**AIGCEV / VDSIC**

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

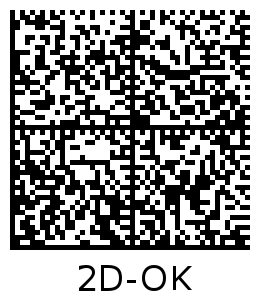
**Visible Digital Seal International Council**

**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 :**

**« Diplôme »**

#### Spécimen de CEV « Diplôme » :



#### Historique des versions

**AIGCEV**

|  |  |  |
| --- | --- | --- |
| *Version* | *Date* |  |
|  |  |  |
| 1.0 | 04 octobre 2017 |  |
| 1.1 | 01 mars 2018 |  |
| 1.2 | 01 mai 2018 |  |
|  |  |  |

|  |  |
| --- | --- |
| Membres du Périmètre Diplôme | |
| Secrétariat | Gilles Barré |
| Présidence |  |
| Vice-Présidence |  |
| Membres |  |
|  |  |
|  |  |
|  |  |

Table des matières

[1 Introduction 4](#_Toc512963819)

[2 Documents de type « Diplôme » 6](#_Toc512963820)

[2.1 Format, type de document et périmètre 6](#_Toc512963821)

[Entête en Version 3 (V3) 6](#_Toc512963822)

[2.2 Représentation graphique et position du CEV 7](#_Toc512963823)

[2.2.1 Format graphique du CEV « Diplôme » 7](#_Toc512963824)

[2.2.2 Marquage du code à barres 7](#_Toc512963825)

[2.2.3 Positionnement du CEV 7](#_Toc512963826)

[2.2.4 Zone vierge 7](#_Toc512963827)

[2.3 Dimension 8](#_Toc512963828)

[2.4 Message 9](#_Toc512963829)

[2.4.1 Identifiants de données non spécifiques au « Diplôme » 9](#_Toc512963830)

[2.4.2 Identifiants de données propres au type de document « Diplômes » 11](#_Toc512963831)

[2.4.3 Données obligatoires propres aux documents académiques 15](#_Toc512963832)

[2.5 Signature des données et type de sécurité 16](#_Toc512963833)

[3 Traitements sur les données 17](#_Toc512963834)

[3.1 Troncature des champs 17](#_Toc512963835)

[3.2 Retrait de la ponctuation 17](#_Toc512963836)

[4 Exemple complet d’encodage : « Diplôme » 18](#_Toc512963837)

# 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 « Diplôme »

## 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 ‘**B0**’, spécifiquement attribuée au « Diplôme ».

Le champ « Périmètre » prend la valeur ‘**03**’ qui correspond au Périmètre « Ressources humaines » qui contient le Type « Diplôme ».

|  |  |
| --- | --- |
| Marqueur | DC |
| Version | 03 |
| Identifiant de l’AC | FR03 |
| Identifiant du certificat | AIG0 |
| Date d’émission | 1917 |
| Date de signature | 1917 |
| Type de document | B0 |
| Périmètre | 03 |
| Entête | **DC03FR03AIG019171917B003** |

L’Entête se compose de 24 caractères.

## Représentation graphique et position du CEV

### Format graphique du CEV « Diplôme »

Le mode de représentation graphique retenu pour le CEV « Diplôme » 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 « Diplôme », 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 |  |

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 « Diplôme » sont indiquées ci-après.

### Identifiants de données non spécifiques au « Diplôme »

|  |  |
| --- | --- |
| **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’en-tête, 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’en-tête, 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 « Diplômes »

|  |  |
| --- | --- |
| **Liste des prénoms** | |
| *ID* | B0 |
| *Taille Min.* | 0 |
| *Taille Max.* | 60 |
| *Type* | Alphanumérique |
| *Description* | Les prénoms composes 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 plusoeurs prénoms (au maximum 6). |
| **Prénom** | |
| *ID* | B1 |
| *Taille Min.* | 0 |
| *Taille Max.* | 20 |
| *Type* | Alphanumérique |
| *Description* | Ce champ correspond au premier prénom de l'état civil ou au prénom d'usage. Les prénoms composés sont séparés par un espace. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces. |
| **Nom patronymique**   |  |  | | --- | --- | | *ID* | B2 | | *Taille Min.* | 0 | | *Taille Max.* | 38 | | *Type* | Alphanumérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces. Les noms composés sont séparés par un espace. |   **Nom d'usage**   |  |  | | --- | --- | | *ID* | B3 | | *Taille Min.* | 0 | | *Taille Max.* | 38 | | *Type* | Alphanumérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces. Les noms composés sont séparés par un espace |   **Nom d'épouse/époux**   |  |  | | --- | --- | | *ID* | B4 | | *Taille Min.* | 0 | | *Taille Max.* | 38 | | *Type* | Alphanumérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces. Les noms composés sont séparés par un espace. |   **Nationalité**   |  |  | | --- | --- | | *ID* | B5 | | *Taille Min.* | 2 | | *Taille Max.* | 2 | | *Type* | Alphanumérique | | *Description* | Le pays est encodé en utilisant son code pays au format ISO3166-1 Alpha 2. |   **Genre**   |  |  | | --- | --- | | *ID* | B6 | | *Taille Min.* | 1 | | *Taille Max.* | 1 | | *Type* | Alphanumérique | | *Description* | Genre masculin (M) ou féminin (F) ou autre (X). |   **Date de naissance**   |  |  | | --- | --- | | *ID* | B7 | | *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* | B8 | | *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 |   **Pays de naissance**   |  |  | | --- | --- | | *ID* | B9 | | *Taille Min.* | 2 | | *Taille Max.* | 2 | | *Type* | Alphanumérique | | *Description* | Le pays est encodé en utilisant son code pays au format ISO3166-1 Alpha 2 |   **Mention obtenue**   |  |  | | --- | --- | | *ID* | BA | | *Taille Min.* | 1 | | *Taille Max.* | 1 | | *Type* | Numérique | | *Description* | 0 aucune 1 Passable 2 Assez Bien 3 Bien 4 Très Bien 5 Très Honorable 6 Félicitations du jury. |   **Numéro ou code d'identification de l'étudiant**   |  |  | | --- | --- | | *ID* | BB | | *Taille Min.* | 0 | | *Taille Max.* | 50 | | *Type* | Alphanumérique | | *Description* | Correspond en France au numéro INE, ou à défaut d'un numéro interne à l'établissement mentionné sur le diplôme. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces. |   **Numéro de diplôme**   |  |  | | --- | --- | | *ID* | BC | | *Taille Min.* | 0 | | *Taille Max.* | 20 | | *Type* | Alphanumérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] des chiffres [0-9] et des espaces. |   **Niveau du Diplôme selon le classification CEC**   |  |  | | --- | --- | | *ID* | BD | | *Taille Min.* | 1 | | *Taille Max.* | 1 | | *Type* | Numérique | | *Description* | Entre autres : Bac=4, BTS/DUT=5, Licence=6, Master=7, Doctorat=8 |   **Crédits ECTS obtenus**   |  |  | | --- | --- | | *ID* | BE | | *Taille Min.* | 3 | | *Taille Max.* | 3 | | *Type* | Numérique | | *Description* | Entier positif. |   **Année universitaire**   |  |  | | --- | --- | | *ID* | BF | | *Taille Min.* | 4 | | *Taille Max.* | 4 | | *Type* | Numérique | | *Description* | Pour l’année 2015-2016, l’année 2016 est encodée dans le champ. |   **Type de diplôme**   |  |  | | --- | --- | | *ID* | BG | | *Taille Min.* | 2 | | *Taille Max.* | 2 | | *Type* | Alphanumérique | | *Description* | Type de diplôme : MA=Master. |   **Domaine**   |  |  | | --- | --- | | *ID* | BH | | *Taille Min.* | 0 | | *Taille Max.* | 30 | | *Type* | Alphanumérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] des chiffres [0-9] et des espaces. |   **Mention**   |  |  | | --- | --- | | *ID* | BI | | *Taille Min.* | 0 | | *Taille Max.* | 30 | | *Type* | Alphanumérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] des chiffres [0-9] et des espaces. |   **Spécialité**   |  |  | | --- | --- | | *ID* | BJ | | *Taille Min.* | 0 | | *Taille Max.* | 30 | | *Type* | Alphanumérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] des chiffres [0-9] et des espaces. | | |
|  |  |
|  |  |
|  |  |

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

### 2.4.3 Données obligatoires propres aux documents académiques

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | **Type de Document** | |
| **ID** | **Description** | | **B0** | |
| **B0** | Liste des prénoms | | O[2](#_bookmark62) | |
| **B1** | Prénom | | O | |
| **B2** | Nom patronymique | | O | |
| **B6** | Genre | | O | |
| **B7** | Date de naissance | | O | |
| **B9** | Pays de naissance | | O | |
| **BD** | Niveau du diplôme selon la nomenclature CEC | | O | |
| **BG** | Type de diplôme | | O | |
| **BH** | Domaine | | O | |
| **BI** | Mention | | O | |
| **BJ** | Spécialité | O | |

2 Les données B0 et B1 sont interchangeables.

De plus, l’ensemble des champs non mentionnés dans le tableau des catégories suivantes peuvent être utilisés en tant que champ facultatif :

* [Identifiants de données complémentaires](#_bookmark41) (cf. 2.4.1),
* [Identifiants de données pour les diplômes](#_bookmark48) (cf. 2.4.2).

Dans le tableau ci-dessous, (O) signifie Obligatoire, (F) signifie Facultative, (\_) signifie Interdite.

## 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 : « Diplôme »

Pour cet exemple, les données suivantes seront utilisées :

|  |  |
| --- | --- |
| **Données du Diplôme** | **Données de signature** |
| Prénom : Natacha  Nom patronymique : Specimen  Genre : F  Date de naissance : 12071973  Pays de naissance : FR  Niveau de diplôme : Master  Type de diplôme : Master  Domaine : Sciences Technologies Santé  Mention : Informatique  Lieu de naissance : Toulon  Spécialité : Informatique du logiciel | Information du certificat :  Identifiant de l’autorité de certification : FR03  Identifiant du certificat: AIGO  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 DataMatrix a une dimension de symboles de 48x48 et une capacité totale de 174 octets.

Pour encoder un diplôme 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 (en-tête non comprise).
2. Il faut ensuite commencer à construire la zone de données en commençant par l’en-tête. Celle-ci est présentée 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 | B0 | 03 |

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 Diplôme (cf. section 2.4.3).
   1. Le champ « Prénom » (DI=B1) correspond au premier prénom de l'état civil ou au prénom d'usage. Les prénoms composés sont séparés par un espace. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces. 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 B1NATACHA<GS> et il reste (130 – 11) 119 valeurs C40 disponibles. La chaine a une longueur de 11 caractères, le caractère <GS> occupant deux valeurs C40.

* 1. Le champ « Nom patronymique » (DI=B2) est encodé en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces. Les noms composés sont séparés par un espace.

La chaine à encoder est donc B2SPECIMEN<GS> et il reste (119 – 12) 107 valeurs C40 disponibles.

* 1. Le champ « Genre » (DI=B6) peut prendre 3 valeurs : Genre masculin (M) ou féminin (F) ou autre (X). La chaine à encoder est B6F et il reste (107 - 3) 104 valeurs C40 disponibles.
  2. Le champ « Date de naissance » (DI=B7) 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 chaîne à encoder est B712071973 et il reste (104 – 10) 94 valeurs C40 disponibles.
  3. Le champ « Pays de naissance » (DI=B9) est encodé en utilisant son code pays au format ISO3166-1 Alpha 2 (France = FR). La chaîne à encoder est B9FR et il reste (94 -4) 90 valeurs C40 disponibles.
  4. Le champ « Niveau de diplôme » (DI=BD) est encodé selon la nomenclature CEC. Entre autres : Bac=4, BTS/DUT=5, Licence=6, Master=7, Doctorat=8. La chaîne à encoder est BD7 et il reste (90 – 3) 87 valeurs C40 disponibles.
  5. Le champ « Type de diplôme » (DI=BG) s’encode sur 2 valeurs alphanumériques. Il prend ici la valeur MA pour Master. La chaine à encoder est BGMA et il restera (87 – 4) 83 valeurs C40 disponibles.
  6. Le champ « Domaine » (DI=BH) est encodé en utilisant uniquement des lettres majuscules non accentuées [A-Z] des chiffres [0-9] et des espaces. La chaîne à encoder est BHSCIENCES TECHNOLOGIES SANTE<GS> et il restera (83 – 31) 52 valeurs C40 disponibles.
  7. Le champ « Mention » (DI=BI) est encodé en utilisant uniquement des lettres majuscules non accentuées [A-Z] des chiffres [0-9] et des espaces. La chaîne à encoder est BIINFORMATIQUE<GS> et il restera (52 – 16) 36 valeurs C40 disponibles.
  8. Le champ “Lieu de naissance” (DI=B8) est encodé en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des espaces. Ici le lieu de naissance est Toulon; la chaîne à encoder est B8TOULON<GS> et il ne restera (36 – 10) 26 valeurs C40 disponibles.
  9. Le champ « Spécialité » (DI=BJ) est encodé en utilisant uniquement des lettres majuscules non accentuées [A-Z] des chiffres [0-9] et des espaces. De ce fait la chaîne à encoder est BJINFORMATIQUE DU LOGICIEL et il restera (26 – 26) 0 valeur C40 disponible.

1. Après l’encodage des champs obligatoires, il est possible d’ajouter des champs facultatifs tant qu’il reste de la place.
2. La zone de données est donc égale à la chaîne suivante :

DC03FR03AIG019171917B003B1NATACHA<GS>B2SPECIMEN<GS>B6FB712071973B9FRBD7BGMABHSCIENCES TECHNOLOGIES SANTE<GS>BIINFORMATIQUE<GS>B8TOULON<GS>BJINFORMATIQUE DU LOGICIEL

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 :

DC03FR03AIG019171917B003B1NATACHA<GS>B2SPECIMEN<GS>B6FB712071973B9FRBD7BGMABHSCIENCES TECHNOLOGIES SANTE<GS>BIINFORMATIQUE<GS>B8TOULON<GS>BJINFORMATIQUE DU LOGICI<RS><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 259 valeurs C40 (24 pour l’en-tête, 130 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 175 octets (1 octet pour le passage en C40 et 174 pour le message lui-même), il ne reste donc plus de place disponible.

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-OK | C:\Users\gilles\AppData\Local\Microsoft\Windows\INetCache\Content.Word\05_2D-OK-1.png | |
| Date d’émission | 1220 – 14 septembre 2012 | |
| Date de signature | 16A2 – 12 novembre 2015 | |
| Type de document | Diplôme – code B0 | |
| Périmètre | Code 01 | |
| Champs obligatoires | B1 | NATACHA |
| B2 | SPECIMEN |
| B6 | F |
| B7 | 12071973 |
| B9 | FR (ce qui correspond à France) |
| BD | 7 |
| BG | MA (ce qui correspond à Master) |

|  |  |  |
| --- | --- | --- |
|  | BH | SCIENCES TECHNOLOGIES SANTE |
| BI | INFORMATIQUE |
| BJ | INFORMATIQUE DU LOGICIEL |
| Champs facultatifs | B8 | TOULON |
| BB |  |
| BC |  |
| BF |  |
| Message complet | DC03FR03AIG019171917B003B1NATACHA<GS>B2SPECIMEN<GS>B6FB712071973B9FRBD7BGMABHSCIENCES TECHNOLOGIES SANTE<GS>BIINFORMATIQUE<GS>B8TOULON<GS>BJINFORMATIQUE DU LOGICIEL<US>UYV65YOQ6PNXV6GKTYWSLVQNB3Z573UO3CJPHIE636SFXLQLS3W3WJSSOAGCQTUDBRTSHDALIT7YUIOJPEXWUEL6DPUDZ7CNIRRSDQI | |
| Données signées | DC03FR03AIG019171917B003B1NATACHA<GS>B2SPECIMEN<GS>B6FB712071973B9FRBD7BGMABHSCIENCES TECHNOLOGIES SANTE<GS>BIINFORMATIQUE<GS>B8TOULON<GS>BJINFORMATIQUE DU LOGICIEL | |
| Signature (binaire) | A6 2B EE E1 D0 F3 DB 7A F8 CA 9E 2D 25 D6 0D 0E F3 DF EE 8E D8 92 F3 A0 9E DF A4 5B AE 0B 96 ED BB 26 52 70 0C 28 4E 83 0C 67 23 8C 0B 44 FF 8A 21 C9 79 2F 6A 11 7E 1B E8 3C FC 4D 44 63 21 C1 | |