



Comité Français d'Organisation
et de Normalisation Bancaires

GUIDE D'UTILISATION PAR LES BANQUES DE DOCUMENTS PORTANT UN CACHET ELECTRONIQUE VISIBLE (CEV) EMIS OU ACCEPTÉS PAR LES SERVICES DE L'ETAT

- Cas d'usage : Dossier de Connaissance Client (Entrée en relation et actualisation)**

Version 1.0
Guide élaboré par le CFONB
Date : Janvier 2025
Statut : Document validé en groupe de travail

Table des matières

1	Préambule	5
2	Introduction.....	5
2.1	Pourquoi la rédaction d'un guide destiné à la profession bancaire pour l'utilisation de documents portant un Cachet Electronique Visible ?.....	5
2.2	Le contexte : la lutte contre la fraude documentaire.....	6
2.3	Une réponse : un cachet électronique visible (CEV)	7
2.3.1	A l'origine : la création du standard « 2D-DOC » par l'ANTS	7
2.3.2	Le cadre réglementaire de l'application du « 2D-DOC », une assise juridique forte.....	7
2.3.3	Extension du champ d'application : du 2D-DOC/ANTS au CEV/AIGCEV	8
3	Principes du CEV : 4 phases – schéma de base du CEV.....	9
3.1	Phase I : Emission du document portant un CEV	9
3.2	Phase II : transmission du document portant le CEV au client.....	10
3.3	Phase III : Le client / usager présente le document portant le CEV à l'utilisateur.....	10
3.4	Phase IV : L'utilisateur procède à la lecture des données du CEV	11
4	Les évolutions du CEV depuis sa conception : vers une simplification de sa génération et vers sa diffusion à l'international.	13
4.1	Pourquoi avoir fait évoluer le CEV ?.....	13
4.2	Le nouveau format du CEV dans ses versions NF Z42-105 et ISO 22 376.....	13
5	Les perspectives de déploiement des cas d'usages du CEV.....	14
6	Documents portant CEV pour une utilisation potentielle par la profession bancaire.....	15
6.1	Identification des documents portant CEV pour une utilisation potentielle par la profession bancaire.....	15
6.1.1	Documents créés et émis par la sphère publique.....	15
6.1.2	Documents créés par le secteur marchand et utilisés dans la sphère publique.....	15
6.1.3	Limite à l'utilisation potentielle de documents CEV par la profession bancaire	15
6.2	Besoin en informations demandées pour le Dossier de connaissance client selon la 5ème Directive LAB - LAT et des pratiques bancaires les plus communes de la Communauté Bancaire Française	15
7	Documents utilisables pour le KYC par la profession bancaire.....	18
7.1	Documents CEV existants et complétude des besoins KYC	18
7.2	Remarques sur les documents candidats.....	18
7.2.1	CNIe (Carte Nationale d'Identité électronique).....	18
7.2.2	Avis fiscal.....	18
7.2.3	Justificatif de domicile.....	18
7.2.4	Cas du bulletin de paie	18
7.3	Modalités d'exploitation des données des CEV	19
8	Annexes	20
8.1	Mini glossaire	20
8.2	Eléments des normes AFNOR dites CEV : « NF Z42-101 », « NF Z42-102 », « NF Z42-103 », « NF Z42-104 » et « NF Z42-105 »	21
8.3	Eléments des normes Internationales ISO	22
8.4	Outils de lecture du CEV	22

8.5	Focus sur les fonctionnalités d'un lecteur complet : l'application <i>OtentiK Reader</i>	24
8.5.1	Présentation du lecteur <i>OtentiK Reader</i>	24
8.5.2	Lecture de codes 2D par <i>OtentiK Reader</i>	26

1 Préambule

Voici une histoire récente et authentique. Un client est contacté par son conseiller bancaire pour une mise à jour du KYC de son dossier client. Pour cela, conformément à la demande de sa banque, il a envoyé les documents par la messagerie interne de sa banque en ligne et s'est rendu au rendez-vous proposé par cet établissement. Les trois documents demandés, titre d'identité, justificatif de domicile et avis d'imposition, comportaient des Cachets Electroniques Visibles et pourtant, en conformité avec le process mis en place par cette banque, le conseiller a consacré une vingtaine de minutes, sans pouvoir échanger avec son client, pour imprimer les documents électroniques, scanner ces documents imprimés pour les transmettre au back-office bancaire, et saisir les informations nouvelles dans le dossier client informatisé. Ce temps perdu, qui pourrait être apprécié comme un irritant par certains clients, pourrait être réduit à quelques minutes en exploitant les dispositifs de fiabilisation que sont les CEV Cachets Electroniques Visibles.

Ce document a pour but de présenter aux banques tous les bénéfices en matière de gains opérationnels et de fiabilisation des données issues de l'exploitation des CEV pour transformer les échanges d'une entrée en relation d'affaire ou d'une mise à jour de KYC en une véritable valeur ajoutée pour la banque et pour son client.

2 Introduction

2.1 Pourquoi la rédaction d'un guide destiné à la profession bancaire pour l'utilisation de documents portant un Cachet Electronique Visible ?

Les retours d'expérience des secteurs d'activité en France utilisant des documents avec un code à barres à 2 dimensions dans leurs processus métiers sont positifs et avérés. Des administrations publiques et des services du secteur privé sont émetteurs ou utilisateurs de tels documents sécurisés.

Certains acteurs du secteur privé, notamment les grands facturiers, sont émetteurs de documents portant CEV utilisés par les administrations publiques. Les acteurs du secteur privé peuvent être également utilisateurs de tels documents, par exemple, le bulletin de salaire, les titres d'identité, l'avis d'imposition, le justificatif de domicile et aussi des documents très sensibles comme, pendant la dernière crise sanitaire, le certificat de vaccination ou pass-vaccinal pour accéder à des lieux privés contrôlés (cinéma, restaurant, salons ...). Ce dernier exemple, malgré le contexte pénible qui y était associé, a été un vecteur de vulgarisation des codes à barres à 2 dimensions.

Cette très forte augmentation des codes 2 dimensions, agrégés sous le vocable commun « QRCode¹ », a également fait naître un nouveau type de fraude qui peut être très dangereux lorsque le code 2 dimensions n'est pas sécurisé, c'est-à-dire lorsqu'il ne fait pas partie de la famille des CEV, Cachet Electronique Visible.

L'actualité médiatique vient confirmer les risques associés à cette diffusion accrue des codes 2D. On nomme le **Quishing**², la fraude liée à ces codes lorsque ceux-ci ne sont pas sécurisés

¹ Dans la famille des Codes à barre 2 dimensions, le plus connu est le QRcode pour *Quick Response code*, mais d'autres codes standardisés existent comme le Datamatrix, l'Aztec, le Flashcode, ...

² Le Quishing est une variante émergente du phishing, une menace pour la cybersécurité. Il implique l'utilisation de codes QR ou codes 2D malveillants créés par des attaquants pour tromper les utilisateurs et leur soutirer des données sensibles.

(contrairement au CEV) avec, par exemple, des faux avis de contravention ou la substitution, avec un simple autocollant sur les bornes de recharge électrique recouvrant le code à barre 2 dimensions de l'opérateur pour orienter l'utilisateur vers un faux site Web de paiement.

Le secteur bancaire français participe depuis le début aux travaux de Place sur ce sujet.

Les documents portant un CEV offrent un niveau de sécurité (authentification et intégrité) certifié par des organismes de l'Etat (Ministères, Administration ou Agences comme l'ANTS, Agence Nationale des Titres Sécurisés) et lequel repose sur une chaîne de confiance reconnue (Autorités de Certification, RGS Référentiel Général de Sécurité et maintenant le règlement européen eIDAS).

Les avantages attendus de l'utilisation de ces documents sont des données sécurisées et certifiées, une optimisation des process de vérification permettant une plus grande réactivité opérationnelle et une réduction de coût.

Le Bureau du Conseil du CFONB a acté ce constat et a demandé au Groupe de travail « Miroir AIGCEV » la rédaction d'un guide d'identification et d'utilisation de documents portant un code à barres 2 dimensions sécurisé de type cachet électronique visible (CEV) par la profession bancaire.

2.2 Le contexte : la lutte contre la fraude documentaire

La fraude documentaire recouvre à la fois la fraude sur le document lui-même en tant que support matériel électronique ou physique, et la fraude intellectuelle qui permet d'obtenir un document authentique de manière induue, à partir d'un justificatif falsifié fourni par le demandeur/fraudeur.

Dans le domaine du Régalien, si la sécurisation des titres d'identité tend à limiter la fraude documentaire, l'utilisation de faux documents justificatifs en vue d'obtenir des titres d'identité est toujours d'actualité.

D'après les estimations de la DGME (Direction Générale de la Modernisation de l'Etat), chaque année, en France, plus de 20 millions de documents sont utilisés comme justificatifs pour les démarches administratives (principalement des factures justifiant d'un domicile, relevés d'identité bancaire et avis d'imposition), dont plus de 15 millions de justificatifs de domicile.

Ce n'est plus seulement le document lui-même qui est attaqué mais aussi les pièces justificatives et constitutives du dossier de demande. Parmi celles-ci, le justificatif de domicile non sécurisé représente un risque avéré de fraude. Il est donc particulièrement important de sécuriser la composante « adresse » de la facture ou de l'attestation des contrats adressée au client particulier, compte-tenu de son utilisation fréquente comme justificatif de domicile.

Les falsifications des données sur l'identité et sur les avis d'imposition sont aussi des cas de fraude avérés.

Pour ces raisons, le dispositif de sécurisation de documents par codes à barres à 2 dimensions a été choisi par l'Etat comme moyen de confiance.

2.3 Une réponse : un cachet électronique visible (CEV)

2.3.1 A l'origine : la création du standard « 2D-DOC » par l'ANTS

Débuté dès 2010 ce projet du BFD (Bureau de la Fraude Documentaire) devenu MDST (Mission Délivrance Sécurisée des Titres) du Ministère de l'Intérieur est mis en œuvre d'abord dans la sphère publique avec le « 2D-DOC ».

Il vise à sécuriser des documents nativement électroniques à l'appui d'un code à barres 2 dimensions. Cette technologie s'applique notamment sur des documents présentés sous forme matérialisée ou non en tant que justificatifs (factures justifiant un domicile, avis d'imposition, etc.).

C'est un projet intersectoriel qui implique notamment les administrations, la sphère sociale, et les grands facturiers (opérateurs de fluides, les opérateurs de télécommunication).

L'ANTS¹, sous la tutelle du Ministère de l'Intérieur, assure la Maîtrise d'Ouvrage des Titres Sécurisés pour la sphère publique portant notamment sur la Carte Nationale d'Identité, les titres de résidents, les cartes mobilité inclusion, Chauffeur et Véhicules VTC, Vignette Crit'Air, etc.

La profession bancaire pourrait les exploiter notamment en tant que justificatifs présentés par des clients ou prospects dans le cadre de processus métiers *Know Your Customer* (KYC), en français le « *Dossier de Connaissance Client* ».

Ce projet, qui s'appuie sur un standard d'encodage graphique sur 2 dimensions de données structurées, a été nommé « 2D-DOC », marque déposée du Ministère de l'Intérieur. Les données sélectionnées du document y sont encodées. La sécurité est basée sur l'inclusion d'une signature numérique serveur (cachet électronique).

Ce qui permet de garantir l'intégrité et l'authentification de l'émetteur de ces données structurées.

2.3.2 Le cadre réglementaire de l'application du « 2D-DOC », une assise juridique forte

Le cadre de référence juridique est le **décret no 2013-629 du 16 juillet 2013 modifiant le décret no 2000-1277 du 26 décembre 2000**, qui porte simplification de formalités administratives et suppression de la fiche d'état civil NOR : RDFJ1242016D.

Cette réglementation s'adresse à un public précis : les usagers qui fournissent des pièces justificatives, les agents publics qui les reçoivent, les émetteurs de documents justificatifs de domicile. Aussi elle vise à sécuriser les pièces justificatives de domicile requises pour la délivrance d'un titre d'identité, de voyage, de séjour, d'un certificat d'immatriculation d'un véhicule, de la délivrance d'une attestation d'accueil ou d'une inscription volontaire sur les listes électorales à partir d'un dispositif technique garantissant leur authenticité.

Dans la foulée du décret paru en juillet 2013, l'**arrêté du 27 septembre 2013** est venu préciser les conditions de 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, en l'occurrence le cachet électronique visible.

Ainsi depuis 2013 les services de l'Etat notamment les mairies et les préfectures sont tenues d'accepter des documents portant un code « 2D-DOC » comme pièces justificatives à l'appui d'une demande d'un titre sécurisé.

¹ ANTS : Depuis Janvier 2024 est dénommée France TITRE, JO 2024-146

2.3.3 Extension du champ d'application : du 2D-DOC/ANTS au CEV/AIGCEV

En 2015, le ministère de l'Intérieur décide de centrer ses responsabilités sur son périmètre régalien d'émetteur de documents et de définition des documents pour son usage, notamment les documents permettant de justifier un domicile, les titres d'identité, les cartes et permis pour les citoyens et les professionnels.

Il demande à la Fédération des Tiers de Confiance du Numérique (FnTC) de reprendre en plus de la labellisation des fournisseurs de solutions (générateurs et lecteurs) qu'il assure pour l'ANTS, la responsabilité d'organiser la gestion des autres cas usages de 2D-DOC pour la sphère privée.

En octobre 2016, pour les secteurs autres que le régalien, la gestion globale du 2D-DOC devenu le CEV (Cachet Electronique Visible) est confiée à une nouvelle association professionnelle issue de la FnTC, l'AIGCEV, dont sont, entre autres membres fondateurs, le ministère de l'Intérieur, l'ANTS, la DNLF, la CdC, le groupe La Poste, le CSOEC, la CNCJ et **le CFONB**.

3 Principes du CEV : 4 phases – schéma de base du CEV

3.1 Phase I : Emission du document portant un CEV

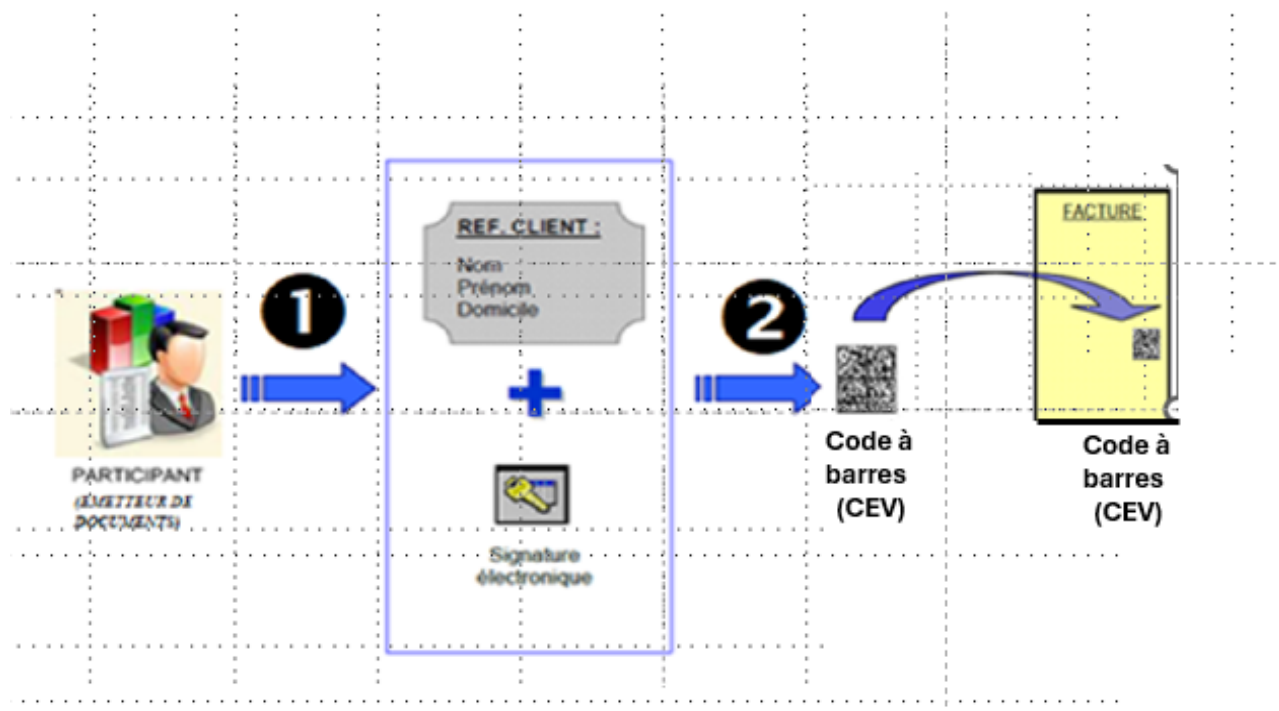
Le créateur du document (*le Participant*) émet un document contenant un CEV.

Le CEV contient les données principales du document.

Le CEV est signé par l'émetteur du document (*le Participant*).

Schéma simplifié de création et d'émission d'un document portant un CEV

(exemple d'un document « Facture » ou « attestation de contrat » émis par un facturier qui va servir de justificatif de domicile)



❶ Le Participant (émetteur de documents) sélectionne les données à sécuriser (Identité et Adresse pour le justificatif de domicile) qui apparaissent sur ses factures ou sur ses attestations de contrat, et les signe électroniquement ;

② L'ensemble est mis en forme dans un CEV, dans cet exemple un CEV identifié 2D-DOC, marque déposée de l'ANTS, et apposé sur le document facture ou l'attestation de contrat. Il est à noter que, dans cet exemple de justificatif de domicile sur une facture, les seules données sécurisées n'ont rien à voir avec les données propres à la facturation, ce sont des données d'identification du client (Nom, Prénom et Adresse) qui intéressent le cas d'usage. La facture n'est que le support (papier ou électronique soit PDF) qui va véhiculer les données d'adresse et d'informations authentifiées du destinataire de la facture. C'est pourquoi, on peut trouver des CEV contenant ces mêmes données d'identification servant de justificatif de domicile sur d'autres documents comme une attestation de contrat. C'est la pertinence et la confiance dans les données signées reprises dans le CEV qui comptent pour la confiance globale dans le cas d'usage. En reprenant la facture, et pour le cas d'usage du justificatif de domicile, il faut que la facture soit émise par un opérateur de confiance capable de garantir l'adresse identifiée et la relation entre l'adresse et les informations d'identité. C'est pourquoi on retrouvera ces éléments sur des documents reconnus comme des justificatifs de domicile par l'état et dument listés dans un décret ou un arrêté. Ici par exemple, pour l'enregistrement du permis de conduire.

Arrêté du 23 décembre 2016 relatif à la justification de l'identité, du domicile, de la résidence normale et de la régularité du séjour pour l'obtention du permis de conduire

Article 4

La justification du domicile s'établit selon les modalités suivantes :

I. - Pour les personnes disposant d'une adresse personnelle, au moyen de l'un des justificatifs suivants :

1° Un avis d'imposition ou de non-imposition.

2° Une quittance de loyer non manuscrite.

3° Une facture de moins de six mois de téléphone fixe ou mobile, de gaz, d'électricité ou d'eau.

3.2 Phase II : transmission du document portant le CEV au client

Le document avec CEV est transmis au client/usager (propriétaire ou destinataire du document et/ou des informations du document).

3.3 Phase III : Le client / usager présente le document portant le CEV à l'utilisateur

Le client/usager remet le document portant le CEV à un service utilisateur pour l'exploitation par ce dernier des informations validées y figurant. Dans le cas présent, le service utilisateur est un établissement bancaire teneur de compte, un ASPSP (*Account Servicing Payment Service Provider*).

3.4 Phase IV : L'utilisateur procède à la lecture des données du CEV

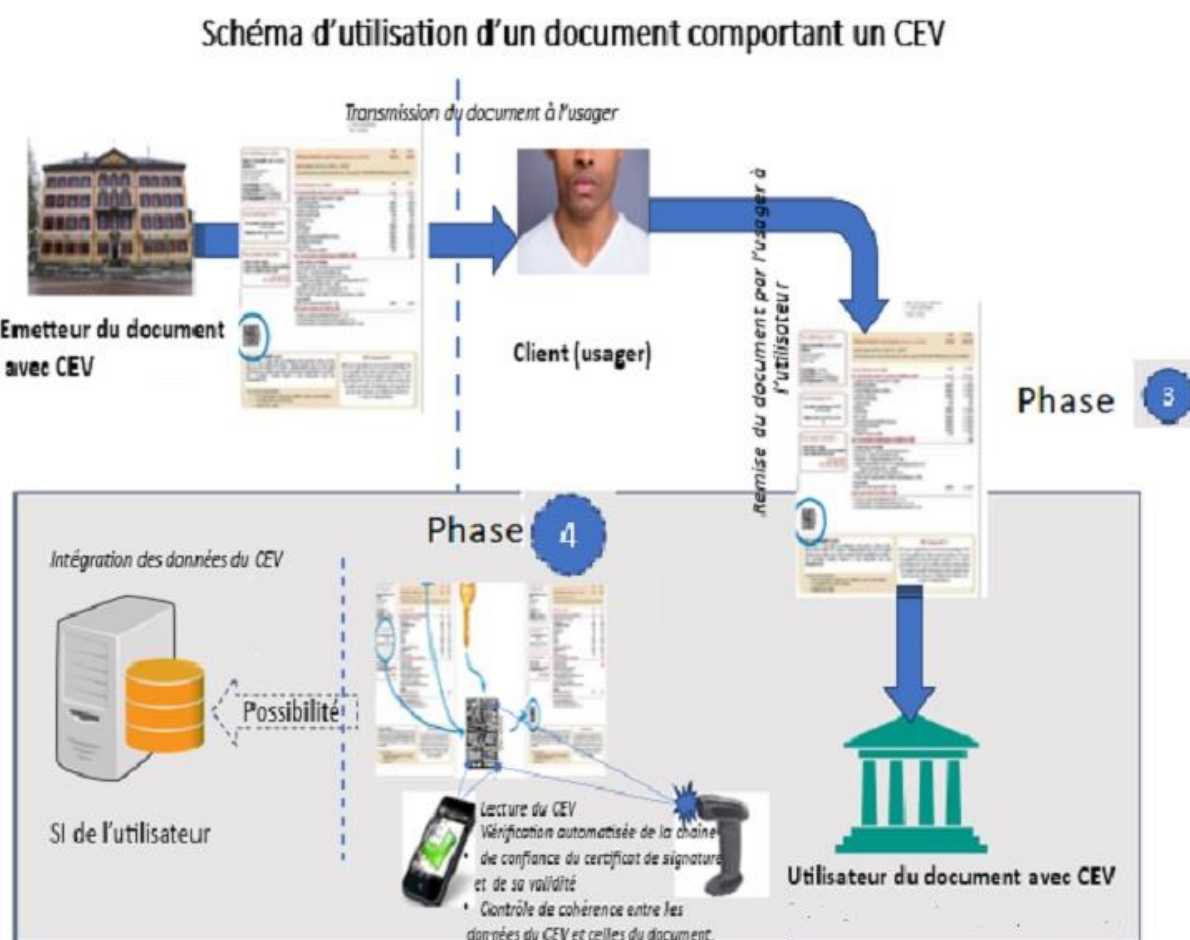
Le service utilisateur est l'exploitant du document portant le CEV.

Il procède à la lecture du document, vérifie la validité de l'intégrité des données figurant sur le CEV. Il vérifie également la validité de la chaîne de confiance du certificat de l'émetteur du document.

Ces vérifications sont effectuées automatiquement lors de la lecture du CEV.

Le service utilisateur peut éventuellement intégrer les données du CEV. Pour rappel, il ne doit exploiter que les données utiles à son traitement dans son système d'information, en respectant le principe de la minimisation des données¹ défini par l'article 5.1.c du RGPD.

Le schéma ci-après résume les étapes de l'exploitation par le service utilisateur du document reçu.



¹ <https://www.cnil.fr/fr/definition/minimisation>

Le service Utilisateur (l'« exploitant » du document, ex. préfecture, etc.) scanne le CEV et effectue par ce moyen les vérifications et contrôles nécessaires.

Pour ce faire, il utilise un outil de lecture de codes à barres 2D compatibles avec les formats du CEV (Normes AFNOR NF Z42-101, AFNOR NF Z42-105 ou ISO 22 376).

La vérification se déroule en 2 temps :

1-Détails du processus automatisé de vérification

- *L'identifiant de l'Autorité de Certification (A.C.), choisie par le Participant pour sa signature électronique, est extrait du Code à Barres (CEV) ;*
- *L'identifiant permet d'obtenir l'adresse électronique de l'A.C. émettrice, dans l'annuaire des Autorités de Certifications (A.C.) publié ;*
- *Le certificat et la clé publique du Participant sont récupérés sur le site de l'A.C. émettrice ;*
- *La validité du certificat et la signature du Participant sont vérifiées ;*
- *Les informations sécurisées sont validées.*

2-Détail du processus manuel de vérification

- *L'Utilisateur s'assure de la concordance des données certifiées par le CEV avec les données effectivement présentes sur le document fourni.*

L'Utilisateur peut éventuellement procéder à l'intégration de données vérifiées et validées dans son système d'information (par ERP, API, ...), ce qui peut nécessiter un niveau d'interface d'intégration à développer.

4 Les évolutions du CEV depuis sa conception : vers une simplification de sa génération et vers sa diffusion à l'international.

4.1 Pourquoi avoir fait évoluer le CEV ?

Dans sa version initiale, le CEV avait été conçu pour les besoins exclusifs de l'état pour sécuriser les données d'un petit nombre de documents. Cela impliquait un nombre réduit d'acteurs dans le système et un contrôle facile du système par les autorités qui contrôlaient tous les cas d'usages, les signataires des CEV et les Autorités de Certification émettrices des Cachets Serveurs.

Le cycle de création et de vie des CEV était également associé à la mise à jour des applications de lecture qui devaient évoluer à chaque nouvelle création de CEV. Dans la pratique cela se concrétisait par la création de 2 à 3 nouveaux cas d'usage par an, avec la nécessité de produire une nouvelle version des spécifications à chaque création (avec près de 50 versions à ce jour) et corrélativement avec un retard considérable dans la mise à jour des applications de lecture dont les fournisseurs attendaient le lancement de plusieurs CEV avant de mettre à jour leur application de lecture.

L'ambition, en déléguant la gestion du secteur privé national et la diffusion du CEV à l'international à l'association AIGCEV, était de trouver une évolution permettant l'agilité dans la création et la lecture des CEV et une gouvernance permettant la diffusion du CEV avec un niveau de sécurité du plus haut niveau, en conformité avec le règlement eIDAS.

L'ensemble de ces propositions ont été portées à la normalisation française, à l'AFNOR, pour la première version avec les normes NF Z42-101, NF Z42-102, NF Z42-103 et NF Z42-105, et pour les évolutions avec la norme française Z42-105 et au niveau international, à l'ISO avec la norme de format ISO 22 376 et la norme de gouvernance ISO 22 385.

4.2 Le nouveau format du CEV dans ses versions NF Z42-105 et ISO 22 376

Les grandes évolutions par rapport à la version initiale NF Z42-101 :

- La définition des données relatives au cas d'usage ne fait plus partie de la spécification technique, mais elle est décrite dans un fichier « intelligent » encodé en XML et signé par l'opérateur en responsabilité de l'émission de ce cas d'usage (en France le Ministère de l'Intérieur via l'ANTS ou l'AIGCEV, à l'étranger via des opérateurs gouvernementaux ou privés répondants aux critères définis par la norme ISO 22 385). Il est à noter que ce fichier descripteur, appelé « *Manifest* » dans la norme ISO 22 376 peut contenir une partie « présentation » permettant d'aller jusqu'à la restitution du graphisme de la version « papier » ou « électronique » du document.
- La mise à jour de l'application de lecture est devenue automatique lorsqu'un nouveau CEV est émis, ce qui est équivalent à une mise à jour en temps réel de la lecture.
- Le CEV est implémentable et peut utiliser toutes les langues. Par exemple pour l'outil de lecture *OtentiK Reader* décrit en annexe, actuellement 25 langues, dont l'arabe, le grec ou le cyrillique sont disponibles.

5 Les perspectives de déploiement des cas d'usages du CEV

Actuellement le CEV ISO est en cours d'intégration dans le portefeuille d'identité numérique compatible eIDAS développé par *France Identité Numérique* et qui sera interopérable avec tous les portefeuilles européens eIDAS à partir de fin 2026.

De nouveaux documents émis par l'ANTS intégreront également ce CEV ISO comme le permis de conduire, les certificats d'immatriculation ou la prochaine évolution de la Carte Nationale d'Identité électronique.

Le projet européen de DPP, « *Digital Product Passport* », passeport numérique produit, intégrera une restitution par CEV ISO et sera obligatoire dès 2026 pour les batteries et les vêtements. Il sera étendu par la suite à tous les produits, sauf les secteurs de l'alimentaire et de la pharmacie.

6 Documents portant CEV pour une utilisation potentielle par la profession bancaire

6.1 Identification des documents portant CEV pour une utilisation potentielle par la profession bancaire

Dans ce paragraphe, est établi un inventaire (exhaustif à fin 2024) des documents portant CEVs lorsque ceux-ci peuvent potentiellement participer à une utilisation par la profession bancaire. Il s'agit d'une part de documents produits par le régalien, et d'autre part de documents créés dans le secteur marchand et certifiés par l'autorité publique.

6.1.1 Documents créés et émis par la sphère publique

Il s'agit par exemple des Cartes d'identité numérique (CNle) et des justificatifs d'identité produits par France Identité Numérique (FIN). Ces documents permettent de sécuriser via le CEV les informations d'identité suivantes : *Nom de famille, Prénom(s), Sexe, Nationalité, Pays de naissance, Type de document et, Numéro du titre.*

Sont également disponibles dans cette catégorie des documents fiscaux, comme les avis d'imposition.

6.1.2 Documents créés par le secteur marchand et utilisés dans la sphère publique

A côté des documents portant CEV créés par le Régalien, les services de l'Etat sont par ailleurs utilisateurs de documents CEV émis par des acteurs du secteur marchand. Il s'agit des documents servant de justificatifs de domicile. En effet, le CEV est présent de manière systématique sur toute une série de documents servant de justificatifs de domicile qui présentent des informations comme le nom/prénom, ainsi que les 6 lignes de l'adresse de la norme AFNOR NF Z10.11 (dont le contenu est homogène entre facturiers).

6.1.3 Limite à l'utilisation potentielle de documents CEV par la profession bancaire

Si les documents CEV précités sont des candidats à l'utilisation par les banques, d'autres documents, produits pour des autorités publiques et/ou des entités privées semblent plus difficilement exploitables à court terme.

Certains documents notamment les fiches et bulletins de paie n'ont pas pu être retenus comme candidats en raison de leur hétérogénéité par rapport aux informations figurant dans leur CEV.

6.2 Besoin en informations demandées pour le Dossier de connaissance client selon la 5ème Directive LAB - LAT et des pratiques bancaires les plus communes de la Communauté Bancaire Française

Dans le tableau ci-dessous sont présentées les informations demandées pour le KYC selon la 5ème Directive LAB-LAT.

Nous avons recherché parmi les documents portant un CEV lequel pouvait répondre au mieux au besoin. Puis, nous avons procédé au « scoring » du taux de couverture du besoin KYC par le document.

Légende : ☒ Donnée présente
☐ Donnée absente

Catégorie de données KYC 5 ^{ème} Directive LAB-LAT et principales pratiques bancaires françaises		Document portant un CEV créé ou utilisé par les services de l'Etat --- <i>Candidats potentiels à l'utilisation par la profession bancaire</i>	Existence donnée en CEV pour le KYC	Taux couverture du document CEV/ Données KYC	Observations
	Données personnelles				
KYC DE BASE	Identité	CNIe (Données du CEV)		5/7 soit 71%	
	Nom (nom d'usage et nom de famille de naissance)	<i>Nom de famille</i>	☒		
	Prénom(s)	<i>Prénom(s)</i>	☒		
		<i>Sexe</i>	☒		
		<i>Nationalité</i>	☒		
	Date de naissance		☐		<i>Information nécessaire manquante au CEV</i>
	Commune de naissance		☐		<i>Information nécessaire manquante au CEV</i>
	Pays de naissance	<i>Pays de naissance</i>	☒		
	Type de document d'identité	<i>Type de document</i>	☒		
	Numéros du titre (CNI, passeport, carte de séjour, permis de conduire)	<i>Numéro du titre</i>	☒		
	Situation familiale				
	Statut matrimonial		☐		<i>Information manquante</i>
	Régime matrimonial		☐		<i>Information manquante</i>
	Nombre des enfants à charge (âges ou dates de naissance des enfants à charge)		☐		<i>Information manquante</i>
		Justificatif d'identité à usage unique		4/7 soit 57%	Document créé par l'application du programme France identité Numérique (FIN) en test dans 3 départements (à fin 2024). Prérequis : posséder la nouvelle CNIe
	Nom (nom d'usage et nom de famille de naissance)	<i>Nom</i>	☒		
	Prénom(s)	<i>Prénom(s)</i>	☒		
		<i>Sexe</i>	☒		
		<i>Nationalité</i>	☐		
	Date de naissance	<i>Date de naissance</i>	☒		
	Commune de naissance	<i>Lieu de naissance</i>	☒		
	Pays de naissance		☐		

• Type de document d'identité				Prérequis est de posséder la nouvelle CNiE
• Numéros du titre (CNI, passeport, carte de séjour, permis de conduire)				Prérequis est de posséder la nouvelle CNiE
Situation professionnelle	Fiches/Bulletin de paie secteur privé			Les informations à vérifier par rapport au CEV du bulletin de paie ne sont pas normalisées
• Statut de l'emploi				
• Domaine d'activité				
• Nom et coordonnées de l'employeur				
• Ou Pour les clients entrepreneurs individuels, le SIRET, la raison sociale...				
Situation financière et patrimoniale				
Justificatif de revenus	Avis d'imposition		2/4 soit 50%	
• Revenus (revenus du travail et autres revenus, pensions, allocations)	• <i>Revenu fiscal de référence</i>	☒		
• Charges (montant des impôts, tranche d'imposition, indicateur ISF, endettement et les charges notamment loyers, autres crédits)	• <i>Nombre de parts</i>	☒		Informations obtenues par calcul et déduction du Revenu fiscal et du nombre de parts
• Résidence fiscale				La lecture du CEV indique que la personne est résidente française
• Patrimoine (mode hébergement, patrimoine immobilier et financier déclaré ...)		☐		
	• <i>Année de référence</i>			
	• <i>Coordonnées du déclarant</i>			
	• <i>Numéro fiscal</i>			
	• <i>Date de mise en recouvrement</i>			
Domicile & Moyens de contact				
Justificatif de domicile	Factures		2/2 soit 100%	Il s'agit de factures émises par les grands facturiers (fournisseur d'eau, gaz, électricité, télécoms, ...)
	• <i>Nom, Prénom(s)</i>			
• Adresse postale	• <i>Les 6 lignes adresse de la norme AFNOR NF Z10.11</i>	☒		
• Pays de résidence		☒		
Moyens de contact			0/2 soit 0%	
• e-mail				
• Téléphone fixe et/ou mobile				

7 Documents utilisables pour le KYC par la profession bancaire

7.1 Documents CEV existants et complétude des besoins KYC

Le tableau ci-dessus montre l'importance de la couverture en informations KYC présentes sur les documents portant CEV.

Les banques pourraient exploiter dans le cadre du KYC d'entrée en relation ou de mise à jour, les documents suivants : **la CNle, l'attestation d'identité, l'avis fiscal, les factures des grands facturiers.**

Pour autant, ces documents avec des données certifiées, ne sont pas suffisants pour renseigner avec complétude les besoins en KYC d'entrée en relation. Notamment les informations de contact et celles de nature financière et patrimoniale ne sont pas ou peu couvertes à ce jour par les documents actuels portant CEV.

Les données complémentaires manquantes sont à collecter par ailleurs, souvent auto-attestées par le déclarant, ou par croisement avec d'autres documents.

Dans ce dernier cas, le fait que les données issues de la lecture d'un CEV sont fiabilisées, pourrait orienter la cohérence avec des données complémentaires (non CEV) par exemple et pour illustration avec une analyse IA.

7.2 Remarques sur les documents candidats

7.2.1 CNle (Carte Nationale d'Identité électronique)

La CNle permet de couvrir pour une large part les besoins en certification d'identité. En proposant de la coupler avec le justificatif d'identité issu de l'application France Identité, cela permettrait de couvrir en totalité le besoin d'information certifiée d'identité pour le KYC.

7.2.2 Avis fiscal

L'avis fiscal ne couvre que très partiellement les besoins en certification de la situation financière et patrimoniale. Cependant, les éléments manquants peuvent être récupérés par ailleurs.

7.2.3 Justificatif de domicile

Les informations de justificatifs de domicile nécessaires au KYC, c'est à dire les données comme le nom/prénom, ainsi que l'adresse, nous sont fournies par les factures portant CEV avec notamment les 6 lignes de l'adresse de la norme AFNOR NF Z10.11 (contenus homogènes entre facturiers).

7.2.4 Cas du bulletin de paie

Bien que potentiellement pourvus de CEV, certains documents, produits pour des autorités publiques et/ou des entités privées semblent plus difficilement exploitables à court terme, en raison de leur hétérogénéité : c'est notamment le cas des bulletins de paie. Toutefois, il n'est pas à exclure que ces documents arrivent à maturité technique et opérationnelle, nous permettant ainsi de pouvoir les intégrer dans le périmètre des documents couverts.

7.3 Modalités d'exploitation des données des CEV

Pour les documents comportant un Cachet Électronique Visible, les données contenues dans le CEV sont scellées par une signature électronique apposée par l'organisme officiel qui détient ces données. Ce qui garantit l'authenticité et l'intégrité de ces informations.

Le CEV peut être lu par de nombreux outils de lecture, en vérifiant la validité de la signature. Toutefois seuls certains lecteurs restituent la chaîne de confiance de la signature complète.

Pour cela, il convient d'utiliser une application capable de :

- Contrôler le certificat et l'autorité de certification du CEV ;
- Reconstruire la signature électronique en utilisant la clé publique associée aux documents d'identité français (dérivée du "CSCA France") et le certificat de signature du titre.

Les banques en tant qu'organismes habilités peuvent donc scanner le code afin de lire les données contenues dans le CEV et ainsi s'assurer de l'intégrité du document.

Au-delà de la seule lecture du CEV, l'exportation des données directement dans une application de la Banque permettrait une véritable exploitation efficiente dans le cadre du KYC mené par les établissements bancaires.

Parmi les avantages attendus de l'utilisation des documents CEV, autres que les données sécurisées et certifiées, il y a une optimisation des process de vérification permettant une plus grande réactivité opérationnelle et une réduction de coût. Il est également imaginable une contribution au processus de l'enrôlement client, par la participation à l'automatisation de celui-ci.

En annexe ont été décrits plusieurs dispositifs de lecture et un tableau comparatif des différents lecteurs est disponible.

On trouvera également dans ce document l'application de lecture « *OtentiK Reader* », qui est disponible sur smartphone Apple ou Androïd et aussi en version *SDK* pour être implémentée sur des lecteurs de code à barre connectés sur PC ou tablette.

De plus, une fonction intégrée permet de lire dans l'application un code reçu en PDF directement dans l'application sans impression intermédiaire.

Le CFONB comme membre fondateur participe aux travaux de l'AIGCEV. Le lecteur universel « *OtentiK Reader* » est propriété de l'AIGCEV.

Cette application permet également de lire tous les formats de CEV (AFNOR Z42-101, Z42-105) et ISO, mais permet également de lire tous les formats d'encodage 2D (QR Code, Datamatrix, ...) en indiquant si le Code est sécurisé ou non afin de prévenir les tentatives de *Quishing*. Cette version affiche également le chemin de certification et les informations de validité du certificat de signature.

8 Annexes

8.1 Mini glossaire

- **A.C ou Autorité de Certification** : autorité de certification, référencée par l'ANTS, qui émet des certificats selon les standards adoptés par l'ANTS et gère un annuaire des certificats émis. Ce rôle peut être assuré par le Participant ou un prestataire de service.
- **Annuaire de Certification** : liste des certificats émis par l'Autorité de Certification. A l'aide d'une TSL (Trust-Service Status List) publiée sur le site de l'ANTS, l'Utilisateur vérifie que l'identifiant de l'A.C existe et récupère le certificat de l'A.C. ainsi que l'adresse où l'annuaire est publié.
- **ANTS** : Agence Nationale des Titres Sécurisés, représentée par son Directeur ou un de ses membres qu'il désigne pour agir en son nom. Depuis Janvier 2024 est dénommée France TITRE, JO 2024-146. Cette agence fixe les normes techniques 2D-DOC, valide les applications, assure les référencements et exerce un contrôle continu sur le respect des prescriptions techniques. Le site internet de l'ANTS est à l'adresse suivante : www.ants.interieur.gouv.fr.
- **Code à Barres 2D-DOC** : code à barres en deux dimensions, constitué de modules noirs disposés dans un carré à fond blanc. Destiné à être lu par un lecteur de code-barres, il permet de sécuriser des données signées électroniquement ; le certificat n'est pas inclus dans le Code à Barres 2D-DOC.
- **CRL ou liste de révocation des certificats** : éditée par l'Autorité de Certification, cette liste de certificats révoqués est accessible à une adresse précisée dans le certificat.
- **DPDA** : le Département des Projets et du Développement des Applications, représenté par son chef ou un de ses membres, est chargé de la partie administrative et de la coordination du dispositif, de la mise en place des modalités de travail avec les acteurs de la lutte contre la fraude et des relations avec les Participants.
- **Document sécurisé** : document émis par un Participant comportant un Code à Barres bidimensionnel conforme aux spécifications publiées sur le site internet de l'ANTS.
- **Editeur de Code à Barres 2D-DOC** : prestataire agissant au profit d'un Participant, mettant sous la forme d'un Code à Barres bidimensionnel, conforme aux spécifications techniques, les informations sélectionnées sur le document émis et la signature. Ce rôle peut être assuré par le Participant.
- **MDST** : la Mission de Délivrance Sécurisée des Titres, du Ministère de l'Intérieur, est représentée par le Département des Projets et du Développement des Applications
- **Partenaires** : ensemble des parties impliquées dans le dispositif de gouvernance : A.C., ANTS, DPDA, éditeurs de code à barres 2D-DOC, MDST, participants.
- **Participant** : émetteur de Code à Barres 2D-DOC se conformant aux procédures prévues par le fonds documentaire. La participation est matérialisée par l'apposition d'un Code à Barres 2D- DOC sur les documents remis ou transmis aux Usagers.
- **Référencement** : Le référencement est le fait d'enregistrer les Autorités de Certification et les Editeurs de Code à Barres dans les annuaires de l'ANTS, après validation de leurs

solutions sur la base des règles de sécurité et d'interopérabilité édictées dans le Processus et les Spécifications Techniques.

- **RGS** : Le Référentiel Général de Sécurité définit un ensemble de règles de sécurité qui s'imposent aux autorités administratives dans la sécurisation de leurs systèmes d'information. Il propose également des bonnes pratiques en matière de sécurité des systèmes d'information que les autorités administratives sont libres d'appliquer.
- **Usager** : toute personne physique ou morale présentant un document contenant un Code à Barres 2D-DOC.
- **Utilisateur** : toute personne physique ou morale vérifiant l'authenticité des données contenues dans un Code à Barres 2D-DOC.

8.2 Eléments des normes AFNOR dites CEV : « NF Z42-101 », « NF Z42-102 », « NF Z42-103 », « NF Z42-104 » et « NF Z42-105 »

La création et la publication des corpus normatifs AFNOR auprès de l'AFNOR, Normalisation Française, comportent deux ensembles. Le premier, constitué des normes NF Z42-101 à 104, est directement issu des travaux en commun effectués avec l'ANTS et correspond au format et annexes du CEV initial :

1. La norme NF Z42-101 décrit le format général du CEV avec l'encodage des parties entête, données, signature et annexe.
2. La norme NF Z42-102 décrit le dictionnaire des données, c'est-à-dire l'ensemble de la définition et de l'encodage des données disponibles à la date de création de la norme.
3. La norme NF Z42-103 décrit le cas d'usage du CEV dans la création d'un justificatif de domicile.
4. La norme NF Z42-104 fournit un ensemble de spécifications concernant les mesures techniques à mettre en œuvre pour apposer un cachet électronique visible (CEV) sur les documents dans leur forme numérique et leur forme matérielle (après impression).

On peut voir les limites de ces propositions avec le document NF Z42-102 qui doit évoluer à chaque création d'une nouvelle donnée et, à l'instar du document NF Z42-103, un nouveau document à produire pour chaque cas d'usage.

C'est ce bilan, peu avantageux avec l'ambition d'une diffusion en masse de cas d'usage de CEV, qui a conduit le Groupe d'Experts de Normalisation AFNOR à imaginer une évolution de la norme NF Z42-101 pouvant effacer les freins d'une diffusion massive du CEV.

La norme NF Z42-105 est la nouvelle version du format du CEV qui apporte la notion de description dynamique du CEV encapsulée dans un fichier XML (appelé « *Manifest* »), et signé électroniquement par l'opérateur du réseau CEV.

Cette nouvelle notion apporte au CEV le bénéfice d'une mise à jour en temps réel de l'application de lecture et la stabilité du document de format (cf. NF Z42-101), la suppression du document normatif de dictionnaire (cf. NF Z42-102) ainsi que tous les documents normatifs des cas d'usage (cf. NF Z42-103 pour un seul cas d'usage).

La réalisation du réseau de confiance devra se doter d'un document de gouvernance afin de définir les engagements de l'opérateur de confiance pour assurer la sécurité de l'organisation. Ce dernier document ne fait pas partie du corpus documentaire initial AFNOR et a été créé dans la cadre de la version ISO internationale sous la référence ISO 22 385.

8.3 Eléments des normes Internationales ISO

Norme de format ISO 22 376 :

C'est la version portée à la normalisation internationale de la norme française NF Z42-105. Elle décrit le format d'encodage du CEV et du descripteur XML « *Manifest* » et s'accompagne de son organisation de confiance selon la norme ISO 22 385.

Norme de gouvernance ISO 22 385 :

C'est la norme indiquant les exigences relatives à la sécurité et l'interopérabilité d'un réseau d'opérateurs de confiance pour gérer, entre autres, les CEV de format ISO 22 376.

Cette norme de management, imaginée pour le CEV et les réseaux d'opérateurs de confiance du CEV, est de portée plus large et peut concerner d'autres domaines d'application que le CEV.

En résumé, la norme ISO 22 376 vient occuper le domaine de compétence de toutes les normes AFNOR « NF Z42-10n », et la norme ISO 22 385 garantit la sécurité et l'interopérabilité d'un réseau d'opérateurs de confiance de CEV, fédération d'opérateurs de confiances nationaux (pour la partie régalienne gouvernementale), sectoriels nationaux ou internationaux.

8.4 Outils de lecture du CEV

Il existe sur le marché plusieurs lecteurs de CEV. La plupart sont dédiés à un certain type de CEV et sont accessibles uniquement pour une utilisation sur smartphone ou tablette, iOS Apple ou Android Google.

Deux lecteurs sont disponibles pour une intégration sur des terminaux spécialisés (stations de Travail ou Tablette) équipées d'un lecteur de type « douchette ». Dans ce cas, l'usage n'est pas gratuit.

Le tableau disponible page suivante résume les principales caractéristiques des différents lecteurs de CEV disponibles.

Tableau comparatif des caractéristiques des lecteurs de CEV sur smartphone

Application	Editeur	Lecture Z42-101	Lecture Z42-105	Lecture ISO 22 376	Lecture CEV téléchargé	Chemin de Certification	Fac-similé	Mode OFF LINE	Export des données	API SDK	Android Apple	Gratuit	Langues	Lecture autres codes
VDS Verify	Stelau	OUI	OUI mais sans interopérabilité	NON	NON	OUI	NON	NON	NON	NON	OUI	OUI	1 (FR)	NON
VDSeal Reader	Lex Persona	OUI	NON	NON	NON	NON	NON	NON	NON	NON	OUI	OUI	1 (FR)	NON
Smart Verify ¹	IN Group	OUI	NON	NON	NON	NON	NON	OUI	NON	OUI	OUI	OUI	1 (FR)	OUI ²
BioSeal ³	Id3 Technologies	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	NON	6 dont FR	OUI
2D-Origin	Certigna TESSI	OUI	NON	NON	NON	NON	NON	NON	NON	NON	OUI	OUI	1 (FR)	NON
2D-Doc Reader	AriadNext IdNow	OUI	NON	NON	NON	NON	NON	NON	NON	NON	OUI	OUI	1 (FR)	NON
France Identité Numérique	ANTS	NON	OUI mais sans interopérabilité	NON	NON	NON	NON	OUI	NON	NON	OUI	OUI	1 (FR)	NON
OtentiK Reader ⁴	AIGCEV	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	25 dont FR ⁵	OUI ⁶

¹ Caractéristique de la partie publique du vérificateur, SmartVerify existe aussi en mode connecté pour les usages des professions réglementées, les Forces de l’Ordre en particulier.

² Seulement quelques QR Codes spécialisés non signés (autres que des CEV) comme la carte Famille Nombreuse ou certaines étiquettes d’identification des vélos FNUCI (Fichier National Unique des Cycles Identifiés).

³ Lecture codes HAN XIN, AZTEC, Intégration des gabarits de biométrie empreintes digitales et visage, Lecture codes conforme 15 459 (préfixe obligatoire enregistré à l’AIM, <https://www.aimglobal.org/registration-authority-iso-iec-15459/>)

⁴ Également disponible en marque blanche pour être spécialisé ou personnalisé comme, par exemple, la version pour les services de l’Identité de la Côte d’Ivoire, l’ONECI avec la version ‘VERIF by ONECI’ téléchargeable également sur les stores Android et iOS.

⁵ Arabe, Russe, Tchèque, Danois, Allemand, Grec, Anglais, Espagnol, Estonien, Finois, Français, Croate, Hongrois, Italien, Coréen, Lituanien, Letton, Malte, Hollandais (Flamand), Polonais, Portugais, Roumain, Slovène, Slovaque, Suédois.

⁶ Lecture des URL en QR Code pour prévenir du *Quishing*.

8.5 Focus sur les fonctionnalités d'un lecteur complet : l'application *OtentiK Reader*

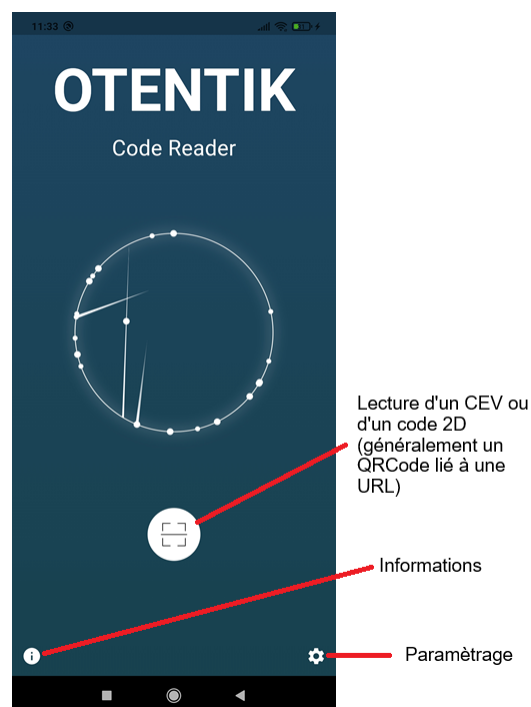
Le lecteur présenté est l'application *OtentiK Reader* développé par l'AIGCEV, Association Internationale de Gouvernance du Cachet Electronique Visible, et mis à disposition gratuitement pour le grand public sur les stores Android Google Play et Apple iOS.

Des versions sont personnalisables pour les usages professionnels et également disponibles en SDK pour être intégrées dans les applications métier, ayant aussi une possibilité d'exporter les données issues de la lecture.

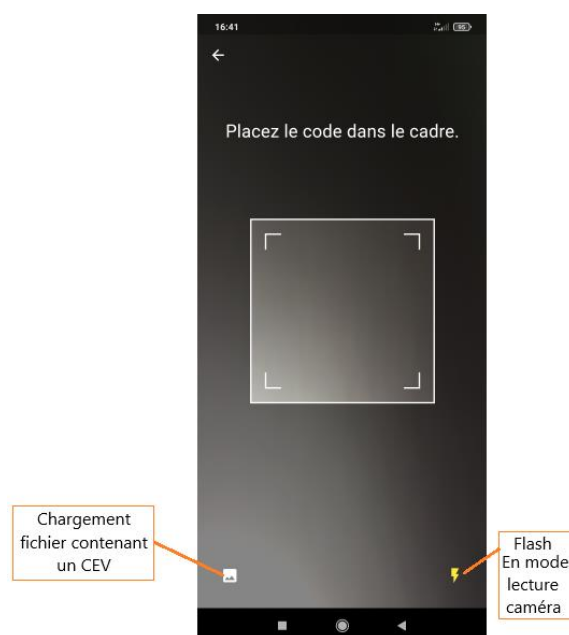
Les informations et copies d'écran qui suivent sont extraites de documents issus de travaux de l'AIGCEV.

8.5.1 Présentation du lecteur *OtentiK Reader*

Ecran d'accueil



Trois fonctions, lecture d'un code 2D, Informations (A propos) sur l'application et paramétrage de l'application



Ecran d'informations sur le logiciel



Information sur le concept du CEV et du réseau de confiance associé. Lien vers le site web pour plus d'information.

Version du logiciel

Lien vers les mentions légale

Lien vers la politique de confidentialité

Editeur de l'application

Liste des logiciels tiers utilisés

Ecran de paramétrage



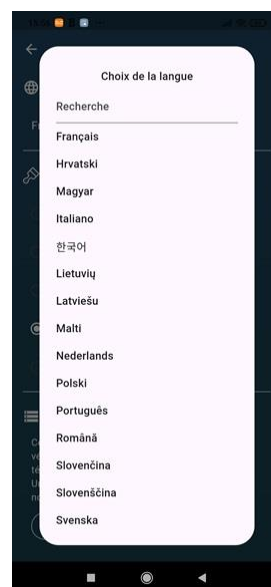
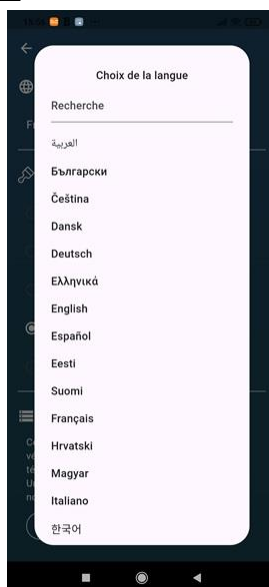
Choix de la langue de restitution parmi 25 langues configurables :

Choix du thème parmi 5 thèmes enregistrés

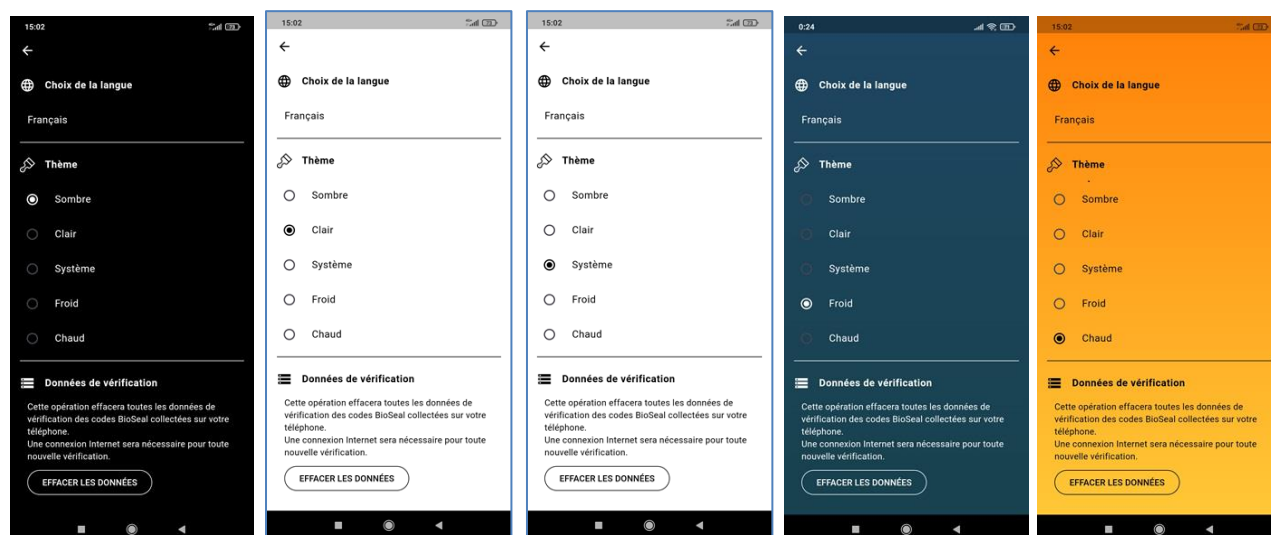
Bouton d'effacement du cache

Choix de la langue

Parmi les 25 langues : Arabe, Russe, Tchèque, Danois, Allemand, Grec, Anglais, Espagnol, Estonien, Finois, Français, Croate, Hongrois, Italien, Coréen, Lituanien, Letton, Malte, Hollandais (Flamand), Polonais, Portugais, Roumain, Slovène, Slovaque, Suédois.

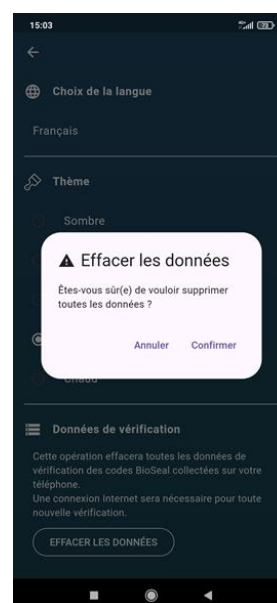


Choix du thème d'écran : sombre (noir), blanc, système (blanc), froid (bleu) et chaud (orange).



Effacement des données téléchargées (cache mémoire)

Effacement des manifestes et clés publiques de signature en mémoire. Un rafraîchissement de ces données est automatique à tous changements dans les « trusted-list », manifestes et autorités de certification (liste des certificats révoqués). En cas d'effacement, le fonctionnement « off line » n'est plus possible, une connexion internet est nécessaire pour acquérir de nouveau les informations et fonctionner à nouveau en mode « off line ».



8.5.2 Lecture de codes 2D par OtentiK Reader

Lecture d'un code 2D

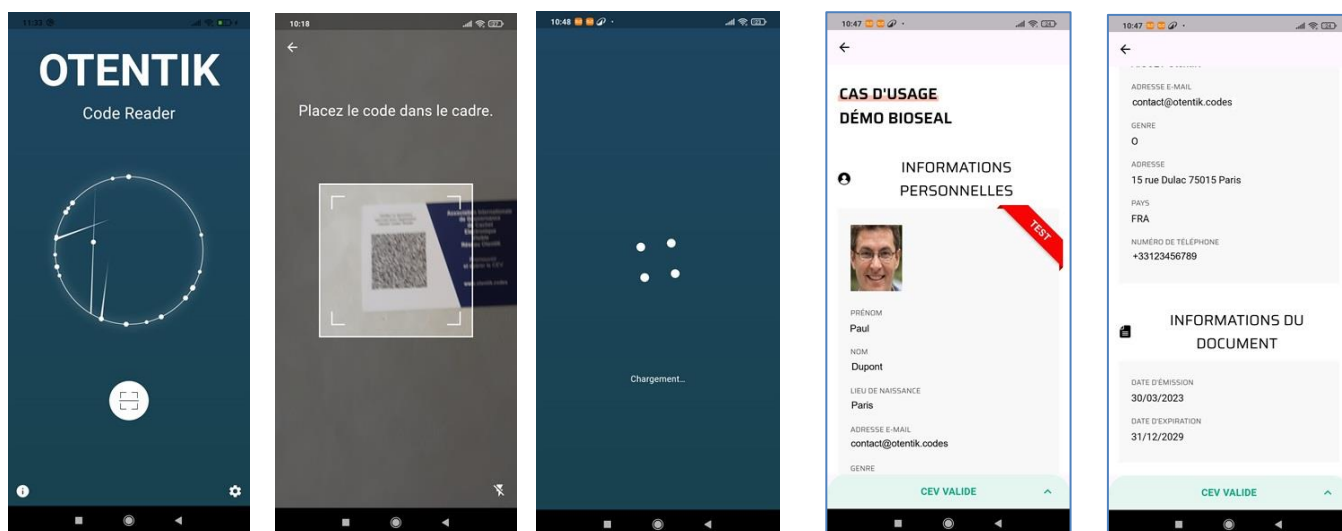
Dans cette version, la lecture d'un code à 2 dimensions s'applique à tous les types de code 2D et pour des « form-factors ¹ » imprimés et scannés par la caméra du smartphone ou téléchargés sur le smartphone sous forme de fichier PdF ou « picture » (JPEG, BMP, PNG, ...).

Les exemples abordés sont les suivants :

1. CEV sans fac-similé de présentation et contenant ou non des données biométriques (par exemple la photo).
2. CEV avec fac-similé de présentation.
3. Code 2D non sécurisé (non CEV normalisé) et contenant un lien de redirection. Cette fonction est utile pour lutter contre le *Qhishing*.
4. CEV ou Code 2D téléchargé depuis un document ou une photo.

¹ Facteurs de forme ou représentations

1- Lecture d'un CEV sans fac-similé



Dans l'exemple présenté ici, il s'agit de la lecture d'un document « Carte de visite » avec donnée biométrique (photo) sans fac-similé. Dans ce cas, les données sont affichées sous forme de tableau.

Visualisation du chemin de certification

Dans le cas où le CEV est valide, l'information est indiquée en couleur verte avec le détail suivant :

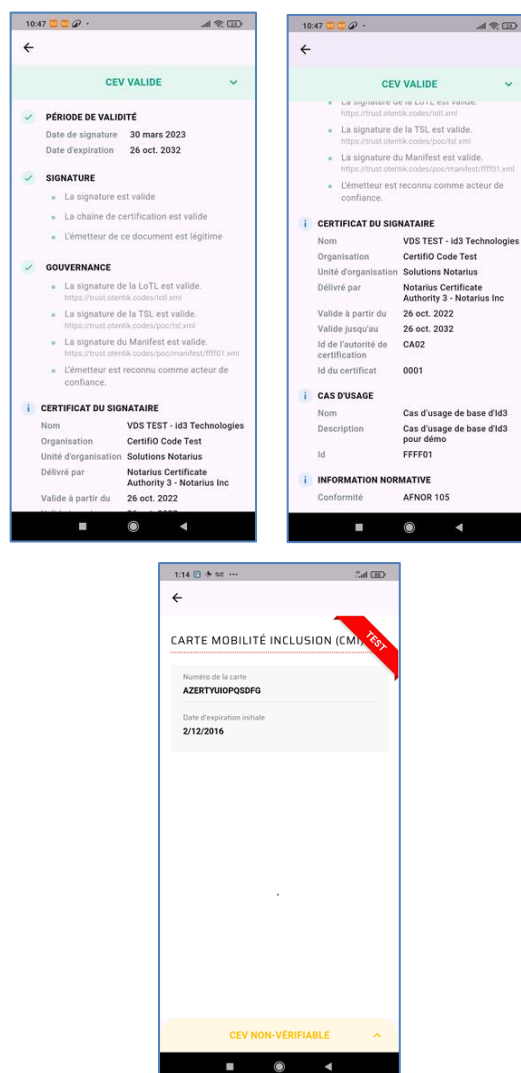
Information sur la période de validité du certificat, de la signature et de l'environnement de gouvernance (validité de la signature de la LoTL (List of Trusted List), de la TSL et du Manifest.

Information du détail du certificat de signature (Nom, Organisation, Autorité de Certification, Date de début et de fin de validité du certificat, identification de l'AC (information figurant dans l'entête du CEV) et de l'identifiant du certificat dans la TLS de l'AC (information figurant également dans l'entête du CEV).

Information sur le cas d'usage enregistré dans le Manifeste et information sur la Norme AFNOR ou ISO d'encodage (Z42-101, Z42-105 ou ISO 22 376).

Dans le cas où le CEV n'est pas valide, une information en rouge est affichée (CEV non valide) ou en orange (CEV non vérifiable).

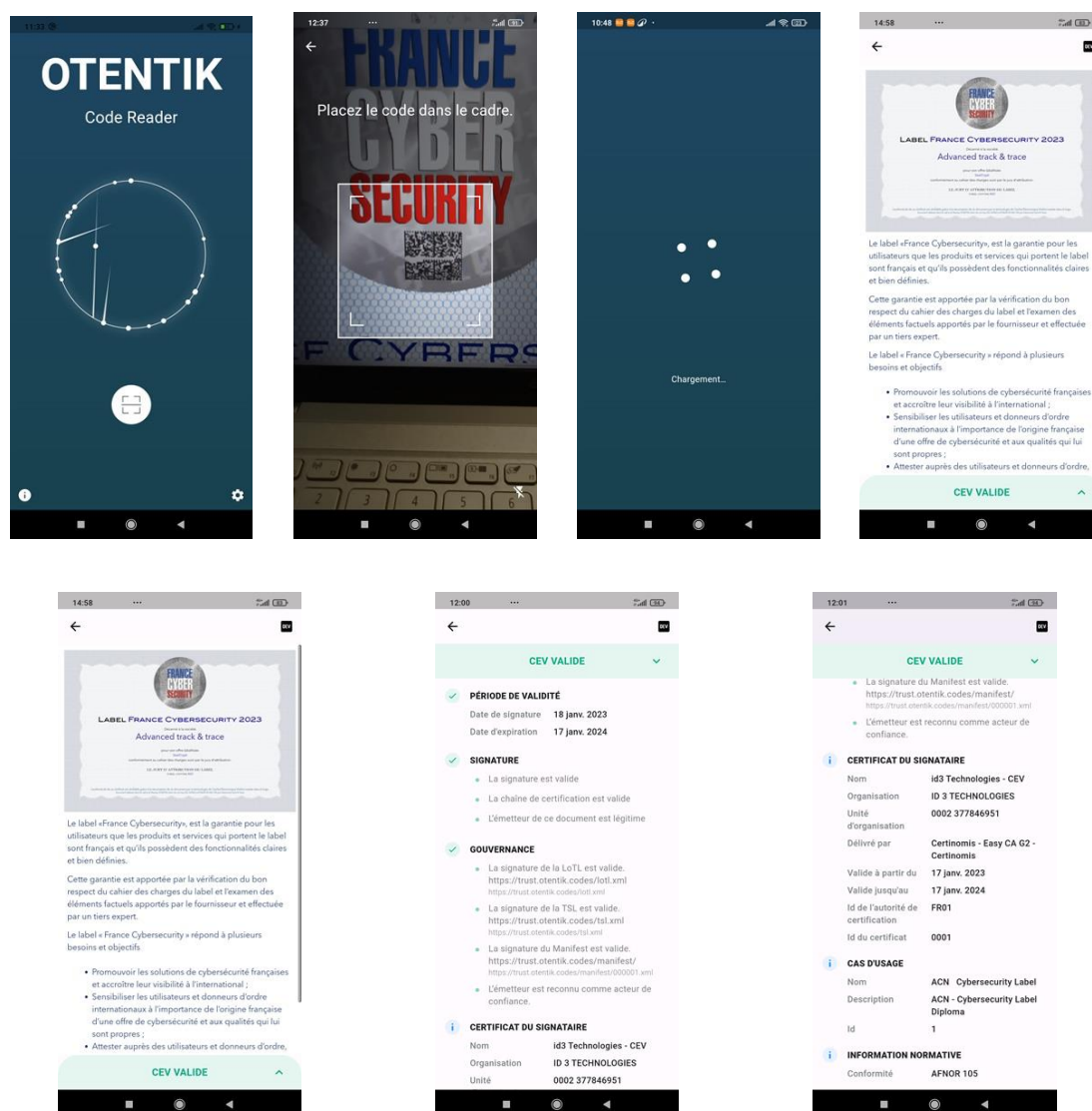
En option, si le profil du manifeste l'autorise, l'export des données est disponible sous forme de fichier XML ou CSV.



2- Lecture d'un CEV avec Fac-Similé



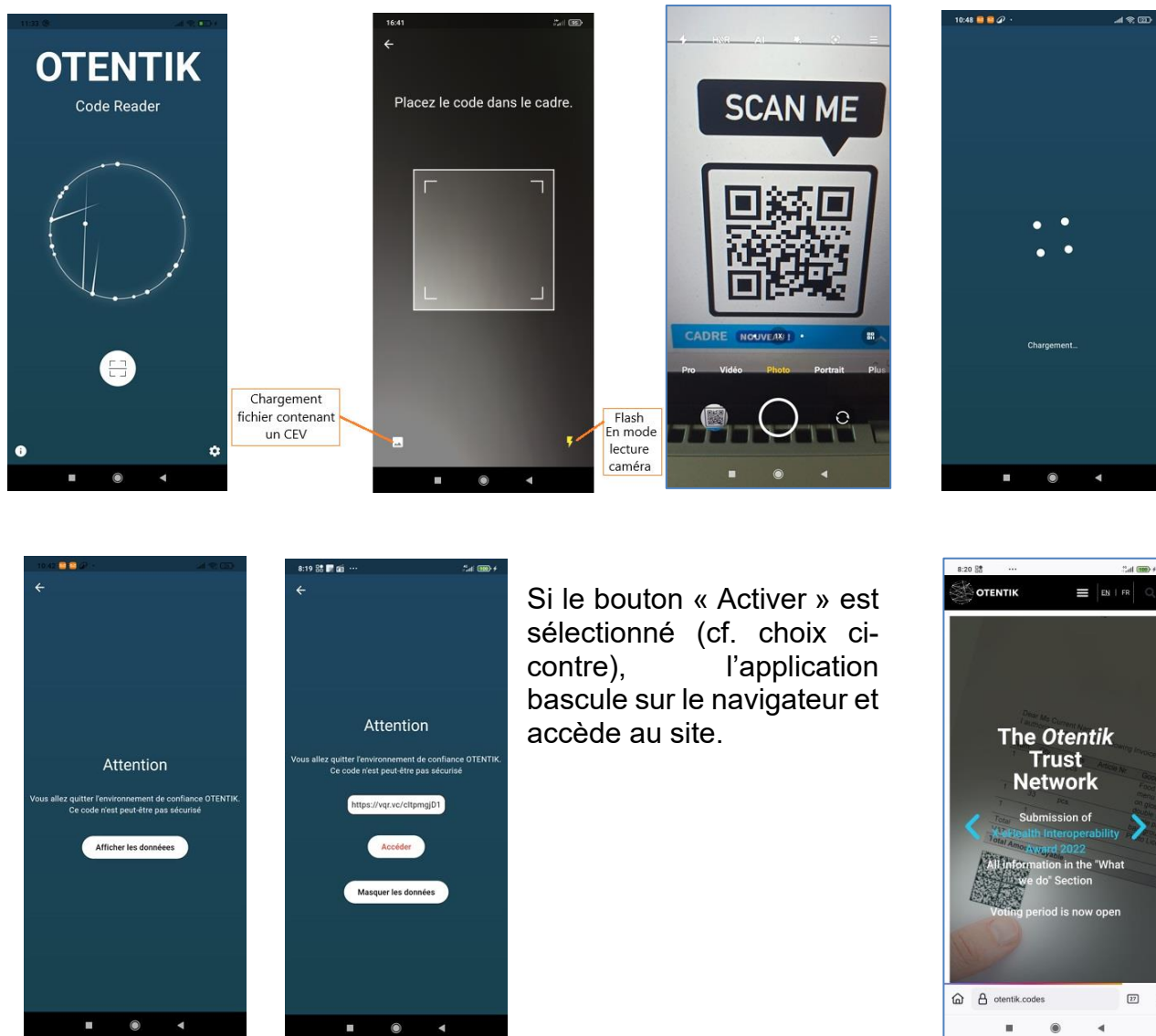
Dans cet exemple, le CEV est inclus dans le logo de « France Cyber Security » et sa lecture va restituer le fac-similé du diplôme original ainsi que le chemin de certification et la validité du CEV.



3- Lecture d'un Code 2D non CEV (Service de prévention contre le *Quishing*)

Il est possible de lire un code 2D, généralement un QR Code qui renvoie sur un lien pouvant donc être potentiellement frauduleux.

Dans ce cas, le lecteur OtentiK informe que le lien n'est pas signé et n'est donc pas sécurisé. Le contenu du lien encapsulé dans le code 2D est affiché et l'utilisateur a le choix de renoncer à poursuivre sa navigation ou bien de charger le lien et de s'y rendre.



4- Lecture d'un code 2D, CEV ou Non CEV enregistré sur le smartphone

En plus de lire les CEV avec la caméra du smartphone, il est également possible de télécharger un document contenant un code 2D, CEV ou non CEV, et de le lire directement avec l'application.

Une fois le code 2D détecté, il est lu, et le résultat s'affiche de la même manière que les codes 2D lus avec la caméra du smartphone.

