**AIGCEV / VDSIC**

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

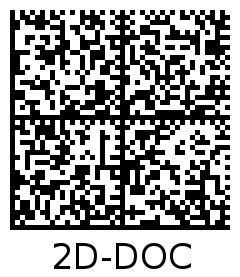
**Visible Digital Seal International Council**

**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 :**

**« Avis d’impôt sur le revenu »**

#### Spécimen de CEV d’ « Avis d’impôt sur le revenu » :



#### C’est l’autorité régalienne qui décide des évolutions de l’« Avis d’impôt sur le revenu ».

#### 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 2018 |  |  |  |
| 1.2 | 01 mai 2018 |  |  |  |
|  |  |  |  |  |

Table des matières

[1 Introduction 3](#_Toc512960551)

[2 Documents de type « Avis d’impôt sur le revenu » 5](#_Toc512960552)

[2.1 Format, type de document et périmètre 5](#_Toc512960553)

[Entête en Version 3 (V3) 5](#_Toc512960554)

[2.2 Représentation graphique et position du CEV 6](#_Toc512960555)

[2.2.1 Format graphique du CEV « Avis d’Impôt sur le Revenu » 6](#_Toc512960556)

[2.2.2 Marquage du code à barres 6](#_Toc512960557)

[2.2.3 Positionnement du CEV 6](#_Toc512960558)

[2.2.4 Zone vierge 6](#_Toc512960559)

[2.3 Dimenssion 7](#_Toc512960560)

[2.4 Message 8](#_Toc512960561)

[2.4.1 Identifiants de données non spécifiques au « Avis d’impôt sur le revenu » 8](#_Toc512960562)

[2.4.2 Identifiants de données propres au type de document « Avis d’impôt sur le revenus » 10](#_Toc512960563)

[2.4.3 Données obligatoires et facultatives des « Avis d’impôt sur le revenu » 11](#_Toc512960564)

[2.5 Signature des données et type de sécurité 12](#_Toc512960565)

[3 Traitements sur les données 13](#_Toc512960566)

[3.1 Troncature des champs 13](#_Toc512960567)

[3.2 Retrait de la ponctuation 13](#_Toc512960568)

[4 Exemple complet d’encodage : « Avis d’impôt sur le revenu » 14](#_Toc512960569)

# 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 « Avis d’impôt sur le revenu »

## 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 « Avis d’impôt sur le revenu » par l’émetteur, contient 4 caractères alphanumériques [A-Z][0-9]. Ici, 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 ‘**04**’, spécifiquement attribuée au « Avis d’impôt sur le revenu ».

Le champ « Périmètre » prend la valeur ‘**01**’ qui correspond au Périmètre « Régalien » qui contient le Type « Avis d’impôt sur le revenu ».

|  |  |
| --- | --- |
| Marqueur | DC |
| Version | 03 |
| Identifiant de l’AC | FR03 |
| Identifiant du certificat | AIG0 |
| Date d’émission | 1917 |
| Date de signature | 1917 |
| Type de document | 04 |
| Périmètre | 01 |
| **Entête** | **DC03FR03AIG0191719170401** |

En V3 l’Entête se compose de 24 caractères.

## Représentation graphique et position du CEV

### Format graphique du CEV « Avis d’Impôt sur le Revenu »

Le mode de représentation graphique retenu pour le CEV « Avis d’Impôt sur le Revenu » 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 « Avis d’Impôt sur le Revenu », 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 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.

## Dimenssion

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 « Avis d’impôt sur le revenu » sont indiquées ci-après.

### Identifiants de données non spécifiques au « Avis d’impôt sur le revenu »

|  |  |
| --- | --- |
| **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. |
| **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. |
| **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. |
| **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. |

### Identifiants de données propres au type de document « Avis d’impôt sur le revenus »

|  |  |
| --- | --- |
| **Ligne 1 de la norme adresse postale du bénéficiaire de la prestation** | |
| *ID* | 10 |
| *Taille Min.* | 0 |
| *Taille Max.* | 38 |
| *Type* | Alphanumérique |
| *Description* | Qualité – Nom – Prénom – éventuellement titre ou profession du bénéficiaire de la prestation. Les items Qualité, Nom et Prénom doivent être indiqués dans cet ordre et peuvent être séparés par le caractère ‘/’ pour faciliter leur lecture. Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9], des espaces et éventuellement des ‘/’ pour séparer les zones Qualité, Nom et Prénom. Dans le cas, d’un nom de société, il n’est pas nécessaire d’utiliser des séparateurs |
| **Qualité et/ou titre de la personne bénéficiaire de la prestation** | |
| *ID* | 11 |
| *Taille Min.* | 0 |
| *Taille Max.* | 38 |
| *Type* | Alphanumérique |
| *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] et des espaces. |
| **Prénom de la personne bénéficiaire de la prestation**   |  |  | | --- | --- | | *ID* | 12 | | *Taille Min.* | 0 | | *Taille Max.* | 38 | | *Type* | Alphanumérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] et des espaces. |   **Nom de la personne bénéficiaire de la prestation**   |  |  | | --- | --- | | *ID* | 13 | | *Taille Min.* | 0 | | *Taille Max.* | 38 | | *Type* | Alphanumérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] et des espaces. |   **Numéro fiscal**   |  |  | | --- | --- | | *ID* | 40 | | *Taille Min.* | 13 | | *Taille Max.* | 13 | | *Type* | Alphanumérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] et des espaces. |   **Revenu fiscal de référence**   |  |  | | --- | --- | | *ID* | 41 | | *Taille Min.* | 0 | | *Taille Max.* | Aucune | | *Type* | Numérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] et des chiffres [0-9] (cf. norme ISO 13616). S’il y a des espaces, ils sont retirés. |   **Situation du foyer**   |  |  | | --- | --- | | *ID* | 42 | | *Taille Min.* | 0 | | *Taille Max.* | Aucune | | *Type* | Alphanumérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] et des espaces. |   **Nombre de parts**   |  |  | | --- | --- | | *ID* | 43 | | *Taille Min.* | 0 | | *Taille Max.* | Aucune | | *Type* | Numérique | | *Description* | Le nombre de parts n’étant pas nécessairement un nombre entier, il est encodé en utilisant uniquement des chiffres[0-9] et le caractère « virgule » avec au plus deux décimales. |   **Reférence d’avis d’impôt**   |  |  | | --- | --- | | *ID* | 44 | | *Taille Min.* | 13 | | *Taille Max.* | 13 | | *Type* | Alphanumérique | | *Description* | Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] et des chiffres {0-9]. S’il y a des espaces, ils sont retirés. | | |
|  |  |
|  |  |
|  |  |
|  |  |

### 2.4.3 Données obligatoires et facultatives des « Avis d’impôt sur le revenu »

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **Type de Document** | | | |
| **ID** | **Description** |  |  | **04** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **10** | Ligne 1 de la norme adresse postale du bénéficiaire de la prestation |  |  | O\* |  |
| **11** | Qualité et/ou titre de la personne bénéficiaire de la prestation |  |  | O\* |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **12** | Prénom de la personne bénéficiaire de la prestation |  |  | O\* |  |
| **13** | Nom de la personne bénéficiaire de la prestation |  |  | O\* |  |
| **40** | Numéro fiscal |  |  | O |  |
| **41** | Revenu fiscal de référence |  |  | O |  |
| **42** | Situation du foyer |  |  | F |  |
| **43** | Nombre de parts |  |  | F |  |
| **44** | Référence d’avis d’impôt |  |  | 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.

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 : « Avis d’impôt sur le revenu »

Pour cet exemple, les données suivantes seront utilisées :

|  |  |
| --- | --- |
| **Données de l’Avis d’impôt sur le revenu** | **Données de signature** |
| Ligne 1 de la norme adresse postale du bénéficiaire de la prestation : M/IMPOSABLE/FRANCOIS  Numéro fiscal : 1234567890123  Revenu fiscal de référence : 1042876 | 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 Data Matrix a une dimension de symboles de 48x48 et une capacité totale de 174 octets.

Pour encoder un « Avis d’impôt sur le revenu » 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 | 04 | 01 |

Les deux champs qui nécessitent un calcul sont :

* celui de la date de début de période : 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 fin de période : 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 Avis d’impôt sur le revenu (cf. section 2.4.3).
   1. Le champ « Ligne 1 de la norme adresse postale du bénéficiaire de la prestation » est normalisé en mettant le champ en majuscule et en séparant le titre, nom et prénom par des ‘/’. 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 10M/IMPOSABLE/FRANCOIS<GS> et il reste (130 – 26) 104 valeurs C40 disponibles.La chaine a une longueur de 26 caractères, sachant que le caractère <GS> et le caractère ‘/’ occupent deux valeurs C40.

* 1. Le champ Numéro fiscal (DI=40) comporte toujours 13 caractères numériques. La chaîne à encoder est 401234567890123 Il reste donc (104 -15) 89 valeurs C40 disponibles.
  2. Le champ Revenu fiscal de référence (DI=41) ne comporte aucune limite. La chaine à encoder est 411042876 et il restera (89 – 9) 80 valeurs C40 disponibles. La chaine a une longueur de 9 caractères. Il n’y a pas ici de caractère <GS> pour marquer la fin de ce champ de longueur variable car c’est le dernier champ utilisé.

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 :

DC03FR03AIG019171917040110M/IMPOSABLE/FRANCOIS<GS>401234567890123411042876

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 :

DC03FR03AIGO19171917040110M/IMPOSABLE/FRANCOIS<GS>401234567890123411042876<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 179 valeurs C40 (24 pour l’entête, 50 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 121 octets (1 octet pour le passage en C40 et 120 pour le message lui-même), il ne reste donc que 53 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\Avis IRPP.PNG | |
| Date d’émission | 1917 – 2 août 2017 | |
| Date de signature | 1917 – 2 août 2017 | |
| Type de document | Avis d’impôt sur le revenu – code 04 | |
| Périmètre | Code 01 | |
| Champs obligatoires | 40 | 1234567890123 |
| 41 | 1042876 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |
|  |  |
| Message complet | DC03FR03AIG019171917040110M/IMPOSABLE/FRANCOIS<GS>401234567890123411042876<US>CGBFE6B5ASNMC3S7LFRHJ2NFOUY4XOCXR5ZAIXH3E4O6VKF47FYJNMXC435ROAHVGDUDEWB5YTACAFYTRAKGSZRAI62TZMWKHNJCSDQ | |
| Données signées | DC03FR03AIG019171917040110M/IMPOSABLE/FRANCOIS<GS>401234567890123411042876 | |
| Signature (binaire) | 11 82 52 78 3D 04 9A C1 6E 5F 59 62  74 E9 A5 75 31 CB B8 57 8F 72 04 5C  FB 27 1D EA A8 BC F9 70 96 B2 E2 E6  FB 17 00 F5 30 E8 32 58 3D C4 C0 20  17 13 88 14 69 66 20 47 B5 3C B2 CA  3B 52 29 0E | |