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 :

« Attestation de Versement de la Contribution à la Vie Etudiante »

Historique des versions

AIGCEV

Version	*Date*
1.0	11 avril 2018
1.1	19 avril 2018
1.2	23 avril 2018
1.3	17 mai 2018
1.4	17 juin 2018
1.5	09 juillet 2018

Membres du Périmètre Attestation de versement de la CVE	
Secrétariat	Gilles Barré, AIGCEV
Présidence	Michel Affre, CNOUS
Vice-Présidence	Jean-Yves Frémont, CNOUS
Membres	Yves Le Querrec, AIGCEV
	François Devoret, AIGCEV, LEX PERSONA
	Charles-Henri Menseau, AIGCEV, ANTS

Table des matières

1 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.

1.1 Structures et codage du CEV :

	Entête DC et DD	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.

1.2 Structures de l'Entête et Nombre de caractères enC40 :

	Marqueur	Version	Identifiant de l'AC	Identifiant du certificat	Date d'émission	Date de signature	Type de document	Périmètre	Pays	Nombre de 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

1.3 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 en C40, l'utilisation de la V4 est recommandée.

2 Documents de type « Attestation de Versement de la CVE »

2.1 Entête en Version 4 (V4)

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

Le champ « Version » en V4 prend la valeur '**04**'.

Le champ « Identifiant de l'AC » qui a émis le certificat utilisé pour le type « Attestation de versement à la CVE » par l'émetteur, contient 4 caractères alphanumériques [A-Z][0-9]. Ici pour l'exemple, 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 qui est 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 '**B1**', spécifiquement attribuée à « l'Attestation de versement de la Contribution à la Vie Etudiante ».

Le champ « Périmètre » prend la valeur '**01**' qui correspond au Périmètre Régalien qui contient le Type « Attestation de versement à la CVE ».

Marqueur	DC
Version	04
Identifiant de l'AC	FR03
Identifiant du certificat	AIG0
Date d'émission	1917
Date de signature	1917
Type de document	B1
Périmètre	01
Pays	FR
Entête	**DC04FR03AIG019171917B101FR**

En V4 l'Entête se compose de 26 caractères.

2.2 Représentation graphique et position du CEV

2.2.1 Format graphique du CEV « Attestation de versement de la Contribution à la Vie Etudiante »

Le mode de représentation graphique retenu pour le CEV « Attestation de versement de la Contribution à la Vie Etudiante » 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 « Attestation de versement de la Contribution à la Vie Etudiante », 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.

2.2.2 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.

2.2.3 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.

2.2.4 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.

2.2.5 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 Version 4 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	42	40	38
17,6	144	87	85	83
19,2	174	132	131	**129**
20,8	204	177	175	173
25,6	280	291	289	287
28,8	368	423	421	419
32	456	555	553	551
35,2	576	735	733	731
38,4	696	915	913	911
41,6	816	1095	1093	1091
48	1050	1446	1444	1442
52,8	1304	1827	1825	1823
57,6	1558	2208	2206	2204

2.3 Message

Les données qui peuvent être encodées dans le type de document « Attestation de Versement de la CVE» sont indiquées ci-après.

2.3.1 Identifiants de données non spécifiques au « Attestation de Versement de la CVE »

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) écoulés 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) écoulés 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.

2.3.2 Identifiants de données propres au type de document « Attestation de Versement de la Contribution à la Vie Etudiante »

Numéro de l'Attestation de versement à la CVE.
ID **BK**
Taille Min. 14
Taille Max. 14
Type Alphanumérique
Description Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z], des chiffres [0-9] et des tirets [-].

Liste des prénoms.
ID **B0**
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).

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
.

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.
.

Numéro Identifiant National Etudiant (INE)
ID **BL**
Taille Min. 11
Taille Max. 11
Type Alphanumérique
Description Cette donnée est encodée en utilisant uniquement des lettres majuscules non accentuées [A-Z] et des chiffres [0-9].

3 Données obligatoires et facultatives de l'attestation de versement de la CVE

	Périmètre :	**01**
	Type de Document :	**B1**
	Version de l'application de composition :	**V4**
ID	**Description**	
01	Identifiant unique du document.	F
02	Catégorie de document	F
03	Sous-catégorie de document	F
04	Application de composition	F
05	Version de l'application de composition	F
06	Date de l'association entre le document et le CEV	F
07	Heure de l'association entre le document et le CEV	F
08	Date d'expiration du document	F
09	Nombre de pages	F
0A	Editeur du CEV	F
0B	Intégrateur du CEV	F
BK	Numéro de l'Attestation de versement de la contribution à la vie étudiante	O
B0	Liste des Prénoms de la personne bénéficiaire de la prestation	O
B2	Nom patronymique de la personne bénéficiaire de la prestation	O
B3	Nom d'usage de la personne bénéficiaire de la prestation	O
B7	Date de naissance de la personne bénéficiaire de la prestation	O
BL	Numéro" Identifiant National Etudiant" (INE) de la personne bénéficiaire de la prestation	O

3.1 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 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'algorithme suivant : SHA-256.
Chaque certificat précise le « protocole » qu'il utilise (type de clé, algorithme de hachage).

4 Traitements sur les données

4.1 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 le codage de l'ensemble des champs obligatoires.
Un champ obligatoire ne peut être tronqué pour ajouter un champ facultatif.
Un champ facultatif peut être tronqué.

4.2 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 consommer ainsi au moins deux caractères C40.

5 Exemple complet d'encodage : « Attestation de versement de la Contribution à la Vie Etudiante »

Pour cet exemple, en **V04**, les données suivantes seront utilisées :

Données Attestation de versement à la CVE	Données de signature
Numéro de l'attestation : 18ROSWFTHR3500 Liste des Prénoms : Pierre, Alfred Nom patronymique : Dupont Date de naissance : 16 novembre 1998 Numéro INE : 9654321785T	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 Datamatrix a une dimension de symboles de 48x48 et une capacité totale de 174 octets.

Pour encoder l'Attestation de versement de la CVE 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 signatu re. Dans le cas présent, le Tableau en paragraphe 2.3 nous indique que l'on dispose de 129 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	Pays
DC	04	FR03	AIGO	1917	1917	B1	01	FR

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.

3. Il faut ensuite ajouter les champs obligatoires pour l'Attestation de versement de la CVE (cf. section 2.4.3).

   a. Pour le numéro d'Attestation (DI=BK) la valeur est directement encodée. La chaîne à encoder est donc BK18ROSWFTHR3500 et il reste (129 - 16) 113 valeurs C40 disponibles.

   b. Pour la liste des prénoms (DI=B0) les prénoms sont séparés par un '/'. 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 chaîne à encoder est donc B0PIERRE/ALFRED<GS> et il reste (113 - 18) 95 valeurs C40 disponibles.

   c. Pour le nom patronymique (DI=B2) la valeur est directement encodée. La chaîne à encoder est donc B2DUPONT<GS> et il reste (95 - 10) 85 valeurs C40 disponibles.

d. Pour le nom d'usage (DI=B3) la valeur est directement encodée. Comme c'est une donnée obligatoire, dans ce cas bien qu'il n'y ait pas de nom d'usage, il faut quand même faire apparaître ce champ, ce qui donne B3<GS> et il reste (85 - 4) 81 valeurs C40 disponibles.

e. Pour la date de naissance (DI=B7) la valeur est encodée au format JJMMAAAA. La chaîne à encoder est donc B716111998 et il reste (81 - 10) 71 valeurs C40 disponibles.

f. Pour encoder le numéro d'étudiant INE (DI=BL) la valeur est directement encodée. La chaîne à encoder est donc BL9654321785T et il reste (71 – 13) 58 valeurs C40 disponibles.

4. Après l'encodage des champs obligatoires, il est possible d'ajouter des champs facultatifs tant qu'il reste de la place.

5. La zone de données est donc égale à la chaîne suivante :

```
DC04FR03AIG019171917B101FRBK18ROSWFTHR3500B0PIERRE/ALFRED<GS>B2DUPONT<GS>B3<GS>
B716111998BL9654321785T
```

6. 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.

7. 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.
8. 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 202 valeurs C40 (26 pour l'entête, 71 pour la zone de message, 2 pour le séparateur <US> et 103 pour la signature).

9. 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	 2D-DOC	
Date d'émission	1917- 2 août 2017	
Date de signature	1917- 2 août 2017	
Type de document	Attestation de versement à la CVE – code B1	
Périmètre	Code 01	
Pays	Code FR	
Champs obligatoires	BK	18ROSWFTHR3500
	B0	Pierre Alfred
	B2	Dupont
	B3	
	B7	16111998
	BL	9654321785T
Champs facultatifs		
Message complet	DC04FR03AIG019171917B101FRBK18ROSWFTHR3500B0PIERRE/ALFRED<GS>B2DUPONT<GS>B3<GS>B716111998BL9654321785T<US>G7SJOXSFNCGTDKIOCNVTPWG6EYCPAT4NP55FMLXPC3F5GHPJP4AXQ25I46TRSDBVDUG6PTEFDW4Y4FVX2TLTYZYNGRCBGGBL6SNKNKQ	
Données signées	DC04FR03AIG019171917B101FRBK18ROSWFTHR3500B0PIERRE/ALFRED<GS>B2DUPONT<GS>B3<GS>B716111998BL9654321785T	
Signature (binaire)	37 E4 97 5E 45 68 8D 31 A9 0E 13 6B 37 D8 DE 26 04 F0 4F 8D 7F 7A 56 2E EF 16 CB D3 1D E9 7F 01 78 6B A8 E7 A7 19 0C 35 1D 0D E7 CC 85 1D B9 8E 16 B7 D4 D7 3C 67 0D 34 44 13 18 2B F4 9A A6 AA	