

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la
Propriété Intellectuelle
Bureau international



(10) Numéro de publication internationale
WO 2019/092327 A1

(43) Date de la publication internationale
16 mai 2019 (16.05.2019)

(51) Classification internationale des brevets :

G06Q 50/26 (2012.01) H04W 12/02 (2009.01)
G09C 1/00 (2006.01) H04W 12/04 (2009.01)
H04L 9/00 (2006.01)

(21) Numéro de la demande internationale :

PCT/FR2018/000244

(22) Date de dépôt international :

09 novembre 2018 (09.11.2018)

(25) Langue de dépôt :

français

(26) Langue de publication :

français

(30) Données relatives à la priorité :

1701149 10 novembre 2017 (10.11.2017) FR

(71) Déposant : **IMPRIMERIE NATIONALE S.A.** [FR/FR] ;
104 avenue du Président Kennedy, 75016 Paris (FR).

(72) Inventeurs : **LION, Stéphanie** ; c/o Imprimerie Nationale S.A., 104 avenue du Président Kennedy, 75016 Paris (FR).
FOUTREIN, Thomas ; c/o Imprimerie Nationale S.A., 104 avenue du Président Kennedy, 75016 Paris (FR). **FLEURY, Thomas** ; c/o Imprimerie Nationale S.A., 104 avenue du Président Kennedy, 75016 Paris (FR).

(74) Mandataire : **NONNENMACHER, Bernard** ; Global Inventions, Les Portes de Rousset - Bâtiment B - 1er étage, 1200 avenue Olivier Perroy, 13790 Rousset (FR).

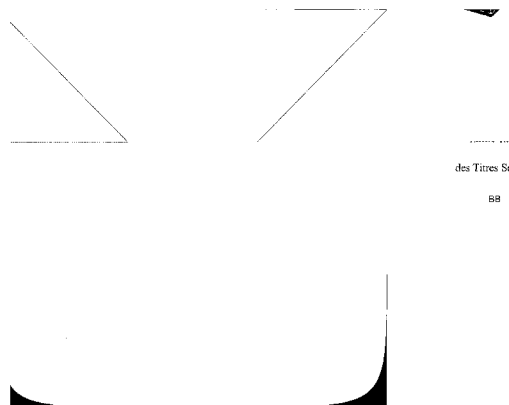
(81) États désignés (*sauf indication contraire, pour tout titre de protection nationale disponible*) : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ,

(54) Title: METHOD FOR OBTAINING A DIGITAL ID WITH A HIGH LEVEL OF SECURITY

(54) Titre : PROCÉDÉ D'OBTENTION D'UNE IDENTITÉ NUMÉRIQUE DE NIVEAU DE SÉCURITÉ ÉLEVÉ

Figure 1

AA Phase 1 : Le citoyen X demande un Passeport ou une CNI et en profite pour demander une identité numérique régalienn



AA Phase 1: Citizen X applies for a passport or national ID card and at the same time applies for a government digital ID

(57) Abstract: The invention relates to a method for creating a digital ID and making same available to a citizen, said citizen having previously transmitted personal identification information to a government agency capable of verifying this personal information and of securely transmitting same to a State-licensed industrial production site for the production of physical ID cards, characterised in that it includes steps that consist of: - creating a digital duplicate of a physical government ID card, comprising at least one digital photograph of said card; - encoding said digital duplicate in at least one QR code; - sending the citizen a URL link to a digital ID management application, as well as a code for activating his or her digital ID in said management application; - for the citizen, downloading said application onto a telephone provided with a screen capable of displaying QR codes, and activating his or her digital ID using the



WO 2019/092327 A1

EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés (*sauf indication contraire, pour tout titre de protection régionale disponible*) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

- *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17(ii))*
- *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17(iii))*

Publiée:

- *avec rapport de recherche internationale (Art. 21(3))*

received activation code, so that the citizen can display the QR codes containing his or her digital ID in encoded form.

(57) Abrégé : L'invention concerne un procédé de création et de mise à disposition d'un citoyen d'une identité numérique, ledit citoyen ayant préalablement transmis des informations personnelles d'identité à un service régalién apte à vérifier ces informations personnelles et à les transmettre de façon sécurisée à un site de production industriel agréé par un État pour la production de titres d'identité physiques, caractérisé en ce qu'il comporte des étapes consistant à: - créer un double numérique du titre régalién physique, comprenant au moins une photographie numérique dudit titre; - coder ledit double numérique dans au moins un QR Code; - transmettre au citoyen un lien url vers une application de gestion d'identités numériques, ainsi qu'un code d'activation de son identité numérique auprès de ladite application de gestion; - pour le citoyen, télécharger ladite application sur un téléphone pourvu d'un écran apte à afficher des QR Codes, et activer son identité numérique à l'aide du code d'activation reçu, de sorte que le citoyen peut afficher les QR Codes contenant son identité numérique sous forme codée.

Procédé d'obtention d'une identité numérique de niveau de sécurité élevé

L'invention concerne un procédé pour obtenir une identité numérique de niveau de sécurité substantiel ou élevé (niveau régalien), apte à être utilisée par les citoyens en particulier pour s'identifier auprès des forces de l'ordre, mais aussi dans tous types de services en face à face ou en ligne pour assurer l'identification fiable des personnes qui utilisent ces services.

Etat de la technique

10

Actuellement lorsque des agents des forces de l'ordre souhaitent contrôler l'identité d'un citoyen qui se présente physiquement à un point de contrôle, ils demandent à celui-ci de présenter une pièce d'identité (Carte Nationale d'Identité, Passeport, Titre de séjour,...). Ils peuvent alors être confrontés à l'une des problématiques suivantes :

15

- le citoyen n'a pas de document d'identité avec lui (oubli, perte,...),
- le document présenté est falsifié,
- le document présenté n'appartient pas au citoyen qui le présente.

20

Par ailleurs, dans le domaine de la sécurisation des transactions en ligne comme sur internet, les géants du Web, avec des services tels que "Facebook Connect", "Google Account", "Yahoo !ID" ou "Paypal" ont conquis des millions d'internautes. En échange d'une gestion d'identité simple mais peu sécurisée, les internautes doivent accepter d'être tracés, voire risquent d'être dépossédés de la maîtrise de leur propre identité numérique.

25

Or on peut noter qu'aujourd'hui la majorité des citoyens a plus souvent avec elle son téléphone intelligent, encore appelé "smartphone", que ses documents d'identité. La question de l'intérêt d'une dématérialisation des documents d'identité régaliens vers les smartphones peut alors se poser.

30

La problématique posée par la dématérialisation d'un document régalien vers un smartphone est de pouvoir s'assurer de l'authenticité du document numérique

présenté et des données qu'il contient (nom, prénom, date et lieu de naissance, données biométriques,...).

On sait, par exemple de par le brevet FR 2 987 464 B1 (THALES) que l'utilisation d'un ou de plusieurs QR Codes biométriques permet de créer une image, lisible par une machine, de données d'identité encodées et protégées sur un document de type carte à puce. Ce QR Code présente les caractéristiques suivantes :

- il peut contenir une image qui est une photographie de la pièce d'identité régaliennne correspondante;
- 10 - il peut contenir les données personnelles du porteur de la pièce d'identité régaliennne correspondante : nom, prénom, date et lieu de naissance, genre, taille;
- il peut contenir une ou plusieurs données biométriques caractéristiques du porteur de la pièce d'identité régaliennne correspondante : photo d'identité, caractéristiques de l'empreinte, caractéristiques de l'iris;
- 15 - il peut être chiffré pour n'être lisible que par certains dispositifs de lecture, par exemple ceux des agents assermentés;
- il peut être signé numériquement avec des algorithmes cryptographiques adéquats pour garantir l'authenticité de la source émettrice des données et l'intégrité des données contenues.
- 20

Cependant, le document cité ci-dessus ne résout pas plusieurs inconvénients. En particulier, il n'y a pas d'assurance concernant l'authenticité des données sources du porteur, ni concernant le bien fondé du lien entre ces données source et un document d'identité régalien existant. En outre, s'agissant d'un document de type carte à puce, il ne fait pas de lien avec un dispositif porté plus souvent par les utilisateurs, comme un smartphone ou un autre objet électronique portable, comme une tablette électronique ou une montre connectée.

Buts de l'invention

Un but général de l'invention est par conséquent de proposer un procédé d'obtention d'une identité numérique de niveau de sécurité substantiel ou élevé, apte à éviter les inconvénients des procédés connus.

Un but plus spécifique de l'invention est de proposer un procédé pour créer
5 une identité numérique de niveau substantiel ou élevé, équivalente au titre régalien dans sa capacité à authentifier l'identité d'une personne et efficace pour lutter contre la fraude identitaire, et en tout cas de niveau de sécurité supérieur à la sécurité des procédés d'identification numérique couramment utilisés sur internet.

Un autre but de l'invention est de proposer un procédé de création d'une
10 identité numérique forte utilisant comme support un dispositif portable usuel des utilisateurs, comme par exemple un téléphone portable pourvu d'un écran.

Principe de la solution selon l'invention

15 Il est admis dans la plupart des États que l'identification des personnes physiques ou morales est une responsabilité régaliennne: les États demeurent les garants de l'identité de leurs ressortissants. En ce sens, l'identité numérique constitue un sujet de souveraineté nationale, et il est admis qu'un « certificat électronique » émis par un organisme privé, quel qu'il soit, ne saurait égaler la
20 puissance probatoire d'une identité régaliennne.

Par conséquent, le principe de la présente invention consiste à créer un original numérique d'un titre régalien, à savoir une identité numérique construite à partir d'un titre régalien physique (carte nationale d'identité, passeport, ...), et à rendre cette identité numérique disponible sur des dispositifs électroniques mobiles,
25 tels que les smartphones des citoyens ou d'autres dispositifs électroniques portables pourvus d'un écran d'affichage, pour une utilisation dans le cadre de l'identification physique du porteur, ou de son identification électronique pour la conduite de transactions en ligne.

30 **Résumé de l'invention**

L'invention a par conséquent pour objet un procédé de création et de mise à disposition d'un citoyen d'une identité numérique, ledit citoyen ayant préalablement transmis des informations personnelles d'identité à un service régalién apte à vérifier ces informations personnelles et à les transmettre de façon sécurisée à un site de production industriel agréé par un État pour la production de titres d'identité physiques, caractérisé en ce qu'il comporte des étapes consistant à:

- créer un double numérique du titre régalién physique, comprenant au moins une photographie numérique dudit titre;

- coder ledit double numérique dans au moins un QR Code, de préférence un ensemble de QR Codes;

- transmettre au citoyen un lien url vers une application de gestion d'identités numériques, ainsi qu'un code d'activation de son identité numérique auprès de ladite application de gestion;

- pour le citoyen, télécharger ladite application de gestion sur un dispositif électronique portable pourvu d'un écran apte à afficher un QR Code, et activer son identité numérique à l'aide du code d'activation reçu, de sorte que le citoyen peut afficher le ou les QR Code(s) contenant son identité numérique sous forme codée.

De préférence, ladite photographie numérique est une photographie à haute définition.

Ledit dispositif électronique portable pourvu d'un écran d'affichage est avantageusement un smartphone, une tablette électronique, ou une montre connectée, sans que cette liste ne soit exhaustive.

Selon l'invention, les QR Codes sont soit stockés dans une base de données sécurisée, soit recalculés à la demande à partir des informations personnelles du demandeur.

Selon un mode de réalisation de l'invention, l'identité numérique comporte en plus d'une photographie numérique du titre régalién physique, des informations

administratives (nom, taille, genre, adresse, ...) et/ou biométriques du citoyen, codées dans le ou les QR Code(s).

Les informations biométriques sont par exemple constituées par un codage des empreintes digitales du citoyen, un codage de l'iris, et/ou une photographie d'identité du citoyen, sans que cette liste ne soit exhaustive.

Selon un mode de mise en œuvre du procédé, l'identité numérique du citoyen ainsi obtenue est stockée dans une base de données sécurisée, avec les données administratives et/ou biométriques du citoyen qui ont permis de produire le titre physique associé et les données propres au titre physique (numéro unique, date d'émission,...).

La base de données peut être soit gérée par un industriel agréé pour la fabrication de titres d'identité régaliens, avec une autorisation d'accès par le service régalien en charge de la gestion des demandes d'identité numérique, soit gérée directement par un État.

De préférence, les identités numériques stockées sont chiffrées avec une clé de chiffrement spécifique aux forces de l'ordre de sorte que seuls les agents des forces de l'ordre équipés de terminaux pourvus d'un lecteur de QR Code et d'une clé de déchiffrement adéquate puissent déchiffrer et lire ces données.

L'invention a également pour objet l'utilisation d'une identité numérique pour l'identification par les forces de l'ordre d'un citoyen pourvu d'un terminal portable tel qu'un smartphone dans lequel est stockée l'identité numérique sous forme codée par un ensemble de QR Code(s), caractérisée en ce qu'elle comporte des étapes consistant à:

- pour un agent des forces de l'ordre, demander la présentation d'un document d'identité régalien;

- pour le citoyen, lancer sur son smartphone une application de gestion des identités numériques et afficher les QR Codes contenant l'identité numérique;

- pour l'agent des forces de l'ordre, lire les QR Codes affichés, au moyen d'un terminal de lecture de QR Codes, et déchiffrer les QR Codes au moyen d'une

application de déchiffrement et d'une clé de déchiffrement apte à extraire des QR Codes affichés, les informations d'identification du citoyen (photographie, informations administrative, informations biométriques).

5 D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée et des dessins annexés dans lesquels :

- la figure 1 est un schéma représentant les étapes de préparation d'une identité numérique faisant suite à une demande de titre régalien par un citoyen;
- la figure 2 est un schéma représentant les étapes pour l'activation d'une
10 identité numérique obtenue telle que décrit en relation avec la figure 1;
- la figure 3 est un schéma représentant les étapes mises en œuvre dans le cadre d'un exemple d'utilisation d'une identité numérique obtenue grâce au procédé selon l'invention.

15 **Description détaillée**

On rappelle le procédé connu de délivrance en France d'un titre régalien physique seul, étant entendu que des procédés similaires existent dans la plupart des pays.

20

- 1- Le citoyen X demande un nouveau titre d'identité (Passeport, Carte Nationale d'Identité) auprès d'un représentant de l'État (par exemple en Mairie) en fournissant les documents et informations demandés, ainsi que les empreintes de ses doigts.
- 25 2- Une vérification des informations du citoyen est faite par une entité étatique (par exemple une Préfecture) avant de demander la production du titre d'identité par un industriel autorisé.
- 3- A la réception de la demande de production de la part du représentant de l'État concerné, l'industriel agréé par l'État lance la fabrication du titre à partir
30 des données transmises de façon sécurisée par l'entité étatique.

- 4- Le titre fabriqué est envoyé par l'industriel au représentant de l'État demandeur (par exemple la Mairie du domicile du citoyen).
- 5- Les informations concernant le titre (numéro de série, date d'émission,...) sont transmises à une entité étatique qui centralise et sauvegarde ce type de données, par exemple en France: l'Agence Nationale des Titres Sécurisés (ANTS).
- 6- Le citoyen est invité à venir retirer son titre régalién physique en mairie.
- 7- Lors de la remise du titre au citoyen, l'agent d'Etat vérifie qu'il est bien le demandeur initial du titre, par exemple en comparant les empreintes de la personne qui retire le titre, avec celles encodées dans le titre. Cette comparaison se fait au moyen d'un capteur d'empreintes pour obtenir les empreintes du demandeur, et un logiciel d'analyse d'empreintes qui peut indiquer si les empreintes présentées par le demandeur correspondent à celles stockées en mémoire du dispositif d'analyse.
- 8- Le titre est remis au citoyen, qui peut ensuite l'utiliser pour s'identifier auprès d'une autorité en cas de contrôle d'identité physique.

Comme on l'a vu plus haut, le citoyen n'a pas toujours le document d'identité physique avec lui, ce qui ne lui permet pas de s'identifier. En outre, le document d'identité physique ne lui permet pas de s'identifier en ligne, en particulier pour des transactions sécurisées sur internet.

Il est donc nécessaire de proposer un procédé apte à construire une identité numérique, dont la force probante soit équivalente à celle d'un document régalién physique classique.

1ère variante du procédé selon l'invention : construction d'une identité numérique en cas de production d'un titre physique

Selon une première variante de base du procédé selon l'invention, une identité numérique est construite dans la foulée de la production d'un titre d'identité physique, et remise de façon sécurisée au demandeur du titre physique.

Les étapes de ce procédé sont schématisées dans les figures 1 et 2.

1) Le citoyen X demande un nouveau titre régalien auprès d'un représentant de l'État (par exemple une Mairie) en fournissant ses informations administratives requises, à savoir nom, prénom, date et lieu de naissance, genre, adresse email, ainsi qu'un numéro de téléphone où il peut être contacté pour lui annoncer que son titre est prêt. Le processus de demande de titre est donc jusque-là très proche de celui existant à ce jour et rappelé ci-dessus. Toutes les données de la demande de titre sont enregistrées dans une base de données gérée par l'ANTS ou un organisme étatique équivalent. A la différence du procédé connu, le citoyen demande une identité numérique, en plus de la demande d'un titre régalien physique.

2) Une vérification des informations du citoyen est faite par une entité étatique (par exemple une Préfecture en France) avant de demander la production du titre et de l'identité numérique.

3) Après validation des informations, la demande de fabrication du titre physique est transmise à un industriel autorisé par l'État à produire le titre régalien.

4) A la réception de la demande de production de la part de l'entité étatique, l'industriel autorisé lance la fabrication du titre à partir des données reçues.

A la différence du procédé connu, en sortie de la ligne de fabrication du titre, l'industriel crée également un « double » numérique du titre, qui constitue une identité numérique du demandeur. Celle-ci se compose d'une photographie haute définition du titre physique et d'un QR Code (éventuellement un QR Code biométrique tel que celui décrit dans le document FR 2 987 454 A1) qui embarque une ou plusieurs informations codées, comme par exemple un codage des empreintes digitales du demandeur, de certaines caractéristiques de son visage, ou d'une photo d'identité de moindre définition obtenue à partir de la photographie en haute définition. L'identité numérique ainsi obtenue est ensuite stockée temporairement jusqu'à la délivrance du titre, dans une base de données sécurisée de l'industriel, avec les données administratives et/ou biométriques du porteur qui ont permis de produire le titre et les données propres au titre (numéro unique, date d'émission,...).

Alternativement, l'identité numérique peut être recalculée à la demande, à partir des informations du demandeur (photographie du titre physique, empreintes digitales et autres informations biométriques et administratives du demandeur) stockées dans les bases de données sécurisées.

5 Les données stockées ou recalculées peuvent être chiffrées avec une clé de chiffrement spécifique aux forces de l'ordre de sorte que seuls les agents des forces de l'ordre équipés de terminaux adéquats puissent déchiffrer et lire ces données. Les informations concernant le titre (numéro de série, date d'émission,...) sont transmises à une entité étatique, par exemple l'ANTS en France, pour mise à jour
10 de sa base de données des titres régaliens. Le titre physique fabriqué est alors envoyé au représentant de l'État demandeur (Mairie).

5) Le citoyen X est invité à venir chercher en mairie son titre physique, ainsi qu'un code d'activation de son identité numérique. Par exemple, un message SMS est envoyé au citoyen avec deux informations : l'annonce de la disponibilité de son
15 titre et un lien url vers un magasin d'applications logicielles pour smartphone, contenant une application qui lui permet de créer et de gérer un portefeuille individuel de titres régaliens numériques.

6) Le citoyen télécharge l'application de gestion de son identité numérique sur son smartphone ou équivalent.

20 7) (Figure 2) Lors de la remise effective du titre au citoyen, l'agent d'État vérifie qu'il est bien le demandeur, par exemple par comparaison des empreintes digitales comme décrit précédemment.

8) La Mairie demande à l'industriel le lien url d'activation de l'identité numérique du citoyen X.

25 En 9), le titre est remis au citoyen ainsi qu'un lien url et un code d'activation de son identité numérique. Le lien url et le code d'activation peuvent être remis sur un support papier, ou être encodés dans un QR Code. Le citoyen télécharge son identité numérique contenant son ou ses QR Code(s) biométrique(s) à l'aide du lien

url reçu, active en 10) son identité numérique avec le code d'activation qu'il a reçu, et en informe en 11) l'entité qui gère les identités numériques. A partir de là, l'identité numérique du citoyen se trouve sur son smartphone, et est exploitable pour s'authentifier physiquement auprès des autorités, ou en ligne pour l'identification substantielle ou forte auprès d'une application gouvernementale ou non.

A ce stade, le demandeur dispose donc à la fois d'un titre régalién physique, et d'une identité numérique de niveau fort ou substantiel calquée sur le titre physique. Lors de la deuxième visite du demandeur en mairie (phase 2, figure 2), l'agent a en effet vérifié que le titre numérique correspondait bien à la personne qui se présente devant lui, exactement comme pour le titre physique. Le demandeur dispose donc à ce stade de deux « originaux » de titres, l'un physique, l'autre numérique.

15 **2ème variante du procédé : construction d'une identité numérique en l'absence de demande de titre physique**

Le procédé décrit ci-dessus peut être adapté pour une demande d'Identité Numérique sans production d'un titre réel. Dans ce cas, la photographie du titre physique n'est pas prise et n'est pas intégrée aux QR Codes biométriques, néanmoins les données du porteur sont validées par l'État. Le code d'activation et le lien de téléchargement des QR Codes biométriques sont remis en main propre au citoyen lorsque celui-ci vient retirer son identité numérique.

Cette variante du procédé, non représentée dans les figures, est décrite plus en détail ci-dessous, les étapes de la première variante qui sont devenues inutiles sont éliminées.

1a - Le citoyen demande une identité numérique auprès d'un représentant de l'État (Mairie) en fournissant les documents et informations demandés et ses empreintes.

2a - Une vérification des informations du citoyen est faite par une entité étatique (Préfecture) avant de demander la production de l'identité numérique.

3a - Un QR Code biométrique est calculé à partir des données tel que décrit précédemment.

5 4a - Les informations concernant l'identité numérique (numéro de série, date d'émission,...) sont transmises à une entité étatique.

5a - Le citoyen est invité à venir chercher en mairie un code d'activation de son identité numérique.

10 6a - Lors de la remise du code d'activation au citoyen, l'agent d'État vérifie qu'il est bien le demandeur (par exemple par comparaison des empreintes).

7a - Le code d'activation de son identité numérique et le moyen de recevoir son QR Code biométrique sont remis au citoyen. Le citoyen télécharge son identité numérique et doit l'activer avec le code d'activation qu'il a reçu.

15 On décrira maintenant l'utilisation de l'identité numérique obtenue à l'aide du procédé selon l'invention, à l'aide de deux cas d'usage pris à titre d'exemples pratiques.

20 **1er cas: contrôle par les forces de police d'un document d'identité dématérialisé présenté sur un téléphone portable**

Lors d'un contrôle de police, il est demandé à une personne de montrer son titre d'identité à un agent de police :

- 25 - La personne lance alors sur son smartphone l'application logicielle permettant de gérer son identité numérique, et affiche le QR Code biométrique de son titre dématérialisé sur son smartphone, de façon à permettre le contrôle par le policier.
- 30 - Le policier approche un terminal de contrôle portable pourvu d'un lecteur de QR Code du téléphone portable du citoyen, de façon à pouvoir lire et décoder le QR Code affiché sur le téléphone du citoyen, et ainsi retrouver les données biographiques et biométriques du citoyen qui sont stockées

dans le QR Code. Cette opération de contrôle est possible en local même avec un lecteur de QR Code non connecté à un réseau, à condition que le lecteur de QR Code de l'agent possède la ou les clés de décryptage correspondant à celle(s) qui ont servi à encoder les données du citoyen dans le QR Code du smartphone.

Différents niveaux de contrôle sont donc possibles : du simple contrôle visuel d'intégrité des données sur le titre dématérialisé affiché sur l'écran du smartphone, jusqu'au contrôle plus approfondi du citoyen en exploitant ses informations biométriques.

On peut bien entendu envisager un niveau de sécurité renforcé, dans lequel le terminal de contrôle du policier est connecté à internet, et accède en temps réel à la base de données des titres dématérialisés.

2ème cas: authentification forte des internautes pour l'accès à des services en ligne

Dans ce cas de figure, schématisé en figure 3, un internaute souhaite accéder à un service en ligne, par exemple un service de e-gouvernement, un service de banque ou d'assurance en ligne, etc., en utilisant son identité numérique stockée dans son smartphone :

1) Le site internet du service lui affiche une demande d'authentification et lui indique qu'il peut s'identifier à l'aide d'une identité numérique fournie par un fournisseur d'identité d'un niveau suffisant et agréée par le service en ligne;

2) L'internaute choisit de se connecter en utilisant son identité numérique stockée dans son smartphone;

3) Une notification est alors envoyée par le service en ligne, à l'application mobile du téléphone qui gère l'identité numérique de l'internaute, et la notification informe l'internaute qu'un service web veut accéder à ses données;

4) L'internaute accepte et saisit un code de déverrouillage de son application mobile de gestion de son identité numérique, de façon que le service en ligne puisse accéder à l'identité numérique de l'internaute;

5) Les données utiles pour le service de e-gouvernement sont automatiquement partagées avec le service en ligne, de façon sécurisée, et l'internaute accède au service immédiatement.

5 **Avantages de l'invention**

L'invention atteint les buts fixés et présente un grand nombre d'avantages par rapport aux procédés connus d'obtention d'une identité numérique.

Le procédé selon l'invention est aisé à mettre en œuvre.

Du point de vue de la production d'une identité numérique, le fichier principal nécessaire à la compilation des données d'identité existe déjà, puisqu'il est utilisé pour la production de titres régaliens physiques. En outre, dans le cycle de production des titres physiques, l'industriel fabricant peut sans difficulté créer un « original numérique » en sortie de presse, au moment où il produit le titre physique. Le processus de restitution des titres aux demandeurs existe aussi : ceux-ci reçoivent déjà un message de type SMS leur annonçant la disponibilité du titre physique, il serait donc facile d'ajouter à ce SMS un lien url vers une application mobile permettant de gérer et de mettre à disposition les identités numériques.

Le titre numérique obtenu par le procédé est strictement égal au titre physique, et possède la même force probante.

Pour l'obtention de l'identité numérique, il est essentiel que l'original numérique soit dérivé de l'original physique pour plusieurs raisons :

- Par rapport à des dispositifs tels que ceux mis en place par des entreprises privées, il est beaucoup plus sécurisé : là où ces entreprises confient à un salarié non assermenté le soin de valider un titre numérique pour un client, la solution proposée par l'invention l'intègre à la procédure régaliennne d'État civil, avec des agents assermentés et disposant de moyens de contrôle renforcés.

- La solution proposée s'inscrit totalement sous le contrôle d'une entité étatique (par exemple le Ministère de l'Intérieur) qui, directement ou par délégation à un industriel, assigne le QR Code en sortie de ligne et gère la base de données des informations utilisées pour la production de titres régaliens.

Du point de vue de l'utilisation de l'identité numérique obtenue comme décrit plus haut, l'invention permet :

- de conserver les QR Codes biométriques du citoyen afin qu'il puisse les présenter sans connexion réseau à un agent des forces de l'ordre en cas de contrôle d'identité;
- d'afficher, après saisie d'un code de déverrouillage personnel, la photographie du titre original (Carte d'identité, Passeport,...)
- d'afficher, après saisie d'un code de déverrouillage personnel, un QR Code temporaire pour identifier le citoyen sur un terminal de contrôle d'un agent ou sur une borne d'accès à un lieu ou à un service;
- de s'authentifier ou s'identifier auprès d'un service en ligne par l'intermédiaire d'un fournisseur d'identité utilisant une identité numérique construite comme expliqué plus haut.

En définitive, le procédé selon l'invention est également économiquement avantageux. La généralisation d'outils permettant au grand public de prouver de façon sûre son identité aux forces de l'ordre ou à l'égard d'un service en ligne pourrait créer des gains de productivité importants, puisque derrière l'identité numérique se trouve l'identité incontestable du propriétaire de l'identité numérique, ce qui constitue la base de la confiance numérique et de la croissance des services qui y sont rattachés.

REVENDICATIONS

1 - Procédé de création et de mise à disposition d'un citoyen d'une identité numérique, ledit citoyen ayant préalablement transmis des informations personnelles d'identité à un service régalien apte à vérifier ces informations personnelles et à les transmettre de façon sécurisée à un site de production industriel agréé par un État pour la production de titres d'identité physiques, caractérisé en ce qu'il comporte des étapes consistant à:

- créer un double numérique du titre régalien physique, comprenant au moins une photographie numérique dudit titre;

- coder ledit double numérique dans au moins un QR Code ou plusieurs QR Codes;

- transmettre au citoyen un lien url vers une application de gestion d'identités numériques, ainsi qu'un code d'activation de son identité numérique auprès de ladite application de gestion;

- pour le citoyen, télécharger ladite application sur un dispositif électronique portable pourvu d'un écran apte à afficher des QR Codes, et activer son identité numérique à l'aide du code d'activation reçu, de sorte que le citoyen peut afficher les QR Codes contenant son identité numérique sous forme codée.

2 - Procédé selon la revendication 1, caractérisé en ce que ledit dispositif électronique portable est un smartphone, une tablette électronique, ou une montre connectée.

3 - Procédé selon l'une des revendications précédentes, caractérisé en ce que les QR Codes sont soit stockés dans une base de données sécurisée, soit recalculés à la demande à partir des informations personnelles du demandeur.

4 - Procédé selon l'une des revendications précédentes, caractérisé en ce que ladite photographie numérique est une photographie à haute définition.

5 - Procédé selon l'une des revendications précédentes, caractérisé en ce que l'identité numérique comporte en plus d'une photographie numérique du titre régalien physique, des informations administratives (nom, taille, genre, adresse, ...) et/ou biométriques du citoyen, codées dans les QR Codes.

5 **6** - Procédé selon la revendication 5, caractérisé en ce que les informations biométriques sont constituées par un codage des empreintes digitales du citoyen, un codage de l'iris, et/ou une photographie d'identité du citoyen.

7 - Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'identité numérique du citoyen ainsi obtenue est stockée dans
10 une base de données sécurisée, avec les données administratives et/ou biométriques du citoyen qui ont permis de produire le titre physique associé et les données propres au titre physique (numéro unique, date d'émission,...).

8 - Procédé selon la revendication 7, caractérisé en ce que la base de données sécurisée est gérée par le site industriel, avec une autorisation d'accès par
15 le service régalien en charge de la gestion des demandes d'identité numérique.

9 - Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que les identités numériques stockées sont chiffrées avec une clé de chiffrement spécifique aux forces de l'ordre de sorte que seuls les agents des forces de l'ordre équipés de terminaux pourvus d'un lecteur de QR Code et d'une
20 clé de déchiffrement puissent déchiffrer et lire ces données.

10 - Utilisation d'une identité numérique obtenue selon le procédé conforme à l'une des revendications précédentes, pour l'identification par les forces de l'ordre d'un citoyen pourvu d'un terminal portable pourvu d'un écran, tel qu'un smartphone, une tablette électronique ou une montre connectée, dans lequel est
25 stockée l'identité numérique sous forme codée dans au moins un QR Code, caractérisée en ce qu'elle comporte des étapes consistant à:

- pour un agent des forces de l'ordre, demander la présentation d'un document d'identité régalien;

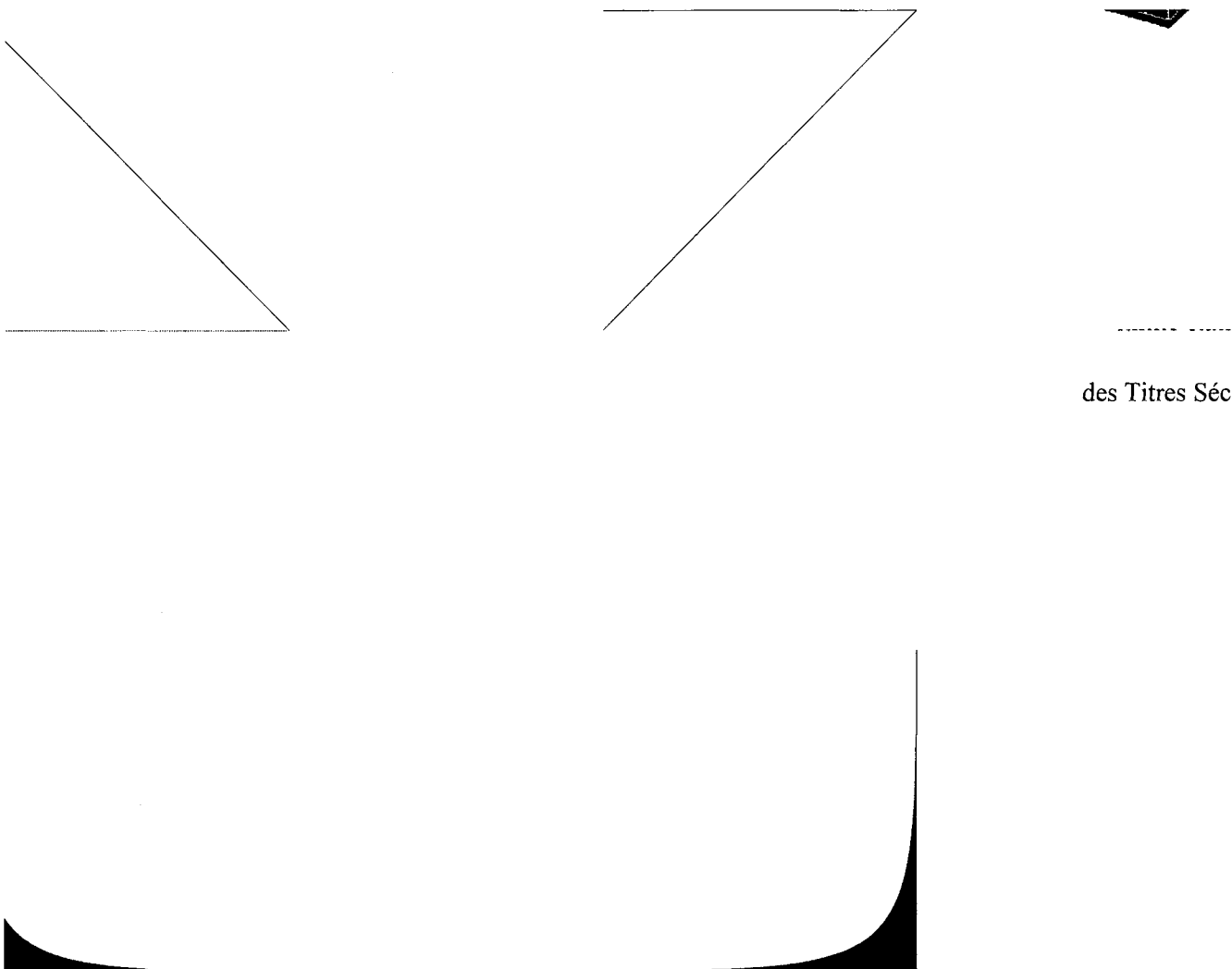
- pour le citoyen, lancer sur son terminal portable une application de gestion des identités numériques et afficher au moins un QR Code contenant l'identité numérique;

5 - pour l'agent des forces de l'ordre, lire le ou les QR Code(s) affiché(s) sur le terminal du citoyen, au moyen d'un terminal de lecture de QR Codes, et déchiffrer le ou les QR Code(s) au moyen d'une application de déchiffrement et d'une clé de déchiffrement apte à extraire des QR Codes affichés, les informations d'identification du citoyen (photographie, informations administrative, informations biométriques).

1/3

Figure 1

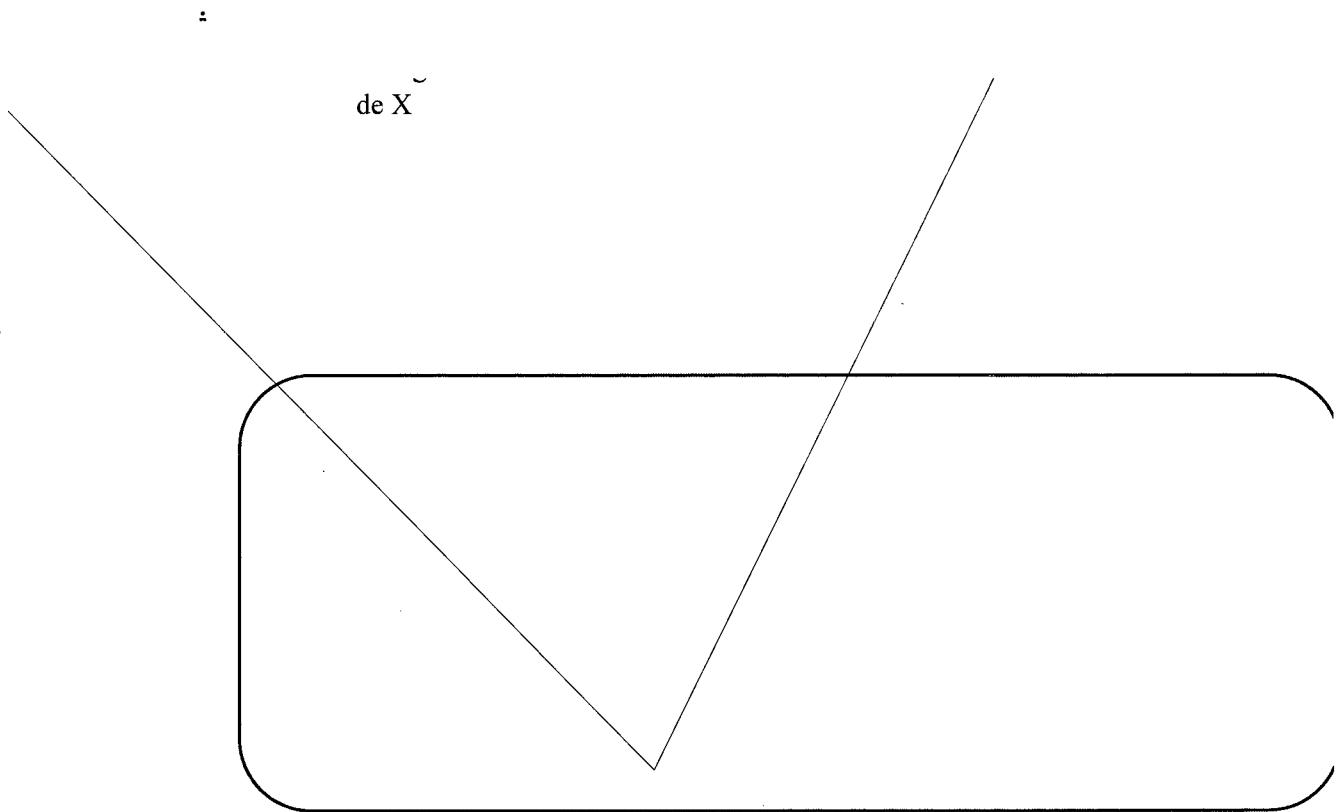
Phase 1 : Le citoyen X demande un Passeport ou une CNI et en profite pour demander une identité numérique régalienn



2/3

Figure 2

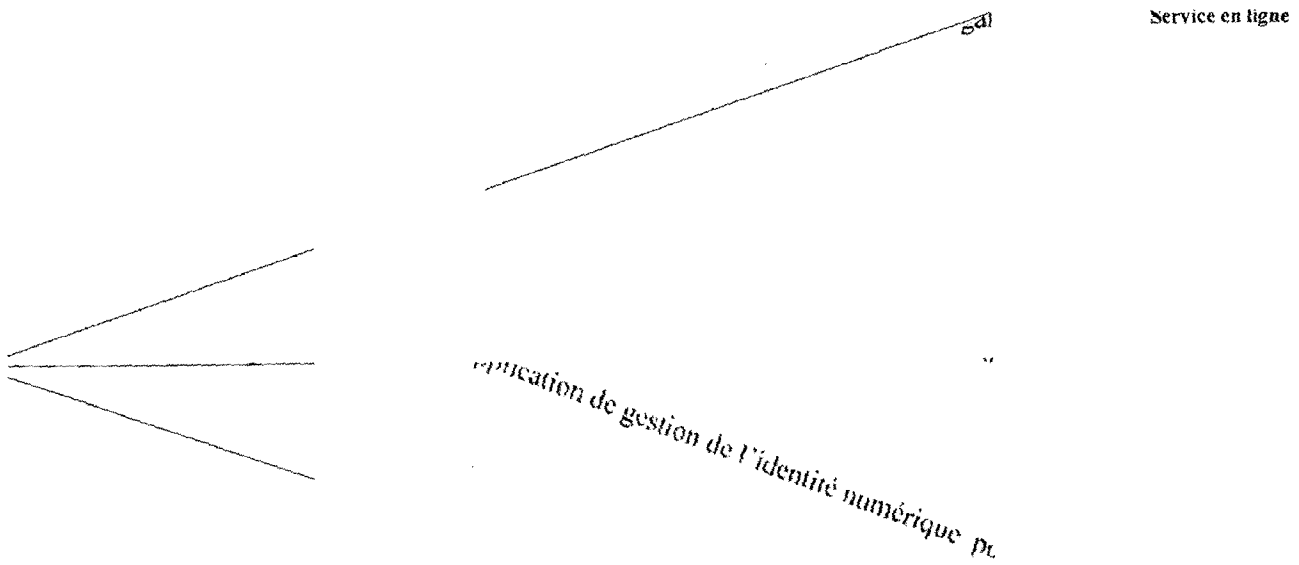
Phase 2 : Le citoyen X va chercher en mairie son titre régalien et active son identité numérique de niveau élevé



3/3

Figure 3

Authentification/Identification à un service en ligne



INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2018/000244

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q50/26 G09C1/00 H04L9/00 H04W12/02 H04W12/04
ADD.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
G06Q G09C H04L H04W
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CA 2 978 920 A1 (YE MAO [CA]) 11 June 2015 (2015-06-11) abstract paragraph [0028] - paragraph [0063] paragraph [0084] - paragraph [0102] -----	1-10
A	KR 2009 0110660 A (KT CORP [KR]) 22 October 2009 (2009-10-22) abstract paragraph [0005] - paragraph [0038] figures 1-3 -----	1-10
A	WO 2017/111521 A2 (HAN MIJUNG [KR]) 29 June 2017 (2017-06-29) abstract paragraph [0025] - paragraph [0045] figures 1, 5 -----	1-10
	-/--	

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search 15 February 2019	Date of mailing of the international search report 25/02/2019
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Bertolissi, Edy

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2018/000244

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003/023858 A1 (BANERJEE DWIP N [US] ET AL) 30 January 2003 (2003-01-30) abstract paragraph [0049] - paragraph [0052] figure 6 -----	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FR2018/000244

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CA 2978920	A1	11-06-2015	CA 2978920 A1
			EP 3174240 A1
			US 2017169422 A1
			WO 2015081899 A1

KR 20090110660	A	22-10-2009	NONE

WO 2017111521	A2	29-06-2017	KR 101685161 B1
			SG 11201805396T A
			WO 2017111521 A2

US 2003023858	A1	30-01-2003	NONE

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>US 2003/023858 A1 (BANERJEE DWIP N [US] ET AL) 30 janvier 2003 (2003-01-30) abrégé alinéa [0049] - alinéa [0052] figure 6</p> <p style="text-align: center;">-----</p>	1-10

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2018/000244

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
CA 2978920	A1	11-06-2015	CA 2978920 A1 11-06-2015
			EP 3174240 A1 31-05-2017
			US 2017169422 A1 15-06-2017
			WO 2015081899 A1 11-06-2015

KR 20090110660	A	22-10-2009	AUCUN

WO 2017111521	A2	29-06-2017	KR 101685161 B1 09-12-2016
			SG 11201805396T A 30-07-2018
			WO 2017111521 A2 29-06-2017

US 2003023858	A1	30-01-2003	AUCUN
