours depuis le 1er janvier 2000, encodé en hexadécimal. Ici, ces deux champs contiennent la même date du 2 août 2017, ce qui donne la valeur ‘**1917**’ en hexadécimal, pour ces deux champs.

Le champ « Type de document » prend la valeur ‘**A1**’, spécifiquement attribuée au « Courrier permis à points ».

Le champ « Périmètre » prend la valeur ‘**01**’ qui correspond au Périmètre « Régalien » qui contient le Type « Courrier permis à points ».

|  |  |
| --- | --- |
| Marqueur | DC |
| Version | 03 |
| Identifiant de l’AC | FR03 |
| Identifiant du certificat | AIG0 |
| Date d’émission | 1917 |
| Date de signature | 1917 |
| Type de document | A1 |
| Périmètre | 01 |
| Entête | **DC03FR03AIG019171917A101** |

En V3 l’Entête se compose de 24 caractères.

### Entête en version 2 (V2)

Le champ « Marqueur » CEV prend la valeur ’**DC**’ (cf. tableau supra).

Le champ « Version » en V2 prend la valeur ’**02**’.

Le champ « Identifiant de l’AC » qui a émis le certificat utilisé pour le type « Bulletin de salaire » par l’émetteur, contient 4 caractères alphanumériques [A-Z][0-9]. Pour l’exemple ci-après, il prend la valeur ‘**FR03**’.

Le champ « Identification du certificat » (du certificat utilisé pour signer les données de ce Type de document) est composé de 4 caractères alphanumériques [A-Z][0- 9]. Ici, il prend la valeur ‘**AIG0**’ qui correspond au certificat utilisé par l’AIGCEV pour éditer des Spécimens

Les champs « Date d’émission du document » et « Dates de signature du CEV » ont une date exprimée par le nombre de jours depuis le 1er janvier 2000, encodé en hexadécimal. Ici, ces deux champs contiennent la même date du 2 août 2017, ce qui donne la valeur ‘**1917**’ en hexadécimal, pour ces deux champs.

Le champ « Type de document » prend la valeur ‘**A1**’, spécifiquement attribuée au « Courrier permis à points ».

Il n’y a pas de champ « Périmètre », celui-ci n’apparaissant qu’à partir de la V3.

|  |  |
| --- | --- |
| Marqueur | DC |
| Version | 02 |
| Identifiant de l’AC | FR03 |
| Identifiant du certificat | AIG0 |
| Date d’émission | 1917 |
| Date de signature | 1917 |
| Type de document | A1 |
| **Entête** | **DC02FR03AIG019171917A1** |

En V2 l’Entête se compose de 22 caractères.

## Représentation graphique et position du CEV

### Format graphique du CEV « Courrier Permis à Points »

Le mode de représentation graphique retenu pour le CEV « Courrier Permis à Points » est le format Datamatrix ISO/IEC 16022 de forme carrée avec niveau de correction ECC200.

Un code à barres Datamatrix générique peut inclure plusieurs niveaux de correction. Pour le CEV « Courrier Permis à Points », le seul niveau reconnu est le code à barres Datamatrix de type ECC 200. Seul ce type de code permet de situer d’éventuelles erreurs dans le code à barres.

### Marquage du code à barres

Pour être identifié, le code est marqué de manière objectivement lisible de la marque 2D-OK, sur l’un des quatre côtés comme indiqué ci-dessous.

|  |  |  |  |
| --- | --- | --- | --- |
| 125_2D-OK | 125_2D-OK | 125_2D-OK |  |

Le marquage doit respecter la « zone de silence » (ou quiet zone) nécessaire à une lecture efficace du code Datamatrix.

* + 1. **Positionnement du CEV**

Le CEV DEVRAIT être positionné sur la même page que les données qui y sont encodées, afin de permettre par la numérisation d’une seule page de vérifier que les données du code à barres sont identiques à celles du document.

* + 1. **Zone vierge**

Pour s’assurer de la lecture du code CEV, celui-ci DOIT être entouré d’une zone vierge (Quiet zone). Celle-ci se matérialise par une zone vierge, présente sur les quatre côtés du code.

La taille de la zone vierge DOIT être supérieure ou égale à la taille d’un module, qui correspond, dans le cadre d’un Datamatrix, à un carré élémentaire du code à barres.

## Dimension

Pour la technologie Datamatrix, les machines utilisées par les particuliers étant disparates et afin d’assurer une robustesse minimale de la technologie jet d’encre, les modules devront avoir une taille minimale de 0,4 mm.

De plus, pour s’assurer de la lecture du code à barres, celui-ci doit être entouré d’une « Zone blanche », sur les quatre côtés, de 0.,4 mm au moins (soit au moins la taille d’un module).

La taille minimale du code en Version 2 comme en Version 3 est de 19,2 mm (20 mm avec la Zone blanche), taille qui garantit le stockage des champs obligatoires d’un Courrier permis à points.

Les méthodes de compression et de troncature sont présentées dans la section de la partie 2 de la Norme.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Taille d'un côté** | **Capacité de stockage** | **Capacité de la zone** | **de message (Nombre** | **de caractères AN)** |
| **Datamatrix** | **du Datamatrix** |  | **NIST P-256** |  |
| (mm) | (en octet) | V2 | V3 | V4 |
| 16 | 114 | 41 | 39 | 37 |
| 17,6 | 144 | 86 | 84 | 82 |
| 19,2 | 174 | 132 | 130 | 128 |
| 20,8 | 204 | 176 | 174 | 172 |
| 25,6 | 280 | 290 | 288 | 286 |
| 28,8 | 368 | 422 | 420 | 418 |
| 32 | 456 | 554 | 552 | 550 |
| 35,2 | 576 | 734 | 732 | 730 |
| 38,4 | 696 | 914 | 912 | 910 |
| 41,6 | 806 | 1094 | 1092 | 1090 |
| 48 | 1050 | 1445 | 1443 | 1441 |
| 52,8 | 1304 | 1826 | 1824 | 1822 |
| 57,6 | 1558 | 2207 | 2205 | 2203 |

En P-384 et P-521, la capacité de la zone de message sera moindre qu’en P-256 (cf. tableau ci-dessus).

## Message

Les données qui peuvent être encodées dans le type de document « Courrier permis à points » sont indiquées ci-après.

### Identifiants de données non spécifiques au « Courrier permis à points »

|  |  |
| --- | --- |
| **Identifiant unique du document.** | |
| *ID* | 01 |
| *Taille Min.* | 0 |
| *Taille Max.* | Aucune |
| *Type* | Alphanumérique |
| *Description* | Cet identifiant permet en fonction de l’émetteur (si celui-ci fournit le service) de récupérer le document correspondant. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] et des chiffres [0-9]. |
| **Catégorie de document** | |
| *ID* | 02 |
| *Taille Min.* | 0 |
| *Taille Max.* | Aucune |
| *Type* | Alphanumérique |
| *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces. |
| **Sous-catégorie de document** | |
| *ID* | 03 |
| *Taille Min.* | 0 |
| *Taille Max.* | Aucune |
| *Type* | Alphanumérique |
| *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces. |
| **Application de composition** | |
| *ID* | 04 |
| *Taille Min.* | 0 |
| *Taille Max.* | Aucune |
| *Type* | Alphanumérique |
| *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces. |
| **Version de l’application de composition** | |
| *ID* | 05 |
| *Taille Min.* | 0 |
| *Taille Max.* | Aucune |
| *Type* | Alphanumérique |
| *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces. |
| **Date de l’association entre le document et le CEV.** | |
| *ID* | 06 |
| *Taille Min.* | 4 |
| *Taille Max.* | 4 |
| *Type* | Alphanumérique |
| *Description* | Cette date est indiquée par le nombre de jours encodé en hexadécimal depuis le 1er janvier 2000 de la même manière que les dates fournies dans l’entête, soit [A-F][0-9]. |
| **Heure de l’association entre le document et le CEV.** | |
| *ID* | 07 |
| *Taille Min.* | 6 |
| *Taille Max.* | 6 |
| *Type* | Numérique |
| *Description* | Cette donnée est composée uniquement de 6 chiffres au format HHMMSS où HH représente l’heure, MM les minutes et SS les secondes. Les heures, les minutes et les secondes sont encodées sur 2 chiffres préfixés par 0 si nécessaire. |
| **Date d’expiration du document** | |
| *ID* | 08 |
| *Taille Min.* | 4 |
| *Taille Max.* | 4 |
| *Type* | Alphanumérique |
| *Description* | Cette date est indiquée par le nombre de jours encodé en hexadécimal depuis le 1er janvier 2000 de la même manière que les dates fournies dans l’entête, soit [A-F][0-9]. |
| **Nombre de pages du document** | |
| *ID* | 09 |
| *Taille Min.* | 4 |
| *Taille Max.* | 4 |
| *Type* | Numérique |
| *Description* | Cette donnée est encodée en utilisant uniquement des chiffres [0-9]. Le nombre devra être préfixé par des 0 si nécessaire. |
| **Editeur du CEV** | |
| *ID* | 0A |
| *Taille Min.* | 9 |
| *Taille Max.* | 9 |
| *Type* | Numérique |
| *Description* | Correspond au numéro de SIREN de l’éditeur, sur 9 caractères numériques, soit [0-9]. |
| **Intégrateur du CEV** | |
| *ID* | 0B |
| *Taille Min.* | 9 |
| *Taille Max.* | 9 |
| *Type* | Numérique |
| *Description* | Correspond au numéro de SIREN de l’intégrateur, sur 9 caractères numériques, soit [0-9]. |

### Identifiants de données propres au type de document « Courrier permis à points »

|  |  |
| --- | --- |
|  |  |
| **Type de lettre**   |  |  | | --- | --- | | *ID* | AB | | *Taille Min.* | 0 | | *Taille Max.* | 8 | | *Type* | Alphanumérique | | *Description* | Caractères autorisés (A-F][0-9) |   **Numéro de dossier**   |  |  | | --- | --- | | *ID* | AC | | *Taille Min.* | 0 | | *Taille Max.* | 19 | | *Type* | Alphanumérique | | *Description* | Caractères autorisés (A-F][0-9) |   **Civilité**   |  |  | | --- | --- | | *ID* | 6H | | *Taille Min.* | 1 | | *Taille Max.* | 10 | | *Type* | Alphabétique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non  accentuées [A-Z] et des espaces. |   **Nom**   |  |  | | --- | --- | | *ID* | 6G | | *Taille Min.* | 1 | | *Taille Max.* | 38 | | *Type* | Alphabtique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non  accentuées [A-Z] et des espaces. |   **Prénoms**   |  |  | | --- | --- | | *ID* | 60 | | *Taille Min.* | 0 | | *Taille Max.* | 60 | | *Type* | Alphanumérique | | *Description* | Les prénoms composés sont séparés par un espace. Les différents prénoms sont séparés par ‘/’. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9], des espaces et des ‘/’ s’il y a plusieurs prénoms (au maximum 6). |   **Date de naissance**   |  |  | | --- | --- | | *ID* | 69 | | *Taille Min.* | 8 | | *Taille Max.* | 8 | | *Type* | Numérique | | *Description* | Cette date est composée uniquement de 8 chiffres au format JJMMAAAA où JJ représente le jour dans le mois, MM le mois et AAAA l’année. Le jour et le numéro du mois sont encodés sur 2 chiffres préfixés par 0 si nécessaire | | |
| **Lieu de naissance**   |  |  | | --- | --- | | *ID* | 6A | | *Taille Min.* | 0 | | *Taille Max.* | 32 | | *Type* | Alphanumérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces |   **Date d’infraction**   |  |  | | --- | --- | | *ID* | AD | | *Taille Min.* | 4 | | *Taille Max.* | 4 | | *Type* | Alphanumérique | | *Description* | Date de l’infraction en nombre de jours après le 01/01/2000 encodée en hexadécimal, soit [A-F][0-9]. |   **Heure de l’infraction**   |  |  | | --- | --- | | *ID* | AE | | *Taille Min.* | 4 | | *Taille Max.* | 4 | | *Type* | Numérique | | *Description* | Heure au format HHmm, préfixée au besoin par 0. |   **Nombre de points retires lors de l’infraction**   |  |  | | --- | --- | | *ID* | AF | | *Taille Min.* | 1 | | *Taille Max.* | 1 | | *Type* | Alphanumérique | | *Description* | Valeur entre 0 à 35 points. Encodée en base 36 (0-9][A\_Z) |   **Solde de points**   |  |  | | --- | --- | | *ID* | AG | | *Taille Min.* | 1 | | *Taille Max.* | 1 | | *Type* | Alphanumérique | | *Description* | Valeur entre 0 à 35 points. Encodée en base 36 (0-9][A\_Z) | |  |
|  |  |

|  |  |
| --- | --- |
|  |  |

### 2.4.3 Données obligatoires et facultatives spécifiques du ‘Courrier permis à points’

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **Type de Document** | | | |
| **ID** | **Description** |  |  | **A1** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AB** | Type de lettre |  |  | O |  |
| **AC** | N° Dossier |  |  | O |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **6H** | Civilité |  |  | O |  |
| **6G** | Nom |  |  | O |  |
| **60** | Prénoms |  |  | O |  |
| **69** | Date de naissance |  |  | O |  |
| **6A** | Lieu de naissance |  |  | F |  |
| **AD** | Date d’infraction |  |  | F |  |
| **AE** | Heure de l’infraction |  |  | F |  |
| **AF** | Nombre de points retirés lors de l’infraction |  |  | F |  |
| **AG** | Solde de points |  |  | F |  |

## Signature des données et type de sécurité

La signature électronique des données est au format C40, donc encodée en base32.

Chaque acteur réalisera la signature des documents émis avec une clé valide.

Les courbes utilisées sont les courbes P-256, P-384 ou P-521 du NIST.

L’encodage des signatures ECDSA est réalisé conformément au standard PKCS#11

L’algorithme pour les fonctions de calcul du condensat est l’un des 3 algorithmes suivants : SHA-256, SHA- 384, SHA-512, correspondants respectivement aux algorithmes ECCC P-256, P-384, P-521.

Chaque certificat précise le « protocole » qu’il utilise (type de clé, algorithme de hashage).

# Traitements sur les données

## Troncature des champs

Si la taille des données est plus importante que l’espace disponible dans le code à barres, alors l’information DOIT être tronquée à la taille restante.

Un champ obligatoire n’est tronqué que si la taille des champs obligatoires est supérieure à la taille disponible dans le code à barres.

Les champs facultatifs ne sont rajoutés qu’à partir du moment où de la place est disponible après l’ajout de l’ensemble des champs obligatoires.

Un champ obligatoire ne peut être tronqué pour ajouter un champ facultatif.

Un champ facultatif peut être tronqué.

## Retrait de la ponctuation

La ponctuation et les symboles peuvent être nécessaires dans certains cas, comme par exemple le symbole ‘-‘ (moins) pour décrire une somme négative. Dans d’autres cas, comme par exemple pour les nom et prénoms, la ponctuation peut être retirée, ce qui permet de limiter le nombre de caractères où l’encodage C40 nécessite de sortir du sous-ensemble de base des caractères et ainsi nécessite de prendre au moins deux valeurs C40.

# Exemple complet d’encodage : « Courrier permis à points »

Pour cet exemple, les données suivantes seront utilisées :

|  |  |
| --- | --- |
| **Données du Courrier permis à point** | **Données de signature** |
| Type de lettre : 48M  Numéro de dossier : 156985632  Civilité :MME  Nom :SPECIMEN  Prénom :NATACHA  Date de naissance :25111973  Lieu de naissance :TOULON  Date d’infraction :16DA  Heure de l’infraction : 0132  Nombre de points retirés lors de l’infraction : 4  Solde de points : 8 | Information du certificat:   * Identifiant de l’autorité de certification : FR03 * Identifiant du certificat: AIG0 * Type de clé : NIST P-256 * Algorithme de calcul du condensat : SHA-256   Date d’émission du certificat : 2 août 2017  Date de signature du CEV : 2 août 2017 |

L’objectif est d’encoder ici le CEV dans un Datamatrix de 19,2 mm de côté. Pour cette taille, le code à barres Datamatrix a une dimension de symboles de 48x48 et une capacité totale de 174 octets.

Pour encoder un « Courrier Permis à points » avec les informations précédentes, il faut suivre les étapes suivantes :

1. Il faut calculer l’espace disponible pour la zone de message en fonction de la taille du code à barres et des informations concernant le type de clé de signature. Dans le cas présent, le Tableau en 2.3 nous indique que l’on dispose de 130 caractères AN (ou valeurs C40) pour encoder la zone de message (entête non compris).
2. Il faut ensuite commencer à construire la zone de données en commençant par l’entête. Celui-ci est présenté dans le tableau suivant :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Marqueur**  **CEV** | **Version** | **Identifiant de l’AC** | **Identifiant du certificat** | **Date d’émission** | **Date de signature** | **Type de document** | **Périmètre** |
| DC | 03 | FR03 | AIG0 | 1917 | 1917 | A1 | 01 |

Les deux champs qui nécessitent un calcul sont :

* celui de la date d’émission : Il y a 6423 jours entre la date de signature le 1er janvier 2000, ce qui fait en hexadécimal 1917.
* et celui de la date de signature : Il y a 6423 jours entre la date d’e signature le 1er janvier 2000, ce qui fait en hexadécimal 1917.

1. Il faut ensuite ajouter les champs obligatoires pour un « Courrier permis à points » (cf section 2.4.3).
   1. Le champ « Type de lettre » (DI=AB) est normalisé. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] et des chiffres [0-9]. De plus, puisque c’est un champ de taille variable qui n’a pas atteint sa taille maximale, il faut utiliser un caractère <GS>. La chaine à encoder est donc AB48M<GS> et il reste (130 – 7) 123 valeurs C40 disponibles. La chaine a une longueur de 7 caractères, le caractère <GS> occupant deux valeurs C40.
   2. Le champ « Numéro de dossier » (DI=AC) est encodé en utilisant uniquement des lettres majuscules non accentuées [A-Z] et des chiffres [0-9]. La chaine à encoder est donc AC156985632<GS> et il reste (123 – 13) 110 valeurs C40 disponibles. La chaine a une longueur de 13 caractères, le caractère <GS> occupant deux valeurs C40.
   3. Le champ « Civilité » (DI=6H) est encodé en utilisant uniquement des lettres majuscules non accentuées [A-Z] et des espaces. La chaine à encoder est 6HMME<GS> et il restera (110 – 7) 103 valeurs C40 disponibles.
   4. Le champ « Nom » (DI=6G) est encodé en utilisant uniquement des lettres majuscules non accentuées [A-Z] et des espaces. La chaine à encoder est 6GSPECIMEN<GS> et il restera (103 – 12) 91 valeurs C40 disponibles.
   5. Le champ « Prénom » (DI=60) est encodé en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9], des espaces et des ‘/’ s’il y a plusieurs prénoms (au maximum 6). Les prénoms composés sont séparés par un espace. Les différents prénoms sont séparés par ‘/’. La chaine à encoder est 60NATACHA<GS> et il restera (91 – 11) 80 valeurs C40 disponibles.
   6. Le champ « Date de naissance » (DI=69) est composé uniquement de 8 chiffres au format JJMMAAAA où JJ représente le jour dans le mois, MM le mois et AAAA l’année. Le jour et le numéro du mois sont encodés sur 2 chiffres préfixés par 0 si nécessaire. La chaine à encoder est 6925111973 et il restera (80 – 10) 70 valeurs C40 disponibles.
   7. Le champ « Lieu de naissance » (DI=6A) est encodé en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces. La chaine à encoder est 6ATOULON<GS> et il restera (70 – 10) 60 valeurs C40 disponibles.
   8. Le champ « Date d’infraction » (DI=AD) est encodé en nombre de jours après le 01/01/2000 en hexadécimal. La chaine à encoder est AD16D4 et il restera (60 – 6) 54 valeurs C40 disponibles.
   9. Le champ « Heure de l’infraction » (DI=AE) est encodé au format HHmm. La chaine à encoder est AE0132 et il restera (54 – 6) 48 valeurs C40 disponibles.
   10. Le champ « Nombre de points retirés lors de l’infraction » (DI=AF) prend une valeur entre 0 à 35 points, encodée en base 36 [0-9][A\_Z]. La chaine à encoder est AF4 et il restera (48 – 3) 45 valeurs C40 disponibles.
   11. Le champ « Solde de points » (DI=AG) prend une valeur entre 0 à 35 points, encodée en base 36 [0-9][A\_Z]. La chaine à encoder est AG8 et il restera (45 – 3) 42 valeurs C40 disponibles.
2. Après l’encodage des champs obligatoires, il est possible d’ajouter des champs facultatifs tant qu’il reste de la place.
3. La zone de données est donc égale à la chaîne suivante :

DC03FR03AIG019171917A101AB48M<GS>AC156985632<GS>6HMME<GS>6GSPECIMEN<GS>60NATACHA<GS>69251119736ATOULON<GS>AD16D4AE0132AF4AG8

1. Une fois la zone de données construite, celle-ci doit être hachée et signée en fonction des données de l’émetteur. Dans cet exemple, il faut d’abord calculer le condensat en utilisant l’algorithme SHA-256, puis de signer avec l’algorithme ECDSA avec la clé de type NIST P-256.
2. Une fois la signature au format binaire obtenue, il faut convertir cette signature au format Base32. La taille d’une signature pour une clé de type NIST P-256 est de 64 octets, ce qui correspond à 103 caractères (une fois le(s) caractère(s) de padding retiré) en Base32 précédés par le caractère <US> indiquant le début de la signature. Ainsi, le message à encoder en C40 correspond à la chaine suivante :

DC03FR00000117491766A102AB48M<GS>AC156985632<GS>6HMME<GS>6GSPECIMEN<GS>60NATACHA<GS>69251119736ATOULON<GS>AD16D4AE0132AF4AG8<US><suite de 103 valeurs Base32>

1. L’étape suivante consiste à encoder le message en Datamatrix selon le format présenté dans la section 2.3.

La zone à encoder en C40 a une taille de 217 valeurs C40 (24 pour l’entête, 88 pour la zone de message, 2 pour le séparateur <US> et 103 pour la signature.

L’encodage de ces valeurs C40, conformément à la section 2.3, occupe 147 octets (1 octet pour le passage en C40 et 146 pour le message lui-même), il ne reste donc que 27 octet disponible(s).

1. Il est nécessaire d’occuper l’intégralité de l’espace disponible, donc il faut ajouter des octets de padding. Pour cela, il faut d’abord repasser au format ASCII en ajoutant un octet de valeur 254 pour quitter l’encodage C40. Cet octet supplémentaire permet d’occuper l’intégralité de l’espace du Datamatrix

|  |  |
| --- | --- |
| Code 2D-Doc | C:\Users\gilles\AppData\Local\Microsoft\Windows\INetCache\Content.Word\06.png |
| Date d’émission | 1749 – 27 avril 2016 |
| Date de signature | 1766 – 26 mai 2016 |

|  |  |  |
| --- | --- | --- |
| Type de document | Courrier Permis à points – code A1 | |
| Périmètre | Code 01 | |
| Champs obligatoires | AB | 48M |
| AC | 156985632 |
| 6H | MME |
| 6G | SPECIMEN |
| 60 | NATACHA |
| 69 | 25111973 |
| Champs facultatifs | 6A | TOULON |
| AD | 16D4 (ce qui correspond à la date du 1er janvier 2016) |
| AE | 0132 |
| AF | 4 |
| AG | 8 |
| Message complet | DC03FR03AIG019171917A102AB48M<GS>AC156985632<GS>6HMME<GS>6GSPECIMEN<GS>60NATACHA<GS>69251119736ATOULON<GS>AD16D4AE0132AF4AG8<US>HXL6WSGWBIFFY2XKLCM6IA2EMWT7YVP3W2O5KZCG3URIZGZWQO75R5MEMNP5JWYANTFVXFG2X5CO4FKIQWT46TC7CUKRNRIKCFIMWAQ | |
| Données signées | DC03FR03AIG019171917A102AB48M<GS>AC156985632<GS>6HMME<GS>6GSPECIMEN<GS>60NATACHA<GS>69251119736ATOULON<GS>AD16D4AE0132AF4AG8 | |
| Signature (binaire) | 3D D7 EB 48 D6 0A 0A 5C 6A EA 58 99  E4 03 44 65 A7 FC 55 FB B6 9D D5 64  46 DD 22 8C 9B 36 83 BF D8 F5 84 63  5F D4 DB 00 6C CB 5B 94 DA BF 44 EE  15 48 85 A7 CF 4C 5F 15 15 16 C5 0A  11 50 CB 02 | |