(19) RÉPUBLIQUE FRANÇAISE

**INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE**

COURBEVOIE

(11) **N° de publication :** ***3 064 778***

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

(21) **N° d'enregistrement national :** **18 52730**

(51) Int Cl[8] : ***G 06 F 21/31*** *(2017.01), G 06 F 3/048, G 06 K 9/62*

# (12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 29.03.18.

(30) **Priorité :** 29.03.17 IT 10201700003457.

(43) **Date de mise à la disposition du public de la demande :** 05.10.18 Bulletin 18/40.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

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

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

(71) **Demandeur(s) :** *ALIASLAB S.P.A.* — IT.

(72) **Inventeur(s) :** BUELLONI GIANLUCA et MAGAGNOTTI ROMEO.

(73) **Titulaire(s) :** ALIASLAB S.P.A..

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

## (54) METHODE D'IDENTIFICATION A DISTANCE POUR LA SIGNATURE D'UN DOCUMENT ELECTRONIQUE.

(57) Méthode d'identification à distance pour la signature d'un document électronique, ladite méthode comprenant les étapes suivantes : première acquisition d'au moins une première photographie au moins du recto d'un document d'identité d'un utilisateur sur lequel figure le visage dudit utilisateur ; deuxième acquisition d'une deuxième photographie qui prend en même temps le visage dudit utilisateur et ledit recto dudit document d'identité ; ensuite, première comparaison entre le visage reproduit sur ledit recto dudit document d'identité pris au moyen de ladite première photographie et le visage de l'utilisateur acquis au moyen de ladite deuxième photographie afin de vérifier leur coïncidence ; dans laquelle ladite méthode est exécutée au moyen d'une application (App) installée sur un appareil portable dudit utilisateur connecté à Internet.

FR 3 064 778 - A1

# "MÉTHODE D'IDENTIFICATION À DISTANCE POUR LA SIGNATURE D'UN DOCUMENT ÉLECTRONIQUE"

## Revendication de priorité

La présente demande revendique la priorité de la demande de brevet italien n° 102017000034573, déposée le 29 mars 2017, dont le contenu est incorporé ici par référence.

## Domaine d'application de l'invention

La présente invention concerne une méthode et une infrastructure matérielle/logicielle associée pour identifier un utilisateur dans le cadre d'une signature d'au moins un document électronique.

## État de la technique

On sait qu'un document d'identité comporte une image du visage de l'individu concerné, en plus d'autres détails tels que le nom et le prénom, la date de naissance et autres.

L'accès à des services télématiques peut être autorisé de différentes manières plus ou moins fiables du point de vue de la pertinence du service proposé.

Les services télématiques ayant une importance majeure sont assurément la banque en ligne et la signature électronique de documents, étant donné que, dans le premier cas, il est possible de transférer des sommes d'argent à distance et sans la supervision d'un opérateur humain, tandis que, dans le second cas,

il est possible de signer des documents de toute nature en apposant une signature électronique dont la validité est au moins équivalente à celle d'une signature apposée à la main.

Il est donc essentiel de pouvoir reconnaître correctement l'utilisateur qui souscrit le service.

La plupart du temps, l'utilisateur doit se rendre dans un bureau prédéterminé où un opérateur humain peut vérifier l'identité dudit utilisateur avant d'activer son accès à un service télématique.

Il existe des méthodes de vérification qui se basent sur des certificats électroniques attribués à un utilisateur. Mais même dans ce cas, ladite attribution de certificat nécessite que l'utilisateur se rende dans un bureau prédéterminé et se fasse reconnaître *de visu* en ayant sur lui un document d'identité en cours de validité.

## Résumé de l'invention

La présente invention a pour but de présenter une méthode de souscription d'un service télématique qui permet une reconnaissance robuste de l'utilisateur souscripteur sans que celui-ci doive se rendre physiquement dans un bureau pour être reconnu *de visu* par un opérateur.

L'idée sous-jacente à la présente invention est de baser la reconnaissance sur l'utilisation d'un smartphone adéquatement doté d'une App qui permet d'acquérir, par une procédure guidée, au moins une première photographie du recto d'un document

d'identité de l'utilisateur en cours de validité et une deuxième photographie qui prend en même temps le visage de l'utilisateur souscripteur et au moins le recto du document d'identité le concernant.

Ensuite la première photographie est comparée à la deuxième photographie pour vérifier que le visage qui figure dans le document d'identité coïncide avec le visage de l'utilisateur acquis avec la deuxième photographie.

De manière avantageuse, ceci rend extrêmement compliquée la contrefaçon du document d'identité reproduit dans les deux images capturées.

De préférence, la comparaison s'effectue entre la première photographie et une partie de la deuxième photographie dans laquelle le recto du document d'identité est capturé, pour vérifier que le document d'identité coïncide entre la première et la deuxième photographie. Ceci renforce encore plus la vérification de la coïncidence entre les visages représentés, accroissant ainsi la robustesse de la méthode, surtout lorsque celle-ci est mise en œuvre de manière automatique.

En effet, le visage de l'utilisateur est présent deux fois dans la deuxième photographie : il est présent suite à son acquisition directe et suite à l'acquisition indirecte de sa reproduction dans le document d'identité correspondant.

La double acquisition permet d'obtenir en outre une haute définition du document d'identité acquis seul afin de pouvoir

acquérir facilement, avec la première photographie, les détails qui figurent sur ledit document d'identité.

De manière avantageuse, dans la mesure où le visage de l'utilisateur est certainement plus grand que le document d'identité correspondant, la résolution de l'image du visage de l'utilisateur est suffisamment élevée pour permettre une comparaison efficace avec la représentation du visage de l'utilisateur reproduite dans le document d'identité et acquise avec la première photographie et, en même temps, contrefaire l'image du visage de l'utilisateur devient compliqué puisque celui-ci le présente lors de la deuxième prise de photographie.

Selon une variante préférée de l'invention, l'une au moins des première et/ou deuxième comparaisons précitées est effectuée à distance par un opérateur préposé à cet effet.

Selon une autre variante préférée de l'invention, qui peut être combinée avec la précédente, l'une au moins des première et/ou deuxième comparaisons précitées s'effectue automatiquement au moyen de modules logiciels biométriques en soi connus.

La mise en œuvre de modules logiciels biométriques capables d'effectuer de manière autonome les comparaisons précitées n'exclut pas la possibilité de prévoir une procédure de supervision par un opérateur humain.

De préférence, il devient possible, au moyen d'autres logiciels d'OCR (reconnaissance optique de caractères) en soi connus,

d'acquérir une ou plusieurs des informations qui figurent sur le document d'identité en employant des caractères alphanumériques.

Selon une autre variante préférée de l'invention, un appel vocal est également mis en œuvre au moyen dudit smartphone dans le cadre de la procédure précitée.

Une fois que l'utilisateur a été reconnu, la procédure peut comprendre :

- La signature électronique d'un document électronique au moyen d'une signature numérique qualifiée, le certificat de signature étant détenu par une autorité de certification tierce,
- La signature électronique d'un document électronique au moyen d'une signature électronique avancée, une paire de clés publique/privée étant associée à l'App de l'utilisateur. Cette paire peut être détenue localement par l'App et débloquée (c'est-à-dire activée) à l'occasion de la signature d'un document électronique par la saisie d'un code secret et/ou d'un mot de passe et/ou d'une donnée biométrique par l'utilisateur ; à la fin de la signature, une copie du document signé est transmise à l'organisme, qui en conserve une copie ; ou
- la signature électronique d'un document électronique au moyen d'une signature électronique avancée, l'utilisateur fournissant une donnée biométrique propre ou un code secret ou un mot de passe qui lui permet de s'authentifier auprès de

la plateforme, tandis que la plateforme a un certificat de signature détenu physiquement par une autorité de certification tierce. La procédure de signature électronique demandée par l'utilisateur prévoit que l'utilisateur active la signature électronique en saisissant ledit code secret, mot de passe ou donnée biométrique propre dans l'App, laquelle le transfère à la plateforme ou au site web de la plateforme. La plateforme introduit à son tour ladite donnée biométrique ou ledit code secret/mot de passe dans le document électronique à signer et l'envoie à l'autorité de certification tierce afin de procéder à la signature électronique dudit document. Pour finir, l'autorité de certification tierce renvoie le document électronique signé à l'organisme et ledit organisme en transmet une copie à l'utilisateur concerné.

Selon une variante préférée de l'invention, un appel vocal est également passé par la plateforme ou par le smartphone pour vérifier la véracité de certaines données fournies ou acquises précédemment par l'utilisateur, de préférence pour acquérir des échantillons de la voix de l'utilisateur.

La présente invention concerne une méthode d'identification à distance pour la signature d'un document électronique, selon la revendication 1.

La présente invention concerne également un module logiciel, mettant en œuvre l'App précitée, destiné à être installé sur un smartphone d'un utilisateur souscripteur dudit service.

Un autre objet de la présente invention est une plateforme matérielle/logicielle qui est spécifiquement programmée pour exécuter la méthode précitée.

Les revendications décrivent des variantes préférées de l'invention et elles font partie intégrante de la présente description.

Brève description des dessins

D'autres buts et avantages de la présente invention ressortiront clairement de la description détaillée ci-après d'un exemple de réalisation de ladite invention (et de ses variantes) et des dessins d'accompagnement joints à titre purement explicatif et non limitatif, sur lesquels :

La figure 1 est une représentation schématique d'une plateforme matérielle/logicielle montrant l'interaction entre la plateforme et un utilisateur et un organisme impliqués selon la présente invention ;

La figure 2 indique toutes les alternatives possibles d'une méthode de signature d'un document électronique qui prévoit au moins deux processus différents d'identification d'un utilisateur (A1 - A4 / B1 - B4) et quelques variantes du processus de signature électronique commun à certaines étapes (C1, C2).

Les séquences des blocs A1 - A4 et B1 - B4 peuvent se substituer l'une à l'autre, de même que les séquences E1 - E6, F1 - F3 et G1, G2 peuvent se substituer l'une à l'autre.

Sur les figures, les mêmes numéros et les mêmes lettres de repère désignent les mêmes éléments ou composants.

Dans la présente description, le terme "deuxième" composant n'implique pas la présence d'un "premier" composant. En effet, ces termes sont utilisés uniquement par souci de clarté et ils ne doivent pas être compris de manière limitative.

Description détaillée d'exemples de réalisation

Un utilisateur est celui qui demande à bénéficier d'un service de souscription à un service pour lequel la signature objet de la présente invention est demandée.

Le terme organisme désigne une banque ou un organisme en général ou une autorité offrant le service de signature d'un document électronique selon la présente invention.

Le processus décrit dans la présente invention peut être exécuté autant de fois qu'il y a de documents à signer ou il peut être exécuté une seule fois pour obtenir une association entre l'App de l'utilisateur et une clé cryptographique privée de signature.

L'expression service de signature désigne un service fourni par l'organisme au moyen d'une infrastructure matérielle/ logicielle gérée par l'organisme.

L'infrastructure comprend :

- une App - une application logicielle - à charger sur un smartphone ou une tablette de l'utilisateur,
- un site WEB de l'organisme,
- une plateforme comprenant un ou plusieurs serveurs informatiques aptes à définir ce que l'on appelle l'hébergement du site web et à gérer une communication avec ladite App.

De préférence, ladite plateforme est capable non seulement de communiquer avec ladite App par l'Internet, mais aussi elle comprend au moins un canal phonique pour permettre la réception d'appels téléphoniques par un smartphone mettant en œuvre ladite App.

L'organisme peut travailler en cloud pour le compte d'un autre organisme permettant de signer un contrat de fourniture entre l'utilisateur et ledit autre organisme.

L'infrastructure peut être mieux comprise en se référant à la figure 1.

Il est fait référence à un smartphone dans la suite du texte mais il est possible d'employer n'importe quel appareil portable disponible équivalent à celui-ci, de préférence appartenant à l'utilisateur.

Au lieu d'un smartphone, l'utilisateur peut donc utiliser une tablette ou un pc, ou éventuellement un téléviseur Smart TV s'il est doté des fonctionnalités adéquates de connexion à Internet et d'installation de l'App précitée de l'infrastructure.

L'App peut donc être développée de manière à pouvoir être installée commodément dans l'appareil (à la disposition) de l'utilisateur et effectuer les opérations de la présente méthode.

De préférence, grâce à une procédure guidée, l'App guide l'utilisateur en vue d'acquérir une image du document d'identité de l'utilisateur (étape 1) depuis le côté qui comporte la reproduction du visage du sujet identifié par ledit document d'identité.

L'App guide l'utilisateur pour acquérir une image globale de son visage et de son document d'identité depuis le côté qui comporte la reproduction de son visage (étape 2).

De préférence, pendant l'acquisition des images au moyen du smartphone, l'App affiche une ou plusieurs zones de guidage dans lesquelles les sujets enregistrés doivent être centrés, à savoir le document d'identité ou le document d'identité et le visage de l'utilisateur.

L'ordre d'acquisition desdites au moins deux images est indifférent.

Selon une variante préférée de l'invention, l'App demande aussi l'acquisition d'une troisième image relative au second côté - ou verso - du document d'identité. Dans ce cas également, l'ordre d'acquisition est sans importance. L'App peut demander ensuite de photographier d'autres documents, par exemple le permis de conduire ou la carte d'assurance maladie.

L'App communique en outre avec la plateforme dans les phases de reconnaissance de l'utilisateur en transférant les images acquises et en effectuant le cas échéant un prétraitement desdites images. Dans la suite du texte, les termes images et photographies sont utilisés comme des synonymes.

À titre d'exemple, les données relatives à l'utilisateur qui figurent sur ledit document d'identité peuvent être acquises et reconnues automatiquement par l'App, laquelle les intègre automatiquement dans des champs correspondants d'un formulaire. Lesdites données peuvent être ensuite chargées dans un modèle de document qui définit un contrat de fourniture d'un service nécessitant une acceptation et une signature de la part de l'utilisateur.

En variante, ces informations sont extraites par la plateforme, qui se charge de les intégrer dans ledit formulaire et de les envoyer à l'App, déjà compilées, afin de poursuivre la procédure de signature. Bien entendu, les images doivent avoir été transférées précédemment à la plateforme par l'App.

Un exemple préféré de réalisation de l'invention est décrit ci-après à l'aide de l'organigramme de la figure 2, qui décrit les alternatives possibles précitées :

A1. L'utilisateur accède au moyen de son smartphone au site web de l'organisme et remplit un formulaire de signature en y saisissant ses propres données personnelles, dont son numéro de

téléphone portable et/ou son adresse mail et, facultativement, ses données d'état civil ;

A2. La page web indique au smartphone de l'utilisateur de télécharger et installer l'App ;

A3. En suivant la procédure guidée affichée par l'App, l'utilisateur photographie au moins son document d'identité, par exemple sa carte d'identité ou son passeport ou son permis de conduire et aussi, le cas échéant, la carte de code fiscal/CNS, et il effectue ce que l'on appelle un selfie de son visage tout en maintenant le document d'identité près de son visage avec le recto, c'est-à-dire le côté où figure la reproduction de son visage, tourné vers l'objectif du smartphone ; il est tout à fait équivalent de se photographier par le biais d'un miroir.

De préférence, pendant ces prises de photographies, l'App effectue ce que l'on appelle le tracking (repérage) du visage et du ou des documents dans le champ, selon une technique en soi connue, afin d'obtenir une photo optimale, au point, pour identifier l'utilisateur ; de préférence, l'App empêche aussi tout téléchargement montant depuis la mémoire de masse de l'appareil. En effet, l'acquisition des images est gérée exclusivement par la mémoire volatile dans laquelle ladite App est chargée. De manière avantageuse, ceci rend encore plus difficile la contrefaçon des images acquises.

A4. Envoi des images acquises à la plateforme, laquelle les traite à l'étape C1 suivante, par exemple en effectuant une comparaison

biométrique des caractéristiques physiques du visage de l'utilisateur (deuxième image) avec celles qui figurent dans la reproduction du visage dudit utilisateur à partir du document d'identité (première image) ; de préférence, on effectue également une comparaison entre les caractéristiques physiques reproduites à la fois par la première et par la deuxième image à partir du même document d'identité, pour les raisons décrites ci-dessus.

Selon une autre variante préférée de l'invention, il est prévu que les données qui figurent sur le document d'identité, acquises avec la première image, soient lues par l'App par OCR. Les étapes de ladite variante préférée, décrites également sur la figure 2, sont les suivantes :

B1. L'utilisateur télécharge et accède à l'App de l'organisme, par exemple en la recherchant sur le marché via Google® ou des équivalents d'autres producteurs.

B2. L'étape A3 précitée est exécutée.

B3. L'App scanne et reconnaît les données qui figurent dans la première image acquise et le cas échéant dans les suivantes, les documents par OCR, et remplit de manière autonome un formulaire de souscription avec les données alphanumériques provenant de ces images ou, en variante,

B3 bis. L'étape A4 précitée est exécutée et la plateforme traite les images par OCR et remplit de manière autonome un formulaire avec les données alphanumériques reconnues à partir de ces images, puis elle envoie le formulaire pré-rempli à l'App ;

B4. Facultativement, après que la plateforme a transmis ledit formulaire à l'App, le formulaire est rendu disponible dans l'App en mode de modification afin de pouvoir corriger le cas échéant des erreurs de reconnaissance.

Quelle que soit la variante du processus de reconnaissance de l'utilisateur, les étapes suivantes, décrites sur la figure 2, sont exécutées :

C1. La plateforme acquiert les images envoyées par l'App à l'étape A4 (et B4) et permet d'effectuer la comparaison biométrique précitée entre les caractéristiques physiques du visage de l'utilisateur (deuxième image) et celles qui figurent dans la reproduction du visage dudit utilisateur à partir du recto du document d'identité (première image) (étape 3) et, de préférence, elle permet aussi de comparer les caractéristiques physiques reproduites à la fois par la première et par la deuxième image à partir du même document d'identité (étape 4), pour les raisons décrites ci-dessus. Lorsque la comparaison est faite par un opérateur humain, la plateforme présente les images précitées à un opérateur humain connecté à ladite plateforme afin de les comparer, ou bien une ou les deux comparaisons précitées sont effectuées automatiquement au moyen d'un logiciel d'analyse biométrique en soi connu.

Le cas échéant, la comparaison humaine est effectuée si le logiciel de comparaison automatique a rencontré des problèmes.

Les deux comparaisons, automatique et humaine, peuvent donc être effectuées.

Facultativement, les sous-étapes suivantes sont également effectuées :

- vérification si l'utilisateur est déjà enregistré et, si oui, détermination de l'identifiant correspondant ;
- vérification de la lisibilité des images chargées ;
- comparaison entre les données saisies dans le portail et celles qui figurent dans les documents d'identité chargés, uniquement pour la première variante A1 – A4 ;
- vérification dans une base de données officielle de la validité du document d'identité utilisé pendant les prises de vues précitées ;

C2. Facultativement, selon les deux variantes A1 – A4/B1 – B4, l'utilisateur reçoit un appel vocal ; ou bien l'App lance automatiquement un appel vocal vers/depuis un service téléphonique connecté à la plateforme.

Un opérateur humain ou une voix de synthèse fait à l'utilisateur des demandes inhérentes aux données acquises dans les étapes A1 – A4/B1 – B4 précitées, en effectuant une vérification croisée de l'identité.

Il est à noter que le logiciel capable de reconnaître le parler est en soi connu, par conséquent cette vérification croisée, encore une fois, peut se faire automatiquement comme par le biais d'un opérateur humain ; de préférence, l'appel est enregistré et

des échantillons vocaux sont conservés par l'organisme conjointement avec les données acquises par l'utilisateur en même temps que les images précitées pendant la reconnaissance de l'utilisateur.

Si le résultat des vérifications précitées est positif, deux macroscénarios sont alors envisagés :

- On effectue une signature qualifiée d'au moins un document électronique, ce qui implique donc également une autorité de certification tierce.
- On fournit un service de signature électronique avancée et, par conséquent, ledit organisme représente une autorité de certification.

Si on se trouve dans le premier cas, les étapes suivantes sont effectuées, comme le montre la figure 2 :

E1. La plateforme demande à une autorité de certification tierce de générer un certificat numérique qualifié pour l'utilisateur et envoie à l'autorité un contrat, accepté au préalable par l'utilisateur par le biais de l'App ou du site web de l'organisme, de fourniture d'un service de signature qualifiée par l'organisme à l'utilisateur ;

E2. L'autorité pourvoit à signer ledit contrat de fourniture avec le certificat de l'utilisateur ; elle envoie une copie du contrat signé à l'organisme en même temps qu'un code secret/mot de passe de déblocage ; l'autorité transfère le certificat dans un dispositif matériel appelé HSM (acronyme de Hardware Security

Module), en soi connu et détenu par ladite autorité de certification tierce.

E3. L'organisme transmet à son tour à l'utilisateur ce qu'il a reçu de l'autorité ;

E4. Lorsque l'utilisateur souhaite signer un document électronique, il le transfère à la plateforme en même temps que le code secret/mot de passe de déblocage du certificat résident dans le HSM et la plateforme transfère le tout à l'autorité de certification tierce ;

E5. L'autorité tierce procède à la signature avec le certificat de l'utilisateur du document électronique et le renvoie signé à l'organisme.

E6. Comme à l'étape E3, l'organisme transfère à son tour à l'utilisateur ce qu'il a reçu de l'autorité.

Dans le second cas, la paire de clés publique/privée peut être générée par l'App, laquelle envoie uniquement la clé publique à la plateforme, ou la paire est générée par la plateforme et détenue par elle pour effectuer de la même manière ce que l'on a vu ci-dessus. Si la paire est générée par l'App, un document électronique est signé localement par l'App et envoyé signé à la plateforme, laquelle en conserve une copie ; si la paire est générée par la plateforme, les clés sont détenues par la plateforme comme ci-dessus dans le cas de l'autorité tierce et la signature du document électronique se fait au niveau de la plateforme et le code secret/mot de passe de déblocage doit être

saisi au cas par cas dans l'App du smartphone de l'utilisateur qui demande la signature dudit document électronique.

On comprend que dans ce second cas, l'organisme fait office d'autorité de certification et fournit seulement le service de signature électronique avancée.

Dans le détail, ainsi que décrit sur la figure 2 :

F1. L'App génère une ou plusieurs paires de clés publiques/privées et les sauvegarde localement, validant leur utilisation uniquement si l'utilisateur saisit un code secret/mot de passe spécifique correspondant ;

F2. L'App envoie à la plateforme la clé publique ou une donnée imputable de manière univoque à la clé publique, par exemple le hashtag de la clé publique.

F3. Lorsque l'utilisateur veut signer un document électronique, il le fait localement depuis l'App en saisissant le code secret/mot de passe de déblocage et une copie du document signé est envoyée à la plateforme.

En variante, lorsque la plateforme possède un certificat auprès d'une autorité de certification tierce :

G1. Lorsque l'utilisateur veut signer un document électronique, il envoie à la plateforme une donnée biométrique ou un code secret/mot de passe à partir de l'App ou du site de l'organisme.

G2. La plateforme intègre cette donnée dans le document électronique ou le code secret/mot de passe et demande à

l'autorité de certification tierce de le signer avec son propre certificat.

De manière avantageuse, l'utilisateur est ainsi autorisé à signer n'importe quel document électronique par le biais du site web de l'organisme ou au moyen de l'App.

Il va de soi que l'utilisation de la méthode B1 - B4, qui ne fait pas usage du site web rattaché à la plateforme, n'exclut pas que la signature d'un document électronique puisse se faire par la suite par le biais dudit site web rattaché à la plateforme.

Dans tous les cas, pour pouvoir valider la signature, il est nécessaire que l'utilisateur possède le code secret/mot de passe de déblocage du certificat ou de la clé privée. Ledit code secret/mot de passe peut être envoyé à l'utilisateur par SMS, de préférence après la vérification téléphonique précitée, ou il peut être affiché par l'App ou par le site web de l'organisme à la fin de la phase d'identification et d'enregistrement (étapes A1 - A4/B1 - B4) et ensuite annulé, ou il peut être choisi par ledit utilisateur et mémorisé localement, c'est-à-dire dans l'App, si la signature numérique se fait localement, ou par la plateforme si la signature numérique se fait au niveau de la plateforme.

Suivant ce qui est décrit ci-dessus, l'infrastructure matérielle/logicielle objet de la présente invention comprend :

- une plateforme distante, comprenant un ou plusieurs serveurs, qui propose facultativement un site web pour effectuer l'enregistrement de l'utilisateur (étapes A1 - A4) et qui

permet aussi le cas échéant la signature électronique qualifiée et/ou avancée ;

- un appareil portable à l'usage privé de l'utilisateur, doté de l'App précitée : il peut s'agir d'un smartphone ou d'une tablette ou d'un pc en liaison télématique avec ladite plateforme ;
- facultativement, une autorité de certification tierce en liaison télématique avec ladite plateforme.

Facultativement, la plateforme peut être dotée d'un canal vocal pour effectuer la vérification facultative des données concernant l'utilisateur et l'échantillonnage de la voix de l'utilisateur ainsi que décrit ci-dessus. La figure 1 peut aider à comprendre ladite structure.

De manière avantageuse, la présente invention peut être réalisée au moyen d'un programme pour ordinateur qui comprend des moyens de codage pour exécuter une ou plusieurs étapes de la méthode lorsque ledit programme est exécuté sur un ordinateur. Par conséquent, il reste entendu que l'étendue de la protection englobe ledit programme pour ordinateur et en outre des moyens lisibles par un ordinateur qui comprennent un message enregistré, lesdits moyens lisibles par un ordinateur comprenant des moyens de codage de programme pour exécuter une ou plusieurs étapes de la méthode lorsque ledit programme est exécuté sur un ordinateur.

Des variantes de réalisation de l'exemple non limitatif décrit sont possibles, sans pour autant sortir de l'étendue de protection

de la présente invention, comprenant toutes les réalisations équivalentes pour une personne du métier.

À partir de la description ci-dessus, la personne du métier est en mesure de réaliser l'objet de l'invention sans y introduire de détails constructifs supplémentaires. Les caractéristiques et les éléments illustrés dans les différents modes de réalisation préférés, y compris les dessins, peuvent être combinés les uns avec les autres sans pour autant sortir de l'étendue de protection de la présente demande. Ce qui a été décrit au chapitre concernant l'état de la technique vise uniquement à mieux comprendre l'invention et ne constitue pas une déclaration d'existence de ce qui est décrit. En outre, sauf exclusion spécifiquement mentionnée dans la description détaillée, ce qui est décrit au chapitre sur l'état de la technique doit être considéré comme faisant partie intégrante de ladite description détaillée.

## REVENDICATIONS

**1.** Méthode d'identification à distance par la signature d'un document électronique, ladite méthode comprenant les étapes suivantes :

- première acquisition d'au moins une première photographie d'au moins le recto d'un document d'identité d'un utilisateur où figure le visage dudit utilisateur ;
- deuxième acquisition d'une deuxième photographie qui prend en même temps le visage dudit utilisateur et ledit recto dudit document d'identité ;
- ensuite, première comparaison entre le visage figurant sur ledit recto dudit document d'identité pris au moyen de ladite première photographie et le visage de l'utilisateur acquis au moyen de ladite deuxième photographie afin de vérifier leur coïncidence ;

au moins lesdites première et deuxième acquisitions étant effectuées au moyen d'une App (application logicielle) installée dans un appareil portable dudit utilisateur connecté à Internet.

**2.** Méthode selon la revendication 1, comprenant en outre une étape de réalisation d'une deuxième comparaison avant, pendant ou après ladite première comparaison entre le visage qui figure au recto dudit document d'identité pris au moyen de ladite première photographie et le visage pris au recto dudit document d'identité pris au moyen de ladite deuxième photographie.

**3.** Méthode selon l'une quelconque des revendications précédentes, dans laquelle lesdites comparaisons sont effectuées à distance :

- au moyen d'une plateforme matérielle/logicielle connectée audit appareil portable via Internet et comprenant un logiciel d'analyse et de comparaison de caractéristiques physiques ;
- au moyen d'une plateforme matérielle/logicielle connectée audit appareil portable via Internet et configurée pour afficher à l'écran, simultanément, lesdites première et seconde photographies afin de faire effectuer lesdites comparaisons par un opérateur humain.

**4.** Méthode selon l'une quelconque des revendications précédentes, exécutée au moyen d'une infrastructure matérielle/logicielle qui comprend une plateforme distante, formée par un ou plusieurs serveurs, qui propose un site web pour effectuer ladite identification à distance de l'utilisateur, ledit appareil portable de l'utilisateur communiquant via Internet avec ladite plateforme ; la méthode comprenant les étapes suivantes :

- (A1.) L'utilisateur accède audit site web et remplit un formulaire de signature en y saisissant les données personnelles correspondantes, parmi lesquelles son numéro de téléphone portable et/ou son adresse mail et, facultativement, ses données d'état civil ;
- (A2.) Ladite page web invite à télécharger et installer ladite App ;

- (A3.) L'utilisateur acquiert lesdites première et deuxième photographies au moyen de ladite App ;

- (A4.) Les photographies acquises sont envoyées à la plateforme ;

- (C1.) Ladite plateforme traite lesdites première et deuxième photographies pour exécuter ladite première et aussi, le cas échéant, ladite deuxième comparaison.

**5.** Méthode selon l'une quelconque des revendications 1 à 3 précédentes, exécutée au moyen d'une infrastructure matérielle/ logicielle qui comprend une plateforme distante formée d'un ou plusieurs serveurs, ledit appareil portable de l'utilisateur communiquant via Internet avec ladite plateforme ; la méthode comprenant les étapes suivantes :

- (B1.) Téléchargement et installation de ladite App sur ledit appareil portable ;

- (B2.) Acquisition par l'utilisateur desdites première et deuxième photographies au moyen de ladite App ;

- (B3.) Scannage et reconnaissance par ladite App des données qui figurent dans la première image acquise et le cas échéant les autres images au moyen d'un logiciel de reconnaissance automatique de caractères (OCR) et remplissage automatique d'un formulaire de signature avec les données alphanumériques reconnues ou, en variante,

- (B3 bis.) Envoi desdites première et deuxième photographies à ladite plateforme ; et scannage et reconnaissance par ladite

plateforme des données figurant dans la première image acquise et le cas échéant dans les autres images au moyen d'un logiciel de reconnaissance automatique de caractères (OCR) et remplissage automatique d'un formulaire de signature avec les données alphanumériques reconnues ;

- (B4.) Facultativement, reprise dudit formulaire précédemment rempli dans ladite App afin de pouvoir corriger manuellement ledit formulaire ;

- (C1.) Traitement par ladite plateforme desdites première et deuxième photographies afin d'exécuter ladite première et aussi, le cas échéant, ladite deuxième comparaison.

**6.** Méthode selon l'une des revendications 4 ou 5, comprenant en outre les étapes suivantes :

- (C2.) Passation entre ledit appareil portable et ladite plateforme d'un appel vocal pendant lequel un opérateur humain ou une voix de synthèse fait à l'utilisateur certaines demandes inhérentes aux données acquises précédemment et dans lequel des échantillons vocaux de l'utilisateur sont acquis et mémorisés par ladite plateforme.

**7.** Méthode de signature d'un document électronique, comprenant une identification à distance d'un utilisateur selon l'une quelconque des revendications 1 à 6.

**8.** Méthode selon la revendication 7, comprenant en outre une étape de signature d'un document électronique approuvé par ledit utilisateur précédemment identifié au moyen d'un certificat fourni à ladite plateforme par une autorité de certification tierce, ou une étape de génération d'une paire de clés publique/privée dans laquelle ladite clé privée est détenue par ladite App ou par ladite plateforme et dans laquelle une signature électronique dudit document électronique est effectuée au moyen d'une saisie d'un code secret/mot de passe de déblocage respectivement dans ladite App ou dans ledit site web proposé par ladite plateforme.

**9.** Programme d'ordinateur qui comprend des moyens de codage de programme aptes à réaliser toutes les étapes des revendications 1 à 8 lorsqu'on fait tourner ledit programme sur un ordinateur.

**10.** Architecture matérielle/logicielle comprenant une plateforme matérielle/logicielle connectée à un appareil portable via Internet et dans laquelle ledit appareil portable est configuré pour exécuter au moins toutes les étapes de la revendication 1 et facultativement celles de la revendication 2, et dans laquelle ladite plateforme est configurée pour coopérer avec ledit appareil portable pour exécuter toutes les étapes correspondantes des revendications 3 ou 4.

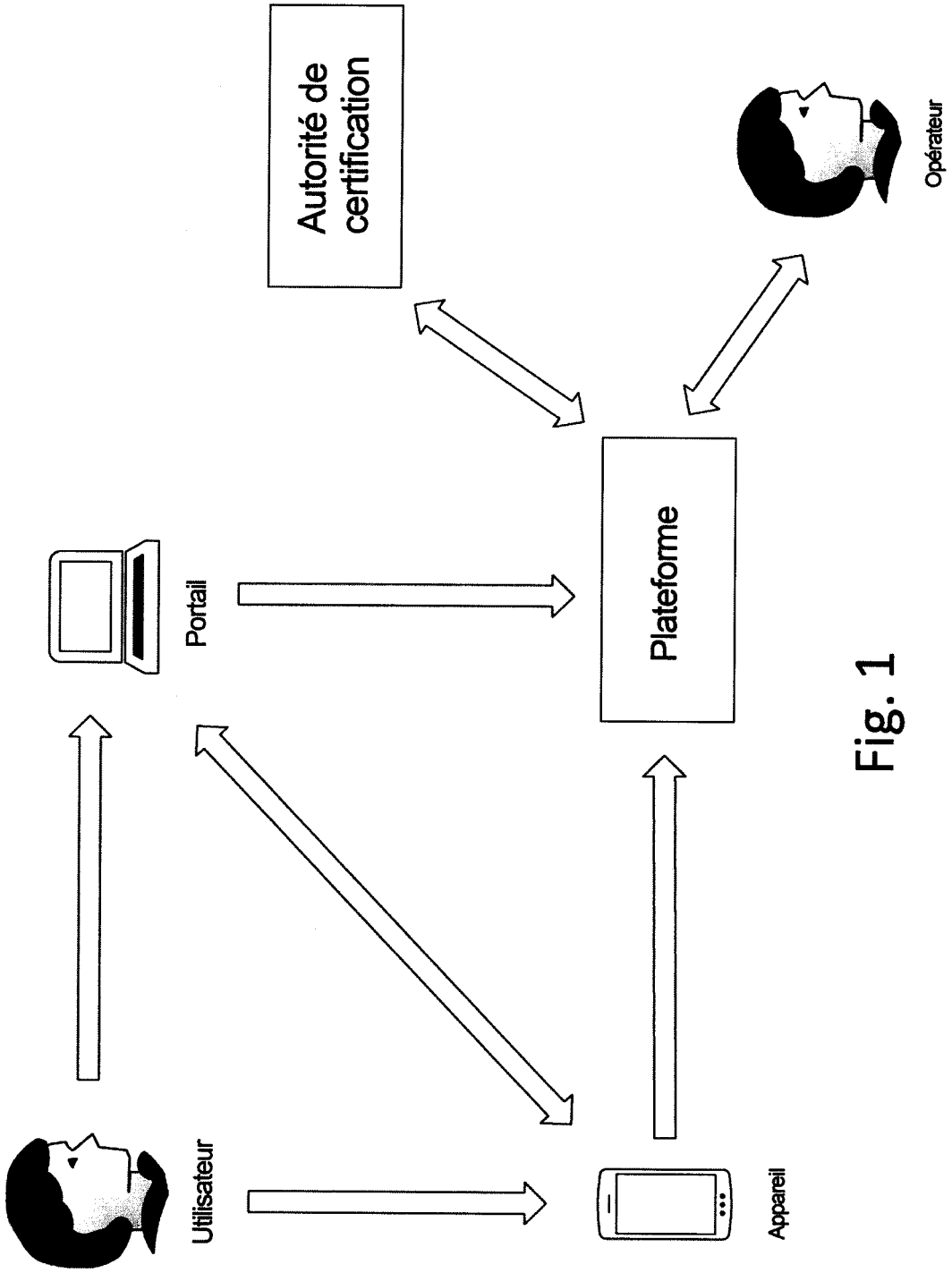
Autorité de certification
Opérateur
Plateforme
Portail
Utilisateur
Appareil

Fig. 1

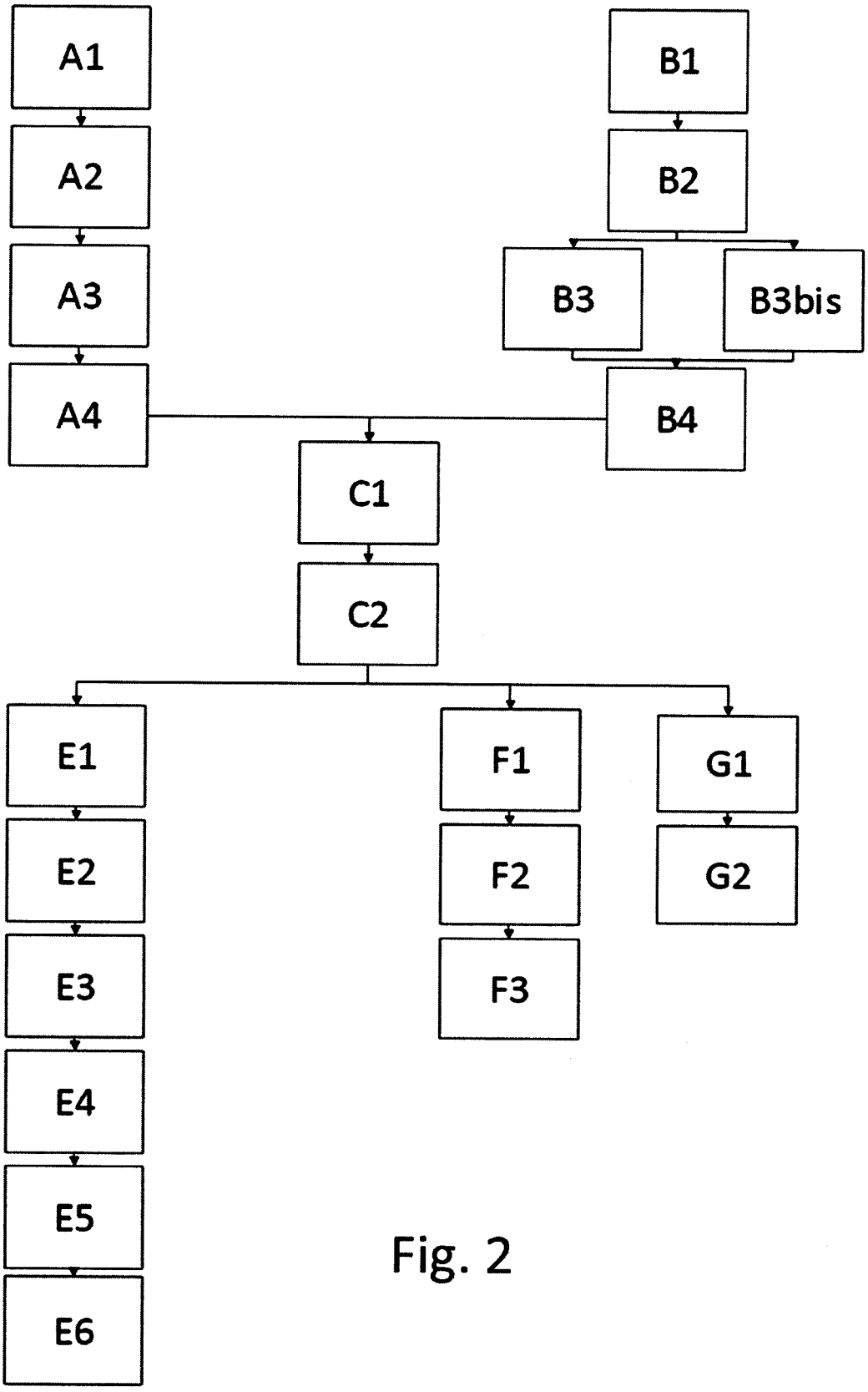


Fig. 2