

CONFÉDÉRATION SUISSE
INSTITUT FÉDÉRAL DE LA PROPRIÉTÉ INTELLECTUELLE

(11) CH 710 819 B1

(51) Int. Cl.: **G06Q 10/02 (2012.01)**
G06Q 50/10 (2012.01)
G07C 9/00 (2006.01)

Brevet d'invention délivré pour la Suisse et le Liechtenstein

Traité sur les brevets, du 22 décembre 1978, entre la Suisse et le Liechtenstein

(12) FASCICULE DU BREVET

(21) Numéro de la demande:	00299/15	(73) Titulaire(s): Icare Institut de recherche en informatique, Techno-pôle Sierre 3 3960 Sierre (CH)
(22) Date de dépôt:	05.03.2015	
(43) Demande publiée:	15.09.2016	(72) Inventeur(s): Nouredine Hussain, 3960 Corin-de-la-Crête (CH) Benoit Golay, 1180 Bex (CH) David Werden, 1950 Sion (CH) Laurent Sciboz, 1688 Sommentier (CH)
(24) Brevet délivré:	15.07.2019	
(45) Fascicule du brevet publié:	15.07.2019	(74) Mandataire: P&TS SA, Av. J.-J. Rousseau 4 P.O. Box 2848 2001 Neuchâtel (CH)

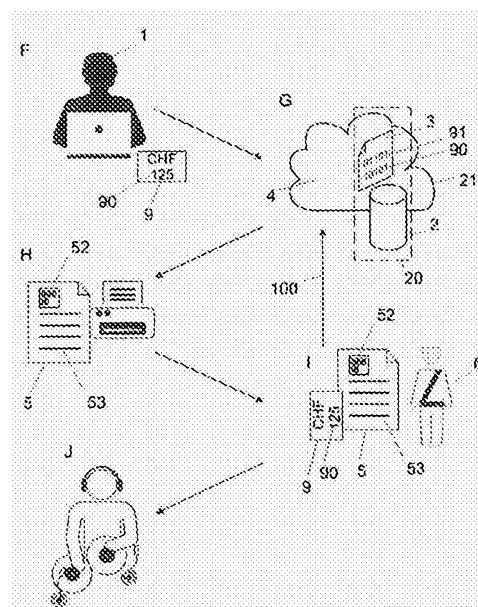
(54) **Système et procédé de contrôle d'accès à une prestation.**

(57) L'invention concerne un procédé de contrôle d'accès à une prestation comportant les étapes suivantes:

- génération au moyen d'un scanner de données correspondant à l'image d'un billet de banque (9) muni d'un numéro de série (90) unique, ledit billet de banque constituant une clé d'autorisation;
- extraction dudit numéro de série (90) à partir desdites données;
- autorisation ou refus d'une prestation en fonction dudit numéro de série.

Il est aussi possible d'extraire la devise et la coupure afin d'identifier la prestation à autoriser, et/ou de valider le numéro de série.

L'invention concerne également un système pour mettre en œuvre le procédé.



Description

Domaine technique

[0001] La présente invention concerne un procédé technique de contrôle d'accès à une prestation, par exemple un procédé de contrôle d'accès à un emplacement, un véhicule, une ressource ou un équipement.

Etat de la technique

[0002] Il existe dans l'art antérieur de nombreux systèmes techniques et informatiques pour contrôler l'accès à une prestation. Les prestations autorisées peuvent être très diverses; par exemple, des systèmes existent pour contrôler l'accès à un ordinateur, à un réseau, à un site web, à une application, à une prestation offerte par un site web ou une application, ou à un espace physique tel qu'un bâtiment, une salle ou un lieu de spectacle, etc.

[0003] Les systèmes techniques de contrôle d'accès sont souvent basés sur une identification ou une authentification de l'utilisateur. Cette identification ou authentification est typiquement donnée par une preuve de la connaissance d'un secret (par exemple un mot de passe, un code secret, un datagramme, etc.), par un contrôle biométrique et/ou par la preuve de la possession d'un élément difficile à reproduire, par exemple une signature manuscrite ou électronique, une clé, un dongle, un document difficilement répliquable, etc.

[0004] La présente invention concerne plus particulièrement cette dernière catégorie, c'est-à-dire le contrôle d'accès à la prestation à celui qui apporte la preuve de la possession d'un élément difficilement répliquable. Dans la suite de la description, un tel élément est appelé de manière générale «clé d'autorisation», quel que soit son mode de réalisation sous forme d'objet physique ou virtuel.

[0005] Une limitation dans l'utilisation de ce type d'autorisation tient à la difficulté et au coût de production de telles clés d'autorisation difficilement répliquables. Une clé d'autorisation est considérée comme difficilement répliquable si le coût de falsification dépasse la valeur de la prestation à laquelle la clé donne accès.

[0006] La fabrication de telles clés d'autorisation est généralement coûteuse et met en œuvre des technologies difficilement disponibles; si leur fabrication était simple, leur réplication le serait également. Ces difficultés de fabrication limitent cependant le nombre de prestations pour lesquelles la mise en œuvre de ces autorisations par clés est adaptée. Il n'est par exemple pas judicieux de fabriquer des clés coûteuses pour protéger l'accès à des prestations à faible valeur ajoutée. C'est en particulier le cas si les clés d'autorisation sont destinées à être utilisées une seule fois.

[0007] Dans le cas de prestations correspondant à des accès à des manifestations, par exemple des concerts, ou des véhicules, la clé d'autorisation est généralement constituée par un ticket d'entrée ou un ticket de transport. Il est difficile de sécuriser un tel ticket contre la copie ou la contrefaçon, car son coût de production doit rester bas.

[0008] Une alternative consiste à distribuer un code unique à chaque acheteur de billet, par exemple en cas d'achat sur Internet. Ce procédé est connu généralement sous le nom de «print@home» et comporte par exemple les étapes suivantes, illustrées sur la fig. 1:

- A. Un utilisateur 1 achète via le réseau Internet 21 une prestation sur un site web. Le règlement se fait par exemple avec une carte de crédit, par facture ou via une plateforme de paiement électronique. Dans certains cas, l'utilisateur introduit son identité ou d'autres données personnelles.
- B. Le fournisseur de la prestation enregistre cette commande dans une base de données 2 et lui attribue un code numérique unique dans un enregistrement 3. La commande peut être associée à l'identité 4 de l'utilisateur 1.
- C. L'utilisateur imprime ensuite à domicile une attestation 5 avec ce code numérique, par exemple sous forme de code visuel 50 (code-barre, QR-code, DataMatrix, etc.). L'identité de l'utilisateur 51, d'autres données introduites par l'utilisateur et des informations relatives à la prestation peuvent également être imprimées.
- D. Lorsque la prestation achetée est réclamée, par exemple à l'entrée d'un concert ou d'une manifestation, l'utilisateur 1 présente cette attestation 5 qui est scannée. Le contrôleur 6 se connecte à la base de données 2 pour vérifier que le code 50 présenté corresponde à une prestation commandée, et qu'il n'a pas été présenté auparavant.
Si plusieurs utilisateurs présentent la même attestation, la prestation sera fournie au premier utilisateur à se présenter. Dans une variante, l'identité 51 qui figure sur l'attestation est contrôlée, par exemple en demandant à l'utilisateur 1 de présenter une pièce d'identité 7.
- E. Si le code 50 est valide, l'utilisateur 1 client accède à la prestation. Le code 3 est marqué dans la base de données comme ayant été utilisé; un autre utilisateur présentant le même code ne sera plus admis.

[0009] Dans ce procédé, la clé d'autorisation est donc constituée par l'attestation portant un code numérique unique généré par le fournisseur de la prestation. Une telle attestation peut cependant être copiée et reproduite facilement, par

exemple en la photocopiant ou en l'imprimant à plusieurs exemplaires. Elle ne constitue donc pas une clé d'autorisation difficilement reproductible.

[0010] Par conséquent, un usurpateur peut ensuite requérir la prestation réservée avant l'utilisateur légitime; celui-ci se voit alors refuser la prestation. Un contrôle d'identité permet de limiter ce risque, mais s'avère lent, coûteux, pas toujours fiable, et parfois impossible à mettre en œuvre.

[0011] D'autre part, l'accès au service recherché est refusé même à des utilisateurs légitimes s'ils ne sont pas parvenus à l'imprimer avec une qualité suffisante sur leur imprimante domestique par exemple.

Bref résumé de l'invention

[0012] Un but de la présente invention est donc de proposer un système et un procédé technique de contrôle d'accès à la prestation basé sur un nouveau type de clé d'autorisation.

[0013] Un but de la présente invention est aussi de proposer un système et un procédé de contrôle d'accès basé sur un nouveau type de clé d'autorisation qui soit à la fois plus sûr et moins coûteux à produire que la plupart des systèmes d'autorisation existants.

[0014] Selon l'invention, ces buts sont atteints notamment au moyen d'un procédé de contrôle d'accès à une prestation comportant les étapes suivantes:

- génération au moyen d'un scanner de données correspondant à l'image d'un billet de banque muni d'un numéro de série, ledit billet de banque constituant une clé d'autorisation;
- extraction dudit numéro de série à partir desdites données, et
- vérification à l'aide dudit numéro de série afin de déterminer si ledit billet de banque correspond à une coupure préalablement autorisée et autorisation d'une prestation en cas de vérification positive ou refus d'une prestation en cas de vérifications négative.

[0015] L'invention part notamment de la constatation qu'un billet de banque constitue un objet technique difficilement reproductible et porteur d'une information (le numéro de série) unique ou quasiment unique. Il peut donc être utilisé dans un but inattendu et complètement différent de sa fonction première de paiement, c'est-à-dire comme clé d'autorisation pour accéder à une prestation, par exemple pour authentifier son porteur et par exemple pour confirmer une réservation ou l'authenticité d'une information sur une attestation.

[0016] Chaque billet de banque est marqué avec un code d'identification, par exemple un numéro de série unique. Il comporte de nombreux éléments pour rendre sa reproduction difficile et aisément détectable. Par ailleurs, la falsification d'un billet de banque est répréhensible pénalement dans la plupart des Etats. Le coût de reproduction d'un billet de banque est en général largement supérieur à la valeur nominale de la coupure la plus élevée. Un billet de banque peut ainsi être utilisé comme clé d'autorisation particulièrement sûre et comme élément d'autorisation au porteur.

[0017] Les billets de banque ont en outre l'avantage d'être disponibles à la quasi-totalité de la population. Il n'est donc pas nécessaire de fabriquer une clé d'autorisation dédiée pour autoriser une prestation ou pour authentifier un utilisateur; n'importe quel billet de banque peut être utilisé à cet effet, après une simple phase d'enrôlement au cours de laquelle le numéro de série du billet est associé à la prestation à autoriser.

[0018] La valeur de la prestation peut être différente de la valeur du billet de banque. Elle peut être indépendante de la valeur du billet de banque. Par exemple, une prestation d'une valeur de CHF 100.– peut être autorisée en apportant la preuve de la possession d'un billet de banque particulier d'une valeur nominale de CHF 10.–. Un billet de banque peut être utilisé pour authentifier ou confirmer la réservation d'une prestation gratuite, ou d'une prestation de valeur supérieure à celle du billet de banque et dont le paiement peut être effectué différemment.

[0019] Le procédé de contrôle d'accès de l'invention peut être utilisé indépendamment de toute transaction commerciale. Par exemple, un billet de banque peut être utilisé comme clé d'autorisation pour autoriser et/ou pour déclencher l'ouverture d'une serrure en fonction du numéro de série.

[0020] Le procédé peut comporter en outre une étape préliminaire de réservation d'une prestation par l'utilisateur, au cours de laquelle l'utilisateur associe la prestation à un numéro de série d'un billet de banque qu'il détient.

[0021] La prestation peut être payée au moyen d'informations introduites lors de la réservation, le billet de banque ne servant alors qu'à authentifier la réservation. Par exemple, la réservation peut être effectuée via Internet et payée par carte de crédit ou via une plateforme de paiement électronique. La prestation peut aussi être payée au moyen d'informations introduites lors de la réservation avec un montant prépayé à l'avance sur un compte à prépaiement. Le paiement peut aussi être effectué sur la base d'informations introduites lors de la réservation, mais après cette réservation, ou même après la prestation, par exemple à la fin du mois, via une facture téléphonique ou une autre facture périodique.

[0022] La prestation peut aussi être payée en partie au moyen d'informations introduites lors de la réservation et en partie au moyen du billet de banque échangé lors de l'autorisation de la prestation. Dans ce cas, le billet de banque sert à la fois à authentifier la réservation et à effectuer une partie du paiement de la prestation.

[0023] La prestation peut par exemple être une prestation d'accès à un emplacement ou à une manifestation, une prestation d'achat, une prestation d'utilisation de transports publics, etc.

[0024] Le numéro de série sur le billet de banque peut être reconnu avec un logiciel de reconnaissance d'image, par exemple un logiciel de reconnaissance de caractères (OCR).

[0025] Dans un mode de réalisation, un enregistrement correspondant au numéro de série reconnu sur le billet de banque est recherché par un module de recherche dans une base de données. Cette base de données peut contenir une liste de numéros de série de billets de banque (ou des données dépendant de ces numéros de série, par exemple une partie du numéro de série, un hash du numéro de série, etc.) associés à des prestations autorisées.

[0026] Dans un mode de réalisation, un billet de banque est associé dans une base de données à un enregistrement; il peut être stocké dans cet enregistrement. L'autorisation ou le refus de la prestation dépend alors de cet enregistrement. L'enregistrement associé à chaque numéro de série permet aussi de déterminer la nature de la prestation autorisée, ou ses paramètres. L'enregistrement associé à chaque numéro de série peut contenir d'autres champs indiquant par exemple si la prestation a déjà été consommée, à quelle date elle a été consommée, le coût de la prestation associée au billet de banque, des paramètres de la prestation, etc. Cette variante permet de contrôler, par exemple de manière centralisée, si un billet de banque particulier a déjà été utilisé pour authentifier une réservation et d'éviter par exemple qu'une même prestation ne soit réutilisée plusieurs fois.

[0027] L'enregistrement associé à un numéro de série particulier peut être modifié lorsque la prestation a été autorisée. La même prestation est alors refusée si un utilisateur la requiert ultérieurement en présentant le même billet de banque.

[0028] Dans un mode de réalisation optionnel, l'utilisateur imprime ou affiche une attestation comportant des informations dépendant du numéro de série. Cette attestation peut être contrôlée avant l'autorisation de la prestation.

[0029] L'attestation peut se présenter par exemple sous la forme d'un imprimé, d'un billet de transport, d'un ticket d'accès à une manifestation, etc. Elle peut être imprimée sur papier ou affichée par exemple sur un smartphone ou une tablette. Le contrôle peut être manuel, par exemple par un contrôleur qui la lit, ou semi-automatique, par exemple en la scannant et en vérifiant automatiquement des informations qui y figurent.

[0030] L'attestation peut inclure des informations relatives à la prestation, par exemple le nom de la prestation, la date à laquelle il peut y être fait droit, un numéro de siège ou un emplacement, etc.

[0031] Les informations figurant l'attestation et dépendant du numéro de série peuvent inclure le numéro de série du billet de banque. Ce numéro de série peut être affiché en clair afin de permettre en contrôle humain, avec une écriture lisible par ordinateur, et/ou codé sous forme de code visuel. Il peut être crypté, par exemple avec une clé de cryptage public, de manière à pouvoir être décrypté uniquement à l'aide de la clé de décryptage correspondante. De cette manière, même un usurpateur qui dispose d'une copie de l'attestation ne sait pas quel billet de banque il doit présenter pour l'authentifier.

[0032] Au moins une partie des informations sur l'attestation relatives à la prestation peuvent être codées sous forme de code visuel, par exemple de code-barre, QR-code, DataMatrix, etc.

[0033] Les informations sur l'attestation qui dépendent du numéro de série peuvent être signées électroniquement avec une clé asymétrique privée, le contrôle de l'attestation incluant la vérification de la signature électronique avec la clé asymétrique publique correspondant à ladite clé privée. Le contrôleur peut ainsi vérifier que l'attestation a bien été générée par une personne ou un dispositif autorisé et disposant de la clé privée nécessaire.

[0034] L'enregistrement déterminant la prestation peut être recherché dans la base de données à partir des informations lues sur l'attestation relatives à la prestation. Il peut aussi être recherché à partir des informations dépendant du numéro de série, par exemple directement à partir du numéro de série.

[0035] L'enregistrement peut contenir un champ indiquant à quelle date la prestation a été consommée.

[0036] L'enregistrement peut contenir un champ indiquant un paramètre de la prestation.

[0037] Selon le mode de réalisation, la mise en œuvre de l'invention implique ainsi de nombreuses étapes techniques dans un système technique complexe, y compris pour le scannage de billet de banques, l'utilisation de tels billets de banque comme clé d'autorisation unique difficilement reproductible, le stockage de numéros de série dans une base de données, la lecture et l'écriture de données dans divers enregistrements de cette base de données, la signature électronique de numéros de série au moyen de modules cryptographiques, la vérification de ces signatures au moyen d'autres modules cryptographiques, l'impression d'attestations incluant des codes visuels, la lecture et la vérification de ces codes, etc.

[0038] L'invention concerne aussi un système d'autorisation de prestation comprenant:
un système de scannage de billet de banque permettant une extraction d'un numéro de série sur un billet de banque;
un système informatique, par exemple un serveur relié au réseau internet, adapté pour exécuter un programme informatique configuré pour déterminer à partir dudit numéro de série si la prestation peut être autorisée.

[0039] Le système de scannage peut comprendre un logiciel de reconnaissance de caractères pour reconnaître le numéro de série.

[0040] Il est aussi possible d'identifier la devise du billet (CHF, Euro, \$, etc.) et/ou la coupure (10, 20, 50, etc.), afin d'identifier la prestation à autoriser, et/ou de valider le numéro de série. Cette identification peut être faite par un algorithme de reconnaissance d'image, à l'instar de l'extraction du numéro de série.

[0041] Le système peut comprendre une base de données avec une pluralité d'enregistrements correspondant à des numéros de série de billets de banque, lesdits enregistrements incluant un champ indiquant si ladite prestation a été autorisée.

[0042] Le système peut comprendre un module de signature électronique de numéros de série au moyen d'une clé privée, et un module de vérification de la signature électronique au moyen d'une clé publique correspondant à la clé privée.

[0043] Le système peut constituer une serrure pour contrôler l'accès à un emplacement ou à un équipement et pour autoriser cet accès à un utilisateur détenant un billet de banque préalablement accepté à cet effet.

[0044] Le système peut constituer un contrôle d'accès à un équipement électronique, par exemple un système de contrôle d'accès à un ordinateur, un smartphone, une application, afin de permettre l'accès aux utilisateurs qui sont munis d'un billet de banque autorisé.

[0045] Le système d'autorisation peut générer un signal électrique ou mécanique pour autoriser la prestation, par exemple un signal déclenchant l'ouverture d'une porte, d'un portail, l'affichage d'une information d'autorisation d'accès, ou le déclenchement d'une routine informatique afin d'autoriser la prestation.

Brève description des figures

[0046] Des exemples de mise en œuvre de l'invention sont indiqués dans la description illustrée par les figures annexées dans lesquelles:

- La fig. 1 illustre de manière schématique les principales étapes d'un procédé de type «print@home» selon l'art antérieur.
- La fig. 2 illustre de manière schématique les principales étapes d'un premier mode de réalisation du procédé selon l'invention.
- La fig. 3 illustre de manière schématique les principales étapes d'un deuxième mode de réalisation du procédé selon l'invention.
- La fig. 4 montre un exemple d'enregistrement dans la base de données.

Exemple(s) de mode de réalisation de l'invention

[0047] La fig. 2 illustre de manière schématique les principales étapes d'un procédé selon l'invention. Ce procédé est mis en œuvre notamment au moyen de nouveaux programmes informatiques exécutés par un serveur 20 relié au réseau Internet 21 et éventuellement de nouveaux programmes exécutés sur un ordinateur, un smartphone ou une tablette de l'utilisateur.

[0048] Au cours de l'étape F, un utilisateur 1 réserve en ligne une prestation, par exemple au travers d'un site web accessible via le réseau Internet 21, ou d'une application exécutée par exemple sur un smartphone ou un ordinateur de l'utilisateur. Pour que l'achat soit validé, l'utilisateur doit saisir un numéro de série 90 d'un billet de banque 9 à sa disposition, soit manuellement, soit en scannant ce billet de banque par exemple au moyen de l'application dédiée. Dans ce dernier cas, un algorithme de reconnaissance visuel, par exemple un algorithme de reconnaissance de caractère, peut être mis en œuvre pour extraire le numéro de série à partir de l'image scannée.

[0049] Le numéro de série 90 peut être constitué par une suite de chiffres; en option, ce numéro de série peut aussi inclure des lettres ou d'autres symboles alphanumériques. L'expression «numéro de série» peut donc inclure des symboles numériques et/ou non numériques.

[0050] Le type de coupure accepté peut être imposé. L'application peut vérifier que le billet de banque scanné correspond à une coupure autorisée. L'utilisateur 1 indique en outre un moyen de paiement pour cette prestation, par exemple un numéro de carte de crédit, un mot de passe sur une plateforme de paiement, etc. Le moyen de paiement peut aussi être implicite, par exemple dans le cas d'un paiement au moyen d'une facture téléphonique, ou d'un moyen de paiement pré-enregistré. Le paiement peut être effectué immédiatement, ou par débit d'un compte à prépaiement, ou ajouté à une liste de paiement débités par exemple à la fin du mois.

[0051] La prestation réservée peut correspondre par exemple à un billet pour une manifestation (par exemple un billet de concert), à un titre de transport, à un bien ou un service acheté, à un droit d'accès, etc.

[0052] La réservation peut aussi inclure des paramètres de la prestation, par exemple une date, un emplacement, un numéro de siège, etc. Elle peut aussi inclure, en option, des données personnelles relatives à l'utilisateur, par exemple son identité.

[0053] Au cours de l'étape G, le fournisseur de prestation (ou un tiers mandaté par ce fournisseur) vérifie de préférence si le numéro de série 90 introduit correspond à un numéro de série possible sur les coupures admises. Il vérifie aussi de préférence si la prestation réservée est disponible. Si ces deux conditions sont remplies, ou non testées, il enregistre numériquement de la base de données 2 la réservation de prestation. Il crée à cet effet un enregistrement 3 (fig. 4) qui contient des informations 91 telles que l'identification de la prestation réservée, les paramètres de cette prestation, des données personnelles optionnelles relatives à l'utilisateur (par exemple son identité), ainsi que le numéro de série introduit 90. Le champ 92 indique si la prestation a déjà été autorisée, c'est-à-dire si un utilisateur l'a réclamée à un point de contrôle. Ces différentes vérifications et opérations peuvent être effectuées au moyen d'une infrastructure technique, par exemple un serveur 20.

[0054] Au cours de l'étape H optionnelle, l'utilisateur imprime ou affiche sur un écran d'un dispositif personnel une attestation 5 qui contient d'une part des données 52 dépendant du numéro de série 90 introduit, et d'autre part, en option, des informations 53 relatives à la prestation (par exemple les paramètres 91) et/ou à l'utilisateur. Les données 52 dépendant du numéro de série 90 utilisé pour authentifier la réservation peuvent être affichées en clair ou codées sous forme de code visuel pour en faciliter la lecture automatique, par exemple sous forme de code-barre, de QR-code, de DataMatrix, etc. Elles peuvent être signées électroniquement par un module cryptographique avec une clé privée du prestataire, afin de permettre à un contrôleur de vérifier leur authenticité. Elles peuvent être encryptées avec une clé de cryptage symétrique ou asymétrique du prestataire.

[0055] Au cours de l'étape I, lorsque la prestation réservée est réclamée, l'utilisateur présente le billet de banque 9 utilisé pour l'authentifier. En option, il présente aussi l'attestation 5 préalablement imprimée. Un contrôleur 6 humain ou automatique vérifie l'authenticité du billet de banque (par exemple en vérifiant des marques difficilement reproductibles comme le filigrane, etc.), et lit le numéro de série sur ce billet. De préférence, il vérifie aussi l'attestation 5, contrôle visuellement si elle correspond à la prestation réclamée, et s'assure de préférence que le numéro de série 52 imprimé ou codé sur cette attestation correspond au numéro de série 90 sur le billet de banque présenté.

[0056] Le contrôleur 6 communique ensuite avec une base de données, par exemple à la base de données 2 à distance (flèche 100), et lui transmet le numéro de série 90 sur le billet de banque, ou le code correspondant 52 sur l'attestation, par exemple un code visuel, ou un autre code sur cette attestation. En recherchant l'enregistrement correspondant dans la base données, on vérifie ensuite:

si l'attestation et/ou le billet correspond à une prestation effectivement réservée et autorisée, et/ou
si cette attestation/ce billet a déjà été utilisé pour réclamer la même prestation.

[0057] Si ces conditions sont réunies, le contrôleur 6 autorise ensuite la prestation demandée, par exemple l'entrée à une manifestation; dans le cas contraire, il refuse cette autorisation. L'enregistrement correspondant au billet de banque est de préférence marqué dans la base de données pour indiquer que la prestation a été utilisée, par exemple au moyen d'un fanion (champ binaire) ou d'un champ date.

[0058] L'utilisateur peut ensuite accéder la prestation commandée (par exemple une manifestation, l'utilisation d'un véhicule ou d'un équipement, l'achat d'un objet ou d'un service ...) au cours de l'étape J.

[0059] Le procédé décrit ci-dessus et illustré sur la fig. 2 requiert l'accès à une base de données centralisée, par exemple la base de données 2, depuis un terminal du contrôleur 6. Un tel accès n'est pas toujours possible, ou peut engendrer des frais ou des délais indésirables.

[0060] Il est possible d'éviter un tel accès en vérifiant dans une base de données locale, près du contrôleur 6, ou dans un dispositif du contrôleur 6, si une attestation ou un numéro de série a déjà été utilisé. Un tel contrôle est par exemple possible lorsque l'accès à la prestation se fait par un seul point de contrôle, ou par plusieurs points de contrôle qui peuvent se transmettre des informations de l'un à l'autre.

[0061] Une autre possibilité d'empêcher la réutilisation d'un billet de banque par un deuxième utilisateur est de prendre son billet de banque lors de l'accès à la prestation. Par exemple, il est possible de payer la prestation, ou une partie du prix de la prestation, avec le billet de banque utilisé pour la réserver et pour l'authentifier. Dans ce cas, le billet de banque est saisi et ne peut donc plus être réutilisé par un tiers disposant d'une attestation falsifiée.

[0062] La fig. 3 illustre de manière schématique une variante du procédé dans laquelle une communication avec la base de données 2 n'est pas indispensable (même si elle peut aussi être établie). Dans ce procédé, l'étape de réservation F peut être identique à l'étape F décrite plus haut en relation avec la fig. 2.

[0063] Au cours de l'étape ultérieure G', le fournisseur de prestation (ou un tiers mandaté par ce fournisseur) vérifie de préférence si le numéro de série introduit correspond à un numéro de série possible sur les coupures admises. Il vérifie aussi de préférence si la prestation réservée est disponible. Si ces deux conditions sont remplies, ou non testées, il enregistre numériquement dans la base de données 2 la réservation de prestation. Il crée à cet effet un enregistrement 3 qui contient des informations 91 telles que l'identification de la prestation réservée, les paramètres de cette prestation, les données personnelles optionnelles relatives à l'utilisateur ainsi que le numéro de série introduit 90. Ces vérifications et opérations peuvent être effectués au moyen d'un serveur 20 opéré par le fournisseur de prestation et capable d'exécuter le programme de gestion de la base de données 2 et des modules cryptographiques.

[0064] Le fournisseur de prestation signe ensuite le numéro de série 90 transmis par ce client, ou une information dépendant de ce numéro de série, avec un module cryptographique employant une méthode de chiffrement asymétrique et une clé de signature privée. La signature permet de garantir que le numéro de série 90 a été reçu et accepté par le fournisseur de prestation exploitant la base de données 2.

[0065] Le numéro de série peut aussi être encodé au moyen d'une clé de cryptage symétrique ou asymétrique; il est ainsi nécessaire de disposer de la clé de décryptage correspondante pour vérifier à quel billet une attestation particulière est associée.

[0066] Au cours de l'étape H', l'utilisateur imprime ou affiche sur un écran d'un terminal personnel une attestation 5' qui contient d'une part des données 52' dépendant du numéro de série 90 ainsi signé (et éventuellement crypté), et d'autre part, en option, des informations 53 relatives à la prestation et/ou à l'utilisateur. Les données 52' et/ou 53 peuvent être affichées en clair ou codées sous forme de code visuel pour en faciliter la lecture automatique, par exemple sous forme de code-barre, de QR-code, de DataMatrix, etc.

[0067] Au cours de l'étape I', lorsque la prestation réservée est réclamée, l'utilisateur présente le billet de banque 9 utilisé pour l'authentifier. Il présente aussi l'attestation 5' préalablement imprimée. Un contrôleur 6 humain ou automatique vérifie l'authenticité du billet de banque 9 (par exemple en vérifiant des marques difficilement reproductibles comme le filigrane, etc.), et lit le numéro de série 90 sur ce billet. De préférence, il vérifie aussi l'attestation 5' et contrôle visuellement si elle correspond à la prestation réclamée.

[0068] Le contrôleur 6 vérifie ensuite la signature associée au code numérique 52', par exemple en décodant ce code avec un module cryptographique et en employant une clé publique stockée dans son terminal et correspondant à la clé privée du prestataire de service. Si la signature est authentifiée et que le numéro de série 52' ainsi codé sur cette attestation correspond au numéro de série 90 sur le billet de banque présenté, le contrôleur a la garantie, sans se connecter à la base de données 2, que le numéro de série est valide et qu'il a été accepté par le prestataire de service 2 pour authentifier une réservation.

[0069] L'utilisation d'une clé privée connue uniquement du prestataire 2 implique que seul ce prestataire peut générer des attestations; en revanche, le contrôleur et tout tiers disposant d'une application adaptée et de la clé publique correspondant peut vérifier si cette attestation a été générée par ce prestataire. Il n'est cependant pas possible de vérifier directement si l'attestation a déjà été utilisée.

[0070] Si l'attestation est authentifiée, le contrôleur autorise ensuite la prestation demandée, par exemple l'entrée à une manifestation; dans le cas contraire, il refuse cette autorisation.

[0071] L'utilisateur peut ensuite accéder à la prestation commandée (par exemple une manifestation, l'utilisation d'un véhicule ou d'un équipement, l'achat d'un objet ou d'un service ...) au cours de l'étape J.

[0072] Les deux procédés ci-dessus permettent la revente d'attestation, par exemple de tickets, à un tiers à qui le billet de banque correspondant utilisé pour l'authentifier doit aussi être remis. L'authentification n'est pas personnelle; elle est liée au détenteur du billet de banque.

[0073] Nous allons maintenant détailler quelques cas d'utilisation dans lesquels la solution technique ci-dessus peut avantageusement être mise en place.

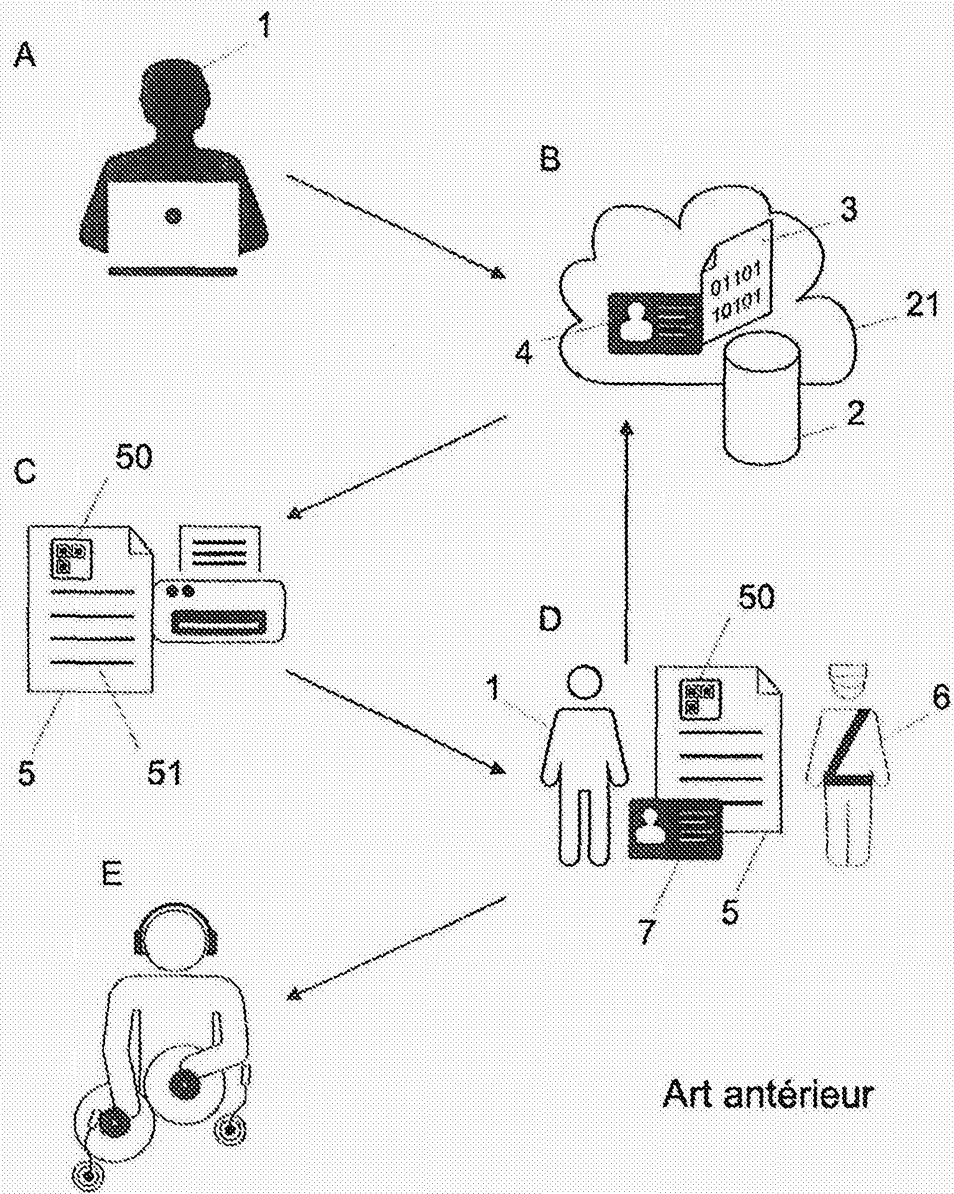
[0074] Dans un premier exemple, un utilisateur souhaite acheter des tickets pour un événement musical. Il se connecte donc à site de vente en ligne, afin d'acheter ses billets. Le site de vente propose le procédé ci-dessus. L'utilisateur est intéressé par cette méthode qui lui évite de devoir livrer son nom ou d'autres informations personnelles à un site en ligne. Le procédé lui permet aussi de revendre ses billets, s'il renonce à aller au concert. L'utilisateur a en outre la garantie qu'aucun utilisateur ne pourra se présenter avant lui à l'entrée de la manifestation avec une copie frauduleuse de son ticket (attestation).

[0075] Dans un deuxième scénario, une compagnie qui effectue des sondages téléphoniques souhaite récompenser les participants avec un bon d'achat offert aux personnes qui le complètent. La société souhaite néanmoins s'assurer qu'un même bon d'achat ne pourra être utilisé simultanément dans plusieurs magasins, car pour de raisons techniques, il y a un délai de quelques minutes pour qu'une information émise par un magasin soit transmise aux autres. Dans ce but, et avant que le sondage téléphonique ne commence, il est demandé à l'utilisateur participant de fournir le numéro de série d'un billet de banque d'une valeur quelconque. Si le participant complète le sondage anonyme, il pourra se présenter à n'importe quel magasin autorisé et en présentant le billet de banque, il recevra un bon d'achat d'une valeur non nécessairement liée à celle du billet présenté.

[0076] Cette solution résout le problème d'authentification. Le problème que rencontre la société est l'absence de connectivité lors qu'il s'agit de vérifier la non-réutilisation d'une information authentifiée. En effet le délai de quelques minutes est suffisant pour mettre à jour la liste des billets de banque valides (le sondage prend à lui tout seul plus de quelques minutes), un utilisateur ne pouvant donc pas se présenter aux magasins avant que l'information concernant son billet ne soit arrivée. Par contre, ce délai ne suffit pas pour vérifier que deux personnes différentes ne sont pas en train d'utiliser le même bon en même temps dans deux magasins différents. Le fait de devoir présenter un billet de banque élimine ce risque.

Revendications

1. Procédé de contrôle d'accès à une prestation comportant les étapes suivantes:
 - génération au moyen d'un scanner de données correspondant à l'image d'un billet de banque (9) muni d'un numéro de série (90), ledit billet de banque constituant une clé d'autorisation;
 - extraction dudit numéro de série (90) à partir desdites données, et
 - vérification à l'aide dudit numéro de série (90) afin de déterminer si ledit billet de banque correspond à une coupure préalablement autorisée et autorisation d'une prestation en cas de vérification positive ou refus d'une prestation en cas de vérification négative.
2. Procédé de la revendication 1, comprenant en outre une extraction de la devise et/ou de la coupure dudit billet de banque (9), par un logiciel de reconnaissance d'image, afin d'identifier la prestation à autoriser, et/ou de valider le numéro de série.
3. Procédé selon la revendication 1 ou 2, ledit numéro de série (90) étant reconnu avec un algorithme de reconnaissance d'image, par exemple un algorithme de reconnaissance de caractères.
4. Procédé selon l'une des revendications 1 à 3, dans lequel:
 - un enregistrement (3) correspondant au numéro de série (90) reconnu est recherché dans une base de données (2);
 - l'autorisation ou le refus de ladite prestation dépendant de cet enregistrement (3).
5. Procédé selon la revendication 4, ledit enregistrement (3) étant modifié lorsque la prestation a été autorisée, la même prestation étant refusée si un utilisateur la requiert ultérieurement en présentant le même billet de banque (9).
6. Procédé selon l'une des revendications 1 à 5, comportant en outre une étape consistant à imprimer ou afficher une attestation (5; 5') comportant des informations d'identification (52; 52') représentatives dudit numéro de série (90), ces informations pouvant être affichées ou imprimées en clair ou codées sous forme de code visuel pour en faciliter la lecture automatique, ladite attestation (5; 5') étant authentifiée avant l'autorisation de la prestation.
7. Procédé selon la revendication 6, ladite attestation (5; 5') incluant des informations (53) relatives à ladite prestation telles que l'identification de la prestation.
8. Procédé selon l'une des revendications 6 ou 7, l'authentification de ladite attestation (5; 5') comportant un scannage de ladite attestation.
9. Procédé selon l'une des revendications 6 à 8, lesdites informations (52; 52') représentatives du numéro de série étant signées électroniquement avec une clé asymétrique privée, l'authentification de ladite attestation incluant la vérification de la signature électronique avec la clé asymétrique publique correspondant à ladite clé privée.
10. Procédé selon l'une des revendications 6 à 9, lesdites informations représentatives du numéro de série (52; 52') étant encryptées électroniquement, l'authentification de ladite attestation (5; 5') incluant le décryptage desdites informations.
11. Procédé selon l'une des revendications 7 à 10, dans lequel ledit enregistrement (3) est recherché dans la base de données (2) à partir de l'identification de la prestation (53).
12. Procédé selon l'une des revendications 1 à 11, comportant en outre une étape préliminaire (F) de réservation de la prestation par l'utilisateur (1), au cours de laquelle ledit utilisateur associe la prestation audit numéro de série (90) dudit billet de banque (9) qu'il détient.
13. Procédé selon l'une des revendications 4 à 12, ledit enregistrement (3) contenant un champ (92) indiquant à quelle date la prestation a été consommée, et un champ (91) indiquant un paramètre de la prestation.
14. Système d'autorisation de prestation comprenant:
 - un système de scannage de billet de banque permettant une extraction d'un numéro de série (90) sur un billet de banque (9);
 - un système informatique, par exemple un serveur (20) relié au réseau Internet (21), munie d'un programme informatique configuré pour déterminer à partir dudit numéro de série si la prestation peut être autorisée.
15. Système selon la revendication 14, comprenant en outre un logiciel de reconnaissance de caractères pour reconnaître ledit numéro de série (90).
16. Système selon l'une des revendications 14 et 15, comprenant une base de données (2) avec une pluralité d'enregistrements (3) correspondant auxdits numéros de série (90), lesdits enregistrements incluant un champ indiquant si ladite prestation a été autorisée.
17. Système selon l'une des revendications 14 à 16, comprenant un module de signature électronique dudit numéro de série au moyen d'une clé privée, et un module de vérification de ladite signature électronique au moyen d'une clé publique correspondant à ladite clé privée.



Art antérieur

Fig. 1

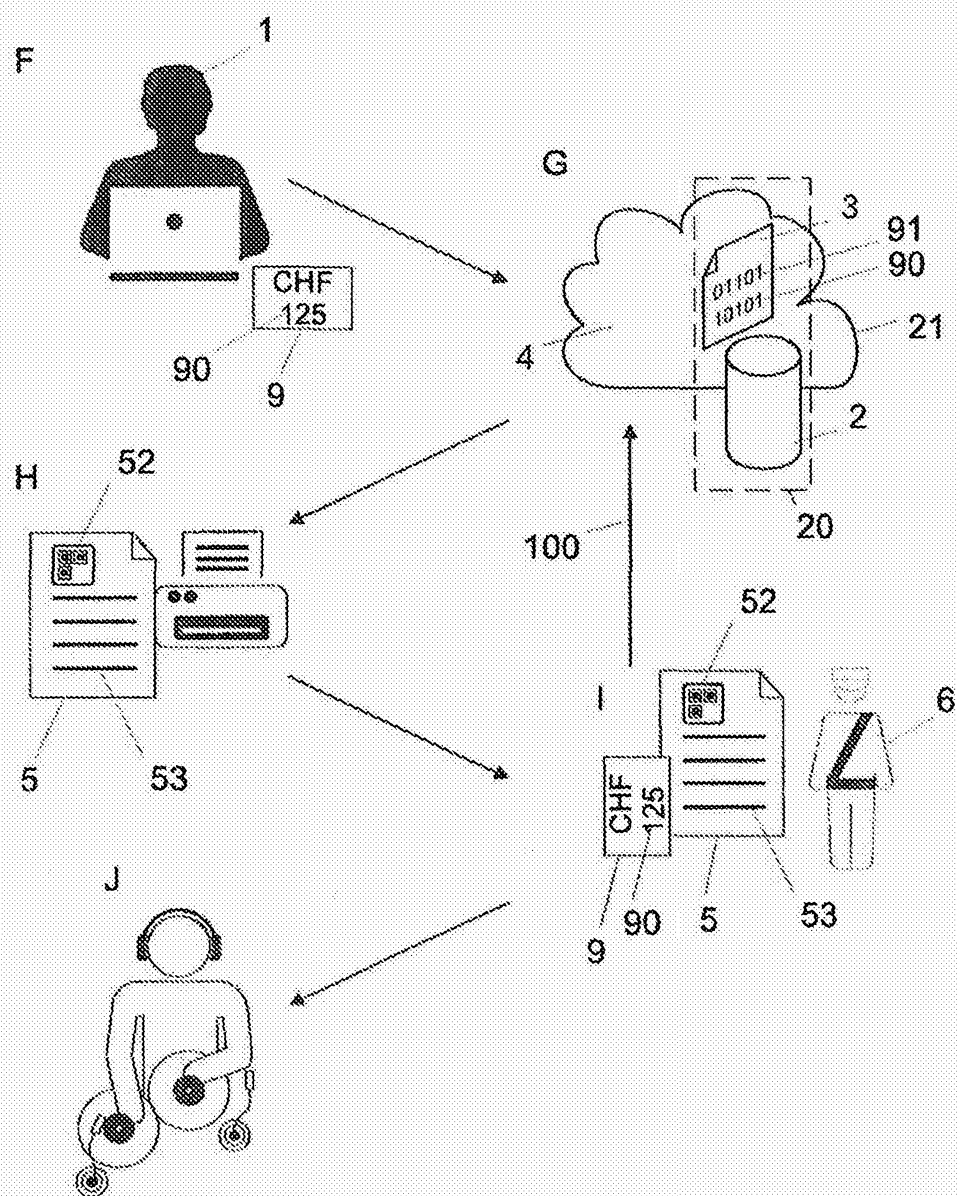


Fig. 2

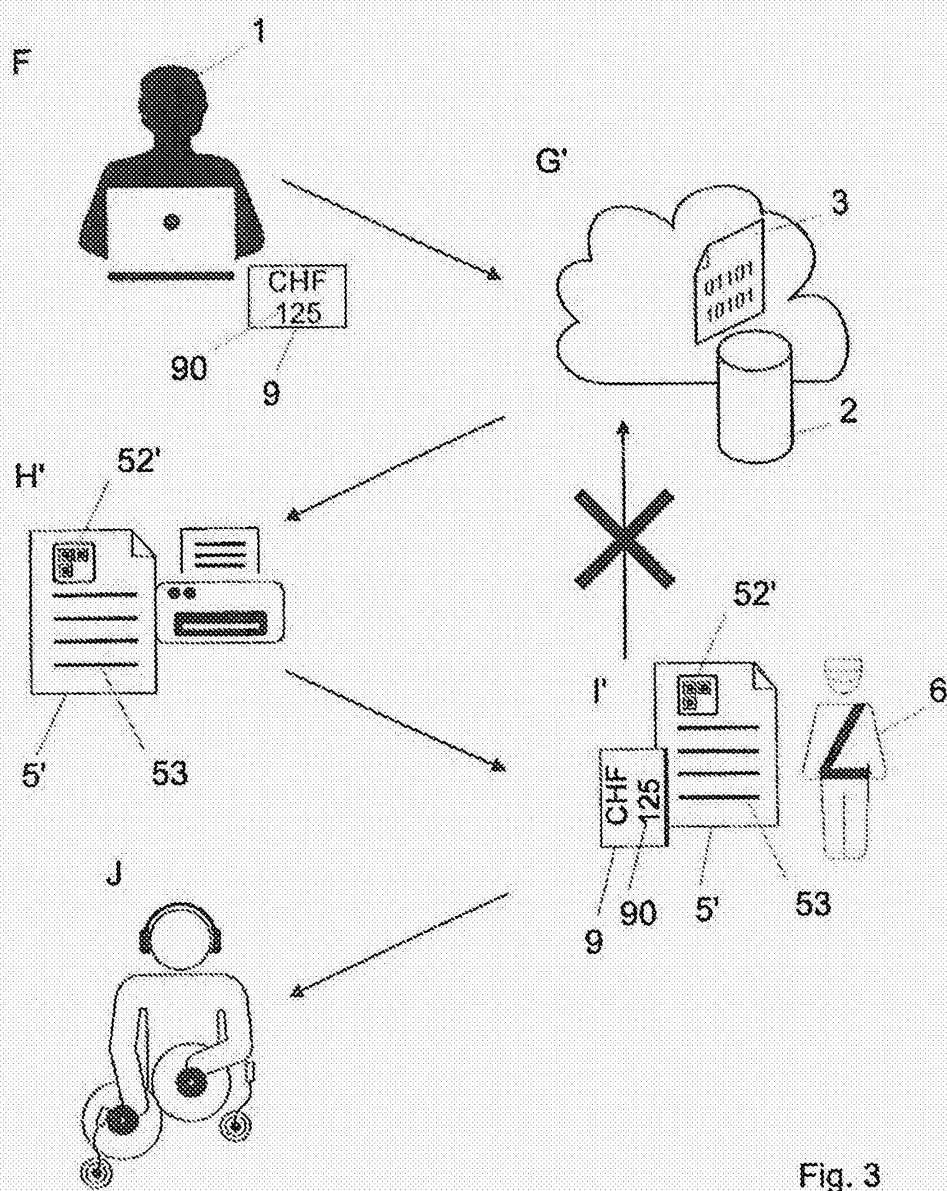


Fig. 3

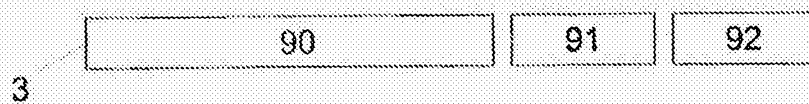


Fig. 4

© 2013