(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 150 010***

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

(21) **N° d'enregistrement national :** **23 06169**

(51) Int Cl[8] : ***G 06 F 21/60*** *(2024.01)*

(12) DEMANDE DE CERTIFICAT D'UTILITE A3

(22) **Date de dépôt :** 16.06.23.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 20.12.24 Bulletin 24/51.

(56) **Les certificats d'utilité ne sont pas soumis à la procédure de rapport de recherche.**

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

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *GUIGAN Franck* — FR.

(72) **Inventeur(s) :** GUIGAN Franck.

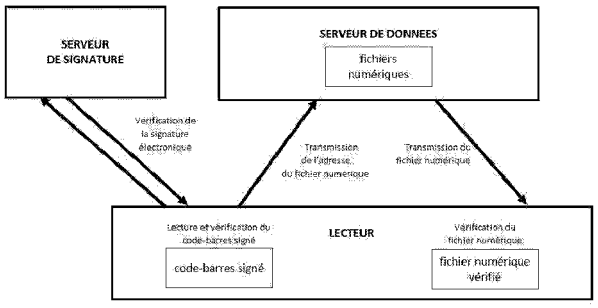
(73) **Titulaire(s) :** GUIGAN Franck.

(54) **Ensemble de données sécurisé et procédure d'émission et de lecture d'un tel ensemble.**

(57) L'invention est un ensemble de données sécurisé contenant un fichier numérique signé électroniquement situé sur un serveur et une donnée numérique ou alphanumérique signée électroniquement comportant cette adresse et un élément de contrôle d'intégrité du fichier numérique considéré et optionnellement d'autres informations.

L'avantage est que chacun de ces deux éléments, le fichier d'une part et la donnée numérique ou alphanumérique d'autre part, contiennent des données complémentaires qui ne peuvent pas être rassemblées facilement par un fraudeur, et qu'il suffit d'une donnée numérique ou alphanumérique courte pouvant être représentée par un code-barres de petite taille pour mettre à la disposition d'un lecteur des informations sécurisées de grand volume comme une image haute définition, un fichier sonore ou une vidéo par exemple.

Figure de l'abrégé : Fig. 1



FR 3 150 010 - A3

Description

Titre de l'invention : Ensemble de données sécurisé et procédure d'émission et de lecture d'un tel ensemble

Domaine technique

[0001] L'invention est un moyen de sécurisation d'un ensemble de données dont certaines sont volumineuses comme une photographie, un fichier sonore, une vidéo, une page html ou un ensemble de pages html ou des plans tri-dimensionnels par exemple.

Technique antérieure

[0002] On connait des procédés de vérification d'un fichier par un élément de contrôle de son intégrité, comme un hash ou une checksum par exemple.

[0003] On connait aussi des dispositifs de vérification de données d'identité consistant à munir un fichier contenant les données considérées d'un tel élément de contrôle.

[0004] On connait de tels dispositifs dans lesquels tout ou partie d'un fichier ou son lien d'accès est représenté par une chaine de caractères numériques ou alphanumériques et on sait signer de tels chaines pour garantir leur origine et leur intégrité. On sait aussi représenter de telles chaînes par des codes-barres.

[0005] On connait enfin une méthode consistant à donner à une personne une identité numérique en lui fournissant un fichier signé comportant sa photographie et tous les détails de son identité.

Problème technique

[0006] La représentation d'un média comme une photo, un enregistrement sonore ou une vidéo par une chaine de caractères numériques ou alphanumériques n'est pas intelligible, et les codes-barres peuvent comporter des données complexes telles que des références alphanumériques, des noms, des adresses, mais il est difficile de leur ajouter les données d'un tel média car ces données sont très volumineuses et conduiraient à des codes-barres à très grande densité, donc difficiles à imprimer et à lire ou de très grande taille.

[0007] Une identité numérique composée d'un fichier contenant des informations d'identité dont un média comme une photo d'identité et un élément de contrôle de ces informations, a pour inconvénient de mettre à la disposition de tiers ce fichier qui est sensible et pourrait permettre de réaliser de faux documents d'identité.

[0008] L'objectif de la présente invention est de permettre la transmission d'éléments d'information volumineux ou sensibles à un lecteur, tout en munissant ces éléments d'information d'un moyen de contrôle de leur intégrité et en les protégeant contre la fraude.

Brève description des dessins

[0009] L'invention sera bien comprise, et d'autres buts, avantages et caractéristiques de celle-ci apparaîtront plus clairement à la lecture de la description qui va suivre, laquelle est illustrée par la [Fig.1].

[0010] [Fig.1] est un diagramme montrant une procédure de lecture et de vérification d'un fichier numérique selon l'invention. Le lecteur lit le code-barres signé contenant l'adresse d'un fichier numérique sur un serveur de données et un élément de contrôle d'intégrité de ce fichier numérique. Il vérifie ce code-barres par sa signature électronique en contactant si nécessaire un serveur de signature, et transmet ensuite l'adresse du fichier numérique au serveur de données contenant le fichier numérique. Il reçoit en retour le fichier numérique et le vérifie par l'élément de contrôle d'intégrité.

Exposé de l'invention

[0011] L'invention est un ensemble de données sécurisé comprenant
- d'une part un fichier numérique situé sur un serveur accessible à une adresse,
- et d'autre part une donnée numérique ou alphanumérique ci-après dénommée message-signifiant comportant un moyen d'obtenir ladite adresse,
- ledit message-signifiant étant signé électroniquement,
caractérisé en ce que ledit message-signifiant contient également des informations complémentaires permettant de rendre ledit fichier numérique intelligible et/ou un élément de contrôle d'intégrité dudit fichier numérique.

Description détaillée de l'invention

[0012] Le principe de la présente invention est de séparer un fichier numérique situé sur un serveur accessible par un réseau à une adresse, du message-signifiant signé électroniquement comportant cette adresse ou un moyen de l'obtenir, et de munir ce message-signifiant d'un élément de contrôle d'intégrité dudit fichier numérique. Ce serveur peut être situé sur un ordinateur ou un Smartphone de l'émetteur de l'ensemble de données sécurisé, mais il est avantageusement distant et protégé contre des consultations non autorisées.

[0013] Cet élément de contrôle est par exemple un hash ou une checksum.

[0014] L'adresse est avantageusement compliquée pour être imprévisible.

[0015] Pour prendre un exemple, le message-signifiant contient les informations d'identité d'une personne, et le fichier numérique est sa photo d'identité en haute résolution, ou des données biométriques permettant de le reconnaître. Ces informations ne peuvent être obtenues du serveur qu'en envoyant au serveur qui les contient leur adresse ou leur référence. Dans une version perfectionnée, ce n'est pas l'adresse réelle qui est contenue dans le message-signifiant, mais un lien permettant de l'obtenir après avoir justifié d'une autorisation conforme

[0016] Une version dégradée du fichier numérique peut être jointe au message-signifiant. Le message-signifiant peut par exemple être imprimé ou affiché sur une copie de cette version.

[0017] Avantageusement la photo n'est accompagnée sur le serveur d'aucune autre information que son adresse ou référence, de telle sorte qu'un piratage de ce serveur ne permette pas de reconstituer des données d'informations, par exemple des bases de données d'identités ou des cartes d'identité.

[0018] Un serveur web ou une page web ou n'importe quel document ou produit peuvent être munis d'un message-signifiant servant par exemple à vérifier l'identité de leur propriétaire, et ce message-signifiant peut être vu sous forme de lien html ou sous forme de code-barres ou sous toute autre forme.

[0019] Un fichier numérique peut être une représentation sous forme d'image de tout ou partie des informations contenues dans le message-signifiant. Ce peut par exemple être la copie d'une ordonnance dont les détails sont indiqués dans le message-signifiant.

[0020] Pour émettre un tel ensemble de données sécurisé, l'émetteur dépose une copie d'un fichier numérique sur un serveur de données accessible par un réseau à une adresse, et émet un message-signifiant signé électroniquement comportant un élément de contrôle d'intégrité de ce fichier numérique et un moyen comme l'adresse permettant d'y accéder.

[0021] Pour lire et certifier le document, le lecteur lit le message-signifiant signé, en vérifie l'intégrité et l'authenticité par sa cohérence avec la signature numérique, vérifie la non-répudiation de la signature numérique, télécharge du serveur de données le fichier numérique à partir de l'adresse et vérifie l'intégrité et l'authenticité du fichier numérique par l'élément de contrôle d'intégrité.

[0022] Dans une variante, le lecteur peut aussi lire le message-signifiant signé, en vérifier l'intégrité et l'authenticité par sa cohérence avec la signature numérique, vérifier la non-répudiation de la signature numérique, envoyer au serveur de données l'élément de contrôle d'intégrité, pour que le serveur vérifie l'intégrité et l'authenticité du fichier numérique et mette à disposition une copie modifiée, par exemple dégradée, du fichier numérique, et télécharger du serveur la copie modifiée.

[0023] Cette copie modifiée peut par exemple être dans une résolution inférieure, ou ne comporter qu'une partie du fichier numérique ou encore avoir reçu de subtiles modifications de couleurs pour être unique. Cela garantit que le lecteur ne pourra pas reconstruire un fichier identique à celui qui est hébergé sur le serveur de données.

[0024] Le procédé de lecture et de certification selon l'invention peut comporter une procédure d'identification de la personne le mettant en œuvre, pour qu'aucune information se rapportant au fichier numérique ne soit transmise sans que cette procédure d'identification ait conduit à autoriser une telle transmission. Cela a

l'avantage d'éviter le téléchargement abusif des données contenues dans le fichier de données.

[0025] Dans une variante préférée pour l'application de la présente invention à l'identification des personnes par biométrie, le fichier numérique conservé par le serveur et mis à disposition du lecteur est partiel pour être inintelligible, et il ne peut être lu que par combinaison avec des éléments du fichier numérique complet qui sont inclus dans le message-signifiant. Ceci garantit qu'un pirate ayant accès au serveur de fichiers ou écoutant une conversation entre ce serveur et un lecteur ne pourra pas rétablir une copie intelligible du fichier numérique. L'élément de contrôle d'identité peut se rapporter aussi bien au fichier partiel inintelligible qu'au fichier complet obtenu par combinaison du fichier transmis avec des éléments du fichier numérique complet qui sont inclus dans le message-signifiant.

[0026] Voici à titre d'exemple le fonctionnement d'un service d'émission de documents sécurisés.

[0027] Etape 1 : après s'être identifié selon une méthode d'identification convenue (par exemple par la combinaison d'un identifiant et d'un mot de passe ou par identification forte), l'émetteur envoie au serveur de l'opérateur une requête comportant deux ensembles d'informations :

- des informations à inclure dans le message-signifiant dites informations-code,
- des informations formant le ou les fichiers numériques,

et les paramètres de l'opération comme par exemple :

- la nécessité ou non de vérifier l'identité du ou des lecteur(s) et le cas échéant les éléments d'identité à vérifier,
- la forme complète ou dégradée sous laquelle le ou les fichier(s) numérique(s) doi(ven)t être fournie à l'émetteur s'il en demande le téléchargement, cette forme pouvant être différente selon les lecteurs.

Dans une variante, le serveur de l'opérateur reçoit des informations et en déduit selon une règle convenue les informations à inclure dans le message-signifiant, celles formant le fichier numérique, et les paramètres de l'opération.

[0028] Etape 2 : le serveur de l'opérateur

- calcule à partir du ou des fichiers numériques un élément de contrôle d'intégrité du ou des fichiers numérique(s), ou de plusieurs éléments de contrôle correspondant chacun à un ou plusieurs fichiers numériques,
- stocke le(s) fichier(s) numérique(s) sur un serveur de fichiers numériques (qui peut être le serveur de l'opérateur),
- compose un message-signifiant signé contenant
- les informations-code,

- l'adresse du serveur de fichiers et la référence ou les références du ou des fichier(s) numérique(s) sur ce serveur de fichiers,
- le ou les élément(s) de contrôle d'intégrité du ou des fichier(s) numérique(s),
- et la signature numérique de cet ensemble,
- et transfère le message-signifiant signé à l'émetteur, en réponse à sa requête, ainsi optionnellement qu'une copie du ou des fichier(s) numérique(s).

Dans une variante préférée pour l'application de la présente invention à l'identification des personnes par biométrie, le serveur de l'opérateur répartit les informations formant le fichier numérique reçu de l'émetteur en deux parties, la première étant intégrée au fichier numérique qui est stocké sur le serveur et la seconde étant intégrée dans le message-signifiant. Cela a pour effet que le fichier numérique est inintelligible et ne peut le devenir que pour le destinataire disposant du message-signifiant et pouvant de ce fait le combiner avec la partie manquante qui est inclue dans le message-signifiant.

[0029] Etape 3 : l'émetteur communique à un ou plusieurs lecteur(s) le message-signifiant signé, soit seul soit accompagné d'une copie du ou des fichier(s) numérique(s) qui peu(ven)t être modifié(s) (à une plus faible résolution par exemple).

[0030] Etape 4 : un lecteur

- lit le message-signifiant signé, ce qui lui communique
- les informations-code,
- l'adresse du serveur de fichiers et la ou les références du ou des fichier(s) numérique(s),
- le ou les élément(s) de contrôle d'intégrité de ce ou ces fichier(s) numérique(s),
- et la signature numérique de ce message-signifiant signé, et le cas échéant la ou les copie(s) du ou des fichier(s) numérique(s) qui lui ont été communiqués avec le message-signifiant,
- vérifie ou faire vérifier l'intégrité et l'authenticité par sa cohérence avec ladite signature numérique,
- vérifie ou fait vérifier la non-répudiation de la signature numérique,
- s'identifie auprès du serveur de l'opérateur selon la méthode d'identification convenue si une telle identification est prévue par les paramètres,
- indique au serveur de l'opérateur la référence la ou les références (s) lue(s) dans le message-signifiant signé,
- et, selon les paramètres de l'opération :
- ou bien reçoit le ou les fichiers dont la fourniture est prévue et vérifie leur compatibilité avec le ou les élément(s) de contrôle d'intégrité du ou des fichier(s),
- ou bien envoie au serveur le ou les élément(s) de contrôle reçus, pour que le serveur vérifie la compatibilité avec le ou les fichier(s) numériques avant de les lui transmettre, optionnellement sous forme modifiée,

- ou bien envoie au serveur la copie du ou des fichier numérique(s) qu'il a reçue(s) et le ou les élément(s) de contrôle reçus, pour que le serveur lui indique si cette ou ces copie(s) est (sont) bien représentative(s) du ou des fichier(s) numérique(s) correspondant(s).

Dans la variante préférée pour l'application de la présente invention à l'identification des personnes par biométrie, le lecteur reçoit le ou les fichiers inintelligible(s) dont la fourniture est prévue et les complète avec la ou les partie(s) du ou des fichier(s) d'origine intégrée(s) dans le message-signifiant, vérifie leur compatibilité avec le ou les élément(s) de contrôle d'intégrité du ou des fichier(s) inintelligibles reçus ou à ce fichier complété par la ou les partie(s) du ou des fichier(s) d'origine intégrée(s) dans le message-signifiant.

[0031] Divers perfectionnements peuvent être envisagés :

[0032] Un fichier numérique peut être découpé en morceaux séparés, et placés à des adresses qui n'ont pas de lien entre elles, de telle sorte que personne ne puisse les rassembler sans disposer du message-signifiant. Il peut aussi être crypté et ne pouvoir être décrypté que par l'émetteur ou l'opérateur du serveur de l'opérateur.

[0033] Tout ou partie du contenu du message-signifiant peut être crypté par le serveur de l'opérateur, le seul à connaître cette clé, et c'est lors de l'envoi du message-signifiant au serveur qu'a lieu le décryptage. Dans le cas où l'accès au serveur est limité par des autorisations dont doit disposer le lecteur, personne d'autre que lui ne peut lancer ce décryptage. Le message-signifiant ne peut pas être décrypté par le lecteur mais uniquement par l'opérateur du serveur de l'opérateur ou par l'émetteur.

[0034] Tout ou partie du fichier numérique stocké sur le serveur et pouvant être téléchargé par le lecteur est crypté avec une clé qui est incluse dans le message-signifiant. Ce cryptage peut être spécifique à chaque fichier numérique pour être unique, ce qui fait que la connaissance d'une règle de cryptage se rapportant à un fichier numérique ne peut pas permettre de déchiffrer un autre fichier numérique.

[0035] Le fichier numérique peut comporter une date de péremption ou être associé à une telle date, de telle sorte qu'après la date considérée, il ne puisse plus être téléchargé.

[0036] Un fichier numérique peut-être invalidé par une légère modification, pratiquée par l'opérateur ou par l'émetteur s'il est autorisé à la provoquer. Elle a pour conséquence une incompatibilité entre l'élément de contrôle et le fichier qui devient donc invalide. Cette modification peut être conçue pour être imperceptible et ne pas empêcher la conception d'un nouveau message-signifiant pour remettre en service le fichier numérique en l'état.

[0037] L'opérateur peut délivrer différents codes-barres comportant des informations différentes, par exemple des informations partielles. Cela permet par exemple à une

administration publique de délivrer des certificats de majorité pour la consultation de sites internet pour adultes.

[0038] L'opérateur peut délivrer des codes-barres permettant d'identifier une personne par sa photographie d'identité, le message-signifiant ne contenant qu'un pseudonyme en lieu et place des détails d'identité du titulaire. Ce dernier pourra signer des messages de son pseudonyme, apparaître comme quelqu'un qui ne veut pas donner son identité réelle tout en montrant qu'elle existe bel et bien et pourra être révélée par l'opérateur dans certaines conditions, par exemple par une décision de justice.

[0039] Les principaux avantages de la présente invention sont que,

- par la lecture du message-signifiant, le lecteur peut vérifier l'intégrité des informations-code et des fichiers numériques,
- la signature du message-signifiant peut être révoquée,
- les fichiers numériques sont stockés sur un moyen de stockage qui peut être mieux sécurisé que celui de l'émetteur,
- les fichiers numériques peuvent être rendus inexploitables par le cryptage, le découpage en morceaux comme exposé plus haut,
- les fichiers numériques sont stockés séparément des informations-code ce qui empêche un pirate de les rassembler pour former une information complète,
- la lecture des fichiers numériques peut être réservée aux seules personnes autorisées.

Applications

[0040] Les principales applications sont

- l'identité numérique dont le titulaire peut ne conserver qu'un message-signifiant signé, sous forme imprimée ou électronique pour s'identifier,
- les ordonnances médicales, certificats et attestations de toutes natures, contrats, bons de commande, factures, etc. qui deviennent aisément authentifiables par leurs lecteurs,
- les services de musique ou vidéo à la demande, les journaux et magazines, les jeux vidéo, les moyens de contrôle des objets connectés,
- et d'une façon générale la sécurisation de tout type de données volumineuses ou sensibles.

Revendications

[Revendication 1] Ensemble de données sécurisé comprenant
- d'une part un fichier numérique situé sur un serveur accessible à une adresse,
- et d'autre part une donnée numérique ou alphanumérique ci-après dénommée message-signifiant comportant un moyen d'obtenir ladite adresse,
- ledit message-signifiant étant signé électroniquement,
caractérisé en ce que ledit message-signifiant contient également des informations complémentaires permettant de rendre ledit fichier numérique intelligible et/ou un élément de contrôle d'intégrité dudit fichier numérique.

[Revendication 2] Ensemble de données sécurisé selon la revendication 1 caractérisé en ce que le fichier numérique est partiel pour être inintelligible, et ne peut être lu que par combinaison avec des éléments inclus dans le message-signifiant.

[Revendication 3] Procédé d'émission de documents sécurisés selon la revendication 1 ou la revendication 2 comprenant les étapes suivantes :
- Etape 1 réalisée par l'émetteur: envoi à un serveur dit serveur de l'opérateur d'une requête comportant deux ensembles d'informations :
- des informations dites informations-code à encoder dans le message-signifiant,
- des informations formant ledit fichier numérique,
- Etape 2 réalisée par ledit serveur de l'opérateur :
- calcul, à partir dudit fichier numérique, d'un élément de contrôle d'intégrité dudit fichier numérique,
- stockage dudit fichier numérique sur un serveur de fichiers numériques,
- composition d'un message-signifiant contenant
- lesdites informations-code,
- l'adresse dudit serveur de fichiers et la référence dudit fichier numérique sur ledit serveur de fichiers,
- ledit élément de contrôle d'intégrité dudit fichier numérique,
- et ladite signature numérique de cet ensemble,
- transfert dudit message-signifiant signé audit émetteur, en réponse à sa requête, ainsi optionnellement qu'une copie du fichier numérique.

[Revendication 4] Procédé d'émission de documents sécurisés selon la revendication 3 comprenant en outre une étape 3 réalisée par ledit émetteur consistant à communiquer à un lecteur ledit message-signifiant signé, soit seul soit accompagné d'une copie dudit fichier numérique qui peut optionnellement être dégradée.

[Revendication 5] Procédé de lecture et de certification d'un ensemble de données sécurisé selon la revendication 1 ou la revendication 2 consistant
- à lire ledit message-signifiant signé,
- à en vérifier ou faire vérifier l'intégrité et l'authenticité par sa cohérence avec ladite signature numérique,
- à vérifier ou faire vérifier la non-répudiation de ladite signature numérique,
- à télécharger ledit fichier numérique à partir de ladite adresse,
- et à vérifier l'intégrité et l'authenticité dudit fichier numérique par ledit élément de contrôle d'intégrité.

[Revendication 6] Procédé de lecture et de certification d'un ensemble de données sécurisé selon la revendication 1 ou la revendication 2 consistant
- à lire ledit message-signifiant signé,
- à en vérifier ou faire vérifier l'intégrité et l'authenticité par sa cohérence avec ladite signature numérique,
- à vérifier ou faire vérifier la non-répudiation de ladite signature numérique,
- à envoyer audit serveur ledit élément de contrôle d'intégrité, pour que ledit serveur vérifie l'intégrité et l'authenticité dudit fichier numérique, et mette à disposition dudit lecteur ledit fichier numérique ou une copie modifiée de ce fichier numérique,
- à télécharger dudit serveur ledit fichier ou ladite copie modifiée de ce fichier.

[Revendication 7] Procédé de lecture et de certification d'un ensemble de données sécurisé selon la revendication 1 ou la revendication 2 consistant
- à lire ledit message-signifiant signé,
- à en vérifier ou faire vérifier l'intégrité et l'authenticité par sa cohérence avec ladite signature numérique,
- à vérifier ou faire vérifier la non-répudiation de ladite signature numérique,
- à envoyer audit serveur une copie dudit fichier numérique et ledit élément de contrôle reçus préalablement par ledit émetteur, pour que

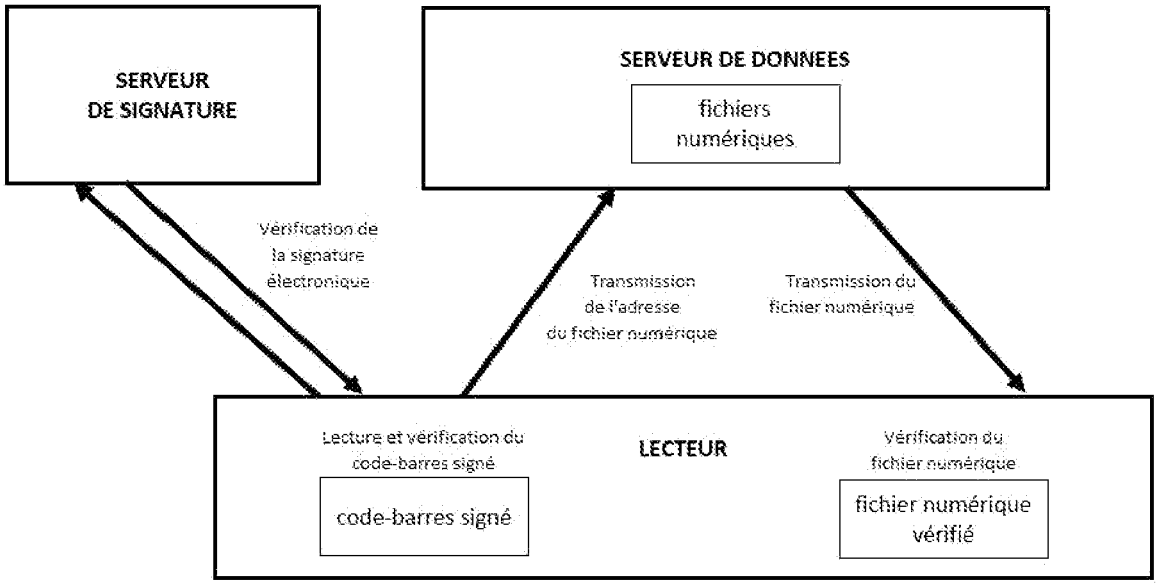
le serveur indique audit lecteur si ladite copie est bien représentative dudit fichier numérique.

[Revendication 8] Procédé de lecture et de certification selon l'une quelconque des revendications 5 à 7 caractérisée en ce qu'il comporte une procédure d'identification du lecteur la mettant en œuvre, et qu'aucune information se rapportant audit fichier numérique ne soit transmise sans que cette procédure d'identification ait conduit à autoriser une telle transmission.

[Revendication 9] Ensemble de données sécurisé émis selon la revendication 3 ou la revendication 4 caractérisé en ce que tout ou partie dudit message-signifiant est crypté et ne peut pas être décrypté par ledit lecteur.

[Revendication 10] Ensemble de données sécurisé émis selon la revendication 3 ou la revendication 4 caractérisé en ce que le fichier numérique est découpé en morceaux séparés situés à des adresses qui n'ont pas de lien entre elles.

[Fig. 1]


SERVEUR
DE SIGNATURE
SERVEUR DE DONNEES
fichiers
numériques
Vérification de
la signature
électronique
Transmission
de l'adresse
du fichier numérique
Transmission du
fichier numérique
Lecture et vérification du
code-barres signé
LECTEUR
Vérification du
fichier numérique
code-barres signé
fichier numérique
vérifié