ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية
المكتب المغربي للملكية الصناعية و التجارية

(12) **BREVET D'INVENTION**

(11) N° de publication :
MA 45510 A1

(43) Date de publication :
28.10.2020

(51) Cl. internationale :
H04L 29/06; H04L 63/126; H04L 63/123

(21) N° Dépôt :
45510

(22) Date de Dépôt :
08.04.2019

(71) Demandeur(s) :
BRAHIM CHAOUI, 134 BD ZERKTOUNI 5EME ETAGE CASABLANCA (MA)

(72) Inventeur(s) :
BRAHIM CHAOUI

(54) Titre : **DISPOSITIF INFORMATIQUE D'AUTHENTIFICATION ELECTRONIQUE DE SÉCURISATION, DE CONFIRMATION ET D'AUTHENTIFICATION D'UN CONTENU TEXTUEL INDIVIDUALISE**

(57) Abrégé : Ensemble de dispositifs imbriqués visant à :- Démocratiser l'authentlflcation de documents importants normés avec ou sans photo (carte d'identité, passeport, diplôme...),·ou non normés (rapport, jugement, contrat, notification...) et cela sur simple Smartphone avec une connexion ordinaire. En levant par des solutions techniques les contraintes techniques tel que la confidentialité des données et le risque de vol de la base de donnée à travers le piratage} la démocratisation de l'authentification devient envisageable;- Empêcher à 100% les attaques informatiques extérieures affectant la base de donnée servant à l'authentification à travers un dispositif primaire et simple. La solution réside dans le fait que la base d'authentification est mise sur un serveur déconnecté de toute forme de connexion connu et la demande d'authentification arrive à se serveur à travers un moyen de communication primaire et elle en ressort aussi à travers ce moyen de communication. cette transmission de donnée est réalisé à l'aide de technique ne permettant pas d'avoir la main sur la machine, tel que l'affichage sur écran (exemple planche de dessin 2/2) par un serveur émettant des données qui sont mises chacune dans un emplacement précis et un logiciel spécial sur le serveur réceptionnant lit les données à partir d'une photo prise par une caméra} ou autre système de reconnaissance} après son passage sur un logiciel de reconnaissance de caractère. Le même système peut être fait par impression par un premier serveur et la réalisation d'un scan par un deuxième serveur. Stockage dans la base précédente} de simples empreintes de données ne permettant pas la. reconstitution des données en cas de leur vol} chose qui est tout à fait contraire au cryptage- Les empreintes peuvent être obtenus à travers des modèles inspirés de la géométrie et de la physique et dans cet état d'esprit l'empreinte peut correspondre aux coordonnées lombaires d'un point ou d'une courbe} chose qui ne peut permettre d'obtenir

les données d'un simple point;- Confirmation électronique de l'approbation d'un acte par ses signataires en utilisant des codes et leur délivrés par des autorités public après lavérlflcatlon de l'identité des signataires;- Peut être combiné avec d'autre techniques tei que le PAPIER POSTAL et permettre d'avoir des actes physique totalement protégé à un niveau très élevé de sécurité contre la falsification d'acte et l'usurpation d'identité.

MA 45510A1

"E-AUTHENTIFICATION"
(DISPOSITIF INFORMATIQUE DE SECURISATION, DE CONFIRMATION ET D'AUTHENTIFICATION D'UN CONTENU TEXTUEL INDIVIDUALISE)

DESCRIPTION ABREGE

Ensemble de dispositifs imbriqués visant à :

- Démocratiser l'authentification de documents importants normés avec ou sans photo *(carte d'identité, passeport, diplôme...),* ou non normés *(rapport, jugement, contrat, notification...)* et cela sur simple Smartphone avec une connexion ordinaire. En levant par des solutions techniques les contraintes techniques tel que la confidentialité des données et le risque de vol de la base de donnée à travers le piratage, la démocratisation de l'authentification devient envisageable ;
- Empêcher à 100% les attaques informatiques extérieures affectant la base de donnée servant à l'authentification à travers un dispositif primaire et simple. La solution réside dans le fait que la base d'authentification est mise sur un serveur déconnecté de toute forme de connexion connu et la demande d'authentification arrive à se serveur à travers un moyen de communication primaire et elle en ressort aussi à travers ce moyen de communication. cette transmission de donnée est réalisé à l'aide de technique ne permettant pas d'avoir la main sur la machine, tel que l'affichage sur écran *(exemple planche de dessin 2/2)* par un serveur émettant des données qui sont mises chacune dans un emplacement précis et un logiciel spécial sur le serveur réceptionnant lit les données à partir d'une photo prise par une caméra, ou autre système de reconnaissance, après son passage sur un logiciel de reconnaissance de caractère. Le même système peut être fait par impression par un premier serveur et la réalisation d'un scan par un deuxième serveur.
- Stockage dans la base précédente, de simples empreintes de données ne permettant pas la reconstitution des données en cas de leur vol, chose qui est tout à fait contraire au cryptage - Les empreintes peuvent être obtenus à travers des modèles inspirés de la géométrie et de la physique et dans cet état d'esprit l'empreinte peut correspondre aux coordonnées lombaires d'un point ou d'une courbe, chose qui ne peut permettre d'obtenir les données d'un simple point ;
- Confirmation électronique de l'approbation d'un acte par ses signataires en utilisant des codes et leur délivrés par des autorités public après la vérification de l'identité des signataires ;
- Peut être combiné avec d'autre techniques tel que le PAPIER POSTAL et permettre d'avoir des actes physique totalement protégé à un niveau très élevé de sécurité contre la falsification d'acte et l'usurpation d'identité.

MA 45510A1

"E-AUTHENTIFICATION"
(DISPOSITIF INFORMATIQUE DE SECURISATION, DE CONFIRMATION ET D'AUTHENTIFICATION D'UN CONTENU TEXTUEL INDIVIDUALISE)

La présente invention vise principalement, pour toute sorte de document, électronique ou imprimé, ayant un contenu textuel individualisé associé éventuellement à une photo, un ensemble de dispositifs imbriqués visant à :

1. Démocratiser l'authentification, rapide et simple, de documents importants *(carte d'identité, passeport, diplôme...)*, soit sur simple Smartphone ou autre matériel et cela à travers une connexion ordinaire ou soit sur automate...

2. Empêcher à 100% les attaques informatiques extérieures affectant la base de donnée servant à l'authentification

3. Stockage dans la base précédente, d'empreintes de données ne permettant pas la reconstitution des données en cas de vol

4. Eviter l'usurpation d'identité à travers la confirmation électronique de l'approbation d'un acte par ses signataires en utilisant des codes fournit pas une ou des autorité(s) publique(s) après vérification de l'identité,

A travers ces dispositifs ont peut permettre par exemple à un employeur potentiel de vérifier l'authenticité des diplômes inscrits sur un CV d'un postulant (*pour éviter l'emploi d'un employé présentant des diplômes falsifiés*) ou encore par exemple permettre à un notaire de vérifier l'authenticité d'un document d'identité d'un vendeur d'un bien immobilier (*pour éviter les cas de spoliation foncière*)....

Pour éviter la re-saisie des données, il sera préférable que les documents normés officiels à vérifier puisse contenir un code QR contenant des informations normées. Dans ce cadre, la personne souhaitant vérifier les données prend une photo du code QR et les informations seront repris automatiquement sur une application et cette personne se devra de vérifier l'adéquation des informations saisies automatiquement avec ceux portées sur le document officiel et puis par la suite demander l'authentification, après éventuellement paiement des droits. Après avoir obtenu les informations de ce code QR par lecture, des applications peuvent permettre par la suite d'obtenir ce même code QR et le convertir par la suite en fichier image, chose qui permettra à un postulant pour un travail par exemple de joindre ces images (des codes QR relatifs à ces diplômes) dans son CV et ainsi permettre aux employeurs potentiels de vérifier préalablement leur authenticité.

Les documents visés ci-dessus à titre non limitatifs sont :

1. *A titre principal : Documents normés*

- Les documents officiels contenant éventuellement une photo tel que les cartes nationales d'identité, les passeports, les livrets de famille, les permis de conduire, les permis de chasse ou de pêche... ;

- Les cartes particulières tel que le badge de police ou les cartes des organismes professionnels... ;

- Les titres de propriété des immeubles, bateaux ou avions.., abrégé de contrat de vente ;

- Les diplômes, les titres honorifiques, les récompenses de concours, les attestations... ;

- Les actes et attestations importantes pouvant être normé tel acte de mariage, autorisation, agrément, attestations... ;

2. *A titre subsidiaire : documents non normés*

- Les contrats ou conventions sous seing privé, authentiques ou autre, fait en papier normal, en papier spécial ou en document électronique tel que : statuts, procès-verbaux, contrats de travail, contrats de vente immobilier, les divers documents des marchés ou des appels d'offre publics ou privés, les différents documents bancaires ou d'assurance, les factures, les reçus, les quittances, les différents documents délivrés par les entités publiques ou entités privées tel que les attestations, déclarations, mains levée, les comptes rendus, les rapports, les requêtes, les notifications, les demandes, les réclamations, les déclarations, les conventions officielles, les jugements, les demandes de brevets d'invention, les PV de police, les notifications des contrôles fiscaux ou sociaux et les réponses à ses notifications, les déclarations fiscales, les états comptables, les rapports d'expertise, les rapports des Commissaires Aux Comptes.... ;

La présente invention peut être utilisée simultanément avec les techniques dites «PAPIER POSTAL» et/ou «TECHNIQUE D'IMPRESSION GARANTISSANT L'INTEGRITE D'UN CONTENU IMPRIME - AMELIORE» . Cela permettra de combiner la garantie à 100% de l'intégrité en nombre de page avec la double garantie (*physique et électronique*) de l'intégrité du contenu et la garantie de la non usurpation d'identité. On obtiendra ainsi des actes non normés protégés à un niveau très élevé jamais égalé contre l'ensemble des risques pouvant être affecté par falsification ou par usurpation d'identité.

****

CONTEXTE ET ETAT DE LA TECHNIQUE

Les documents officiels tel que les cartes nationales d'identité peuvent être vérifiés à travers un système à la disposition uniquement de la police et le ministère de l'intérieur. Dans ce sens un professionnel ou une personne du grand public n'a pas accès à ce genre de base de donnée et l'institution étatique possédant la base de donnée la protège et elle ne peut pas la communiquer à une autre institution. Le grand public y compris les professionnels n'ont pas comment vérifier l'authenticité des carte nationales d'identité et autres documents d'identité et se suffisent à l'appréciation qu'ils se font du document.

Par exemple : Un notaire (*qui peut être une personne profane en matière de détection de la falsification*) vérifie pour un vendeur d'un bien immobilier, premièrement le nom et prénom inscrits sur le titre de propriété et l'attestation de propriété délivré par la conservation foncière, s'ils coïncident avec les mêmes données personnelles inscrites sur la carte d'identité nationale et deuxièmement si la personne qui se présente chez lui ressemble à la photo mise sur la carte d'identité. Une personne mal intentionnée maîtrisant les techniques de falsification est capable de changer la photo de la carte d'identité réelle volée du véritable propriétaire ou de créer une fausse carte d'identité nationale portant la photo du spoliateur foncier et mentionnant les données personnelles du réel propriétaire, dont l'identité a été usurpée.

Le risque d'infection par des virus ou le risque d'attaque des bases de données sont très grand en cas d'ouverture de la consultation de certaines bases de données aux professionnels ou le grand public. De crainte pour ces bases de données contenant des données personnelles sensibles, chaque institution n'est pas en meure d'autoriser la consultation de ces bases par des professionnels ou le grand public et de ce fait elle interdit à tous même les autres institutions ou organismes officiels d'accéder à ces bases. Par ailleurs la technique du cryptage n'est pas adapté à ce besoin. Bien que le cryptage, sous toutes ses variantes, constitue une technique solide en matière de sécurité, il sera toujours possible à un individu mal intentionné, arrivant à se procurer la clé de cryptage, à décrypter les données et les lire.

Ces dernières années l'usage des certificats ou signatures électroniques par les administrations publiques (*l'Administration fiscale, la douane ou la CNSS...*) et les entités privées, tend à se généraliser. L'utilisateur reçoit contre les transactions qu'il effectue électroniquement un reçu électronique protégé contre la copie sauvegardée au niveau de son ordinateur. L'usage des certificats électroniques est confronté à des problématiques tel que la détérioration de l'ordinateur stockant ces informations ou le piratage du système dans l'avenir qui entraînera une absence de preuves ou la non acceptation des certificats électroniques stockés chez l'utilisateur relatif aux opérations antérieurs avant l'avancée technologique permettant de falsifier des certificats ou signatures électroniques.

A date d'aujourd'hui, les documents fait en papier ne sont pas protégés électroniquement contre la falsification de leur contenu ou la remise en cause par leur signataire de l'authenticité des signatures portées sur le document. Par ailleurs toutes les techniques existantes ne protègent pas contre le risque de diffusion du contenu protégé décrypté contenant éventuellement des données personnelles.

****

DESCRIPTIF DE L'INVENTION

La présente invention dite la "E-AUTHENTIFICATION" vise un dispositif informatique de sécurisation contre le vol et piratage, de confirmation et d'authentification d'un contenu textuel individualisé normé associé éventuellement à une photo tel qu'une carte d'identité nationale ou d'un contenu textuel individualisé non normé en terme de contenu et en terme de signatures.

La protection vise trois aspects :

1. Protection des données contre la consultation non autorisé : **Le dispositif stocke une empreinte d'un contenu textuel, qu'il compare à la demande au contenu textuel envoyé. Il ne s'agit pas de cryptage des données.**

   Le dispositif utilise une donnée ou une série de données compilées (*EMPREINTES*) obtenues par l'application au contenu textuel individualisé (*DONNEES SOURCE*) d'un algorithme de calcul (*MOULE*) donné. Le ou les serveurs servant à l'authentification stocke(nt) dans différentes tables : Premièrement pour chaque document dans une première table, la référence unique du document (IDENTIFIANT UNIQUE), ainsi que les *EMPREINTES* et les références des *MOULES* (IDENTIFIANTS MOULES) y correspondants, deuxièmement dans une deuxième table le détail des caractéristiques techniques de chaque *MOULE* (DONNEES MOULES), troisièmement éventuellement les données de la signature ou de la confirmation électronique des *EMPREINTES* du document et quatrièmement éventuellement des photos et chacune de ses photos est dénommée par la référence unique de la photo.

De préférence pour les documents normés avec ou sans photo, l'ensemble des informations sur le document d'origine normé et individualisé sont regroupées, dans un code QR ou équivalent et la personne souhaitant l'authentification scanne ce code et les informations sont reprises sur l'application de cette personne qui doit veiller à les vérifier avec le document d'origine pour éviter qu'il s'agisse d'un code QR mis sur un document falsifié.

Pour les documents non normés tel que le contenu d'un contrat, à titre préférentiel l'utilisateur doit veiller à garder un fichier électronique du document imprimé. Dans un traitement préférentiel, le document physique ou électronique d'origine qu'on souhaite authentifié comprend la référence du moule utilisé. L'utilisateur qui souhaite authentifié compare le fichier électronique avec l'original puis l'introduit dans une application et en mentionnant la référence précise du moule et l'application calcule l'empreinte qui est envoyée par la suite pour être authentifié. Une autre solution pour les documents papier qu'on souhaite authentifié par la suite est d'envoyer le fichier électronique de l'impression crypté avant son impression qui est stocké par un organisme de confiance. Comme ça la personne qui souhaite authentifié le document s'adresse à cet organisme pour prendre ce fichier si on juge qu'elle a le droit de le faire. Une autre solution résiderait de travailler avec un moule léger donnant une empreinte sous forme de courbe reliant des points obtenus par lignes de caractère ou par paragraphe. Dans cette ordre d'idée, il faudrait scanner le document en recto et verso et l'envoyer et le système va calculer les courbes et les comparant en tenant compte d'un jeu. Cette façon de faire et plus réaliste et tient compte de la perte du fichier électronique sans enlever la possibilité d'authentification et le rapport final devra être soumis à un expert qui se prononcera sur l'authentification finale surtout si le document d'origine est altéré par d'autre facteur.

La ligne de la table "*EMPREINTES*" contient l'information du numéro de "MOULE" correspondant préétabli selon des dizaines de milliards de jeu différents et la table des "*MOULES*" est une table distincte de la table "*EMPREINTES*". A titre préférentiel pour rendre l'ensemble des éléments aléatoires et accroitre le niveau d'impossibilité d'extraction des données d'origine des "*EMPREINTES*", il est proposé que le document normé contient dans le code QR joint, outre la référence unique permettant de retrouver le numéro de ligne dans la base "*EMPREINTES*", un code 1 d'une dizaine de chiffre qu'il faudrait ajouter au code 2 dans une colonne du ficher "*EMPREINTES*" pour obtenir la référence du "*MOULE*" correspondant. Sans les informations contenues dans le document normé, il sera impossible de reconstituer les données et dans cet ordre d'idée, les tables "*EMPREINTES*" et les tables "*MOULES*" deviennent totalement déconnectées et sans liaison entre eux à défaut d'avoir les données figurant sur chaque document.

Eventuellement pour les document normé avec photo, par le serveur principal, chaque photo après sa réception est cryptée par son "*CODE PIN PHOTO*" correspondant et on obtient un fichier crypté sans datation et le serveur efface ensuite ce code PIN. Par la suite le serveur stocke chaque photo en lui attribuant la "*REFERENCE PHOTO*" reçue avec la photo. Le "*CODE PIN PHOTO*" et la "*REFERENCE PHOTO*", correspondants à chaque photo, ne sont pas introduits de l'extérieur mais le système procède à un décalage de l'"*EMPREINTE*" reçue de l'extérieur avec les informations du "*CODE PIN PHOTO*" et de la "*REFERENCE PHOTO*", afin d'obtenir une nouvelle "*EMPREINTE*" qui a été calculée par système et c'est cette empreinte qui est stockée par la suite. Le but de ce système est d'avoir d'un côté un ensemble de photos cryptées non datées dans un dossier et une table des "*EMPREINTES*" isolée ne comprenant aucun lien avec les photos. Par ailleurs à titre préférentiel, l'information de la "*REFERENCE PHOTO*" peut être non contenue dans le décalage, ni dans la table "*EMPREINTES*" mais figurant sur le document normé qu'on

souhaite authentifié et cette information est transmise par la personne souhaitant l'authentification.

A titre préférentiel, le passage du moule à l'empreinte peut être réalisé en recourant à des concept physique, tel que le centre de gravité.

Exemple du centre de gravité pour données normées : Le moule correspond à des données sous forme de tableau où chaque ligne correspond à une donnée ou lettre spécifique du contenu textuel qu'on souhaite protégé. Les colonnes de ce tableau stocke un type de police déterminé, un type de taille déterminé, un degré d'italique, un degré d'écriture oblique, un degré de gras, un emplacement déterminé, une rotation déterminé et une densité déterminé de la matière... Le but recherché et en appliquant le MOULE à des données, on puisse obtenir par exemple un centre de gravité qui forme l'EMPREINTE. La référence d'un point est muette en soit et on peut pas en extraire les données individualisées.

C'est comme si chaque caractère relatif à chaque information d'un document donnée *(par exemple le lieu de naissance dans un passeport)* est représentée par un objet 3D précis, fait d'une matière avec un densité précise , mis dans un emplacement précis et une position précise, en référence à un espace normé et fixe. Les endroits vides de chaque zone de l'espace fixe ainsi formé, après avoir inséré toute les objets représentant les caractères de l'ensemble des informations, est rempli par la suite différentes matières précises avec des frontières précises aussi. Toutes ces précisions sont défini dans la table des moules qui est composée pour chaque moule d'une ligne avec des centaines de colonnes représentant ces précisions. Des milliards de combinaison sont arrêtés et sont introduites dans le serveur et forment par la suite un liste figée de milliards de moules avec des caractéristiques précises.

Dans un traitement préférentiel, il n'est pas calculé un seul centre de gravité mais plusieurs centre de gravité qui se calcule uniquement sur des éléments rentrant dans une zone précise *(les zones fixées dans chaque moule sont différentes des autres moules)* et les zones précises sont précisées dans le moule et peuvent se chevaucher totalement ou partiellement. Selon cette conception, on obtiendra plusieurs points, en les reliant selon une méthode précisée dans le moule, on obtiendra une courbe. La courbe obtenue ne peut pas servir pour reconstituer les données, surtout que le contenu du moule n'est pas connu et il permettra de répondre à une demande d'authentification avec une précision très suffisante.

Les moules peuvent se baser sur cette idée de centre de gravité à titre préférentiel, mais ils peuvent aussi retenir une infinité de conceptions qui peuvent en partie être inspirés de la physique tel que le degré de passage de lumière en utilisant des formats translucide à des degrés différents ou encore le poids, les ondes produites suite au mouvement d'objet formés par des objets 3D...

2. Protection contre l'intrusion ou le vol externe des bases de données : Le dispositif protège les bases de donnée servant à l'authentification par **leurs isolations physiques** et la connexion entre les serveurs par un moyen de communication sécurisé relatif à la transmission des demandes d'authentification et du résultat de l'authentification.
   Ce moyen de communication primaire sécurisé est réalisé à l'aide de technique ne permettant pas d'avoir la main sur la machine.
   Tel que l'affichage sur écran *(exemple planche de dessin 2/2)* par un serveur émettant des données qui sont mises chacune dans un emplacement précis et un logiciel spécial sur le serveur réceptionnant qui lit les données à partir d'une photo prise par une caméra, ou autre système de reconnaissance, après son passage sur un logiciel de reconnaissance de

caractère. Le même système peut être fait par impression par un premier serveur et la réalisation d'un scan par un deuxième serveur.

Les serveurs centraux *(visés par le serveur n° 1 dans la planche de dessin 1/2)* **comprenant les bases de données, sont isolés et sont déconnectés de tout réseau et on n'a pas comment faire pénétrer un virus ou comment exécuter à distance une commande sur ces ordinateurs. Les serveurs réceptionnant les demandes** *(visés par le serveur n° 2 dans la planche de dessin 1/2)* **envoient l'information par le moyen de communication sécurisé au serveur central puis après traitement le serveur central envoie l'information aux serveurs de sortie** *(visés par le serveur n° 3 dans la planche de dessin 1/2)* **par le moyen de communication sécurisé.**

A titre préférentiel des zones tampons *(visés par la zone 1 et la zone 2 dans la planche de dessin 1/2)* sont insérés à travers un serveur pivot entre le serveur d'entrée et le serveur central et un autre entre le serveur de sortie et le serveur central. Ces serveurs pivots *(visés par les serveur n° 4 et 5 dans la planche de dessin 1/2)* sont relié par une voie de communication sécurisé à double sens pour communiqué avec un ordinateur géré par un opérateur. L'opérateur de chaque zone tampon est chargé d'autoriser le passage du flux ou de le bloquer et cela bien entendu sans le modifier et cette gestion est opérée pour des raisons de sécurité d'Etat et/ou pour décongestionner la file d'attente en précisant les priorités.

Le backup est réalisé par un serveur ou une série de serveur, connecté à ou aux serveur(s) centraux.

A titre préférentiel, le site des serveurs est protégé contre l'intrusion avec un accès très limité et les caméras sont aussi reliés à un appareil d'enregistrement et une procédure spéciales est réservée aux bandes. A titre préférentiel en cas de panne d'un serveur, le serveur backup prend le relais et un autre serveur vierge est inséré qui est paramétré automatiquement par le serveur ayant pris le relais. Les disques durs du serveur en panne sont retirés et détruit sur place et les détritus sont gardés sur place.

3. <u>Protection contre les usurpations des identités :</u> Eventuellement dans le cas des documents contractuels non normés qui sont de préférence fait en PAPIER-POSTAL, une EMPREINTE du document a été générée à travers un MOULE OBTENU et cette empreinte est envoyée accompagnée d'un "*IDENTIFIANT UNIQUE DU DOCUMENT*" *(constitué du numéro composé de préférence d'une association du numéro unique de la première page et le numéro unique de la dernière page)* pour être stockée *(pour être utilisée selon les deux protections précédentes 1 et 2).*

Les signataires après signature du document physique ou électronique ou avant même impression, procède à une confirmation électronique de leur signature en saisissant dans une application informatique un code et son code PIN correspondant. Les codes sont obtenus de façon officielle après vérification de l'identité de la personne. **L'activation de la confirmation des signatures est matérialisée dans la table "*EMPREINTES*" visée dans le point 2 et pour que le système puisse valider cette confirmation, il faudrait que les codes d'activation soit produites de préférence par ce système.** De préférence des registres peuvent être imprimés du serveur d'authentification pour garder une deuxième trace papier des documents dont les signatures ont été confirmer sous la responsabilité d'un juge par exemple qui paraphera ces registres.

A titre préférentiel, le serveur central de la protection n° 2 précédente génère pour chaque carte nationale à la demande une ou une série de codes uniques ainsi leur CODE PIN correspondant. Après activation le serveur garde une trace de l'activation et la référence du document pour lequel ce code a été activé. De préférence ce serveur imprime des cartes à gratter spécifiques à la personne et comportant ses références personnelles. Les codes PIN sont générés de préférences aussi par impression sur papier à travers une imprimante connectée et ils sont automatiquement mis sous enveloppe et envoyés en recommandé, par courrier ordinaire ou remis par huissier. Les codes aussi peuvent de préférence être envoyer par mail à travers le dernier serveur de la protection n° 2.

Le ou la série de code(s) précédent(s) est obtenu par le signataire après présentation chez un automate ou chez organisme public ou autre tel que la POLICE, qui vérifie l'identité de la personne et lui remet un nombre de carte à gratter comportant un code unique qu'il a commandé et qui sont spécifiques à cette personne *(dans la vérification de la personne, il est possible de revenir à des empreintes biologiques de cette personne)*. Les code PIN peuvent être remis par courrier, mail, message ou directement par tout autre procédé. Ce code unique avec son code sont saisie sur une application téléphonique par l'utilisateur sur un projet de document ayant obtenu préalablement à son impression une empreinte. Par la suite le document est imprimé et signé physiquement. L'ordre de la signature et la confirmation de la signature peut être inverser. Les codes peuvent avoir une durée de péremption.

=> Le dispositif visé dans cette troisième protection a pour but, **premièrement** d'éviter tout opération de falsification du contenu d'un document physique ou électronique en générant une empreinte unique par document formant une sécurité irréfragable du contenu du document qui est stocké pour confirmation dans une base très sécurisée comme décrit précédemment et de préférence chaque signataire garde un fichier électronique du document qui peut être envoyé pour vérifier si son empreinte calculée correspond à l'empreinte stockée, **deuxièmement** de permettre une confirmation de la signature du document par des procédés sécurisés évitant ainsi les conflits sur les usurpations d'identité, **troisièmement** de permettre à tout individu disposant du fichier électronique et le référence de vérifier si le document est original et si les signatures ont été confirmées par les signataires.

****

LES EXPLOITANTS POTENTIELS DE L'INVENTION

La présente invention sera notamment mise en œuvre de façon préférentiel par un organisme officiel, d'un état ou d'un groupe état, créé pour cet objet où déjà existant ayant la confiance des usagers de cet état (*tel que le ministère de l'intérieur, la police, le ministère de la justice, la Poste, l'imprimerie officielle...*). Une interaction entre Etats devra être prévu pour prévoir une norme de traitement à l'international pour la non redondance des numéros uniques et pour normer les identifiants de chaque document officiel et le code de chaque information et ces caractéristique et aussi pour normer le transfert de demande d'authentification émanant d'un état et relatif à des documents d'un autre état.

****

REVENDICATIONS

1. Dispositif informatique sécurisé de confirmation de l'authenticité du contenu textuel individualisé d'un document, physique ou électronique, normé ou non normé, associé éventuellement à une photo, intervenant suite à la réception à travers une connexion donné d'une "*DEMANDE EXTERNE D'AUTHENTIFICATION*" **caractérisé** en ce que
   - **Premièrement,** la base servant à l'authentification contient dans une première table de donnée pour chaque "*REFERENCE UNIQUE DU DOCUMENT*", un "*CODE PIN DU DOCUMENT*", une ou une série de données compilées (*EMPREINTES STOCKEES*) dont chacune est obtenue par l'application au contenu textuel individualisé (*DONNEES SOURCE*) d'un algorithme de calcul (*MOULE*) donné, éventuellement la référence de la "*PHOTO STOCKEE*" dans l'ordinateur qui est éventuellement crypté (photo), ainsi que la référence du "*MOULE*" utilisé pour obtenir chaque "*EMPREINTE STOCKEE*", de tel sorte qu'à partir des "*EMPREINTES STOCKEES*" on ne puisse pas reconstitué les "*DONNEES SOURCE*" et dans une deuxième table de données les détails techniques de chaque "*MOULE*",
   - **Deuxièmement,** la "*DEMANDE EXTERNE D'AUTHENTIFICATION*" contient outre la "*REFERENCE UNIQUE DU DOCUMENT*" et son "CODE PIN DU DOCUMENT", les "*DONNEES SOURCE*" et éventuellement la "*PHOTO RECUE*",
   - **Troisièmement,** l'ordinateur contenant la base d'authentification, après vérification préalable du "*CODE PIN DU DOCUMENT*", procède au calcul des "*EMPREINTES CALCULEES*" en appliquant aux "*DONNEES SOURCE*" le ou les différents moules affectées à chaque "*EMPREINTE STOCKEE*",
   - **Quatrièmement,** le système compare que chaque "*EMPREINTE STOCKEE*" avec l'"*EMPREINTE CALCULEE*" correspondante et éventuellement la "*PHOTO STOCKEE*" avec la "*PHOTO RECUE*",
   - **Et cinquièmement** la base d'authentification délivre une réponse à la demande d'authentification positive si les "*EMPREINTES CALCULEES*" et éventuellement la "*PHOTO RECUE*" coïncident avec les "*EMPREINTES STOCKEES*" et éventuellement la "*PHOTO STOCKEE*" et une réponse négative dans le cas contraire.

2. Dispositif informatique sécurisé de confirmation de l'authenticité du contenu textuel individualisé d'un document, physique ou électronique normé, associé à une photo, intervenant suite à la réception à travers une connexion donnée d'une "*DEMANDE EXTERNE D'AUTHENTIFICATION*", **caractérisé** en ce que,
   - **Premièrement,** les bases servant à l'authentification contiennent dans un premier ordinateur une première table de donnée pour chaque "*REFERENCE UNIQUE DU DOCUMENT*", un "*CODE PIN DU DOCUMENT*", une ou une série de données compilées (*EMPREINTES STOCKEES MODIFIEES*) dont chacune est obtenue par l'application au contenu textuel individualisé (*DONNEES SOURCE*) d'un algorithme de calcul (*MOULE*) donné et décalée par une formule mathématique figurant dans le (MOULE) dont les inconnus sont la "*REFERENCE PHOTO STOCKEE*" et son "*CODE PIN PHOTO STOCKEE*", de tel sorte, en premier, à partir des "*EMPREINTES STOCKEES MODIFIEES*" on ne puisse pas reconstitué les "*DONNEES SOURCE*" et en deuxième lieu, on ne peut pas savoir à partir des "*EMPREINTES STOCKEES MODIFIEES*" la "*REFERENCE PHOTO STOCKEE*" et/ou son "*CODE PIN PHOTO STOCKEE*" , dans une deuxième table de données, éventuellement dans le même ordinateur, les détails techniques de chaque "*MOULE*" et à titre préférentiel dans un deuxième ordinateur les "*PHOTOS STOCKEES*" portant comme dénomination, pour chacune d'elle, la "*REFERENCE PHOTO STOCKEE*" et chaque "*PHOTO STOCKEE*" est cryptée par le "*CODE PIN PHOTO STOCKEE*",

- **Deuxièmement,** la "*DEMANDE EXTERNE D'AUTHENTIFICATION*" contient outre la "*REFERENCE UNIQUE DU DOCUMENT*" et son "CODE PIN DU DOCUMENT", les "*DONNEES SOURCE*" et la "*PHOTO RECUE*",
- **Troisièmement,** l'ordinateur contenant la base d'authentification, après vérification préalable du "*CODE PIN DU DOCUMENT*", procède au calcul des "*EMPREINTES CALCULEES*" en appliquant aux "*DONNEES SOURCE*" les différents moules affectées à chaque "*EMPREINTE STOCKEE*",
- **Quatrièmement,** le système compare chaque "*EMPREINTE STOCKEE MODIFIEE*" avec l'"*EMPREINTE CALCULEE*" correspondante et on obtient après cette comparaison, la "*REFERENCE PHOTO CALCULEE*" et son "*CODE PIN PHOTO CALCULEE*" et cela à partir du décalage obtenue et de la formule mathématique figurant dans le (MOULE) spécifique à chaque "*EMPREINTE STOCKEE MODIFIEE*",
- **Cinquièmement,** le système compare la "*PHOTO RECUE*" avec la "*PHOTO STOCKEE*", portant la "*REFERENCE PHOTO CALCULEE*", après son décryptage par le "*CODE PIN PHOTO CALCULEE*"
- Et **sixièmement,** la base d'authentification délivre une réponse à la demande d'authentification positive si la "*PHOTO RECUE*" coïncide avec la "*PHOTO STOCKEE*" et une réponse négative dans le cas contraire.

3. Dispositif informatique primitif, destiné à se prémunir contre une attaque informatique extérieure, sur une (ou des) base(s) de donnée *(tel que celles servant à l'authentification présenté au niveau de la revendication 1 ou 2),* pour réaliser des opérations non autorisées (*tel que n'importe quel commande du type : copier, couper, dupliquer, modifier, consulter ou supprimer...*), **caractérisé** en ce que :

- **Premièrement,** un premier serveur (*ou un groupe de plusieurs serveurs*), contenant une (*ou plusieurs*) base de donnée, est isolé physiquement et n'est doté d'aucun moyen de connexion externe *(non connecté à un réseau par câble, wifi, bluetooth...)*
- **Deuxièmement** chaque demande de recherche et ses données reçues par un deuxième serveur, est communiquée au premier serveur à l'aide de technique élémentaire, permettant, au niveau du 1er serveur, seulement l'entrée des données de chaque recherche dans la zone de saisie du logiciel de recherche installé au niveau du 1er serveur, de façon ne permettant pas d'avoir la main sur la machine ou le passage de n'importe quel commande en dehors de l'entrée des données, tel que l'affichage sur écran, à grand format, par un deuxième serveur (*isolé physiquement du premier ordinateur*), de la demande de recherche, avec un emplacement précis pour chaque donnée de recherche et la lecture et l'entrée des données dans le logiciel de recherche installé sur le premier serveur sont faites grâce au traitement par un logiciel de reconnaissance de caractère d'une prise de photo par une caméra ou un appareil à photo (*le même résultat peut être obtenu par d'autre technique tel le scan par le premier serveur d'une feuille continue en rouleau imprimée par le deuxième serveur - cette solution permet de garder une trace imprimée),*
- **Troisièmement** le (ou les) résultat de chaque recherche est communiqué par le premier serveur à un troisième serveur (*à titre non préférentiel, le troisième et le deuxième serveur peuvent être confondus en un seul ordinateur*), à travers le même dispositif précité dans le point 2,
- **Quatrièmement** l'entrée des données formant la (ou les) base(s) de donnée dans le premier serveur est faite, à titre non limitatif, à partir du même dispositif précité dans le point 2, par un quatrième serveur ou à travers un scanner relié à ce quatrième serveur *(le 4ème serveur enverra l'information au premier serveur à travers le dispositif précité décrit dans le point 2)* ou à titre non préférentiel par un scanner de documents relié à ce

premier serveur et ces documents scannées sont à titre préférentiel archivés dans le même local,

- **Cinquièmement** à titre préférentiel, les données de chaque serveur ont un backup et en cas de disfonctionnement d'un serveur le serveur backup prend le relais,
- **Sixièmement** à titre préférentiel, le premier serveur n'a ni souris, ni clavier et aucune sortie et en cas de son disfonctionnement, il est remplacé systématiquement par un serveur de sauvegarde, le premier serveur est retiré et détruit intégralement sur place soit automatiquement soit manuellement (les détritus des disques durs peuvent être gardés sur place) et un serveur vierge de sauvegarde est ajouté qui est paramétré par l'ordinateur restant de sauvegarde,
- **Septièmement,** à titre préférentiel, deux zones tampons sont introduites dans le schéma. La première zone entre le serveur premier et le second serveur et la deuxième zone entre le serveur premier et le troisième serveur. Une troisième zone peut aussi être introduite entre le premier serveur et un quatrième serveur destiné à l'introduction des empreintes. Chaque zone tampon comprend premièrement un serveur relié en premier à l'autre serveur par le dispositif précité cité dans le point deux et deuxièmement un ordinateur non relié à aucune connexion avec un opérateur. Cet ordinateur communique avec le serveur de la zone tampon avec le même procédé précité visé dans le point 2. Cette zone tampon sert à réguler l'ordre de transmission des données et la cadence et pour stocker temporairement les demandes en cas de panne du premier serveur. Dans ce sens les demandes ne peuvent pas être modifiés mais simplement passe en file d'attente et ils ne sortent qu'après accord de l'opérateur chargé de la régulation qui peut aussi modifier l'ordre dans la file d'attente,
- **Et huitièmement,** à titre préférentiel, si dans le dispositif précité visé au point 2, il a été utilisé un écran d'affichage et une caméra *(planche de dessin 2),* la caméra est relié aussi à un appareil d'enregistrement et une procédure spéciales est réservée aux bandes.

4. Dispositif permettant à une partie d'un acte physique ou électronique portant une "REFERENCE UNIQUE" et à titre préférentiel un "CODE PIN", la confirmation électronique de sa signature (ou tout autre forme d'approbation), physique ou électronique, , **caractérisé** en ce que,

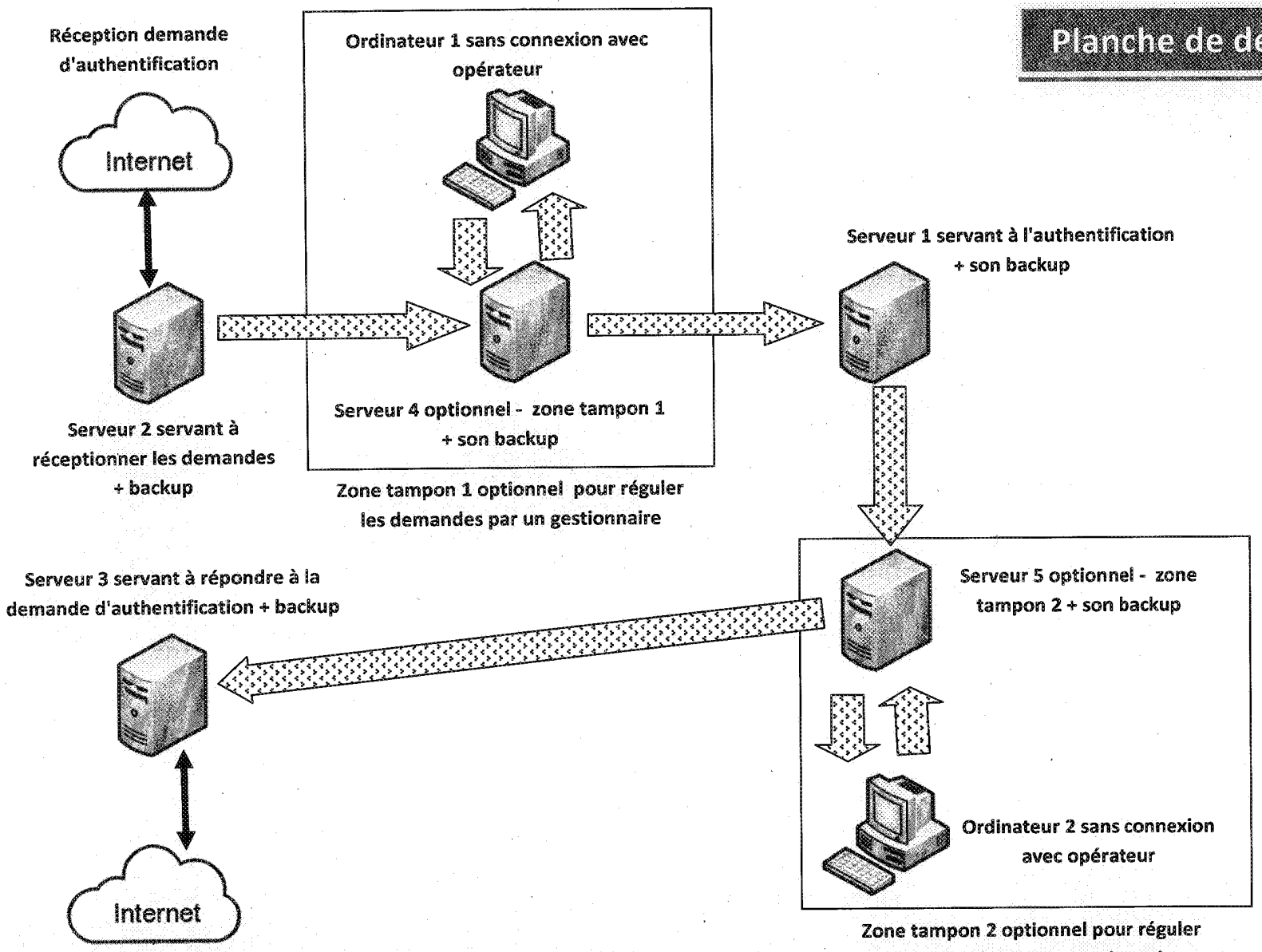
- **Premièrement,** une autorité gouvernementale *(ou autre et de préférence une branche de la police créé à cette effet),* après vérification de l'identité du demandeur *(à titre préférentiel, la partie se présente elle même et des empreintes sont saisies et comparer aux données biométriques en possession de la police),* délivre à la partie précitée un nombre de "CODE D'APPROBATION" *(à titre préférentiel 1 : selon le nombre précommandé - à titre préférentiel 2 : sur la base de sa demande formulée sur un site web - à titre préférentiel 3 : Le code d'approbation contient en premier un code pays, puis un code par centre, puis le numéro de la pièce d'identité de la partie précitée, puis le numéro unique - à titre préférentiel les codes d'approbation ne se suivent pas dans leur série)* et cela sur tout forme de support. De préférence les "CODES D'APPROBATION" ont une durée de péremption et la partie précitée lors de la commande peut choisir une durée moindre que le standard. Aussi de préférence par un parallélisme des formes, la partie précitée peut procéder à l'annulation des "CODES D'APPROBATION".
- **Deuxièmement,** après l'obtention physique des codes d'approbation, à titre préférentiel la partie se présente à un automate qui lui délivre les "CODE PIN D'APPROBATION" ou une autre autorité gouvernementale *(ou autre de préférence une branche du ministère de la justice créé à cette effet),* procède, soit par l'envoie par mail, sms, huissier de justice, courrier simple ou recommandée ou tout autre forme de notification des "CODE PIN D'APPROBATION" sous forme scellé, ou soit par une remise

directe à la partie précitée et cela après vérification de l'identité de la personne qui s'est présentée. Les "CODE PIN D'APPROBATION" ont un numéro d'ordre et sont classés selon ce numéro d'ordre, comme d'ailleurs pour les "CODE D'APPROBATION" précité au point premier et cela pour les deux organismes différentes n'ait pas en leur possession l'ensemble des éléments. A titre préférentiel, pour les sociétés deux personnes physiques peuvent confirmer conjointement leur signatures, mais les codes d'approbation sont remis à la première personne et le code PIN d'approbation sont remis à la deuxième personne.

- **Troisièmement,** après obtention du ou des code(s) d'approbation et leur code PIN correspondant, lors de l'activation par la partie précitée, en saisissant l'ensemble des information sur un logiciel gérant les actes physiques ou électronique *(acte imprimé de préférence : 1 en PAPIER POSTAL amélioré - De préférence 2 : le numéro unique de l'acte est constitué du numéro de l'acte généré par le système et qui est composé du numéro de la première page et le numéro de la dernière page - De préférence 3 : le logiciel génère un code global par acte composé d'une succession de codes comprenant le numéro de l'acte, les références des feuilles physiques, l'empreinte calculée selon la revendication 1 et les codes d'approbation des deux parties ou plus et leur code PIN correspondant - De préférence 4 : les informations ajoutés par le système ou par les parties sont introduits dans le fichier à imprimer et le fichier est imprimé par la suite et les actes sont signés manuellement - De préférence 5 : le code PIN est validé sur Smartphone par son titulaire sur l'acte brouillon à imprimer et code d'approbation est remis au rédacteur d'acte),*
- **Quatrièmement,** à titre préférentiel, les codes d'approbation et leur code PIN sont généré automatiquement par le dispositif figurant dans la revendication n° 3.

****
****
***

Planche de dessin un sur deux



45510A1

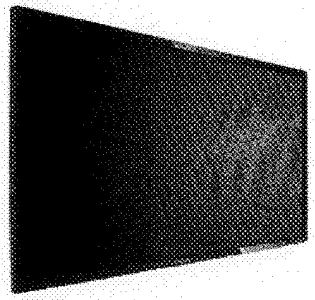
MA

MA 45510A1

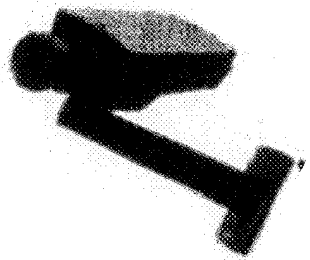
Planche de dessin deux sur deux

Exemple de dispositif de transmission limitée à l'aide de caméra et d'écran d'affichage

Ecran d'affichage mentionnant chaque information dans un emplacement précis et cela selon une norme par type de document



Caméra haute résolution dirigé vers l'écran d'affichage et éventuellement lié au serveur et aussi à un enregistreur et une procédure spéciale est réservée aux bandes stockées



Principe et explication du symbole de la planche de dessin 1

Symbole mis sur la planche n°1 pour viser dispositif de transmission limité visé dans le point 2 de la revendication n°3 (la flèche représente le point de lecture des données transmises et la base de la flèche représente le point d'écriture des données pour réaliser la transmission de données

MA 45510A1

ROYAUME DU MAROC
****
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
****

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13)

Renseignements relatifs à la demande	
N° de la demande : 45510	Date de dépôt : 08/04/2019
Déposant : BRAHIM CHAOUI	
Intitulé de l'invention : DISPOSITIF INFORMATIQUE D'AUTHENTIFICATION ELECTRONIQUE DE SÉCURISATION, DE CONFIRMATION ET D'AUTHENTIFICATION D'UN CONTENU TEXTUEL INDIVIDUALISE	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents brevets cités dans le rapport de recherche sont téléchargeables à partir du site http://worldwide.espacenet.com, et les documents non brevets sont joints au présent document, s'il y en a lieu.

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☒ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☒ Cadre 4 : Remarques de forme et de clarté
- ☐ Cadre 5 : Défaut d'unité d'invention
- ☐ Cadre 6 : Observations à propos de certaines revendications exclues de la brevetabilité
- ☒ Cadre 7 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Examinateur: Ilham Oubiyi	**Date d'établissement du rapport** : 16/04/2019
Téléphone: 212 5 22 58 64 14/00	

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  7 Pages
- Revendications
  4
- Planches de dessin
  2 Pages

Cadre 3 : Titre et Abrégé tel qu'ils sont définitivement arrêtés

- L'intitulé tel qu'il a été déposé "E-AUTHENTIFICATION" (DISPOSITIF INFORMATIQUE DE SÉCURISATION, DE CONFIRMATION ET D'AUTHENTIFICATION D'UN CONTENU TEXTUEL INDIVIDUALISE) a été modifié et arrêté par l'examinateur DISPOSITIF INFORMATIQUE D'AUTHENTIFICATION ELECTRONIQUE DE SÉCURISATION, DE CONFIRMATION ET D'AUTHENTIFICATION D'UN CONTENU TEXTUEL INDIVIDUALISE.

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04L29/06
CPC : H04L63/123 ; H04L63/126

Plateformes et bases de données électroniques de recherche :

EPOQUENET, WPI, ScienceDirect, ORBIT

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
A	US20150341370A1 ; Sal Khan ; 26-11-2015	1-4
A	US20170134167A1 ; Paul L Carter ; 11-05-2017	1-4
A	US9369287B1 ; Seyed Amin Ghorashi Sarvestani ; 14-06-2016	1-4

***Catégories spéciales de documents cités :**

-« **X** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
-« **Y** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« **P** » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« **E** » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

Partie 3 : Opinion sur la brevetabilité

Cadre 4 : Remarques de forme et de clarté

- Remarques de clarté

Les caractéristiques énoncées dans les revendications du procédé 1-2, 4 portent sur les caractéristiques techniques d'un procédé et non pas d'un dispositif. Les limitations visées ne ressortent donc pas clairement de ces revendications conformément aux exigences de l'art. 35 de la loi 17-97 telle que modifiée et complétée par la loi 23-13. Il conviendrait par conséquent d'inclure ces précisions lors de l'évaluation de la nouveauté et l'activité inventives desdites revendications.

Cadre 7 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté	Revendications 1-4 Revendications aucune	Oui Non
Activité inventive	Revendications 1-4 Revendications aucune	Oui Non
Application Industrielle	Revendications 1-4 Revendications aucune	Oui Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : US20150341370A1

1. Nouveauté

Aucun des documents cités ci-dessus ne divulgue l'ensemble des caractéristiques techniques énoncées dans les revendications 1-4. Par conséquent, l'objet desdites revendications est nouveau au sens de l'art. 26 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

2. Activité inventive

Le document D1, qui est considéré comme l'état de la technique le plus proche de l'objet de la revendication 1, divulgue (voir figure10 et revendication 1) un dispositif et son procédé de validation d'un document d'identité comprenant les étapes suivantes :

- numériser le document d'identité avec un dispositif d'imagerie pour produire au moins une image numérisée;
- localiser un identifiant de document sur le document d'identité à l'aide du dispositif d'imagerie;
- localiser, à l'aide d'un serveur de vérification, le numéro d'identité dans une base de données d'identité de juridiction gérée par une autorité qui a délivré le document d'identité;
- déterminer avec le serveur de vérification si tout ou partie de l'image numérisée du document d'identité dans son ensemble, et ses composants correspondent à une image

numérique synthétisée correspondante du document d'identité et aux composants du document d'identité dans une base de données d'informations d'identité de juridiction; et
- générer sur un affichage une indication de la validité ou non du document d'identité sur la base de la détermination.

Par conséquent, l'objet de la revendication 1 diffère de D1 en ce que la base servant à l'authentification contient dans une première table de donnée pour chaque "REFERENCE UNIQUE DU DOCUMENT", un "CODE PIN DU DOCUMENT", une ou une série de données compilées (EMPREINTES STOCKEES) dont chacune est obtenue par l'application au contenu textuel individualisé (DONNEES SOURCE) d'un algorithme de calcul donné, éventuellement la référence de la "PHOTO STOCKEE" dans l'ordinateur qui est éventuellement crypté (photo), ainsi que la référence de l'algorithme de calcul utilisé pour obtenir chaque "EMPREINTE STOCKEE", de tel sorte qu'à partir des "EMPREINTES STOCKEES" on ne puisse pas reconstituer les "DONNEES SOURCE" et dans une deuxième table de données les détails techniques de chaque algorithme de calcul ;
la "DEMANDE EXTERNE D'AUTHENTIFICATION" contient outre la "REFERENCE UNIQUE DU DOCUMENT" et son "CODE PIN DU DOCUMENT", les "DONNEES SOURCE" et éventuellement la "PHOTO RECUE" ;
l'ordinateur contenant la base d'authentification, après vérification préalable du "CODE PIN DU DOCUMENT" procède au calcul des "EMPREINTES CALCULEES" en appliquant aux "DONNEES SOURCE" le ou les différents algorithmes affectés à chaque "EMPREINTE STOCKEE" ;
le système compare 'que chaque "EMPREINTE STOCKEE" avec l'"EMPREINTE CALCULEE" correspondante et éventuellement la "PHOTO STOCKEE" avec la "PHOTO RECUE" ;
la base d'authentification délivre une réponse à la demande d'authentification positive si les "EMPREINTES CALCULEES" et éventuellement la "PHOTO RECUE" coïncident avec les "EMPREINTES STOCKEES" et éventuellement la "PHOTO STOCKEE" et une réponse négative dans le cas contraire.

Le problème que la présente invention se propose de résoudre peut donc être considéré comme celui d'éviter les attaques informatiques extérieures affectant la base de données servant à l'authentification.

La solution à ce problème proposée dans la revendication 1 n'est pas décrite dans l'art antérieur, pris seul ou en combinaison. Aucun enseignement n'a été trouvé dans les documents de l'état de la technique qui aurait incité l'homme du métier, d'arriver à la solution telle que décrite dans la revendication 1. Par conséquent, l'objet de la revendication 1 implique une activité inventive au sens de l'article 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

Les revendications 2-4 dépendent de la revendication 1 dont l'objet est considéré inventif, comme indiqué auparavant, et satisfont donc également, en tant que telles, aux exigences de l'article 28 de la loi 17-97 telle que modifiée et complétée par la loi 23-13.

3. Application industrielle

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible.