(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 960 671**

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

(21) **N° d'enregistrement national :** **10 54272**

(51) Int Cl[8] : ***G 06 F 21/24*** *(2006.01), H 04 L 9/32, 29/06*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 01.06.10.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 02.12.11 Bulletin 11/48.

(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) :** *INSTITUT TELECOM-TELECOM PARIS TECH Etablissement public* — FR.

(72) **Inventeur(s) :** LAURIER PHILIPPE et RIGUIDEL MICHEL.

(73) **Titulaire(s) :** INSTITUT TELECOM-TELECOM PARIS TECH Etablissement public.

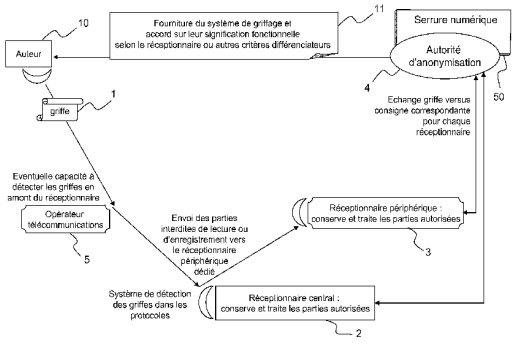
(74) **Mandataire(s) :** MARKS & CLERK FRANCE.

(54) PROCEDE DE SECURISATION DE DONNEES NUMERIQUES ET D'IDENTITES NOTAMMENT AU SEIN DE PROCESSUS UTILISANT DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION.

(57) La présente invention concerne un procédé de contrôle, de sécurisation et de confidentialisation de données au sein de processus déclaratifs, informatifs, administratifs ou productifs utilisant les technologies de l'information et de la communication.

Plus particulièrement l'invention concerne un procédé de sécurisation de données numériques placées dans un fichier informatique ou émises dans un flux de communication par un expéditeur (10) vers au moins un réceptionnaire principal (2) et éventuellement un ou plusieurs réceptionnaires périphériques (3) selon un protocole informatique ou de communication donné, caractérisé en ce qu'une consigne de fonctionnement ou une information dédiée à chaque réceptionnaire est transmise au moyen d'un griffage inséré dans le protocole informatique ou de communication.

La consigne de fonctionnement peut être une autorisation, une interdiction, l'activation, la modification ou l'arrêt d'une fonction d'un réceptionnaire (2, 3) et peut être couplée à la délivrance d'information. L'invention s'applique à la gestion de données régies par des protocoles informatiques ou de communication, notamment pour les opérations de géolocalisation, de traçage, de marquage, de profilage ou d'identification, tels que lors d'activités d'achat en ligne, de valorisation, de déplacement, ou d'expression de sa pensée.



FR 2 960 671 - A1

PROCEDE DE SECURISATION DE DONNEES NUMERIQUES ET D'IDENTITES NOTAMMENT AU SEIN DE PROCESSUS UTILISANT DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

La présente invention concerne un procédé de contrôle, de sécurisation et de protection par confidentialité, de données au sein de processus déclaratifs, informatifs, administratifs ou productifs utilisant les technologies de l'information et de la communication. Cet encadrement définit des manières de pouvoir ou non connaître ces données, y accéder, les détenir, les traiter ou les transmettre. Elle concerne également un procédé de gestion et de démultiplication d'identités numériques par l'insertion de marquages intermédiaires formant écran et par substitution de référents d'identité.

Elle s'applique à la gestion de données régies par des protocoles informatiques ou de communication, notamment pour les opérations de géolocalisation, de traçage, de marquage, de profilage ou d'identification, tels que lors d'activités en ligne d'achat, d'enchères, d'expression de sa pensée. Ce traçage et cette identification pouvant par ailleurs participer à des échanges et des transferts, tels que financiers ou postaux, ainsi qu'aux actions visant à accorder, maintenir, vérifier et garantir une signification, une grandeur ou une valeur à ces marquages. Elle s'applique également à l'activation et au contrôle d'un équipement ou d'une fonction telle que de gestion des commandes, utilisant des données régies par un de ces protocoles, en assurant en particulier un suivi de leur nature, leurs qualités, leur quantité, leur usage ou leur fonctionnement. Elle s'applique aussi à faciliter conjointement la gestion et l'anonymisation des biens ou personnes dotés d'identités numériques, tels que les objets dits intelligents et communicants.

L'invention vise, par ces actions de contrôle et de sécurisation, à remplir des fonctions techniques mais aussi économiques et sociales, en contribuant également à un meilleur respect de la vie privée des personnes et à ce qui relève de leur « intimité numérique », vis-à-vis par exemple d'entreprises commercialement agressives ou de pirates informatiques. Le danger tient à

la diffusion intempestive d'une information élémentaire, telle qu'une identité confidentielle en soi, mais également d'une information composée, telle que cette identité corrélée à un second secret : casier judiciaire, endettement commercial, situation fiscale, état médical, engagement sentimental ou encore prise de position philosophique. Raccorder deux données peu sensibles isolément peut aboutir à des conclusions sensibles, tel qu'établir un lien de propriété entre une personne et un bien, ou un lien de connaissance entre une personne et une autre, ou un lien de dépendance entre deux objets.

Elle s'applique notamment à la réduction des risques résultant de la manipulation de données jugées sensibles qui peuvent être de plusieurs types.

Il peut s'agir d'attributs d'identité : par exemple nom, prénom, date de naissance, sexe, situation matrimoniale, liens de parenté, adresse du domicile, adresse postale ou de télécommunication, coordonnées bancaires, numéro de carte bancaire et date de validité ou d'expiration, numéro de sécurité sociale et autres référents, codes personnels, sceaux, visas ou marques distinctives. Lesquels aident à identifier, autant qu'à accéder par ces informations et bribes d'identité à des espaces personnels ou des fonctions personnelles, tels qu'activer un compte bancaire, pouvoir se rendre au lieu du domicile ou se créer un accès à un registre du personnel.

L'action incriminée peut en particulier consister à se référer indûment d'un interlocuteur, usurper son identité et ses prérogatives, le contacter pour l'importuner, le tracer ou le profiler d'une manière nominative, répertorier ses biens et les gérer. Ces menaces constituent un frein à la consommation, par les réticences sociales qu'elles génèrent, autant qu'une atteinte à l'autonomie et à la liberté des personnes, par les phénomènes d'autocensure qu'ils engendrent. Ils provoquent également des pertes économiques, par les dysfonctionnements techniques ou organisationnels causés. Ces pertes peuvent être patrimoniales lorsqu'elles aboutissent à une destruction, une dénaturation ou un vol.

Les données sensibles peuvent être également les attributs d'une identité comportementale ou situationnelle, tels que des lieux et horaires de

présence lorsqu'ils sont représentatifs d'un métier, ou la nature d'un achat lorsqu'elle est représentative d'une préférence. De même, une adresse peut correspondre à un lieu révélateur d'une appartenance religieuse ou communautaire. Il peut s'agir de toute particularité telle qu'anatomique ou physiologique participant à un processus de traitement et de remboursement de frais médicaux, d'embauche dans le cas d'emploi à un poste réservé pour personne handicapée, d'état de vaccination représentatif de destinations géographiques spécifiques. Particularités que l'on ne désire pas être connues d'un interlocuteur, à l'instar d'une pathologie particulière, d'un degré de handicap ou de tout détail potentiellement révélateur d'une manière d'être. Le procédé tel que défini par l'invention peut également conserver un degré voulu de confidentialité s'attachant à un individu, en termes de diplôme, ou envoi de curriculum vitae en vue d'une évolution de carrière.

Ce cadre situationnel ou comportemental peut englober plus largement l'expression privée d'une volonté ou d'une analyse personnelles, un constat ou un bilan de situation formulés par l'expéditeur, à l'image d'ordres ou de verdicts transmis pour exécution, de contenus annotés pour archivage ou traitement.

L'entité concernée peut être une personne physique ou morale, fragilisable via une connaissance de l'organigramme de l'entreprise ou de sa situation de trésorerie. Ce peut être autant un groupe de personnes constituées en une structure fédératrice ayant des attributs d'identité propre. À l'avenir, au-delà des êtres humains ou animaux, il pourra s'agir d'objets, ou de groupes d'objets, ou d'un objet couplé à une personne, et ayant endossé des identités, notamment dans le cadre des objets dits communicants, à l'instar d'une prothèse avec une composante électronique.

L'invention peut plus généralement s'appliquer à toute donnée qu'il est désirable d'encadrer dans son usage ou son statut, tels que de confidentialité, intégrité, disponibilité, immunité, exhaustivité, complétude, validité, propriété. À ce titre, des données pourront être considérées également sensibles pour des motifs tels que :

- ne se rapportant pas à une identité d'un expéditeur mais à celle du réceptionnaire.
- se rapportant à son lieu, une date ou encore un contexte, à l'image d'une fonction d'interdiction de lecture après une date limite, ou hors d'un espace de stockage donné.

Le caractère important d'une donnée peut se rapporter à sa finalité telle que la mise en fonctionnement d'un équipement anti-incendie ou d'une issue de secours. Elle peut être jugée telle par rapport à l'activité naturelle d'un cabinet d'avocat ou d'un laboratoire de recherche, envers des données judiciaires, scientifiques ou managériales.

Le mot « données » englobe ici un spectre allant du signal analogique jusqu'à la mise en forme structurée de données numériques sous forme d'informations ou de consignes. Cette mise en forme autant que le contenu découlent des connaissances de leur auteur et appartiennent à son patrimoine, avec de mêmes besoins d'être sécurisés en soi et dans leur structure. L'information pourra être autant numérique qu'analogique, indépendamment de son expression finale pour un observateur, par des chiffres, lettres, dessins, vidéos, impulsions, couleurs ou encore sons. Elle peut se trouver sous diverses formes telles que magnétique ou optique. Le critère distinctif de la présente invention, pour son fonctionnement, étant que cette donnée soit véhiculée ou conservée dans un cadre, considéré comme le contenant, qui prenne la forme d'un protocole informatique ou de communication. À l'extrême, il peut s'agir d'un simple contenant, sans contenu, où le simple fait de le recevoir devienne en soi informatif ou déclencheur.

Ces protocoles peuvent être dits « propriétaires », ou « ouverts » lorsque les interfaces sont publiques et qu'on peut donc dialoguer syntaxiquement avec la boîte noire.

Le protocole peut être de communication s'il y a déplacement de ces données sur un réseau de télécommunication ou par exemple sur une carte informatique. Il peut s'agir autant de données statiques sur leur support, pour autant que leur accès, leur intégrité ou leur mise en œuvre dépendent en préalable d'un protocole, s'entendant alors dans sa pleine acception

étymologique : ce qui est collé en premier, protocollum, et définit pour son lecteur des us, des règles d'emploi et des indications nécessaires pour faire opérer ou modifier ces données. Le terme collé, kollân, renvoie également à « étiquette » : enchaînement procédural à respecter scrupuleusement pour la bonne activation ou manipulation de ces données lorsqu'on y accède ou qu'on les réceptionne. Dans les technologies de l'information et de la communication, un protocole peut être assimilé à une passerelle obligatoire, ou un gué pour parvenir à une île. Situation privilégiée à la fois dans l'espace et dans le temps, mais qui n'a jusqu'à présent pas trouvé suffisamment d'expression inventive en matière de sécurité ou de contrôle. Les réflexions en cette matière restent généralement axées sur une logique de camouflage des données elles-mêmes ou de leur blindage, selon l'ancienne rivalité de l'épée et de la cuirasse. Le procédé selon l'invention déporte l'axe de défense initial plus en amont. De manière usuelle, ces protocoles recèlent une caractéristique d'incomplétude, si bien qu'il est possible d'y apporter des ajouts, amputations ou modifications, comme de le détourner, de telle manière qu'une nouvelle propriété surgisse : fonction de sécurité, fonction de production, par exemple.

Un protocole peut faire office « d'étiquette » ou de première interface dans deux sens, entrant ou sortant : soit à destination d'un réceptionnaire dans le cas d'un déplacement des données qu'il accompagne, soit en point d'entrée d'un flux arrivant vers ces mêmes données lorsqu'elles sont statiques.

L'usage de données statiques peut se faire à l'occasion par exemple d'un calcul mathématique ou d'un traitement de texte mené par ordinateur, à partir de données déjà présentes dans un document, un fichier ou un programme, telles que des données scientifiques, comptables ou d'identité d'une personne. Toute consigne, requête ou information qui lui sera envoyée devant en passer initialement par son protocole informatique, donc se trouver face à un éventuel marquage ou signe distinctif selon l'invention qui y serait présent et correspondrait à l'édiction de prescriptions incontournables. Ces prescriptions pourraient notamment viser à encadrer la manipulation des données jugées sensibles. Lesquelles peuvent être à titre d'exemples des photographies archivées sur un agenda numérique, des mots de passe

enregistrés sur un disque dur d'ordinateur, des horaires et durées d'appel conservées sur une mémoire électronique de téléphone mobile. Cet assujettissement à des prescriptions pourra aboutir en particulier à des formes d'interdictions ou d'autorisation, d'activation ou d'arrêt de mécanisme, de limitations d'action, d'attitude dilatoire ou de clauses conditionnelles. Il pourra aboutir encore à une délivrance d'information additionnelle, lorsque ledit signe distinctif inséré dans le protocole, également signe de reconnaissance, fait office de passeport vers ces additifs.

Par la suite sera nommé « fichier », un document ou un programme informatique, un exécutable, une entité logicielle, une entité virtuelle telle qu'une mémoire virtuelle.

L'usage de données dans le cas d'une communication, peut se produire à l'occasion de processus notamment déclaratifs ou informatifs, tel qu'un dialogue, une confession ou l'expression de sa pensée sur un site internet, une enchère ou une candidature à distance, ainsi encore qu'une indication de lieu de présence auprès d'une borne électronique située dans un bus ou automatiquement par voie de télécommunications auprès d'un central. Le terme dialogue concerne effectivement autant un échange sur l'initiative consciente d'une personne, qu'effectué par un de ses équipements, avec ou sans consentement express ni lien obligatoire de propriété.

Ce processus global peut également être administratif ou productif, tel que d'achat d'un produit ou d'un service, utilisation d'un logiciel en ligne, paiement en ligne, recherche en ligne, compétition en ligne, ou encore un test mené via des supports téléphoniques, une homologation menée par voie informatique. Le terme service pouvant englober à titre d'exemples des prestations commerciales, médicales ou industrielles. Il s'agit plus généralement d'activer, par transmission d'information ou de consigne, une fonction par exemple sur un ordinateur, une machine-outil à commande numérique ou un aiguillage automatisé.

Ces diverses situations peuvent rester dans une sphère numérique telle que communiquer via un bloc-notes numérique et activer des avatars sur le web, ou interagir avec des actions physiques réelles telles que la réservation et l'envoi postal d'un billet de train. De fait, une rencontre ou un déplacement

peuvent donner lieu à l'usage de supports informatiques ou de télécommunications.

Par la suite, sera nommé « courrier », un message, un envoi de fichier ou de documents, un appel téléphonique, la participation à un dialogue, une visite faite par voie de télécommunications, et plus généralement toute forme de flux, d'émission ou toute forme d'échange par mise en relation ou connexion. Ce courrier peut s'effectuer entre plusieurs supports, ou à l'intérieur d'un même équipement, s'agissant d'un déplacement de données d'une zone vers une autre au sein par exemple d'un ordinateur ou d'une carte électronique, autant que ce déplacement recoure à l'emploi d'un protocole informatique ou de communication. Le terme courrier s'applique au pair à pair, lorsque le message est déchiqueté comme dans le cas d'une répartition des données sur les disques ou les serveurs connectés à internet.

Sera par la suite nommé « auteur », l'expéditeur de ce courrier. Dans le cas d'un composant passif telle qu'une étiquette RFID, l'auteur sera considéré être l'étiquette et son porteur, et non la borne ayant créé un champ électromagnétique. Dans le cas d'objets communicants dotés d'une identité, l'auteur pourra être par exemple un capteur transmettant un signal, ainsi que son détenteur ou son porteur. Dans le cas d'un fichier informatique statique, le terme auteur pourra englober, outre celui qui l'a conçu, celui qui en est à l'instant concerné le détenteur, le dépositaire ou le gestionnaire.

Le support matériel du courrier peut être un réseau de communication, notamment de télécommunications ou de télédiffusion, ainsi que des moyens physiques mobiles tels qu'une clé USB, une carte à puce ou magnétique, un disque, un badge, un ticket tel que de métro, un passe avec contact ou sans contact comme l'est une carte de transport. La banalisation des objets communicants va élargir ce champ à une infinité de supports moins discernables dans leurs contours mais toujours caractérisés par de mêmes fonctions et utilisant des protocoles informatiques ou de communication.

L'objet réceptionnaire peut être un support ou un terminal de télécommunications, ou de télédiffusion tel qu'un téléviseur, un

magnétoscope ou un décodeur, et plus généralement tout équipement informatique ou électronique apte à participer à une distribution d'information. S'agissant du réceptionnaire d'un support mobile de courrier, ce peut être une machine informatique dotée de prises telle qu'USB, un téléphone portable, un assistant ou agenda numérique, un lecteur de carte ou de disque, un distributeur automatique tel que de billets de banques, un sas d'accès ou encore une borne d'identification, à titre d'exemples.

Le réceptionnaire peut être externe, par exemple un intervenant recevant un courrier ou accédant à un fichier, autant qu'interne, à l'instar d'un contenu de fichier ou de courrier, contenu pourvu de capacités techniques qui en rendent certaines composantes actives, autonomes et aptes à participer à des actions par exemple de recueil de données, tels que le sont des « agents intelligents ». Ces entités autonomes, dotées de cognition et avec des capacités d'interaction avec leur environnement, peuvent se mettre en dialogue avec leur propre protocole, et faire du signe distinctif selon l'invention un usage identique à celui d'un réceptionnaire extérieur. Il peut s'agir alors d'utiliser ce signe, avec ses propriétés fonctionnelles et cryptonymiques, ainsi que comme signe de reconnaissance.

Par la suite, sera nommé « réceptionnaire central », à propos de ce courrier le réceptionnaire considéré par l'auteur comme le destinataire naturel de son courrier. Il peut s'agir en particulier d'un site internet commercial, un forum de discussion politique, un site d'échange ou de mise en relation à caractère amical ou matrimonial, un prestataire de services ou de supports informatiques tel qu'un éditeur de logiciel habitué à mettre à jour en ligne ses versions, un centre d'enregistrement, d'archivage ou de documentation, une administration en charge d'un examen ou d'appels d'offre, un jury, un organisateur de concours, un laboratoire d'analyse biologique ou encore un expert requis dans le cadre d'une expertise que l'on souhaite plus neutre car anonymisée quant à la personne concernée ou requérante. Ce peut être une société d'autoroute gestionnaire de péage, utilisant des tickets, des laissez-passer ou des coupe-files tels que magnétiques ou électroniques, sans désirer toutefois relever chaque passage par le nom véritable de son possesseur. Dans le même esprit, il peut s'agir d'un gestionnaire de cantine

utilisateur de badges et ne désirant pas rapporter des pratiques alimentaires caractéristiques à une personne identifiée.

Le destinataire central peut n'être dans les faits ni obligatoirement le réceptionnaire initial du flux de communication ni son réceptionnaire final.

Les autres réceptionnaires seront par la suite nommés « réceptionnaires périphériques », et pourront être :

- un organisme gestionnaire de cartes bancaires ;
- une banque ;
- une administration postale ;
- une société de routage ou de transport ;
- un opérateur de télécommunications ou un fournisseur d'accès internet ;
- une administration délivrant des documents à caractère nominatif tels que des attestations, des certificats, des laissez-passer ou des visas;
- un organisme paritaire gestionnaire de cartes de santé ou en charge de la couverture de dépenses de santé ;
- une structure gestionnaire des dossiers médicaux de patients ;
- une administration en charge de la conservation de données requérant une gestion partielle d'anonymat tels que de casiers judiciaires ou d'accouchement sous x ;
- un médiateur de conflits ou de contentieux ;
- un officier public ;
- un cabinet d'audit.

Cette liste étant illustrative et non pas limitative. Elle énumère quelques acteurs périphériques participant à un processus complexe relatif à des données sensibles.

L'invention structure et supporte un jeu à plusieurs acteurs, parmi lesquels se trouvent l'auteur, les différents réceptionnaires, des autorités appelées par la suite d'anonymisation. S'y ajoutent une ou plusieurs entités nommées par la suite serrure numérique, qui peuvent être considérées soit actives soit, sous une forme plus achevée, simplement passives et réactives aux gestes des autres acteurs.

Ce jeu se déploie autour d'un signe distinctif et caractéristique inséré dans le protocole informatique ou de communication.

Elle prend la forme d'un triple dispositif :

- d'une part ce marquage par un signe caractéristique, dit griffage, inséré à des fins distinctives, de reconnaissance, ainsi que de transmission de consigne ou d'information. Ce griffage plurifonctionnel, placé au niveau des protocoles informatiques ou de communication, servira, pour un réceptionnaire, d'information en soi ou de moyen d'obtention d'informations complémentaires auprès d'un tiers habilité ;
- d'autre part de cloisonnement et de canalisation des données ou des acteurs, par l'entremise du griffage associé à une autorité d'anonymisation et à une serrure numérique. La sécurité, qui est l'art de partager des secrets, se trouve à la fois dans la possession ou la connaissance de secrets, mais aussi dans une architecture spatio-temporelle de sécurité, qui est ici globalement secrète, c'est-à-dire que les acteurs, étant murés dans des compartiments distincts dans le temps et dans l'espace, ne sont pas en mesure de découvrir ni la topologie, ni la séquence du processus global.

Ces deux premiers dispositifs peuvent fonctionner isolément, mais trouvent leur pleine expression dans leur coordination ou leur coopération.

- Le troisième dispositif tient au fait que le griffage prend la forme d'un cryptonyme variant, lui-même raccordable d'une part à un pseudonyme invariant et stable, d'autre part à ce qui sera nommé par la suite des polynymes, dans une acception particulière.

Au sein de ces dits processus spatio-temporels, le griffage fonctionnel ainsi que le cloisonnement et l'anonymisation permettront de modifier la gestion, l'accessibilité, la présence ou la forme des données en vue de mieux les contrôler, les protéger et les confidentialiser, tout en maintenant une bonne réalisation des processus. Cette réalisation fidèle pouvant aussi consister par exemple en leur suspension, si la hiérarchie des priorités initiales privilégiait cette option à leur bonne fin, en cas de survenue d'un danger précis ou d'une incertitude.

Ce cloisonnement et ces découpages spatio-temporels dans l'architecture du réseau et dans les protocoles permettent de réduire la connaissance de chacun au « besoin d'en connaître ». Le découpage est rendu possible par

les techniques d'interconnectivité des réseaux (virtualisation des ressources, nuage numérique, architecture pair à pair, etc), qui permettent de déchiqueter les fichiers, à l'instar des protocoles de partage de fichiers. Le présent procédé emploie toutefois aussi le déchiquetage des rôles.

D'une manière générale, parmi les trois fonctions centrales des appareillages concernés que sont la communication, l'enregistrement et le traitement de données, la première bénéficie souvent d'assez bonnes protections notamment par les protocoles de sécurisation point à point, comme SSL, TLS, IPSec, le chiffrement des transmissions lorsqu'il s'agit de données bancaires, ou lorsqu'elles transitent par un GSM entre le téléphone portable et la station de base. Tandis que la deuxième (le stockage de données) et la troisième (le calcul) constituent dans de nombreuses entreprises ou administrations un point faible majeur, et le principal talon d'Achille face à des menées illégitimes.

La propension des stockages d'information à se multiplier, s'étoffer et s'interconnecter, ajoute à la fragilité de ce maillon, une attractivité pour les assaillants. Ces mémoires touchent au qui, telle que notre identité, au quoi, tels que nos achats, au comment, telles que nos cartes bancaires, au où autant qu'au quand, à l'image d'un opérateur de télécommunications mobiles qui reçoit connaissance d'une localisation géographique à chaque signal de position d'un téléphone mobile. Plus subtilement, elles conservent aussi mémoire de nos centres d'intérêt, à travers la consultation d'une page de site internet, de nos hésitations retracées par des pérégrinations sur plusieurs pages, de nos appréhensions exprimées par la prise de rendez-vous chez un spécialiste médical.

S'agissant de la prise de connaissance et des opportunités de mise en mémoire, le concept de droit à l'oubli numérique appliqué à des données personnelles et au respect de l'intimité des individus, est doublement fragile en ce qu'il suppose une technique de destruction infaillible et en ce qu'il tolère une période de détention antérieure durant laquelle peuvent se produire des copies écrites, photographiques ou numériques.

Une première particularité de l'invention tient à son constat qu'une manière plus sécurisée de ne pas se faire voler une chose est de ne pas la détenir ni

la connaître, ce dès l'origine. Un site commercial sur internet ayant en stock les données informatiques relatives aux instruments de paiement de ses clients, ne peut offrir à ceux-ci qu'une garantie de sécurité imparfaite face à des pirates informatiques de plus en plus professionnels.

Le traitement des informations appelle également de meilleures protections, de par la multiplication des acteurs qu'il implique au-delà du réceptionnaire, qu'il informe ou à qui il transmet un pouvoir d'appréciation ou d'action. C'est un risque d'action malheureuse qu'il devient possible d'interdire fonctionnellement par le présent procédé. Tant sur la détention que sur l'usage des données, la tendance à l'infogérance ou plus récemment au « nuage numérique », tout comme à la gestion de ses comptes bancaires à domicile par un particulier, multiplie les fragilités dans les systèmes informatiques. Encadrer ces trois fonctions basiques que sont la communication, l'enregistrement ou le traitement, peut s'obtenir par le biais d'un signe distinctif et caractéristique inséré dans le protocole et doté de propriétés fonctionnelles.

La relation entre communication, traitement et enregistrement ne relève pas d'un ordonnancement chronologique standard, ni d'une obligation d'activation des trois : il est ainsi possible de détenir une information sans en avoir connaissance effective, autant qu'il est possible d'en avoir connaissance sans en garder la mémoire. On peut également retransmettre une information sans l'avoir traitée.

Les risques résultant de cette gestion d'information sont manifestes s'agissant d'entreprises, associations ou institutionnels qui ne disposent pas des meilleurs moyens ou savoir-faire pour la protéger ou l'encadrer dans la durée, comme cela est régulièrement montré lors des affaires de captation par des personnes extérieures aussi bien qu'intérieures. Voire d'acteurs légitimes mais susceptibles d'en faire un usage déviant, non désiré ou non permis par l'expéditeur, telle qu'une revente à un tiers pour usage commercial ou fichage.

Toutefois, même un acteur compétent en gestion de la sécurité des informations offrirait un risque résiduel incompressible lié au seul fait de

centraliser et de détenir par-devers lui trop d'informations convergentes à caractère personnel ou sensible.

Un avantage du présent mécanisme tient en sa capacité à encadrer cette communication, cette détention ou ce traitement de données jugées sensibles, pour remédier aux faiblesses évoquées. Il en résulte une réduction du risque, tant durant leurs divers usages que dans la possibilité de leur perte, vol, piratage ou autre forme de déperdition, de mise au rebut imparfaite, de duplication, de sous-traitance, d'externalisation ou encore de transfert juridique de propriété tel qu'un rachat ultérieur de fonds de commerce.

La présente invention modifie, recompose et élargit des dispositifs exprimés dans la demande de brevet FR 2 932 043 portant sur un procédé de traçabilité et de résurgence de flux pseudonymisés sur des réseaux de communication, et procédé d'émission de flux informatif apte à sécuriser le trafic de données et ses destinataires. Ce dernier développait essentiellement des solutions pour harmoniser observation des flux et respect de l'intimité. La nouvelle invention étoffe la partie liée à la confidentialité numérique, et l'articule avec des fonctions nouvelles et ici centrales de sécurisation de données, de contrôle d'action et de distribution d'information. Elle leur adjoint de surcroît de nouvelles formes de masquage d'identité pouvant faire office de démultiplicateur d'identités.

À cette fin, elle s'appuie en partie sur le système de marquage distinctif et caractéristique, inséré au niveau du protocole, et doté de propriétés fonctionnelles, tel que décrit notamment dans la demande de brevet FR 2 932 043.

Ce signe caractéristique est appelé griffage, par analogie avec l'apposition d'une griffe en tant que signature qui personnalise mais aussi en tant que marque qui modifie, signale et sert de signe extérieur de référencement. Ce terme de marquage, qui englobe tout autant une possible encapsulation, recouvre un mode opératoire consistant en un ajout, une amputation ou une modification caractéristique, sur un protocole, tout en respectant le standard de ce protocole. À titre d'exemples, il peut s'agir de l'étiquetage ou du tatouage d'un paquet IP, d'un marquage stéganographique ou encore

l'utilisation d'un protocole supplémentaire. Ce griffage endosse plusieurs statuts :

- signe distinctif, à sa réception ou son observation par un tiers ;
- signe de reconnaissance, lors d'échanges ultérieurs ou parallèles.

Ce double statut permettait, via le jeu d'acteurs nécessaires pour manipuler et interpréter ces griffages, de leur attribuer des fonctionnalités.

Les propriétés générales qui en découlaient pour ce système étaient :

- fonctionnelle ;
- cryptonymique, en tant que griffe d'un auteur apposée dans un protocole, qui le désigne et l'identifie, si de besoin sans le nommer autrement que par une convention arbitraire.

Obtenir connaissance des fonctions et de certains attributs d'identité concernés, nécessite de s'adresser à une autorité d'anonymisation, dont le rôle informateur rend ces deux propriétés opérantes. Le principal emploi conjoint des dispositions fonctionnelle et cryptonymique consiste en une interdiction de lecture de l'identité d'un auteur de courrier, telle qu'elle apparaît sinon dans le reste du protocole. Ce faisant, le dispositif aboutit à un griffage masquant de cette identité, réelle ou de communication, et apte à servir d'identité de substitution, directement ou indirectement.

Hormis ce premier usage, ce système fonctionnel y restait pour l'essentiel circonscrit à des tâches de lecture et de retransmission. Ces fonctions se trouvent présentement accrues, en passant de la seule lecture à l'ensemble des tâches possibles de traitement et de communication, et surtout en leur adjoignant les fonctions relatives à la mise en mémoire. Il pourrait en effet sinon y avoir, chez le destinataire d'un envoi, conservation d'une donnée même sans l'avoir consultée sur l'instant ou a posteriori, conservation qui constitue une menace permanente de rupture d'une règle première d'ignorance.

Un deuxième perfectionnement par rapport au griffage du protocole consiste à varier ses effets, de plusieurs manières :

- Il peut s'agir de disposer simultanément, pour un même auteur, de plusieurs griffages, activables par choix ou selon des chartes d'emploi définies et actualisables si de besoin. Ces signes seront soit

dissemblables en soi, soit distinguables par un autre biais tel par exemple qu'un horaire qui soit ou non de travail au bureau, donc de présence ou non sur place de la personne voulue. Chacun des griffages correspond alors à des informations ou consignes déterminées, telle que la désignation d'un seul des comptes en banque d'une personne. Ceci permettra à cet auteur, en cas d'achat auprès d'un site internet, de choisir son compte à faire débiter. Ce caractère adaptatif se retrouvera sur le fait d'avoir fait préenregistrer plusieurs comptes bancaires, ou plusieurs cartes de paiement ou encore par exemple plusieurs adresses et plus généralement tout attribut susceptible d'exister en plusieurs exemplaires.

- Une autre voie pour varier les effets consisterait à les prédéfinir en fonction de chaque interlocuteur recensé par avance, ou de modalités-types suivies par eux pour effectuer la requête. De la sorte, une même marque ne donnerait pas la délivrance en retour de la même information selon que l'interlocuteur soit une banque ou un office postal. Il pourrait aussi s'agir de deux réponses différentes pour deux banques différentes. D'une manière générale, une réponse pourrait être adaptée au qui demande, en tant que personne aussi bien que de par un statut prédéfini, au quand il demande, au où il envoie sa demande, par exemple depuis telle entreprise référencée ou depuis tel pays, au comment il demande, par exemple selon des procédures ou formulaires qui lui sont exclusivement réservés.

Un troisième perfectionnement tient au fait que le nombre de griffage dans un protocole donné n'est plus envisagé comme un singulier obligatoire. Plusieurs de ces signes distinctifs seront simultanément possibles dans un courrier ou un fichier, soit pour des usages ou des usagers indépendants, soit pour créer entre ces signes des liaisons, des cautionnements respectifs, ou des filiations ponctuelles. Il devient également envisageable que leur présence autant que par exemple leur disposition spatiale respective, soient porteuses d'une signification supplémentaire, interprétable par tous les réceptionnaires ou seulement certains, assistés ou non en cette occasion par l'autorité d'anonymisation.

Un quatrième perfectionnement par rapport au griffage du protocole tient au fait que soient concernés non plus seulement des protocoles de communication, mais des protocoles affectés à des données statiques. Ainsi, il ne s'agit plus seulement de contenus liés à un flux, mais de contenus susceptibles d'être destinataires d'un flux. Toute consigne, demande ou information envoyée à ces contenus se trouvant confrontée initialement à leur protocole et assujettie :

- soit à une consigne déjà connue de l'expéditeur et correspondant au griffage dont la présence est alors constatée par lui dans le protocole dont dépendent ces données.
- soit à la compréhension préalable de ce griffage inséré dans le protocole. Compréhension qui obligera à communiquer avec une autorité d'anonymisation ou avec une entité nommée serrure numérique, capables d'émettre en contrepartie, ou de laisser accès à, des requêtes, des conditions, des limitations ou par exemple encore des interdictions.

Il pourra ainsi s'agir d'interdire l'accès à certaines données vis-à-vis d'un interlocuteur non désiré ou explicitement mis à l'index, ou parmi d'autres possibilités de ne l'autoriser qu'à certains horaires où un opérateur humain serait physiquement présent.

Un cinquième perfectionnement tient au fait que le griffage, également signe de reconnaissance, se voit revêtu de propriétés englobant celles d'un passeport : il permet l'accès ou la délivrance de données autres que fonctionnelles, comme l'étaient les consignes. Il dépasse ce statut de passeport, puisqu'il est en lui-même l'équivalent d'une clé pour accéder à une salle des coffres virtuelle, dans laquelle certains coffres sont prévus pour sa venue.

L'autorité d'anonymisation est couplée avec un mécanisme qualifié de serrure numérique. Ces deux entités peuvent se trouver réunies en une, mais pourront avantageusement être maintenues en situation autonome, complétée par des transferts d'information entre elles.

Par la suite sera nommée « serrure numérique » un dispositif répondant autant à une donnée numérique qu'à un signal analogique, et dont la réponse pourra être aussi bien numérique qu'analogique.

L'autorité d'anonymisation sert d'interface avec l'auteur, en lui octroyant les systèmes de griffage, en convenant de la signification et de l'équivalence de ces griffages en consignes, informations ou valeurs. Elle convient aussi, avec et pour lui, d'un pseudonyme stable lié aux cryptonymes successifs que sont ces griffages, et en le connaissant par son identité réelle. Elle pourra également gérer un autre masquage d'identité réelle, par le moyen de polynymes.

La serrure numérique reçoit, a minima, information des griffages de l'auteur. Dans des configurations plus larges, elle peut recevoir le pseudonyme de cet auteur aussi bien que ses coordonnées ou identité de télécommunications. Celles-ci correspondant à ce qui apparaît dans le protocole de communication complet d'un de ses envois.
Le fonctionnement de cette serrure numérique se subdivise en deux catégories d'affectations.

- Dans un mode premier, elle sert à valider la réalité, l'authenticité et l'actualité d'un griffage présenté à elle par le réceptionnaire d'un envoi portant une telle marque. Le griffage s'apparente alors à une clé physique que l'on chercherait à introduire dans une serrure physique, à seule fin de vérifier leur adéquation. Une telle vérification peut être menée de deux manières différentes :
    - selon la première, on se contentera de vérifier si le profil transversal de la clé, de manière imagée, avec ses rainures spécifiques, correspond bien au découpage de l'orifice d'entrée de la serrure, et donc vérifier si elle peut ou non pénétrer dans ce logement. Cette modalité d'emploi relève soit d'un secret dans l'obscurité si lors du test on ne voit pas le profil de l'entrée de la serrure, ou du domaine du visible pour le vérificateur s'il a connaissance à la fois de la morphologie du profil transversal de la clé, et du profil de l'entrée de la serrure ;
    - selon la seconde, l'action ne consistera plus seulement à introduire la clé, mais à tenter de faire tourner la serrure. Il sera ici considéré que le profil longitudinal a pu demeurer

caché au réceptionnaire, parallèlement au fait qu'il n'aura pas accès à la morphologie interne du barillet. Par transposition, le profil longitudinal caché de la clé correspond ici à la partie restée fonctionnellement interdite d'accès au sein du protocole, et la morphologie interne du barillet correspond à cette même partie telle que connue par la serrure.

Le premier usage servira à valider qu'un griffage présenté par un réceptionnaire est réel, authentique et actuel.
Le deuxième usage servira à confirmer auprès du tiers vérificateur que la partie visible ou accessible pour lui dans le protocole, est bien couplée à la partie qui lui est restée invisible ou inaccessible, par exemple l'identité de communication. Le réceptionnaire saura ainsi que le griffage dont il a eu connaissance n'a pas été usurpé par un autre expéditeur, sans pour autant réellement connaître le vrai.

- Dans un deuxième mode, elle sert à tous les usages courants d'une serrure, tels qu'actionner un mécanisme ou un signal, autoriser ou non un accès, ouvrir un coffre, se faire reconnaître. Il pourra ici s'agir par exemple de procurer au réceptionnaire qui l'utilise, l'accès ou la réception d'une consigne ou d'une information. Cette fonction peut relever aussi bien d'un automatisme indépendant de la volonté de cet utilisateur, qu'à une configuration où il peut choisir ce dont il a besoin dans un coffre préalablement rempli de diverses données par l'auteur du courrier ou du fichier ainsi éventuellement que par l'autorité d'anonymisation. Ce coffre peut être personnalisé et réservé à l'accès d'un seul destinataire pré-désigné, autant qu'être accessible à plusieurs ou tous les destinataires éventuels. Ce coffre peut enfin s'apparenter aussi à un garde-meubles, dans le cas où l'auteur choisisse d'être son propre destinataire. L'accès au coffre peut être assujetti à toutes formes de contraintes ou conditions suspensives, telle qu'une ouverture seulement après une date déterminée.
Le dit coffre-fort d'un auteur donné peut être subdivisé et s'apparenter à un ensemble mural de boîtes aux lettres d'un immeuble, où chaque

résidant, c'est-à-dire ici chaque réceptionnaire, possède le moyen d'accéder au contenu de sa boîte. Chaque boîte comportant à cet effet une porte installée sur charnière. Les portes de l'ensemble des boîtes seraient, toutes ou partie, installées sur un panneau frontal commun, lui aussi sur charnière. De la sorte, l'auteur détenteur du coffre pourrait ouvrir toutes ses boîtes en une seule fois pour y faciliter la distribution des plis : ici des consignes et données.

Dans une variante intermédiaire, un réceptionnaire ponctuellement autorisé à accéder non plus à une mais à plusieurs boîtes, pourrait se voir envoyer une clé :

- soit ouvrant une à une les boîtes concernées ;
- soit ouvrant par exemple un unique panneau frontal correspondant à ces boîtes, à l'exclusion des autres boîtes, et selon une logique de cache qui continue à masquer les contenus ou les serrures de ces autres boîtes ;
- soit donner à ce réceptionnaire des accès discriminés à ces différentes boîtes, par exemple selon des règles chronologiques ou par une succession balisée et prédéterminée qui ne donne accès à telle boîte qu'après ouverture de telle autre ou après l'accomplissement de telle formalité intermédiaire.

Dans une progression optionnelle vers plus de sécurité, de discrétion, ou vers un statut de plus en plus passif de la serrure numérique, ce procédé peut donc s'apparenter en crescendo à un casier, une boîte aux lettres, une consigne automatique en gare, un garde-meubles ou une salle des coffres bancaire, tous sous une forme numérique ou analogique.

De même, la notion de clé et serrure numériques constitue l'extrême d'un éventail de fonctionnalités où des dispositifs moins pourvus pourraient être qualifiés passeport, sceau, sauf-conduit ou blanc-seing numériques.

La juxtaposition et la mise en synergie de ces configurations extrêmes que sont une clé numérique avec une serrure numérique et un coffre numérique, expriment le dispositif selon l'invention dans sa version la plus avantageuse au regard de ses objectifs principaux que sont la sécurité, la confidentialité

ainsi que le rôle passif et neutre du lieu de dépôt des secrets (consignes et données).
D'autres versions dégradées restent envisageables dans des configurations où ces critères tel que de sécurité perdent en importance.

La présente invention se différencie des actuels coffres-forts numériques ou autres systèmes de mise en consigne numérique, en ce que cette fonction n'est que seconde et complémentaire à la fonction principale de validation des divers profils du griffage et de l'éventuelle partie cachée d'un protocole. Outre le fait d'être seconde, elle est facultative puisque la fonction principale peut être installée seule.
L'invention se différencie aussi des systèmes de coffres numériques existants en ce que ceux-ci ne positionnent pas leur marquage ou leur signal de reconnaissance au niveau du protocole d'un courrier ou encore d'un fichier informatique.

Parmi les informations que le réceptionnaire peut recueillir via cette serrure numérique, se trouve en particulier le pseudonyme correspondant à tel griffage faisant cryptonyme. Ce recueil peut se faire à nouveau de manière automatisée autant que par l'ouverture d'un coffre numérique. Le pseudonyme pouvant toutefois, dans son alternative initiale, être accessible auprès de l'autorité d'anonymisation.

Un tel recueil peut également et avantageusement se faire par un système de marquage dans une serrure numérique, où un cryptonyme inséré en elle en ressortirait avec l'empreinte supplémentaire de ce pseudonyme. Ce, de la même manière qu'une clé physique non taillée dans son sens longitudinal peut être introduite dans une serrure et se voir marquée à l'intérieur, par craie ou peinture préalablement aspergée sur les garnitures internes, d'un contour dessinant ce profil recherché. Ou ici, par transposition dans une forme basique, d'un contour dessinant le pseudonyme. Ce procédé n'est pas destiné à ouvrir la serrure, mais à prendre connaissance d'une seconde information, le profil longitudinal de la clé, quand on connaît une première information, le profil transversal de cette même clé, qui permet de l'introduire dans la serrure. Ce mécanisme est utilisable autant pour obtenir un

pseudonyme que pour obtenir connaissance par exemple de la partie restée inaccessible du protocole de communication, ou que toute consigne ou information. Il diffère des précédents « deuxièmes modes » qu'étaient l'actionnement d'un mécanisme, d'un signal, d'un accès ou l'ouverture d'un coffre. Présentement ne se produit en effet aucun actionnement, mais la simple apposition d'une empreinte informatrice sur, avec, autour ou dans une précédente empreinte faisant office de clé.

De la sorte, ne pas disposer d'un griffage faisant cryptonyme empêche de disposer ultérieurement du pseudonyme auquel il est lié, ou de toute autre information ou consigne jugée sensible. Ce faisant, la serrure numérique se distingue d'une fonction dite de « tiers de confiance » en ce que la confiance n'est pas nécessaire mais remplacée par un procédé mécanique où l'accès à une étape informative est matériellement conditionnée à la bonne maîtrise de la précédente étape. De même, cette serrure voit son rôle de distributrice de secrets couplé à celui de facilitateur de vérification. Elle est à la fois active et passive, tout en pouvant a minima se contenter du second de ces deux statuts. Enfin, le caractère classiquement multi-parties des secrets est amendé en ce que la serrure numérique peut être considérée, selon son mode de déploiement, comme un simple jalon passif entre deux communicants.
Ce procédé abolit la trinité entre un producteur et un consommateur arbitrée par un tiers de confiance, ou des tierces parties de confiance intéropérables, qui se partagent des secrets et des informations selon une heuristique temporelle (un protocole cryptographique entre deux sujets, sous la supervision d'une entité de confiance).

La fonction habituellement dévolue à un « tiers de confiance » est de surcroît subdivisée entre une autorité d'anonymisation et cette serrure numérique. Ainsi, l'autorité d'anonymisation peut rester éventuellement ignorante de ce qui sera déposé au coffre, ou de qui vérifiera un griffage. Tout comme la serrure numérique peut ignorer l'identité réelle du possesseur de ce signe.

Dans une variante, le réceptionnaire pourra se voir astreint, pour pouvoir vérifier un griffage auprès de la serrure numérique ou pour activer un

mécanisme, à faire lui-même usage d'un système d'identification, ou plus fréquemment d'authentification, qui le signale comme réceptionnaire connu et autorisé. Tel que le serait un site internet s'étant abonné auprès de ce dispositif de serrure ou auprès d'une autorité habilitante, par exemple l'autorité d'anonymisation. Une configuration pourrait être un coffre à deux serrures, ou au-delà de deux puisqu'un plafond limitatif ne résulterait que de la volonté des parties. Cette seconde clé numérique sera nommée par la suite contre-clé. Cette variante complète et prolonge le principe voulant que chaque nouvelle étape informative soit précédée par la capacité à démontrer la maîtrise de la précédente étape : prouver ici que l'on dispose de sa propre homologation permet ensuite de vérifier un griffage dont la bonne conformité pourra conduire à d'autres informations.

Il serait possible qu'un réceptionnaire telle qu'une entreprise ou une administration dispose de plusieurs contre-clés pour se faire reconnaître et participer à l'ouverture d'un coffre, de manière à garantir que la personne préposée à cette tâche l'ouvre en compagnie par exemple d'un collègue prédéfini et porteur d'une deuxième contre-clé. Ce tiers, auxiliaire, témoin ou garant, pour confirmer sa présence ou sa bonne information, peut être encore un huissier ou un notaire, à titre d'exemple. Ce peut être l'auteur initial d'un courrier, ou le détenteur d'un fichier informatique marqué au niveau de son protocole, et qui désirerait être informé de l'usage ultérieur fait de ce griffage ou de ce fichier, et être présent à cette occasion. Ce peut être également l'autorité d'anonymisation.

Une autre possibilité voudra par exemple que l'ouverture d'un coffre donné nécessite une contre-clé donnée, qui ne sera pas admise pour un autre coffre ou tout autre mécanisme.

Une troisième possibilité serait que cette contre-clé soit active seulement selon conditions, telle qu'être utilisée durant les horaires normaux d'activité de l'entreprise qui la détient.

En résumé de situations où un coffre pourrait avoir plusieurs serrures :

- la deuxième serrure pourrait être destinée à une contre-clé donnée appartenant à un seul réceptionnaire ;

- cette deuxième serrure pourrait recevoir diverses contre-clés, particularisées ou non, appartenant chacune à un réceptionnaire autorisé ;
- ce coffre pourrait avoir un nombre illimité de serrures pour recevoir chacune un ou plusieurs réceptionnaires autorisés ;
- ce coffre pourrait avoir plusieurs serrures pour recevoir plusieurs contre-clés d'un seul réceptionnaire autorisé. Cette même configuration étant autorisée à plusieurs jeux de clés appartenant chacun à un réceptionnaire autorisé.

En expression des mesures possibles pour entourer l'envoi de griffages d'une plus grande sécurité vis-à-vis notamment de pirates informatiques, le fait d'utiliser une clé ou une contre-clé sur une serrure numérique pourrait être déclencheur de son obsolescence. Usage de ces clés pouvant résulter du réceptionnaire prévu, ou a fortiori d'un tiers non autorisé. Cette obsolescence déclencherait sa permutation au niveau de l'auteur s'agissant de la clé, ou du réceptionnaire s'agissant de la contre-clé. Par souci de souplesse, elle peut résulter d'un autre nombre d'usages, ou d'une contrainte tel qu'un respect d'une procédure précise pour le bon accès au contenu du coffre ou au mécanisme.

Une transposition plus générale de cette philosophie serait un griffage à usage unique ou à usage s'achevant au premier débit ou premier emploi, même hors serrure.

Outre ce premier dispositif ci-avant de marquage par un signe distinctif, la demande de brevet FR 2 932 043 repose également sur un double principe :

- chercher à scinder une information sensible en sous-parties, en vue de la disperser. Ceci dans une proportion modérée par des critères de rationalité technique ou de maintien de la bonne gestion des processus administratifs ou productifs auxquels concourre cette information ;
- faire détenir, transiter ou viser chaque sous-partie de l'information par des intervenants techniques autonomes.

La présente invention se différencie premièrement de la demande de brevet FR 2 932 043 sur ce point par le fait qu'elle en modifie l'architecture générale favorite, par l'adoption de lignes de scission différentes. Les entités

antérieures, qui fonctionnaient à la base en mode séquencé et sur un type de tâche central qu'est le contrôle, deviennent aptes à travailler en parallèle, et à des tâches autres. Par ailleurs, la présence initiale de trois entités d'observation se trouve désormais assouplie à un nombre ouvert de réceptionnaires, et plus adaptatif. Le fait qu'il soit potentiellement plus grand sera fréquemment vital pour empêcher qu'un même acteur reste seul impliqué dans le traitement de plusieurs tâches sensibles ou dans la connaissance de trop d'informations susceptibles d'éclairer simultanément plusieurs pans de vie professionnelle ou privée. La bonne canalisation associée au cloisonnement permet que le processus soit mené de front par plusieurs intervenants ne disposant chacun que de certains « morceaux de puzzle » de l'information sensible globale nécessaire aux tâches, préalablement parcellisées, qui leur sont respectivement dévolues. Aucun d'eux, à aucun moment, n'a à connaître la totalité des données sensibles liées à un client ou un auteur.

De plus, l'invention fait désormais détenir chaque sous-partie de l'information par un intervenant technique que l'on peut choisir sur des critères de compétence sécuritaire, d'autonomie, d'éthique ou de performance, plus souples et mieux configurables. Élément qui permet son application à des modèles économiques plus variés, depuis le commerce électronique, avec un numéro de carte bancaire rapporté à un achat de fleurs livrables à une adresse différente de celle du payeur, jusqu'aux informations médicales destinées à un test de laborantin. Ceci lorsqu'il est souhaité de sa part un retour par voie postale ou de télécommunication, mais sans que le laboratoire ait jamais connaissance, à propos de l'expéditeur, de son nom et adresse, ou encore de son prénom ou élément d'état civil tel que « Monsieur », « Madame » ou « Mademoiselle » révélateurs du sexe ou de l'état marital.

L'invention se particularise deuxièmement à propos de ce cloisonnement, en ce qu'elle ne propose pas le même arbitrage entre informations lisibles ou non, au sens notamment d'accessibles par un réceptionnaire donné. Parmi ces nouveaux arbitrages, se trouve le fait de cloisonner, canaliser et, si de besoin par la suite ou en intervalle, confronter, juxtaposer ou composer, des informations présentes à la fois sur le protocole d'un flux de

télécommunications telle que l'adresse de l'expéditeur, et hors de ce protocole voire hors de ce courrier ou même hors de l'autorité d'anonymisation ou de la serrure numérique, tels que les références d'un compte bancaire.

Il en résulte au total des fonctionnalités nouvelles, qui permettent d'élargir le champ des informations protégeables ou contrôlables. De manière plus générale, une particularité de l'invention tient, en matière de protection contre les risques résultant de la détention d'une information, au fait que ce ne soit plus véritablement une détention, avec le fait que ce ne soit plus vraiment « une » information, tant dans son acception singulière qu'exhaustive, tant par rapport à une unité de lieu, de temps et d'action. Le procédé combine dans des proportions ajustables entre elles et évolutives, la modification à la fois des caractères informatif et exhaustif. Elle joue également sur le fait de les rendre à volonté incompréhensibles ou inexpressives en soi. À ce couple de solutions imbriquées, peuvent être ajoutés d'autres protections, telles que rendre certaines données indéchiffrables.

En conséquence de ces perfectionnements en matière de cloisonnement et de canalisation, l'invention se caractérise en ce qu'elle génère un système de contrôle, de segmentation et de dispersion régulée de l'ensemble des données sensibles, qui lui est propre. Tout en permettant cependant que soit mené à bien un processus global sophistiqué de par la multitude et l'imbrication de ses facettes, et nécessitant quant à lui de disposer de toutes ces informations pour sa bonne réalisation. Un exemple de cette sophistication serait la passation d'achat à faire livrer et à payer, tout en restant anonyme en tout point désiré, auprès non pas du prestataire mais des prestataires, au pluriel, s'agissant par exemple d'une enchère sur un site de vente à distance, où l'anonymat sera désiré vis-à-vis du détenteur de l'objet en vente, autant que du site ayant géré la mise aux enchères. L'une des spécificités de l'invention est effectivement de parvenir à coordonner cette forte complexité d'une action avec une forte dispersion de ses ressources informatives. Elle occasionne volontairement une ignorance partielle ou totale, ou une incapacité d'accès, envers des éléments d'identité tels que civile, bancaire, postale, domiciliaire ou encore fiscale, mais

ignorance palliée d'une part par la bonne articulation entre cryptonymes et pseudonyme d'une même personne, et d'autre part par le bon enchaînement programmé et canalisé des communications entre réceptionnaire central et réceptionnaires périphériques.

De fait, l'invention est apte à procéder à une canalisation à la fois parallèle ou séquentielle :

- elle segmente et confine des sujets, des objets, des données, des tâches et des rôles tout en les coordonnant à distance ;
- elle conçoit des enchaînements qui permettront de maintenir le bon fonctionnement d'un processus par étapes tel que prise de commande, réservation, imputation, facturation, débit, expédition.

L'ignorance dans laquelle sera maintenu le réceptionnaire central pourra, dans une variante, affecter d'autres éléments que les seuls attributs d'identité, à l'exemple d'une ignorance de sa part, pour tout ou partie, de la consigne précisant les tâches à accomplir au profit de l'auteur. La sous-partie ignorée renvoyant pour sa prise en compte au même principe d'appel à un réceptionnaire périphérique. À titre d'illustration, il peut s'agir d'une réservation de deux billets d'avion, où l'on ne souhaite pas que l'agence de voyage locale connaisse l'identité de l'auteur, gérée seule par un premier réceptionnaire périphérique. Réservation complétée par une seconde partie de la consigne accessible si de besoin seulement à un deuxième réceptionnaire périphérique, précisant par exemple le nom de la personne accompagnatrice à placer à côté du premier siège réservé. De la sorte, aucun des trois réceptionnaires n'aura mémoire des deux noms de voyageurs. Une autre configuration permettrait qu'aucun des réceptionnaires ayant connaissance d'un des noms ne sache avec certitude qu'il s'agit de deux sièges côte à côte.

La présente logique de cloisonnement est parachevée en ce qu'elle irradie sur la gestion des identités ci-après. De ce point de vue, la présente invention peut se décrire comme un système de cloisonnement et de scission à la fois d'entités, de tâches et d'identités. Chacun de ces deux champs pouvant être activé seul, mais trouve dans leur juxtaposition des effets supplémentaires en matière principalement d'intimité numérique.

Cloisonnement et canalisation affectent plus généralement les quantités et qualités de ces entités ou de ces actions, l'aspect quantitatif concernant leur nombre et leur périmètre, le qualitatif portant sur leur nature et leur identité.

Au sein de ce qui était antérieurement présenté comme un triple dispositif, et relativement au troisième de ceux-ci, existe une autorité dite d'anonymisation, déjà mentionnée dans la demande de brevet FR 2 932 043. Cette entité a originellement une triple fonction :

- accorder à des auteurs la possession d'un signe distinctif et caractéristique qui soit propre à chacun. Griffage inséré dans les protocoles de communication lors de ses futurs courriers. Elle distribue le dispositif de marquage, installable soit dans, sur ou en sortie de l'équipement de l'auteur, tel qu'un ordinateur, soit en un point ultérieur c'est-à-dire notamment sur le réseau ou chez un intermédiaire ;
- distribuer aux réceptionnaires les outils fonctionnels leur empêchant automatiquement l'accès à certaines données, en présence de ce griffage. Ces outils fonctionnels peuvent prendre la forme par exemple d'un logiciel ou d'un composant électronique, pouvant faire office de boîte noire installée en entrée de flux, si de besoin inviolable par son dépositaire. Il peut aussi s'agir de systèmes de dérivation du flux ;
- répondre à la justice, en lui transmettant l'équivalence entre un griffage et l'identité réelle d'une personne, au cas où des situations illégales aient été constatées à l'occasion de l'auscultation des flux, action qui constituait une activité de base de la demande de brevet FR 2 932 043.

Par rapport à cette demande de brevet, la présente invention apporte plusieurs perfectionnements quant à l'anonymisation :

- La première des évolutions fait que l'autorité d'anonymisation peut accorder l'insertion de griffages dans des protocoles de fichiers statiques susceptibles d'être réceptionnaires d'un flux telle qu'une requête.

- La deuxième tient en l'apparition d'une structure de type bicéphale, où l'autorité d'anonymisation se voit adjoindre une seconde entité, nommée serrure numérique. Cette évolution est facilitée par l'enrichissement parallèle des fonctionnalités du griffage, et par la possibilité d'accroître la variété des consignes initiales ou des données destinées au réceptionnaire par le truchement de ce signe de reconnaissance.

- L'invention permet troisièmement l'existence de plusieurs entités d'anonymisation au lieu d'une seule, ainsi que l'expression de préférences émanant de leurs usagers.

- Un quatrième point tient à ce que la frontière entre l'autorité d'anonymisation et les réceptionnaires périphériques est adaptative et déplaçable si de besoin, permettant par exemple à la première de détenir quelques données à caractère bancaire, ou inversement à une banque de connaître ou gérer diverses composantes du lien identité-pseudonyme. Dans un cas de fusion des deux, le rôle d'autorité d'anonymisation pourrait être dévolu à un groupement de cartes bancaires ou à une banque, au même titre qu'elle mettrait en sûreté le bien d'un particulier dans sa salle des coffres. Un cas extrême verrait la fusion partielle entre quelques fonctions de l'autorité d'anonymisation et, non plus un réceptionnaire périphérique, mais le réceptionnaire central. Ainsi ce dernier connaîtrait immédiatement la correspondance entre tel griffage et telle consigne. Toutefois cette configuration possible présenterait des points faibles en matière à la fois de sécurité et de confidentialité, qui atténueraient plusieurs avantages de l'invention. Ce cloisonnement a minima permettrait néanmoins de maintenir une certaine dispersion utile des rôles entre les divers types de réceptionnaires, selon une volonté d'autorégulation.

- En cinquième lieu, les réponses fournissables par cette entité se trouvent élargies. Le griffage n'est plus seulement un moyen de dialogue entre l'autorité d'anonymisation et les réceptionnaires pour permettre à ces derniers la compréhension de consignes initiales jusqu'alors d'empêchement de lecture à propos d'un courrier. Quant aux

informations, dans la demande de brevet FR 2 932 043, il s'agit de transmettre pour l'essentiel la correspondance entre un cryptonyme et un pseudonyme, ou éventuellement de mentionner par exemple si ce visiteur restant inconnu était ou non un habitué.

En sus, simultanément ou par la suite, l'autorité ou la serrure numérique répondront dorénavant en transmettant ou laissant accès, selon leur droit d'en connaître, à l'équivalence entre tel griffage faisant cryptonyme et par exemple une identité réelle ou autre attribut ponctuel d'une personne telle qu'une adresse, aussi bien que tout type de donnée mise en conservation, par exemple un élément de calcul déposé par cette personne, et toute sorte de consigne. Ce peut être un mélange d'informations et de prescriptions : données mathématiques et test à mener avec, données comptables et ventilation à appliquer sur les livres de comptes, cotes et lancement d'un usinage. Le champ des informations ou des prescriptions convenues n'est plus limitatif a priori. Une information déposée peut aussi s'apparenter au principe d'un demi billet de banque, déchiré en deux, et sans laquelle la seconde partie déjà connue ou détenue par un réceptionnaire resterait inemployable, ou incompréhensible s'agissant d'une image moins connue qu'un billet.

Lesquelles données seront diffusables selon des règles convenues avec l'auteur, ou au sein d'un cercle d'entente plus large qui englobera des réceptionnaires. Une consigne transmise peut elle-même être soumise à condition supplémentaire, par exemple procéder à un débit bancaire mais après la fin de mois.

Le champ potentiel des informations et surtout des consignes sera particulièrement varié lors de relations inter-entreprises ou internes à l'une d'elles. La meilleure connaissance interpersonnelle, ajoutée à la facilité à s'aligner collectivement sur un standard technique ou comportemental, facilitera l'adoption de ce dernier. Sa souplesse d'emploi et son évolutivité seront également plus grandes. Le fait que ces activités productives privilégient a priori moins l'anonymat des acteurs, comparativement à d'autres exigences de sécurité, de contrôle

ou de rendement, souligne que la hiérarchie originelle devient adaptative et configurable à l'ordre des priorités des usagers.

En contexte professionnel, le dispositif selon l'invention correspond à des déploiements possibles dans les processus décisionnaires, administratifs, productifs ou de négociation, impliquant plusieurs personnes ou services au sein d'entreprises, les collaborations multi-sites, les sous-traitances, la gestion de projet dite en plateau, où plusieurs sociétés participent à un même développement à partir de procédures collaboratives communes, auxquelles le présent dispositif de griffage fonctionnel apporte une traduction concrète.
Les actions concernées pourront être des passations d'ordre, la supervision de tâches, des obligations de visa ou d'autorisation préalables à une action, et plus généralement toutes activités s'inscrivant dans une chaîne de commandement, une chaîne logistique ou encore un suivi comptable. Entre autres exemples, il peut s'agir du lancement d'une impression de livre chez un imprimeur à partir d'épreuves numérisées, où la consigne correspondant au griffage inséré dans le protocole du fichier stipulera d'obtenir préalablement un bon à tirer de la part de l'ayant-droit ou de l'éditeur. Il peut également s'agir d'assujettir ou coordonner un réseau de capteurs et d'actuateurs, telle qu'une flotte de robots

La sécurité autant que la confidentialité des informations pourra y être subordonnée au droit d'accès, au droit d'en connaître, à la vérification préalable des accréditations d'une personne ou d'une entreprise dans les métiers à haute sécurité qui classifient leurs ressources et habilitent leurs interlocuteurs.
La sécurité des personnes, des biens et des bâtiments peut nécessiter la présence de ces marquages dont le caractère fonctionnellement incontournable pour un réceptionnaire ou un utilisateur les assimileront à des dispositifs dits Poka-Yoké ou « anti-imbécile » : expression désignant un mécanisme entouré ou précédé d'une protection qui empêche son accès ou son emploi à une personne supposée maladroite au point de commettre toute erreur imaginable, ou pour réduire la

probabilité d'occurrence de ces erreurs. Ceci pourra être déployé lorsqu'une donnée ou un signal, délivré par l'autorité d'anonymisation ou la serrure numérique, participe à la bonne mise en œuvre d'un mécanisme dangereux telle que presse hydraulique, portique ou chaîne d'assemblage, ou vital tel qu'un système électrique de bloc opératoire chirurgical, ou encore un processus coûteux et irréversible.

Outre la délivrance de consignes, il peut s'agir de la délivrance d'informations permettant de compléter un travail ou de le faciliter par une connexion avec des modes d'emploi, voire à rendre obligatoire le recours à ces modes d'emploi. Faute d'une traçabilité ou d'une obligation matérialisée, comme le permettra l'invention, diverses pratiques industrielles ou domestiques occasionnent des accidents par simple négligence ou indifférence vis-à-vis de la prise de connaissance préalable de tels modes d'emploi, à l'image des fabricants d'engins de génie civil qui redoutent que le premier geste d'un réceptionnaire lors de la livraison sera de la mettre en marche pour l'essayer sur chantier, avant de vérifier si des prescriptions telle que de lubrification préalable des pièces tournantes étaient exigées de lui. La présence grandissante d'électronique sur ces engins, donc de systèmes d'information ayant recours à des protocoles informatiques, permettra d'y déployer le présent dispositif.

En matière toujours d'information, l'invention pourra faire office de pense-bête relatif à telle intention ou telle tâche. À l'extrême, dans le cas d'un fichier informatique ou d'un courrier sans contenu, le protocole avec griffage sera transmetteur à lui seul, et un pense-bête dans l'absolu, assimilable dans sa finalité aux papillons de papier collables sur un mur et portant une quelconque mention, que l'auteur destine à lui-même ou à autrui lorsqu'il les verra. L'aspect pense-bête rejoignant le principe d'anti-oubli, lui-même souvent raccordable au Poka Yoké ou anti-erreur, tous couvrant au total un spectre allant des besoins de mémorisation et transmission aux besoins de coordination et de sécurisation.

Ce précédent cas de figure d'un fichier informatique ou d'un courrier sans contenu, couvre un champ d'application où le griffage, avec ou sans le reste du protocole, peut notamment servir de :

- système anti-oubli, lorsque la seule fin du dispositif est d'adresser un message ou un signal ;
- système anti-répudiation, puisque le réceptionnaire se sera signalé auprès de l'autorité d'anonymisation pour comprendre la signification du griffage. Cette attestation de réception pouvant rester circonscrite à la dite autorité, donc, selon le mode de déploiement retenu, potentiellement ignorée des autres interlocuteurs, ou sue d'eux seulement pour ce qu'ils ont besoin d'en connaître. Ce, sous des modalités convenues, par exemple à retardement ou en partie anonymisée ;
- système anti-duplication, lorsque le griffage présente en soi un rôle ou une signification ne devenant opérants ou compréhensibles que par le contact obligé avec l'autorité d'anonymisation. Cette dernière étant alors à même d'identifier des doublons, et de les distinguer de transferts normaux du griffage entre acteurs participant à un processus. Cette disposition permettra un usage pour exprimer et garantir des grandeurs, des valeurs ou des symboliques : il peut s'agir d'un équivalent au système d'objet témoin, matérialisé par exemple par un drapeau unique passant de main en main entre conducteurs sur les axes ferroviaires à voie unique, où sa réception et elle seule, en tant qu'indicatrice d'une dépossession d'un précédent train, permet d'y envoyer un nouveau convoi sans risque de collision. Ce principe également de jeton, utilisé dans les technologies informatiques et de communication, s'articulerait ici dans une mise en situation où l'autorité d'anonymisation fait office de chef de gare superviseur de ce signe distinctif passant entre des réceptionnaires successifs. Cette finalité anti-duplication est une possible réponse à des dangers nés de la facilité de cloner des données numériques.

Ces cas de figure confèrent à l'autorité d'anonymisation un statut d'organisateur ou tout au moins de garant, à l'image d'un huissier, d'un notaire ou d'une chambre d'enregistrement apte à prendre acte d'une rencontre, d'un contact ou d'un dialogue. La chambre d'enregistrement pouvant accéder à des fonctions plus sophistiquées telle que de chambre de compensation.

À ces titres, l'autorité d'anonymisation est un distributeur autant qu'un réceptionnaire de secrets. Cette fonction d'officier public est confortée par le fait que la délivrance de contre-clés peut servir à ce qu'un tiers soit présent : ce n'est donc pas seulement sa garantie à travers sa présence que l'autorité d'anonymisation apporte mais aussi à travers celle d'autrui si de besoin.

Le système anti-répudiation présenté ci-avant relève de la traçabilité, et celui sur la duplication ajoute un contrôle quantitatif à ce précédent traçage.

Qu'il s'agisse d'anti-oubli, d'anti-répudiation ou d'anti-doublon, le procédé rejoint des finalités fréquentes d'anti-accident aussi bien que d'aide à la régulation, c'est-à-dire souvent d'anti-gaspillage.

Ces dispositions permettent de créer des équivalents aux envois avec accusé de réception, aux cachets postaux, aux scellés et autres sceaux exprimant une signification doublée d'une exclusivité, d'une rareté ou tout au moins d'une quantité sous contrôle. Dans le même domaine postal, il peut s'agir d'émettre des griffages revêtus de valeur faciale, à l'instar d'un timbre postal ou fiscal.

Par ces précédentes caractéristiques, le dispositif selon l'invention couvre des métiers basés sur la confiance, fiduciarus, dont ceux relatifs à la création ou la manipulation d'argent. La compréhension de ce domaine souffre d'une confusion fréquente entre les diverses formes de monnaie, ainsi qu'avec leurs systèmes de transfert respectifs, dans le cadre ou non de transaction. Un transfert pouvant être un transport virtuel ou non.

Concernant les porte-monnaie électroniques de type carte à puce, leur recours à des protocoles informatiques ou de communication permet d'y déployer les présents griffages.

Concernant les autres solutions, une particularité du dispositif selon l'invention est de pouvoir servir de support tant à un dispositif d'échange

monétaire qu'à un système de paiement électronique, selon son mode de déploiement :

- soit que ce dispositif renforce la confiance dans le lien et le vecteur entre acteurs impliqués dans un même processus ;
- soit qu'il s'oriente autour d'acteurs qui bénéficient du plus de confiance aux yeux des autres ;
- soit enfin qu'il reporte la confiance sur lui dans son entier, alliant alors des sphères virtuelles et électroniques.

Pour les deux premiers cas de figure :

- Si la confiance est centrée dans le lien et le vecteur c'est-à-dire le griffage qui passe d'un expéditeur à un réceptionnaire, il s'apparente dès lors à un jeton, un coupon, un bon au porteur, une pièce ou un timbre fiscal, en revêtant une dimension fiduciaire, à l'instar d'un timbre virtuel. En tant que signe distinctif, il se voit reconnu une valeur, une grandeur ou une symbolique attachée à lui, envoyable vers autrui, libératoire autant que ce dernier veuille partager cette perception de valeur et croire à la robustesse du griffage et du mécanisme qui maintient son caractère unique. De manière basique et triviale, le griffage peut être un montant visiblement exprimé d'emblée par un nombre. Cependant, les propriétés cryptonymiques de ce griffage ouvrent un champ plus subtil et plus solide, où sa correspondance à une valeur renverra à une convention arbitraire entre au moins deux acteurs participant à l'échange, ou à toute autre activité interpersonnelle pouvant découler d'un consensus de valorisation (Le nombre susmentionné n'était lui-même qu'une convention devenue trop universelle). Outre les mondes virtuels, massivement multi-joueurs, l'invention peut toucher notamment les promesses de don et versements, les jeux en ligne, les enchères en ligne voire en direct, les appels à valoriser des biens ou des grandeurs immatérielles ainsi qu'à les échanger ou les fusionner sur ces bases de valorisation respective. Elle peut être partie prenante à un SEL (Système d'échange local) transposé soit totalement soit partiellement sur supports informatiques et de communication. Ce prolongement

pouvant laisser place à des passerelles avec les supports réels de ces SEL.

- Si la confiance est centrée sur un ou plusieurs acteurs, vers qui pointe le cloisonnement mis en œuvre par le dispositif, ceux-ci jouent un rôle pivot lors d'une intermédiation, à l'instar d'une banque. Ici le griffage ne revêt pas, en soi, cette précédente dimension fiduciaire et cette autonomie, mais il est un signe de reconnaissance qui renvoie les parties prenantes à un même secret détenu et géré hors de lui, selon le présent dispositif de réceptionnaires centraux et périphériques, ainsi que d'autorité d'anonymisation et de serrure numérique. Il est aussi fonctionnellement une consigne, telle que de virement. Le griffage est un passeport vers des acteurs aptes à assurer par exemple une transaction tout en apportant leur garantie aux parties prenantes quant à l'unité de compte concernée et à la passation en bonne et due forme du jeu d'écriture promis.

Les statuts des divers intervenants s'apparentent en partie à des entités connues dans la vie économique traditionnelle, à l'instar d'un organisme monétaire dans le premier cas de figure, et d'une chambre de compensation dans le second. Toutefois, le dispositif selon l'invention se particularise par le fait d'asseoir cette transposition au niveau des protocoles informatiques ou de communication, et par un outil multifonctions à la fois signe distinctif et de reconnaissance, doté de propriétés fonctionnelles qui cloisonnent et ainsi façonnent des rôles jusqu'à aboutir par exemple à ceux d'émission ou de compensation. Quoique suffisantes chacune, ces deux options ne s'excluent pas, où le griffage serait tantôt d'ordre fiduciaire et équivalent d'un billet de banque, tantôt d'ordre scriptural et équivalent d'un ordre de virement ou d'un chèque bancaire, voire hybride si le chèque, par la pratique de l'endos, devient en soi un véhicule pour une valeur inscrite. L'invention participe dès lors à la structuration de réseaux sociaux en leur offrant une palette de choix qui se concurrencent mais aussi se complètent en matière à la fois monétaire et financière.

Concernant des paiements pour un achat en ligne, leur protection usuelle par les procédés actuels relève de diverses voies, selon que l'on utilise les supports techniques et les acteurs bancaires déjà existants, ou que soient ajoutés de nouveaux acteurs et de nouveaux supports tel qu'un système de paiement électronique gérant des versements entre plusieurs comptes ouverts chez son prestataire de services. Il s'est agi d'une part souvent de blinder les flux et les entités, via des protocoles de chiffrement, d'encapsulation ou encore d'authentification tels que SSL/TLS au sein des couches de session, 3-D Secure et SET pour l'ajout d'une non répudiation. Ou de juxtaposer les flux et les interfaces relatifs, d'un côté, au site marchand, et de l'autre au site du compte électronique. Cette dernière solution, qui active fréquemment l'affichage d'une fenêtre supplémentaire sur l'écran de l'internaute, n'est pas sans danger, notamment de hameçonnage. D'autre part, à un autre niveau et concernant les modes d'authentification, il est usuel de demander à l'internaute des mots de passe, un numéro de carte bancaire avec sa date de validité ou une date de naissance auxquels s'ajoutent par exemple le report d'un cryptogramme visuel. Certains prestataires se servent de l'adresse électronique de l'auteur comme identifiant, ce qui cependant réduit son intimité numérique. Intimité que cherche à défendre la présente invention par l'adoption de griffage fonctionnellement masquant de l'identité de télécommunications d'un auteur.

Le dispositif selon l'invention n'oblige pas en soi à l'ouverture d'un nouveau compte bancaire ou assimilé, ni à une carte bancaire particulière. Il présente l'avantage de s'adapter aux acteurs économiques existants, en modifiant un processus originel par cloisonnement et canalisation de ses entités, de ses actions et des identités. L'ajout d'un blindage sur les flux ou les entités, voire l'ajout d'un nouvel acteur bancaire ou d'un nouveau support de paiement, demeurent possibles, mais ne feront qu'ajouter des degrés supplémentaires sur une sécurité et une confidentialité déjà logées dans les moyens précités. En cela, le présent dispositif n'est pas nécessairement concurrent des actuelles offres de sécurisation de paiement ou de versement, puisqu'il peut aussi bien être décrit comme complémentaire dans de nombreux cas de figure. Il présente un niveau élevé de neutralité tant vis-à-vis des prestataires que des sécurisations existants. Il offre aux utilisateurs une latitude à mener

des arbitrages et à constituer leur bouquet de sécurités selon qu'elles leur paraissent complémentaires ou redondantes.

Une application complémentaire serait la transposition ou le report d'un cryptonyme ou d'un pseudonyme, sur un support physique tenant lieu de monnaie, en prolongement matériel des monnaies ou timbres créables par le dispositif selon l'invention. Un casino ou un club de vacances seraient capables à l'arrivée d'un visiteur de faire le change de monnaie officielle en variantes informatisées de jetons ou colliers à boules détachables, et agir réciproquement à la sortie, soit selon des valeurs définies par ce tiers, soit selon des formes de cotation convenues. Toutefois, ceci ne ferait qu'apporter une interface conviviale courante, sur un dispositif dont la spécificité tient en ce couplage d'une autorité d'anonymisation avec un griffage à la fois distinctif, fonctionnel et de reconnaissance, inséré dans un protocole informatique ou de communication.

En corollaire de ces multiples évolutions, l'autorité d'anonymisation enregistre une sophistication de sa fonction d'homologation, de notation ou encore de radiation, soit d'un auteur, soit dorénavant aussi de multiples réceptionnaires et porteurs de contre-clés. Cet élargissement se retrouve dans le fait que l'autorité d'anonymisation, associée à la serrure numérique, qui font désormais office de dépositaire généraliste où chaque déposant choisit ce qu'il y entrepose ainsi que les règles d'ouverture et de délivrance de ce contenu, s'adressent à un déposant qui peut être non seulement un auteur mais aussi un réceptionnaire ou autre tiers.
Plus généralement, l'autorité d'anonymisation fonde et organise des contacts et des coopérations, du dialogue, de la confiance, de l'intimité, de la visibilité circonscrite à ce qui est nécessaire et accepté. Elle endosse ce faisant un rôle social et économique, qui aide à la gestion de l'espace numérique de chacun ainsi que des interfaces où ces espaces respectifs doivent coopérer ou risquent de s'interpénétrer et de se nuire.

L'autorité est nommée d'anonymisation eu égard au fait que le griffage qu'elle accorde fait fonction de cryptonyme. Ce cryptonyme généralement

variant, rattaché à un pseudonyme généralement invariant, sont tous deux définis dans la demande de brevet FR 2 932 043.

Toutefois, il trouvera ici un premier élargissement de ses applications à travers l'évolution des fonctions et des cloisonnements, en ce que, tout en délestant le réceptionnaire central de certaines connaissances, il préserve néanmoins en sa faveur une possibilité de capitaliser progressivement une connaissance détaillée sur l'auteur, visiteur de son site internet par exemple, via son comportement actuel ou passé, indépendamment du fait que ses visites préalables aient ou non été accompagnées d'achat. Capitalisation rapportée au pseudonyme, rattaché au cryptonyme inséré dans le protocole du flux. Sans connaître pour autant son identité réelle, le réceptionnaire se voit garantir qu'il s'agit bien du même auteur que lors de son précédent courrier ou de sa précédente visite. Cette disposition permettra à titre d'exemples :

- de profiler ses goûts, préférences ou choix, afin de faciliter de futurs contacts, de personnaliser l'accueil ou d'orienter plus rapidement vers des réponses pertinentes ;
- de savoir s'il bénéficie d'avantages dus à une fidélité, un abonnement ou toute particularité favorable ;
- de se reporter à des antécédents médicaux afin de faciliter de futurs soins ou diagnostics ;

La demande de brevet FR 2 932 043 initie une piste consistant à connaître ses comportements lors de visites antérieures, afin de déterminer s'il a respecté une éthique, une règle du jeu, un accord, en engagement compensatoire, préalable à une autorisation de revenir ou de procéder à de nouvelles visites. Toutefois, ce précédent procédé retenait des cas non marchands et simplement destinés à savoir pour un site internet si un accès sera laissé à tel visiteur. L'évolution des cloisonnements et des fonctionnalités accordées au griffage permettent d'ouvrir la présente invention aux sites de vente sur internet, d'enchères, et plus généralement à toutes les configurations dépassant le simple stade de l'accès pour aboutir notamment à des paiements, des livraisons, des prestations de services tels que diagnostics ou expertises.

En soutien à cette sophistication de la relation bipartite, la garantie de confidentialité et d'intimité en faveur de l'auteur, trouve un pendant dans la garantie de pouvoir durablement le reconnaître par son pseudonyme, à l'exclusion de sa véritable identité.

Il en résulte pour un prestataire commercial un modèle économique avantageux reposant toujours sur une relation au consommateur basée sur une connaissance individualisée. Elle n'est plus nominative au sens de sa vraie identité mais elle reste « nominative » par rapport au pseudonyme de cette personne. Le même principe pourra s'appliquer sur les polynymes, tels qu'ils seront présentés ultérieurement.

En termes de différentiation commerciale, ceci lui permet d'afficher un respect de l'intimité et de la vie privée supérieur aux modèles de profilage nominatif, tels qu'ils se pratiquent très majoritairement. Quelques-uns de ces derniers cherchent toutefois à corriger leur caractère intrusif en proposant soit un effacement ou une anonymisation ultérieurs, soit un stockage ultérieur sur des relais informatiques externes. Ces pratiques, tout en soulignant l'état d'attente du consommateur en la matière, n'apportent pas la même garantie de sécurité, puisque le dit droit à l'oubli ou le transfert a posteriori sur des supports externes aura impliqué une présence même infiniment brève sur les systèmes informatiques de l'entreprise ou de l'administration concernée. Le procédé selon l'invention permet quant à lui de viser de tels résultats d'ignorance ou de neutralité sans laisser naître cet intervalle néfaste de présence, tant il est exact qu'en matière numérique un intervalle perd sa définition temporelle concrète puisqu'il peut donner lieu à une trace, une copie pirate ou des données mal effacées.

De tous ces dispositifs, il résulte que l'invention constitue un mécanisme de meilleure garantie de confidentialité ou d'intimité, destiné à l'auteur, tant pour son identité que pour d'autres attributs personnels ou à caractère sensible, et dans l'usage qui pourrait en être fait. Ce mécanisme s'exerce sur le réceptionnaire central autant que tout autre acteur ayant accès à son fonds documentaire. Cette confidentialité, couplée souvent au meilleur professionnalisme des instances préposées à la conservation des données concernées que sont l'autorité d'anonymisation et les réceptionnaires périphériques, pourra être promue en tant qu'avantage qualitatif, en tant

également que garantie montrable de respect de confidentialité ou d'intimité envers un interlocuteur. Une pareille démarche de faire-savoir pourra prendre la forme d'un label de sécurisation des données bancaires. Ce peut être encore un label anti-pourriel sous certaines conditions de déploiement.

L'absence de prise de connaissance de ces données puis de leur détention sera garante de leur restriction d'usage :

- pour le cas d'interdiction de connaissance de l'adresse de télécommunications de l'expéditeur : limitation de pourriels ultérieurs à son attention, ou de toute forme de relance telles que commerciale, informative, de démarchage, émanant du réceptionnaire central. Ces actes seront rendus moins aisés puisqu'ils devront passer par un tiers avec lequel une charte déontologique peut s'envisager, pour réduire les futurs courriers à ceux motivés par une réelle utilité de contenu. À ce titre, la garantie est non seulement montrable mais configurable et vérifiable.

  Ce label anti-pourriel est surtout opérant par le fait que ces informations, restant confidentielles et non enregistrées, ne pourraient échoir par truchement du réceptionnaire, volontairement ou non, à un tiers mal intentionné ;
- pour le cas d'un empêchement de connaissance de l'adresse postale, limitation de ce fait de possibilité de courrier physique tel que publicitaire, commercial, informatif, de démarchage ou de relance, ainsi que de toute visite physique.

Un deuxième prolongement serait l'étiquetage matériel ou toute forme de nommage d'un support, avec ce pseudonyme ou l'un de ses cryptonymes. Le support pouvant être humain, animal ou matériel.

Un pseudonyme pourrait de la sorte s'exprimer, en substitut de la traditionnelle identité réelle, sur un support physique, telles qu'une sorte de carte d'identité, une carte à puce, un ticket, un jeton ou encore une forme de tatouage personnalisés. Ceci pourrait trouver emploi par exemple pour venir retirer à un guichet une commande préalablement passée et payée par télécommunications ou pour mieux justifier d'un droit auprès d'un contrôleur. Ce pourrait être ainsi une contre-marque, un en-tête de document ou la composante visible d'un billet de train acheté en ligne et imprimé à domicile.

Une autre application concernerait des tatouages ou marquages par peinture tels qu'ils sont utilisés pour signaler avoir déjà acquitté un droit d'entrée dans un établissement de fête, ou avoir déjà voté lors d'un scrutin.

Un usage similaire du cryptonyme serait possible, mais limité par ses cycles de vie et généralement contraint par de préalables sécurisations limitatives de sa connaissance par autrui. Il pourrait surtout venir conforter la présentation du support de pseudonyme. Il serait envisageable qu'un cryptonyme n'endosse que cette seule fonction de report sur un support extérieur.

Ces reports et étiquetages de pseudonyme, de polynyme ou de cryptonyme peuvent se contenter de ne conserver qu'une de leurs sous-parties, ou d'autres dérivés recourrant par exemple à un codage.

Ce procédé général pourrait avantageusement être affecté aussi aux actuels marquages d'objets ou d'animaux, qui sont pour leur part généralement inutilisables simultanément pour de pareils usages informatiques ou de télécommunications. De la sorte, l'autorité d'anonymisation pourrait intégrer et démultiplier des fonctions actuellement dévolues à diverses autorités aptes par exemple à recevoir à leurs guichets ou par voie postale, des objets perdus revêtus d'un de leurs cryptonymes, tel que ceci est mis en œuvre via des porte-clés tatoués. Par cette employabilité duale, le procédé selon l'invention permet d'élaborer une offre de services relevant des deux sphères virtuelle et matérielle.

De même, l'invention pourra être le soubassement d'une anonymisation ou d'une pseudonymisation de la sphère naissante des objets communicants. À ce titre, et par l'ajout d'une couche supplémentaire d'anonymisation, elle concocte un modèle économique original en apportant à l'usager une garantie de confidentialité supplémentaire, dont l'absence apparaît être un obstacle à l'essor commercial de ces objets communicants. Elle peut en effet mettre en place un écran entre par exemple une autorité dite de nommage, perçue comme omnipotente et omnisciente, et un détenteur de tels objets soucieux de son intimité numérique. Le fait d'ajouter une couche supplémentaire où chaque acteur disposera d'une ou plusieurs marques, permet aussi de lui ouvrir un ou plusieurs registres dédiés d'adresses

d'objets, ce qui démultipliera d'autant le nombre d'adresses distribuables. La rareté de telles adresses constitue en effet un autre obstacle à l'essor des objets communicants.

Pour ce faire, la dite couche supplémentaire d'anonymisation reposera sur ce qui sera nommé système de polynymes, dans une acception plus étendue que celle usuellement prêtée. Présentement, elle se déploiera comme telle :

- un polynyme pourra être un cryptonyme accordé simultanément à plusieurs auteurs, ou à des objets communicants de ces auteurs.
- En sens inverse, un auteur pourra disposer d'une pluralité de cryptonymes rattachables à des polynymes différents.

Le premier intérêt d'un tel dispositif selon l'invention est de créer une zone de flou qui protège l'espace numérique des auteurs, réparti sur une multitude de supports matériels. Tout en s'appuyant sur le griffage faisant cryptonyme, inséré dans les protocoles informatiques ou de communication, la présente invention déploie un mécanisme où un réceptionnaire ne pourra plus savoir si tel griffage recouvre un seul auteur ni si ce dernier n'est recouvert que par un seul griffage. Il s'ensuit une possibilité très réduite de traçabilité, d'historicisation ou de profilage. Aspect qui revêt une grande importance lorsque trop de nos objets communicants transmettent des informations complémentaires à notre propos, sur nos achats, nos déplacements ou nos habitudes domestiques.

Le deuxième intérêt tient à ce que le cryptonyme, qui dans la demande de brevet FR 2 932 043 a pour fonction centrale de se substituer fonctionnellement à l'identité de télécommunications de l'auteur, endosse de surcroît le rôle d'une sorte de préfixe précédant soit la suite du contenant qu'est le protocole, soit tout ou partie du contenu. Ce faisant, il allonge la longueur autorisée du message total. Laquelle longueur est parfois contrainte à une grande brièveté par les standards techniques en usage, et réduit d'autant le nombre total d'expressions variantes. Une telle situation est présente dans le débat sur la transition éventuelle des identifications et des adresses des paquets du protocole IP passant de IPv4 (adresses de 32 bits) à IPv6 (adresses de 128 bits), où l'argument de la rareté des identités IPv4

est récurrent. Venant surmonter ce dilemme, le cryptonyme est ici à la fois un multiplicateur d'identités autant qu'un brouilleur d'identité.

La partie restante du protocole qui indique l'identité réelle de l'auteur, sera soit interdite fonctionnellement d'accès, comme cela est le cas dans la demande de brevet FR 2 932 043, soit édulcorée ou amputée par une entité intermédiaire, par exemple l'autorité d'anonymisation. Cette dernière fera ensuite poursuivre son cheminement au courrier jusqu'à l'autorité de nommage. L'utilité de cette intermédiation tenant à ce que l'autorité d'anonymisation pourra bénéficier d'une plus grande confiance de la part des usagers, voire être créée par eux, par des groupements d'entreprises ou de particuliers, ou être placée sous le contrôle d'élus qui ne relèvent pas d'autres juridictions géographiques.
Ce qui est dit d'une autorité de nommage pourrait concerner tout autre destinataire final, de même que l'illustration du procédé par les objets communicants ne fait que désigner le principal marché potentiel de cet aspect de l'invention. D'autres applications ou entités pourraient ainsi être concernées, à l'exemple des systèmes de vote électronique, de sondages en ligne, de test consommateur, de mesure d'audience télévisée, de recensement, d'inventaire. Des usages pourront naître en matière d'archivage, d'indexation et de classification de données, de stock ou de programme informatique puisque le principe du polynyme renvoie à une arborescence qui peut être choisie non pas seulement selon des critères d'intimité et d'invisibilité mais au contraire de formalisation de typologies visibles. L'addition de l'anonymisation avec une classification logique restant possible. Le polynyme peut être aussi bien aléatoire et masquant que rationnel et indicatif, ou un panachage de ces items.

L'utilisation ci-avant du terme « préfixe », à propos d'un cryptonyme inséré dans un protocole, n'est pas une description universelle : cette position première se réfère au contenu du courrier ou du fichier, mais elle peut varier en termes d'unicité, ou spatialement par rapport au reste du contenant, notamment si l'objectif n'est pas d'anonymiser un auteur. Dans ce dernier cas, une notion de suffixe ou toute forme de marquage caractéristique peut convenir. De manière imagée, il peut s'agir d'allonger aussi bien des racines,

le tronc ou les branchages d'un arbre que serait le protocole. Plusieurs allongements simultanés étant une option envisageable.

Toutefois, ce principe général d'allongement peut trouver une variante ne reposant pas sur l'ajout de caractères, mais sur des modifications dans le protocole initial qui aboutissent au même résultat d'accroissement des variantes possibles, à l'image d'un cryptonyme qui permuterait des caractères antérieurement présents dans le protocole au profit de caractères inédits jusqu'alors.

Dans un dispositif le plus simple, l'autorité d'anonymisation pourra accorder à tel auteur un ou plusieurs cryptonymes-préfixes, venant s'insérer dans les protocoles lors des envois de certains de ses objets communicants. Simultanément ou par la suite, elle accordera ce ou ces mêmes cryptonymes-préfixes à d'autres auteurs pour divers de leurs propres objets. La seule contrainte étant alors que ces préfixes ne soient pas suivis ou environnés par des suites identiques de caractères d'identification, qui aboutiraient au total à des doublons.

Il en résulte la création d'un propriétaire qualifié ici de virtuel, qui apparaîtra comme détenteur attitré et unique de ces divers objets.

Le nombre de polynymes n'étant plus lié au nombre avéré d'auteurs, et étant démultipliable selon la nature, la position et la longueur permise au cryptonyme, définit le nombre de propriétaires virtuels fabricables.

En matière d'intimité, l'autorité d'anonymisation pourra avantageusement servir d'intermédiaire entre une autorité de nommage et des auteurs tels que le sont des internautes ou des objets communicants. Cette autorité d'anonymisation multiplierait les propriétaires virtuels, à la convenance des auteurs et usagers, intervertirait les objets de plusieurs propriétaires réels, redistribuerait leurs objets sur plusieurs propriétaires virtuels, agrégerait les objets de plusieurs propriétaires réels sur un seul propriétaire virtuel, tout en gérant l'obligation que ce préfixe ne soit pas environné deux fois de la même suite de caractères. Elle pourrait procéder à des permutations dans le temps, où tel objet d'abord rattaché à tel propriétaire virtuel le soit ensuite à un autre. Elle pourrait, poussant à son extrême sa mission de brouillage et selon une démarche de leurre ou de placebo, créer des propriétaires virtuels ne

correspondant qu'à des objets inventés pour la circonstance. Un polynyme pourra recouvrir zéro, une ou plusieurs vraies personnes ; une personne pourra avoir zéro, un ou plusieurs polynymes. Il pourra y avoir de fausses personnes et de faux objets.

Faisant office d'intermédiaire utilement opaque entre des utilisateurs et une autorité de nommage, l'autorité d'anonymisation apporterait une réponse aux inquiétudes récurrentes nées des pratiques, du poids, de la nationalité voire de l'opacité de fonctionnement de certaines autorités de nommage. À cette opacité de fonctionnement serait opposée une opacité d'emploi et d'appartenance. Tel objet qui un jour apparaîtrait lié à tel propriétaire virtuel, se retrouverait le lendemain lié à un autre, sans facilité de le tracer, et sans pouvoir connaître le contour exact du patrimoine d'un propriétaire réel donné.

En résumé, le signe distinctif inséré dans un protocole voit dans la présente invention la variété de ces usages considérablement élargie. Le cryptonyme variant pourra rester associé à un pseudonyme invariant vis-à-vis de certains interlocuteurs tel qu'un site internet marchand, tandis qu'il endossera une fonction de polynyme masquant et multiplicateur vis-à-vis d'autres interlocuteurs telle qu'une autorité de nommage. Cette dernière précaution présentant de pareils intérêts envers tout observateur malintentionné des réseaux de télécommunication ou tout pirate tentant de pénétrer un système informatique.

L'invention crée une gestion d'identité à tiroirs : une séquence ou une arborescence de noms qui ont une fonction d'identité, de pseudo-identité (pseudonymat, alias), de traçabilité (un anonymat traçable), de permutabilité (identités éphémères au sens temporel), d'identité saupoudrée, avec un dispersement du nom sur l'espace du réseau. Elle aboutit à une gestion d'identité numérisée qui surmonte la contradiction du contrôle face à l'intimité. L'autorité d'anonymisation s'apparente ainsi à un fournisseur de bouquets d'identités numériques à tiroirs. Par-delà cette fourniture initiale, il peut s'agir d'une gestion d'identité dans la durée.

Le procédé selon l'invention contrôle, sécurise et rend confidentiels des processus complexes de type déclaratif, informatif, administratif ou productif. Il se caractérise d'abord en ce qu'à partir d'un quelconque signe distinctif et

caractéristique inséré dans un protocole utilisable par les technologies de l'information et des communications, un interlocuteur entrant ou réceptionnaire puisse à la fois l'interpréter en tant que prescription initiale et l'utiliser en tant que moyen d'accès à des données externes. Le champ de ces informations ou prescriptions n'est pas limitatif. De plus, par un agencement nouveau de cloisonnement et de canalisation séquentielle ou parallèle, le procédé segmente, distribue ou raccorde les entités et les actions concourant à un même processus complexe. Il rend possible une pluralité de réceptionnaires complémentaires ainsi que d'autorités garantes de la confidentialité de données sensibles. Lesquelles s'appuient sur le caractère fonctionnel de masquage de protocole endossé par ce signe distinctif. Ce dernier prend par ailleurs la forme d'un cryptonyme variant raccordable à un pseudonyme invariant ou à un polynyme.

Ce dispositif pourrait s'illustrer en partie par l'image d'un univers à trois dimensions : un message anonymisé, capable d'activer ou de nourrir des fonctions, évolue dans un labyrinthe à deux dimensions fait de cloisons qui l'orientent, le scindent ou le réunissent, et l'activent. Ces cloisons opaques ajoutent de l'ignorance sur le contenu du message ou sur ses interlocuteurs, aussi ce message se promène-t-il muni d'un fanion qui dépasse les cloisons en altitude, et permet de le voir et le reconnaître de loin. Toutefois ce fanion revêt des pseudonymes ou des polynymes et non pas l'identité réelle ou toute autre information réelle.

Plus particulièrement, l'invention a pour objet un procédé de sécurisation et de contrôle de données et d'identités au sein de processus de communication entre un auteur et au moins un réceptionnaire, un griffage, inséré dans un protocole informatique ou de communication, étant couplé à une autorité d'anonymisation, complétée par un dispositif à serrure, recélant et distribuant des données et des consignes, le couplage entre le griffage et l'autorité d'anonymisation cloisonnant et canalisant des entités, des actions et des identités.

Le griffage faisant marquage cryptonymique est par exemple signe de reconnaissance, ou clé vers des consignes ou des données recelées par l'autorité d'anonymisation ou le dispositif à serrure, mode d'activation de

mécanismes ou de signaux, équivalence à pseudonyme ou racine de polynyme gérés par l'autorité d'anonymisation.

Dans un mode de mise en œuvre particulier, un griffage correspond à des fonctionnalités ou des modalités différentes, des réponses différentes ou des manières différentes de répondre de la part de l'autorité d'anonymisation ainsi que du dispositif à serrure, ou des modes de délivrance différents, selon son destinataire, le contexte et l'environnement dans lequel évolue ce destinataire, la chronologie ou la localisation des faits, la manière d'agir ou d'être de ce destinataire, la nature des données ou du signal correspondant à ce griffage ou à ce qu'il va mettre en œuvre, ces modes opératoires pouvant être préétablis et discriminées selon des items convenus avec l'auteur, autant que visés au cas par cas en une ou plusieurs étapes.

Il est possible que plusieurs griffages soient optionnellement disponibles pour un même auteur, de manière séparée ou additionnelle au sein d'un même protocole informatique ou de communication, affectables à des usages différents ou similaires, indépendants ou complémentaires.

Dans un mode de mise en œuvre particulier, d'une part le griffage faisant clé et d'autre part la dite serrure, sont chacune en totalité ou en partie le répondant de l'autre, soit comme profil et contre-profil, soit comme une image et son négatif, soit comme une matrice et son œuvre, soit comme une griffe et sa cicatrice, cette complémentarité vers un tout ou vers une succession générant des capacités de dialogue, de correspondance, de reconstitution du tout ou de la filiation, à des fins de validation, d'identification ou d'authentification, d'actionnement d'un signal ou d'un mécanisme, d'expression d'une signification ou d'une consigne, ou de solidarisation entre eux.

Par exemple, le mécanisme de cloisonnement discrimine, parcellise et rend autonome, masque, démarque ou brouille certains sujets, certaines fonctions et tâches, certaines données et certains objets, certaines identités ou coupons d'identité relatifs à un même processus.

Par exemple, le mécanisme de canalisation distribue de manière parallèle ou séquentielle, compose, crée des liens ou des coopérations, agrège, démasque ou re-marque, certains sujets, certaines fonctions et tâches, certaines données et certains objets, certaines identités ou coupons d'identité relatifs à un même processus.

Par exemple, le cloisonnement et la canalisation engendrent une modification de la quantité ou de la qualité des entités impliquées, avec une modification de leur périmètre ou de leur nature, des substitutions, des permutations, une démultiplication des sujets, des rôles et des identités, ou une division de l'information et des secrets à partager.

L'autorité d'anonymisation ou le dispositif à serrure détient par exemple tout type de consigne, donnée ou signal relatif à la gestion d'un flux ou d'un fichier muni du protocole avec griffage, aussi bien que tout type de consigne, donnée ou signal raccordés à ce griffage ou à une identité donnée, mais indépendants de cette gestion directe et pour leur simple mise à disposition depuis l'auteur envers un réceptionnaire.

Le griffage faisant clé de ladite serrure enclenche par exemple un accès, un actionnement de toute forme de sas et porte donnant sur un espace réservé ou coffre numérique, un mécanisme ou un enregistrement, une action ou une réaction technique, ou encore un signal informatif ou déclaratif.

Dans un mode de mise en œuvre particulier, la serrure existe indépendamment de tout coffre ou autre dispositif subordonné, à des fins de validation de la réalité, l'authenticité et l'actualité d'un griffage faisant clé.

La serrure est par exemple dotée de parties non visibles par un réceptionnaire, permettant la validation d'un griffage cryptonymique, ou d'une donnée restée inconnue et correspondant à ces parties non visibles, ou du lien entre ce cryptonyme connu et cette partie inconnue, ou du lien entre plusieurs parties inconnues, la partie inconnue étant un pseudonyme, une identité réelle, la suite du protocole informatique ou de communication, le contenu du fichier ou du courrier, ou toute autre information ou consigne.

Une serrure peut aligner une juxtaposition, une succession ou une composition des dits contre-profils, des dits négatifs, des dites matrices ou oeuvres ou des dites cicatrices, correspondant à au moins un griffage ainsi qu'à d'autres données tel qu'un pseudonyme.

Avantageusement, la serrure permet lors de son essai par le griffage, l'apposition ou l'insertion de données supplémentaires dans, avec, autour ou sur ce griffage.

Dans un mode de mise en œuvre particulier, le dispositif à serrure nécessite pour son actionnement au moins un griffage faisant clé, trouvé dans un protocole, et au moins une contre-clé permettant d'authentifier au moins un

tiers, réceptionnaire ou autre, doté de sa propre contre-clé, ce tiers pouvant être l'autorité d'anonymisation ou l'auteur, et lesdites clés et contre-clés étant accordées, ou non, par l'autorité d'anonymisation.

L'auteur dispose par exemple d'une pluralité de coffres numériques ou autres mécanismes, destinables chacun à un ou plusieurs réceptionnaires.

Au moins une consigne de fonctionnement dédiée à au moins un réceptionnaire est par exemple transmise ou accessible au moyen du griffage inséré dans le protocole.

Ladite consigne de fonctionnement est par exemple une autorisation, une interdiction, totales ou partielles et discriminées, l'édiction de requêtes ou de clauses conditionnelles, l'activation, la modification ou l'arrêt d'une fonction d'un réceptionnaire.

Par exemple, le flux de communication ou le fichier n'est constitué que du seul protocole marqué du griffage, à l'exclusion de tout contenu.

Une consigne fonctionnelle, relative à la communication, au traitement, à la lecture ou à la mémorisation de données, résulte par exemple de la présence du griffage dans le protocole, la consigne concernant le contenu du flux, du fichier ou le reste du protocole.

L'interdiction ou l'autorisation fonctionnelle partielle, concerne par exemple une partie prédéterminable du courrier ou du fichier, tant dans son contenu que dans son protocole.

L'interdiction de traitement, de lecture, de communication ou de mise en mémoire de certaines données chez un réceptionnaire s'accompagne par exemple de leur orientation vers un autre réceptionnaire périphérique prévu à cet effet.

L'interdiction de mise en mémoire de certaines données chez un réceptionnaire s'accompagne par exemple de l'élimination de ces données.

Le griffage est par exemple utilisé par ses réceptionnaires successifs comme signe de reconnaissance entre eux ou avec l'auteur, ainsi que pour obtenir auprès d'une autorité d'anonymisation ou via une serrure, la correspondance entre ce griffage et des attributs de l'identité à laquelle ledit griffage se rattache, ou toute autre donnée ou signal, conservés par elles en vue de cette transmission.

L'autorité d'anomysation ou le dispositif à serrure est par exemple habilité à transférer à un réceptionnaire ou un tiers homologué, ladite correspondance

ou lesdites données, ledit réceptionnaire ou tiers utilisant ladite correspondance ou lesdites données, pour accomplir une tâche dévolue à lui par un précédent réceptionnaire ou par l'auteur du flux ou du fichier.

Ladite tâche ajoute par exemple une information, reçue de l'autorité d'anomysation ou du dispositif à serrure, sur un travail resté en partie ou totalement anonyme ou incomplet, en attente des attributs d'identité requis pour l'utiliser, l'acheminer ou le finaliser.

Ledit travail est par exemple relatif à une transaction électronique entre l'auteur du courrier ou du fichier et un réceptionnaire principal.

Ledit travail est par exemple relatif à un acheminement physique ou par voie de télécommunication entre un réceptionnaire principal ou périphérique et l'auteur.

Ledit travail est par exemple relatif à un jeu d'écriture, s'effectuant entre l'auteur et un réceptionnaire principal ou périphérique.

Ledit travail est par exemple relatif à une vérification du fonctionnement, du comportement, de l'état, de l'intégrité ou de l'authenticité touchant un terminal ou un support de communication, et les mécanismes qui leur sont raccordés.

Un réceptionnaire périphérique fait par exemple office d'autorité d'anonymisation pour la correspondance entre le griffage et diverses données ou réponses s'y rattachant.

L'autorité d'anonymisation est par exemple avisée d'un réceptionnaire délégué à une tâche ou un rôle, par l'auteur ou par un réceptionnaire précédent.

Le griffage inséré dans un protocole sert par exemple d'allonge ou de modificateur, ou de démultiplicateur, à une identité arbitraire attribuée à une entité physique tel qu'un objet, une entité informatique tel qu'un fichier, un flux de communication, ou une entité virtuelle tel qu'un avatar, ainsi éventuellement qu'à leur auteur, détenteur ou expéditeur.

Le griffage faisant cryptonyme, inséré dans un protocole informatique ou de communication, sert par exemple soit de passerelle vers un pseudonyme, soit de racine commune à diverses identités unifiées en un registre de type polynyme.

Un même griffage inséré dans une pluralité de protocoles sert par exemple de référent commun pour créer un registre unificateur d'identités arbitraires

attribuées à des objets, flux, fichiers ou avatars relevant d'une ou plusieurs identités véritables.

Un même auteur dispose par exemple d'une pluralité de griffage différents correspondant à autant de polynymes, de manière exclusive ou partagée avec d'autres auteurs.

Le griffage inséré dans un protocole informatique ou de communication engendre par exemple le démarquage, sur ce protocole, de l'identité véritable de son auteur, soit de par son rôle fonctionnel d'interdiction de prise de connaissance, soit via une autorité d'anonymisation placée en intermédiaire par rapport au réceptionnaire.

L'autorité d'anonymisation, assistée ou supplée par le dispositif à serrure, transmet par exemple la correspondance entre tel cryptonyme, tel pseudonyme ou telle entité référencée sous un polynyme, et d'autre part des informations comportementales, situationnelles ou se rapportant au passé ou au profil de cet auteur, aux fins de le caractériser sans nécessairement transmettre ni son identité véritable ni un autre de ses pseudonymes.

Un griffage inséré dans un protocole, ou les pseudonymes ou les polynymes qui lui sont rattachés, ou des sous-parties autonomes ou composées de ces trois options, peuvent servir à marquer ou tatouer des objets, des matières ou des êtres réels, à des fins de reconnaissance, de validation de droit ou de statut, de valorisation, d'appartenance ou de dépendance, de liaison, d'identification ou d'authentification sans révéler une identité véritable.

Un contenu de fichier ou de courrier, doté de capacités techniques d'intéraction avec leur environnement, qui en rendent certaines composantes actives et autonomes, peut se mettre en dialogue avec leur propre protocole, et faire du griffage un usage identique à celui d'un réceptionnaire extérieur.

Par exemple, l'autorité d'anonymisation ou l'auteur, attribuent, retirent et changent les griffages faisant racine de polynyme, pour opérer des permutations et redistributions au sein des registres unificateurs d'identités arbitraires.

D'autres caractéristiques et avantages de l'invention apparaîtront à l'aide de la description qui suit, faite en regard de dessins annexés qui représentent :

- la figure 1, une synthèse non exhaustive du dispositif selon l'invention, dans son mécanisme et ses effets sur une quelconque procédure complexe, et sur les entités impliquées dans cette procédure.
- la figure 2a, le procédé de gestion d'un fichier ou d'un courrier porteurs de griffage émis par un auteur ;
- la figure 2b, à titre d'exemple les diverses parties d'un document, sous forme de courrier ou de fichier ;
- la figure 3, le rôle de passeport endossé par le griffage, pour obtenir d'autres informations ou consignes que celles directement rattachables par un réceptionnaire à sa présence dans un protocole ;
- la figure 4, le cas d'un document statique présent par exemple dans un ordinateur, où un griffage est inséré dans un protocole informatique ;
- la figure 5a, un exemple de vérification d'un griffage cryptonymique auprès d'une serrure numérique ;
- la figure 5b, un mode de confirmation auprès de la serrure numérique que le griffage cryptonymique appartient bien à son expéditeur homologué ;
- la figure 5c, un mode d'ouverture de la serrure numérique par le griffage faisant clé et l'obtention de contenus mis au coffre ou l'activation de fonctions ;
- la figure 6, un exemple d'usage d'un griffage faisant clé numérique et requérant l'usage de contre-clés ;
- la figure 7, les étapes possibles d'un procédé selon l'invention appliqué à une commande passée sur un site de commerce en ligne ;
- la figure 8, le cas d'une réponse anonymisée à une candidature elle-même anonymisée, ou une notation d'un test mené en ligne ;
- la figure 9, le maintien d'une relation au consommateur et à l'usager, et la capitalisation de connaissance via un profilage comportemental;
- la figure 10, un autre mode de déploiement du profilage, dans une option où l'accumulation d'information comportementale détaillée laisse place à des classifications plus générales ;
- la figure 11, une configuration dans laquelle une même personne dispose simultanément de plusieurs griffages différents, utilisables selon son choix ou selon des procédures prédéfinissables ;

- la figure 12, des dispositions dans lesquelles des pseudonymes ou des cryptonymes selon l'invention trouvent prolongement et usage dans la vie sociale ou économique matérielle ;
- la figure 13, un mode de déploiement du procédé selon l'invention permettant d'anonymiser et d'encadrer restrictivement la mémorisation d'un flux pour lequel l'auteur ne disposerait pas d'une pleine liberté de choix du destinataire, d'une pleine liberté d'activation ou non de ce flux, ou encore d'un plein contrôle sur le système émetteur de ce flux ;
- la figure 14, un mode de déploiement particulier du procédé selon l'invention où un réceptionnaire aura accès à des attributs d'identité ou d'information présents dans le protocole informatique ou de communication, mais sans connaître la nature et le détail de sa relation à suivre avec l'auteur. Il ne sera de la sorte informé que de l'existence de ce lien ;
- la figure 15a, un emploi du dispositif dans une relation inter-entreprises ou inter-sites, à but administratif ou productif ;
- la figure 15b, une configuration d'emploi en tant que cachet, timbre ou bâton témoin, passant entre porteurs successifs, et transmetteur d'une signification, d'une grandeur ou d'une valeur convenue, ou d'une forme d'exclusivité ;
- la figure 16, un exemple de masquage et démultiplication d'identités par cryptonymes et polynymes ;
- la figure 17, un exemple de masquage et de démultiplication d'identités avec intermédiation par une autorité d'anonymisation ;

La figure 1 résume de manière simplifiée et non exhaustive le principe général du procédé selon l'invention, dans ses moyens, ses actions, ses points d'impact et ses conséquences. L'invention utilise un dispositif 10' essentiellement constitué de trois outils centraux, que sont une autorité d'anonymisation, un moyen de marquage des protocoles informatiques ou de communication par un signe distinctif et caractéristique nommé griffage, et une serrure dite numérique. Cette serrure constitue en soi un pendant au précédent signe distinctif puisqu'elle représente, entre autres fonctionnalités, une empreinte en creux de celui-ci, ou son moule originel puisque la

chronologie de leur naissance respective est renversable autant que plaçable en simultané, tout autant qu'il peut s'agir d'un négatif d'image, d'une contre-silhouette ou d'un contre-profil, de la cicatrice, sillage, d'un événement, éventuellement normé, tel ici que ce griffage. De cette parenté peuvent naître des fonctions multiples d'identification, d'authentification, de validation, mais aussi d'accroche sur le principe des tenons et mortaises. Ce peut être encore l'apparition d'une signification ou d'une action lors de leur réunion.

Ces trois outils complémentaires, qui disposent d'autres qualités décrites par la suite, concourent à élaborer un dispositif 11' qualifiable de spatio-temporel, au sens où il organise un espace où vont intervenir plusieurs acteurs impliqués dans une même procédure complexe tel qu'un achat sur internet ou la géolocalisation d'un objet communicant. Cette organisation de l'espace est une architecture qui s'impose à ces acteurs, à ces objets ainsi qu'à des données donc des connaissances ou des secrets, ou encore à des actions. L'architecture revêt une dimension temporelle puisqu'elle participe à la création d'enchaînements, de séquences, de priorités ou de simultanéités entre ces actions. Ainsi le dispositif spatio-temporel met en place à la fois :

- des cloisonnements : exprimables par le fait notamment de parcelliser des entités autant que des actions, de les séparer et les rendre autonomes ou assujeties à des finalités différentes, ainsi encore que masquer, brouiller, dé-marquer et rendre anonyme.
- un mode de canalisation : exprimable par le fait notamment de les distribuer de manière parallèle ou séquentielle, les composer, créer des liens ou des coopérations, agréger, démasquer ou re-marquer ces entités ou ces actions.

Ce dispositif 11', par son cloisonnement et sa canalisation, affecte de manière définitive ou provisoire ainsi donc que parfois réversible, les entités et les actions concernées 12' sous leurs deux propriétés quantitative et qualitative. Le quantitatif englobe en particulier le fait d'en multiplier ou réduire le nombre, d'en modifier le périmètre, tandis que le qualitatif porte surtout sur la modification de leur nature ou de leur identité. L'identité d'une personne ou d'un objet pouvant être même considérée comme la première de ses qualités constitutives.

L'ensemble de ce dispositif spatio-temporel agissant sur les facettes quantitatives ou qualitatives d'un quelconque processus complexe,

s'appliquera aux trois composantes de ce processus 13', résumables par « qui fait quoi ». « Qui » désignant par exemple les sujets ou les rôles tenus par eux, le verbe faire désignant telle tâche ou telle fonction, et le « quoi » désignant l'objet ou encore les données concernées. Un cloisonnement ou une canalisation peut de la sorte affecter le qui, mais aussi le quoi ou une fonction. Modifier le nombre, le périmètre, la nature voire l'identité est applicable autant à ce qui, à ce faire et à ce quoi.

Les figures 2a, 2b et 3 décrivent ce signe distinctif nommé griffage, son fonctionnement et son rôle. Elles permettent de préciser la différence entre d'une part la valeur fonctionnelle intrinsèque de ce griffage, et d'autre part son statut de passeport pour obtenir auprès de tiers des informations supplémentaires ou d'autres consignes. La dichotomie entre signification intrinsèque et passeport, souligne l'élargissement des rôles de ce signe à la fois distinctif et de reconnaissance par rapport à la demande de brevet FR 2 932 043.

La figure 2a illustre le procédé de gestion d'un document 1 ou d'un courrier porteur de griffage émis par un auteur 10, le mode d'interprétation de ce dernier et les fonctions correspondant à sa présence. Elle détaille l'usage de la signification fonctionnelle intrinsèque de ce griffage, c'est-à-dire le fait que sa présence corresponde en soi à une fonction déclenchable par un réceptionnaire central 2, fonction qui peut être d'interdiction ou d'autorisation, de modification ou d'arrêt d'une action donnée telle que de lecture, accès, traitement, enregistrement ou transmission.

Comme décrit dans la demande de brevet FR 2 932 043, un dispositif 11 géré par une autorité d'anonymisation 4 fournit à l'auteur 10 un système de griffage et une convention d'emploi qui convienne de la signification fonctionnelle de ce griffage selon les réceptionnaires ou selon d'autres critères différentiateurs.

La demande de brevet FR 2 932 043 privilégiait le fait que le griffage inséré dans le protocole soit quasi mono-fonction, centré sur le principe de pouvoir lire ou non certaines données. Il est dorénavant permis une variété de fonctions plus larges, de traitement, enregistrement ou transmission de chaque donnée. Cet élargissement est démultiplié par le fait que le griffage ne corresponde pas constamment à la même consigne selon ses types de

réceptionnaires ou selon d'autres critères tels que de calendrier. Il en résulte une quasi-infinité de variantes, d'autant que chaque type de consigne peut relever d'un niveau total ou partiel.

Dans la figure 2a, un même griffage exprime envers le réceptionnaire central 2 une interdiction d'accès et d'enregistrement à tel contenu, puis exprime une autorisation à un réceptionnaire périphérique 3 qui le recevra à suivre.

Ainsi, pour ce réceptionnaire périphérique 3, le griffage sera consigne pour lancer des actions à partir des informations présentes dans ce courrier ou ce fichier, notamment dans la partie restée éventuellement interdite d'accès pour le seul réceptionnaire central 2.

Soit le réceptionnaire 2 ou 3 a d'emblée connaissance de la signification fonctionnelle du marquage, soit il la demande à l'autorité d'anonymisation 4 ou à la serrure numérique en lui présentant copie de ce griffage ou du protocole dans son ensemble. L'autorité ou la serrure transmet la correspondance entre ce griffage et la consigne correspondant à tel réceptionnaire, ou tel type de réceptionnaire. Il peut donc y avoir plusieurs consignes différentes selon la nature et le nombre des réceptionnaires, voire une progressivité de délivrance de ces consignes.

Dès constat de présence et interprétation du griffage par un réceptionnaire 2 ou 3 ou tout lecteur autorisé, les fonctions correspondantes sont activables.

Dans un autre mode de mise en œuvre, une interdiction d'accès, de lecture, de traitement ou d'enregistrement peut prendre la forme d'un rejet immédiat des documents, tronçons ou espaces d'information incriminés, afin qu'ils ne pénètrent pas dans le système informatique par exemple du réceptionnaire central. Les données correspondantes seront soit refusées et sans destinataire, soit automatiquement orientées vers des réceptionnaires périphériques 3 prédéterminés. Dans une option intermédiaire, il peut s'agir d'une zone tampon ou d'une boîte noire, indépendante du système informatique du réceptionnaire central 2, et placée en amont, sous ou hors de son contrôle.

Dans une autre variante, la présence du griffage sera constatée plus en amont, par exemple au niveau de l'opérateur de télécommunications 5 dès le transit du flux concerné. Par convention préétablie, la coexistence de ce griffage avec l'indication de tel destinataire préenregistré, orientera automatiquement tout ou partie prédéfinie du flux vers une tierce entité

chargée d'une gestion déléguée, en substitut du réceptionnaire central. Cet aiguillage s'accompagnant de tâches éventuelles telles que de rétention partielle ou d'amputation, convenues selon le procédé général de réception initiale. Toutefois, hormis le fait d'intercaler cet opérateur, cette variante ne modifierait pas fondamentalement l'ordonnancement général puisque le destinataire central resterait central car usant d'un simple droit à la délégation, et car restant destinataire dans l'esprit de l'auteur ainsi que responsable de la bonne fin du processus.

La figure 2b illustre à titre d'exemple les diverses parties d'un courrier ou d'un fichier 1 pouvant être affectées en cas par exemple d'une interdiction ou d'un ordre de lecture, traitement, enregistrement ou transmission, destiné à un réceptionnaire 2 :

- une partie prédéterminable de ce protocole, telle que l'identité de télécommunication de l'auteur ;
- éventuellement une partie prédéterminable du contenu, cette partie pouvant prendre la forme par exemple d'encadrés ou d'encarts numériques dans le courrier ou dans le fichier, ou encore de segments de son contenu répondant à une logique de coupon détachable. Ces derniers cas peuvent donner lieu à scission du courrier ou du fichier.
- un autre fichier 21 attaché à un courrier ou un fichier.

La figure 3 détaille le rôle de passeport endossé par le griffage, pour obtenir d'autres informations ou consignes que celles, fonctionnelles, directement rattachables par un réceptionnaire à la gestion du courrier ou du fichier. Elle illustre le jeu respectif des divers réceptionnaires 2, 31, 32 et des autorités d'anonymisation ou de la serrure numérique, entre eux et vis-à-vis des données présentes dans ou hors du courrier ou du fichier 1 régi par le griffage.

La variété des réponses qu'une autorité d'anonymisation ou la serrure pourra délivrer au vu du griffage déborde du champ dans lequel se plaçait la demande de brevet FR 2 932 043. Cette dernière était, hors consignes, cantonée sur des informations 201, 311, 321 souvent minimales, elles-mêmes reliées pour l'essentiel aux seules identités. L'autorité d'anonymisation 4 ou la serrure peut présentement délivrer tout type de

consigne ou d'information, tel qu'une identité, un pseudonyme, une adresse, un élément de calcul comptable ou scientifique, c'est-à-dire plus généralement tout élément manquant pour la réalisation des tâches et pour la compréhension du traitement à leur administrer. À titre d'exemple, il peut s'agir d'une manière de déchiffrer tel contenu puis de s'en servir dans les règles, ainsi que son mode d'emploi général. L'autorité d'anonymisation 4 ou la serrure conserve les informations et consignes 201, 311, 321 pour le compte de l'auteur 10.

L'information ou la consigne pourra varier là aussi selon ses types de réceptionnaires ou selon d'autres critères tels que de calendrier.

À sa réception par des réceptionnaires 31, 32, le griffage inséré dans le protocole, ainsi éventuellement que tout ou partie de ces données restées inconnues dans le courrier ou fichier, servent :

- soit de moyen d'accès à une consigne pour lancer des actions à partir des informations à la fois présentes dans ce courrier ou ce fichier, ajoutées à d'autres déjà en possession du réceptionnaire et à sa seule discrétion. Ces dernières seront nommées informations internes ;
- soit à la fois de moyen d'accès à une consigne et de moyen d'obtention ou d'activation d'autres informations nommées informations externes. Celles-ci, telle qu'une adresse postale, seront obtenues soit :
    - par d'autres voies que le courrier ou fichier, et puisées à des sources externes telle que l'autorité d'anonymisation ou la serrure numérique. Elles pourront être obtenues notamment à partir du griffage présent dans le protocole ;
    - par un autre courrier parvenu directement au réceptionnaire périphérique, activé directement ou non par l'auteur.

Informations internes ou externes sont nécessaires pour accomplir la tâche prévue, ou compléter l'accomplissement de cette tâche, ou nécessaires à la bonne gestion d'une relation avec l'auteur.

Les réceptionnaires périphériques 31, 32, ou le réceptionnaire central 2 peuvent agir de même manière avec la partie éventuelle du courrier ou fichier sur laquelle ils ont eu le droit d'agir, mêlée elle aussi à des informations internes ou externes.

À un niveau plus conceptuel, et le terme inconnu pouvant s'entendre au sens d'inaccessible, illisible, indéchiffrable, incompréhensible ou inexpressif, il peut donc s'agir :

- de mise en relation d'information inconnue avec une autre information inconnue : à l'exemple d'un signe distinctif renvoyant à un autre secret ou code arbitraire, dans le cas d'un dialogue entre l'autorité d'anonymisation ou la serrure numérique et un groupement de carte bancaire connaissant un client à travers un numéro personnel ;
- de mise en relation d'information inconnue avec une information connue, à l'exemple du griffage avec un nom patronymique ;
- l'option de mise en relation d'information connue avec une autre information connue, sans être exclue en tous points, présente des fragilités au regard de l'objectif de sécurisation du processus, qui en restreindra l'usage. Il peut s'agir de renvoyer un nom patronymique avec une adresse postale.

La figure 4 illustre le cas d'un document statique 41 présent par exemple sur un ordinateur, où un griffage 53 est inséré dans son protocole informatique. L'auteur, le détenteur, le dépositaire ou le gestionnaire 43 de ce document 41 peut d'une part apposer le griffage 53 dans le protocole, et d'autre part déposer la signification de ce griffage auprès de l'autorité d'anonymisation 4 ou par exemple d'un coffre numérique 45, protégé par une serrure numérique.

Un visiteur 44 désireux d'accéder à ce document à des fins de connaissance, traitement, transmission ou enregistrement, doit, au vu de la présence du griffage 53, préalablement obtenir sa signification soit auprès de l'autorité d'anonymisation 4, soit auprès du coffre numérique 45.

La signification aura pu être diffusée a priori, ou correspondre à une signalétique connue et renvoyant à des consignes elles-mêmes diffusées.

La signification peut être éventuellement accessible directement auprès de l'auteur qui a émis le griffage. Ceci, par son risque de dérangement répété ou par la perte d'anonymat éventuel qui peut en résulter, ne prend d'intérêt réel que dans des cas limités telles surtout que des activités intra-entreprises voire inter-entreprises où des relations directes entre collègues et sans anonymat sont habituelles.

La figure 5a illustre la vérification du griffage auprès de la serrure numérique 50. L'autorité d'anonymisation 4 sert d'interface avec l'utilisateur des griffages, l'auteur 51 de flux ou le détenteur de fichier, en lui octroyant les systèmes de griffage, en convenant d'un pseudonyme stable lié aux cryptonymes successifs, et en le connaissant par son identité réelle.

La serrure numérique 50 reçoit, a minima, information des griffages de l'auteur. Elle permet de valider la réalité, l'authenticité et l'actualité d'un griffage 53 présenté à elle par un réceptionnaire 52 d'un envoi portant un tel signe 53. Le griffage 53 s'apparente alors à une clé physique que l'on chercherait à introduire dans une serrure physique, à seule fin de vérifier leur adéquation, et s'assurer de ce que le profil transversal de la clé, de manière imagée avec ses rainures spécifiques, corresponde bien au découpage de l'orifice d'entrée de la serrure, et donc vérifier si elle peut ou non pénétrer dans ce logement. Ce sans avoir nécessité de la faire tourner une fois à l'intérieur.

Le réceptionnaire et vérificateur peut toutefois recueillir d'autres informations via l'introduction de la clé dans cette serrure numérique. Ce recueil se fait de manière mécanique par un système de marquage où un griffage inséré dans une serrure numérique en ressortirait avec l'empreinte supplémentaire d'une seconde information. Cela, de la même manière qu'une clé physique non taillée dans son sens longitudinal peut être introduite dans une serrure et se voir marquée à l'intérieur, par craie ou peinture préalablement aspergée sur les garnitures internes, d'un contour dessinant ce profil recherché. Ou ici, par transposition, d'un contour dessinant le pseudonyme correspondant au cryptonyme. Ce mécanisme est utilisable autant pour prendre connaissance par exemple de la partie restée inaccessible du protocole informatique ou de communication, ou encore de toute consigne, information, secret ou signal. Présentement ne se produit aucun actionnement de la serrure, mais la simple apposition d'une empreinte informatrice sur, avec ou dans une précédente empreinte faisant office de clé. Cette apposition est consécutive à la vérification d'adéquation entre cette clé et cette serrure, lors de leur mise en relation.

La figure 5b présente un usage particulier de la serrure numérique, de confirmation auprès d'elle que le griffage appartient bien à son auteur homologué. Il n'est présentement pas encore désiré ouvrir un coffre, un accès, un sas ou actionner un autre mécanisme, et le seul bon fonctionnement de cette serrure sera en soi une information pertinente.

La serrure 50 aura connaissance des coordonnées ou identité de télécommunications d'un auteur aussi bien si nécessaire que de son pseudonyme. Ces coordonnées de communication correspondant à ce qui apparaît dans le protocole complet d'un de ses envois.

L'action consistera à introduire la clé, puis à tenter de faire tourner la serrure. Il sera ici considéré que le profil longitudinal de la clé a pu demeurer caché au réceptionnaire 52, parallèlement au fait qu'il n'aura pas accès à la morphologie interne du barillet 502, avec en particulier la longueur des goupilles ou la position des garnitures internes. Par transposition, le profil longitudinal caché de la clé correspond ici à la partie restée fonctionnellement interdite d'accès 532 au sein du protocole informatique ou de communication, et la morphologie interne du barillet correspond à cette même partie telle que connue et transmise à la serrure par l'autorité d'anonymisation 4.

Cet usage sert notamment à confirmer auprès du réceptionnaire et vérificateur, en cas de correspondance avérée entre la partie fonctionnellement interdite d'accès 532 et la morphologie interne du barillet 502, que la partie visible 531 ou accessible pour lui dans le protocole, est bien couplée à la partie qui lui est restée invisible 532 ou inaccessible. C'est-à-dire par exemple confirmer à ce réceptionnaire que tel griffage dont il a connaissance est bien couplé à l'identité de communication qui l'accompagne, tels que l'autorité d'anonymisation 4 les reconnaît liés.

La figure 5c présente une affectation où la serrure numérique sert à tous les usages courants d'une serrure, tels notamment qu'actionner un mécanisme ou un signal, autoriser ou non un accès, ouvrir un sas ou un coffre 59 pour accéder à son contenu.

Cette fonction peut relever aussi bien d'un automatisme indépendant de la volonté de cet utilisateur, qu'à une configuration où il peut par exemple choisir ce dont il a besoin dans un coffre préalablement rempli de diverses

données par l'auteur ainsi éventuellement que par l'autorité d'anonymisation. Ce coffre 59 peut être personnalisé et réservé à l'accès d'un seul destinataire pré-désigné, autant qu'être accessible à plusieurs ou tous les destinataires éventuels. Ce coffre peut s'apparenter aussi à un garde-meubles, dans le cas où l'auteur choisisse d'être son propre destinataire. L'accès au coffre peut être assujetti à toutes formes de contraintes ou conditions suspensives, telle qu'une ouverture seulement après une date déterminée.

Les contenus que le réceptionnaire peut recueillir via cette serrure et par l'ouverture d'un coffre numérique 59, ne sont pas limités a priori : il peut s'agir d'attributs d'identité, du pseudonyme de l'auteur aussi bien que de toute donnée, consigne, signal informatif ou déclencheur, sous la seule réserve que le dépôt y ait été fait par ou avec l'assentiment soit de l'auteur soit de l'autorité d'anonymisation soit de tiers habilités par eux, selon les diverses chartes d'emploi envisageables. Dans les cas où il ne s'agit pas d'un coffre mais d'un autre type de dispositif tel qu'un sas ou un mécanisme, leur configuration et leur fonctionnement sera réglé à nouveau soit par l'auteur soit par l'autorité d'anonymisation.

La fonction habituellement dévolue à un tiers de confiance est ici subdivisée entre une autorité d'anonymisation 4 et cette serrure 50. Cette serrure numérique peut être une entité unique et autonome faisant office de guichet. Elle peut présenter d'autres configurations, jusqu'à son installation auprès du réceptionnaire 52, dans une logique par exemple de boîte noire recevant prioritairement les flux. Dans ce dernier cas, l'actualisation des données relatives aux griffages variants ou encore contenues dans le coffre numérique, se fera par le truchement soit d'un point central gérant ces serrures numériques décentralisées, soit de l'autorité d'anonymisation, soit d'un panachage des deux. La notion de point central n'implique pas son immuabilité ni son caractère unique.

Dans une variante, le réceptionnaire et vérificateur pourra se voir astreint, pour pouvoir vérifier un griffage faisant cryptonyme auprès de la serrure 50, à faire lui-même usage d'un système d'identification ou d'authentification qui le signale comme réceptionnaire connu et autorisé.

La figure 6 illustre un exemple d'usage d'une clé numérique requérant celui de contre-clés. Un auteur 51 dispose d'un document, ou émet un courrier, avec un griffage 53.

Un coffre donné 45 se voit muni d'une serrure 50 correspondant au griffage 53 inséré dans un protocole, ainsi que d'une seconde serrure 50' correspondant à une marque 53' accordée à un réceptionnaire 52 ou à une autorité déléguée. Ce réceptionnaire 52 ou son délégué, pour ouvrir le coffre ou pour actionner la première serrure 50, doit faire usage à la fois du griffage 53 découvert dans le protocole, nommé clé, et de sa propre marque 53' nommée contre-clé.

Le nombre de serrures n'est pas limité et d'autres contre-clés 53'', correspondant à d'autres serrures 50'', peuvent être attribuées au réceptionnaire, ou à un tiers tel que peut l'être un de ses collègues 61, voire à l'auteur qui a apposé le griffage initial.

L'entité 4 qui accorde ou non, émet et distribue les clés et les contre-clés est une autorité d'anonymisation. Avantageusement, il pourra s'agir d'une entité dédiée à cette fonction. Ce peut être un pluriel d'entités. Une autorité d'anonymisation peut être elle-même détentrice d'une contre-clé pour tel coffre.

La figure 7 présente les grandes étapes possibles d'un procédé selon l'invention, appliqué à titre d'exemple à un réceptionnaire central 2 ayant reçu une commande 1 émanant d'un client dans le cadre d'un achat en ligne par exemple sur internet. Leur relation basée sur un désir de protection de divers attributs d'identité du client, se traduira auprès du gestionnaire de site internet par le fait de lui interdire fonctionnellement par exemple de prendre connaissance ainsi que de conserver et d'archiver, ou de traiter, des données contenues.

Ce réceptionnaire 2 préparera le colis et la facture, mais ne connaîtra ni le nom de l'acheteur, ni ses références bancaires, ni son adresse postale pour faire acheminer le colis. Sa connaissance se réduira à :

- l'existence d'un griffage 71 inséré dans le protocole, lui ayant par ailleurs fonctionnellement interdit d'accéder notamment aux coordonnées de télécommunication de l'auteur ;
- la nature et le détail de la commande ;

À partir de ses tarifs correspondant à cette commande, il émettra une facture mais dépourvue encore du nom du débiteur.

Copie du griffage sera adressée par lui à un groupement de cartes bancaires 72, accompagné de la facture sans nom. Ce signe de reconnaissance permettra au groupement de déterminer l'identité du débiteur à y ajouter, et de procéder au prélèvement financier correspondant.

Le même griffage sera adressé à une administration postale 73, accompagné du colis sans nom de destinataire. Ce signe permettra au postier d'ajouter le nom et l'adresse physique correspondants.

Dans les deux cas, ces destinataires périphériques que sont un groupement de cartes bancaires 72 ou une administration postale 73, demanderont ou auront reçu en parallèle transmission de l'équivalence entre tel griffage et telle information périphérique laissée à leur seule discrétion. Cette mise à disposition parallèle ou séquentielle peut résulter soit d'une communication directement faite à leur attention par l'auteur 10, soit, dans un mode d'organisation plus rationnel, par l'autorité d'anonymisation 4 qui centralisera la gestion des équivalences ou via la serrure numérique. L'une ou l'autre coopérera avec les réceptionnaires périphériques 72, 73, en leur transmettant l'équivalence entre un griffage 71 et une identité réelle ou autre attribut ponctuel d'une personne.

Ce réceptionnaire périphérique,

- dans le cas d'un groupement de cartes bancaires 72, connaîtra généralement déjà les références bancaires liées à l'identité de son client ;
- dans le cas d'une administration postale 73, généralement ignorante des références domiciliaires de la personne, l'autorité d'anonymisation ou la serrure numérique pourra les détenir et les lui transmettre, autant que tout autre adresse non domiciliaire et laissée au choix de l'auteur. Cette dernière adresse pourra être celle de la personne bénéficiaire d'un achat de fleurs ou d'un bijou à faire livrer par un tiers, lorsqu'on désire que le commerçant ne connaisse ni l'acheteur ni la bénéficiaire.

Le nombre de réceptionnaires périphériques n'est pas limité, et l'exemple précédent peut être étoffé. Par exemple, un opérateur de télécommunications 75 est susceptible d'être activé pour acheminer une

réponse à l'auteur 10, en ajoutant son adresse internet sur un libellé provenant du réceptionnaire central 2. Ce dispositif fonctionne aussi si l'auteur du courrier ou de la visite devient à un moment ultérieur bénéficiaire par exemple d'un téléchargement ou pour toute autre réception.

Les informations et consignes transmissibles via l'autorité d'anonymisation 4 ou la serrure numériques ne sont pas limitées a priori. Il peut s'agir non seulement d'un attribut d'identité telle qu'une adresse postale, mais aussi de précisions sur les modalités d'envoi désirées, sur le type d'emballage désiré ou toute autre requête.

Dans une variante, et afin de limiter le pouvoir d'action ou de décision autonome laissé aux réceptionnaires périphériques, il peut être envisagé que ces informations périphériques soient elles-mêmes incomplètes ou insuffisantes pour comprendre ou mener à bien la tâche prévue, sans réception en sus :

- soit d'une partie visible du contenant ou du contenu du courrier, transmise par le destinataire central ;
- soit d'une partie de ce courrier, invisible pour le seul destinataire central, mais transmissible par lui ;
- soit enfin d'une addition des parties visibles et invisibles, présentes au choix tant dans le contenu que le contenant.

Dans la suite du processus, et aux fins de compléter l'anonymisation, le réceptionnaire périphérique en charge du prélèvement financier sur le compte de l'auteur pourra servir de compte intermédiaire lors du versement au réceptionnaire central.

De même qu'une administration postale pourra remplir les mêmes bons offices d'intermédiation pour un accusé de réception.

La figure 8 présente les étapes possibles d'une réponse anonymisée à une candidature elle-même anonymisée, ou à une notation d'un test mené en ligne, puisque les diverses tâches citées dans cette dernière sont susceptibles de motiver de mêmes désirs de confidentialité ou d'intimité en sens retour. Cette configuration peut également suivre chronologiquement celle de la figure 7.

Le réceptionnaire central 2 reçoit la soumission 1 sans pouvoir accéder au contenu, automatiquement transmis à un réceptionnaire périphérique 73 qui en ignore l'auteur. La notation ou réponse est ensuite transmise par l'intermédiaire soit du réceptionnaire central 2 s'il a le droit de connaître l'auteur, soit plus avantageusement pour parfaire l'anonymisation par l'intermédiaire d'un tiers 81, à qui il adresse le griffage ainsi que la notation ou réponse. Ce tiers obtient les coordonnées de l'auteur auprès de l'autorité d'anonymisation 4 ou via la serrure numérique, et lui adresse la réponse sans précision sur l'intervenant qui l'a formulée.

La figure 9 présente les étapes possibles qui permettent à un réceptionnaire de données, tel qu'un site de commerce électronique 2 de poursuivre une partie de ses activités de bonne connaissance ou de profilage de ses consommateurs ou visiteurs, mais via une forme d'anonymisation qui ne la perturbe pas sur sa partie utile. Ne se trouve abolie que la partie intrusive envers l'intimité des personnes, qui consiste à les connaître cette fois nominativement. Laquelle partie intrusive présente le défaut d'être souvent dissuasive, pour certains achats ou certaines visites. Le fait dorénavant de connaître et reconnaître un habitué sous le pseudonyme dédié d'Arlequin 74, par exemple, ne sera dans la quasi-totalité des cas pas moins efficace que sous son vrai nom, pour lui proposer des prestations ou des avantages calqués sur son comportement ou sa situation passés. Le procédé selon l'invention ajoute par ailleurs à cet anonymat garanti au visiteur, une même impossibilité à raccorder son comportement à la facturation pour l'acheteur, via les réceptionnaires périphériques bancaires.

Un réceptionnaire constatant la présence d'un griffage 71 sur un courrier, obtiendra son équivalence sous forme du pseudonyme de l'auteur, tel qu'Arlequin. Le pseudonyme 74 est invariant, tandis que le griffage 71 est variant, susceptible d'avoir changé depuis le dernier courrier. L'autorité d'anonymisation 4 ou la serrure numérique est à même de raccorder cette suite de griffages à leur pseudonyme stable.

Le réceptionnaire principal 2 est ainsi à même de relier la présente visite ou demande de l'auteur, à son passé et aux observations faites antérieurement. Dans le cas d'un laboratoire d'analyse par exemple, il peut s'agir de mesurer l'évolution d'un facteur de santé. Dans le cas d'un site internet, il peut s'agir

d'avoir répertorié ses achats, préférences, centres d'intérêt, ainsi que ses droits ou devoirs tels qu'une remise pour fidélité d'achat. Ce réceptionnaire 2 pourra également envoyer des courriers à cet auteur, sans connaître son identité réelle, et en passant par des réceptionnaires périphériques 73, 75 qui obtiendront ces données confidentielles via l'autorité d'anonymisation 4 ou la serrure numérique, sur présentation du griffage.

De même, le réceptionnaire central 2 pourra personnaliser, par exemple via un webmestre 91, la page visitée, en la configurant en fonction de cette connaissance du passé d'Arlequin.

La figure 10 présente une variante apportant une restriction au principe de reconnaître sans connaître, présenté par la figure 9. Variante possible lorsqu'elle est acceptée par tous les protagonistes, et autorisant plusieurs pseudonymes simultanés ou successifs à un même auteur. Cet arbitrage où un ou plusieurs griffages renvoyant à une pluralité de pseudonymes se raccorderaient tous à la même identité par un jeu d'arborescence, ou formeraient des alias en chaîne unique, renforcerait le secret qui l'entourerait, à l'avantage de l'auteur mais au détriment informatif du réceptionnaire. Ceci peut s'inscrire dans une logique de pseudonymes à la carte, comme il existe des identités à la carte ou des degrés de protection et de sécurité à la carte, et correspondre à une attente de l'auteur supportable par le destinataire.

Dans cette configuration, le réceptionnaire central 2 ignorera le lien existant entre les divers pseudonymes d'un même interlocuteur, mais conservera la garantie que sous ses multiples apparences il reste homologué par l'autorité 4 accordant les pseudonymes. Homologation susceptible de découler de critères sélectifs eux-mêmes connus du réceptionnaire 2, ces critères étant capables de maintenir un interlocuteur comme persona grata ou bénéficiant d'avantages.

En prolongement, le réceptionnaire 2 pourrait signaler auprès de l'autorité 4, qu'elle considère désormais tel interlocuteur comme personna non grata, quel que soit son pseudonyme du moment, et ainsi le proscrire à l'avenir lors d'un courrier ou d'une visite de sa part. L'interdiction pourrait éventuellement être plus absolue par un mécanisme d'élargissement du périmètre de la sanction auprès d'autres réceptionnaires 21, 22 ayant accepté le principe de

cette communauté décisionnaire d'agrément, de notation, de bannissement ou de quarantaine. Par exemple, une banque qui considérerait qu'un veto émis par un groupement de cartes bancaires à l'encontre d'une personne, s'applique automatiquement à elle aussi, au moins à titre conservatoire.

De manière préférable, cette variante pourra être déployée selon un mode où l'auteur 10 peut choisir initialement mais définitivement celui de ses pseudonymes qu'il désire, pour s'adresser à tel réceptionnaire 2, 21, 22. Par la suite, il conservera ce pseudonyme durant ses courriers ultérieurs. De la sorte, deux réceptionnaires différents ne pourraient pas savoir qu'Arlequin, chez l'un, et Pierrot, chez l'autre, correspondent au même auteur, tout en sachant que leur détenteur correspond sous ces deux étiquettes à leurs code comportemental admis. De même, par un effet de partenariat par exemple entre sites de commerce électronique, la fidélité d'un visiteur à deux sites pourrait déboucher sur des remises calculées sur l'addition de ses consommations chez chacun. L'un des intérêts de cette formule est une limitation au croisement des fichiers au-delà de ce qui suffit pour la bonne relation au consommateur.

L'option où l'auteur peut choisir des pseudonymes différents pour s'adresser à un même interlocuteur pourra faire l'objet d'un refus venant de partenaires commerciaux.

Elle est cependant envisageable dans le cas où l'échange relève par exemple d'une expression de sa pensée, tel qu'un visiteur régulier de forum de discussion politique, qui ponctuellement souhaite déroger à son pseudonyme habituel sous lequel ses interlocuteurs le connaissent, pour exprimer un point de vue ponctuel moins orthodoxe.

Avantageusement, et afin de limiter des échanges d'information intempestifs, l'autorité d'anonymisation 4, ou la serrure numérique via un mécanisme de dépôt et d'enregistrement, pourra servir de pôle centralisateur des notations, appréciations ou cotations venant des divers réceptionnaires, et concernant un même auteur quel que soit le pseudonyme 101 sous lequel il est initialement étiqueté. Cette autorité d'anonymisation 4 ou la serrure distribuera ces jugements aux autres réceptionnaires soit à leur demande au vu du griffage transmis, soit de manière plus automatisée selon une charte d'emploi prédéfinissable.

La figure 11 présente une configuration dans laquelle un même auteur 10 peut disposer simultanément de plusieurs griffages différents A, B, utilisables selon son choix ou selon des procédures prédéfinissables.

Ce caractère adaptatif pourra porter aussi sur le fait de faire pré-enregistrer plusieurs comptes bancaires 111, 112 ou plusieurs cartes de paiement ou encore par exemple plusieurs adresses et plus généralement tous attributs. Chaque pré-enregistrement donnant lieu à attribution non seulement d'un griffage A, B, mais d'une filiation de ce signe distinctif, puisque celui-ci est variant.

Cette pluralité de choix offrant la possibilité de rendre préférentiellement activable l'un plus que l'autre, selon des chartes d'emploi prédéfinies et actualisables si de besoin, une charte liant l'auteur 10 à l'autorité d'anonymisation 4, qui dès lors transmettra à un réceptionnaire 72 l'information correspondante.

Une variante consiste par exemple à ce qu'un courrier vers un réceptionnaire 2 soit couplé à une copie avec consigne ponctuelle, vers l'autorité d'anonymisation 4 ou sous serrure numérique. Cette formule moins simple serait envisageable principalement pour des cas de figure suspendus à des réserves, des clauses conditionnelles, suspensives ou moratoires, des confirmations ou validations à venir, tels qu'un choix final de compte à débiter fait après vérification des avoirs réellement disponibles sur les divers comptes de l'auteur. Ce peut être envisagé aussi pour les cas de validation ultérieure d'un choix sur lequel l'auteur a légalement le droit de revenir, ou lorsqu'il attend livraison effective d'un produit ou d'un service pour juger de sa qualité réelle.

La figure 12 présente des dispositions dans lesquelles des pseudonymes, des polynymes ou des cryptonymes selon l'invention sont susceptibles de prolongements et d'usages dans la vie sociale ou économique matérielle.

Le triple niveau constitué d'une identité réelle couverte par des griffages fonctionnellement masquant de cette identité, et eux-mêmes rattachables à un ou plusieurs pseudonymes 123, sont utilisables dans la vie réelle. Un pseudonyme pourra de la sorte s'exprimer, en substitut de la traditionnelle identité réelle, sur un support physique matériel, telles qu'une sorte de carte d'identité, une carte à puce, un ticket, un jeton ou encore une forme de

tatouage ou d'en-tête personnalisés. Ceci pourrait trouver emploi par exemple pour venir retirer à un guichet ou pour justifier auprès d'un contrôleur une commande préalablement passée et payée par télécommunications.

L'auteur par exemple d'une commande sur internet ou via son téléphone mobile pourra d'une part être débité selon les modalités déjà exprimées dans la figure 7, mais de plus passer prendre l'objet ou le service acheté auprès d'un guichet 121. Il se présentera alors muni d'un support physique 122 tel qu'un badge, marqué de son pseudonyme, Arlequin par exemple, et délivré par l'autorité d'anomysation 4. Le guichet aura reçu l'équivalence entre le griffage présent dans le courrier de la commande 1, et ce pseudonyme. Des mesures de sécurisation du badge sont envisageables, soit internes au support, soit par des recoupements complémentaires entre certains codes ou marques distinctives présents sur ce support et référencés par l'autorité d'anonymisation ou la serrure numérique.

La figure 13 présente un mode de déploiement du procédé selon l'invention permettant d'anonymiser et d'encadrer restrictivement la mémorisation d'un flux 1 pour lequel l'auteur 10 ne disposerait pas d'une pleine liberté de choix du destinataire 2, d'une pleine liberté d'activation ou non de ce flux, ou encore d'un plein contrôle sur le système émetteur de ce flux. Ce cas de figure est fréquent, s'agissant de supports de communication à usage unique ou à gestionnaire unique, telles que des sociétés de transports en commun. Celles-ci optent fréquemment en matière d'anonymisation soit sur un effacement de mémoire en une ou plusieurs fois, donc postérieur à la mémorisation, soit sur une anonymisation antérieure à la fabrication et la délivrance du support. La présente solution s'intercalerait entre les deux options précitées.

Le titre de transport électronique d'une personne ne se signalerait en termes d'identité, auprès des bornes de passage 131, que par le griffage, masquant fonctionnellement tout autre attribut d'identité. Ce griffage serait par la suite éventuellement transmis à l'autorité d'anonymisation 4 ou la serrure numérique, via un réceptionnaire central 2, en cas de désir de profilage du comportement dans la durée, mais ne serait connu que par le pseudonyme invariant transmis en retour.

Il peut s'agir à titre de second exemple d'un opérateur de télécommunications mobiles, dont le terminal de chaque abonné adresse par intermittence un signal au réseau d'antennes relais, pour lui signaler sa position géographique actuelle en cas d'appel venant d'un tiers. Faute d'anonymisation selon la présente invention, beaucoup de ces dispositifs aboutissent à des formes de traçabilité qui font dépendre le respect de l'intimité d'une sécurisation aléatoire de la détention ou de l'effacement des données correspondantes, ou d'une déontologie difficile à vérifier. Pareille solution technique trouverait également application dans nombre de terminaux ou supports communicants, et en dialogue tant avec des bornes terrestres ou embarquées qu'avec des satellites de positionnement et de géolocalisation.

Cette voie serait d'autant plus désirable que de tels dialogues, lorsqu'ils se font avec un gestionnaire unique, relèvent généralement du seul vouloir de ce dernier.

Par le procédé selon l'invention, un tel gestionnaire ne connaît le comportement d'un usager qu'à travers le griffage correspondant à un pseudonyme. Selon les cas de figure choisis, il pourrait par ailleurs continuer ou non à gérer parallèlement un client en le connaissant cette fois par son identité puis notamment à travers ses paiements successifs. Toutefois, même en cas d'une pareille connaissance parallèle de son identité réelle, le gestionnaire ne pourrait établir de lien avec un profil comportemental donné, au sein de tous ses clients. Cette option en découpage lui permettrait sur la facette nominative de vérifier des impayés ou, parmi d'autres possibilités relationnelles, de lui assurer des remises ou avantages découlant de sa position de client.

Un troisième exemple d'application concernerait les éditeurs de logiciels ou fabricants de composants électroniques aptes à dialoguer directement et sur leur initiative immédiate ou programmée, avec un logiciel ou équipement installé sur le terminal d'un usager. Le fait de désirer constater en ligne une panne, un comportement ou un état général, ne serait rattaché qu'au seul griffage de cet usager. Cette procédure serait parallèle et découplée de celle de gestion de la relation au client en tant qu'acheteur et payeur connu, selon un mode de déploiement cloisonné : autorité d'anonymisation éventuellement couplée à une serrure numérique d'une part, et réceptionnaires

périphériques d'autre part. Le terme acheteur s'élargit aux formes de contractualisation courantes en informatique, telle que la location.

La figure 14 présente un procédé selon l'invention où un réceptionnaire 2 de courrier 1 aura accès à des attributs d'identité ou d'information présents dans le protocole de communication, mais sans connaître la nature et le détail de sa relation à suivre avec lui. Il ne sera de la sorte informé que de l'existence de ce lien.

Ce mode de déploiement particulier du procédé selon l'invention s'écarterait des fonctions basiques dérivées de la présence de ce griffage. Ces fonctions optionnelles de base étant, pour rappel :

- interdiction de prise de connaissance de tout le contenu du courrier ;
- interdiction de prise de connaissance d'une partie du contenu du courrier, précédemment évoquée par les exemples d'encarts, encadrés ou autres coupons détachables ;
- interdiction de prise de connaissance de documents attachés ;

La fonction dominante et constante ci-dessus restant celle d'interdiction de prise de connaissance de tout ou partie du reste du protocole.

Dans une inversion, il serait possible que, en cas de présence d'un griffage dans ce protocole, le réceptionnaire central 2 ait droit de lire ce protocole et lui seul, d'en connaître donc l'auteur 10 au moins par ses coordonnées de télécommunications, mais sans pouvoir accéder à tout ou partie du contenu. Ce contenu resté inconnu de lui serait transféré à des réceptionnaires périphériques, édulcoré par amputation de son protocole initial. Cette transmission concernera pour tout ou partie par exemple le contenu du courrier et d'éventuels documents attachés. Les réceptionnaires périphériques 72, et indirectement 141 et 142, obtiendront via la serrure numérique ou auprès de l'autorité d'anonymisation 4, contre présentation du griffage, les informations et consignes nécessaires à la bonne réalisation de leur tâche, tel que le compte bancaire à débiter.

De la sorte, le réceptionnaire central 2 saurait avoir tel auteur comme client, comme adhérent ou interlocuteur, mais resterait ignorant de la prestation qui va lui être fournie. Dans pareil cas, si la prestation donnait lieu à une facturation ou autre comptabilité, le montant concerné serait au final par exemple noyable dans la masse des autres encaissements et resterait

inconnu dans le détail par le réceptionnaire central. Un tel cas de figure pourrait utilement trouver application lors de dons versés à un organisme caritatif ou pour une quête en ligne, lorsque les auteurs ne sont pas désireux que le montant versé par chacun soit connu du réceptionnaire ou du bénéficiaire ultime. Ce dernier saurait qui remercier, sans pouvoir porter de jugement quant aux montants respectifs. Le spectre concerné irait d'une cagnotte pour un départ en retraite, jusqu'à une donation ouvrant droit à défiscalisation elle-même gérée par un réceptionnaire périphérique ad hoc.

Une option voisine serait que le réceptionnaire central 2 ne conserve à nouveau que le protocole, mais sans avoir le droit d'y connaître autre chose que le griffage. De la sorte, il sera informé de la fidélité de tel interlocuteur anonyme, de l'acte d'envoi fait par cet auteur à son attention, et sera apte à lui garantir que le courrier est bien parvenu. Ce retour sous forme d'accusé de réception s'effectuant, faute d'adresse de communication, par un réceptionnaire périphérique tel qu'un opérateur de télécommunications.

La figure 15a présente un emploi du dispositif dans une relation telle qu'inter-entreprises ou inter-sites, où le griffage permettra la délivrance de données ou de signaux. Un fichier informatique 1 dont le protocole porte un griffage, et conservé sur l'ordinateur d'une société « auteur » 10, reçoit la visite ou encore la demande de téléchargement d'un employé d'une entreprise partenaire, ou d'un autre site, qui souhaite en utiliser le contenu. La présence du griffage renvoie initialement ce visiteur ou réceptionnaire 2 vers l'autorité d'anonymisation 4 ou la serrure numérique, qui lui délivrent des conditions, requêtes, consignes ou informations, préalables, simultanées ou consécutives à l'éventuelle autorisation d'accès ou de téléchargement, autorisation d'ordre fonctionnel mais qui peut aussi prendre des formes matérielles telle qu'une clé de déchiffrage du contenu. Des outils d'identification et d'authentification peuvent être employés à cette occasion. L'autorisation ou interdiction peut aussi concerner le traitement, la mémorisation ou la retransmission de tout ou partie du fichier et de son contenu.

Dans le présent cas, une requête pourra être de justifier d'un agrément préalable décerné par l'entreprise détentrice à ce partenaire. Une consigne pourra être de prévenir un superviseur 173 ou de lui adresser copie de toute

action ultérieure menée avec ce contenu. Le superviseur pouvant être par exemple un technicien dont la présence est jugée indispensable, un chef dont la mise en connaissance ou le contreseing est désiré, un service comptable ou juridique chargé de reporter cet emploi dans ses livres, aussi bien qu'un système technique autonome tel qu'un minuteur qui enregistrera par exemple la durée de consultation du fichier griffé, dans un cas où une tarification sera basée sur une durée.

L'employé ayant par exemple téléchargé le fichier, pourra le faire suivre à un réceptionnaire ultérieur 171 à des fins de réalisation d'une tâche. Dans l'exemple où le contenu du fichier corresponde aux cotes d'une pièce à usiner, le griffage initial pourra conserver un rôle entier, et obliger les réceptionnaires successifs à s'adresser à l'autorité d'anonymisation ou à la serrure numérique. Une armoire électronique gérant la production d'un atelier, et le recevant, pourra de la sorte se voir signifier un niveau d'urgence de la fabrication, complété par une obligation de prendre connaissance de la grille tarifaire émanant du producteur d'électricité attitré. En fonction du degré d'urgence, confronté à la consigne d'optimiser les coûts de fabrication, un arbitrage pourra être mené au niveau de l'armoire quant à l'attente ou non d'une plage tarifaire basse, correspondant à des horaires de consommation collective faible, sans pic de production ni risque de surcharger les réseaux de distribution internes ou externes. Lors du moment idoine, la machine à commande numérique 172 recevant à son tour le fichier griffé, pourra entre autres possibilités se voir intimer l'activation, préalablement à sa mise en route, d'un signal sonore prévenant les ouvriers alentours ou un personnel d'entretien, de se tenir à distance de sécurité. Ce système de sécurité, ou alarme, 170 pouvant être aussi activé directement par l'autorité d'anonymisation.

Ce dispositif, présenté comme inter-sites, s'applique autant à une entité devant assurer son autonomie et son autocontrôle, telle qu'une cellule d'avion, où divers équipements électrotechniques de transmission des commandes doivent garantir leur bon fonctionnement à chaque étape, notamment pour les avions à commande tout électrique.

La figure 15b illustre une configuration d'emploi où le griffage 200 s'apparente à un cachet, un timbre ou un bâton témoin passant de l'auteur

10 chez des réceptionnaires successifs 176, 177, 178, étant porteur et transmetteur d'une signification, d'une grandeur ou d'une valeur convenue, ou encore d'une forme d'exclusivité.

La notion de cachet souligne l'impossibilité d'accéder sans autorisation à un contenu ou à une signification, la notion de timbre souligne la possibilité d'une valeur faciale, et le bâton témoin exprime un dessaisissement au profit d'un nouveau porteur, en conservant cette valeur initiale, cette grandeur ou cette symbolique.

Un griffage endossant une pareille représentativité, donc se voulant paré de confiance, implique qu'il ne soit pas falsifiable ni imitable et reproductible en série, critères ardus à obtenir au sein de technologies auxquelles la faculté de clonage est quasi inhérente. Cette fragilité est toutefois contournable avec le présent dispositif, par le fait qu'une confiance globale n'est pas seulement placée dans le griffage technique, mais aussi dans la confiance que la communauté qui pratique les échanges se porte à elle-même et à sa solidarité, ainsi que dans la confiance qu'elle accorde à l'organisme qui les accorde. La conjonction de ces trois sous-parties de la confiance en bâtit la somme, et une baisse sur l'une d'elles, autant qu'elle n'atteigne pas un seuil rédhibitoire, peut souvent être compensée par une hausse sur une des deux autres.

Par ses fonctions d'homologation, radiation ou suspension des auteurs et réceptionnaires, via sa latitude à accorder ou retirer un système de griffage ou des contre-clés, l'autorité d'anonymisation 4 assume un rôle de fédérateur de communautés. Communautés aptes à une bonne cohésion interne car se sachant en partage, par exemple, d'une même éthique ou de mêmes normes comportementales intégrées dans ces stipulations pour être et rester homologué. Transférer ces propriétés de transparence et de vérifiabilité dans les télécommunications, tout en passant à une échelle spatiale et quantitative plus large, est habituellement difficile puisque ces dernières, et surtout internet, jouent au contraire sur l'argument de l'anonymat sinon de l'emploi à volonté de fausse identité. À nouveau, le dispositif selon l'invention remédiera à ce dilemme en étant à la fois un outil qui permet de connaître autrui, tout en le laissant anonyme, ce par le truchement de son système de pseudonyme. L'autorité d'anonymisation ou la serrure numérique, informant les réceptionnaires successifs de la signification, de la grandeur ou de la

valeur attachée au griffage en soi, peut en effet en présenter l'auteur expéditeur sous son pseudonyme 74 autant que par sa véritable identité. Cette identité réelle ayant pu jusqu'alors rester inaccessible à ces réceptionnaires de par le griffage fonctionnellement masquant de l'identité de télécommunications de son auteur.

De plus, le fait que le griffage n'exprime ce qu'il représente que via cette requête du réceptionnaire 176, 177, 178 vers cette autorité ou vers la serrure, permet de tracer son parcours, de garantir qu'il ne se retrouve pas contrefait ou dupliqué, tout au moins pas autrement que selon une charte d'emploi convenue au sein de la communauté. Ce faisant, l'autorité d'anonymisation revêt un statut d'observateur de flux, et de garant que s'y applique, dans les proportions désirées, l'adage du rien ne se crée rien ne se perd. Elle est émettrice du système de griffage, puis observatrice apportant sa caution en termes de traçabilité, en partie assimilable dans sa finalité à un envoi avec accusé de réception.

La confiance peut donc être capitalisée dans et autour de l'autorité d'anonymisation :

- en l'autorité elle-même, de par son statut indépendant, d'arbitre, de mémoire et de référent ;
- dans le griffage, de par les capacités techniques de l'autorité d'anonymisation à le rendre robuste ;
- dans la confiance que la communauté a en elle-même, et qui découle de la bonne application par l'autorité d'anonymisation de ses pouvoirs régulateurs. Point accru par la visibilité non intrusive qu'apporte le système de pseudonymes.

Étant organisme émetteur du système de griffage, l'autorité d'anonymisation peut par ce fait s'associer ou fusionner avec un autre organisme 175 apte à lui conférer et faire reconnaître une grandeur, une valeur ou une symbolique donnée, et lui donner cours. Cet organisme, à la fois régulateur et garant, peut être par exemple une société ferroviaire dans le cas où le griffage tienne lieu d'exclusivité momentanée d'usage d'une voie, accordée à tel réceptionnaire. Il pourra s'agir d'une régie postale qui décerne une valeur faciale à une sorte de timbre numérique ou de cachet, lors d'un acheminement sécurisé sur des réseaux. Ce peut être encore une société de services en ligne, un site marchand, une banque privée voire une banque

centrale, dans le cas d'une valeur faciale prenant une dimension monétaire. Cette dernière application n'étant que l'addition d'un timbre ayant valeur, et cessible comme un bâton témoin.

Toutefois, le principe de cloisonnement qui sous-tend la présente invention, prédispose à scinder les rôles pour maintenir la philosophie de protection de l'intimité numérique des utilisateurs. L'articulation entre cette autorité d'anonymisation « émetteur de griffage » et un prestataire de service ou un régulateur 175, « émetteur de valeur », exprimerait le dispositif dans sa variante la plus avantageuse. Une option médiane serait que l'autorité d'anonymisation délègue un tiers à cette tâche de fixation de valeur, de grandeur ou de symbolique. Dans ces deux derniers cas de figure, l'émetteur de base reste cependant, dans les faits, l'autorité d'anonymisation, puisque c'est sur lui que vient se superposer une signification convenue. La scission ne fait que conférer le titre d'organisme émetteur de valeur ou de symbolique, mais non sa matérialité, à l'acteur qui, ferroviairement ou postalement, régule des trafics. Ou qui, bancairement, régule des transferts, gère la comptabilité et la conversion de ces monnaies, accorde d'éventuels prêts, ouvre et ferme des comptes. Ces divers tiers informent l'autorité d'anonymisation de la signification d'un futur griffage concernant tel auteur avec lequel ils viennent de contracter.

Le risque de duplication du griffage par un intervenant, puis l'envoi des clones à plusieurs interlocuteurs, reste circonscrit par le fait que la réception donc son « endossement » par un réceptionnaire, sera enregistrée par l'autorité d'anonymisation 4 lorsque ce réceptionnaire le lui présentera pour en connaître le sens. Tout doublon intempestif sera de ce fait identifié par elle, et d'autant plus si le dispositif retient l'option supplémentaire d'une mise en copie 179 par l'auteur expéditeur, destinée à l'autorité d'anonymisation, et qui lui signale cette forme d'acceptation de dépossession virtuelle.

Cette propriété anti-doublon sera à plus juste titre qualifiée de garant qu'une duplication demeure dans la limite quantitative convenue, puisque l'autorité d'anonymisation recensera le nombre de réceptions d'un même griffage émis par un auteur donné, ou de manière imagée, le nombre de fois où le courrier aura été décacheté.

Une manière alternative de réduire la dangerosité d'éventuels doublons incontrôlés serait de leur faire perdre partiellement ce statut indifférencié en

les personnalisant dès leur première étape, principe par ailleurs extensible à d'autres usages industriels ou ludiques. Sans faire perdre au griffage son caractère distinctif et particularisant, sa partie caractéristique et dotée de propriétés fonctionnelles et cryptonymiques pourrait se voir assortie d'ajouts ou de modifications signalant soit son nombre de réceptionnaires successifs, à l'instar d'un compteur ou d'encoches numériques, soit plus précisément leur nature, leur profil voire leur identité. Un pareil mécanisme serait assimilable à un réel endossement, laissant ici une latitude de choix entre un endos par signature anonymée, pseudonymisée ou porteuse d'une identité véritable.

Une telle conservation de la trace de ses réceptionnaires successifs, selon une forme d'endossement matérialisée par exemple dans ou autour du griffage initial, trouverait un pendant dans le fait qu'un griffage puisse exprimer, dans son apparence formelle, une filiation relative cette fois aux griffages successifs de l'auteur. Ces diverses filiations pourraient s'exprimer par exemple de manière pleinement visible, filigranée, cachée ou codée.

Une autre variante d'application de ce principe se matérialiserait par plusieurs griffages dotés de parentés formelles détectables et interprétables au moins par certains réceptionnaires ou certains observateurs. Ces dernières possibilités s'apparenteraient à un dispositif de type chéquier, où chaque chèque se rattache par des référents à une même souche, tout en étant complété d'autres référents qui le particularisent d'un coup ou progressivement.

À nouveau, une telle configuration n'offrirait qu'une variante d'une mission que l'autorité d'anonymisation est apte à remplir, via le type d'informations qu'elle délivre à chaque nouveau réceptionnaire. De même qu'elle peut remplacer un griffage qu'elle considère caduc ou obsolète, par un autre qui en garde l'empreinte.

La figure 16, illustre un exemple de masquage et démultiplication d'identités par cryptonymes et polynymes. Une autorité de nommage 151 accorde des identités à des entités 152 tels que des objets, artefacts, matériaux, matières vivantes, animaux, personnes, relevant d'un auteur, détenteur ou tuteur 150, 150', 150'', ici dans une configuration où à titre d'exemple n'existent que six possibilités de noms différents. Une autorité d'anonymisation 4 accorde,

émet et distribue des griffages 153 apposés dans le protocole informatique ou de communication de ces entités. Ce griffage faisant cryptonyme 153 vient en préfixe de l'identité 152 préalablement accordée par l'autorité de nommage, ou en toute autre position spatiale aboutissant à la particulariser ou l'allonger.

Ce dit cryptonyme-préfixe permet ultérieurement de permuter l'identité réelle de son détenteur en s'y substituant fonctionnellement et en endossant un rôle d'identité de substitution aux yeux d'un réceptionnaire 155 tel que peut l'être notamment l'autorité de nommage initiale.

Un niveau intermédiaire 154 opère le transfert d'appartenance apparente des entités nommées et portant griffage, depuis leur détenteur réel vers un détenteur inventé. Ce niveau repose sur un dispositif en polynymes, où chaque cryptonyme accordé en plusieurs exemplaires et répartis sur plusieurs entités relevant de plusieurs détenteurs, se retrouve fédéré en un seul polynyme. Ce dernier apparaissant dès lors comme le détenteur des entités concernées. Un polynyme peut regrouper des objets de divers propriétaires originels, tout comme un propriétaire réel peut voir ses entités dispersées sur plusieurs polynymes. Des objets leurres et des polynymes leurres peuvent être créés pour ajouter à cet effet d'écran et de gommage des patrimoines ou des appartenances. Les polynymes peuvent varier dans leur contenu et être éphémères.

L'allongement ou la plus grande variété des identités résultant de l'apposition d'un cryptonyme dans un protocole permet par ailleurs la démultiplication de ces identités. Cette plus grande variété tient aussi à ce que le cryptonyme n'est pas réductible à un ajout de caractères, mais peut être un retrait ou toute modification caractéristique du protocole initial.

La figure 17 illustre un exemple de masquage et démultiplication d'identités avec intermédiation par l'autorité d'anonymisation. Un objectif de masquage des identités réelles des entités et de leur propriétaire s'articule autour d'une autorité d'anonymisation 4 ou de plusieurs. Celle-ci peut, dans l'une de ses configurations, n'être dédiée qu'à cette fonction d'anonymisation.

Cette autorité peut intervenir à un ou plusieurs stades. Elle accorde ou non, émet et distribue à des interlocuteurs, dits auteurs, le droit et le moyen d'apposer des griffages faisant cryptonyme, dans le protocole d'un envoi de

télécommunications ou d'un fichier informatique. Ces griffages sont dotés d'une capacité d'interdiction fonctionnelle de lecture de l'identité réelle de l'auteur.

Un réceptionnaire 161 sera équipé par l'autorité d'anonymisation d'un système de réception apte à détecter et interpréter la signification fonctionnelle de ces griffages. Au cas où le réceptionnaire ne soit pas doté de ce système ou ne présente pas les garanties déontologiques ou matérielles assurant de son bon respect de cette procédure fonctionnelle d'interdiction de lecture d'identité, l'autorité d'anonymisation ou un tiers délégué pourra se voir placée en intermédiaire. Elle sera chargée de supprimer ou rendre inutilisable la partie du protocole apte à identifier une identité réelle, avant de permettre son acheminement ou son usage ultérieur au profit du réceptionnaire prévu.

Griffages, intermédiation et gommage d'identité réelle peuvent intervenir selon divers enchaînements et en divers endroits, en fonction notamment de l'ampleur des fonctions techniques permises à l'équipement de griffage installé sur ou en aval de l'auteur émetteur, ou celles de l'éventuelle boîte noire installée sur ou en amont du réceptionnaire. Il peut également s'agir d'une seule entité et d'un seul lieu, au cas où l'autorité d'anonymisation soit un point de passage obligé entre ces divers acteurs émetteurs et récepteurs.

REVENDICATIONS

1. Procédé de sécurisation et de contrôle de données et d'identités au sein de processus de communication entre un auteur (10, 51) et au moins un réceptionnaire (2), caractérisé en ce que ledit procédé comporte au moins :
- une étape d'insertion d'un griffage (53, 71, 153, 200) dans un protocole informatique ou de communication au moyen d'un système de griffage ;
- une étape de lecture dudit protocole au moyen d'un système de lecture ;
lesdits moyens de griffage et de lecture étant couplés à une autorité d'anonymisation (4), ladite autorité étant complétée par un dispositif à serrure (50), recélant et distribuant des données et des consignes, le couplage entre le griffage et l'autorité d'anonymisation cloisonnant et canalisant des entités, des actions et des identités.

2. Procédé selon la revendication 1, caractérisé en ce que le griffage (53, 71, 153, 200) faisant marquage cryptonymique est signe de reconnaissance, ou clé vers des consignes ou des données recelées par l'autorité d'anonymisation (4) ou le dispositif à serrure (50), mode d'activation de mécanismes ou de signaux, équivalence à pseudonyme ou racine de polynyme gérés par l'autorité d'anonymisation.

3. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'un griffage (53, 71, 153, 200) correspond à des fonctionnalités ou des modalités différentes, des réponses différentes ou des manières différentes de répondre de la part de l'autorité d'anonymisation (4) ainsi que du dispositif à serrure (50), ou des modes de délivrance différents, selon son destinataire, le contexte et l'environnement dans lequel évolue ce destinataire, la chronologie ou la localisation des faits, la manière d'agir ou d'être de ce destinataire, la nature des données ou du signal correspondant à ce griffage ou à ce qu'il va mettre en œuvre, ces modes opératoires pouvant être préétablis et discriminées selon des items convenus avec l'auteur, autant que visés au cas par cas en une ou plusieurs étapes.

4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que plusieurs griffages sont optionnellement disponibles pour un même auteur, de manière séparée ou additionnelle au sein d'un même protocole informatique ou de communication, affectables à des usages différents ou similaires, indépendants ou complémentaires.

5. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que d'une part le griffage (53) faisant clé et d'autre part la dite serrure (50), sont chacune en totalité ou en partie le répondant de l'autre, soit comme profil et contre-profil, soit comme une image et son négatif, soit comme une matrice et son œuvre, soit comme une griffe et sa cicatrice, cette complémentarité vers un tout ou vers une succession générant des capacités de dialogue, de correspondance, de reconstitution du tout ou de la filiation, à des fins de validation, d'identification ou d'authentification, d'actionnement d'un signal ou d'un mécanisme, d'expression d'une signification ou d'une consigne, ou de solidarisation entre eux.

6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le mécanisme de cloisonnement discrimine, parcellise et rend autonome, masque, démarque ou brouille certains sujets, certaines fonctions et tâches, certaines données et certains objets, certaines identités ou coupons d'identité relatifs à un même processus.

7. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le mécanisme de canalisation distribue de manière parallèle ou séquentielle, compose, crée des liens ou des coopérations, agrège, démasque ou re-marque, certains sujets, certaines fonctions et tâches, certaines données et certains objets, certaines identités ou coupons d'identité relatifs à un même processus.

8. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le cloisonnement et la canalisation engendrent une modification de la quantité ou de la qualité des entités impliquées, avec une modification de leur périmètre ou de leur nature, des substitutions, des permutations, une démultiplication des sujets, des rôles et des identités, ou une division de l'information et des secrets à partager.

9. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'autorité d'anonymisation ou le dispositif à serrure détient tout type de consigne, donnée ou signal relatif à la gestion d'un flux ou d'un fichier muni du protocole avec griffage, aussi bien que tout type de consigne, donnée ou signal raccordés à ce griffage ou à une identité donnée, mais indépendants de cette gestion directe et pour leur simple mise à disposition depuis l'auteur envers un réceptionnaire.

10. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le griffage faisant clé de ladite serrure enclenche un accès, un actionnement

de toute forme de sas et porte donnant sur un espace réservé ou coffre numérique, un mécanisme ou un enregistrement, une action ou une réaction technique, ou encore un signal informatif ou déclaratif.

11. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'une serrure (50) existe indépendamment de tout coffre (45, 59) ou autre dispositif subordonné, à des fins de validation de la réalité, l'authenticité et l'actualité d'un griffage faisant clé.

12. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la serrure (50) est dotée de parties non visibles par un réceptionnaire, permettant la validation d'un griffage cryptonymique, ou d'une donnée restée inconnue et correspondant à ces parties non visibles, ou du lien entre ce cryptonyme connu et cette partie inconnue, ou du lien entre plusieurs parties inconnues, la partie inconnue étant un pseudonyme, une identité réelle, la suite du protocole informatique ou de communication, le contenu du fichier ou du courrier, ou toute autre information ou consigne.

13. Procédé selon l'une quelconque des revendications 5 à 12, caractérisé en ce qu'une serrure aligne une juxtaposition, une succession ou une composition des dits contre-profils, des dits négatifs, des dites matrices ou œuvres ou des dites cicatrices, correspondant à au moins un griffage ainsi qu'à d'autres données tel qu'un pseudonyme.

14. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la serrure permet lors de son essai par le griffage, l'apposition ou l'insertion de données supplémentaires dans, avec, autour ou sur ce griffage.

15. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le dispositif à serrure nécessite pour son actionnement au moins un griffage faisant clé, trouvé dans un protocole, et au moins une contre-clé permettant d'authentifier au moins un tiers, réceptionnaire ou autre, doté de sa propre contre-clé, ce tiers pouvant être l'autorité d'anonymisation ou l'auteur, et lesdites clés et contre-clés étant accordées, ou non, par l'autorité d'anonymisation.

16. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'auteur dispose d'une pluralité de coffres numériques ou autres mécanismes, destinables chacun à un ou plusieurs réceptionnaires.

17. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'au moins une consigne de fonctionnement dédiée à au moins un réceptionnaire est transmise ou accessible au moyen du griffage (53, 71, 153, 200) inséré dans le protocole.

18. Procédé selon la revendication 17, caractérisé en ce que ladite consigne de fonctionnement est une autorisation, une interdiction, totales ou partielles et discriminées, l'édiction de requêtes ou de clauses conditionnelles, l'activation, la modification ou l'arrêt d'une fonction d'un réceptionnaire (2, 3, 31, 32).

19. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le flux de communication ou le fichier n'est constitué que du seul protocole marqué du griffage, à l'exclusion de tout contenu.

20. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'une consigne fonctionnelle, relative à la communication, au traitement, à la lecture ou à la mémorisation de données, résulte de la présence du griffage dans le protocole, la consigne concernant le contenu du flux, du fichier ou le reste du protocole.

21. Procédé selon la revendication 20, caractérisé en ce que l'interdiction ou l'autorisation fonctionnelle partielle, concerne une partie prédéterminable du courrier ou du fichier, tant dans son contenu que dans son protocole.

22. Procédé selon l'une quelconque des revendications 20 ou 21, caractérisé en ce que l'interdiction de traitement, de lecture, de communication ou de mise en mémoire de certaines données chez un réceptionnaire (2) s'accompagne de leur orientation vers un autre réceptionnaire périphérique (3, 31, 32) prévu à cet effet.

23. Procédé selon l'une quelconque des revendications 20 ou 21, caractérisé en ce que l'interdiction de mise en mémoire de certaines données chez un réceptionnaire (2, 3, 31, 32) engendre l'élimination de ces données.

24. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le griffage est utilisé par ses réceptionnaires successifs comme signe de reconnaissance entre eux ou avec l'auteur, ainsi que pour obtenir auprès d'une autorité d'anonymisation (4) ou via une serrure (50), la correspondance entre ce

griffage et des attributs de l'identité à laquelle ledit griffage se rattache, ou toute autre donnée ou signal, conservés par elles en vue de cette transmission.

25. Procédé selon la revendication 24, caractérisé en ce que l'autorité d'anomysation (4) ou le dispositif à serrure (50) est habilité à transférer à un réceptionnaire ou un tiers homologué, ladite correspondance ou lesdites données, ledit réceptionnaire ou tiers utilisant ladite correspondance ou lesdites données, pour accomplir une tâche dévolue à lui par un précédent réceptionnaire ou par l'auteur (10) du flux ou du fichier.

26. Procédé selon la revendication 25, caractérisé en ce que ladite tâche ajoute une information, reçue de l'autorité d'anomysation ou du dispositif à serrure, sur un travail resté en partie ou totalement anonyme ou incomplet, en attente des attributs d'identité requis pour l'utiliser, l'acheminer ou le finaliser.

27. Procédé selon la revendication 26, caractérisé en ce que ledit travail est relatif à une transaction électronique entre l'auteur (10) du courrier ou du fichier et un réceptionnaire principal (2).

28. Procédé selon l'une quelconque des revendications 26 ou 27, caractérisé en ce que ledit travail est relatif à un acheminement physique ou par voie de télécommunication entre un réceptionnaire principal ou périphérique et l'auteur (10).

29. Procédé selon l'une quelconque des revendications 26 à 28, caractérisé en ce que ledit travail est relatif à un jeu d'écriture, s'effectuant entre l'auteur (10) et un réceptionnaire principal (2) ou périphérique.

30. Procédé selon l'une quelconque des revendications 26 à 29, caractérisé en ce que ledit travail est relatif à une vérification du fonctionnement, du comportement, de l'état, de l'intégrité ou de l'authenticité touchant un terminal ou un support de communication, et les mécanismes qui leur sont raccordés.

31. Procédé selon l'une quelconque des revendications 24 à 30, caractérisé en ce qu'un réceptionnaire périphérique fait office d'autorité d'anonymisation pour la correspondance entre le griffage et diverses données ou réponses s'y rattachant.

32. Procédé selon l'une quelconque des revendications 24 à 31, caractérisé en ce que l'autorité d'anonymisation (4) est avisée d'un réceptionnaire délégué à une tâche ou un rôle, par l'auteur ou par un réceptionnaire précédent.

33. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le griffage inséré dans un protocole sert d'allonge ou de modificateur, ou de démultiplicateur, à une identité arbitraire attribuée à une entité physique tel qu'un objet, une entité informatique tel qu'un fichier, un flux de communication, ou une entité virtuelle tel qu'un avatar, ainsi éventuellement qu'à leur auteur, détenteur ou expéditeur.

34. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le griffage faisant cryptonyme, inséré dans un protocole informatique ou de communication, sert soit de passerelle vers un pseudonyme, soit de racine commune à diverses identités unifiées en un registre de type polynyme.

35. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'un même griffage inséré dans une pluralité de protocoles sert de référent commun pour créer un registre unificateur d'identités arbitraires attribuées à des objets, flux, fichiers ou avatars relevant d'une ou plusieurs identités véritables.

36. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'un même auteur dispose d'une pluralité de griffages différents correspondant à autant de polynymes, de manière exclusive ou partagée avec d'autres auteurs.

37. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le griffage inséré dans un protocole informatique ou de communication engendre le démarquage, sur ce protocole, de l'identité véritable de son auteur, soit de par son rôle fonctionnel d'interdiction de prise de connaissance, soit via une autorité d'anonymisation placée en intermédiaire par rapport au réceptionnaire.

38. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'autorité d'anonymisation, assistée ou supplée par le dispositif à serrure, transmet ou non la correspondance entre tel cryptonyme, tel pseudonyme ou telle entité référencée sous un polynyme, et d'autre part des informations comportementales, situationnelles ou se rapportant au passé ou au profil de cet auteur, aux fins de le caractériser sans nécessairement transmettre ni son identité véritable ni un autre de ses pseudonymes.

39. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'un griffage inséré dans un protocole, ou les pseudonymes ou les polynymes qui lui sont rattachés, ou des sous-parties autonomes ou composées de ces trois options, servent à marquer ou tatouer des objets, des matières ou des êtres réels, à des fins de reconnaissance, de validation de droit ou de statut, de valorisation, d'appartenance ou de dépendance, de liaison, d'identification ou d'authentification sans révéler une identité véritable.

40. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'un contenu de fichier ou de courrier, doté de capacités techniques d'interaction avec leur environnement, qui en rendent certaines composantes actives et autonomes, se met en dialogue avec son propre protocole, et fait du griffage un usage identique à celui d'un réceptionnaire extérieur.

41. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'autorité d'anonymisation ou l'auteur, attribuent, retirent et changent les griffages faisant racine de polynyme, pour opérer des permutations et redistributions au sein des registres unificateurs d'identités arbitraires.

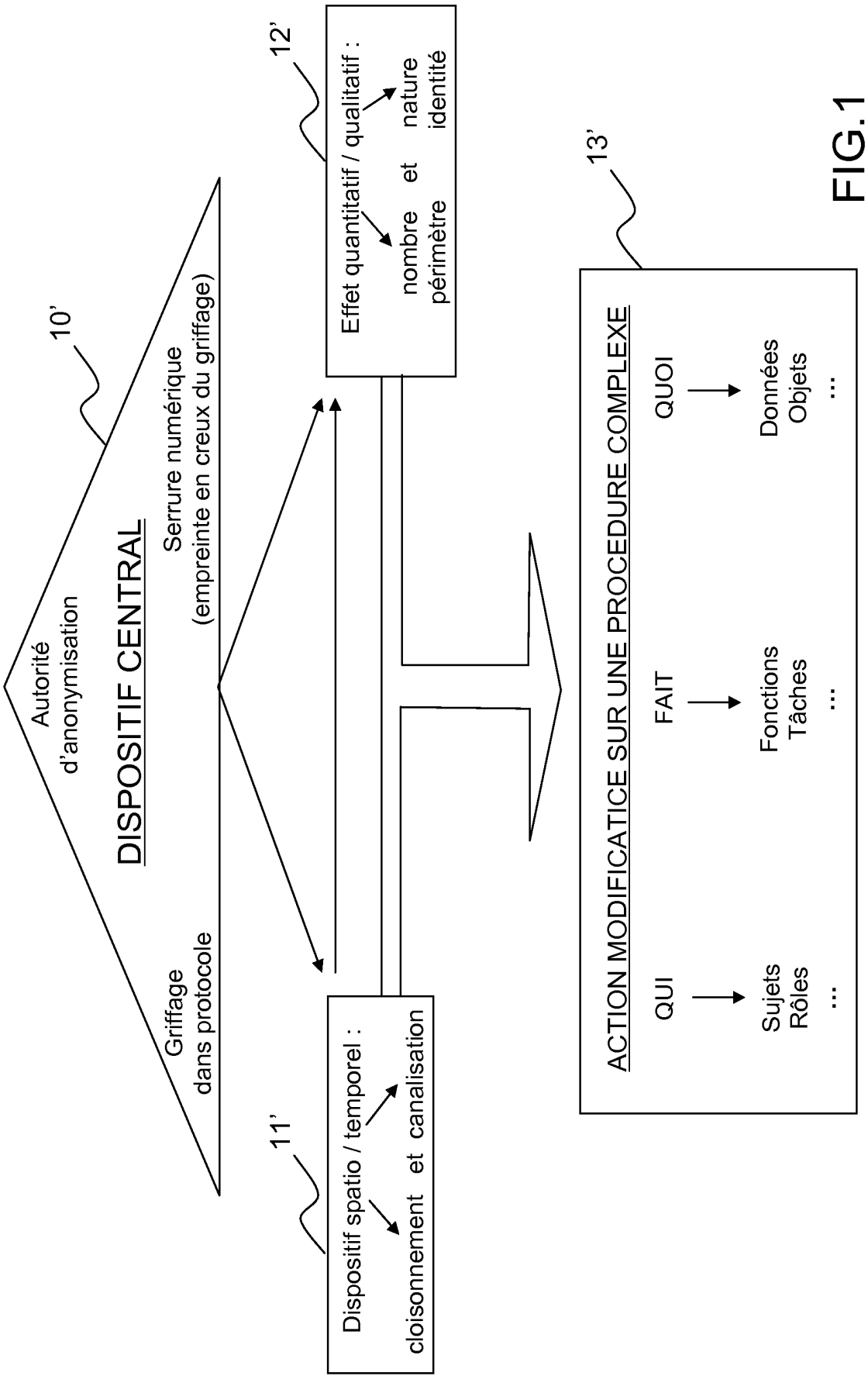

10'
DISPOSITIF CENTRAL
Autorité d'anonymisation
Serrure numérique (empreinte en creux du griffage)
Griffage dans protocole
12'
Effet quantitatif / qualitatif :
nombre et nature
périmètre identité
11'
Dispositif spatio / temporel :
cloisonnement et canalisation
13'
ACTION MODIFICATICE SUR UNE PROCEDURE COMPLEXE
QUI
Sujets
Rôles
...
FAIT
Fonctions
Tâches
...
QUOI
Données
Objets
...

FIG.1

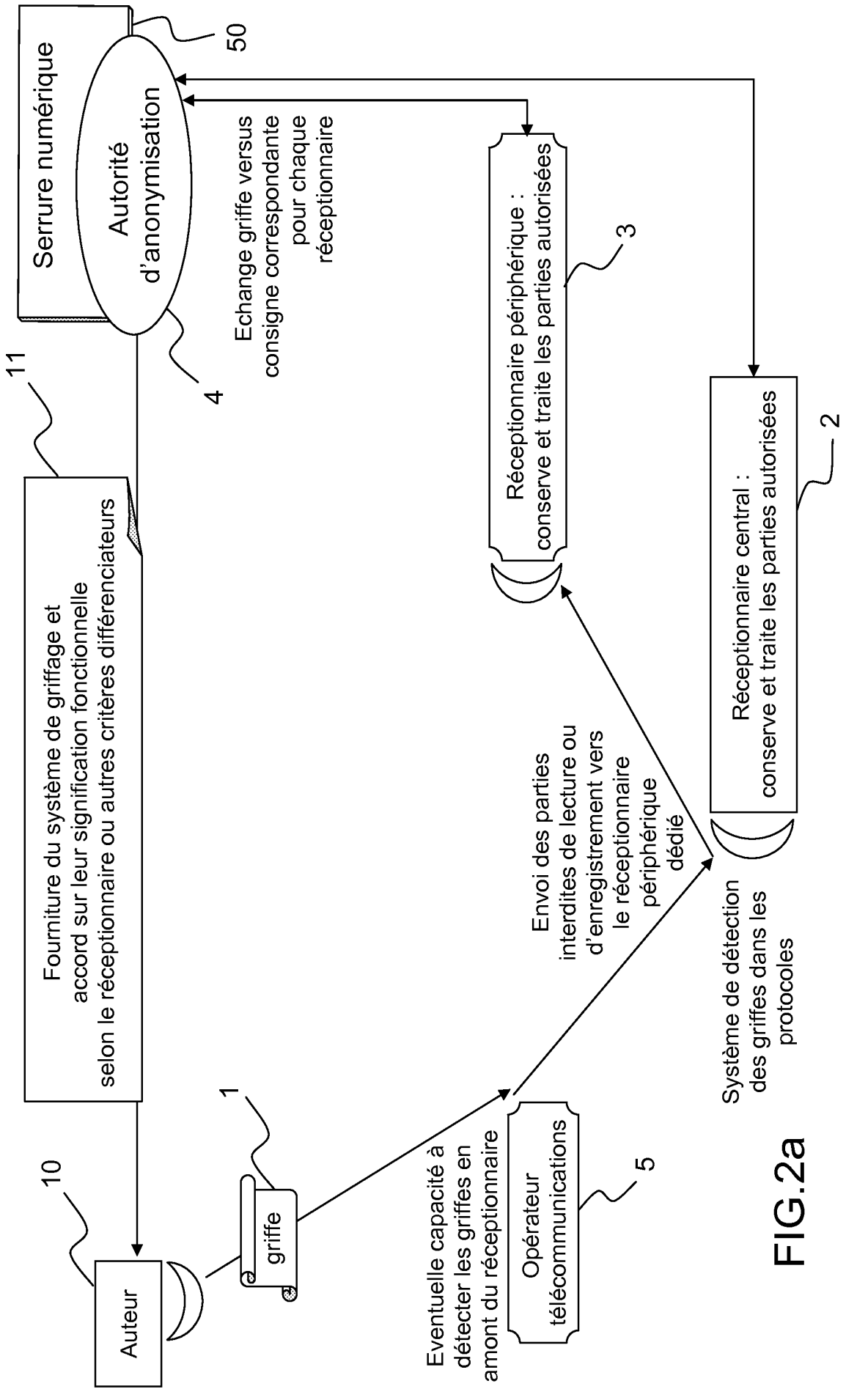

Serrure numérique
Autorité d'anonymisation
50
4
Echange griffe versus consigne correspondante pour chaque réceptionnaire
11
Fourniture du système de griffage et accord sur leur signification fonctionnelle selon le réceptionnaire ou autres critères différenciateurs
Réceptionnaire périphérique : conserve et traite les parties autorisées
3
Réceptionnaire central : conserve et traite les parties autorisées
2
10
Auteur
1
griffe
Eventuelle capacité à détecter les griffes en amont du réceptionnaire
Opérateur télécommunications
5
Envoi des parties interdites de lecture ou d'enregistrement vers le réceptionnaire périphérique dédié
Système de détection des griffes dans les protocoles

FIG.2a

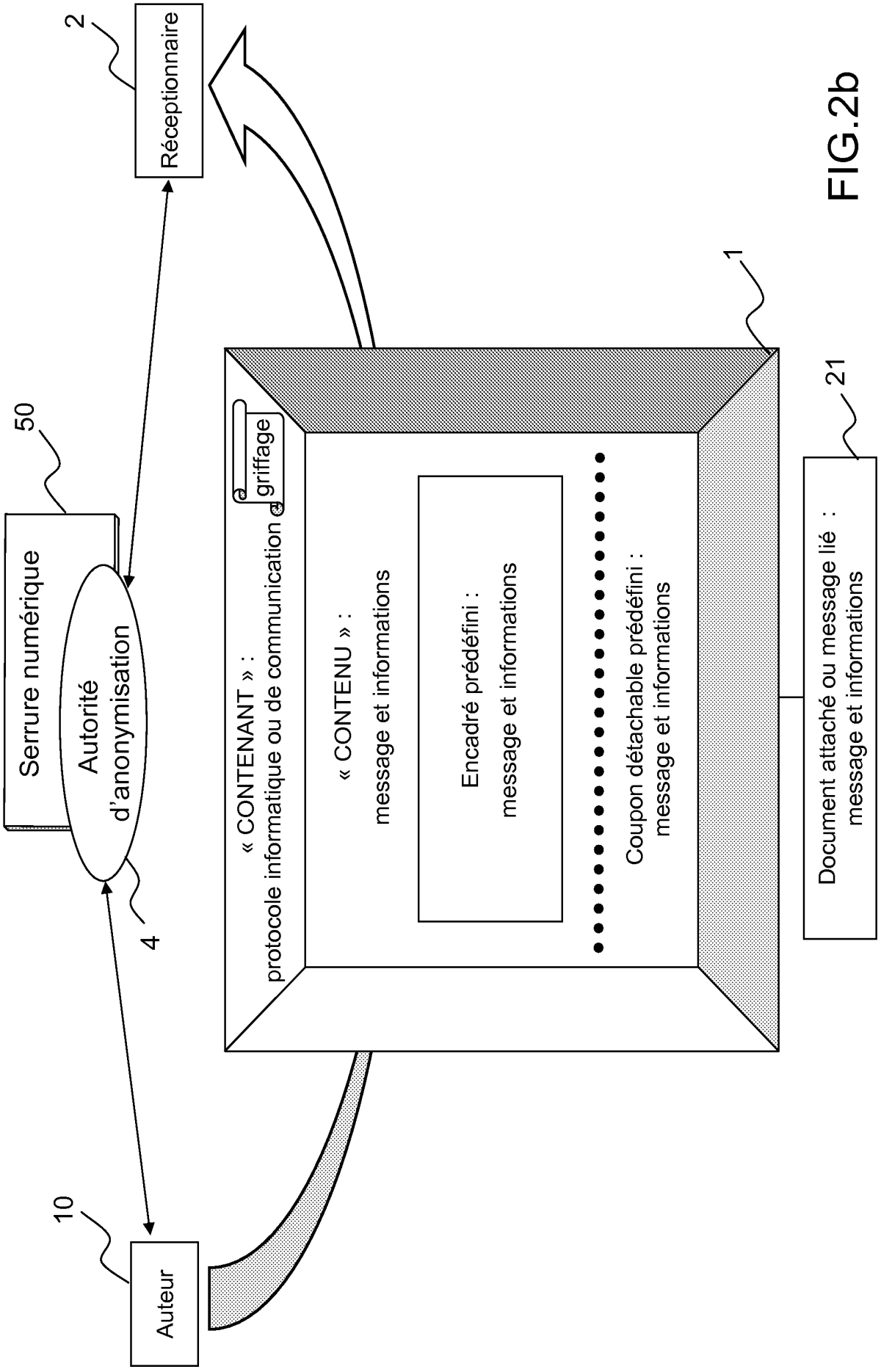

2
Réceptionnaire
50
Serrure numérique
Autorité
d'anonymisation
4
10
Auteur
1
« CONTENANT » :
protocole informatique ou de communication
griffage
« CONTENU » :
message et informations
Encadré prédéfini :
message et informations
Coupon détachable prédéfini :
message et informations
21
Document attaché ou message lié :
message et informations

FIG.2b

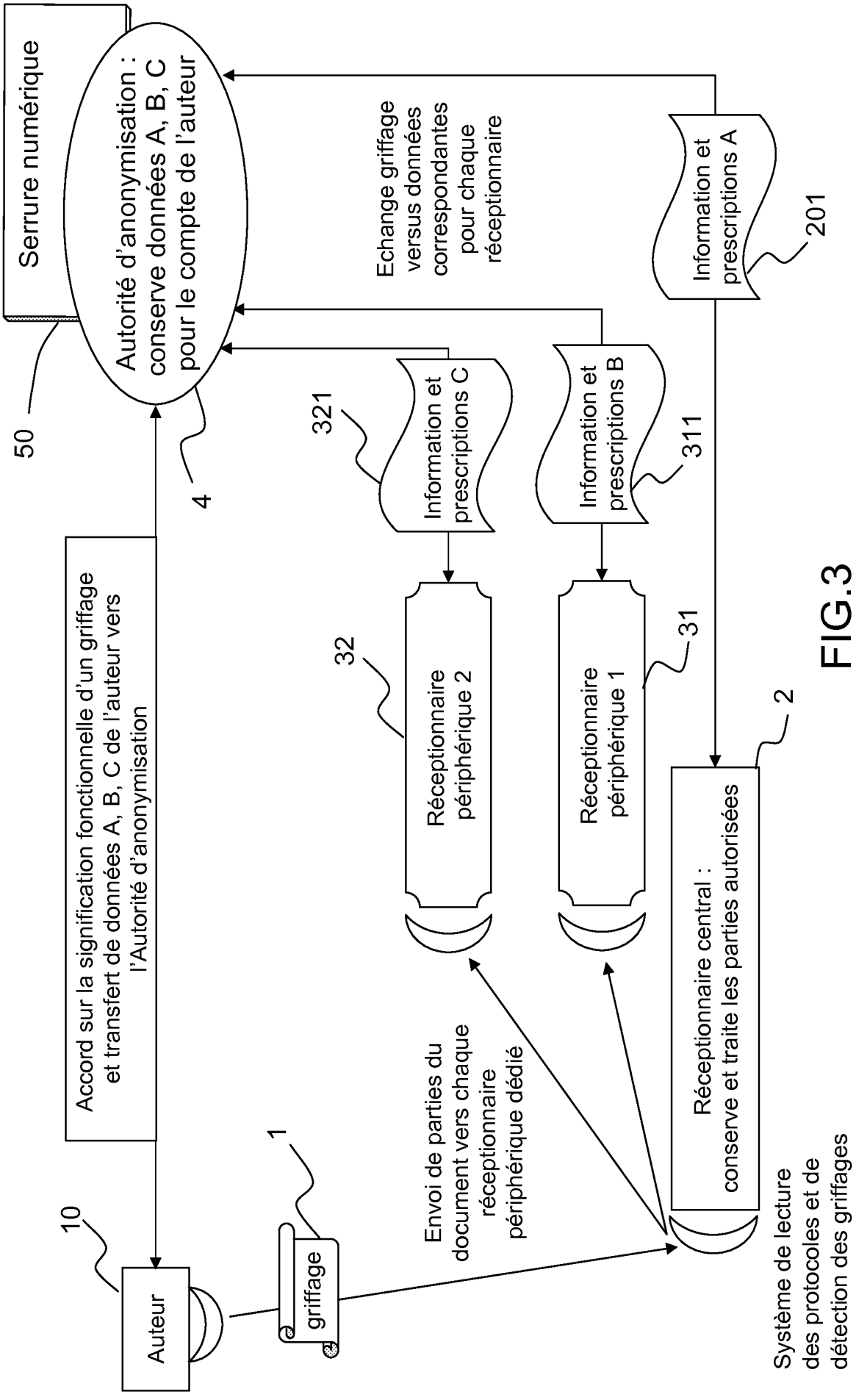

Serrure numérique
Autorité d'anonymisation : conserve données A, B, C pour le compte de l'auteur
Echange griffage versus données correspondantes pour chaque réceptionnaire
Information et prescriptions A
201
50
4
321
Information et prescriptions C
Information et prescriptions B
311
Accord sur la signification fonctionnelle d'un griffage et transfert de données A, B, C de l'auteur vers l'Autorité d'anonymisation
32
Réceptionnaire périphérique 2
Réceptionnaire périphérique 1
31
2
10
1
Auteur
griffage
Envoi de parties du document vers chaque réceptionnaire périphérique dédié
Réceptionnaire central : conserve et traite les parties autorisées
Système de lecture des protocoles et de détection des griffages

FIG.3

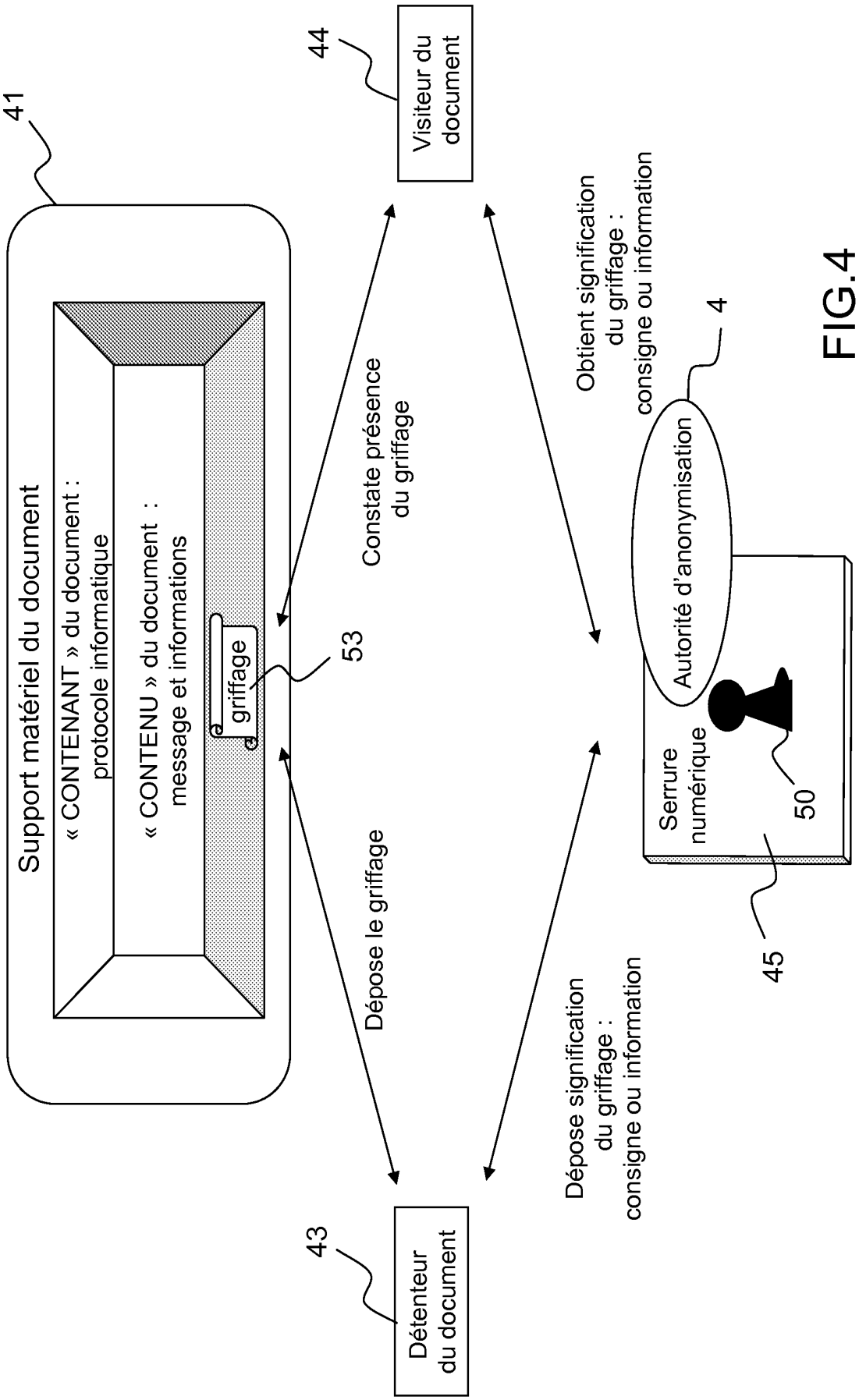

41
Support matériel du document
« CONTENANT » du document : protocole informatique
« CONTENU » du document : message et informations
griffage
53
44
Visiteur du document
Constate présence du griffage
Dépose le griffage
43
Détenteur du document
Obtient signification du griffage : consigne ou information
Dépose signification du griffage : consigne ou information
4
Autorité d'anonymisation
Serrure numérique
50
45

FIG.4

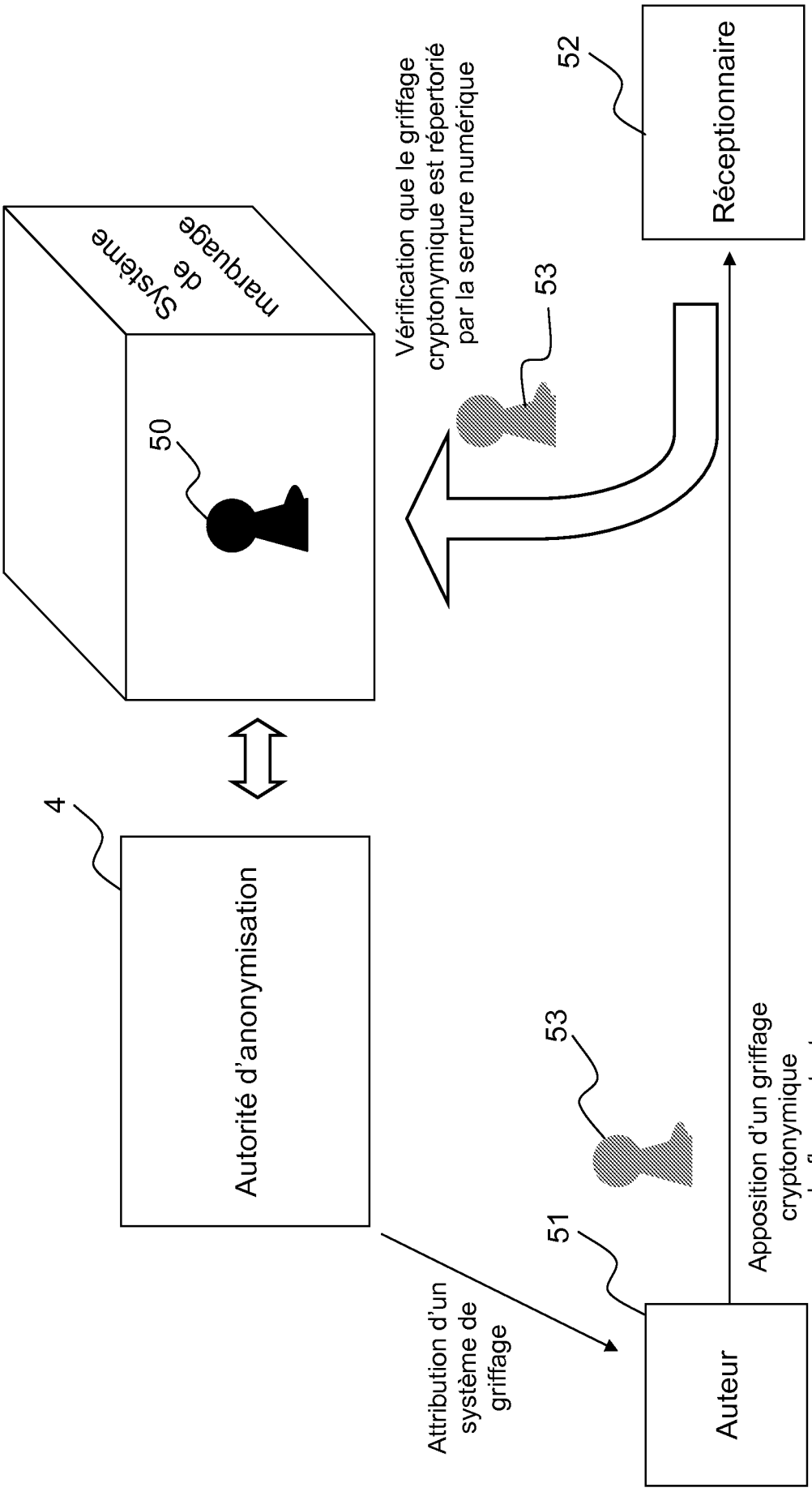

Système de marquage
50
Vérification que le griffage cryptonymique est répertorié par la serrure numérique
53
52
Réceptionnaire
4
Autorité d'anonymisation
53
51
Attribution d'un système de griffage
Apposition d'un griffage cryptonymique sur le flux sortant
Auteur

FIG.5a

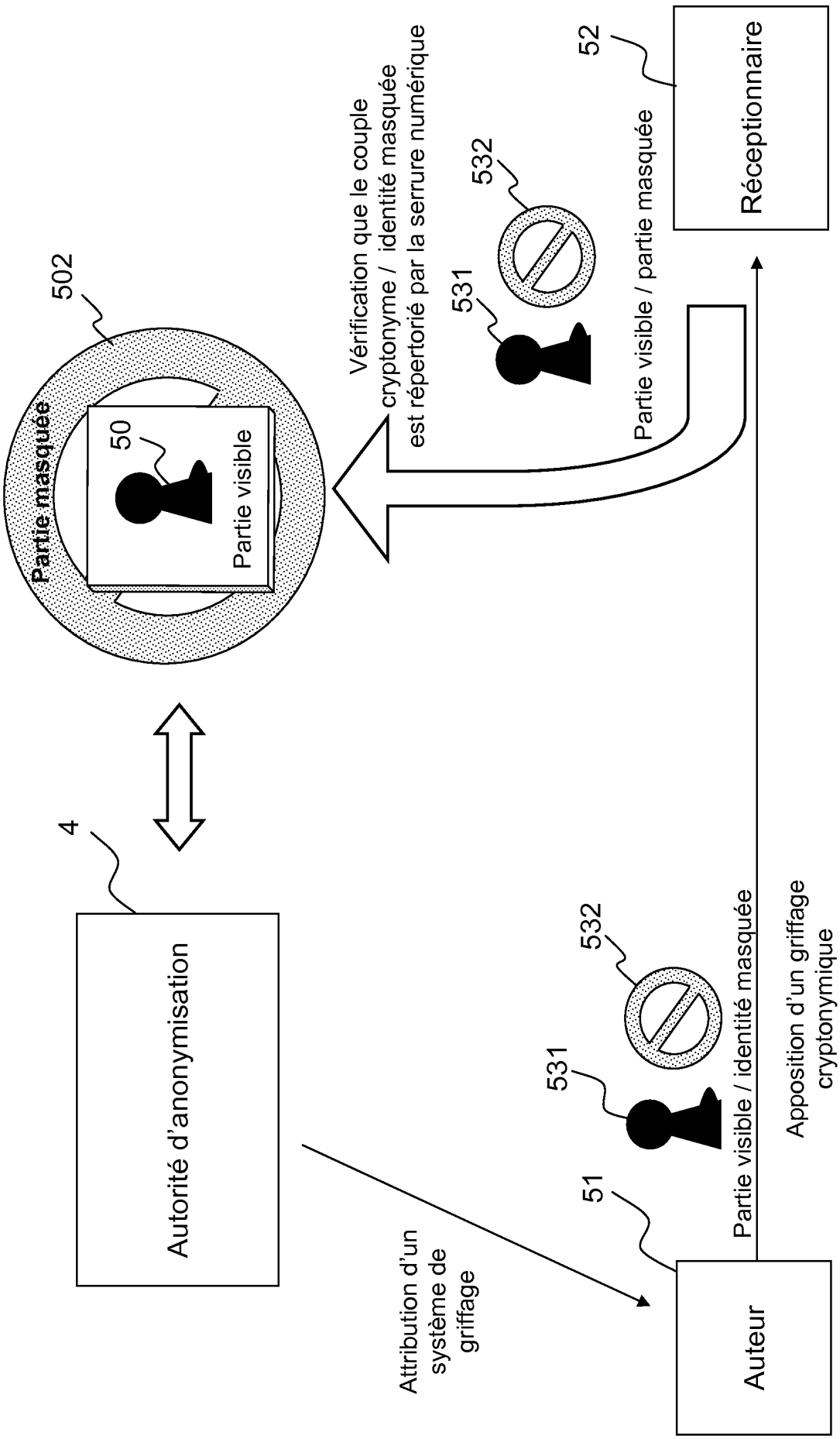

Autorité d'anonymisation
4
Attribution d'un système de griffage
Auteur
51
Apposition d'un griffage cryptonymique fonctionnellement masquant de l'identité de communication
Partie visible / identité masquée
531
532
Réceptionnaire
52
Partie visible / partie masquée
Vérification que le couple cryptonyme / identité masquée est répertorié par la serrure numérique
Partie masquée
Partie visible
50
502

FIG.5b

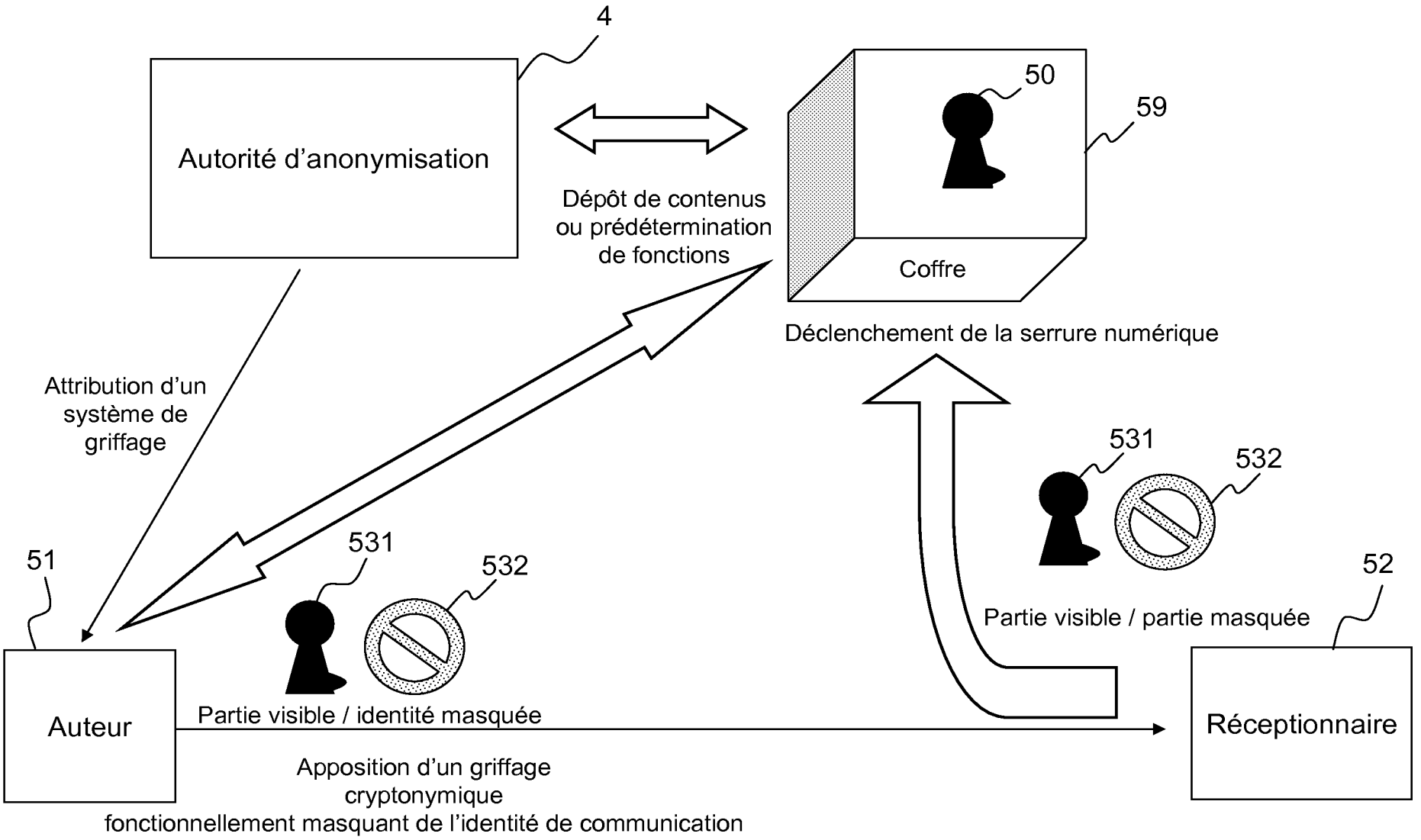

4
Autorité d'anonymisation
Dépôt de contenus
ou prédétermination
de fonctions
50
59
Coffre
Déclenchement de la serrure numérique
Attribution d'un
système de
griffage
531
532
51
531
532
52
Partie visible / partie masquée
Auteur
Partie visible / identité masquée
Réceptionnaire
Apposition d'un griffage
cryptonymique
fonctionnellement masquant de l'identité de communication

FIG.5c

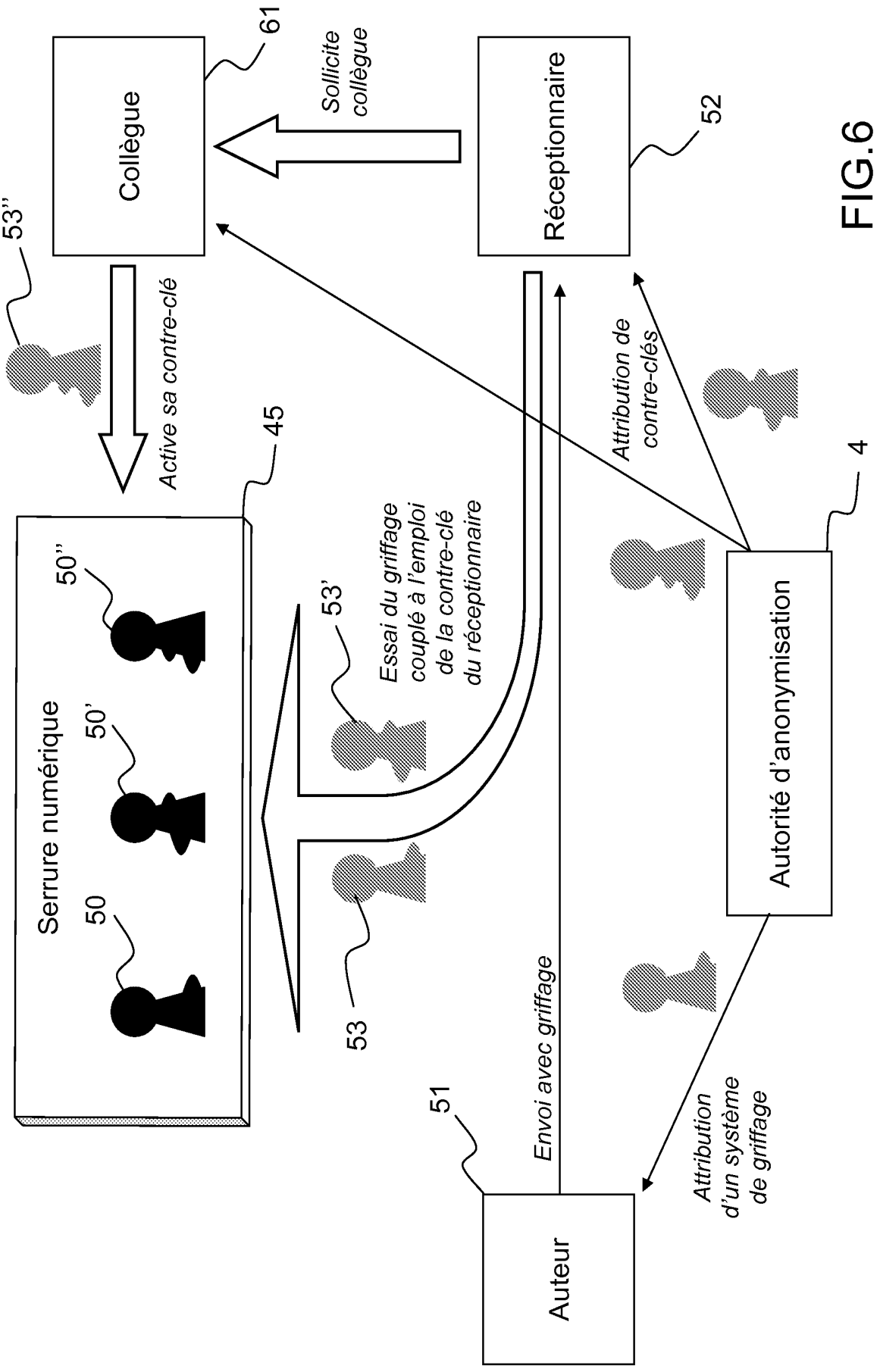

Collègue
61
Sollicite collègue
Réceptionnaire
52
53''
Active sa contre-clé
45
Serrure numérique
50''
50'
50
53'
Essai du griffage couplé à l'emploi de la contre-clé du réceptionnaire
53
Attribution de contre-clés
4
Autorité d'anonymisation
Envoi avec griffage
51
Auteur
Attribution d'un système de griffage

FIG.6

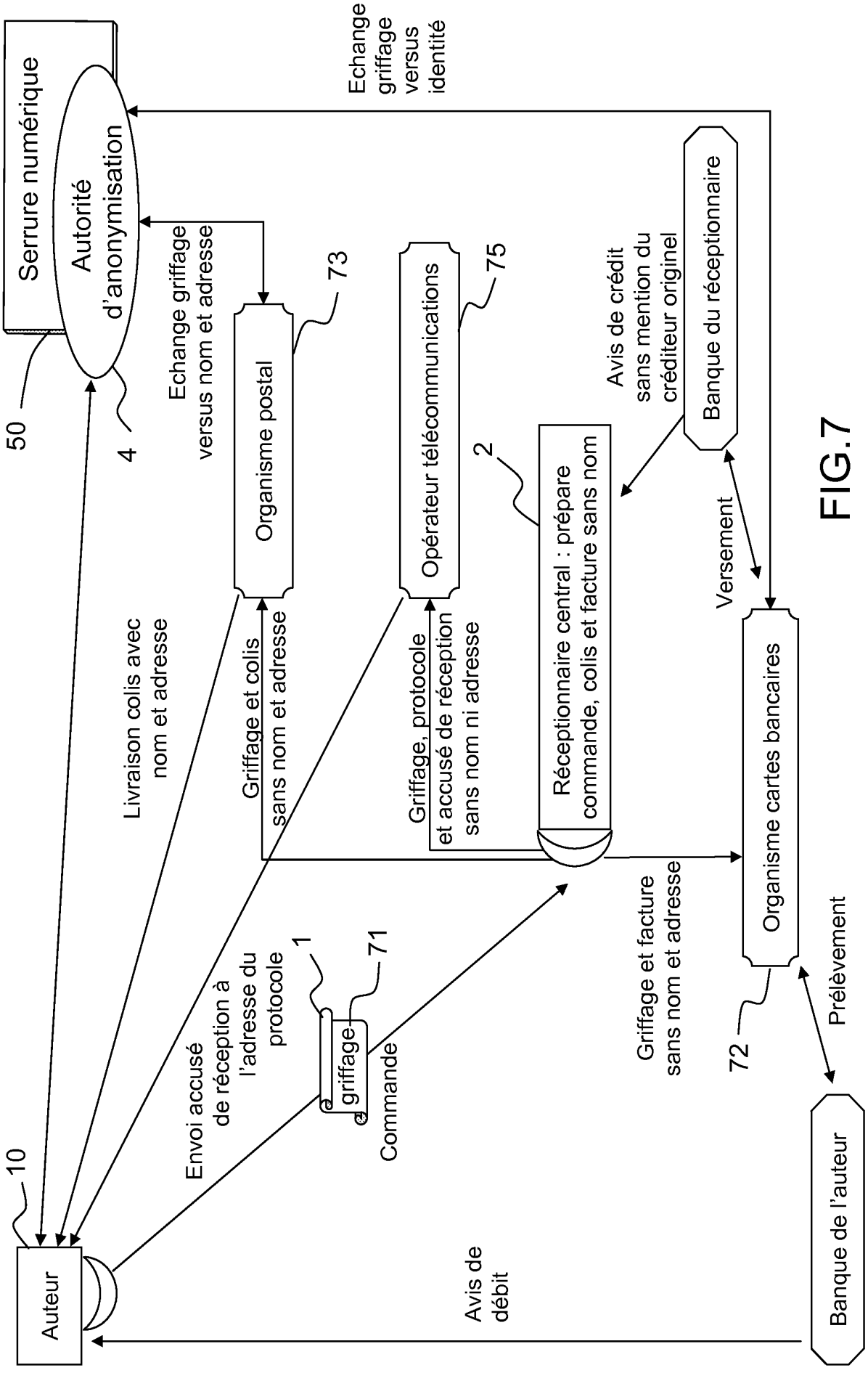

Serrure numérique
Autorité d'anonymisation
50
4
Echange griffage versus identité
Echange griffage versus nom et adresse
Organisme postal
73
Opérateur télécommunications
75
2
Avis de crédit sans mention du créditeur originel
Banque du réceptionnaire
Versement
Livraison colis avec nom et adresse
Griffage et colis sans nom et adresse
Griffage, protocole et accusé de réception sans nom ni adresse
Réceptionnaire central : prépare commande, colis et facture sans nom
Organisme cartes bancaires
Griffage et facture sans nom et adresse
72
Prélèvement
Banque de l'auteur
Avis de débit
Auteur
10
Envoi accusé de réception à l'adresse du protocole
1
griffage
71
Commande

FIG.7

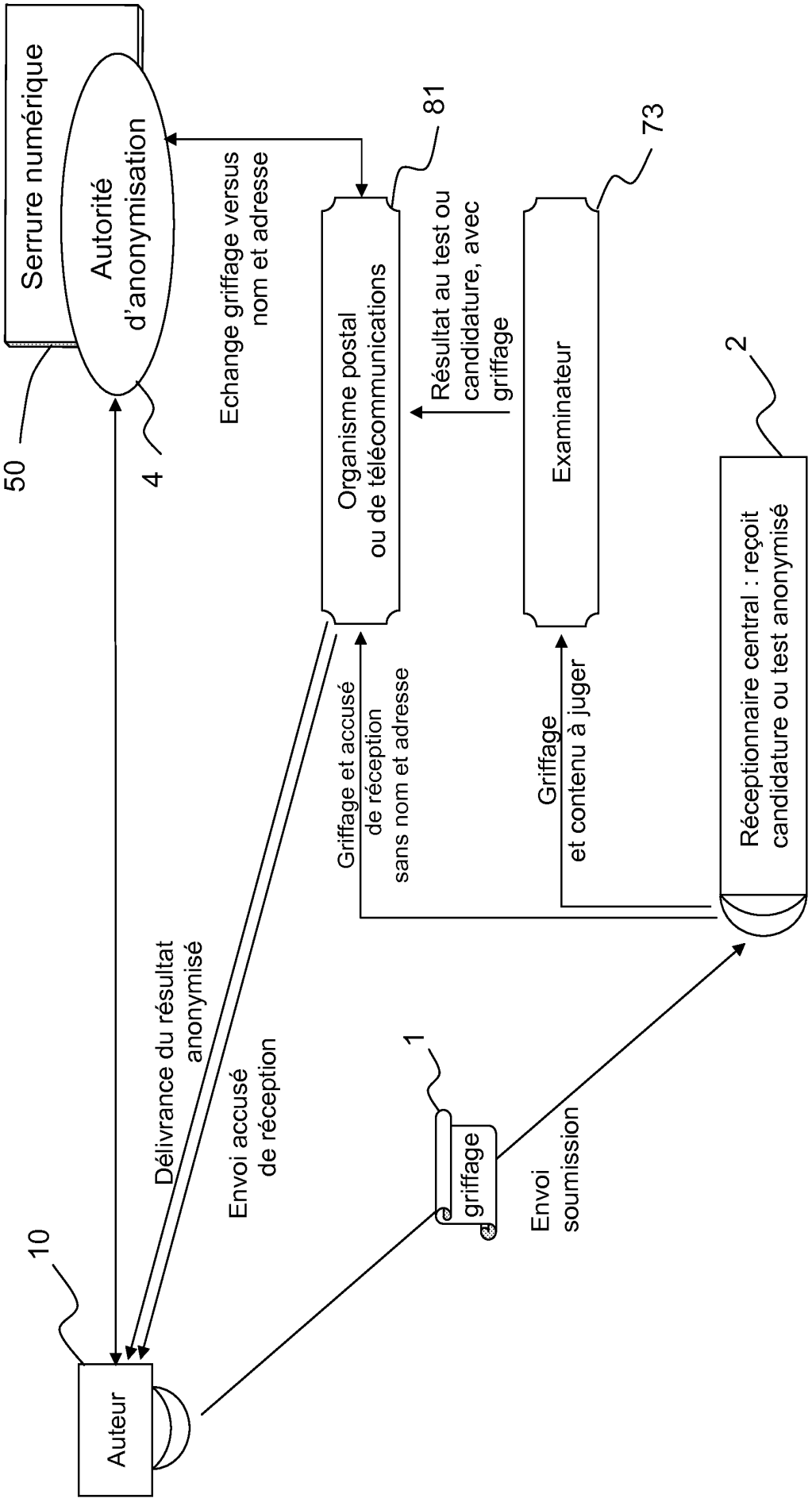

Serrure numérique
Autorité d'anonymisation
50
4
Echange griffage versus nom et adresse
Organisme postal ou de télécommunications
81
Résultat au test ou candidature, avec griffage
Examinateur
73
2
Réceptionnaire central : reçoit candidature ou test anonymisé
Griffage et accusé de réception sans nom et adresse
Griffage et contenu à juger
Délivrance du résultat anonymisé
Envoi accusé de réception
1
griffage
Envoi soumission
10
Auteur

FIG.8

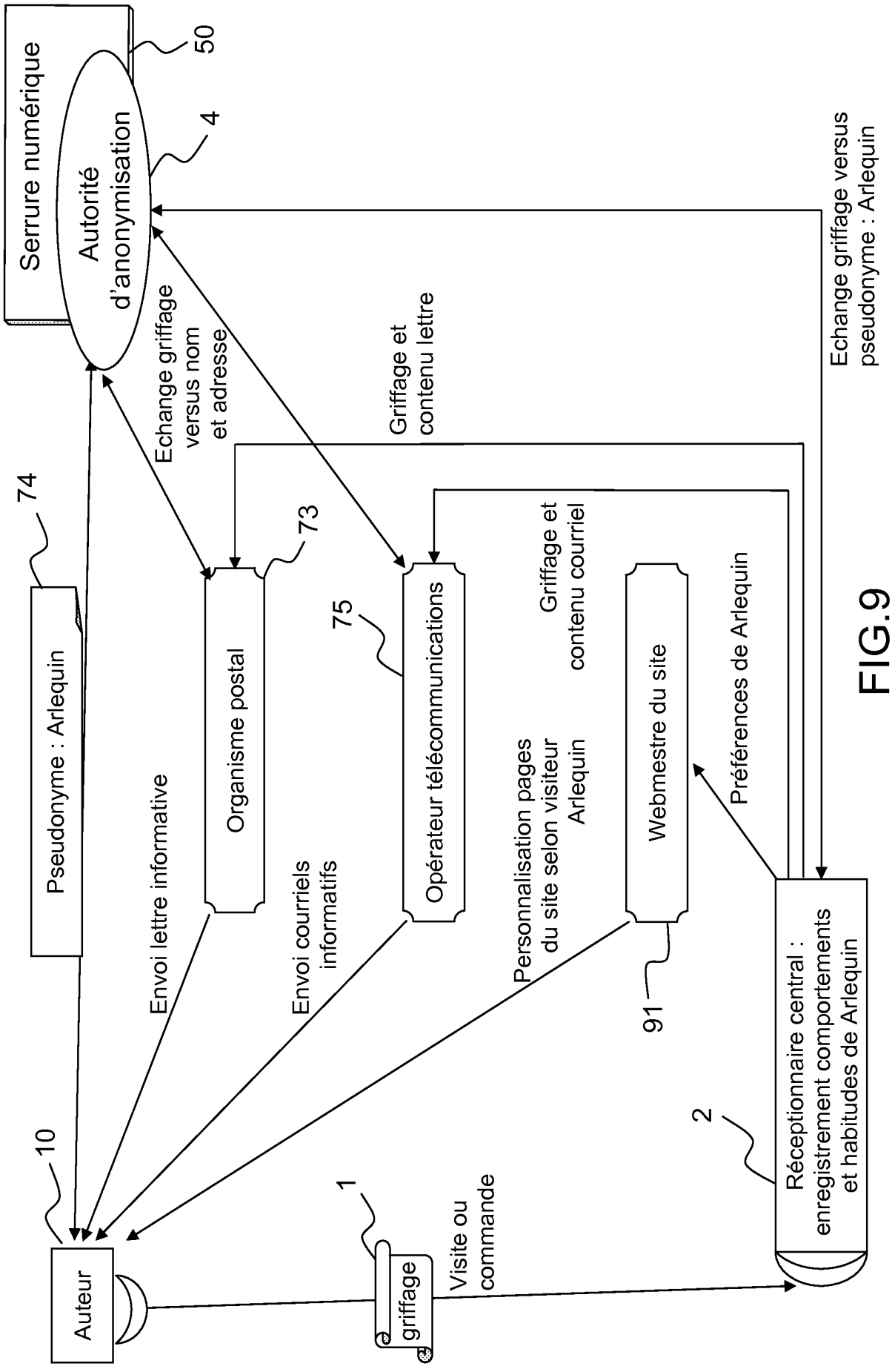

Serrure numérique
Autorité d'anonymisation
50
4
Echange griffage versus nom et adresse
Griffage et contenu lettre
Echange griffage versus pseudonyme : Arlequin
74
Pseudonyme : Arlequin
73
Organisme postal
75
Opérateur télécommunications
Webmestre du site
Envoi lettre informative
Envoi courriels informatifs
Personnalisation pages du site selon visiteur Arlequin
Griffage et contenu courriel
Préférences de Arlequin
91
10
Auteur
1
griffage
Visite ou commande
2
Réceptionnaire central : enregistrement comportements et habitudes de Arlequin

FIG.9

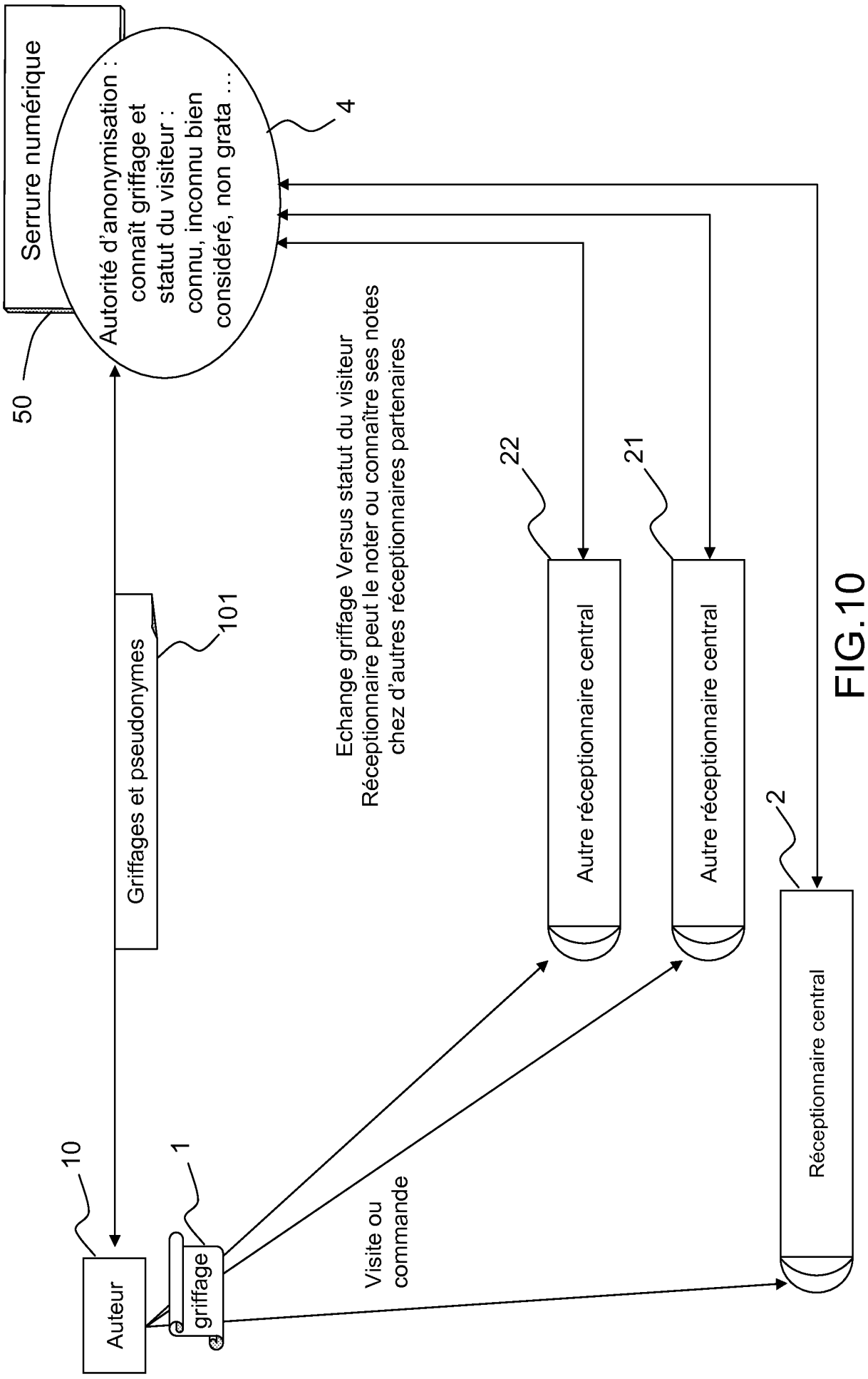

Serrure numérique
Autorité d'anonymisation : connaît griffage et statut du visiteur : connu, inconnu bien considéré, non grata ...
4
50
Griffages et pseudonymes
101
Echange griffage Versus statut du visiteur
Réceptionnaire peut le noter ou connaître ses notes chez d'autres réceptionnaires partenaires
22
21
Autre réceptionnaire central
Autre réceptionnaire central
2
Réceptionnaire central
10
1
Auteur
griffage
Visite ou commande

FIG.10

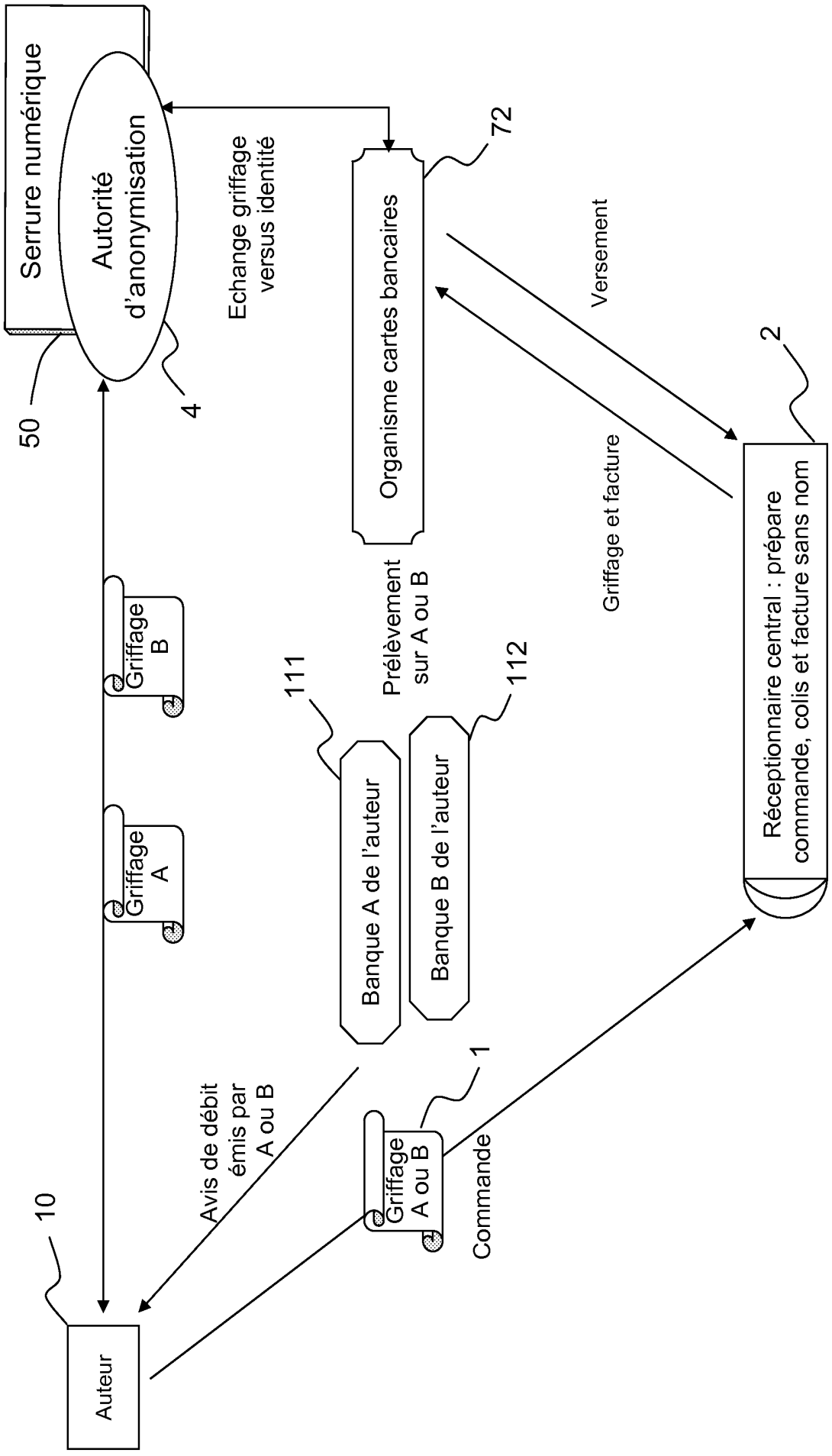

Serrure numérique
Autorité d'anonymisation
50
4
Echange griffage versus identité
Organisme cartes bancaires
72
Versement
Griffage et facture
2
Réceptionnaire central : prépare commande, colis et facture sans nom
Griffage B
Griffage A
Prélèvement sur A ou B
111
112
Banque A de l'auteur
Banque B de l'auteur
Avis de débit émis par A ou B
Griffage A ou B
1
Commande
10
Auteur

FIG.11

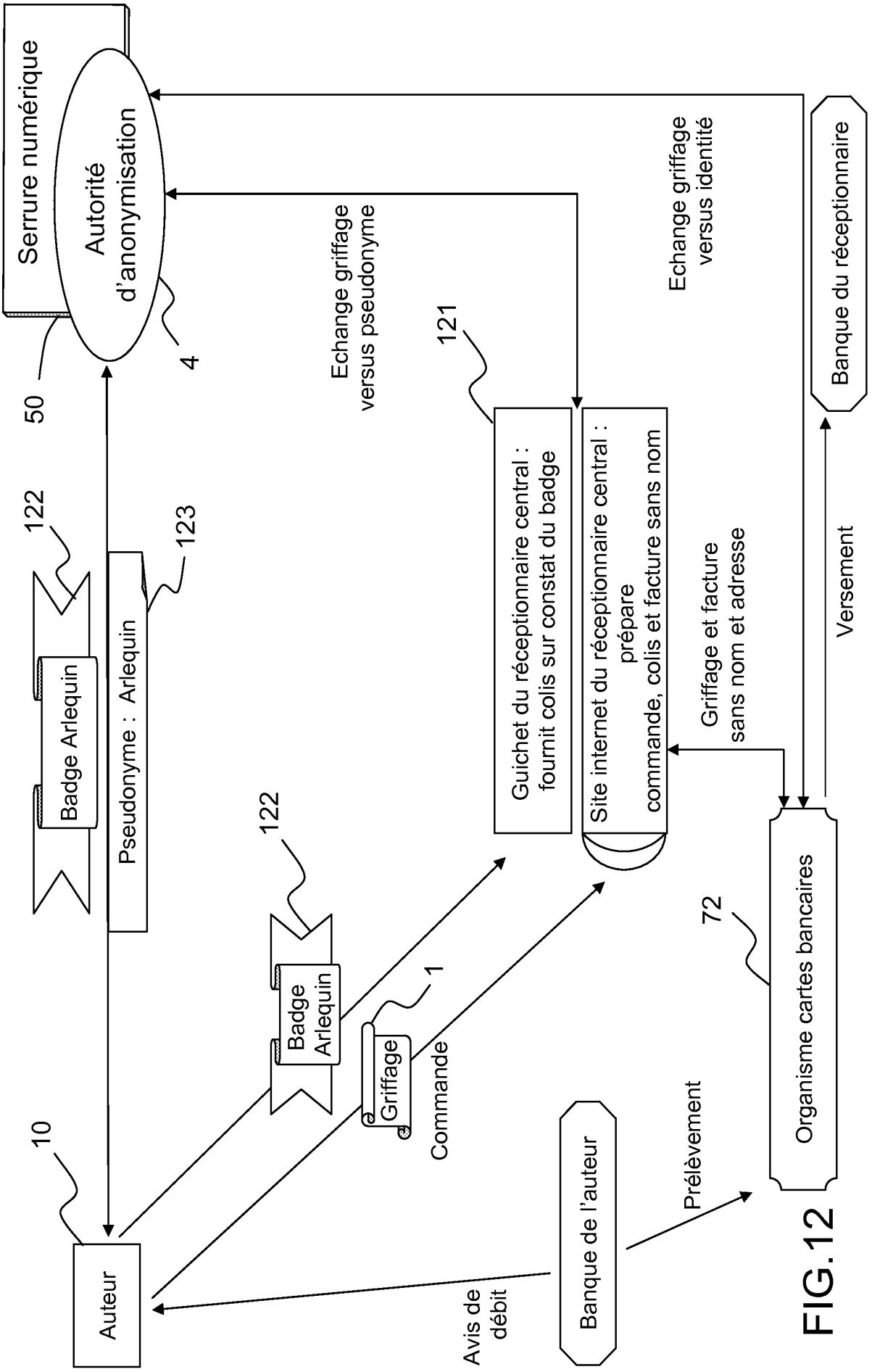

Serrure numérique
Autorité d'anonymisation
50
4
Echange griffage versus pseudonyme
Echange griffage versus identité
Banque du réceptionnaire
121
Guichet du réceptionnaire central : fournit colis sur constat du badge
Site internet du réceptionnaire central : prépare commande, colis et facture sans nom
Griffage et facture sans nom et adresse
Versement
122
Badge Arlequin
123
Pseudonyme : Arlequin
122
Badge Arlequin
1
Griffage
Commande
10
Auteur
Avis de débit
Banque de l'auteur
Prélèvement
72
Organisme cartes bancaires

FIG.12

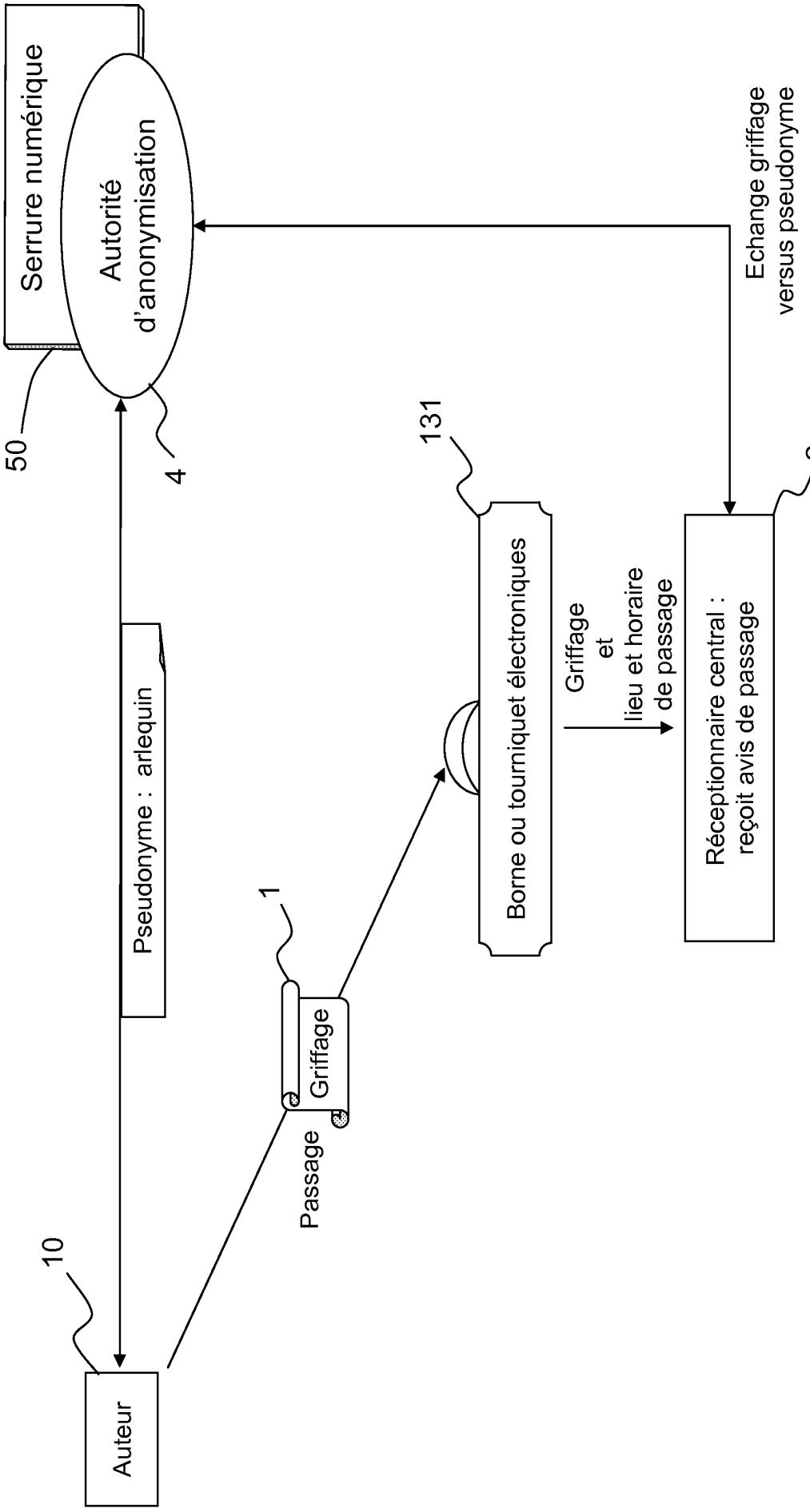

Serrure numérique
Autorité d'anonymisation
50
4
Echange griffage versus pseudonyme
131
2
Pseudonyme : arlequin
Borne ou tourniquet électroniques
Griffage et lieu et horaire de passage
Réceptionnaire central : reçoit avis de passage
1
Griffage
Passage
10
Auteur

FIG.13

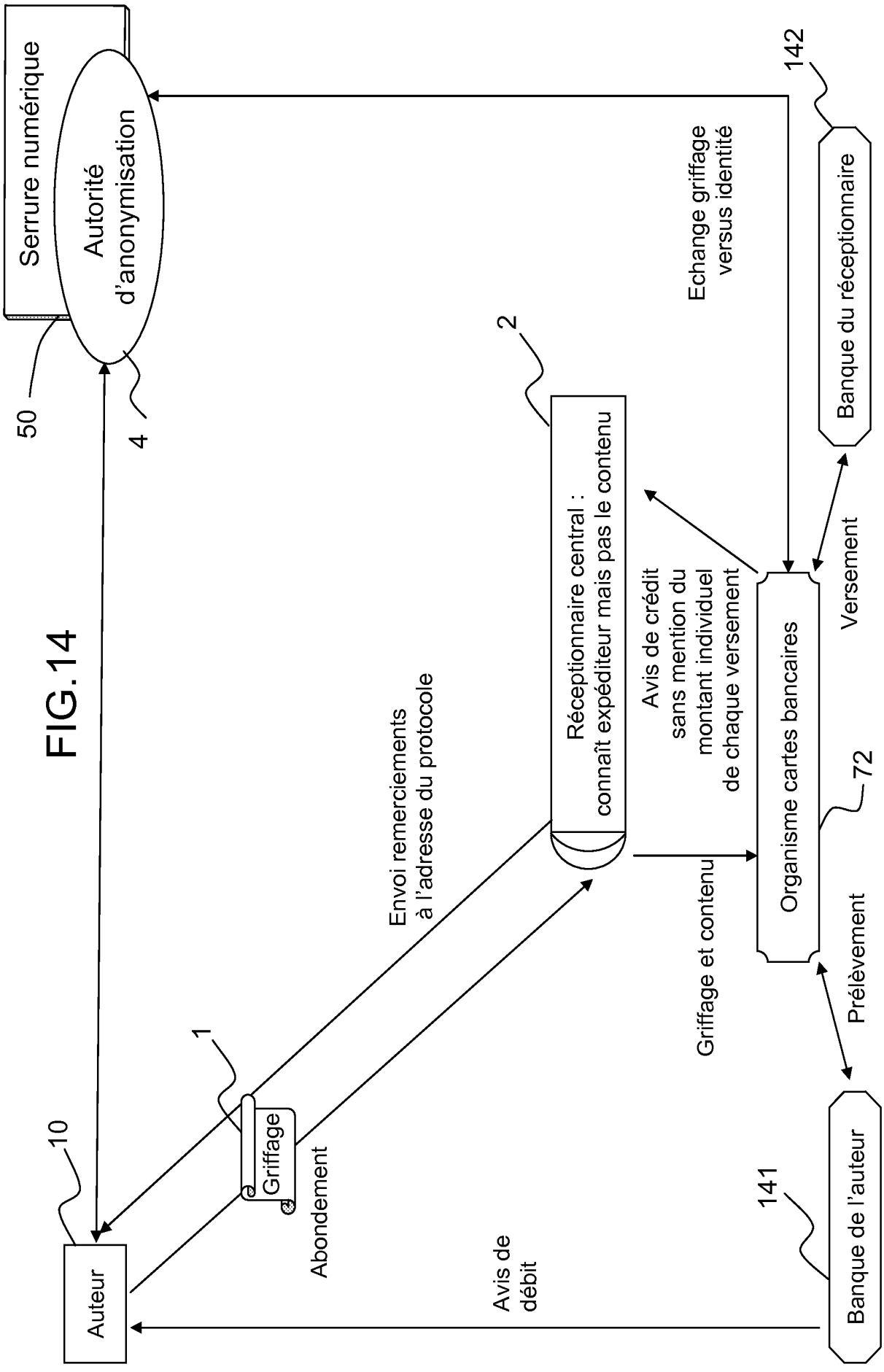

Serrure numérique
Autorité d'anonymisation
50
4
2
142
Banque du réceptionnaire
Echange griffage versus identité
Réceptionnaire central : connaît expéditeur mais pas le contenu
Avis de crédit sans mention du montant individuel de chaque versement
Versement
Envoi remerciements à l'adresse du protocole
Organisme cartes bancaires
72
Griffage et contenu
Prélèvement
1
Griffage
Abondement
10
Auteur
Avis de débit
141
Banque de l'auteur

FIG.14

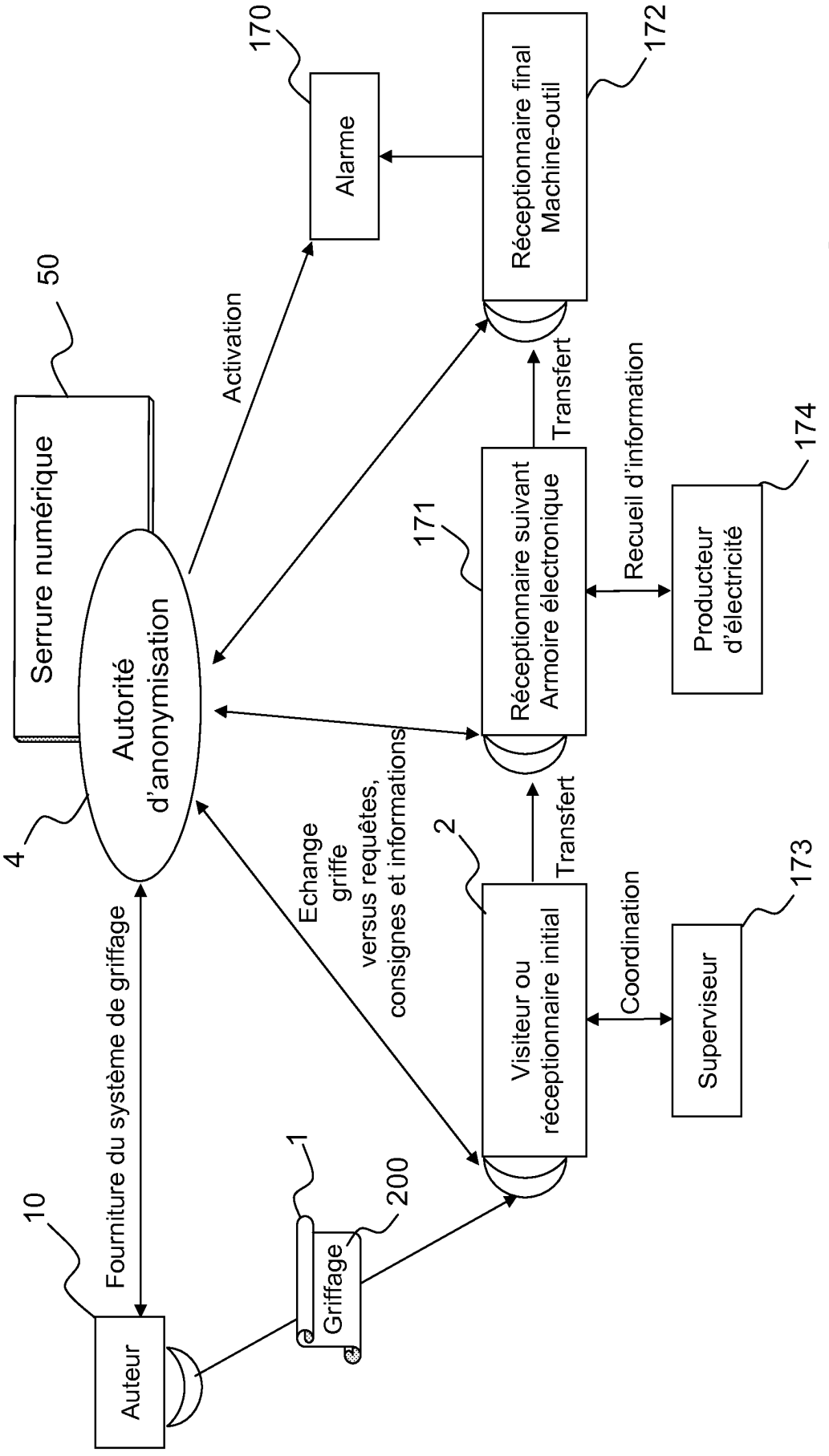

Auteur
Griffage
Serrure numérique
Autorité d'anonymisation
Alarme
Réceptionnaire final Machine-outil
Réceptionnaire suivant Armoire électronique
Visiteur ou réceptionnaire initial
Superviseur
Producteur d'électricité
Fourniture du système de griffage
Activation
Transfert
Transfert
Recueil d'information
Coordination
Echange griffe versus requêtes, consignes et informations
10
1
200
50
4
170
172
171
174
2
173

FIG.15a

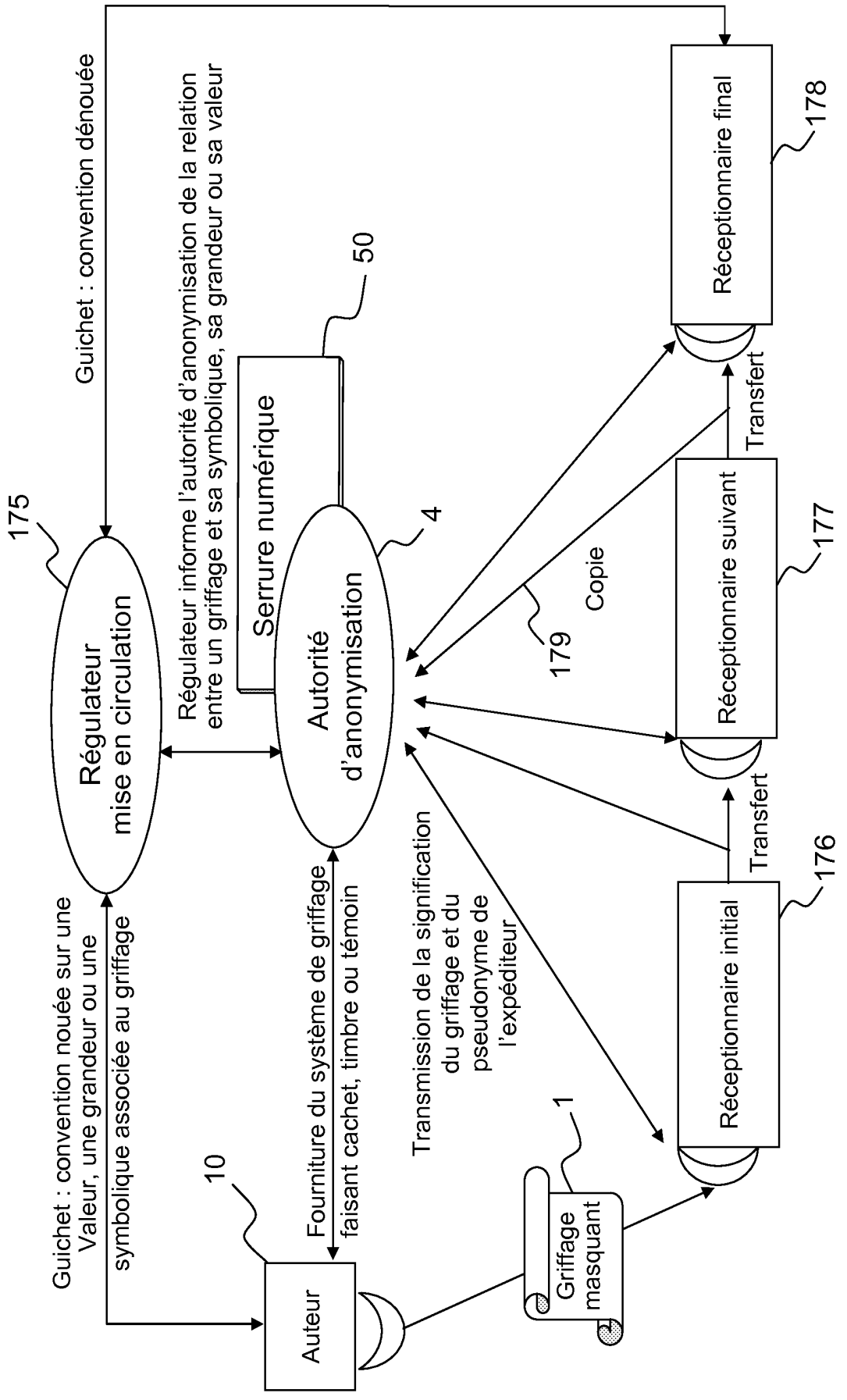

Guichet : convention dénouée
Régulateur informe l'autorité d'anonymisation de la relation entre un griffage et sa symbolique, sa grandeur ou sa valeur
Serrure numérique
50
175
Régulateur mise en circulation
Autorité d'anonymisation
4
Réceptionnaire final
178
Réceptionnaire suivant
177
Réceptionnaire initial
176
Transfert
Transfert
Copie
179
Guichet : convention nouée sur une Valeur, une grandeur ou une symbolique associée au griffage
Fourniture du système de griffage faisant cachet, timbre ou témoin
Transmission de la signification du griffage et du pseudonyme de l'expéditeur
10
Auteur
1
Griffage masquant

FIG.15b

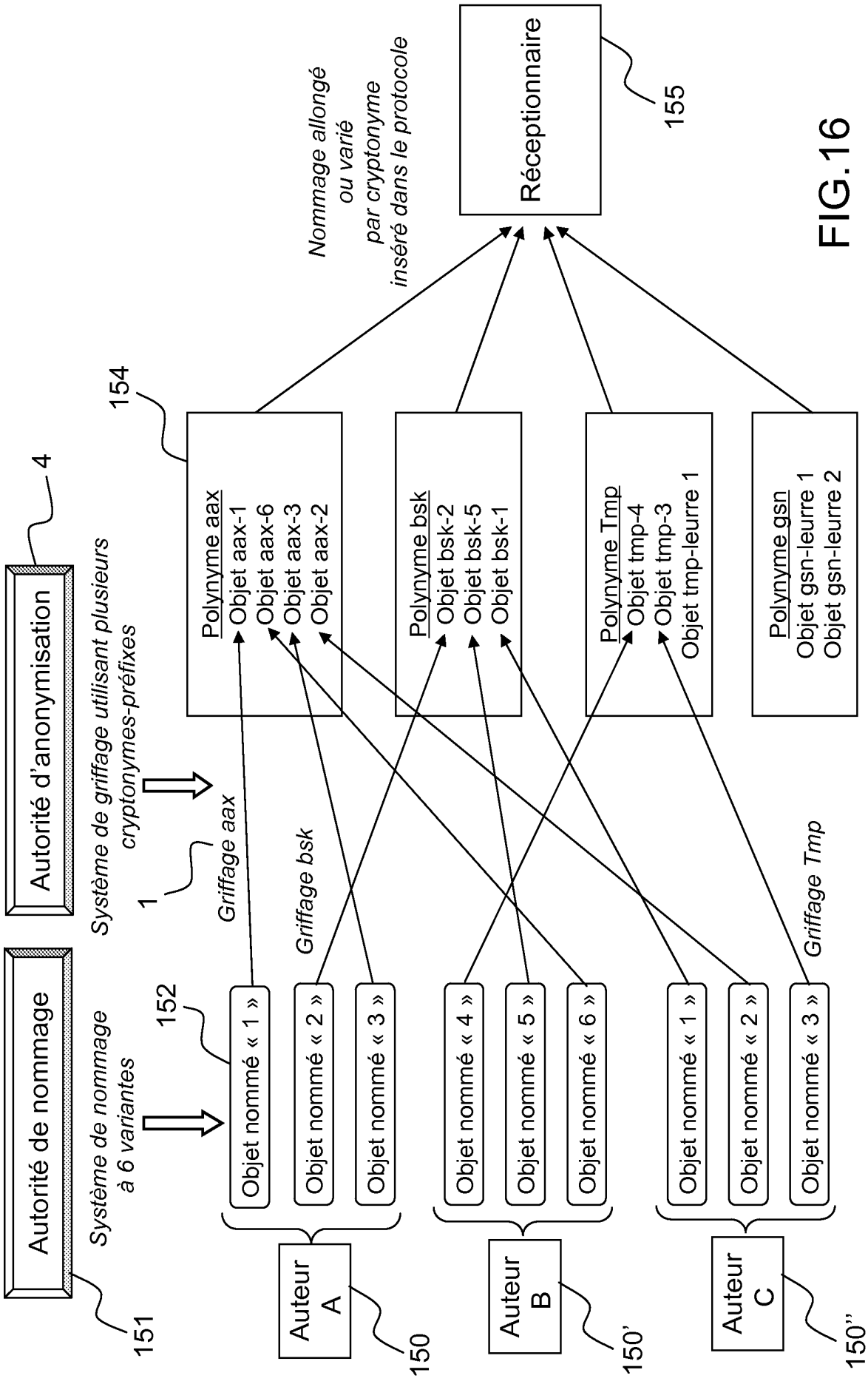

Autorité de nommage
Autorité d'anonymisation
4
Système de nommage à 6 variantes
151
Système de griffage utilisant plusieurs cryptonymes-préfixes
1
Griffage aax
Griffage bsk
Griffage Tmp
152
Objet nommé « 1 »
Objet nommé « 2 »
Objet nommé « 3 »
Objet nommé « 4 »
Objet nommé « 5 »
Objet nommé « 6 »
Objet nommé « 1 »
Objet nommé « 2 »
Objet nommé « 3 »
Auteur A
150
Auteur B
150'
Auteur C
150''
154
Polynyme aax
Objet aax-1
Objet aax-6
Objet aax-3
Objet aax-2
Polynyme bsk
Objet bsk-2
Objet bsk-5
Objet bsk-1
Polynyme Tmp
Objet tmp-4
Objet tmp-3
Objet tmp-leurre 1
Polynyme gsn
Objet gsn-leurre 1
Objet gsn-leurre 2
Nommage allongé ou varié par cryptonyme inséré dans le protocole
Réceptionnaire
155

FIG.16

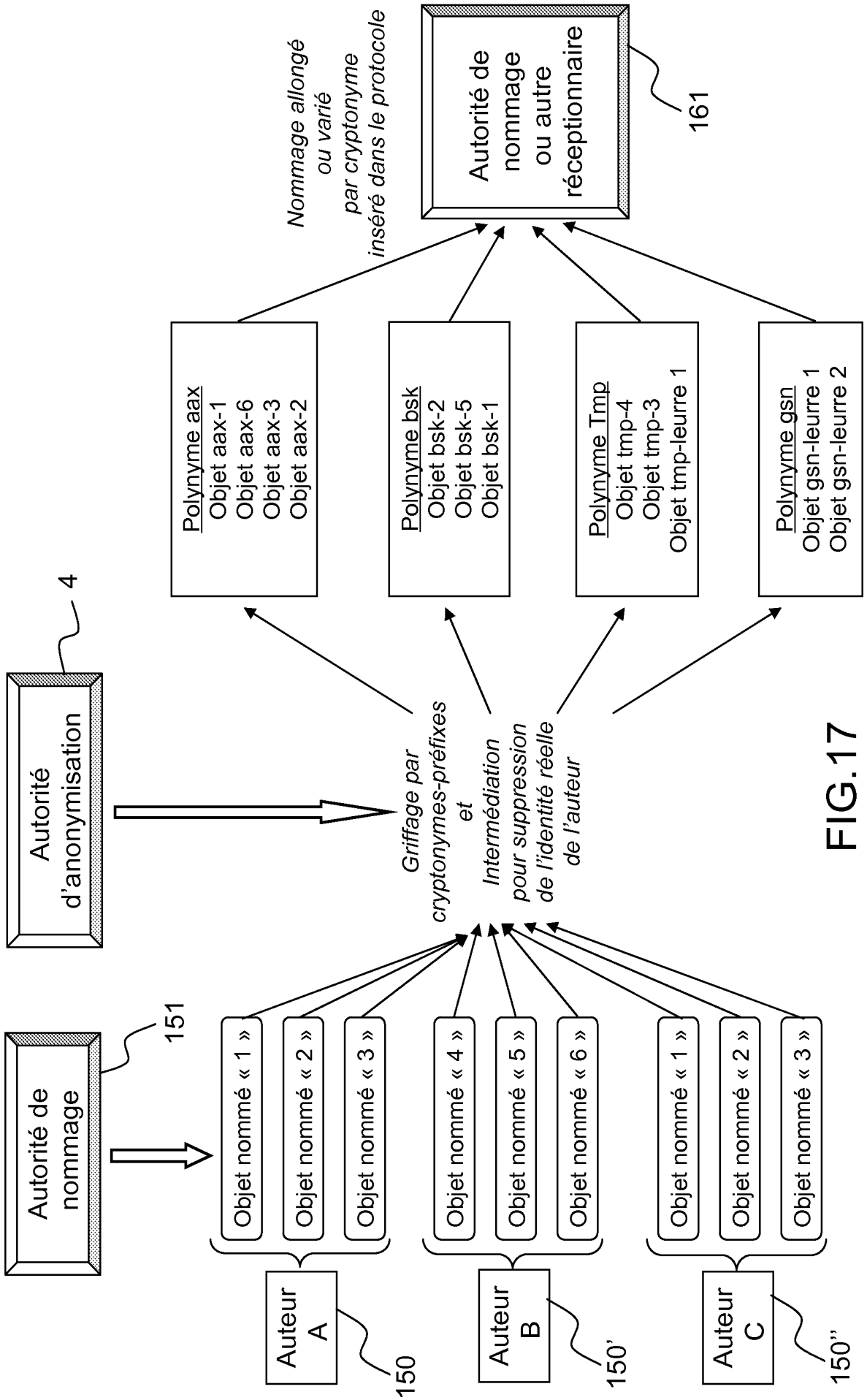

Autorité de nommage
151
Autorité d'anonymisation
4
Auteur A
150
Auteur B
150'
Auteur C
150''
Objet nommé « 1 »
Objet nommé « 2 »
Objet nommé « 3 »
Objet nommé « 4 »
Objet nommé « 5 »
Objet nommé « 6 »
Objet nommé « 1 »
Objet nommé « 2 »
Objet nommé « 3 »
Griffage par cryptonymes-préfixes et Intermédiation pour suppression de l'identité réelle de l'auteur
Polynyme aax
Objet aax-1
Objet aax-6
Objet aax-3
Objet aax-2
Polynyme bsk
Objet bsk-2
Objet bsk-5
Objet bsk-1
Polynyme Tmp
Objet tmp-4
Objet tmp-3
Objet tmp-leurre 1
Polynyme gsn
Objet gsn-leurre 1
Objet gsn-leurre 2
Nommage allongé ou varié par cryptonyme inséré dans le protocole
Autorité de nommage ou autre réceptionnaire
161

FIG.17

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 741095
FR 1054272

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X,D	WO 2009/147163 A1 (GROUPE ECOLES TELECOMM [FR]; RIGUIDEL MICHEL [FR]; LAURIER PHILIPPE [F) 10 décembre 2009 (2009-12-10) * page 6, ligne 4 - page 8, ligne 7 * * page 9, ligne 29 - page 10, ligne 31 * * page 13, ligne 28 - page 14, ligne 34 * * page 16, ligne 24-34 * * page 19, ligne 3 - page 24, ligne 2 * * page 27, ligne 1 - page 31, ligne 10; figures 7,8 * -----	1-41	G06F21/24 H04L9/32 H04L29/06
X	US 2009/158030 A1 (RASTI MEHRAN RANDALL [US]) 18 juin 2009 (2009-06-18) * alinéas [0009] - [0020] * * alinéa [0036] * * alinéas [0074] - [0078] * * alinéa [0101] * * alinéa [0120] * -----	1-41	
X	WO 2009/105996 A1 (HUAWEI TECH CO LTD [CN]; LIU YIJUN [CN]; GAO HONGTAO [CN]) 3 septembre 2009 (2009-09-03) * abrégé * & US 2010/229241 A1 (LIU YIJUN [CN] ET AL) 9 septembre 2010 (2010-09-09) * alinéas [0047] - [0049] * * alinéas [0082] - [0084] * * alinéas [0110] - [0117] * * alinéas [0171] - [0177] * * alinéas [0209] - [0215] * -----	1-41	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04L G06F

Date d'achèvement de la recherche	Examinateur
18 février 2011	Ruiz Sanchez, J

CATÉGORIE DES DOCUMENTS CITÉS

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

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

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1054272 FA 741095

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 18-02-2011
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2009147163 A1	10-12-2009	FR 2932043 A1	04-12-2009
US 2009158030 A1	18-06-2009	AUCUN	
WO 2009105996 A1	03-09-2009	CN 101521569 A	02-09-2009
		US 2010229241 A1	09-09-2010

EPO FORM P0465