(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 958 101**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **10 01229**

(51) Int Cl[8] : ***H 04 L 9/32*** *(2006.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 26.03.10.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 30.09.11 Bulletin 11/39.

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

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

(71) **Demandeur(s) :** *NTX RESEARCH* — FR.

(72) **Inventeur(s) :** THONIEL PASCAL DANIEL GEORGES.

(73) **Titulaire(s) :** NTX RESEARCH.

(74) **Mandataire(s) :** NTX RESEARCH SA.

(54) INFRASTRUCTURE DE GESTION DE BI-CLES DE SECURITE DE PERSONNES PHYSIQUES (IGCP/PKI).

(57) L'invention concerne une infrastructure de gestion de bi-clés de sécurité de personnes physiques comportant une clé publique et une clé privée avec un certificat de clé publique, ladite structure comportant au moins une autorité d'enregistrement et son serveur notaire électronique.

On prévoit au moins une autorité d'enregistrement et son serveur notaire électronique pour chacun des cercles de confiance, l'autorité d'enregistrement comprend des agences locales d'enregistrement. L'agence locale d'enregistrement établit, après vérification en face à face de l'identité, un certificat de propriété de clé publique qui est transmis de façon sécurisée au serveur notaire électronique associé qui le stocke de manière sécurisée. Le certificat de propriété de clé publique est chiffré avec la clé privée de la personne physique.

Le certificat de propriété de clé publique peut être requêté en ligne sur le serveur notaire électronique pour vérifier l'authenticité du certificat de clé publique correspondant. Application aux citoyens, consommateurs et professionnels.

FR 2 958 101 - A1

L'invention concerne une infrastructure de gestion de clés publiques (IGCP) ou *Public Key Infrastructure* (PKI) - système de cryptographie asymétrique appliquée comportant un couple de clés (bi-clé) à savoir une clé publique et une clé privée - son organisation, ses protocoles cryptographiques, ainsi qu'un dispositif pour la mise en œuvre du procédé.

L'invention s'applique notamment à la sécurisation des communications sur un réseau distant tel que par exemple le réseau Internet ou de téléphonie, notamment pour la banque en ligne, le paiement en ligne, l'administration en ligne, la santé en ligne ou tout autre type de transaction nécessitant une fiabilité et une sécurité importante.

L'invention vise à fournir une infrastructure de sécurité capable d'assurer les fonctions de sécurité d'authentification et de confidentialité ainsi que la technique cryptographique de la signature électronique.

La sécurité d'un système cryptographique utilisant un algorithme asymétrique repose en grande partie sur la gestion des clés publiques.

Dès qu'un système cryptographique possède un grand nombre d'utilisateurs, il faut mettre en œuvre une infrastructure de gestion de clés. Les IGCP sont créées pour rendre opérationnelle la cryptographie asymétrique (bi-clé) dans le monde réel.

La cryptographie à clé publique est confrontée à un problème extrêmement difficile : comment garantir la validité des clés publiques ? Dès qu'un utilisateur veut chiffrer un message à l'aide d'un algorithme asymétrique ou vérifier une signature, il doit se procurer la clé publique de son interlocuteur (le destinataire du message) ou celle du signataire. Si les clés publiques sont stockées dans des annuaires non sécurisés, elles risquent d'être interceptées et/ou remplacées par d'autres clés. Il est donc possible de fabriquer de fausses signatures simplement en substituant la clé publique d'un utilisateur.

Ce problème crucial pour toute la cryptographie à clé publique peut être résolu en introduisant une tierce partie de confiance, appelée Autorité de Certification (AC), qui valide le lien entre l'identité des utilisateurs et leurs clés publiques. Formellement, un certificat de clé publique est composé d'un texte clair et d'une signature. Le texte clair contient en particulier une clé publique et une chaîne de caractères identifiant le

propriétaire de cette clé. La signature correspond à la signature numérique du texte clair précédent par l'AC. Si cette signature est authentique, elle prouve que l'AC valide le lien entre l'identité d'un utilisateur et sa clé publique.

On connaît des IGCP dans lesquelles la pierre angulaire de la sécurité de la clé publique est assurée par une Autorité de Certification (AC).

Une Autorité de Certification (AC) est une tierce partie de confiance pour la génération, la signature, la publication et la révocation des certificats de clés publiques.

Il existe des systèmes très hiérarchisés, tel celui décrit dans la norme ISO X.509v3, dans lesquels la clé publique d'un utilisateur est certifiée par une autorité dont la clé publique est à son tour certifiée par une autorité supérieure.

L'IGCP "internationale" ou "reconnue" revient à confier à des sociétés tierces spécialisées - les Autorités de Certification (AC) comme « Verisign », « Entrust », « Thawte », « Keynectis », « CertiNomis »... - le soin de certifier la clé publique d'une entité ou d'un individu. Ces sociétés, parce qu'elles sont des autorités de certification reconnues, garantissent et assurent la validité d'une clé publique et surtout son appartenance à son propriétaire légitime depuis n'importe quel navigateur Internet. Ainsi, l'utilisation du certificat de clé publique devient sûre.

L'IGCP "interne" revient à substituer aux Autorités de Certification (AC) tierces évoquées ci-dessus sa propre organisation. Autrement dit, une entité suffisamment importante peut déployer sa propre architecture interne en devenant de ce fait sa propre Autorité d'Enregistrement (AE) et sa propre Autorité de Certification pour ses membres (certificats "client"). Cette solution est souvent déployée pour une utilisation interne aux grandes entreprises et administrations.

Ces deux IGCP sont éprouvées sur le plan de la sécurité (cryptographie). Elles sont aussi viables sur les plans technologique, organisationnel et économique.

Cependant, chacune est adaptée à un contexte particulier qui ne correspond pas au besoin d'un déploiement à grande échelle au niveau du Particulier, qu'il soit citoyen, consommateur et/ou professionnel.

Les Autorités de Certification sont centralisées. Cela pose des problèmes d'organisation pratique et de sécurité pour l'enregistrement et la délivrance des certificats à de nombreux utilisateurs venant d'horizons divers.

Le point d'achoppement des IGCP traditionnelles est l'Autorité de Certification dès lors qu'elles adressent un grand nombre d'utilisateurs comme c'est le cas des personnes physiques ou Particuliers, qu'ils soient citoyen, consommateur et/ou professionnel.

En effet, les Autorités de Certification des IGCP "internationales" ne disposent pas d'agences d'enregistrement de proximité pour "enrôler" les utilisateurs de manière satisfaisante (présence physique obligatoire) et imposent une redevance annuelle non négligeable pour chaque Particulier. Dans le présent contexte, il y en a des millions.

Il y a par ailleurs confusion des rôles puisque l'Autorité de Certification assure également la mission d'Autorité d'Enregistrement lors de la délivrance d'un certificat à distance, ce qui est souvent le cas dans le monde réel.

L'invention propose une IGCP sans Autorité de Certification afin que le système soit "centré" sur le Particulier (citoyen/ consommateur/professionnel). L'organisation proposée comprend de nombreuses agences de proximité réparties sur le territoire afin de faciliter l'accès à l'enrôlement et de garantir la sécurité par des procédures en "face à face".

On connaît déjà des systèmes sans Autorité de Certification comme le système PGP (*Pretty Good Privacy*) qui utilise au contraire une architecture qui repose sur la confiance. On accepte la clé publique d'un utilisateur parce qu'elle est signée par une personne dont la clé est elle-même signée par quelqu'un que l'on connaît et en qui on a confiance.

Ce système reste toutefois limité car il n'adresse que des groupes restreints d'individus et peut difficilement être déployé à très grande échelle.

L'invention vise donc à améliorer les procédés précédemment cités, et à permettre à de nombreux utilisateurs de s'authentifier, de signer des transactions et de chiffrer des messages facilement et à un coût minime.

L'invention consiste en une nouvelle IGCP dite "2.0" construite sur trois niveaux. Cette nouvelle IGCP a pour but d'apporter à un grand nombre de Particuliers citoyens/consommateurs/professionnels d'horizons divers les moyens de sécurité cryptographique nécessaires à la confiance dans la vie numérique. L'invention permet à de nombreuses personnes physiques d'horizons divers de s'authentifier, de signer des transactions et de chiffrer des messages facilement et à un coût minime.

Le problème ne se pose pas dans le déploiement, la gestion et l'utilisation des certificats "serveur" qui sont bien gérés par l'IGCP "internationale" au troisième niveau. Le problème se pose plutôt dans celui des certificats "client", c'est-à-dire ceux destinés aux agents d'enregistrement d'une part (deuxième niveau), et aux particuliers d'autre part (troisième niveau).

L'invention propose donc un deuxième niveau pour gérer les certificats client des agents d'enregistrement par une IGCP "interne" : une par acteur d'un cercle de confiance, comme par exemple une banque ou un opérateur télécom.

L'invention propose aussi un premier niveau pour traiter le cas du Particulier citoyen/consommateur/professionnel avec l'innovation de l'IGCP dite "utilisateur".

L'infrastructure proposée comprend donc trois niveaux : une IGCP "internationale" (ou "reconnue") pour délivrer et gérer les certificats serveur des fournisseurs d'identité (IDP), des fournisseurs d'attributs (AP) et des fournisseurs de services (SP) ; une IGCP "interne" déployée par les Autorités d'Enregistrement pour leurs agences locales ; et une IGCP "utilisateur" pour le Particulier citoyen/consommateur/professionnel.

Afin d'assurer une efficacité maximale pour un coût minimal en prenant le meilleur de chaque IGCP, l'IGCP à 3 niveaux consiste à déployer : au troisième niveau (central) une IGCP "internationale" (ou "reconnue") sur un minimum d'acteurs ; au deuxième niveau (intermédiaire) autant d'IGCP "internes" que d'Autorités d'Enregistrement

(nombre d'acteurs significatifs) ; au premier niveau l'IGCP "utilisateur" pour le Particulier citoyen/consommateur/professionnel (très nombreux acteurs).

L'IGCP à 3 niveaux définit donc une organisation nouvelle qui devient possible grâce à une architecture multi-niveaux d'une part, et aux protocoles cryptographiques de l'IGCP "utilisateur" adressant les utilisateurs du premier niveau, d'autre part.

Selon l'invention, l'IGCP "2.0" préconise la mise en place au troisième niveau d'une IGCP "internationale" qui a pour mission de délivrer et de gérer les certificats serveur des acteurs centraux.

Les acteurs centraux d'une architecture de gestion des identités sont les fournisseurs d'identité (IDP *IDentity Provider*, IP/STS *Identity Provider/Security Token Service*), les fournisseurs d'attributs (AP *Attribute Provider*) et les fournisseurs de service (SP *Service Provider*, RP *Relying Party*). Ces acteurs doivent communiquer entre eux de façon sécurisée.

Ces acteurs centraux évoluent dans des cercles de confiance distincts. Les cercles de confiance sont : 1) le cercle Régalien, 2) le cercle Collectivités Territoriales, 3) le cercle Santé, 4) le cercle Banque, Finance et Assurance, 5) le cercle Internet et Télécommunication.

Selon l'invention, l'IGCP "2.0" préconise la mise en place au deuxième niveau d'Autorités d'Enregistrement (AE) qui ont pour mission d'intégrer les citoyens/consommateurs/professionnels dans le système. Elles servent d'intermédiaires de proximité dans chacun des cercles de confiance.

Les Autorités d'Enregistrement assurent deux fonctions principales: agent de proximité et tiers de confiance. Leur rôle est de délivrer les certificats "client" des citoyens/consommateurs/professionnels.

Les Autorités d'Enregistrement (AE) doivent remplir trois conditions. Premièrement, les AE doivent disposer d'agences de proximité suffisamment nombreuses et réparties de manière relativement uniforme sur le territoire et les différentes zones de population pour constituer de bons agents de proximité. Deuxièmement, les AE doivent pouvoir être reconnues et acceptées par le Particulier citoyen/ consommateur/professionnel comme tiers de confiance (notoriété,

respectabilité, reconnaissance légale). Troisièmement, les AE doivent être habilitées par chacun des cercles de confiance pour être un tiers de confiance dudit cercle.

L'IGCP "2.0" propose de mettre en place des réseaux d'Agences Locales d'Enregistrement (ALE) dans le monde réel, par cercle de confiance. Dans le cercle Régalien : les notaires de famille, les huissiers... Dans le cercle Collectivités Territoriales : les mairies, les bureaux de poste... Dans le cercle Santé : les caisses d'assurance maladie, les pharmacies... Dans le cercle Banque, Finance et Assurance : les agences bancaires, les cabinets d'agent d'assurance... Dans le cercle Internet et Télécommunication : les agences télécom...

Selon l'invention, l'IGCP "2.0" préconise la mise en place au premier niveau d'une IGCP "utilisateur" pour servir les particuliers citoyens/consommateurs/professionnels.

Le protocole cryptographique de l'IGCP "utilisateur" s'affranchit d'une Autorité de Certification au profit d'un Notaire Electronique.

Dans le crypto-système de l'IGCP "utilisateur", le choix du type d'algorithme asymétrique est indifférent, qu'il soit fondé sur la factorisation des grands nombres en deux nombres premiers (« RSA », « Rivest Shamir Adleman »), sur des logiques d'empilements, le calcul de logarithmes discrets ou bien encore sur les courbes elliptiques (ECC, *Elliptic Curve Cryptography*, variante des logarithmes discrets).

Le protocole cryptographique de l'IGCP "utilisateur" s'appuie : d'une part sur un "certificat de clé publique" auto-signé par l'utilisateur, c'est-à-dire signé avec sa propre clé privée et, d'autre part, sur un "certificat de propriété de clé publique" auto-scellé par l'utilisateur, c'est-à-dire chiffré avec sa propre clé privée.

Les certificats de personne associant une clé publique à son propriétaire légitime (dits "certificats de clé publique") sont consultables directement par tous les acteurs. Aucune Autorité de Certification n'est nécessaire puisque le certificat de personne est auto-signé. Cette auto-signature n'apporte bien sûr aucune garantie sur la validité du "certificat de clé publique", elle permet simplement de rendre ce certificat conforme à la norme X.509v3 afin de pouvoir être utilisé par les applications existantes.

Contrairement à l'IGCP traditionnelle avec Autorité de Certification, un acteur est en mesure de s'assurer de la validité du certificat de clé publique d'une personne par la bonne exécution d'un protocole cryptographique entre cet acteur et le serveur du Notaire Electronique. Ce protocole implique directement l'usage de cette clé. C'est la bonne ouverture, par la clé publique à vérifier, du certificat de propriété consultable en ligne dans la base/annuaire du Notaire Electronique et la vérification de son empreinte qui attestent au final la validité de cette même clé.

Selon la présente invention, la représentation de la clé publique de la personne physique est la clé publique en clair.

Dans les IGCP traditionnelles, le certificat de personne doit être au préalable signé par une Autorité de Certification (AC) ayant son propre certificat "racine" pré-embarqué dans les navigateurs Internet. Si l'autorité de certification signataire est "exotique" et non reconnue, l'acteur n'est pas en mesure de vérifier la validité de la clé publique présentée dans le certificat de personne.

Selon une source Wikipedia®, « Les certificats racines sont des clés publiques non signées, ou auto-signées, mais dignes de confiance. Des autorités de certification commerciales détiennent des certificats racines présents dans de nombreux logiciels, par exemple les navigateurs. Internet Explorer® ou Firefox® contiennent quelques certificats racines préinstallés. Quand le navigateur ouvre une connexion sécurisée (SSL) à un site ayant acheté une certification auprès d'une autorité connue, il considère que le site est sûr, et le passage en mode sécurisé est transparent. Si le certificat est auto-signé (autorité de certification et créateur de la clé publique ne font qu'un), le navigateur propose de l'examiner, puis de l'accepter ou de le refuser selon la confiance qu'on lui accorde. »

Selon l'invention, l'IGCP "utilisateur" propose que tout acteur connecté à Internet soit en mesure de vérifier la validité d'une clé publique proposée ou récupérée. Pour cela, l'acteur doit interroger le Notaire Electronique (spécifié dans le certificat de clé publique) en émettant une requête sur le serveur Notaire Electronique en ligne.

En cas d'indisponibilité temporaire du serveur du Notaire Electronique contenant le "certificat de propriété de clé publique" correspondant, le système n'est pas bloqué pour autant bien que la réponse de sécurité soit différée. En effet, rien n'empêche un acteur d'utiliser quand même la clé publique d'une personne, s'il décide de lui faire confiance. Il peut par exemple chiffrer un message à l'intention de cette personne ou bien vérifier un document, un message ou une transaction signée par cette même personne.

A l'échelle d'un pays comme la France, l'IGCP "2.0" réduit à quelques dizaines le nombre de serveurs "Notaire Electronique" à administrer et à protéger afin d'assurer l'infrastructure globale des clés publiques des personnes sur les plans de l'e-commerce (*B to C*), de l'e-administration et des échanges privés. C'est à la fois un nombre suffisant pour éviter une attaque d'envergure concentrée sur un seul point et suffisamment peu pour ne pas compliquer la gestion de l'ensemble.

Aujourd'hui, il est déjà possible d'assurer un niveau très élevé de disponibilité et d'intégrité des serveurs stratégiques, comme c'est déjà le cas pour les serveurs des grands acteurs du Web. Il n'existe donc pas de surcoût d'infrastructure lié à l'innovation présentée.

Dans le cas de l'IGCP "utilisateur", les clés et les certificats concernent individuellement les personnes physiques. On parle communément de certificats "client" ou de "certificats de personne" afin de les distinguer des certificats "serveur".

Selon les termes du Référentiel Général de la Sécurité (RGS) édité par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), « Un certificat électronique "serveur" est un fichier électronique attestant qu'une bi-clé [clé privée et sa clé publique associée] appartient à l'autorité administrative identifiée directement ou indirectement, dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'Autorité de Certification valide le lien entre l'autorité administrative, le nom de domaine du serveur et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Ce certificat "serveur" et cette bi-clé vont permettre au serveur les possédant et agissant pour le compte de cette autorité administrative de s'authentifier

vis à vis d'un poste "usager" (SSL mode client/serveur) ou d'un autre serveur (Services Web). Dans ce contexte le terme serveur ne désigne pas la machine elle-même mais le serveur applicatif ou le service ou le téléservice fonctionnant sur une machine. »

Dans une IGCP traditionnelle, selon les termes du Référentiel Général de la Sécurité (RGS) : « Un certificat électronique "particulier" est un fichier électronique attestant qu'une bi-clé appartient à la personne physique identifiée directement ou indirectement (pseudonyme) dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'autorité de certification valide le lien entre l'identité du particulier et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. »

Dans le cadre de la présente invention, les personnes physiques concernées sont des citoyens/consommateurs/professionnels, c'est-à-dire des particuliers.

Au niveau du cercle régalien, ce particulier doit être un citoyen français. Un étranger devra être enrôlé par l'Autorité d'Enregistrement régalienne de son pays d'origine. Pour les cercles "Banque, Finance et Assurance" et "Internet et Télécommunication", la notion de proximité devient la règle. Pour les citoyens de l'Union Européenne, la possession d'un compte bancaire dans une banque française ou d'un contrat auprès d'un opérateur télécom français suffit à légitimer son enrôlement par l'Autorité d'Enregistrement correspondante.

La présente invention ne change pas l'usage des clés cryptographiques. Les clés privées et les certificats de clé publique d'une personne vont lui permettre : de s'authentifier auprès d'un serveur (serveur applicatif, service ou téléservice fonctionnant sur une machine) ; de chiffrer un document pour en assurer la confidentialité à l'égard de tous, excepté lui-même ; de signer un document, une transaction ou un message.

Les clés publiques et les certificats de clé publique des autres personnes vont permettre à une personne donnée : d'authentifier un autre particulier, un employé, un agent ou un serveur ; de chiffrer un document, une transaction ou un message à destination d'un autre particulier, d'un

employé, d'un agent ou d'un serveur (confidentialité) ; de vérifier la signature apposée sur un document, une transaction ou un message par un autre particulier, un employé, un agent ou un serveur.

Au delà du citoyen/consommateur, ce système s'étend à des personnes physiques d'autres entités. Pour les entreprises, des certificats de propriété de clé publique de mandataires sociaux, de comptables, de trésoriers, de responsables de paye, etc. peuvent être délivrés par les Greffes de Tribunaux de Commerce.

Pour les commerçants et artisans, ils pourront être délivrés par La chambre des Métiers. Pour les professions libérales, ils seraient délivrés par la chambre des Métiers ou les Ordres professionnels (avocats, experts comptables, commissaires aux comptes, médecins, etc.). Pour les salariés ou fonctionnaires, lorsqu'ils interviennent nominativement (et non pas dans le cadre de leur fonction respective) ils seraient délivrés par les Prud'Hommes ou encore la Sécurité Sociale.

Le cycle de vie d'une clé et des certificats de personne associés comporte plusieurs phases : 1) Demande, 2) Génération, 3) Affectation, 4) Introduction, 5) Utilisation, 6) Fin de vie, 7) Renouvellement et 8) Recouvrement.

1) Demande. Le Particulier doit demander de façon explicite ou implicite la création pour son usage personnel de clés cryptographiques et des certificats correspondants. Cette demande correspond au début du cycle de vie d'une clé et d'un certificat. La formalisation de cette demande peut être utile au suivi de la clé ou du certificat dans son cycle de vie.

Le Particulier n'a pas forcément conscience de l'intérêt ou l'utilité posséder des clés et des certificats cryptographiques pour profiter des services d'Internet. La notion de "clé de sécurité pour Internet" est peut-être plus simple à comprendre. Cette demande correspond à une démarche volontaire de la part du Particulier. Elle peut toutefois être proposée à l'utilisateur lors d'un passage dans une Agence Locale d'Enregistrement (ALE), par exemple lors de la souscription à un abonnement de téléphonie mobile. A cette occasion, le téléphone mobile

peut devenir le support privilégié du certificat de clé publique et de la clé privée de l'utilisateur.

2) Génération. L'opération de génération des clés dépend des algorithmes cryptographiques utilisés. Celle des certificats dépend des normes adoptées. La génération des clés peut être effectuée de façon individuelle, décentralisée ou centralisée. Génération individuelle : le Particulier utilise localement un outil logiciel mis à sa disposition dans le sélecteur d'identité de son ordinateur, dans son téléphone mobile ou son "Smartphone". Génération décentralisée : le Particulier se rend physiquement à son Agence Locale d'Enregistrement qui procède pour le compte du Particulier à la génération de ses clés. Génération centralisée : une Autorité d'Enregistrement commune à tous les Particuliers - une au moins par cercle de confiance - génère les clés de chaque Particulier et se charge de leur délivrer.

La génération individuelle est privative avec un contrôle total du Particulier. L'absence de connexion avec Internet est recommandée pendant le processus de génération. Elle nécessite toutefois des utilisateurs avertis.

La génération décentralisée est effectuée dans un environnement de confiance. Le Particulier est néanmoins présent lors du processus de génération. Dans ce cas, le Particulier doit faire confiance à un tiers (l'Agence Locale d'Enregistrement par délégation de son Autorité d'Enregistrement) pour la génération de ses éléments secrets et privés.

La génération centralisée est effectuée sans aucun contrôle du Particulier. Ce schéma n'est pas idéal pour rassurer les particuliers. De plus, l'opération de délivrance des clés (une fois générées) à chaque Particulier implique une logistique lourde et coûteuse. Cette procédure n'apparaît pas la plus optimale, en termes de perception utilisateur ou de coût de mise en place.

La génération de clé aléatoire peut se faire de deux façons : indirectement par le procédé de dérivation de clé, directement par un générateur d'aléa. La dérivation de clé consiste à utiliser un procédé cryptographique pour obtenir à partir d'une clé dite maître et d'éléments publics d'identification de l'utilisateur final une clé secrète ou privée. Ce

procédé est déconseillé car il affaiblit la sécurité (la sécurité est alors limitée à l'entropie et à la complexité de la clé maître qui est en général un mot de passe mémorisable donc plutôt court et faible).

La génération de clé aléatoire consiste à utiliser un générateur d'aléa pour fabriquer selon un procédé cryptographique les clés secrètes, privées et publiques.

En prenant bien soin d'être hors ligne, c'est-à-dire déconnecté de tout réseau et d'Internet, le Particulier, qui sera appelé par exemple Alice, utilise ce programme pour générer chez lui (ou à l'Agence Locale d'Enregistrement) sa paire de clés ou bi-clé : une privée et une publique : $K_{pri}A$ et $K_{pub}A$, où A correspond à Alice, K_{pri} à la clé privée et K_{pub} à la clé publique.

3) Affectation. Une fois une clé cryptographique générée, son admission dans le système d'information est une opération cruciale en termes de sécurité. Cette opération associe à une valeur numérique : l'identité du Particulier auquel elle est affectée, l'usage qui lui est dévolu (signature, chiffrement, échange de clé...). Pour des raisons de sécurité, la séparation des usages authentification et signature est recommandée.

L'IGCP "utilisateur" préconise, pour chaque particulier, le stockage sur un support physique d'authentification et de signature de deux couples de bi-clé : le premier pour l'authentification (avec présomption de fiabilité) ; le second pour la signature électronique afin de valider une transaction en marquant son consentement.

Les deux clés privés sont stockées de façon sécurisée : soit en étant chiffrées et stockées dans une mémoire à accès libre, soit en étant stockées en clair dans une mémoire sécurisée avec contrôle d'accès, soit en étant stockées chiffrées dans une mémoire sécurisée avec contrôle d'accès. Le dernier cas étant préférable.

Les certificats de clé publique X.509v3 auto-signés sont stockés en clair. Le premier est un certificat d'authentification. Le second est un certificat de signature dont la valeur juridique découle de la Directive Européenne 1999/93.

L'opération d'affectation devient cruciale lorsqu'il s'agit de la première admission dans le système. Dans ce cas, il s'agit du premier enrôlement du particulier dans un système.

Comme le stipule l'ANSSI dans le RGS : « La sécurité de l'opération ne peut résulter que de procédés non cryptographiques, de nature physique et organisationnel. C'est lors de ce premier enrôlement que seront affectés au Particulier les premiers éléments cryptographiques permettant ultérieurement de le reconnaître de façon sûre et de lui affecter de nouvelles clés. »

C'est bien ce à quoi s'attache la présente invention, afin de garantir un enrôlement dit "en face à face" et non de façon distante par télécommunication ou par correspondance.

L'opération de génération des certificats dépend des normes adoptées. La génération des certificats peut aussi être effectuée de façon individuelle, décentralisée ou centralisée. Génération individuelle : pour le certificat de clé publique qui n'est plus signé par une Autorité de Certification, le Particulier utilise localement un outil logiciel certifié et mis à sa disposition dans le sélecteur d'identité de son ordinateur ou dans son téléphone mobile. Génération décentralisée : le Particulier se rend physiquement à son Agence Locale d'Enregistrement qui procède pour le compte du Particulier à la création de son "certificat de clé publique" et de son "certificat de propriété de clé publique". Génération centralisée : une Autorité d'Enregistrement commune à tous les Particuliers - au moins une par cercle de confiance - génère les certificats de chaque Particulier et se charge de leur délivrer.

L'IGCP "utilisateur" ne préconise pas la procédure centralisée pour trois raisons : elle est effectuée sans aucun contrôle du Particulier (ce schéma n'est pas fait pour rassurer les particuliers) ; l'opération de délivrance des certificats (une fois créés) à chaque Particulier implique une logistique lourde et coûteuse ; il est difficile pour le Particulier de prouver son identité à l'Autorité d'Enregistrement, éloignée géographiquement (envoi de photocopies de pièces d'identité qui peuvent être compromises...).

La procédure individuelle permet bien de créer un "certificat de clé publique" auto-signé, mais non pris en charge par une Autorité de Certification comme cela prévu dans le protocole IGCP "utilisateur". Elle ne permet pas de créer un "certificat de propriété de clé publique". Elle ne permet pas surtout de l'introduire dans le système car il ne peut pas être publié sur un serveur Notaire Electronique. L'IGCP "utilisateur" ne préconise pas cette procédure.

La procédure décentralisée permet de créer un "certificat de clé publique" auto-signé, non signé par une Autorité de Certification comme cela est prévu dans le protocole IGCP "utilisateur". Elle permet également de créer un "certificat de propriété de clé publique" avec vérification de son authenticité. Elle permet en outre son introduction dans le système (publication sur le serveur Notaire Electronique). L'IGCP "utilisateur" préconise cette procédure.

Le Particulier (Alice) se rend physiquement à son Agence Locale d'Enregistrement (ALE). C'est là qu'Alice va pouvoir obtenir deux certificats : son "certificat de clé publique", son "certificat de propriété de clé publique".

La présente invention propose un processus en trois étapes.

Première étape, le Particulier Alice présente une ou plusieurs pièces d'identité (passeport, Carte Nationale d'Identité, permis de conduire...) à l'agent d'enregistrement qui les valide et authentifie physiquement Alice. Cette étape de vérification d'identité est indispensable pour établir un vrai système de confiance. A contrario, une IGCP "internationale" ou "reconnue" peut difficilement proposer cette démarche physique à tous car elle ne dispose pas d'Agences Locales d'Enregistrement de proximité réparties sur tout le territoire.

Deuxième étape, le Particulier Alice utilise le programme (certifié) de certification de l'Agence Locale d'Enregistrement pour générer son "certificat de clé publique". Ce certificat est lisible et auto-signé par la clé privée d'Alice.

Ce "certificat de clé publique" contient notamment : {nationalité du tiers (FR), type de tiers (Autorité d'Enregistrement), nature du tiers (exemple Banque, Assurance, Opérateur télécom...), cercle de confiance

du tiers, horodatage, identité d'Alice, $K_{pub}A$, auto-signature}. Ce certificat respecte le format X.509v3 pour être compatible avec le standard international.

Troisième étape, le Particulier Alice utilise le programme (certifié) de l'Agence Locale d'Enregistrement pour garantir la propriété légitime de sa clé publique : qu'Alice a apportée dans sa clé USB, sa carte à puce ou son téléphone mobile (procédure de génération individuelle), ou qu'Alice vient juste de générer à l'Agence Locale d'Enregistrement (procédure de génération décentralisée).

L'agent d'enregistrement saisit dans le programme l'identité du Particulier Alice (par exemple les nom et prénoms d'Alice, ses date et lieu de naissance, sa nationalité) et précise les emplacements respectifs de la clé publique et de la clé privée d'Alice (en pointant sur les fichiers correspondants dans la clé USB, la carte à puce ou le mobile d'Alice).

Le programme calcule l'empreinte (e) de la clé publique d'Alice avec une fonction de hachage à sens unique de type RIPE-MD ou SHA-256 :

$H(K_{pub}A) = e_{pub}A$, avec H la fonction de hachage à sens unique.

Le certificat de propriété de clé publique est alors composé de la manière suivante :

{nationalité du tiers (FR), type de tiers (Autorité d'Enregistrement), nature du tiers, cercle de confiance du tiers, horodatage, identité d'Alice, $e_{pub}A$}.

Ce certificat de propriété est ensuite scellé avec la clé privée d'Alice (signature opaque). C'est-à-dire chiffré avec la clé privée d'Alice, stockée dans sa clé USB, sa carte-à-puce ou son mobile et jamais montrée à l'agent d'enregistrement.

L'IGCP "utilisateur" établit la responsabilité du Particulier (citoyen/consommateur/professionnel) et dispose qu'il (le Particulier) certifie lui-même la propriété de sa clé publique, sous le contrôle d'une Autorité d'Enregistrement (représentée par son ALE) mais sans l'intervention d'une quelconque Autorité de Certification.

Cela donne :

$E(K_{pri}A$, {nationalité du tiers (FR), type de tiers (Autorité d'Enregistrement), nature du tiers, cercle de confiance du tiers, horodatage, identité d'Alice,

$e_{pub}A\}$) = [nationalité du tiers (FR), type de tiers (Autorité d'Enregistrement), nature du tiers, cercle de confiance du tiers, horodatage, identité d'Alice, $e_{pub}A$].

Notation : E algorithme de chiffrement asymétrique ; { } signifie un certificat ouvert et lisible ; [ ] signifie un certificat fermé et chiffré (scellé) donc illisible en l'état.

La présente invention institue un "certificat de propriété de clé publique" de Particulier personne physique avec les caractéristiques suivantes : il ne contient pas la clé publique de ce Particulier mais seulement l'empreinte de cette clé ; il est scellé (chiffré) avec la propre clé privée du Particulier et n'est pas signé avec la clé privé d'une quelconque Autorité de Certification.

4) Introduction. Selon le RGS de l'ANSSI, « Une fois que son rôle a été correctement défini, un autre aspect de la gestion d'une clé consiste à l'introduire physiquement ou logiquement dans l'ensemble du système applicatif. Cet aspect recouvre la distribution et le transport de la clé jusqu'à l'utilisateur ou à l'équipement, puis son injection éventuelle dans l'environnement de confiance du Particulier. L'introduction est donc l'opération qui fait passer la clé affectée du système de gestion de clés proprement dit au système applicatif qui va l'utiliser. »

Le Particulier possède maintenant sa clé privée et son "certificat de clé publique" sur son support de clés.

La présente invention crée un module automatique, intégré au sélecteur d'identité ou au programme certifié de l'ALE, qui a pour fonction de publier auprès des fournisseurs d'identité et des annuaires la nouvelle clé publique (certificat de clé publique) du Particulier afin d'intégrer rapidement la confiance dans sa vie numérique.

Selon la présente invention, l'agent d'enregistrement a pour tâche de publier le "certificat de propriété de clé publique" du Particulier sur le serveur "Notaire Electronique" de l'Autorité d'Enregistrement à laquelle il appartient.

Selon la présente invention, le serveur Notaire Electronique contient un annuaire centralisé (ou une base de données) de tous les

"certificats de propriété de clé publique" des Particuliers servis par le réseau de proximité de ses Agences Locales d'Enregistrement.

Selon la présente invention, chacun des enregistrements de cette base comprend une valeur d'index du certificat (le numéro du certificat), le certificat de propriété de clé publique et une empreinte des deux valeurs précédentes chiffrée par la clé privée du Notaire Electronique. Cette clé privée du Notaire Electronique est liée à un certificat émis par l'Autorité de Certification interne de l'Autorité d'Enregistrement à laquelle le serveur appartient. Cette signature permet de préserver l'intégrité de l'annuaire.

Dans ces conditions, la clé publique de chacun des serveurs Notaire Electronique (certifiée par une autorité de certification reconnue) permet alors de vérifier qu'un enregistrement de sa base/annuaire est bien légitime et non un ajout ou une substitution effectué frauduleusement par un pirate.

Selon la présente invention, l'agent d'enregistrement fait partie de l'IGCP "interne" de son Autorité d'Enregistrement. Ce qui lui permet de signer son envoi au serveur Notaire Electronique qu'il a préalablement authentifié, afin de publier le "certificat de propriété de clé publique" du Particulier en toute sécurité. Le Notaire Electronique ne publie donc que des "certificats de propriété de clé publique" de Particuliers, émis par ses propres agents d'enregistrement autorisés. Par exemple, une IGCP "interne" existe déjà pour les Notaires de France (cercle Régalien).

La sécurité des échanges entre l'ALE et son serveur Notaire Electronique est assuré en ce que :

- Le serveur Notaire Electronique est authentifié par l'ALE grâce au certificat de clé publique dudit serveur, délivré par lui-même (IGCP interne).

- L'ALE est authentifiée par le serveur Notaire Electronique grâce au certificat de clé publique de ladite ALE, délivré par l'Autorité d'Enregistrement (IGCP interne).

- La confidentialité des échanges est obtenue par le chiffrement des données transmises, par exemple grâce au protocole TLS 1.0, initié par le serveur.

5) Utilisation. Selon le RGS de l'ANSSI, « De par leur nature même, les éléments privés ou secrets ne peuvent être employés que dans un environnement de confiance. Cet environnement est en effet responsable du stockage des clés et de leur bonne gestion pendant la durée où elles sont utilisées. Il peut en découler notamment des exigences quant à la protection de l'environnement de confiance applicatif.»

Il existe trois types d'utilisation des clés : chiffrement/déchiffrement pour la confidentialité, signature électronique, authentification (par cryptographie asymétrique, par mot de passe à usage unique ou *One Time Password*, OTP).

Déroulement du processus de chiffrement/déchiffrement pour la confidentialité dans la présente invention.

Selon la présente invention, on prévoit un module de requête qui prend en entrée le certificat de clé publique de la personne physique, interroge le serveur notaire électronique dont l'adresse figure dans ledit certificat de clé publique, en communiquant le numéro de ce certificat de clé publique et la clé publique incluse dans ledit certificat de clé publique, et qui reçoit en retour de la part du serveur notaire électronique dont l'adresse figure dans ledit certificat de clé publique une assertion sur l'authenticité ou la non-authenticité de la prétendue clé publique de la personne physique.

Selon la présente invention, le module de requête est placé par exemple dans les navigateurs internet, les logiciels de messagerie électronique, les serveurs fournisseurs d'identité (IDP, IP/STS), les applications informatiques, les processus informatiques.

Selon la présente invention, on prévoit un module de réponse qui est installé sur tous les serveurs notaire électronique, qui reçoit en entrée la requête du module de requête, qui recherche dans la base de données dudit serveur notaire électronique s'il existe un numéro de certificat de propriété de clé publique identique au numéro de certificat de clé publique reçu et qui

délivre une assertion « la clé publique n'est pas authentique » si le résultat de la recherche est négatif.

Selon la présente invention, on prévoit un module de réponse qui est installé sur tous les serveurs notaire électronique, qui reçoit en entrée la requête du module de requête, qui recherche dans la base de données dudit serveur notaire électronique s'il existe un numéro de certificat de propriété de clé publique identique au numéro de certificat de clé publique reçu, en ce que si le résultat de la recherche est positif, ce module de réponse fait une tentative de déchiffrement du certificat de propriété de clé publique trouvé avec la clé publique reçue et délivre une assertion « la clé publique n'est pas authentique » si le déchiffrement ne réussit pas ou une assertion « la clé publique est authentique» si le déchiffrement réussit.

Selon la présente invention, on prévoit un module de réponse qui est installé sur tous les serveurs notaire électronique, qui reçoit en entrée la requête du module de requête, qui recherche dans la base de données dudit serveur notaire électronique s'il existe un numéro de certificat de propriété de clé publique identique au numéro de certificat de clé publique reçu, en ce que si le résultat de la recherche est positif, ledit module de réponse fait une tentative de déchiffrement du certificat de propriété de clé publique trouvé avec la clé publique reçue, en ce que si le déchiffrement réussit, ledit module de réponse calcule l'empreinte de la clé publique reçue, puis la compare avec l'empreinte de la clé publique stockée dans le certificat de propriété de clé publique préalablement déchiffré et en ce que ledit module de réponse délivre une assertion « la clé publique n'est pas authentique », si les deux empreintes sont différentes ou une assertion « la clé publique est authentique », si les deux empreintes sont identiques.

Voici les étapes selon l'invention, lorsque qu'un Particulier, appelé Bernard, ou un fournisseur de service (SP/RP) souhaite envoyer un message secret à un autre Particulier appelé Alice.

Bernard se procure le certificat de clé publique d'Alice : soit en consultant un fournisseur d'identité (IDP/IP) de son cercle de confiance, soit en consultant un des annuaires de certificats de clé publique où Alice l'a déjà publié, soit directement auprès d'Alice.

Bernard doit maintenant s'assurer que cette clé publique « $K_{pub}X$ » écrite dans le "certificat de clé publique" d'Alice est bien celle d'Alice et qu'un pirate n'est pas déjà passé par là pour substituer sa propre clé publique à celle d'Alice (ou bien par la fameuse attaque de l'intercepteur dite encore « man-in-the-middle »).

Bernard récupère d'abord le numéro du certificat et la clé publique « $K_{pub}X$ » lisible dans le certificat, prétendument celle d'Alice. Bernard envoie une requête en temps réel au serveur du Notaire Electronique indiqué dans le "certificat de clé publique" pour consulter le "certificat de propriété de clé publique" d'Alice qui y est normalement stocké.

S'il n'existe pas de "certificat de propriété de clé publique" d'Alice sur le serveur Notaire Electronique indiqué (aucune correspondance du numéro de certificat dans la base ou l'annuaire), la validité de la clé publique d'Alice en possession de Bernard n'est pas prouvée.

Si le "certificat de propriété de clé publique" d'Alice existe bien sur le serveur Notaire Electronique indiqué (correspondance du numéro de certificat dans la base ou l'annuaire), ce certificat est fermé. La requête envoyée par Bernard va utiliser « $K_{pub}X$ » pour tenter de l'ouvrir : E($K_{pub}X$, [nationalité du tiers (FR), type de tiers (Autorité d'Enregistrement), nature du tiers, cercle de confiance du tiers, horodatage, identité d'Alice, $e_{pub}A$]) = {nationalité du tiers (FR), type de tiers (agent d'enregistrement), nature du tiers, cercle de confiance du tiers, horodatage, identité d'Alice, $e_{pub}A$}.

Si la clé publique ($K_{pub}X$) récupérée dans le "certificat de clé publique" d'Alice est bien la clé publique originale d'Alice ($K_{pub}A$) alors le "certificat de propriété de clé publique" s'ouvre, contrairement à n'importe quelle autre clé publique fallacieuse qui ne pourra pas ouvrir ce certificat.

Selon la présente invention, le module serveur calcule alors l'empreinte de la clé publique reçue dans la requête : $H(K_{pub}X) = e_{pub}X$. Cette valeur est ensuite comparée à l'empreinte stockée dans le "certificat de propriété de clé publique" d'Alice qui vient d'être ouvert. Si les deux empreintes sont égales ($e_{pub}X = e_{pub}A$) alors la réponse à la requête de Bernard spécifie que la clé publique envoyée dans sa requête est bien la clé publique originale d'Alice, "certifiée" (scellée pour être exact) par elle-même et garantie par le serveur du Notaire Electronique.

Ainsi, Bernard est vraiment sûr qu'il a bien récupéré la clé publique authentique d'Alice. Il ne lui reste plus qu'à chiffrer son message secret pour Alice avec la clé publique authentique d'Alice et s'en remettre avec confiance au fait que seule Alice possède bien l'unique clé privée ($K_{pri}A$) capable de déchiffrer correctement son message. La confidentialité du message de Bernard pour Alice est alors garantie.

La sécurité des échanges entre le client requêteur et le serveur Notaire Electronique est assuré en ce que :

- Le serveur Notaire Electronique est authentifié par le client grâce au certificat de clé publique dudit serveur, délivré par une Autorité de Certification reconnue.

- La confidentialité des échanges est obtenue par le chiffrement des données transmises, par exemple grâce au protocole TLS 1.0, initié par le serveur.

- L'intégrité de l'URL du serveur Notaire Electronique contenue dans le certificat de clé publique est vérifiable par la signature dudit certificat.

Déroulement du processus de signature électronique dans la présente invention.

Voici les étapes selon l'invention, lorsque qu'un acteur (un Particulier, appelé Bernard, ou un fournisseur de service (SP/RP) souhaite vérifier la signature d'un autre Particulier appelé Alice. Cette entité a besoin de la clé publique authentique d'Alice afin de vérifier sa signature sur une transaction. Cette transaction a été horodatée et signée avec la clé privée d'Alice.

L'entité se procure le certificat de clé publique d'Alice : soit en consultant un fournisseur d'identité (IDP/IP) de son cercle de confiance, soit en consultant un des annuaires de certificats de clé publique où Alice l'a déjà publié, soit directement auprès d'Alice.

L'entité doit maintenant s'assurer que cette clé publique « $K_{pub}X$ » écrite dans le "certificat de clé publique" d'Alice est bien celle d'Alice et qu'un pirate n'est pas déjà passée par là pour substituer sa propre clé publique à celle d'Alice (ou bien par la fameuse attaque de l'intercepteur dite encore « man-in-the-middle »).

Le processus de vérification de la validité de la clé publique d'Alice est exactement le même que celui détaillé dans le cas précédent.

A l'issue de ces étapes, l'entité est vraiment sûre qu'elle a bien récupéré la clé publique authentique d'Alice. Il ne reste plus à l'entité qu'à vérifier la signature d'Alice avec la clé publique authentique d'Alice et s'en remettre avec confiance au fait que seule Alice possède bien l'unique clé privée ($K_{pri}A$) capable d'avoir signé correctement la transaction en question. La signature de la transaction par Alice est alors garantie.

Déroulement du processus d'authentification d'Alice à l'aide de la cryptographie asymétrique dans la présente invention.

Voici les étapes selon l'invention, lorsque qu'un acteur (un Particulier, appelé Bernard, ou un fournisseur de service (SP/RP) souhaite vérifier la signature d'un autre Particulier appelé Alice. Cette entité a besoin de la clé publique authentique d'Alice afin de vérifier le chiffrement opéré par la clé privée d'Alice lors d'un protocole défi-réponse.

Après une première phase d'identification d'Alice auprès du serveur de l'entité, le serveur envoie un aléa (le défi) à Alice qui le chiffre avec sa clé privée ($K_{pri}A$) pour obtenir la réponse qu'elle envoie au serveur. Pour déchiffrer la réponse obtenue et retrouver son défi d'origine, le serveur a besoin de la clé publique d'Alice.

L'entité se procure le certificat de clé publique d'Alice : soit en consultant un fournisseur d'identité (IDP/IP) de son cercle de confiance, soit en consultant un des annuaires de certificats de clé publique où Alice l'a déjà publié, soit directement auprès d'Alice.

L'entité doit maintenant s'assurer que cette clé publique « $K_{pub}X$ » écrite dans le "certificat de clé publique" d'Alice est bien celle d'Alice et qu'un pirate n'est pas déjà passée par là pour substituer sa propre clé publique à celle d'Alice (ou bien par la fameuse attaque de l'intercepteur dite encore « man-in-the-middle »).

Le processus de vérification de la validité de la clé publique d'Alice est exactement le même que celui détaillé dans le cas précédent.

A l'issue de ces étapes, l'entité est vraiment sûre qu'elle a bien récupéré la clé publique originale d'Alice. Il ne reste plus à l'entité qu'à déchiffrer la réponse (au défi) envoyée par Alice avec la clé publique originale d'Alice. Si la valeur ainsi déchiffrée est la même valeur que l'aléa (le défi) envoyé au préalable, alors l'entité peut être sûre que seule Alice possède bien l'unique clé privée ($K_{pri}A$) capable d'avoir chiffré correctement le défi pour en faire une réponse valable. Alice est bien authentifiée par l'entité.

6) Fin de vie. Selon le RGS de l'ANSSI, « La fin de vie d'une clé cryptographique donne lieu à une révocation, un retrait, voire une destruction. Révoquer une clé n'est pas synonyme de retrait en ce sens qu'une clé peut avoir été révoquée et continuer d'être utilisée pour des opérations de vérification ou de compatibilité ascendante. De même le retrait ne signifie pas forcément que la clé ne sera plus jamais utilisée : elle peut être archivée pour permettre, par exemple, de mener une enquête postérieurement à son retrait. »

Selon la présente invention, un certificat de propriété de clé publique est émis sans durée de fin de validité. Tant qu'il est présent sur le serveur du Notaire Electronique, il est considéré comme valide et peut être consulté en ligne par quiconque (fournisseurs d'identité, organisations, particuliers) pour s'assurer de la valeur de la clé publique et de son appartenance à la bonne personne.

Selon la présente invention, le Particulier retrouve la maîtrise de ses éléments de sécurité et redevient responsable de son identité. Personne d'autre que lui n'est en droit de mettre fin à ce certificat de propriété.

Le problème récurrent de la gestion complexe des listes de certificats révoqués dans l'IGCP traditionnelle (CRL *Certificate Revocation List*) ne se pose plus.

En cas de perte, de compromission ou de vol de sa clé privée, le Particulier doit bien évidemment réagir en demandant le plus tôt possible auprès de son Agence Locale d'Enregistrement la suppression de la publication de son certificat de propriété sur le serveur Notaire Electronique.

7) Renouvellement. Selon le RGS de l'ANSSI, « Le renouvellement d'une clé cryptographique est un processus à prévoir dès la conception d'un système d'information. Ce renouvellement peut intervenir de façon normale ou provoquée par des événements fortuits comme une compromission. »

Selon la présente invention, en cas de perte, de compromission ou de vol de sa clé privée, le Particulier doit d'abord demander auprès de son Agence Locale d'Enregistrement la suppression de la publication de son certificat de propriété de clé publique sur le serveur Notaire Electronique. Seule une Agence Locale d'Enregistrement (ALE) liée au Notaire Electronique est en mesure de donner un ordre de suppression d'un certificat de propriété de clé publique. Seul le Particulier peut mandater son ALE pour le faire.

Selon la présente invention, un formulaire papier de révocation pré-affranchi, délivré lors de l'enrôlement du Particulier peut également être un vecteur de révocation. Ce formulaire à poster comprend deux volets : un pour la centrale de l'AE, un pour l'ALE. Un seul quelconque sur les deux permet la suspension de la publication du certificat de propriété de clé publique sur le serveur NE. La combinaison des deux permet de supprimer le certificat de propriété de clé publique sur le serveur NE après une ultime vérification auprès du Particulier.

La suite logique de la démarche est la génération d'une nouvelle bi-clé, d'un nouveau "certificat de clé publique" et du nouveau "certificat de propriété de clé publique" correspondant.

L'usage du module automatique de publication de sa nouvelle clé publique (certificat de clé publique) auprès des fournisseurs d'identité et

des annuaires facilite la vie du Particulier lors de la phase de renouvellement.

7) Renouvellement. Selon le RGS de l'ANSSI, « Le recouvrement de clé est une opération qui peut avoir pour objectif d'assurer la disponibilité d'un service ou de répondre à des exigences légales. Ce type de fonctionnalité est d'autant plus difficile à mettre en œuvre que ses objectifs sont par nature contraires aux objectifs de sécurité visés par ailleurs. La définition précise de la fonctionnalité visée est indispensable de même qu'une expertise cryptographique globale. »

Le Cabinet « Baker & McKenzie » apporte son expertise sur le sujet du séquestre des clés. « La question du séquestre des clés est vrai problème notamment dans le cadre de la lutte contre la cybercriminalité. Aujourd'hui, à notre connaissance, aucune société n'assure cette fonction de séquestre pour le compte de la justice. Cette obligation de séquestre semble résulter de l'article 434-15-2 du Code Pénal, selon lequel toutes les personnes amenées à connaître d'une convention secrète, c'est-à-dire le titulaire, l'émetteur, le ou les destinataires des messages chiffrés et les prestataires de services de cryptographie (et donc également les fournisseurs de clés de signature asymétriques), ont l'obligation de remettre et de mettre en œuvre les conventions secrètes aux autorités judiciaires. Il y a un risque dans le cas où l'utilisateur est gardien des clés qu'il soit dans l'impossibilité de s'acquitter de ses obligations légales dans le cas où il a perdu ses clés ou les a détruit involontairement. »

Un autre usage de la présente invention permet de sécuriser le Portefeuille De Cartes (PoDeCa) d'un Particulier en combinant les certificats de clé publique et de propriété de clé publique.

Le processus est le suivant.

1) Le contenu du PoDeCa est en clair.

2) L'utilisateur légitime du PoDeCa souhaite chiffrer le contenu du PoDeCa et transmet son certificat de clé publique "utilisateur" au PoDeCa.

3) Le Sélecteur d'identité requête le serveur Notaire Electronique mentionné dans le certificat.

4) Le serveur Notaire Electronique prouve son identité au Sélecteur d'identité grâce à son certificat serveur délivré par une Autorité de

Certification reconnue (certificat SSL/TLS, *Secure Socket Layer/Transport Layer Security*).

5) Le serveur Notaire Electronique envoie la réponse à la requête sur le certificat de propriété de l'utilisateur au Sélecteur d'identité.

6) En cas de réponse positive sur la validité de la clé publique et son appartenance, le contenu du PoDeCa est chiffré par le Sélecteur d'identité avec cette clé publique, verrouillant ainsi l'accès à son contenu à toute personne autre que le détenteur de la clé privée correspondante (c'est-à-dire l'utilisateur légitime).

7) Le propriétaire légitime du PoDeCa est seul en mesure de déchiffrer le contenu du PoDeCa avec sa clé privée.

Ce qui est important grâce à 3), 4), 5) et 6) c'est que personne hormis l'utilisateur légitime ne peut chiffrer le contenu du PoDeCa et ainsi empêcher l'usage légitime d'un PoDeCa "ouvert" à l'origine.

La CNIE (Carte Nationale d'Identité Electronique) ou *e-ID Card* existe déjà dans de nombreux pays et est en projet dans de nombreux autres. La cohabitation avec la présente invention est donc inévitable et doit être abordée.

On peut considérer que la *e-ID Card* doit être employée essentiellement pour des démarches à enjeu important dont l'objet concerne le Régalien ou bien les Collectivités Territoriales. Le déploiement de "Terminaux Point Administratif" (TPA) dans les relais et les centres administratifs à l'instar des Terminaux Point de Vente (TPV) dans les commerces actuels est une voie à privilégier. Le reste des démarches administratives à enjeu plus faible se fait par Internet, sans utilisation obligatoire de la *e-ID Card*. Il est difficile en effet d'imaginer à court terme dans certains pays un déploiement massif de lecteurs de cartes à puce auprès d'une population très nombreuse. Ce projet a déjà été maintes fois envisagé par le passé dans d'autres contextes mais n'a jamais abouti.

Selon l'invention, les deux systèmes, *e-ID Card* et IGCP "2.0" doivent cohabiter de la façon suivante.

L'*e-ID Card* est utilisée pour les démarches administratives physiques à enjeu dans les centres et relais administratifs tous équipés de

TPA. L'*e-ID Card* est utilisée pour les démarches administratives en ligne lorsque l'utilisateur disposera d'un lecteur de carte à puce. L'*e-ID Card* est utilisée au choix de l'utilisateur pour d'autres services en ligne lorsque l'utilisateur disposera d'un lecteur de carte à puce.

Le certificat de clé publique "utilisateur" pourra être utilisé au choix de l'utilisateur pour des services en ligne (tous supports physiques confondus). Le certificat de clé publique "utilisateur" pourra être utilisé au choix de l'utilisateur pour des démarches administratives en ligne avec faible enjeu autorisées par l'Etat (tous supports physiques confondus).

L'absence de déploiement à grande échelle des IGCP actuelles au niveau du Particulier (citoyen/consommateur/professionnel) tient davantage à des problèmes d'organisation et de coût qu'à des problèmes liés à une technologie déjà éprouvée.

L'IGCP à trois niveaux propose une architecture multi-niveaux et de nouveaux protocoles cryptographiques qui adressent le niveau des Particuliers et définit une nouvelle organisation. Cette nouvelle organisation est à la fois plus réaliste sur un plan pratique et implique une réduction significative des coûts.

La présente invention implique et responsabilise davantage le Particulier que dans le cadre d'une IGCP traditionnelle. Toutefois, elle préserve le Particulier de la complexité du modèle actuel ou le rôle des Autorités de Certification apparait nébuleux.

Le modèle économique de l'invention prévoit la gratuité du service de base ou, au maximum, un prix correspondant au coût de la délivrance du certificat de propriété de clé publique. Des options proposées par les Agences Locales d'Enregistrement (ALE) peuvent être payantes, parmi lesquelles : la fourniture de l'authentifieur physique (par exemple, clé USB, crypto-clé USB, carte à puce...), le délai de la publication du certificat de propriété de clé publique sur le serveur Notaire Electronique (par exemple, gratuit sous 48 heures, payant sous 4 heures), la remise d'un formulaire pré-affranchi de demande de révocation du certificat de propriété de clé publique, la publication automatique par l'ALE du certificat de clé publique du Particulier sur les principaux annuaires de clé publique et fournisseurs d'identité (IDP et IP/STS) de son choix, etc.

Le modèle économique de l'invention supprime le coût récurrent d'une redevance annuelle comme c'est le cas actuellement avec les certificats payants des Autorités de Certification privées.

Le modèle économique de l'invention diminue le coût de l'IGCP pour le Particulier (gratuit pour le service de base et peu onéreux avec les options) pour permettre son adoption à grande échelle.

D'autres inconvénients des IGCP traditionnelles sont connus, et notamment sur l'Autorité de Certification (AC) qui constitue la clé de voute de sa sécurité. En effet, la clé privée de l'AC qui signe les certificats de personne supporte à elle-seule tout le poids de la sécurité.

Selon le RGS de l'ANSSI, « Dans beaucoup de systèmes cryptographiques, notamment ceux faisant intervenir des tiers de confiance, il existe une ou plusieurs clés dont la compromission ou l'atteinte à l'intégrité peut entraîner des atteintes aux objectifs de sécurité de tout ou d'une grande partie des acteurs du système. Il s'agit par exemple des clés maîtres d'un système de dérivation de clé, d'une clé de réseau ou de la clé privée d'une autorité de certification. Nous parlerons dans ce cas de clé présentant un risque d'impact systémique ou de façon plus concise de *clé à risque systémique*. [...] Cette règle vise à sensibiliser les concepteurs au risque qu'il y aurait à faire reposer l'ensemble d'un système cryptographique sur une clé à risque systémique sans prévoir le cas où les objectifs de sécurité sur cette clé seraient remis en cause. [...] Aucun dispositif purement technique n'est à même de protéger de façon satisfaisante une clé présentant un risque systémique. [...] L'expérience prouve qu'une étude systématique de l'impact de chaque clé apporte beaucoup pour l'amélioration de la robustesse du système, notamment en identifiant justement les clés présentant un impact systémique. »

La compromission de la clé privée d'une Autorité de Certification (AC) revient à rendre obsolète l'ensemble des certificats émis jusqu'à ce jour par cette AC. Assurer la sécurité de la clé privée de l'AC (dont la durée de vie est grande) pour la préserver d'un risque systémique est donc très coûteux. Ce coût est forcément répercuté sur le prix de la redevance annuelle des certificats de personnes.

Selon la présente invention, le poids de la sécurité est mieux réparti entre les acteurs. Il n'existe pas véritablement de clés à risque systémique. La sécurité du système n'en est que meilleure car l'enjeu collectif diminue, surtout lorsque de très nombreux Particuliers sont concernés.

Chaque particulier assume la responsabilité de la certification individuelle de sa clé publique. L'agent d'enregistrement, quant à lui, en garantit seulement le processus. L'Autorité d'Enregistrement ne supporte donc pas le poids des responsabilités d'une Autorité de Certification qui doit assumer l'ensemble des certificats de clé publique qu'elle a émis.

La présente invention introduit la notion de Notaire Electronique (NE). Le notaire électronique et l'Autorité de Certification (AC) sont tous deux des Tiers de Confiance (TC). Cela dit, une AC correspond à un type précis de tiers de confiance qui suit des règles spécifiques (clé privée de l'AC qui signe les certificats émis, CRL *Certificate revocation List*, protocole OCSP *On-line Certificate Status Protocol*) et a ses propres exigences de sécurité.

Le Notaire Electronique ne rentre pas dans cette catégorie : il est un annuaire (ou une base de données) de "certificats de propriété de clé publique" de son espace de confiance. Ses exigences de sécurité concernent sa disponibilité (comme tout serveur critique), son intégrité et son authenticité qui peuvent être facilement assurées par la signature de son contenu, c'est-à-dire des enregistrements de l'annuaire. Le Notaire Electronique ne détient pas la clé publique des personnes physiques et il n'a signé aucun certificat de clé publique. L'enjeu de la sécurité du Notaire Electronique est donc différent de celui d'une Autorité de Certification.

Le serveur Notaire Electronique possède : une bi-clé "interne" de son IGCP Interne pour ses échanges sécurisés avec ses propres Agences Locales d'Enregistrement ; une bi-clé "externe" dont la clé publique est certifiée par une AC "internationale" vérifiable par tous (Particulier avec son navigateur et Service sur Internet).

Selon la présente invention, la clé privée "externe" du Notaire Electronique est placée dans un HSM (*Hardware Security Module)* hors-ligne et signe chaque nouvel enregistrement publié ensuite sur le serveur

(en ligne) du NE. Chaque enregistrement correspond à un "certificat de propriété de clé publique" de la base. Ainsi chacun peut vérifier l'intégrité et l'authenticité du contenu proposé par le Notaire Electronique grâce au certificat de la clé publique externe du notaire électronique signé par une Autorité de Certification "reconnue".

Selon l'invention, un enregistrement de l'annuaire de "certificats de propriété de clé publique" du Notaire Electronique (NE) est composé des éléments suivants : un Numéro de série du certificat de propriété (ce numéro qui sert d'index ou d'identifiant à l'enregistrement est le même que celui du certificat de clé publique X.509v3 du Particulier) ; une Version qui indique à quelle version de la norme correspond ce certificat ; un Algorithme de scellement (identifiant de l'algorithme qui a servi à chiffrer/sceller le "certificat de propriété de clé publique") ; le Certificat de propriété de clé publique du Particulier (scellé) ; la Signature du Notaire Electronique sur l'ensemble des champs précédents (et donc sur la totalité de l'enregistrement).

Selon l'invention, le protocole de vérification par une entité de la clé publique d'un Particulier (nommé Alice) est le suivant :

1) Récupération du certificat de clé publique d'Alice (comment être sûr que cette clé publique $K_{pub}X$ écrite dans le certificat de clé publique d'Alice est bien celle d'Alice ?).

2) Lecture du numéro (de série) du certificat.

3) Lecture de la clé publique $K_{pub}X$ lisible dans le certificat.

4) Lecture de l'adresse du serveur du Notaire Electronique (dans par exemple X509v3 *CRL Distribution Points*) contenu dans le certificat de clé publique.

5) Requête en temps réel sur le serveur du Notaire Electronique pour lire le "certificat de propriété de clé publique" d'Alice à la valeur d'index égale au numéro de série du "certificat de clé publique".

6) Vérification de l'intégrité de l'enregistrement trouvé et authentification du Notaire Electronique qui l'a publié : vérification de la signature de l'enregistrement avec le certificat du Notaire Electronique présent dans le navigateur ou le serveur de l'Entité (en effet le Notaire Electronique signe

chaque enregistrement de son annuaire avec sa clé privée dont la clé publique correspondante a été certifiée par une AC "reconnue").

7) Si l'enregistrement est intègre et que le NE est bien authentifié, tentative d'ouverture du certificat de propriété avec la clé publique $K_{pub}X$.

8) Si $K_{pub}X = K_{pub}A$ (c'est-à-dire est la bonne) alors le certificat de propriété s'ouvre et devient lisible sinon il reste illisible (pas de divulgation d'information) : première vérification.

9) Calcul de l'empreinte de cette clé publique : $H(K_{pub}X) = e_{pub}X$.

10) Si le certificat de propriété est ouvert, comparaison de $e_{pub}X$ calculée à l'étape 9) avec l'empreinte lue dans le certificat $e_{pub}A$. Si égalité alors la clé publique d'Alice est bien vérifiée : seconde vérification.

A l'issue de ce protocole, l'Entité peut utiliser la clé publique d'Alice en toute confiance.

Selon l'invention, l'IGCP "2.0" à trois niveaux s'appuie sur deux IGCP éprouvées ("internationale" et "interne") combinées à une nouvelle IGCP dite "utilisateur" pour traiter le cas d'utilisateurs finaux en grand nombre (les Particuliers), point faible des deux premières.

La présente invention règle le problème lié à la révocation des certificats des utilisateurs finaux (consultation et mise-à-jour de la liste des certificats révoqués) car les "certificats de propriété de clé publique" sont consultables en temps réel sur le serveur Notaire Electronique.

L'avantage initial de l'IGCP traditionnelle qui consiste à ne pas avoir besoin d'être en ligne pour vérifier un certificat émis par un tiers ne semble plus d'actualité compte tenu de la quasi-nécessité de télécharger fréquemment des listes de certificats révoqués (CRL, *Certificate Revocation List*) et plus encore avec le protocole OCSP (*On-line Certificate Status Protocol*) de vérification en ligne de la validité des certificats. Le désavantage hypothétique de la nécessité de consulter en ligne les certificats de propriété dans l'IGCP "utilisateur" n'en est donc plus vraiment un.

Selon la présente invention, les "certificats de clé publique" de l'IGCP "utilisateur" sont conformes à la norme X.509v3 afin de pouvoir être utilisés par les applications existantes.

Le "certificat de clé publique" associe à la clé publique des

informations spécifiques à l'utilisateur auquel elle se rapporte. Ces informations s'ajoutent aux informations de base du type numéro de version, numéro de série, algorithme de signature, période de validité, etc.

Les extensions introduites dans la norme X.509v3 permettent de spécifier un certain nombre d'informations en fonction de l'usage prévu d'un certificat. Version : (indique à quelle version de X.509 correspond ce certificat). Numéro de série : Numéro de série du certificat.

Selon l'invention, ce même numéro est repris comme index de l'enregistrement dans l'annuaire (ou la base de données) des "certificats de propriété de clé publique" publié par le Notaire Electronique. Algorithme de signature : Identifiant du type de signature utilisée.

Selon l'invention, Emetteur : Distinguished Name (DN) de l'Autorité d'Enregistrement (et non de certification) qui a contrôlé la création de ce certificat (et non qui a émis ce certificat).

Selon l'invention, Valide à partir de : La date de création du certificat (et non la date de début de validité de certificat).

Selon l'invention, Valide jusqu'à : Il n'y a plus de date de fin de validité de certificat car c'est le certificat de propriété qui fait foi. Selon une forme d'application de l'invention, une durée de 10 ans peut être appliquée par défaut à compter de la date de création.

Objet : Distinguished Name (DN) du détenteur de la clé publique (l'utilisateur c'est-à-dire le particulier citoyen/consommateur/professionnel). Clé publique : Informations sur la clé publique de ce certificat. Extensions X509v3 : Extensions génériques optionnelles, introduites avec la version 3 de X.509.

Selon l'invention, Signature : Signature de l'utilisateur sur l'ensemble des champs précédents (et non la signature de l'Autorité de Certification).

Parmi les extensions utiles, on trouve les informations suivantes. X509v3 Basic Constraint : Indique s'il s'agit du certificat d'une Autorité de Certification ou non, c'est à dire permettant d'émettre des certificats. Selon l'invention, la valeur est fixée à CA:FALSE (ce certificat ne peut pas servir à générer d'autres certificats).

Netscape Cert Type : SSL Client, S/MIME, Object Signing : ces

extensions permettent au possesseur du certificat de s'authentifier auprès de serveurs SSL, de signer des courriels et de les déchiffrer (par exemple extensions pour Thunderbird® et Firefox®).

X509v3 Key Usage : Donne une ou plusieurs fonctions de sécurité auxquelles la clé publique est destinée. Ce champ permet de spécifier plusieurs services de sécurité.

Digital Signature/Non Repudiation/Key Encipherment : ces extensions permettent de signer des messages, de s'assurer que le possesseur est bien l'auteur d'une action. Key Encipherment permet d'utiliser le chiffrement S/MIME.)

X509v3 subjectAltName : ce champ contient un ou plusieurs noms alternatifs pour le porteur de certificat, exprimé sous diverses formes possibles. Selon une forme d'application de l'invention, ce champ pourrait être l'adresse de courriel de l'utilisateur, par exemple "particulier@monfournisseurdemessagerie.fr".

Selon l'invention, X509v3 issuerAltName : ce champ contient un ou plusieurs noms alternatifs pour l'Autorité d'Enregistrement qui a contrôlé la création de ce certificat, exprimé sous diverses formes possibles.

X509v3 CRL Distribution Points : normalement ce champ contient l'adresse de la *Certificate Revocation List* (CRL) ou liste de révocation des certificats permettant de connaître le statut de ce certificat. Selon l'invention, ce champ contient l'adresse du serveur Notaire Electronique de l'Autorité d'Enregistrement qui a contrôlé la création de ce certificat. Par exemple :

"URI:http://notaireelectronique.notairesdefrance.fr",
"URI:http://notaireelectronique.monoperateurtelecom.fr",
"URI:http://notaireelectronique.mabanque.fr".

Selon la présente invention, la vie privée du Particulier citoyen/consommateur/professionnel n'est pas confiée directement, soit à un seul Etat tout puissant (à l'exécutif), soit à quelques sociétés commerciales privées (les Autorités de Certification, parfois des sociétés étrangères) qui jouissent de quasi-monopoles. L'Etat est un garant pour assurer la confiance (via l'autorité judiciaire et les notaires) mais pas un acteur direct.

Dans le cas du cercle Régalien, le notaire rend compte à l'Etat, car il est assermenté en tant qu'officier ministériel (il dépend du ministère de la justice) ; mais il ne rend compte ni à l'exécutif (le gouvernement) ni au législatif (le parlement) : dans ces conditions l'Etat peut difficilement jouer les « Big Brother ». La personne, l'individu, est mis au centre de la nouvelle infrastructure car il fait établir son propre "certificat de propriété de clé publique" sans déléguer la certification à une Autorité de Certification. Le Particulier citoyen/consommateur/professionnel dispose ensuite de plus de liberté dans la publication de ses "certificats de clé publique".

L'administration française a établi pour ses besoins propres, et pour les organismes étant amenés à travailler dans le cadre de commandes publiques, une politique de référencement de sécurité PRIS (Politique de Référencement Intersectorielle de Sécurité) version 2.1 de novembre 2006. Cette politique s'applique en particulier à la dématérialisation des échanges électroniques. Les préconisations de la PRIS concernent l'usage d'architectures à clé publique (PKI). La PRIS définit 3 niveaux de sécurité qui vont de une étoile à trois étoiles. Le niveau 3*** impose : l'authentification forte, un enregistrement en face à face, une remise/acceptation d'un certificat en face à face si non fait lors de l'enregistrement, si l'Autorité de Certification ne génère pas la bi-clé, vérification que le certificat est bien associé à la clé privée correspondante (chargement à distance sur une carte à puce), acceptation explicite du certificat par le porteur.

L'enregistrement et la délivrance des certificats de personne mis en oeuvre par l'IGCP "utilisateur" respectent les conditions du niveau 3***.

L'IGCP "utilisateur" préconise, pour chaque Particulier citoyen/consommateur/professionnel, le stockage sur un support physique d'authentification et de signature de deux couples de bi-clé : le premier pour l'authentification (avec présomption de fiabilité), le second pour la signature électronique afin de valider une transaction en marquant son consentement. Les deux clés privées devront être stockées de façon sécurisée : soit en étant chiffrées et stockées dans une mémoire à accès libre, soit en étant stockées en clair dans une mémoire sécurisée avec

contrôle d'accès, soit en étant stockées chiffrées dans une mémoire sécurisée avec contrôle d'accès (la solution la plus sûre).

Selon la présente invention, les certificats de clé publique X.509v3 auto-signés sont stockés en clair. Le premier est un certificat d'authentification. Le second est un certificat de (vérification) de signature dont la valeur juridique découle de la Directive Européenne 1999/93.

Selon l'invention, l'agent d'enregistrement assure un service de proximité délégué par l'Autorité d'Enregistrement. Cet agent d'enregistrement est le garant du processus d'enregistrement et de délivrance des certificats mais il n'en détient pas pour autant toutes les clés. Il ne détient pas la clé privée des Particuliers ce qui est la moindre des choses, mais pas non plus leurs clés publiques dont il ne stocke que l'empreinte dans le "certificat de propriété de clé publique" qu'il publie sur le serveur Notaire Electronique de son Autorité.

Selon l'invention, c'est un notaire qui fait office d'Agent/Autorité d'Enregistrement pour le cercle Régalien. Le notariat français dispose déjà d'une IGCP "interne" qui donne à chaque notaire le pouvoir de signer numériquement des actes authentiques. Le notariat est organisé au niveau international et il n'est pas spécifique à la France. Cette nouvelle organisation a donc vocation à devenir mondiale.

Selon un mode d'application de l'invention, les navigateurs Web, les sélecteurs d'identité et les logiciels de messagerie contiennent « en dur » les adresses des quelques dizaines de serveurs Notaire Electronique par pays avec leurs propres certificats (pour la vérification de l'intégrité de leur base) en plus des certificats des principales Autorités de Certification actuelles.

Selon un mode d'application de l'invention, la gratuité doit rester la règle pour le Particulier. Les banques comme les opérateurs télécom peuvent assumer le coût de l'opération d'enrôlement des consommateurs à l'IGCP "utilisateur" par leurs agences d'enregistrement respectives en la combinant avec une action commerciale et/ou de fidélisation liées au déplacement physique des Particuliers. Les bénéfices attendus de la confiance ainsi instaurée dans les nombreuses transactions électroniques qui impliquent la banque ou l'opérateur télécom compensent largement le

temps et le coût de l'enrôlement. Par ailleurs, il existe de nombreuses options payantes qui apportent de la valeur ajoutée au Particulier et qui permettent aux agences de se rémunérer.

Selon un mode d'application de l'invention, les mairies ont pour mission l'enrôlement des citoyens à l'IGCP "utilisateur" pour le cercle Collectivités Territoriales. Cette mission, à l'instar de la délivrance de la Carte Nationale d'Identité Electronique (CNIE) ou e-ID Card, est compatible avec les nombreux services déjà proposés aux administrés.

Selon un mode d'application de l'invention, le gouvernement impose aux Notaires de France la quasi-gratuité du service de délivrance des certificats "utilisateur" (de clé publique et de propriété) aux citoyens en permettant aux notaires de mieux faire connaitre leur activité pendant cette opération. En effet, les notaires ont habituellement peu d'occasions (achat d'un bien, contrat de mariage, succession) de faire venir leurs clients dans leurs études. Un prix psychologique équivalent à celui d'une consultation médicale chez un généraliste pour l'enregistrement du Particulier, payable une seule fois à l'acte est un maximum à ne pas dépasser.

Selon un mode d'application de l'invention, la gratuité étant l'objectif à atteindre pour le service de base, des services optionnels pourraient être payant : fourniture de l'authentifieur physique (carte à puce, lecteur ou crypto-clé USB), délai raccourci de publication du "certificat de propriété de clé publique" du Particulier sur le serveur Notaire Electronique, publication automatique du certificat de clé publique du Particulier sur les principaux annuaires et autres fournisseurs d'identité, etc..

Des informations personnelles se trouvent dans le "certificat de clé publique" : nom, prénom, date et lieu de naissance. Ces informations sont jugées comme confidentielles : même l'identifiant persistant entre chaque couple (fournisseur d'identité, fournisseur de service) est unique et opaque afin de ne pas dévoiler d'information confidentielles sur un utilisateur à son insu. Le fait de transmettre ces informations pour s'authentifier peut ainsi être une entrave au besoin d'en connaître. Comment peut-on contourner cette contrainte ? Comment ne pas inclure d'informations confidentielles

sur l'utilisateur dans les "certificats de clé publique" ? Quelles informations y faire figurer dans ce cas ?

Selon un mode particulier d'application de l'invention, l'identité en clair de l'utilisateur est remplacée dans le "certificat de clé publique" par un identifiant ou plus précisément une empreinte identitaire. Cette empreinte identitaire est par exemple : eid = H (nom+prénom+date de naissance+lieu de naissance), avec H une fonction cryptographique de hachage à sens unique, ce qui correspond à une empreinte identitaire. La chaine à hacher à sens unique est suffisamment longue pour éviter une attaque par dictionnaire. Lorsqu'un interlocuteur connait suffisamment bien la personne (ou bien en lisant sa CNI), il est possible de vérifier au cas par cas que c'est bien lui. Par exemple, si je connais bien le Particulier Alice, je connais aussi ses date et lieu de naissance et je calcule : H (NomAlice+Alice+01/01/1962+Saint-Etienne) pour vérifier que l'empreinte identitaire "eid" stockée dans le "certificat de clé publique" lui correspond bien.

L'IGCP "utilisateur" est centrée sur l'utilisateur final à qui elle apporte confiance et sécurité. Doter les utilisateurs finaux, c'est-à-dire les Particuliers citoyens/consommateurs/professionnels, de moyens cryptographiques de sécurité est un réel besoin. Ce besoin n'est pas satisfait à l'heure actuelle par les solutions que sont les IGCP "internationales" (ou reconnues) et "internes" qui n'atteignent pas le particulier citoyen/consommateur/professionnel selon un ratio sécurité+responsabilité+contrainte / coût raisonnable.

L'IGCP "utilisateur" est plus économique car, à sécurité et périmètre de confiance équivalents, le coût d'un certificat utilisateur délivré et géré par une Autorité de Certification "internationale" ou reconnue est beaucoup plus élevé.

Dans la présente invention, la gestion des serveurs Notaire Electronique des Autorités d'Enregistrement ainsi que leur sécurité sur les plans de la disponibilité et de l'intégrité ne présentent pas de surcoût significatif comme c'est le cas pour les infrastructures des Autorités de Certification, soumises à des risques systémiques.

Selon un extrait du Guide de la signature électronique édité en octobre 2008 par la FNTC (Fédération Nationale des Tiers de Confiance) : « La signature électronique a la même valeur que la signature manuscrite dès lors qu'elle permet l'identification de celui qui l'appose ainsi que la manifestation du consentement des parties aux obligations qui découlent de cet acte (article 1316-4 du Code civil). Il est important de noter qu'en cas de litige, c'est le juge qui appréciera souverainement le caractère probant de la signature et par là sa valeur juridique, et ce que la signature soit manuscrite ou électronique (articles 285 et suivants du Code de procédure civile). Rappelons que, d'un point de vue strictement juridique, peu importe que les signatures électroniques soient « simples », « sécurisées », ou qu'elles utilisent des « certificats qualifiés » : elles ont toutes la même valeur juridique. On met souvent en avant la « présomption de fiabilité », attachée aux signatures électroniques sécurisées réalisées selon le dispositif spécifié à l'article 1316-4, al. 2 du Code civil et à l'article 2 du décret du 30 mars 2001.

Il faut toutefois rappeler à ce sujet deux éléments : L'apport juridique de la signature « emportant présomption de fiabilité » est faible dans le cadre de relations B to B (*Business to Business*) ou B to C (*Business to Consumer*) ; les exigences relatives à la signature sécurisée sont contraignantes à mettre en œuvre, et ne concerneront dans la pratique qu'une population très réduite, principalement les professions réglementées pour la perfection des actes authentiques. »

« Depuis la réforme du code civil, la signature électronique a la même valeur qu'une signature manuscrite. Pour bénéficier de la présomption de fiabilité, il faut que la signature électronique soit créée en conformité avec le décret du 30 mars 2001. Notamment, il faut que le système de signature électronique repose sur un dispositif sécurisé de création de signature électronique. Ce dispositif est évalué par un centre d'évaluation agréé par l'ANSSI avant d'être certifié conforme par l'ANSSI (article 3.II du décret du 30 mars 2001). La vérification de la signature électronique repose sur l'utilisation d'un certificat électronique qualifié (c'est-à-dire délivré par un prestataire de certification électronique qui

s'engage à respecter un certain nombre de conditions – article 6 du décret – ou qui a été accrédité par le COFRAC – article 7 du décret). »

Dans la présente invention, il existe bien un "certificat de propriété de clé publique", mais qui ne s'appuie pas sur une Autorité de Certification reconnue.

La signature électronique créée par le mécanisme d'une IGCP "utilisateur" est donc parfaitement valide.

Il existe toutefois des limitations à la signature électronique créée dans le cadre d'une IGCP "utilisateur" car elle ne repose pas sur un dispositif sécurisé de création ni sur un certificat qualifié au sens du code civil. Par conséquent, la signature électronique créée ne bénéficie pas de la présomption de fiabilité en termes de preuve. En conséquence, il incombe aux utilisateurs de la signature électronique de prouver que le lien entre la signature électronique et l'acte auquel elle se rattache est fiable (article 1316-4 du code civil).

En cas d'usurpation de signature, la responsabilité est limitée car la signature électronique créée par une IGCP "utilisateur" n'est pas qualifiée et n'a pas de présomption de fiabilité. En particulier, cette signature électronique n'utilise pas de certificats qualifiés et les Autorités d'Enregistrement ne s'engagent pas à respecter les conditions de l'article 6.II du décret du 30 mars 2001. Ce sera à l'utilisateur de prouver que c'est bien lui qui a signé. De même pour le fournisseur de service.

Dans la présente invention, la signature créée par l'IGCP "utilisateur" fonctionne dans un cadre contractuel. L'Autorité d'Enregistrement définit contractuellement le périmètre des responsabilités par l'ajout d'un contrat spécifique entre l'Autorité d'Enregistrement (banque ou opérateur télécoms = il y a déjà un contrat) et l'utilisateur final qui précise les responsabilités de l'Autorité d'Enregistrement et indique notamment que la signature électronique ne bénéficiant pas d'une présomption de fiabilité au sens de l'article 1316-4 du code civil, il conviendra de sécuriser sa force probante par contrat. Ainsi, la valeur probante de l'acte sur lequel est apposée la signature électronique créée dans le cadre d'une IGCP "utilisateur", doit être contractuellement reconnue par les parties au contrat.

A cet égard, il convient de distinguer différents cas de figure. En ce qui concerne les contrats conclus entre commerçants, la preuve est libre et une telle convention de preuve ne soulève pas de problème. En ce qui concerne les contrats conclus entre un commerçant et un consommateur, il convient de distinguer selon la valeur du contrat. Pour les contrats d'une valeur inférieure à 1 500 €, la preuve est libre et il est possible de prévoir dans le contrat avec l'utilisateur une convention de preuve. En revanche, le Code civil exige que les contrats d'une valeur supérieure à 1 500 € soient passés par écrit (article 1341 du Code civil et décret n° 80-533 du 15 juillet 1980 modifié par décret n° 2001-476 du 30 mai 2001 et décret n° 2004-836 du 20 août 2004). Selon l'article 1316-1 du Code civil, l'écrit sous forme électronique a la même valeur que l'écrit papier « sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité » (article 1316-1 du Code civil).

Ces conditions ne sont pas remplies de facto par la signature électronique délivrée dans le cadre d'une ICGP "utilisateur", ce qui implique que les actes juridiques sur lesquels est apposée cette signature électronique ne sont pas considérés comme des écrits. Cependant, il semble que l'exigence d'un écrit de l'article 1341 du Code civil puisse être exclue dans le cadre d'une convention de preuve. La Cour de cassation a ainsi reconnu la validité d'une telle convention à propos de l'utilisation du code de la carte bancaire (Cour de cassation, Civ. 1ère, 8 novembre 1989). Néanmoins, la validité d'une telle convention de preuve peut être remise en cause sur le terrain du droit de la consommation : en effet, les clauses qui renversent la charge de la preuve au détriment du consommateur ou limiteraient ses moyens de preuve sont généralement considérées comme abusives, lorsqu'une partie s'en remet purement et simplement à un système probatoire qui serait entièrement sous le contrôle de l'autre partie, serait valable. A noter qu'outre ces règles de preuve, il convient également de respecter des règles de validité des contrats conclus de manière électronique avec les consommateurs qui restent soumis à l'exigence du « double click » de l'article 1369-1 du Code civil qui est d'ordre public et ne peut être exclue par une convention de preuve (sauf

entre professionnels). En l'absence d'un tel mécanisme, ces contrats ne sont pas valables.

En termes d'usages, la solution d'une IGCP "utilisateur" est bien adaptée au contexte du *B to B* des petites entreprises. Pour le *B to C*, cela pourrait constituer une solution intermédiaire entre une présomption simple (des milliers de contrats sont signés tous les jours sous ce régime) et l'utilisation d'un certificat qualifié.

Selon l'IGCP "2.0", le Particulier est responsable de ses clés (privée et publique) ainsi que de ses certificats de clé publique.

Selon l'IGCP "2.0", l'Autorité d'Enregistrement est responsable des "certificats de propriété de clé publique" qu'elle a émis et qu'elle publie sur son serveur Notaire Electronique. L'Autorité d'Enregistrement garantit l'enregistrement, la délivrance et l'authenticité du certificat de propriété de clé publique. Elle ne stocke aucune clé du Particulier.

Selon l'IGCP "2.0", aucun organisme central n'endosse la responsabilité du "certificat de clé publique" de millions de Particuliers citoyens/consommateurs/professionnels. Le pouvoir exécutif n'est pas non plus soupçonné d'être le maître du jeu (cf. les problèmes posés par le fichier "Edvige").

Dans le cas d'une IGCP "interne" déployée à grande échelle, se pose le problème de la responsabilité de l'Autorité de Certification, de sa légitimité et du respect de la vie privée.

Si cette IGCP est de nature Etatique : sa responsabilité est normale mais budgétée (à un coût), sa légitimité est normale, son Respect de la vie privée ne convient pas.

Si cette IGCP est de nature privée : sa responsabilité est normale mais facturée, sa légitimité est normale et son respect de la vie privée ne convient pas.

Si cette IGCP est de nature "organisme dédié" : sa responsabilité est normale, sa légitimité est difficile à acquérir, son respect de la vie privée ne convient pas.

Aucune de ces IGCP n'est pleinement satisfaisante.

La vie privée du Particulier citoyen/consommateur/professionnel ne doit pas être confiée directement à un seul Etat tout puissant (à l'exécutif).

L'Etat doit un être un garant pour assurer la confiance (via l'autorité judiciaire) mais pas un acteur direct.

La vie privée du citoyen/consommateur/professionnel ne doit pas être confiée directement à une grande société commerciale privée qui jouirait d'un quasi-monopole. En cas de multiplicité des Autorités de Certification (AC) privées, on retrouverait l'imbroglio de l'architecture pyramidale des AC pour adresser des utilisateurs d'horizons très divers.

L'IGCP "2.0" à trois niveaux conserve les avantages indéniables des IGCP "internationale" et "interne" pour leurs usages respectifs. L'IGCP "internationale" adresse peu d'acteurs : IDPs/IPs, APs, SPs/RPs, Notaires Electroniques... Les IGCP "internes" adressent un nombre d'acteurs significatifs (quelques milliers) à savoir les agences de proximité des Autorités d'Enregistrement : les Agences Locales d'Enregistrement.

Dans la présente invention, l'IGCP "utilisateur" qui adresse la masse des Particuliers citoyens/consommateurs/professionnels s'affranchit des Autorités de Certification et donc de leur faiblesse avérée dans le traitement d'un très grand nombre d'utilisateurs d'horizons divers.

L'IGCP "utilisateur" s'appuie au contraire sur des Autorités d'Enregistrement disposant d'un réseau existant d'agences de proximité et d'un serveur Notaire Electronique, qui elles, y sont parfaitement adaptées.

Dans la présente invention, l'IGCP "utilisateur" donne au Particulier le contrôle de son identité numérique en tant qu'acteur central, incontournable et responsable.

REVENDICATIONS

1. Infrastructure de gestion de bi-clés de sécurité de personnes physiques comportant une clé publique et une clé privée avec un certificat de clé publique, ladite structure comportant au moins une autorité d'enregistrement et son serveur notaire électronique, caractérisée en ce que l'on prévoit au moins une autorité d'enregistrement et son serveur notaire électronique pour chacun des cercles de confiance tels que par exemple le cercle régalien, le cercle collectivités territoriales, le cercle banque, finance et assurance, le cercle internet et télécommunication et le cercle santé, ladite autorité d'enregistrement comprenant des agences locales d'enregistrement de proximité (respectivement, par exemple, notaires et huissiers, mairies et bureaux de poste, agences de banques et d'assurance, agences et boutiques de télécommunications, caisses d'assurance maladie et pharmacies), en ce qu'une agence locale d'enregistrement établit, pour chaque personne physique, après vérification en face à face de son identité, un certificat de propriété de clé publique qui est transmis de façon sécurisée au serveur notaire électronique associé qui le stocke de manière sécurisée et en ce que le certificat de propriété de clé publique est chiffré avec la clé privée de la personne physique.

2. Structure selon la revendication 1, caractérisée en ce que le certificat de propriété de clé publique contient une représentation de la clé publique de la personne physique.

3. Structure selon la revendication 2, caractérisée en ce que la représentation de la clé publique de la personne physique est la clé publique en clair.

4. Structure selon la revendication 2, caractérisée en ce que la représentation de la clé publique de la personne physique est une empreinte de la clé publique.

5. Structure selon la revendication 1, caractérisée en ce que l'adresse du serveur notaire électronique de l'autorité d'enregistrement dont l'agence locale a enregistré la personne physique est indiquée dans le certificat de clé publique de ladite personne physique.

6. Structure selon la revendication 1, caractérisée en ce que les certificats de clé publique des personnes physiques sont éventuellement publiés sur des annuaires de clés publiques et en ce que les certificats de propriété de clé publique sont conservés de manière sécurisée sur le serveur notaire électronique de l'autorité d'enregistrement.

7. Structure selon la revendication 1, caractérisée en ce qu'elle comporte un module de requête qui prend en entrée le certificat de clé publique de la personne physique, interroge le serveur notaire électronique dont l'adresse figure dans ledit certificat de clé publique, en communiquant le numéro de ce certificat de clé publique et la clé publique incluse dans ledit certificat de clé publique, et qui reçoit en retour de la part du serveur notaire électronique dont l'adresse figure dans ledit certificat de clé publique une assertion sur l'authenticité ou la non-authenticité de la prétendue clé publique de la personne physique.

8. Structure selon la revendication 7, caractérisée en ce que le module de requête est placé par exemple dans les navigateurs internet, les logiciels de messagerie électronique, les serveurs fournisseurs d'identité (IDP, IP/STS), les applications informatiques, les processus informatiques.

9. Structure selon la revendication 7, caractérisée en ce qu'elle comporte un module de réponse qui est installé sur tous les serveurs notaire électronique, qui reçoit en entrée la requête du module de requête, qui recherche dans la base de données dudit serveur notaire électronique s'il existe un numéro de certificat de propriété de clé publique identique au numéro de certificat de clé publique reçu et qui délivre une

assertion « la clé publique n'est pas authentique » si le résultat de la recherche est négatif.

10. Structure selon la revendication 7, caractérisée en ce qu'elle comporte un module de réponse qui est installé sur tous les serveurs notaire électronique, qui reçoit en entrée la requête du module de requête, qui recherche dans la base de données dudit serveur notaire électronique s'il existe un numéro de certificat de propriété de clé publique identique au numéro de certificat de clé publique reçu, en ce que si le résultat de la recherche est positif, ce module de réponse fait une tentative de déchiffrement du certificat de propriété de clé publique trouvé avec la clé publique reçue et délivre une assertion « la clé publique n'est pas authentique » si le déchiffrement ne réussit pas ou une assertion « la clé publique est authentique» si le déchiffrement réussit.

11. Structure selon la revendication 7, caractérisée en ce qu'elle comporte un module de réponse qui est installé sur tous les serveurs notaire électronique, qui reçoit en entrée la requête du module de requête, qui recherche dans la base de données dudit serveur notaire électronique s'il existe un numéro de certificat de propriété de clé publique identique au numéro de certificat de clé publique reçu, en ce que si le résultat de la recherche est positif, ledit module de réponse fait une tentative de déchiffrement du certificat de propriété de clé publique trouvé avec la clé publique reçue, en ce que si le déchiffrement réussit, ledit module de réponse calcule l'empreinte de la clé publique reçue, puis la compare avec l'empreinte de la clé publique stockée dans le certificat de propriété de clé publique préalablement déchiffré et en ce que ledit module de réponse délivre une assertion « la clé publique n'est pas authentique », si les deux empreintes sont différentes ou une assertion « la clé publique est authentique », si les deux empreintes sont identiques.

12. Structure selon la revendication 9, caractérisée en ce que l'assertion est signée avec la clé privée du serveur notaire électronique et en ce que le module requêteur, vérifie la signature de l'assertion en utilisant la clé publique du serveur notaire électronique.

13. Structure selon la revendication 7, caractérisée en ce que la clé publique du serveur notaire électronique est certifiée par une autorité de certification internationalement reconnue, telle que par exemple « Verisign », « Entrust », « Keynectis » ou « Certinomis ».

14. Structure selon la revendication 1, caractérisée en ce que la génération de la bi-clé de sécurité d'une personne physique est réalisée individuellement au moyen d'un outil logiciel mis à sa disposition (par exemple par téléchargement) dans un appareil personnel tel qu'un ordinateur, un téléphone mobile ou un téléphone du type terminal communiquant (tel que « Smartphone »), en ce que la personne physique se rend ensuite à son agence locale d'enregistrement qui procède à la génération effective de son certificat de clé publique et de son certificat de propriété de clé publique associé et en ce que les numéros de ces deux certificats sont identiques.

15. Structure selon la revendication 1, caractérisée en ce que la génération de la bi-clé de sécurité d'une personne physique est réalisée en sa présence par l'agence locale d'enregistrement qui procède ensuite à la génération effective de son certificat de clé publique et de son certificat de propriété de clé publique associé et en ce que les numéros de ces deux certificats sont identiques.

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 742255
FR 1001229

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	ITU-T: "ITU-T Rec. X.509, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T X-SERIES RECOMMENDATIONS. DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY,, no. X.509, 1 août 2005 (2005-08-01), XP007913144, * sections 7, 8, 12 and 18 *	1-15	H04L9/32
T	"Certificat électronique", INTERNET CITATION, 6 mars 2010 (2010-03-06), XP007917056, [extrait le 2011-02-08] * le document en entier *		
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04L

Date d'achèvement de la recherche	Examinateur
9 février 2011	Manet, Pascal

CATÉGORIE DES DOCUMENTS CITÉS

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

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

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)