(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 092 414**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **19 01001**

(51) Int Cl[8] : ***G 06 F 21/44*** *(2019.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 01.02.19.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 07.08.20 Bulletin 20/32.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *IDEMIA IDENTITY & SECURITY FRANCE Société par actions simplifiée (SAS)* — FR.

(72) **Inventeur(s) :** MERCIER Laurent, HEURTIER Olivier, BONI Laurent et KERAUTRET Laurent.

(73) **Titulaire(s) :** IDEMIA IDENTITY & SECURITY FRANCE Société par actions simplifiée (SAS).

(74) **Mandataire(s) :** REGIMBEAU.

(54) Procédé d'authentification, serveur et dispositif électronique d'identité.

(57) L'invention propose un procédé d'authentification d'un dispositif électronique d'identité (1) présenté par un individu, le procédé étant caractérisé en ce qu'il comprend la mise en œuvre d'étapes de :

(b) Réception par des moyens de de traitement de données (21) d'un serveur (2) d'une image acquise dudit dispositif électronique d'identité (1), l'image représentant au moins un élément visuel personnel de l'individu et un code dynamique de vérification visibles sur ledit dispositif électronique d'identité (1), ledit code dynamique de vérification contenant au moins une information de référence représentative d'une apparence attendue dudit élément visuel ;

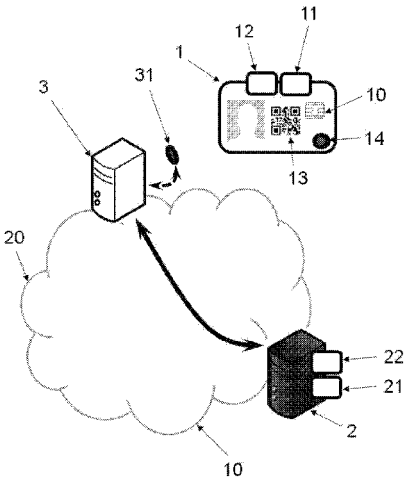
(c) Extraction par analyse de ladite image acquise par les moyens de de traitement de données (21) du serveur (2) de :

une information candidate représentative de l'apparence dudit élément visuel tel que représenté dans l'image acquise ; l'information de référence représentative de l'apparence attendue dudit élément visuel contenue dans ledit code dynamique de vérification tel que représenté dans l'image acquise ;

(d) Vérification par les moyens de de traitement de données (21) du serveur (2) que l'information candidate et l'information de référence extraites coïncident.

L'invention concerne également un serveur et un dispositif électronique d'identité à cet effet.

Figure pour l'abrégé : Fig. 1



FR 3 092 414 - A1

Description

Titre de l'invention : Procédé d'authentification, serveur et dispositif électronique d'identité

Domaine technique

[0001] L'invention concerne un procédé de contrôle à distance d'un équipement de verrouillage d'un véhicule via un terminal mobile, comprenant la comparaison entre une donnée biométrique candidate et au moins une donnée biométrique de référence.

Technique antérieure

[0002] La détention d'un document d'identité (carte d'identité, passeport, permis de conduire, carte de sécurité sociale, etc.) en cours de validité justifie de l'identité d'un individu auprès d'une autorité.

[0003] Les documents d'identité consistent en un support généralement en papier ou en plastique sur lequel sont imprimées une photo ainsi que des informations alphanumériques personnelles (nom, prénom, date de naissance, etc.) de son détenteur. On trouve également une bande appelée MRZ (Machine-Readable Zone, Zone de lecture optique), qui contient un code (généralement deux lignes de 36 caractères) résumant les informations alphanumériques du document.

[0004] Généralement, les documents d'identité présentent un grand nombre d'éléments de sécurité de haut niveau tels des filigranes ou des hologrammes pour prévenir la falsification. La durée de vie d'un tel document est généralement limitée (10 ou 15 ans), car l'apparence de son possesseur change progressivement, et les éléments de sécurité évoluent.

[0005] Ainsi, les documents d'identité originaux apportent satisfaction et s'avèrent très difficiles à contrefaire parfaitement, mais une difficulté se pose lorsque l'on en fait des copies.

[0006] En effet, de très nombreux tiers tels que des hôtels, des banques, des services de transports, etc., demandent occasionnellement un scan ou une photocopie d'un document d'identité par sécurité (par exemple pour récupérer une voiture de location).

[0007] Cela fait que sur la durée de vie d'un document d'identité, vont exister des centaines de copies de celui-ci, qui s'avèrent bien plus facilement falsifiables que l'original puisque ne permettant pas de contrôler les éléments de sécurité. Et on ne peut pas exclure que certaines de ces copies trainent dans des endroits accessibles comme sur un guichet ou sur un serveur non sécurisé.

[0008] En d'autres termes, le risque existe qu'un tiers mal intentionné récupère une photocopie de votre passeport, et modifie celle-ci de sorte à mettre sa photo à la place de la votre et usurpe votre identité pour ouvrir un compte bancaire, et ce peut-être des

années après que cette photocopie a été faite.

[0009] On note que la MRZ, qui apparait sur les copies, permet uniquement une lecture informatisée plus rapide (cela permet d'extraire directement les informations alphanumériques plutôt que de les retaper à la main), mais ne constitue pas un moyen de prouver la validité ou l'authenticité du document d'identité. De surcroit, la MRZ est aussi facile à falsifier sur une copie que la photo.

[0010] Pour résoudre ces difficultés, il a été proposé de rendre les documents d'identité électroniques, en embarquant un microprocesseur. Typiquement, on utilise à présent un support de type carte à puce, stockant dans son microprocesseur les données du document d'identité :

- La photo numérisée ;
- Tout ou partie des données alphanumériques imprimées sur la carte ;
- Un ou plusieurs certificats d'authentification (typiquement RSA, pour signature électronique).

[0011] Une lecture de la carte à puce (éventuellement sans contact) remplace alors avantageusement la fourniture d'une copie : par exemple, au guichet de la banque, au lieu de laisser une photocopie on s'authentifie en insérant la carte dans le lecteur, et les informations sont directement transmises au système d'information de la banque.

[0012] Une telle solution apporte satisfaction, mais reste conditionnée à la présence d'un lecteur. De surcroit, elle ne peut pas être mise en œuvre à distance, et il reste nécessaire dans ce cas de transmettre un scan (soit en l'envoyant par e-mail, sont en l'uploadant sur un serveur).

[0013] Plus récemment il a été proposé dans la demande EP3206192 un mécanisme très astucieux de génération à partir d'un élément visuel d'un document d'identité (en particulier la photo) d'une donnée de sécurité appelée « Digital Photo Seal ». Cette donnée de sécurité constitue une sorte d'empreinte de l'élément visuel : des images acquises d'un même élément visuel, quelles que soient les conditions d'acquisition (i.e. y compris suite à scan ou photocopie), conduisent à l'obtention de données de sécurité sensiblement identiques. Au contraire, la moindre modification de l'élément visuel entraîne une forte variation de cet élément de sécurité.

[0014] Ainsi, il suffit de stocker sur un serveur la donnée de sécurité de référence « attendue » pour un document donné, et de la comparer avec celle « candidate » générée à partir d'une copie de ce document, pour savoir si l'élément visuel de ce document est intègre ou non.

[0015] Cette solution permet donc un progrès notable en ce qu'on peut garantir qu'une copie d'un document d'identité est authentique.

[0016] Néanmoins, il reste dans un certain nombre de cas possible d'usurper une identité même sur la base d'une copie authentique d'un document d'identité, car il n'y a pas

toujours de contrôle de visu. Par exemple, on peut ouvrir un compte bancaire en ligne sans montrer son visage à personne : un usurpateur peut fournir une copie authentique d'une pièce d'identité d'un tiers même ne lui ressemblant pas. A noter que de plus en plus souvent les procédures d'authentification en ligne requièrent de montrer son visage en utilisant une webcam ou un smartphone pour comparaison visuelle avec la photo de la copie fournie, mais ce n'est pas systématique.

[0017] Et même lorsqu'il y a une telle comparaison, il y a toujours le risque qu'un usurpateur soit fournisse une fausse photo (une photo du détenteur légitime du document d'identité qu'il tente d'utiliser, par exemple trouvée sur un réseau social), voire même dupe la personne réalisant la comparaison. En effet, la vérification qu'un individu « ressemble » à la photo d'un document d'identité est subjective et soumise à l'aléa humain, a fortiori si la copie fournie est de mauvaise qualité (photocopie en noir et blanc, photo par smartphone, etc.), ce d'autant plus que l'on sait que sur toute la durée de vie d'un document d'identité l'apparence de son détenteur peut beaucoup évoluer, d'om une certaine tolérance.

[0018] Il serait ainsi souhaitable de disposer d'une solution simple, universelle, fiable, et totalement sécurisée d'authentification prévenant tout usage non contrôlé d'une copie d'un document d'identité.

Exposé de l'invention

[0019] Selon un premier aspect, l'invention concerne un procédé d'authentification d'un dispositif électronique d'identité présenté par un individu, le procédé étant caractérisé en ce qu'il comprend la mise en œuvre d'étapes de :

[0020] (b) Réception par des moyens de de traitement de données d'un serveur d'une image acquise dudit dispositif électronique d'identité, l'image représentant au moins un élément visuel personnel de l'individu et un code dynamique de vérification visibles sur ledit dispositif électronique d'identité, ledit code dynamique de vérification contenant au moins une information de référence représentative d'une apparence attendue dudit élément visuel ;

[0021] (c) Extraction par analyse de ladite image acquise par les moyens de de traitement de données du serveur de :

- une information candidate représentative de l'apparence dudit élément visuel tel que représenté dans l'image acquise ;
- l'information de référence représentative de l'apparence attendue dudit élément visuel contenue dans ledit code dynamique de vérification tel que représenté dans l'image acquise ;

[0022] (d) Vérification par les moyens de de traitement de données du serveur que l'information candidate et l'information de référence extraites coïncident.

[0023] Selon d'autres caractéristiques avantageuses et non limitatives :

- Le procédé comprend une étape (a) d'affichage par des moyens d'affichage dudit dispositif électronique d'identité dudit code dynamique de vérification ;
- l'étape (a) comprend la génération préalable dudit code dynamique de vérification par des moyens de traitement de données dudit dispositif électronique d'identité en fonction d'au moins ladite information de référence représentative d'une apparence attendue dudit élément visuel et un mot de passe à usage unique, OTP ;
- l'étape (a) et l'étape (c) comprennent chacune la génération dudit OTP, respectivement par les moyens de traitement de données du dispositif électronique d'identité et les moyens de de traitement de données du serveur, en fonction d'un secret partagé ;
- ledit mot de passe à usage unique est un mot de passe à usage unique basé sur le temps, TOTP, la génération dudit TOTP par les moyens de traitement de données du dispositif électronique d'identité et les moyens de de traitement de données du serveur étant également fonction d'une information temporelle ;
- ledit code dynamique de vérification contient également au moins une donnée descriptive dudit OTP généré par les moyens de traitement de données du dispositif électronique d'identité, l'étape (c) comprenant également l'extraction de la donnée descriptive dudit OTP contenue dans ledit code dynamique de vérification tel que représenté dans l'image acquise, l'étape (d) comprenant également la vérification que l'OTP généré les moyens de de traitement de données du serveur coïncide avec ladite donnée descriptive de l'OTP extraite ;
- ledit code dynamique de vérification est affiché sous la forme d'un code QR et/ou d'un code alphanumérique ;
- ledit code dynamique de vérification contient également une signature électronique de ladite information de référence représentative d'une apparence attendue dudit élément visuel, l'étape (c) comprenant également l'extraction de la signature électronique contenue dans ledit code dynamique de vérification tel que représenté dans l'image acquise, l'étape (d) comprenant également la vérification que ladite signature électronique extraite est valide ;
- ledit élément visuel personnel de l'individu est imprimé sur le dispositif électronique d'identité ;
- un élément visuel visible sur ledit dispositif électronique d'identité est un élément graphique, en particulier une photographie ou une signature manuscrite de l'individu, l'information de référence représentative d'une apparence attendue dudit élément graphique étant une donnée de sécurité de

type Digital Photo Seal ;

- un élément visuel visible sur ledit dispositif électronique d'identité est un attribut alphanumérique associé à l'individu, l'information représentative d'une apparence de cet élément visuel étant la valeur ou un haché de cet attribut alphanumérique associé à l'individu.

[0024] Selon un deuxième aspect, l'invention concerne un serveur d'authentification, caractérisé en ce qu'il comprend des moyens de de traitement de données configurés pour :

- Recevoir une image acquise d'un dispositif électronique d'identité présenté par un individu, l'image représentant au moins un élément visuel personnel de l'individu et un code dynamique de vérification visibles sur ledit dispositif électronique d'identité, ledit code dynamique de vérification contenant au moins une information de référence représentative d'une apparence attendue dudit élément visuel ;
- Extraire par analyse de ladite image acquise :
  - une information candidate représentative de l'apparence dudit élément visuel tel que représenté dans l'image acquise ;
  - l'information de référence représentative de l'apparence attendue dudit élément visuel contenue dans ledit code dynamique de vérification tel que représenté dans l'image acquise ;
- Vérifier que l'information candidate et l'information de référence extraites coïncident.

[0025] Selon un troisième aspect, l'invention concerne un dispositif électronique d'identité d'un individu sur lequel est visible au moins un élément visuel personnel dudit individu, caractérisé en ce qu'il comprend des moyens de de traitement de données configurés pour :

- Générer et afficher sur des moyens d'affichage un code dynamique de vérification contenant au moins une information de référence représentative d'une apparence attendue dudit élément visuel.

[0026] Selon d'autres caractéristiques avantageuses et non limitatives, les moyens de de traitement de données sont en outre configurés pour générer préalablement un mot de passe à usage unique, OTP, ledit code dynamique de vérification étant généré en fonction d'au moins ladite information de référence représentative d'une apparence attendue dudit élément visuel et dudit OTP généré.

[0027] Selon un quatrième aspect, l'invention concerne un système d'authentification comprenant un serveur d'authentification selon le deuxième aspect, au moins un dispositif électronique d'identité selon le troisième aspect, et au moins un équipement client comprenant des moyens d'acquisition optique pour l'acquisition de ladite image

représentant au moins l'élément visuel personnel de l'individu et le code dynamique de vérification visibles sur ledit dispositif électronique d'identité.

[0028] Selon un cinquième et un sixième aspects, l'invention concerne un produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé selon le premier aspect d'authentification d'un dispositif électronique d'identité présenté par un individu ; et un moyen de stockage lisible par un équipement informatique sur lequel un produit programme d'ordinateur comprend des instructions de code pour l'exécution d'un procédé selon le premier aspect d'authentification d'un dispositif électronique d'identité présenté par d'un individu.

Brève description des dessins

[0029] D'autres caractéristiques, buts et avantages de la présente invention apparaîtront à la lecture de la description détaillée qui va suivre, au regard des figures annexées, données à titre d'exemples non limitatifs et sur lesquelles :

[0030] [fig.1]

La figure 1 représente schématiquement un système pour la mise en œuvre du procédé selon l'invention ;

[0031] [fig.2a]

La figure 2a représente un type (carte à puce) de dispositif électronique d'identité pouvant être utilisé dans le procédé selon l'invention ;

[0032] [fig.2b]

La figure 2b représente un type (terminal de type smartphone) de dispositif électronique d'identité pouvant être utilisé dans le procédé selon l'invention ;

[0033] [fig.3a]

La figure 3a représente schématiquement un exemple de configuration du premier type de dispositif électronique d'identité pouvant être utilisée dans le procédé selon l'invention ;

[0034] [fig.3b]

La figure 3b représente schématiquement un exemple de configuration du premier type de dispositif électronique d'identité pouvant être utilisée dans le procédé selon l'invention ;

[0035] [fig.3c]

La figure 3c représente schématiquement un exemple de configuration du premier type de dispositif électronique d'identité pouvant être utilisée dans le procédé selon l'invention ;

[0036] [fig.3d]

La figure 3d représente schématiquement un exemple de configuration du premier type de dispositif électronique d'identité pouvant être utilisée dans le procédé selon

l'invention ;

[0037] [fig.4]

La figure 4 illustre un exemple d'évolution de code dynamique de vérification pour la mise en œuvre du procédé selon l'invention.

Description des modes de réalisation

[0038] *Architecture*

[0039] En référence à la **figure 1**, on a représenté schématiquement une architecture de système d'authentification pour la mise en œuvre du présent procédé d'authentification d'un dispositif électronique d'identité 1 présenté par un individu (i.e. de validation de l'authenticité dudit dispositif électronique d'identité 1), notamment en vue de l'authentification/identification dudit individu sur la base de ce dispositif 1. Ce système comprend au moins ledit dispositif électronique d'identité 1 et un serveur 2. Le système peut également comprendre un équipement client 3 connecté au serveur 2 via un réseau 20 tel qu'Internet.

[0040] Le dispositif électronique d'identité 1 est un équipement personnel à un individu (de nombreux individus peuvent posséder chacun un tel dispositif électronique d'identité), et constitue un document d'identité officiel, avantageusement émis par un organisme gouvernemental. Selon un mode de réalisation préféré, il prend la forme d'une carte à puce (de type « smart card », voir **figure 2a**) aux dimensions standard et généralement en PVC ou polycarbonate, mais il peut s'agir également d'un terminal de type smartphone ou tablette tactile, voir **figure 2b**.

[0041] Dans tous les cas, le dispositif électronique d'identité 1 comporte des moyens de traitement de données 11, i.e. un calculateur tel que par exemple un processeur, un microprocesseur, un contrôleur, un microcontrôleur, un FPGA etc. Ce calculateur est adapté pour exécuter des instructions de code pour mettre en œuvre le procédé ci-après. On note que si le dispositif électronique d'identité 1 est une carte à puce, les moyens de traitement de données 11 peuvent être distincts de la « puce » 10 (et le cas échéant en connexion avec cette dernière ou totalement isolés, voir plus loin), laquelle peut avoir un fonctionnement classique lorsqu'en interaction avec un lecteur. Plus précisément, on peut partir d'une carte à puce d'identité existante, et y rajouter les moyens de traitement 11.

[0042] Le dispositif 1 peut également comprendre des moyens de stockage de données 12 (une mémoire, par exemple flash), des moyens d'affichage 13 (typiquement un écran, en particulier de type à encre électronique si le dispositif 1 est une carte à puce), une batterie, et éventuellement un bouton 14. Divers modes de réalisation du dispositif 1 de type carte à puce sont représentés sur les **figures 3a-3d** (leurs avantages et inconvénients seront décrits plus en détail plus loin) :

- sur la figure 3a, la puce 10 et les moyens de traitement de données 11 sont complètement isolés ;
- sur la figure 3b, la puce 10 et les moyens de traitement de données 11 sont connectés de sorte à ce que les moyens de traitement de données 11 puissent accéder aux données de la puce 10 ;
- sur la figure 3c, la puce 10 et les moyens de traitement de données 11 sont connectés électriquement, de sorte à permettre une alimentation électrique et/ ou une recharge de la batterie par contact (lors d'une communication avec un lecteur conventionnel) ou par induction (lors d'une communication sans contact) ;
- sur la figure 3d, le dispositif électronique d'identité 1 comprend un bouton 14 connecté aux moyens 11. Sur cette figure 3d, on trouve la double liaison entre la puce 10 et les moyens de traitement de données 11 de la figure 3c, mais on pourrait alternativement trouver un bouton 14 dans les architectures des figures 3a et 3d. Et on répète que dans toutes ces figures, la batterie et le bloc timer restent optionnels.

[0043] Le serveur 2 est un équipement distant, sécurisé, typiquement d'une autorité ou d'un fournisseur de solution de sécurité. A nouveau il comprend des moyens de traitement de données 21 et une mémoire 22.

[0044] L'équipement client 3 est un terminal local comprenant des moyens d'acquisition optique 31, et adapté pour acquérir et le cas échéant transmettre au serveur 2 une image (du dispositif 1 comme on le verra). L'équipement client 3 et le serveur 2 comprennent avantageusement des interfaces de communications leur permettant de dialoguer à distance.

[0045] On note que l'équipement 3 reste optionnel, et peut prendre de nombreux modes de réalisation. Plus précisément et comme l'on verra, il suffit pour la mise en œuvre du procédé que le serveur 2 puisse recevoir une image acquise du dispositif électronique d'identité 1 d'une façon ou d'une autre, y compris indirectement :

- Selon un premier mode de réalisation, l'équipement client 3 est directement connecté au serveur 2 via le réseau 20, et est notamment un terminal mobile de type smartphone, un scanner, une webcam, etc., lequel peut prendre en photo/scanner le dispositif électronique d'identité 1 (ou une copie de ce dernier, en particulier une photocopie) et envoyer l'image acquise au serveur via un réseau filaire (Ethernet), sans-fil (Wi-Fi) ou de téléphonie mobile (GPRS, 3G, 4G ou autre). Par exemple, l'équipement client 3 peut être un scanner à un guichet de banque, utilisé par un employé qui souhaite authentifier en direct le dispositif électronique d'identité 1 d'un individu devant lui ;

- Selon un deuxième mode de réalisation, l'équipement client 3 n'est pas connecté directement au serveur 2, qu'il soit offline ou que la connexion soit indirecte. On peut envisager par exemple que :
  - l'équipement client 3 est à nouveau un terminal mobile de type smartphone, un scanner ou une webcam, cette fois personnel à l'individu qui souhaite l'authentification, qui acquiert toujours l'image du dispositif électronique d'identité 1 mais la transfère (par exemple par e-mail ou via upload sur un site internet) à un tiers (par exemple un loueur de véhicule : typiquement, il doit fournir son permis de conduire pour conclure une location par internet), et c'est ce dernier qui va se connecter au serveur 2 pour la mise en œuvre du procédé ;
  - L'équipement client 3 est un équipement non connecté tel qu'un appareil photo numérique, devant transmettre l'image acquise par exemple par câble usb à un équipement tiers (par exemple un PC), lequel est connecté directement ou indirectement au serveur 2 ;
- Selon un troisième mode de réalisation, l'équipement client 3 est confondu avec le dispositif électronique d'identité 1, en particulier si ce dernier est un terminal mobile de type smartphone. On peut imaginer que l'image du dispositif électronique d'identité 1 s'acquière par exemple en prenant une photo de lui-même dans un miroir, ou via une capture d'écran.

[0046] Dans tous les cas, comme expliqué l'équipement client 3 peut acquérir une image d'une image du dispositif électronique d'identité 1, i.e. photographie une photocopie plutôt que le dispositif 1 directement, voire d'une photocopie d'une photocopie, etc. Comme l'on verra, il suffira que l'image acquise représente le dispositif 1. On comprendra que le présent procédé n'est limité à aucune façon d'obtenir cette image et aucune nature en particulier (l'image acquise peut être en noir et blanc, de mauvaise qualité, etc.).

[0047] *Principe*

[0048] La présente invention propose qu'au moins un élément visuel personnel de l'individu et un code dynamique de vérification soient visibles sur ledit dispositif électronique d'identité 1, ledit code dynamique de vérification contenant au moins une information de référence représentative d'une apparence attendue dudit élément visuel.

[0049] Par élément visuel personnel de l'individu, on entend soit un élément graphique et en particulier une photographie de l'individu (comme on trouve aujourd'hui sur tous les documents d'identité) mais également une signature manuscrite de l'individu, soit un attribut alphanumérique associé à l'individu, généralement choisi parmi une liste de possibilités :

- Numéro du document d'identité que constitue le dispositif 1 ;
- Date d'expiration ;
- Date de délivrance ;
- Nom ;
- Prénom(s) ;
- Nationalité ;
- Date de Naissance ;
- Lieu de Naissance ;
- Sexe ;
- Taille ;
- Adresse ;
- etc.

[0050] On comprendra qu'il peut y avoir une pluralité d'éléments visuels personnels visibles, avantageusement au moins un élément graphique de type photographie, et que ledit code dynamique de vérification contient pour chacun d'au moins une partie de (avantageusement toute) cette pluralité d'éléments visuels une information de référence représentative d'une apparence attendue de cet élément visuel personnel.

[0051] Ce ou ces éléments visuels personnels sont imprimés sur le dispositif électronique d'identité 1 (typiquement si le dispositif électronique d'identité 1 est une carte à puce, voir exemple de la figure 2a), et/ou affichés par les moyens d'affichage 13 (typiquement si le dispositif électronique d'identité 1 est un smartphone, voir l'exemple de la figure 2b). Dans le premier cas (élément visuels imprimés sur le dispositif électronique d'identité 1), on comprend que leur apparence est donc permanente sur la durée de vie du dispositif 1.

[0052] A noter que préférentiellement les éléments visuels pour lesquels une information de référence est contenue dans le code de vérification dynamique sont disposés de sorte à être visibles simultanément, et en même temps que ce code de vérification dynamique (par exemple sur la même face, ce qui est cas dans l'exemple de la Figure 2a), ce qui permet l'acquisition d'une seule image représentant en même temps chaque élément visuel personnel de l'individu et le code dynamique de vérification, mais on comprendra qu'il est possible qu'une partie de ces éléments visuels soient par exemple disposés sur un verso de la carte, ce qui oblige à acquérir deux images (recto et verso) pour que l'ensemble des éléments visuels soit représenté. Dans tous les cas, il faut qu'au moins un élément visuel et le code dynamique de vérification soient visibles en même temps pour éviter la fraude, et dans la suite de la description on prendra l'exemple préféré d'une carte à puce à une face du type de celle de la Figure 2a.

[0053] Le code de vérification dynamique est affiché quant à lui nécessairement sur les moyens d'affichage 13, puisqu'il est dynamique. Cela signifie qu'il varie au cours du

temps comme représenté par exemple sur la **Figure 4** (on verra différents algorithmes plus loin), et donc change d'apparence, mais pour autant il contient toujours la ou lesdites informations de référence représentatives d'une apparence attendue d'un élément visuel.

[0054] Par information représentative d'une apparence d'un élément visuel, on entend une donnée descriptive d'au moins un fragment de cet élément visuel tel qu'il apparait, i.e. une « empreinte », qui va permettre des comparaisons.

[0055] On désigne comme information « de référence » l'information représentative de l'apparence « théorique » de l'élément visuel, i.e. tel qu'attendue. Par contraste, on désigne comme information « candidate » l'information représentative de l'apparence constatée de l'élément visuel, i.e. tel que représenté dans une image acquise. On comprend que cette apparence constatée n'est généralement pas parfaitement identique à l'apparence attendue, du fait des conditions des défauts inhérents à l'acquisition d'une image, et à la variabilité des conditions de prise de vue (éclairage, bougé, distance, etc.).

[0056] Néanmoins, ladite information représentative de l'apparence est choisie de telle sorte que si deux éléments visuels ont des apparences qui coïncident (i.e. il s'agit du même élément visuel même si les conditions de prise de vue ne sont pas identiques), alors leurs informations représentatives coïncident (i.e. présentent une distance selon une métrique donnée inférieure à un seuil) également.

[0057] Ainsi, l'information de référence et l'information candidate coïncident si et seulement si l'apparence constatée et l'apparence attendue de l'élément visuel coïncide, i.e. qu'il s'agit bien du même élément visuel, en d'autres termes que l'élément visuel imprimé/affiché sur le dispositif électronique d'identité 1 n'a pas été frauduleusement altérée. Cette vérification peut être faite pour chaque élément visuel pour lequel une information représentative est contenu par le code dynamique de vérification.

[0058] Si l'élément visuel est un élément graphique tel qu'une photographie ou une signature, on pourra utiliser comme information représentative de l'apparence de l'élément graphique le « Digital Photo Seal », i.e. la donnée de sécurité telle que décrite dans la demande EP3206192, basée sur la position de points singuliers de l'élément graphique.

[0059] Si l'élément visuel est un attribut alphanumérique, l'information de référence représentative d'une apparence attendue de cet élément visuel peut directement être la valeur de cet attribut alphanumérique ou un haché (en anglais un « hash », c'est-à-dire une empreinte cryptographique) de cet attribut alphanumérique en utilisant une fonction de hachage cryptographique quelconque.

[0060] En résumé, on comprend que le dispositif électronique d'identité affiche sa propre

« clé » de vérification (elle n'a besoin d'être stockée nulle part), et ce de façon dynamique, ce qui rend caduc les vieilles copies du dispositif 1. Plus précisément, un code généré n'est valide que pour une durée brève, ce qui permet sans difficulté son utilisation pour une authentification comme dans l'art antérieur, y compris sur la base d'une copie, mais de manière temporaire. Ainsi, il est impossible qu'un tiers utilise postérieurement une copie à des fins détournées : le code dynamique de vérification, bien que valide, aura expiré.

[0061] Le code dynamique de vérification est préférentiellement affiché sous la forme d'un code QR, ou toute autre code matriciel, comme visible sur les figures, de fait du volume de données qu'il peut contenir et sa robustesse. Néanmoins, on pourra afficher n'importe quel type de signal visuel, y compris un watermark (« tatouage numérique » en français), un code alphanumérique, une lumière clignotante, etc. Avantageusement, le code dynamique de vérification peut être affiché sous plusieurs formes à la fois, comme l'on voit sur les figures (un code QR plus un code à six chiffres), i.e. une partie primaire contenant toutes les données à transmettre (le code QR dans les figures) et une partie secondaire de redondance contenant tout ou partie des données (le code à six chiffres), préférentiellement sous forme alphanumérique pour pouvoir être lisible et saisie sur une interface. Cette partie secondaire a de nombreux usages. Elle peut permettre d'une part à l'utilisateur de visualiser plus facilement la mise à jour dynamique du code de vérification, elle peut augmenter la sécurité (caractère redondant), voire même être utilisé dans des authentifications supplémentaires, voir plus loin.

[0062] On note que des cartes à puce avec affichage d'un code de vérification dynamique sont connues, notamment le cryptogramme visuel (CVV) d'une carte bancaire, voir par exemple la demande FR3038418. On parle alors de D-CVV. On comprendra que de tels codes sont juste des clés permettant une transaction, ne sont par destinés à être représentés dans une image, et surtout ne contiennent pas d'information de référence représentative d'une apparence attendue d'un élément visuel personnel visible sur la carte.

[0063] L'utilisation d'une technologie à encre électronique (e-ink) pour les moyens d'affichage permet de limiter au maximum la consommation électrique (l'affichage en lui-même ne consomme rien, c'est le changement d'état qui consomme) et d'être compatible avec un dispositif 1 de type carte à puce.

[0064] A noter que si les moyens de traitement de données 11 peuvent accéder aux données de la puce 10 (la puce 10 et les moyens de traitement de données 11 sont connectés comme dans la figure 3c), le code dynamique de vérification comprend en outre avantageusement une signature des informations de référence. En effet, la puce 10 stocke des certificats pouvant être utilisés pour signature électronique. On rappelle qu'une

signature électronique d'une donnée est typiquement un chiffré d'un haché de cette donnée au moyen d'une clé privée.

[0065] *Génération du code dynamique de vérification*

[0066] Dans un mode de réalisation préféré, le procédé commence par une étape (a) d'affichage par des moyens d'affichage 13 dudit dispositif électronique d'identité 1 dudit code dynamique de vérification de génération, avantageusement précédée par la génération dudit code dynamique de vérification par des moyens de traitement de données 11 dudit dispositif électronique d'identité 1 en fonction d'au moins ladite information de référence représentative d'une apparence attendue dudit élément visuel et un mot de passe à usage unique, OTP. C'est cet OTP qui permet le caractère dynamique.

[0067] Par OTP, on entend une donnée valide pour une seule « session » (par session on entend soit une utilisation du dispositif électronique d'identité 1, i.e. une authentification, soit un intervalle temporel, par exemple 10 minutes). De façon connue, la génération du code dynamique met typiquement en œuvre une fonction cryptographique (par exemple en utilisant une clé publique du serveur 2) dans laquelle l'OTP est utilisé comme aléa.

[0068] L'étape (a) comprend à ce titre préférentiellement chacune la génération dudit OTP, sur la base d'un secret stocké par le dispositif électronique d'identité 1 (par exemple sur sa mémoire 12).

[0069] Selon un premier mode de réalisation, l'OTP est « basé sur les événements » (event-based). Cela signifie qu'il faut un événement pour générer un OTP, par exemple l'appui sur un bouton 14 s'il y en a un. De nombreux algorithmes de génération d'un tel OTP sont connus, par exemple on va appliquer récursivement une fonction de hachage cryptographique à une valeur initiale, cette valeur et/ou un paramètre de la fonction constituant le secret. Alternativement, le secret peut directement être une liste d'OTP pré-générés, la liste étant dépilée à chaque événement. Encore alternativement, l'OTP peut être de type HOTP, i.e. « HMAC-based », où un HMAC (hash-based message authentication code) est un type de code d'authentification de message. La génération d'un HOTP utilise un compteur, incrémenté à chaque utilisation.

[0070] Dans un tel mode réalisation, préférentiellement les moyens d'affichage 13 ne sont actifs que pendant une durée prédéterminée après la génération du code dynamique de vérification, par exemple 1 minute, pour économiser la batterie.

[0071] Selon un deuxième mode de réalisation, l'OTP est « basé sur le temps » (time-based). On parle alors de TOTP. Ici la génération de l'OTP est également fonction d'une information temporelle, en particulier fournie par un timer mis en œuvre par les moyens de traitement de données 11. Ainsi, le code dynamique de vérification généré est valide pendant un intervalle de temps prédéterminé, par exemple 30 secondes. A l'expiration

de cet intervalle, un nouveau TOTP et donc un nouveau code de vérification est généré, et ainsi de suite. De nombreux algorithmes de génération d'un TOTP sont connus, on citera par exemple une extension de l'algorithme de génération des HOTP, dans lequel le compteur est remplacé par l'information temporelle.

[0072] Dans ce second mode de réalisation, les moyens d'affichages 13 peuvent afficher en permanence le code dynamique de vérification actuellement valide (en particulier si les moyens sont à encre électronique et à basse consommation), i.e. mettre à jour l'affichage à l'expiration de chaque intervalle de temps de validité, ou bien n'activer l'affichage que par exemple lorsque le bouton 14 est pressé. On note que la consommation électrique peut être plus élevée, mais un tel mode est particulièrement préféré car il n'y a pas de risque de « décalage » d'OTP qui pourrait survenir si par exemple dans le mode de réalisation event-based l'utilisateur appuyait par erreur plusieurs fois de suite sur le bouton 14 : à un instant donné il y a un unique TOTP possible.

[0073] La génération en elle-même du code dynamique de vérification à partir de la ou les informations de référence et de l'OTP pourra être mise en œuvre de n'importe quelle façon connue, notamment en chiffrant les informations en utilisant l'OTP comme aléa.

[0074] A noter que le code dynamique de vérification peut également contenir une ou plusieurs données représentatives de l'OTP, i.e. soit l'OTP en lui-même soit des données de vérification de l'OTP, par exemple un haché de l'OTP et/ou une information temporelle sur la génération de l'OTP (notamment la date de génération, ou bien l'information temporelle utilisée pour la génération si c'est un TOTP), pour éviter que l'on puisse accéder aux informations de référence en déchiffrant le code dynamique. A noter qu'il est tout à fait possible que le code contienne à la fois l'OTP en lui-même et une autre donnée représentative telle que la date de génération. Comme l'on verra cela permettra notamment de détecter des cas dans lesquels l'image du dispositif électronique d'identité n'est pas frauduleuse mais simplement expirée. Le code dynamique de vérification peut contenir le cas échéant une signature électronique de la ou les données représentatives de l'OTP, pour garantir encore davantage leur authenticité. Selon un mode de réalisation, ladite information représentative de l'OTP constitue la partie secondaire l'OTP (le code alphanumérique à six chiffres visible sur les figures).

[0075] En résumé, le code dynamique de vérification peut contenir :

- les informations de référence représentant l'apparence attendue de chacun des éléments visuels ;
- une signature électronique de ces informations de référence ;
- l'OTP et/ou d'autres données représentatives de l'OTP ;
- une signature électronique de ces données représentatives de l'OTP.

[0076] A ce stade, le dispositif électronique d'identité 1 peut être utilisable par son détenteur à n'importe quel moment : il lui suffit comme expliqué d'acquérir d'une façon ou d'une autre (par exemple via les moyens d'acquisition 31 du client 3) d'une image acquise du dispositif électronique d'identité 1, l'image représentant au moins un élément visuel personnel de l'individu et un code dynamique de vérification visibles sur ledit dispositif électronique d'identité 1. Préférentiellement, ladite image représente tout le dispositif électronique d'identité 1, du moins toute une face. Comme expliqué, il peut être nécessaire d'acquérir plusieurs images, par exemple pour voir toutes les faces.

[0077] *Vérification*

[0078] On va à présent décrire la partie principale du procédé selon l'invention d'authentification d'un dispositif électronique d'identité 1 présenté par un individu comme étant le sien, et fournissant à ce titre d'une manière ou d'une autre une image acquise de ce dispositif électronique d'identité 1.

[0079] L'objectif est de vérifier que l'étape (a) s'est bien déroulée comme décrit précédemment, et qu'on n'est pas en présence d'un faux (par exemple une image qui aurait être modifiée frauduleusement). Pour cela, l'entité qui souhaite l'authentification (par exemple une banque) soumet cette image au serveur 2.

[0080] Dans une étape (b), les moyens de de traitement de données 21 du serveur 2 reçoivent ladite image acquise d'un dispositif électronique d'identité 1 présenté par ledit individu. Comme expliqué, l'image représente au moins un élément visuel personnel de l'individu et un code dynamique de vérification visibles sur ledit dispositif électronique d'identité 1.

[0081] Dans une étape (c), les moyens de de traitement de données 21 du serveur 2 analysent l'image, de sorte à extraire :

- une information candidate représentative de l'apparence dudit élément visuel tel que représenté dans l'image acquise ;
- l'information de référence représentative de l'apparence attendue dudit élément visuel contenue dans ledit code dynamique de vérification tel que représenté dans l'image acquise (et le cas échant la donnée représentative de l'OTP et/ou la signature électronique).

[0082] L'extraction de l'information candidate comprend l'identification de l'élément visuel qui apparait dans l'image (à nouveau un élément graphique, un attribut alphanumérique, etc.), et l'obtention de l'information candidate de la même façon que l'information de référence à été obtenue de l'élément visuel attendu. L'identification des éléments visuel peut être faite grâce à des modèles et des masques (en effet, les divers éléments visuels et le code dynamique de vérification apparaissent toujours au même endroit sur la surface du dispositif électronique d'identité 1), et ainsi, l'analyse

de l'image peut comprendre la reconnaissance d'un contour du dispositif électronique d'identité 1, le recadrage de ce contour, et l'application des masques prédéterminés. Pour cela, des réseaux de neurones à convolutions adaptés pourront être utilisés astucieusement.

[0083] Une fois que les éléments visuels et le code dynamique de vérification ont été « isolés » sur l'image, on applique les mêmes algorithmes que ceux qui ont été appliqués sur les éléments visuels d'identités pour obtenir les informations candidates représentatives de l'apparence dudit élément visuel tel que représenté.

[0084] Par exemple, si un élément visuel est un élément graphique tel qu'une image, l'information représentative de l'apparence dudit élément visuel peut être une donnée de sécurité de type « Digital Photo Seal ». Similairement, si un élément visuel est un attribut alphanumérique, on peut mettre en œuvre une reconnaissance optique de caractères (OCR) de sorte à lire cet attribut alphanumérique.

[0085] On comprend que les informations de référence et candidate devront être obtenues de manière identique de sorte à pouvoir être comparées.

[0086] En ce qui concerne l'information de référence représentative de l'apparence attendue dudit élément visuel contenue dans ledit code dynamique de vérification tel que représenté dans l'image acquise, il faut lire le code dynamique de vérification (ce qui est facile si par exemple il prend la forme d'un code QR), et le déchiffrer.

[0087] Cela nécessite la connaissance de l'OTP. Dans tous les cas, l'étape (c) comprend également la génération dudit OTP du coté serveur 2 de manière identique à la génération qui a eu lieu du coté dispositif électronique d'identité 1, de sorte soit à vérifier un OTP contenu dans le code dynamique lu, soit à déchiffrer ce code dynamique.

[0088] En d'autres termes, l'étape (a) et l'étape (c) comprennent chacune la génération dudit OTP, respectivement par les moyens de traitement de données 11 du dispositif électronique d'identité 1 et les moyens de de traitement de données 21 du serveur 2, en fonction d'un secret partagé. On comprend ainsi qu'à la création du dispositif électronique d'identité 1 (généralement par une entité gouvernementale), le même secret est généré et chargé dans la mémoire 12 du dispositif électronique d'identité 1 et la mémoire 22 du serveur 2, associé en particulier à un identifiant du dispositif électronique d'identité 1.

[0089] Si l'OTP est un TOTP, une information temporelle est également prise en compte du coté serveur 2. Naturellement, on comprend qu'elle ne peut être exactement la même que celle lors de la mise en œuvre de l'étape (a), car il faut quelques secondes d'acquisition de l'image, de transfert par le réseau 20 et de traitement, mais dans la mesure où le TOTP est généré par intervalle de temps, le même TOTP restera généré du coté serveur 2.

[0090] Dans une étape (d), les moyens de de traitement de données 21 du serveur vérifient 2

que l'information candidate et l'information de référence coïncident.

[0091] Le terme « coïncide » signifie de façon générale que le résultat d'une comparaison de l'information candidate et de l'information de référence doit montrer qu'elles sont identiques, ou du moins présenter une distance inférieure à un seuil d'erreur prédéterminé. Cela dépend du type d'élément visuel. Par exemple, pour les éléments graphiques, des données de sécurité de type Digital Photo Seal coïncident si elle différent de moins de 10%. En ce qui concernent des attributs alphanumériques, ils doivent être identiques.

[0092] Si le dispositif 1 ou l'image acquise le représentant a été altéré (par exemple en remplaçant la photographie), alors les informations candidates et de référence correspondantes ne coïncideront pas (pour au moins un élément visuel), et l'authentification sera rejetée. Une alerte pour utilisation frauduleuse peut être émise.

[0093] De façon préférée, si l'OTP ou une donnée représentative de l'OTP est contenue dans le code dynamique de vérification, l'étape (d) comprend la comparaison de cet OTP ou donnée représentative de l'OTP obtenu avec l'OTP généré par les moyens de de traitement de données 21 du serveur 2. Par exemple, si la donnée représentative de l'OTP obtenue est un haché, alors les moyens de de traitement de données 21 du serveur 2 calculent le haché de l'OTP généré, et vérifient qu'ils sont identiques. Sinon, c'est que l'OTP utilisé pour générer le code dynamique de vérification représenté dans l'image acquise est expiré. A noter que cela ne signifie pas nécessairement une utilisation frauduleuse, mais a priori que la copie est trop ancienne. Il suffit d'inviter l'individu à renouveler sa tentative d'authentification, avec un OTP plus récent.

[0094] De façon préférée, si le code dynamique de vérification contient une signature, l'étape (d) comprend également la vérification de cette signature, typiquement en la déchiffrant (c'est un chiffré d'un haché des informations de référence) avec une clé publique, elle permet de garantir l'authenticité des informations contenues dans le code de vérification dynamique. Si ce n'est pas le cas, c'est qu'on a tenté de générer un faux code dynamique de vérification (sur la base d'éléments visuels attendus « contrefaits »), et donc une alerte pour utilisation frauduleuse peut être émise.

[0095] Au contraire, si :

- Chaque information de référence obtenue coïncide avec l'information candidate correspondante ;
- Chaque donnée descriptive de l'OTP obtenue coïncide avec l'OTP généré ;
- Chaque signature électronique est valide ;

[0096] Alors l'authentification est confirmée.

[0097] A noter que pour des authentifications supplémentaires (une fois qu'une première authentification selon le présent procédé a été accomplie), on peut mettre en œuvre des authentifications simplifiées sur la base du dispositif électronique d'identité 1,

notamment dans un contexte d'authentification forte (par exemple, la première authentification complète est requise pour ouvrir un compte en banque, et ensuite l'authentification simplifié est utilisée en complément d'un mécanisme de login/mot de passe pour accéder en ligne aux comptes).

[0098] Par « simplifiée », on entend que l'acquisition d'une image n'est plus nécessaire, il suffit par exemple de saisir la partie secondaire du code dynamique de vérification (i.e. le code alphanumérique à six chiffres, voir avant).

[0099] Une authentification complète peut être réexigée au bout d'un certain temps, par exemple un an.

[0100] *Equipements*

[0101] Selon un deuxième et un troisième aspect, sont proposés le serveur 2 d'authentification et le dispositif électronique d'identité 1 pour la mise en œuvre du procédé selon le premier aspect, i.e. l'authentification du dispositif électronique d'identité 1.

[0102] Le serveur 2 est typiquement connecté à un réseau 20, et comprend des moyens de de traitement de données 21 configurés pour :

- Recevoir une image acquise d'un dispositif électronique d'identité 1 présenté par un individu, l'image représentant au moins un élément visuel personnel de l'individu et un code dynamique de vérification visibles sur ledit dispositif électronique d'identité 1, ledit code dynamique de vérification contenant au moins une information de référence représentative d'une apparence attendue dudit élément visuel ;
- Extraire par analyse de ladite image acquise :
  - une information candidate représentative de l'apparence dudit élément visuel tel que représenté dans l'image acquise ;
  - l'information (ou les informations) de référence représentative(s) de l'apparence attendue dudit (ou desdits) élément(s) visuel(s) contenue(s) dans ledit code dynamique de vérification tel que représenté dans l'image acquise (et le cas échéant au moins une donnée représentative d'un OTP et/ou une signature électronique) ;
- Vérifier que l'information candidate et l'information de référence extraites coïncident, avantageusement après avoir généré un OTP, et le cas échéant vérifier que cet OTP coïncidait avec la ou les données représentatives d'un OTP extraites, et/ou vérifier la signature électronique extraite.

[0103] Le dispositif électronique d'identité 1 d'un individu est comme expliqué une carte à puce ou un terminal de type smartphone, sur lequel est visible au moins un élément visuel personnel dudit individu (préférentiellement imprimé si c'est une carte à puce).

[0104] Il comprend des moyens de de traitement de données 11, une mémoire 12, des

moyens d'affichage 13, et potentiellement un bouton 14 et/ou une batterie.

[0105] Les moyens de de traitement de données 11 sont configurés pour :

- Avantageusement générer un mot de passe à usage unique, OTP, en fonction d'un secret préférentiellement partagé avec le serveur 2 ;
- Générer et afficher sur les moyens d'affichage 13 un code dynamique de vérification contenant au moins une information de référence représentative d'une apparence attendue dudit élément visuel (et le cas échéant au moins une donnée représentative d'un OTP et/ou une signature électronique), ledit code dynamique de vérification étant préférentiellement généré en fonction d'au moins ladite information de référence représentative d'une apparence attendue dudit élément visuel et dudit OTP généré.

[0106] Selon un quatrième aspect, est proposé le système d'authentification comprenant un serveur d'authentification 2 selon le deuxième aspect et au moins un dispositif électronique d'identité 1 (en particulier un pour chaque individu) selon le troisième aspect.

[0107] Le système peut en outre comprendre au moins un équipement client 3 (typiquement connecté au serveur 2 via le réseau 20, directement ou indirectement) comprenant des moyens d'acquisition optique 31 pour l'acquisition de ladite image représentant au moins l'élément visuel personnel de l'individu et le code dynamique de vérification visibles sur ledit dispositif électronique d'identité 1.

[0108] *Produit programme d'ordinateur*

[0109] Selon un cinquième et un sixième aspects, l'invention concerne un produit programme d'ordinateur comprenant des instructions de code pour l'exécution (en particulier sur les moyens de traitement de données 11, 21, du dispositif électronique d'identité 1 et/ou du serveur 2) d'un procédé selon le premier aspect de l'invention d'authentification d'un dispositif électronique d'identité 1, ainsi que des moyens de stockage lisibles par un équipement informatique (une mémoire 12, 22, des équipements 1, 2) sur lequel on trouve ce produit programme d'ordinateur.

Revendications

[Revendication 1] Procédé d'authentification d'un dispositif électronique d'identité (1) présenté par un individu, le procédé étant caractérisé en ce qu'il comprend la mise en œuvre d'étapes de :
(b) Réception par des moyens de de traitement de données (21) d'un serveur (2) d'une image acquise dudit dispositif électronique d'identité (1), l'image représentant au moins un élément visuel personnel de l'individu et un code dynamique de vérification visibles sur ledit dispositif électronique d'identité (1), ledit code dynamique de vérification contenant au moins une information de référence représentative d'une apparence attendue dudit élément visuel ;
(c) Extraction par analyse de ladite image acquise par les moyens de de traitement de données (21) du serveur (2) de :
- une information candidate représentative de l'apparence dudit élément visuel tel que représenté dans l'image acquise ;
- l'information de référence représentative de l'apparence attendue dudit élément visuel contenue dans ledit code dynamique de vérification tel que représenté dans l'image acquise ;
(d) Vérification par les moyens de de traitement de données (21) du serveur (2) que l'information candidate et l'information de référence extraites coïncident.

[Revendication 2] Procédé selon la revendication 1, comprenant une étape (a) d'affichage par des moyens d'affichage (13) dudit dispositif électronique d'identité (1) dudit code dynamique de vérification.

[Revendication 3] Procédé selon la revendication 2, dans lequel l'étape (a) comprend la génération préalable dudit code dynamique de vérification par des moyens de traitement de données (11) dudit dispositif électronique d'identité (1) en fonction d'au moins ladite information de référence représentative d'une apparence attendue dudit élément visuel et un mot de passe à usage unique, OTP.

[Revendication 4] Procédé selon la revendication 3, dans lequel l'étape (a) et l'étape (c) comprennent chacune la génération dudit OTP, respectivement par les moyens de traitement de données (11) du dispositif électronique d'identité (1) et les moyens de de traitement de données (21) du serveur (2), en fonction d'un secret partagé.

[Revendication 5] Procédé selon la revendication 4, dans lequel ledit mot de passe à usage unique est un mot de passe à usage unique basé sur le temps, TOTP, la

génération dudit TOTP par les moyens de traitement de données (11) du dispositif électronique d'identité (1) et les moyens de de traitement de données (21) du serveur (2) étant également fonction d'une information temporelle.

[Revendication 6] Procédé selon l'une des revendications 3 à 5, dans lequel ledit code dynamique de vérification contient également au moins une donnée descriptive dudit OTP généré par les moyens de traitement de données (11) du dispositif électronique d'identité (1), l'étape (c) comprenant également l'extraction de la donnée descriptive dudit OTP contenue dans ledit code dynamique de vérification tel que représenté dans l'image acquise, l'étape (d) comprenant également la vérification que l'OTP généré les moyens de de traitement de données (21) du serveur (2) coïncide avec ladite donnée descriptive de l'OTP extraite.

[Revendication 7] Procédé selon l'une des revendications 2 à 6, dans lequel ledit code dynamique de vérification est affiché sous la forme d'un code QR et/ou d'un code alphanumérique.

[Revendication 8] Procédé selon l'une des revendications 1 à 7, dans lequel ledit code dynamique de vérification contient également une signature électronique de ladite information de référence représentative d'une apparence attendue dudit élément visuel, l'étape (c) comprenant également l'extraction de la signature électronique contenue dans ledit code dynamique de vérification tel que représenté dans l'image acquise, l'étape (d) comprenant également la vérification que ladite signature électronique extraite est valide.

[Revendication 9] Procédé selon l'une des revendications 1 à 8, dans lequel ledit élément visuel personnel de l'individu est imprimé sur le dispositif électronique d'identité (1).

[Revendication 10] Procédé selon l'une des revendications 1 à 9, dans lequel un élément visuel visible sur ledit dispositif électronique d'identité (1) est un élément graphique, en particulier une photographie ou une signature manuscrite de l'individu, l'information de référence représentative d'une apparence attendue dudit élément graphique étant une donnée de sécurité de type Digital Photo Seal.

[Revendication 11] Procédé selon l'une des revendications 1 à 10, dans lequel un élément visuel visible sur ledit dispositif électronique d'identité (1) est un attribut alphanumérique associé à l'individu, l'information représentative d'une apparence de cet élément visuel étant la valeur ou un haché de cet attribut alphanumérique associé à l'individu.

[Revendication 12] Serveur d'authentification (2), caractérisé en ce qu'il comprend des moyens de de traitement de données (21) configurés pour :
- Recevoir une image acquise d'un dispositif électronique d'identité (1) présenté par un individu, l'image représentant au moins un élément visuel personnel de l'individu et un code dynamique de vérification visibles sur ledit dispositif électronique d'identité (1), ledit code dynamique de vérification contenant au moins une information de référence représentative d'une apparence attendue dudit élément visuel ;
- Extraire par analyse de ladite image acquise :
- une information candidate représentative de l'apparence dudit élément visuel tel que représenté dans l'image acquise ;
- l'information de référence représentative de l'apparence attendue dudit élément visuel contenue dans ledit code dynamique de vérification tel que représenté dans l'image acquise ;
- Vérifier que l'information candidate et l'information de référence extraites coïncident.

[Revendication 13] Dispositif électronique d'identité (1) d'un individu sur lequel est visible au moins un élément visuel personnel dudit individu, caractérisé en ce qu'il comprend des moyens de de traitement de données (11) configurés pour :
- Générer et afficher sur des moyens d'affichage (13) un code dynamique de vérification contenant au moins une information de référence représentative d'une apparence attendue dudit élément visuel ;

[Revendication 14] Dispositif selon la revendication 13, dans lequel les moyens de de traitement de données (11) sont en outre configurés pour générer préalablement un mot de passe à usage unique, OTP, ledit code dynamique de vérification étant généré en fonction d'au moins ladite information de référence représentative d'une apparence attendue dudit élément visuel et dudit OTP généré.

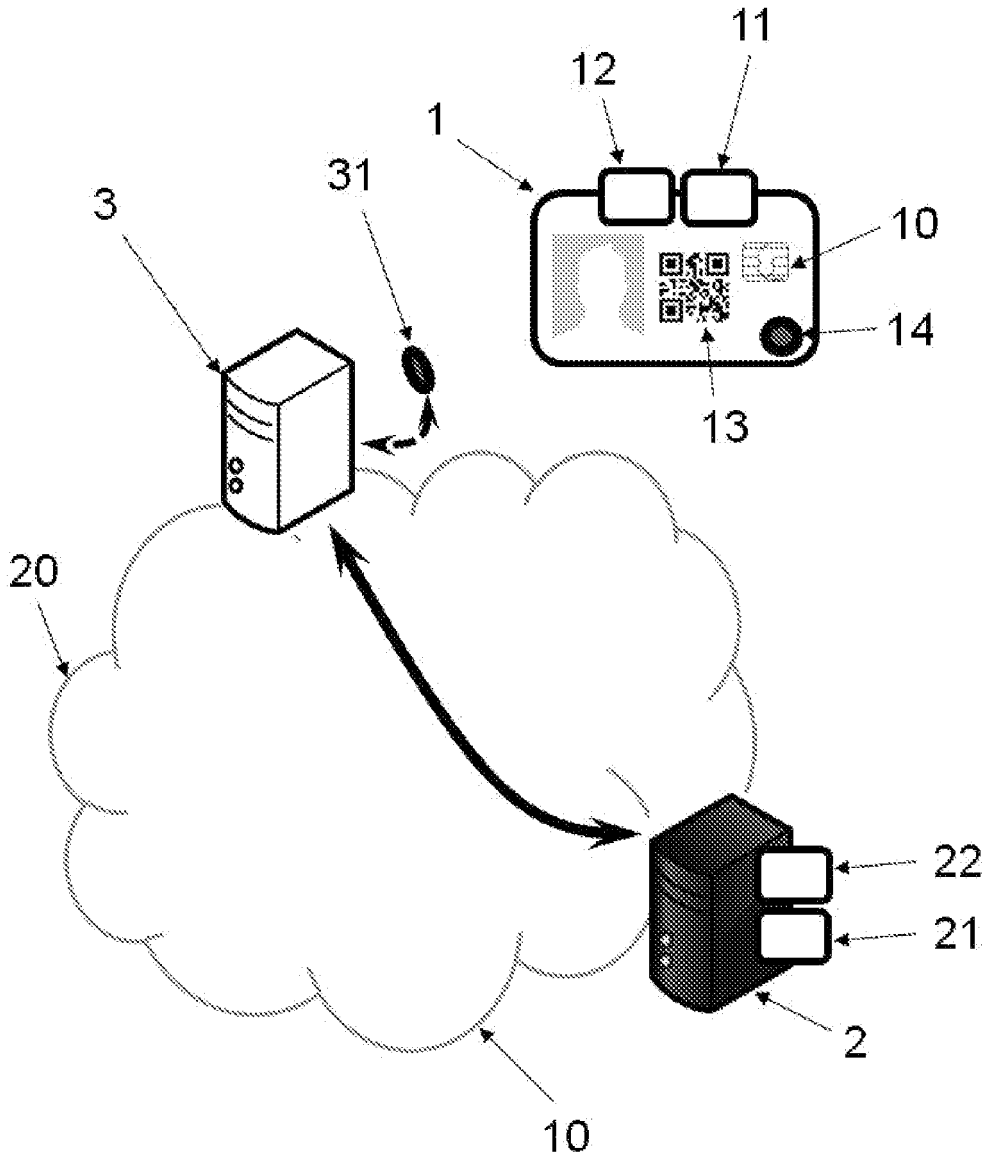
[Revendication 15] Système d'authentification comprenant un serveur d'authentification (2) selon la revendication 12, au moins un dispositif électronique d'identité (1) selon l'une des revendications 13 et 14, et au moins un équipement client (3) comprenant des moyens d'acquisition optique (31) pour l'acquisition de ladite image représentant au moins l'élément visuel personnel de l'individu et le code dynamique de vérification visibles sur ledit dispositif électronique d'identité (1).

[Revendication 16] Produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé selon l'une des revendications 1 à 11

d'authentification d'un dispositif électronique d'identité (1) présenté par un individu, lorsque ledit procédé est exécuté sur un ordinateur.

[Revendication 17] Moyen de stockage lisible par un équipement informatique sur lequel un produit programme d'ordinateur comprend des instructions de code pour l'exécution d'un procédé selon l'une des revendications 1 à 11 d'authentification d'un dispositif électronique d'identité (1) présenté par d'un individu.

[Fig. 1]



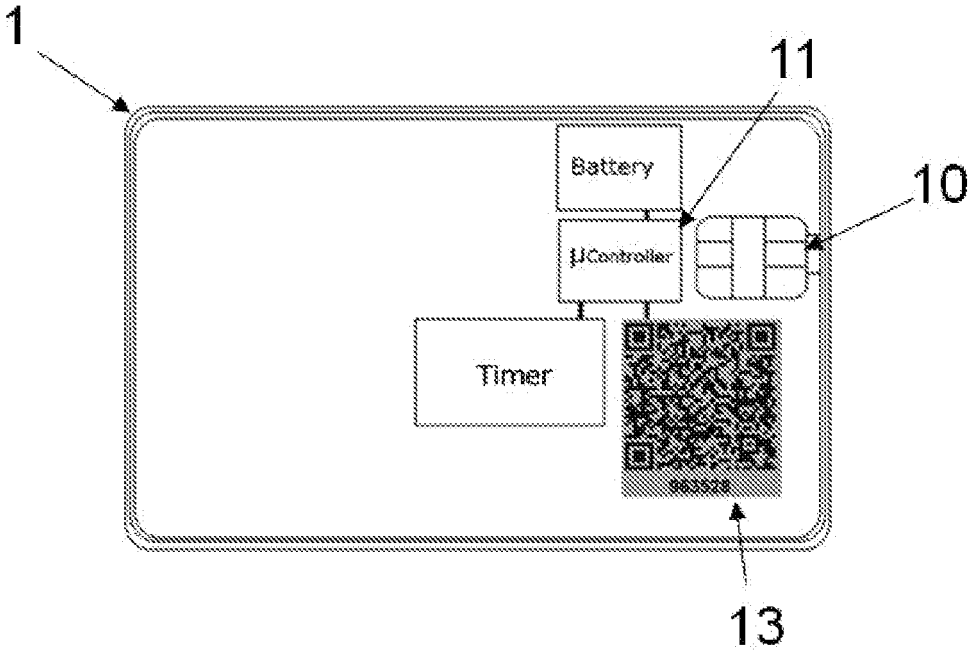
[Fig. 2a]


1
DYNAMIC IDENTITY CARD
CARTE D'IDENTITÉ DYNAMIQUE
ABROADIA
Document No./ N° du document
123456789
Date of expiry/ Date d'expiration
2025 - 02 - 02
Date of issue/ Date de délivrance
2018 - 10 - 18
Name/ Nom
Given names/ Prénoms
Nationality/ Nationalité
Reich
Date of birth/ Date de naissance
1945 - 05 - 09
Holder's signature/ Signature du titulaire
Sex/ Sexe
Male
963528

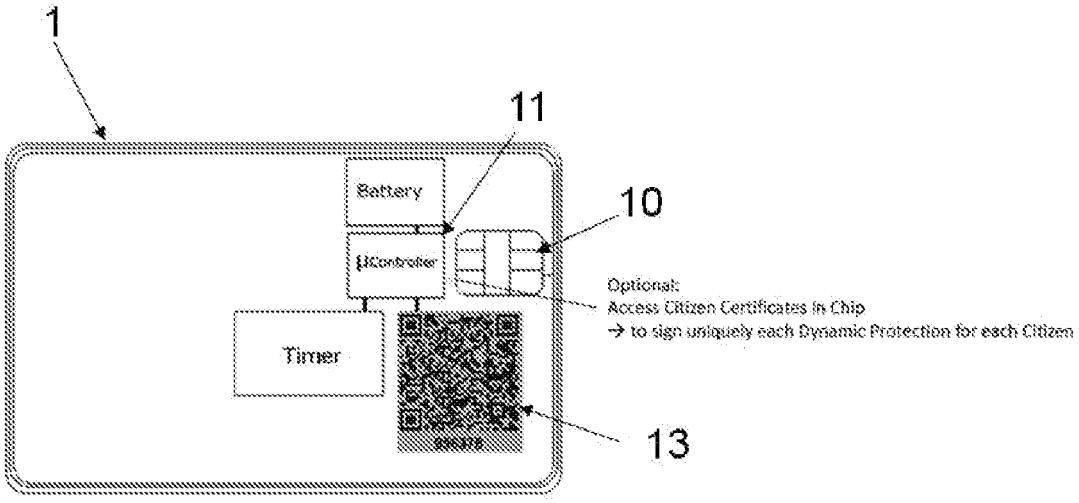
[Fig. 2b]


1
963528

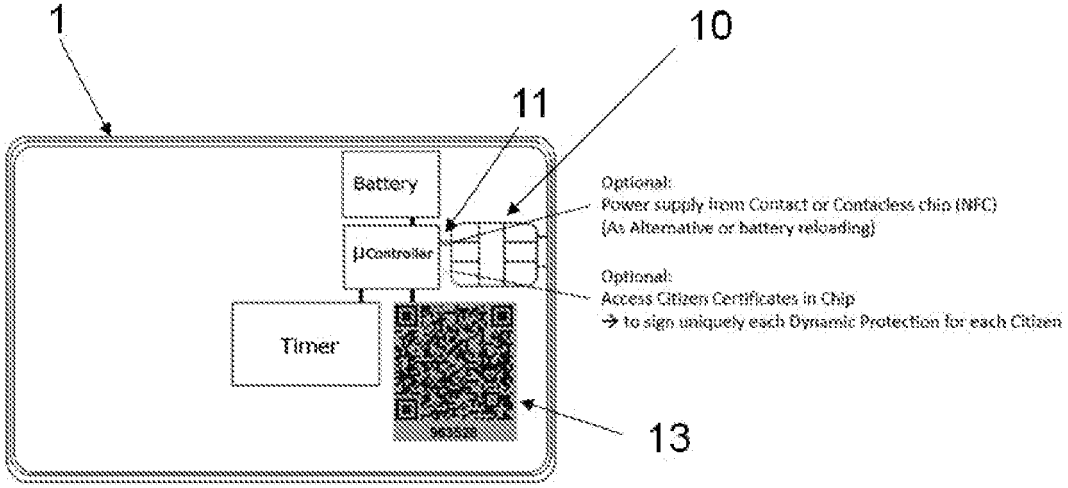
[Fig. 3a]



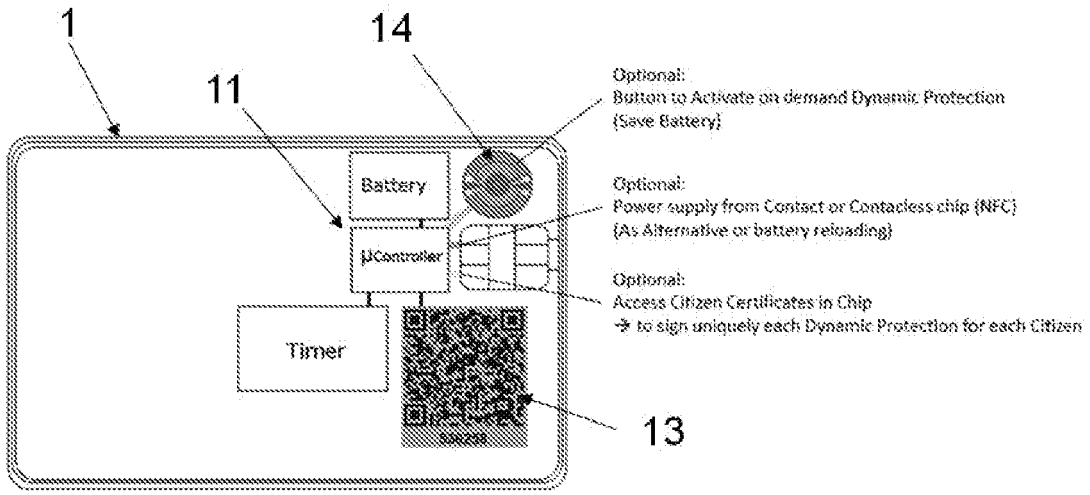
[Fig. 3b]



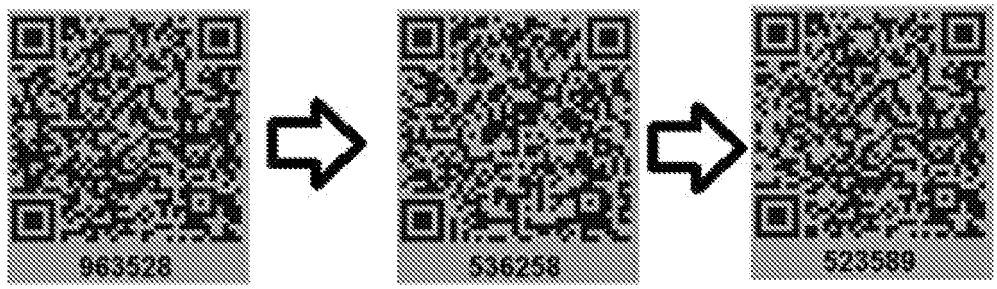
[Fig. 3c]



[Fig. 3d]


1
14
11
Optional:
Button to Activate on demand Dynamic Protection
(Save Battery)
Battery
Optional:
Power supply from Contact or Contactless chip (NFC)
(As Alternative or battery reloading)
µController
Optional:
Access Citizen Certificates in Chip
→ to sign uniquely each Dynamic Protection for each Citizen
Timer
13

[Fig. 4]


963528
536258
523589

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 865343
FR 1901001

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X,D	FR 3 038 418 A1 (OBERTHUR TECHNOLOGIES [FR]) 6 janvier 2017 (2017-01-06)	13,14	G06F21/44
Y	* page 7, ligne 20 - page 19, ligne 10 *	1-12, 15-17	

X	WO 2016/183338 A1 (DYNAMICS INC [US]; MULLEN JEFFREY D [US] ET AL.) 17 novembre 2016 (2016-11-17)	13,14	
Y	* alinéa [0021] - alinéa [0023] * * alinéa [0063] * * alinéa [0070] * * alinéa [0160] * * alinéa [0167] * * alinéa [0171] *	1-12, 15-17	

A,D	EP 3 206 192 A1 (SAFRAN IDENTITY & SECURITY [FR]) 16 août 2017 (2017-08-16) * alinéa [0022] - alinéa [0091] *	1-17	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

G06F
G07D
G07F
G06Q
G07C

Date d'achèvement de la recherche	Examinateur
14 octobre 2019	Meis, Marc

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

.....

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1901001 FA 865343

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 14-10-2019
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 3038418 A1	06-01-2017	FR 3038418 A1	06-01-2017
		WO 2017001757 A1	05-01-2017
WO 2016183338 A1	17-11-2016	AUCUN	
EP 3206192 A1	16-08-2017	AU 2017200935 A1	31-08-2017
		CA 2957774 A1	11-08-2017
		EP 3206192 A1	16-08-2017
		FR 3047688 A1	18-08-2017
		US 2017236355 A1	17-08-2017

EPO FORM P0465