



1 La description

Le Cachet Electronique Visible (CEV) est une technologie réellement « disruptive », où l'écosystème est une œuvre collective avec des composantes en technologies ouvertes et normalisées.

En effet, pour en retirer le maximum de bénéfices, chaque utilisateur, émetteur de documents, offre aux autres utilisateurs la sécurisation des données sur ses propres documents et bénéficiera de la sécurité des documents émis par les autres émetteurs.

Pour augmenter l'attrait et la diffusion du système, une démarche de normalisation des principaux composants a été entreprise et est en cours d'achèvement au niveau national, et bientôt lancé au niveau mondial.

Le Cachet Electronique Visible (CEV) est un dispositif qui garantit l'origine et l'intégrité des données clés d'un document, quel que soit le support, électronique ou papier. Pour ce faire, le CEV encapsule ces données clés, accompagnées de leur signature électronique dans un code 2dimensions.

Cette signature étant générée par le serveur de l'émetteur, elle prend le nom de cachet (seal en anglais), appellation retenue pour distinguer la signature d'un serveur de la signature électronique personnelle. Le bénéfice de la présence de ce cachet électronique est d'authentifier très fortement l'émetteur du document, ainsi que les données qui ont été signées. Ces données, valides au moment de la génération du cachet, bénéficient de la non-répudiation par son émetteur. La date de validité de ces données fait partie des données signées électroniquement.

Pour réaliser l'éco système de confiance, il est nécessaire de spécifier :

1. Les données que l'on va inclure dans le cachet,
2. Le support de restitution (Datamatrix, QR Code, Alphacode, Aztec, etc...),
3. Les exigences sécuritaires attendues des autorités de certification qui vont délivrer les cachets serveurs aux émetteurs de document,
4. Les profils techniques des certificats cachet serveurs,
5. Les formats de signature électroniques,
6. Les agréments et labellisation des différentes parties prenantes de l'écosystème de confiance (Autorités de certifications, Intégrateurs de solution d'émission et de lecture)

L'objectif de l'Association Internationale de Gouvernance du cachet Electronique Visible, AIGCEV, est d'assurer la gouvernance nécessaire à l'administration de ce nouvel écosystème de confiance, d'organiser collectivement la définition du format des données propres à chaque document, et d'accompagner l'ensemble dans les processus de normalisation tant en France qu'en Europe et dans le monde entier.

2 L'origine

Le « 2D-Doc » est le premier CEV interopérable. Il est né du besoin de sécuriser les justificatifs de domicile présentés lors de la demande de passeport. Le Ministère de l'Intérieur ayant identifié qu'ils constituaient le maillon faible de la délivrance de ce titre. Maillon faible, suite au développement de la dématérialisation, avec le remplacement d'un document imprimé par le fournisseur par un document imprimé par l'abonné et facilement modifiable à l'aide de logiciels disponibles sur tous les postes de travail.

A la recherche d'une technologie fiable et très peu coûteuse, adaptée à ce besoin de sécurisation, l'Agence Nationale des Titres Sécurisés (ANTS) a retenu la proposition d'AriadNEXT, société rennaise spécialisée dans l'enrôlement sécurisé dématérialisé.

C'est de leur travail commun qu'est née la solution « 2D-Doc » qui est maintenant opérationnelle, notamment les attestations de contrat EDF étant aujourd'hui revêtues d'un « 2D-Doc », comme les factures Bouygues Télécom et bientôt les attestations de contrat d'Engie.

Tout postulant à un Passeport peut se procurer immédiatement son attestation de contrat EDF en se connectant sur son espace personnel, rubrique « Contrat », sur le site www.EDF.fr.

Le groupe de travail, monté par le Ministère de l'Intérieur et l'ANTS a dès son origine été étendu à d'autres communautés comme la profession bancaire avec le Comité Français d'Organisation et de Normalisation Bancaire(CFONB), le Ministère de l'Economie et des Finances, la Délégation Nationale de la Lutte contre la Fraude (DNLF) et d'industriels ou associations liés au document (Groupe La Poste, Fédération des Tiers de Confiance du Numérique (FNTC), AriadNEXT, Lex Persona, Dhimyotis, ...).

3 Les autres avantages du CEV

Plus qu'une simple sécurisation des données, le CEV est aussi un véritable pont, chaînon manquant, entre applications, sans avoir à recourir et à développer de complexes processus de transferts de données.

En effet, l'enrôlement dans une application passe toujours par une phase de saisie/vérification de données. Phase coûteuse et source de dysfonctionnements suite aux erreurs de retranscription de la saisie (et malgré le recours, aussi très lourd, d'algorithmes de détection/correction d'erreur).

Il suffit de lire, contrôler, et importer les données contenues dans le CEV pour à la fois réduire le coût, vérifier automatiquement et fiabiliser l'ensemble du processus.

4 Le contexte juridique

Décret no 2013-629 du 16 juillet 2013 modifiant le décret no 2000-1277 du 26 décembre 2000 portant simplification de formalités administratives et suppression de la fiche d'état civil

Art. 1er L'article 6 du décret du 26 décembre 2000 susvisé est complété par deux alinéas ainsi rédigés :

« Les pièces justificatives de domicile présentées en vue de l'obtention d'un titre d'identité, de voyage, de séjour, d'un certificat d'immatriculation d'un véhicule ou de la délivrance d'une attestation d'accueil ou de l'inscription volontaire sur les listes électorales, comportant un dispositif technique en assurant l'authenticité, ne peuvent être refusées par les services chargés de l'instruction de ces procédures. Un arrêté du ministre de l'intérieur fixe les conditions de mise en œuvre de ce dispositif. »

Arrêté du 27 septembre 2013 relatif à la sécurisation des pièces justificatives de domicile requises pour la délivrance d'un titre d'identité au moyen d'un dispositif électronique propre à garantir l'authenticité

Art. 1er. – La sécurisation des pièces justificatives mentionnées au troisième alinéa de l'article 6 du décret du 26 décembre 2000 susvisé dans sa version issue du décret no 2013-629 du 16 juillet 2013 s'effectue par l'insertion d'un code-barres à deux dimensions, dénommé 2D-doc.

Art. 4. – A compter du 1er novembre 2013, les dispositions du troisième alinéa de l'article 6 du décret du 26 décembre 2000 susvisé dans sa version issue du décret no 2013-629 du 16 juillet 2013 s'appliquent aux demandes de passeport.

La présentation de justificatifs de domicile revêtus d'un « 2D-Doc » a rapidement permis d'identifier des demandes frauduleuses, qui sans cela n'aurait pas été identifiées.

5 La place de la FNTC

La Fédération des Tiers de Confiance du Numérique (FNTC) s'est intéressée très tôt aux travaux menés par l'ANTS, et les a identifiés comme une avancée majeure. C'est ainsi qu'elle a décerné en 2011, à l'occasion de la 9^{ème} édition des Trophées de la Confiance dans l'économie numérique, le Trophée de l'Innovation des Tiers de Confiance à AriadNEXT, et le Trophée de la Promotion de la Confiance dans l'Economie numérique à l'ANTS.

Le référencement des Editeurs de solution par l'ANTS nécessitant la vérification préalable de leurs applicatifs, l'ANTS n'ayant pas vocation à y procéder elle-même, s'est appuyée sur la FNTC qui a créé les Labels Cachet Electronique Visible « mention 2D-Doc » tant pour la Génération que pour la Vérification. Leur obtention par les Editeurs est devenue la condition préalable au référencement de leurs solutions par l'ANTS. La dénomination « Cachet Electronique Visible » est d'ailleurs l'invention du Groupe de travail « Mode Hybride » de la FNTC.

L'ANTS ayant annoncé, fin 2014, son impossibilité d'administrer d'autres documents que ceux émis ou utilisés par la sphère publique, a proposé à la FNTC de reprendre la partie relative à la sphère privée. La FNTC a accueilli très favorablement cette proposition en construisant, avec le concours de l'ANTS, un écosystème spécifique pour donner le maximum de chance de réussite à ce projet.

Pour cela, en accord avec l'ANTS, la FNTC a décidé :

- de porter le CEV à la normalisation pour augmenter la visibilité de ce concept, tout en assurant le financement du processus,
- et de créer une Association Internationale de Gouvernance du Cachet Électronique Visible, AIGCEV, afin de créer les conditions nécessaires au développement de l'utilisation du CEV dans un environnement sécurisé.

6 La démarche de normalisation

Dès 2015, une démarche de normalisation du CEV a été entreprise auprès de l'AFNOR, membre officiel français auprès des Organisations Internationales de Normalisation CEN (Comité Européen de Normalisation) et ISO (Organisation Internationale de Normalisation).

Cette démarche pragmatique se concrétisera par une Norme Expérimentale en tout début 2017, qui sera suivie par un travail de promotion à l'international pour rédiger une norme ISO en 2018. A noter, que l'avancée actuelle des travaux, déjà stabilisés sur l'objectif et la définition technique, a permis d'en faire la promotion le 14 octobre 2016 lors d'un atelier sur les « Breeder Documents » à Berlin. Cet atelier s'est déroulé dans le cadre des projets européens ORIGINS et FIDELITY sur ce sujet.

L'objectif de la Norme est de définir un format d'enveloppe (partie 1) commun à tous les CEV, un dictionnaire de données communes (partie 2) et un premier cas d'usage (partie 3) qui est repris du cas d'usage justificatif de domicile déjà en production en France.

D'autres documents cas d'usage pourront, en fonction de la volonté des parties prenantes, faire l'objet d'une norme garantissant l'interopérabilité du format de données et de restitution graphique.

Sans passer nécessairement par la normalisation, tous les autres cas d'usages pourront être imaginés grâce au travail de l'AIGCEV.

La partie 1 de la norme, fruit de la réflexion étendue, grâce à l'AFNOR, à un groupe de travail regroupant l'ensemble des représentants de l'économie, de l'industrie, des pouvoirs publics et des représentants tiers (consommateurs en particulier), reprend non seulement les travaux identifiés (2D-Doc pour la France, BSI (Bundesamt für Sicherheit in der Informationstechnik, Agence de la Sécurité des Systèmes d'information pour l'Allemagne, ICAO (International Civil Aviation Organization) pour l'aéronautique internationale) en respectant une compatibilité ascendante, mais propose également des avancées vers la gestion de fonctions supplémentaires comme :

1. La gestion des données binaires en plus des données textes (photo par exemple)
2. La récupération d'une copie originale du document en coffre-fort numérique,
3. La gestion des codes de représentation de caractères élargie à l'ensemble des polices ISO 8859-XX et UTF8 et UTF16,
4. La possibilité de placer des données complémentaires non signées, mais intéressant la récupération automatique de données, autre fonction fondamentale du CEV.

Il existe 4 types de CEV :

Type A : Assure la compatibilité ascendante avec le 2D-Doc et inclut les données binaires.

Type A			
Parties			
1	2		3
EN-TETE	MESSAGE		SIGNATURE
	DI	Donnée 1 DI Donnée 2 DI Donnée 3 GS ... DI Donnée n RS	
Données signées			
Encodage C40	Encodage C40 puis éventuellement binaire en TLV sans retour possible au C40		Binaire
Magic Number = DC	Champs Textes en C40		

Type B : Assure la compatibilité ascendante avec le format du BSI, son utilisation est réservée au BSI et à l'ICAO.

Type B			
Parties			
1	2		3
EN-TETE	MESSAGE		SIGNATURE
	DI	Donnée 1 DI Donnée 2 DI Donnée 3 ... DI Donnée n	
Données signées			
Encodage binaire	Encodage Binaire TLV		Binaire
Magic Number = DC	Champs Texte en C40		

Type C : Embarque les dispositifs complémentaires à partir du Type A

Type C				
Parties				
1	2		3	4
EN-TETE	MESSAGE		SIGNATURE	ANNEXE
	DI	Donnée 1 DI Donnée 2 DI Donnée 3 GS ... DI Donnée n RS		
Données signées				
Encodage C40	Encodage C40 puis éventuellement binaire en TLV sans retour possible au C40		Binaire	Idem Message
Magic Number = DD	Champs textes en C40, ISO 8859-XX, UTF 8 ou UTF16			Idem Message

Type D : Embarque les dispositifs complémentaires à partir du type B

Type D				
Parties				
1	2		3	4
EN-TETE	MESSAGE		SIGNATURE	ANNEXE
	DI	Donnée 1 DI Donnée 2 DI Donnée 3 ... DI Donnée n		
Données signées				
Encodage binaire	Encodage Binaire TLV		Binaire	Idem Message
Magic Number = DD	Champs textes en C40, ISO 8859-XX, UTF 8 ou UTF16			Idem Message

La partie 2 de la norme définit le dictionnaire des données normalisées et leur format. Les émetteurs de documents doivent respecter ce format pour que les CEV puissent être lus par toutes les applications référencées, et donc être interoperables.

L'AIGCEV a pour rôle de vérifier le respect de l'usage des parties 1 et 2 de la norme par tous les acteurs de l'écosystème de confiance.

La partie 3 de la norme, cas d'usage du Type A, définit les données, les algorithmes de troncature éventuels de ces données lorsqu'elles dépassent les 35 caractères de l'adresse normalisée et le format de restitution (Datamatrix) pour les justificatifs de domicile français.



7 L'Association Internationale de Gouvernance du Cachet Electronique Visible (AIGCEV).

L'AIGCEV a été constituée le 12 octobre 2016.

Elle matérialise le rapprochement des intérêts publics et privés dans une entité associative loi de 1901 commune pour créer et opérer les CEV au niveau international.

7.1 Son objet :

L'Association a pour objet de développer et promouvoir un système intersectoriel et international du CEV, conçu initialement par l'ANTS, en rassemblant les acteurs présents et futurs, directs ou indirects. L'Association agit en qualité d'Opérateur de Services de Confiance, tiers de confiance du CEV. A ce titre, afin d'assurer l'interopérabilité du CEV et son développement sécurisé, l'Association doit en particulier :

- Procéder à la normalisation du CEV et de ses évolutions, tant au niveau national qu'international,

Après l'obtention de la norme expérimentale AFNOR, l'Association travaillera à obtenir une Norme ISO.

- Gérer la partie métier du CEV en en organisant la déclinaison par type de document,

Au sein des « Périmètres » déjà créés (Banque, Ressources Humaines, Documents comptables, Assurance, Santé) ou à créer, seront définis les couples CEV/Type de document. Au sein de ces Périmètres, les professionnels concernés définiront les données à sécuriser ainsi que la ou les formes de représentation du CEV.

Le périmètre régalien reste sous la responsabilité et la gestion de l'ANTS.

- Définir les exigences de sécurité du système,
- Niveau eIDAS des certificats,
- Profil de référencement ETSI/RGS des familles et autorités de certification,
- Profils des certificats,
- Normes utilisées pour la signature cachet électronique.
- Tenir la Trusted List et la diffuser auprès des Autorités de Certification
- Référencer les Autorités de certifications (AC) autorisées,
- Créer et maintenir les référentiels de labellisation,
- Attribuer les labels aux Editeurs de solution de génération et de vérification,
- Référencer les Emetteurs de documents revêtus d'un CEV.

De même que l'ANTS a précisément défini les entités autorisées à émettre des CEV sur leurs documents servant de justificatif de domicile, l'Association référencera, pour chaque Type de document, les entités autorisées. Exemple : listes des banques autorisées à apposer un CEV sur leurs RIB.

7.2 Les membres de l'AIGCEV

Membres Fondateurs	Représenté par
Chambre Nationale des Huissiers de Justice	Alain Bobant
Comité Français d'Organisation et de Normalisation Bancaire	Xavier Mendiboure
Conseil National des Greffiers des Tribunaux de Commerce	Thomas Denfer
Conseil Supérieur de l'Ordre des Experts Comptables	Jean Saphores
Fédération des Tiers de Confiance du Numérique	Jean-Pierre Doussot
Imprimerie Nationale	Jacques Velot
Advanced Track & Trace	Zbigniew Sagan
Alphacode	Gilles Barré
AriadNEXT	Marc Norlain
Digiposte Groupe La Poste	Olaf Klargaard
Dhimyotis	Arnauld Dubois
Lex Persona	François Devoret
Notarius	Patrick Drolet
Caisse des Dépôts et Consignations	José Morata
Bruno Couderc Conseil	Bruno Couderc
Florian Hoefle	Florian Hoefle
Yves Le Querrec	Yves Le Querrec
Membres Associés	Représenté par
Agence Nationale des Titres Sécurisés (ANTS)	Charles-Henri Menseau
Délégation Nationale à la Lutte contre la Fraude (DNLF)	Alexandre Bullier
Mission de Délivrance Sécurisée des Titres (MDST)	Julien Anthonioz-Blanc

Le Ministère de l'Intérieur, via la Mission de Délivrance Sécurisée des Titres (MDST), a demandé à passer de Membre Associé à Membre de plein exercice. Ce sera formellement fait à l'issue d'une AGE convoquée à cet effet avant la fin de l'année 2016.

Les Institutionnels ci-dessus, sont devenus Membres Fondateurs parce qu'ils trouvent un intérêt direct, ayant pour projet d'apposer un CEV sur tel ou tel document lié à leur activité, notamment :

- Sécurisation du Relevé d'Identité Bancaire, pour les Banques,
- Sécurisation de la facture fiscale, pour les Experts Comptables.

A noter que :

- pour les Experts Comptables, outre la fonction sécuritaire, le CEV leur permettra la saisie automatique et sans erreur des données comptables,
- pour l'Imprimerie Nationale, le CEV constitue une priorité ; elle est déjà l'opérateur de la vignette Crit'Air, ainsi que de la Carte Mobilité Inclusion (permettant l'accès aux places de stationnement pour handicapés).

7.3 Le bureau de l'AIGCEV

	Membres du Bureau
Président	Gilles Barré
Secrétaire Général	Yves Le Querrec
Trésorier	Marc Norlain
	François Devoret
	Jean-Pierre Doussot
	Arnauld Dubois
	Zbigniew Sagan
	Jacques Velot