**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 :**

**« Certificat qualité de l’air »**

#### Spécimen CEV « Certificat qualité de l’air » :



#### C’est l’autorité régalienne qui décide des évolutions du « Certificat qualité de l’air ».

#### Historique des versions

**AIGCEV** **ANTS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Version* | *Date* |  | *Version* | *Date* |
|  |  |  | 3.0.0 | 14 février 2017 |
| 1.0 | 04 octobre 2017 |  | 3.0.4 | 06 septembre 2017 |
| 1.1 | 01 mars 218 |  |  |  |
| 1.2 | 01 mai 2018 |  |  |  |
|  |  |  |  |  |

Table des matières

[1 Introduction 3](#_Toc512961888)

[2 Documents de type « Certificat qualité de l’air » 5](#_Toc512961889)

[2.1 Format, type de document et périmètre 5](#_Toc512961890)

[Entête en Version 3 (V3) exclusivement 5](#_Toc512961891)

[2.2 Représentation graphique et position du CEV 6](#_Toc512961892)

[2.2.1 Format graphique du CEV « Certificat Qualité de l’Air » 6](#_Toc512961893)

[2.2.2 Marquage du code à barres 6](#_Toc512961894)

[2.2.3 Positionnement du CEV 6](#_Toc512961895)

[2.2.4 Zone vierge 6](#_Toc512961896)

[2.3 Dimension 7](#_Toc512961897)

[2.4 Message 8](#_Toc512961898)

[2.4.1 Identifiants de données non spécifiques au « Certificat qualité de l’air » 8](#_Toc512961899)

[2.4.2 Identifiants de données propres au type de document « Certificat qualité de l’air » 10](#_Toc512961900)

[2.4.3 Données obligatoires et facultatives propres au Certificat qualité de l’air 13](#_Toc512961901)

[2.5 Signature des données et type de sécurité 13](#_Toc512961902)

[3 Traitements sur les données 14](#_Toc512961903)

[3.1 Troncature des champs 14](#_Toc512961904)

[3.2 Retrait de la ponctuation 14](#_Toc512961905)

[4 Exemple complet d’encodage : « Certificat qualité de l’air » 15](#_Toc512961906)

# 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 « Certificat qualité de l’air »

## Format, type de document et périmètre

### Entête en Version 3 (V3) exclusivement

Le type de document « Certificat qualité de l’air » est défini dans le format d’encodage C40, avec un entête au format DC-C40. Aucun passage au format binaire n’est autorisé.

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 ‘**A0**’, spécifiquement attribuée au « Certificat Qualité de l’Air ».

Le champ « Périmètre » prend la valeur ‘**01**’ qui correspond au Périmètre « Régalien » qui contient le Type « Certificat qualité de l’air ».

|  |  |
| --- | --- |
| Marqueur | DC |
| Version | 03 |
| Identifiant de l’AC | FR03 |
| Identifiant du certificat | AIG0 |
| Date d’émission | 1917 |
| Date de signature | 1917 |
| Type de document | A0 |
| Périmètre | 01 |
| Entête | **DC03FR03AIG019171917A001** |

L’Entête se compose de 24 caractères.

## Représentation graphique et position du CEV

### Format graphique du CEV « Certificat Qualité de l’Air »

Le mode de représentation graphique retenu pour le CEV « Certificat Qualité de l’Air » 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 « Certificat Qualité de l’Air », 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-DOC, sur l’un des quatre côtés comme indiqué ci-dessous.

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

NB : les codes ci-dessus ne sont pas opérationnels

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

Dans les cas où le dispositif d’impression n’est pas connu lors de la génération du CEV, la taille minimale recommandée pour les modules est de 0.4mm.

Dans le cas où le dispositif d’impression et le support d’impression sont connus lors de la génération du CEV, la taille minimale du module DEVRAIT être définie de telle sorte que le CEV soit lisible en utilisant un scanner 600 dpi.

De manière générale, les problématiques d’impression et de lecture doivent être prises en compte dans la définition d’un CEV. En particulier, les scénarios d’utilisation d’un CEV doivent être étudiés pour s’assurer de la qualité globale de la solution mise en œuvre. En effet, les erreurs ou impossibilités ou difficultés de lecture peuvent handicaper significativement une solution intégrant un CEV. La technologie d’impression ainsi que le type de support sont des éléments importants. Par exemple des impressions laser, jet d’encre ou argentique donneront des résultats très différents. De même qu’une impression sur papier blanc standard donnera un résultat très différent de celui obtenu sur un papier coloré ou sécurisé.

La robustesse de la lecture et du décodage doit être prise en compte dans la détermination du mode de représentation du CEV. En particulier, si la symbologie permet de faire varier la quantité d’information présente dans le code pour corriger d’éventuelles erreurs de lecture, le niveau de celle-ci ne doit pas être choisi au détriment de la bonne lecture du CEV.

Le niveau de contraste entre le code et le fond du document doit aussi être pris en compte.

Dans le cas d’un support physique pérenne, la résistance du code dans le temps doit aussi faire partie des considérations à prendre en compte pour le choix du format, la taille du module et le type d’impression.

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.

La taille minimale du code est de 19,2 mm (20 mm avec la Zone blanche).

| **Taille d'un côté Datamatrix** | **Capacité de stockage du Datamatrix** | **Capacité de la zone de messages (Nombre de caractères AN)**  **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 |

## Message

Les données qui peuvent être encodées dans le type de document « Certificat qualité de l’air » sont indiquées ci-après.

### Identifiants de données non spécifiques au « Certificat qualité de l’air »

|  |  |
| --- | --- |
| **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 « Certificat qualité de l’air »

|  |  |
| --- | --- |
|  |  |
| **Pays ayant émis l’immatriculation du véhicule**   |  |  | | --- | --- | | *ID* | A0 | | *Taille Min.* | 2 | | *Taille Max.* | 2 | | *Type* | Alphanumérique | | *Description* | Le pays est encodé en utilisant son code pays au format ISO3166-1 Alpha 2 |   **Immatriculation du véhicule**   |  |  | | --- | --- | | *ID* | A1 | | *Taille Min.* | 0 | | *Taille Max.* | 17 | | *Type* | Alphanumérique | | *Description* | Cette donnée correspond au champ A du certificat d’immatriculation. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées, des chiffres, des espaces ou des tirets [A-Z][0-9 -]. |   **Marque du véhicule**   |  |  | | --- | --- | | *ID* | A2 | | *Taille Min.* | 4 | | *Taille Max.* | 4 | | *Type* | Alphanumérique | | *Description* | Cette donnée correspond au champ A du certificat d’immatriculation. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées, des chiffres, des espaces ou des tirets [A-Z][0-9 -]. |   **Nom commercial du véhicule**   |  |  | | --- | --- | | *ID* | A3 | | *Taille Min.* | 8 | | *Taille Max.* | 8 | | *Type* | Numérique | | *Description* | Cette donnée correspond au champ A du certificat d’immatriculation. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées, des chiffres, des espaces ou des tirets [A-Z][0-9 -]. |   **Numéro de série du véhicule (VIN)**   |  |  | | --- | --- | | *ID* | A4 | | *Taille Min.* | 17 | | *Taille Max.* | 17 | | *Type* | Alphanumérique | | *Description* | Cette donnée correspond au champ E du certificat d’immatriculation. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées et des  chiffres [A-Z0-9]. Des espaces peuvent être utilisés pour suffixer les numéros de série ayant une taille inférieure à la taille du champ. |   **Catégorie du véhicule**   |  |  | | --- | --- | | *ID* | A5 | | *Taille Min.* | 3 | | *Taille Max.* | 3 | | *Type* | Alphanumérique | | *Description* | Cette donnée est extraite du champ J du certificat d’immatriculation. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées, des chiffres et des espaces [A-Z] [0-9 ]. |   **Carburant**   |  |  | | --- | --- | | *ID* | A6 | | *Taille Min.* | 2 | | *Taille Max.* | 2 | | *Type* | Alphanumérique | | *Description* | Cette donnée est extraite du champ J du certificat d’immatriculation. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées, des chiffres et des espaces [A-Z][0-9]. |   **Taux d’émission de CO2 du véhicule (en g/km)**   |  |  | | --- | --- | | *ID* | A7 | | *Taille Min.* | 3 | | *Taille Max.* | 3 | | *Type* | Alphanumérique | | *Description* | Cette donnée correspond au champ V.7 du certificat d’immatriculation. L’entier correspondant à cette donnée est encodée en hexadécimal préfixé par des 0 si  nécessaire. Cette donnée est encodée en utilisant [0-9][A-F]. |   **Classe environnementale de réception CE**   |  |  | | --- | --- | | *ID* | A8 | | *Taille Min.* | 0 | | *Taille Max.* | 12 | | *Type* | Alphanumérique | | *Description* | Cette donnée est extraite du champ V.9 du certificat d’immatriculation. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées, des chiffres, des espaces et des barres obliques [A-Z][0-9 /]. |   **Classe d’émission polluante**   |  |  | | --- | --- | | *ID* | A9 | | *Taille Min.* | 3 | | *Taille Max.* | 3 | | *Type* | Alphanumérique | | *Description* | Le champ classe d’émission polluante contient un agrégat de 3 valeurs chacune encodée sur un caractère alphanumérique majuscules sans accents dans l’ordre suivant :  Le premier caractère indique la version de la spécification concernant la classe d’émission polluante. Actuellement, seule la version initiale (c’est-à-dire la version 0) est définie et autorisée.  Le second caractère indique la classe du véhicule lui-même  Le troisième caractère indique le motif de sur-classement du véhicule.  Pour la version initiale, les valeurs possibles pour la classe du véhicule (du moins polluant au plus polluant) sont les suivantes :  Encodage Signification E Véhicule électrique   1. Classe 1 2. Classe 2 3. Classe 3 4. Classe 4 5. Classe 5 6. Classe 6   La version initiale ne définit aucun motif de sur-classement du véhicule, donc la seule valeur autorisée est 0 indiquant l’absence de motif. |   **Date de première immatriculation du véhicule**   |  |  | | --- | --- | | *ID* | AA | | *Taille Min.* | 8 | | *Taille Max.* | 8 | | *Type* | Numérique | | *Description* | Cette donnée correspond au champ B du certificat d’immatriculation. 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. | | |

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

### 2.4.3 Données obligatoires et facultatives propres au Certificat qualité de l’air

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **Type de Document** | | | |
| **ID** | **Description** |  |  | **A0** |  |
| **A0** | Pays ayant émis l’immatriculation du véhicule. |  |  | O |  |
| **A1** | Immatriculation du véhicule |  |  | O |  |
| **A2** | Marque du véhicule. |  |  | O |  |
| **A3** | Nom commercial du véhicule. |  |  | O |  |
| **A4** | Numéro de série du véhicule (VIN). |  |  | O |  |
| **A5** | Catégorie du véhicule. |  |  | O |  |
| **A6** | Carburant |  |  | O |  |
| **A7** | Taux d’émission de CO2 du véhicule (en g/km). |  |  | O |  |
| **A9** | Classe d’émission polluante. |  |  | O |  |
| **A8** | Classe environnementale de réception CE |  |  | F |  |
| **AA** | Date de première immatriculation du véhicule |  |  | 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 : « Certificat qualité de l’air »

Pour cet exemple, les données suivantes seront utilisées :

|  |  |
| --- | --- |
| **Données du Certificat qualité de l’air** | **Données de signature** |
| Pays ayant émis l’immatriculation du véhicule : FR  Immatriculation du véhicule : BH-999-VX  Marque du véhicule : RENAULT  Nom commercial du véhicule : MEGANE SCENIC  Numéro de série du véhicule (VIN) :  1M8GDM 9AXKP042788  Catégorie du véhicule : M1 *suffixé avec un espace*  Carburant : GO  Taux d’émission de CO2 du véhicule :082  Classe d’émission polluante : 050  Classe environnementale de réception CE :  2008EURO5  Date de première immatriculation du véhicule :  01011999 | 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 document : 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 Data Matrix a une dimension de symboles de 48x48 et une capacité totale de 174 octets.

Pour encoder un « Certificat Qualité de l’Air » 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 | A0 | 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 Certificat Qualité de l’Air (cf section 2.4.3).
   1. Le champ « Pays ayant émis l’immatriculation du véhicule » (DI=A0) est encodé en utilisant le code pays au format ISO3166-1 Alpha 2. La chaîne à encoder est donc A0FR et il reste (130-4) 126 valeurs C40 disponibles.
   2. Le champ « Immatriculation du véhicule » (DI=A1) est encodé en utilisant uniquement des lettres majuscules non accentuées, des chiffres, des espaces ou des tirets [A-Z0-9 -]. Cette donnée correspond au champ A du certificat d’immatriculation. La chaine à encoder est A1BH-999-VX<GS> et il reste (126 - 15) 111 valeurs C40 disponibles. Puisque c’est un champ de taille variable qui n’a pas atteint sa taille maximale, il faut utiliser un caractère <GS>.
   3. Le champ « Marque du véhicule » (DI=A2) est encodé en utilisant uniquement des lettres majuscules non accentuées, des chiffres, des espaces ou des tirets [A-Z0-9 -]. Cette donnée correspond au champ A du certificat d’immatriculation. La chaine à encoder est A2RENAULT<GS> et il reste (111 - 11) 100 valeurs C40 disponibles.
   4. Le champ « Nom commercial du véhicule » (DI=A3) est encodé en utilisant uniquement des lettres majuscules non accentuées, des chiffres, des espaces ou des tirets [A-Z0-9 -]. Cette donnée correspond au champ A du certificat d’immatriculation. La chaine à encoder est A3MEGANE SCENIC<GS> et il reste (100 - 17) 83 valeurs C40 disponibles.
   5. Le champ « Numéro de série du véhicule (VIN) » (DI=A4) est encodé en utilisant uniquement des lettres majuscules non accentuées et des chiffres [A-Z0-9]. Des espaces peuvent être utilisés pour suffixer les numéros de série ayant une taille inférieure à la taille du champ. Cette donnée correspond au champ E du certificat d’immatriculation. La chaine à encoder est A41M8GDM9AXKP042788 et il reste (83 - 19) 64 valeurs C40 disponibles.
   6. Le champ « Catégorie du véhicule » (DI=A5) est encodé en utilisant uniquement des lettres majuscules non accentuées, des chiffres et des espaces [A-Z0-9 ]. Cette donnée est extraite du champ J du certificat d’immatriculation. La chaine à encoder est A5M1 *suffixé avec un espace (cf. longueur fixe de 3)* et il reste (64 - 5) 59 valeurs C40 disponibles.
   7. Le champ « Carburant » (DI=A6) est encodé en utilisant uniquement des lettres majuscules non accentuées, des chiffres et des espaces [A-Z][0-9]. Cette donnée est extraite du champ J du certificat d’immatriculation. La chaine à encoder est A6GO et il reste (59 - 4) 55 valeurs C40 disponibles.
   8. Le champ « Taux d’émission de CO2 » (DI=A7) est encodé en hexadécimal préfixé par des 0 si nécessaire. Cette donnée est encodée en utilisant [0-9][A-F]. Cette donnée correspond au champ V.7 du certificat d’immatriculation. La chaine à encoder est A7082 et il reste (55 - 5) 50 valeurs C40 disponibles.
   9. Le champ « Classe d’émission polluante » (DI=A9) contient un agrégat de 3 valeurs chacune encodée sur un caractère alphanumérique majuscules sans accents. Le premier caractère indique la version de la spécification concernant la classe d’émission polluante (actuellement, seule la valeur 0 est autorisée). Le second caractère indique la classe du véhicule lui-même, les valeurs autorisées étant : E, 1, 2, 3, 4, 5, 6. Le troisième caractère indique le motif de sur-classement du véhicule (actuellement, seule la valeur 0 est autorisée). La chaîne à encoder est A9050 et il reste (50 – 5) 45 valeurs C40 disponibles.
   10. Le champ « Indication de la classe environnementale de réception CE » (DI=A8) est encodé en utilisant uniquement des lettres majuscules non accentuées, des chiffres, des espaces et des barres obliques [A-Z0-9 /]. Cette donnée est extraite du champ V.9 du certificat d’immatriculation. La chaîne à encoder est A82008EURO<GS> et il reste (45 – 12) 33 valeurs C40 disponibles.
   11. Le champ « Date de première immatriculation du véhicule » (DI=AA) 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. Cette donnée correspond au champ B du certificat d’immatriculation. La chaîne à encoder est AA01011999 et il reste (33 – 10) 23 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 :

DC03FR03AIG019171917A001A0FRA1BH-999-VX<GS>A2RENAULT<GS>A3MEGANE SCENIC<GS>A41M8GDM9AXKP042788A5M1 A6GOA7082A905A7082A82008EURO5<GS>AA01011999

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 :

DC03FR03AIG019171917A001A0FRA1BH-999-VX<GS>A2RENAULT<GS>A3MEGANE SCENIC<GS>A41M8GDM9AXKP042788A5M1 A6GOA7082A905A82008EURO5<GS>AA01011999<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 235 valeurs C40 (24 pour l’entête, 107 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 159 octets (1 octet pour le passage en C40 et 158 pour le message lui-même), il ne reste donc que 15 octets disponibles.

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\03.png | |
| Date d’émission | 165A – 1er septembre 2015 | |
| Date de signature | 164D - 19 août 2015 | |
| Type de document | Certificat de qualité de l’air – code A0 | |
| Périmètre | Code 01 | |
| Champs obligatoires | A0 | FR (ce qui correspond à France) |
| A1 | BH-999-VX |
| A2 | RENAULT |
| A3 | MEGANE SCENIC |
| A4 | 1M8GDM9AXKP042788 |
| A5 | M1 |
| A6 | GO |
| A7 | 082 (ce qui correspond à 130g/km) |
| A9 | 050 |
| Champs facultatifs | A8 | 2008EURO5 |
| AA | 01011999 (ce qui correspond à la date du 1er janvier 1999) |
| Message complet | DC03FR03AIG019171917A001A0FRA1BH-999-VX<GS>A2RENAULT<GS>A3MEGANE SCENIC<GS>A41M8GDM9AXKP042788A5M1 A6GOA7082A9050A82008EURO5<GS>AA01011999<US>QXLLQD5RQS4VWARLA5LV73PDTQGAYCPW7UPGHKUWJC3G5VLDR6EZUG6BM7SQVEUG2C3DT6W5DYCIUICJ455KIKLYU3SNMYX2GVWK5IQ | |
| Données signées | DC03FR03AIG019171917A001A0FRA1BH-999-VX<GS>A2RENAULT<GS>A3MEGANE SCENIC<GS>A41M8GDM9AXKP042788A5M1 A6GOA7082A9050A82008EURO5<GS>AA01011999 | |
| Signature (binaire) | 85 D6 B8 0F B1 84 B9 5B 02 2B 07 57  5F ED E3 9C 0C 0C 09 F6 FD 1E 63 AA  96 48 B6 6E D5 63 8F 89 9A 1B C1 67  E5 0A 92 86 D0 B6 39 FA DD 1E 04 8A  20 49 E7 7A A4 29 78 A6 E4 D6 62 FA  35 6C AE A2 | |