

①9 RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

①1 N° de publication :

2 967 276

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

②1 N° d'enregistrement national :

10 59291

⑤1 Int Cl⁸ : G 06 F 21/24 (2012.01), G 06 F 21/22, H 04 L 9/00,
G 06 Q 30/00

⑫

DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 10.11.10.

③0 Priorité :

④3 Date de mise à la disposition du public de la
demande : 11.05.12 Bulletin 12/19.

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) : NETHEOS Société par actions simpli-
fiée — FR.

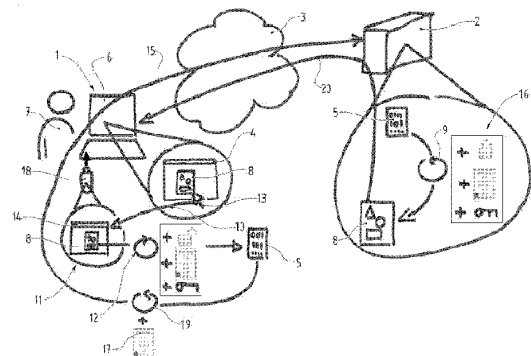
⑦2 Inventeur(s) : FACELINA XAVIER et DETOUR OLI-
VIER.

⑦3 Titulaire(s) : NETHEOS Société par actions simplifiée.

⑦4 Mandataire(s) : CABINET BREV&SUD.

⑤4 TRANSMISSION DE DONNEES NUMERIQUES SOUS FORME D'IMAGE AVEC GLISSER-DEPOSER.

⑤7 La présente invention concerne un procédé de transmission de données numériques (5), dans lequel un utilisateur (7) se connecte depuis un terminal client (1) vers un serveur (2) via un navigateur (4); ledit terminal client (1) initie une transaction; ledit serveur (2) transmet audit terminal client (1) des données numériques (5) relatives à ladite transaction; caractérisé en ce que: ledit serveur (2) encapsule lesdites données (5) sous forme d'image (8); ledit serveur (2) transmet ladite image (8) vers ledit terminal client (1); ladite image (8) est affichée par ledit navigateur (4) au niveau dudit terminal client (1); ledit utilisateur (7) effectue une action de glisser-déposer (10) de ladite image (8) affichée vers une application distincte (11); ladite application (11) récupère à partir de ladite image (8) lesdites données encapsulées (5). L'invention concerne aussi le dispositif (18) de mise en oeuvre d'un tel procédé.



FR 2 967 276 - A1



La présente invention entre dans le domaine informatique de la sécurisation des communications.

L'invention concerne plus particulièrement la sécurisation lors de la transmission de données numériques, notamment une
5 transaction, au sein d'un réseau de communication, préférentiellement de type informatique, notamment Internet.

L'invention trouvera une application préférentielle, mais aucunement limitative, dans la sécurisation lors de la transmission de données sensibles ou à risques, par exemple des
10 données ou transactions bancaires, effectuée au travers d'un réseau informatique.

L'invention trouvera en outre une application particulière dans la signature électronique de transaction bancaire.

De manière connue, lors d'un échange de données numériques
15 sur un réseau de communication, un utilisateur se connecte depuis un terminal client vers un serveur, la plupart du temps un serveur distant, connecté à un portail virtuel accessible au travers dudit réseau par l'intermédiaire d'un navigateur s'exécutant sur ledit terminal client.

20 La sécurisation de données lors de leur transmission sur un réseau informatique, tel Internet, s'effectue au niveau de la couche réseau au travers de connexions entre le client et le serveur utilisant des protocoles de chiffrement (tel TLS pour « Transport Layer Security »).

25 La réponse est moins évidente au niveau de la couche applicative, pour laquelle aucune norme de sécurité n'a été implémentée dans l'ensemble des navigateurs déployés auprès des clients. C'est pour cette raison que certaines applications au niveau du serveur utilisent les capacités d'extension dynamique
30 des navigateurs afin d'effectuer des opérations locales de sécurité.

C'est pourtant à cause de cette même faculté d'extension que la réception, le traitement et l'affichage des données au niveau du navigateur du client n'est pas forcément assurée de
35 manière sûre, notamment en cas de corruption dudit navigateur par un logiciel tiers, tel un « malware ».

A titre d'exemple, il est connu des logiciels malveillants communément appelés « chevaux de Troie » (Trojan). Ils s'installent au niveau du terminal client, de manière invisible pour l'utilisateur, et interviennent au moment de la transmission de données entre le serveur et ledit client, afin de récupérer ou falsifier les données sensibles reçues et émises, et notamment leur affichage. Dans le cadre d'une transmission de type transaction bancaire, un tel logiciel peut récupérer les autorisations bancaires de l'utilisateur ou simplement modifier les paramètres de la transaction (par exemple : le destinataire et le montant).

En somme, les logiciels utilisés pour la navigation se focalisent sur la nécessité d'obtenir de bonnes fonctionnalités, plutôt que d'assurer une sécurité infaillible. Il convient donc d'améliorer la sécurisation de la transmission des données au niveau de la couche applicative.

Un navigateur n'étant donc pas nécessairement prévu pour effectuer des opérations offrant un degré de sécurité satisfaisant, il a été imaginé de dédier l'aspect sécuritaire à des applications tierces spécifiques. Toutefois, aucune d'entre elles ne s'affranchit de l'utilisation peu sécurisée dudit navigateur.

L'invention a pour but de pallier les inconvénients de l'état de la technique en proposant un système de transmission de données numériques sans adhérence, entre le navigateur et une application tierce entièrement dédiée à la sécurité.

En particulier, un tel système s'affranchit de toute installation logicielle complémentaire sur ledit navigateur, qui devient alors un simple média de transmission, sans aucun risque de compromission, même s'il venait à être corrompu.

Pour ce faire, l'invention prévoit une encapsulation des données transmises depuis le serveur sous une forme compatible avec tout type de navigateur, sans nécessiter l'installation d'aucune application complémentaire. Plus précisément, l'encapsulation au sens de l'invention consiste à introduire au sein d'une image, plus particulièrement d'un fichier d'une

image numérisée, les données numériques, puis de les transférer sous cette forme vers le terminal client, en particulier le navigateur afin qu'il affiche ladite image. L'utilisateur sera alors à même de récupérer ladite image affichée pour la
5 transmettre à une application distincte, dédiée à la sécurité.

Dès lors, l'utilisation d'une image, au sein de laquelle sont introduites des données, offre une compatibilité totale avec tous les systèmes et navigateurs existants, sans installation préalable de logiciel ou de module complémentaire
10 au navigateur.

Par ailleurs, la récupération des données encapsulées au sein de l'image s'effectue automatiquement au niveau de l'application dédiée à la sécurité, sans faire intervenir l'utilisateur ou le navigateur. Cette étape est alors
15 entièrement invisible, limitant les risques d'erreur de saisie et s'affranchissant d'étapes complexes, fastidieuses et plus longues en temps.

Une fois les données récupérées par l'application, elles peuvent être affichées en dehors du navigateur pour une
20 utilisation locale, notamment une validation, et éventuellement le renvoi d'informations vers le serveur, directement depuis l'application tierce, sans passer par le navigateur.

De plus, l'utilisation d'une image offre une ergonomie améliorée et simplifie les manipulations par l'utilisateur. En effet, il est alors possible d'effectuer un glisser-déposer (« drag-and-drop ») ou un copier-coller de l'image, opération
25 très instinctive, rapide et sans risque d'erreur, même pour un utilisateur novice. Ainsi, le système sécurisé selon l'invention comprend un procédé sécurisé de transaction de données numériques.
30

Pour ce faire, dans un tel procédé, un utilisateur se connecte depuis un terminal client vers un serveur au travers d'un réseau de communication, notamment informatique, par l'intermédiaire d'un navigateur s'exécutant sur ledit terminal
35 client ; ledit terminal client initie une transaction ; ledit serveur transmet audit client des données numériques relatives

à ladite transaction.

Ledit procédé selon l'invention se caractérise en ce que ledit serveur encapsule lesdites données sous forme d'image ; ledit serveur transmet ladite image vers ledit terminal client ; ladite image est affichée par ledit navigateur au niveau dudit terminal client ; ledit utilisateur effectue une action de glisser-déposer de ladite image affichée vers une application distincte ; ladite application récupère à partir de ladite image lesdites données encapsulées.

10 L'invention concerne aussi un dispositif amovible de mise en œuvre d'un tel procédé.

Un tel dispositif amovible de transmission de données numérique comprend des moyens de connexion à un terminal et des moyens de stockage de données personnelles à un utilisateur, lesdits moyens de stockage se présentant sous forme d'une mémoire, caractérisé par le fait que ladite mémoire comprend au moins une application de mise en œuvre du procédé selon l'invention.

20 D'autres caractéristiques et avantages de l'invention ressortiront de la description détaillée qui va suivre des modes de réalisation non limitatifs de l'invention, en référence à la figure unique annexée représentant schématiquement l'architecture et les étapes du système de transmission de données numériques selon l'invention.

25 La présente invention concerne un système sécurisé de transmission de données numériques.

Ladite transmission s'effectue par une connexion entre un terminal client 1 et un serveur 2 au travers d'un réseau de communication 3.

30 Dans le mode préférentiel de réalisation, aucunement limitatif, ladite transmission s'effectue par une connexion au travers d'un réseau informatique 3, tel Internet, entre un serveur 2 informatique distant un terminal 1 client de type ordinateur personnel.

35 Plus particulièrement, un utilisateur se connecte depuis ledit terminal client 1 vers ledit serveur 2 par

l'intermédiaire d'un navigateur 4.

Ledit navigateur 4 est un logiciel s'exécutant localement au niveau dudit terminal client 1. Il permet de se connecter audit serveur distant 2, notamment à un portail virtuel dudit serveur 2, et d'échanger des données 5 entre ledit terminal client 1 et ledit serveur 2, dans un sens comme dans l'autre. De plus, ledit navigateur 4 permet de visualiser les informations transmises par ledit serveur 2, au travers de moyens d'affichage 6 propres audit terminal client 1, tel un écran.

De plus, ledit navigateur 4 peut intégrer les éléments logiciels nécessaires pour sécuriser les connexions entre le terminal client 1 et ledit serveur 2, notamment une connexion de type HTTPS ou TLS. Dès lors, pour protéger l'étape de transmission des données 5 entre ledit terminal client 1 et ledit serveur 2, ladite connexion peut être sécurisée, mais pas nécessairement.

A ce titre, on notera que lesdites données 5 peuvent consister au moins en partie en des informations numérisées et dédiées à ladite transmission. Ces données peuvent être sensibles, à savoir qu'on doit en assurer la confidentialité, en interdisant l'accès par un tiers, et qu'on doit en vérifier l'authenticité, c'est à dire l'intégrité et la provenance.

Pour ce faire, ledit utilisateur 7 initie au moins une transaction de données numériques depuis le terminal client 1 vers ledit serveur 2. Cette transaction peut être demandée en envoyant une requête audit serveur 2.

Cette requête inclut des données préalablement échangée entre le client 1 et le serveur 2, ou un autre serveur distant (non représenté).

Par exemple, dans le cadre d'une transaction bancaire, cette requête peut comprendre les données liées au montant de la transaction s'effectuant entre un serveur (le vendeur ou la banque du vendeur ou de l'acheteur) et le client 1 (l'acheteur), ainsi que les données de la carte bancaire de l'acheteur.

A réception de ladite requête, ledit serveur 2 transmet des données relatives 5 à ladite transaction vers ledit terminal client 1.

Un avantage de la présente invention réside dans le choix
5 d'un format d'encapsulation spécifique des données envoyées 5, format qui s'affranchit de toute contrainte au niveau du navigateur 4 du terminal client 1. En somme, un tel format est compatible avec tout type de navigateur 4, sans ajout de logiciels complémentaires ou de configuration particulière au
10 niveau dudit navigateur 4. Ce dernier ne sert alors que de média de transmission de sorte que les données 5 transmises par le serveur 2 n'aient même pas été affichées dans le terminal client 1.

Pour ce faire, le procédé consiste à encapsuler 9 dans une
15 image 8 lesdites données 5.

En particulier, cette encapsulation 9 s'effectue au niveau dudit serveur 2, en introduisant lesdites données 5 de la transaction au sein d'un fichier de type image 8, à savoir qu'il s'agit d'un fichier contenant des données numériques
20 correspondant à une représentation numérique compressée d'une image 8.

A titre d'exemple non limitatif, un tel fichier peut être d'un format d'enregistrement, lié à son algorithme d'encodage et de décodage, largement répandu et lisible par tous les
25 navigateurs, comme le format de JPEG (pour « Joint Photographic Experts Group »), GIF (pour « Graphic Interchange Image »), BMP (pour « BitMaP ») ou tout autre format adapté.

Selon différents modes de réalisation, l'insertion des données 5 au sein du fichier image 8 peut consister à copier
30 lesdites données 5 dans une partie du fichier, notamment au sein de l'entête d'un tel fichier, ou bien à introduire les données directement dans une partie de la visualisation de l'image 8, de manière visible ou non pour l'utilisateur 7 (typiquement par stéganographie).

35 Une fois encapsulées sous forme d'image 8, lesdites données 5 de la transaction sont transmises 20 depuis ledit

serveur 2 vers ledit terminal client 1. Cette image 8 est affichée par ledit navigateur 4 au niveau dudit terminal client 1.

En somme, dans le cadre d'une connexion Internet, l'utilisateur 7 envoie une requête audit serveur 2 qui renvoie une page Web (pour « World Wide Web ») incluant ladite image 8, de sorte que le navigateur 4 affiche cette dernière, afin que l'utilisateur 7 puisse la visualiser et interagir avec.

Une action dudit utilisateur 7 peut alors consister en un glisser-déposer 10 (« drag and drop ») de ladite image 8 affichée vers une application distincte 11 à même de décapsuler 12 ladite image 8. Cette action 10 consiste à sélectionner ladite image 8 et à la déplacer, en vue de la placer au sein de ladite application 11. Ce déplacement peut s'effectuer par l'intermédiaire de moyens classiques utilisés sur ledit terminal client 1, notamment par le déplacement du curseur 13 sous l'action d'un périphérique commandé manuellement par l'utilisateur 7, telle une souris, une tablette tactile ou analogue.

Plus particulièrement, ladite application 11 est exécutée sur ledit terminal client 1, l'exécution s'effectuant préalablement à l'action de glisser-déposer 10 par l'utilisateur 7.

Comme évoqué précédemment, ladite application 11 permet, au cours de son exécution, de récupérer ladite image 8 lors de l'action de glisser-déposer 10. En somme, ladite application 11 permet de récupérer l'image 8 au moment de sa dépose par l'utilisateur 7.

On notera que l'action de glisser-déposer 10 de l'image 8 peut se traduire différemment en fonction du système d'exploitation s'opérant et le navigateur s'exécutant sur ledit terminal client. Selon le cas, le glisser-déposer 10 s'effectue par un transfert local du fichier image 8, notamment sous forme d'un fichier temporaire, pour être collé au sein de ladite application 11. Dans un autre cas, ladite application 11 reçoit un lien incluant l'adresse de ladite image 8 au niveau du

serveur 2. Dans cette seconde hypothèse, l'application 11 devra être en mesure de récupérer au niveau dudit serveur 2 ladite image 8 et les données 5 qu'elle contient.

Par ailleurs, afin de faciliter l'action de glisser-déposer 10, ladite application 11 peut, au cours de son exécution, afficher sur le terminal client 1 une fenêtre 14 de réception de ladite image 8, à l'intérieure de laquelle est déposée l'image 8 par l'utilisateur 7.

Ensuite, l'application 11 récupère à partir de ladite image 8 lesdites données encapsulées. Ainsi, l'application 11 assure la décapsulation 12 des données 5 à partir de l'image 8, ainsi que l'affichage des données décapsulées 5 au niveau dudit terminal client 1, au sein de l'application 11 et donc en dehors dudit navigateur 4.

Dans le cas spécifique d'une transaction, l'utilisateur 7 visualise sur le terminal client 1 un récapitulatif de l'intégralité de la transaction (montant, date, coordonnées bancaires, etc.). Il peut ainsi valider, ou non, les données ainsi affichées. En cas de validation, ladite application 11 peut renvoyer 15 les données validées directement audit serveur 2, en initiant une connexion entre l'application 11 et le serveur 2, sans passer par ledit navigateur 4, assurant une sécurité totale même si le navigateur 4 est corrompu.

Selon un mode préférentiel de réalisation, l'encapsulation 9 consiste préalablement à signer numériquement lesdites données 5. En somme, ledit serveur 2 signe toute ou partie des données 5 au moyen d'un protocole 16 et d'une clé cryptographique qui lui est propre, par exemple un certificat électronique, puis encapsule sous forme d'image 8 les données signées 5, puis transmet ladite image 8 vers ledit terminal client 1.

Au moment de la récupération des données 5, ladite application 11 est à même de vérifier la signature dudit serveur 2 en validant son authenticité, c'est à dire son intégrité et sa provenance.

En particulier, afin de permettre cette vérification, ledit serveur 2 peut transmettre son certificat électronique avec les données signées 5 ou au sein de ladite image 8.

Selon un autre mode de réalisation particulier, à défaut
5 de recevoir le certificat du serveur 2 dans l'image 8, ladite application 11 peut accéder au certificat ou à la clef publique attachés à la clef privée ayant servie à effectuer ladite signature du serveur 2.

Dès lors, l'application 11 sera à même de vérifier
10 l'authenticité des données 5 qui lui seront transmises. Le serveur 2, à savoir l'émetteur des données 5, peut être considéré comme sûr par le terminal client 1. L'utilisateur 7 est alors certain de manipuler des données 5 authentiques.

Dans le cas spécifique d'une transaction, l'application 11
15 affichera sur le terminal client 1 les données 5 vérifiées comme authentiques, de sorte que l'utilisateur 7 puisse les visualiser et les vérifier. Il devra à son tour les valider en les signant numériquement avec son propre matériel cryptographique avant de les renvoyer 15 au serveur 2. Cette
20 signature pourra nécessiter une authentification locale de l'utilisateur 7 auprès de ladite application 11. A réception, le serveur 2 pourra modifier l'état du navigateur 4 au niveau dudit terminal client 1, notamment en rafraichissant la page ou en redirigeant la page actuelle vers une nouvelle page.

Dans le cas spécifique d'une authentification de
25 l'utilisateur 7 au portail virtuel, l'application 11 n'affichera pas à l'utilisateur 7 les données vérifiées 5 comme authentiques. Ledit utilisateur 7 devra à son tour les valider, sans les visualiser, en les signant numériquement avec son
30 propre matériel cryptographique avant de les renvoyer au serveur 2. Cette signature pourra nécessiter l'authentification locale de l'utilisateur 7 auprès de ladite application 11. A réception et validation des données reçues, le serveur 2 pourra modifier l'état du navigateur 4 au niveau dudit terminal client
35 1, notamment en rafraichissant la page ou en redirigeant la page actuelle vers une nouvelle page, donnant notamment accès

au portail et aux services proposés par ledit serveur 2.

Selon un mode alternatif de réalisation, l'encapsulation 9 consiste préalablement à chiffrer au moins en partie lesdites données 5, de manière à assurer leur confidentialité. Le
5 chiffrement des données 5 par le serveur 2 est prévu de sorte que ladite application 11 puisse les déchiffrer au moment de la récupération desdites données 5. Ce déchiffrement pourra nécessiter l'authentification locale de l'utilisateur 7 au niveau de ladite application 11.

10 Dès lors, le navigateur 4 n'est pas en possession des moyens cryptographiques permettant le déchiffrement des données chiffrées 5, même s'il était à même de les récupérer dans l'image 8 qu'il affiche. Il ne joue alors que le rôle d'intermédiaire, servant de média de transmission de l'image 8
15 depuis le serveur 2 vers ladite application 11.

Comme évoqué précédemment, ladite application 11 est exécutée sur ledit terminal client 1 et comprend une étape d'authentification locale dudit utilisateur 7. Au moment de l'exécution de ladite application 11, l'invention peut prévoir
20 de s'assurer que l'utilisateur 7 est autorisé à se servir de l'application 11 et des données associées. C'est pourquoi le procédé comprend une étape d'authentification locale dudit utilisateur 7, notamment par saisie d'un code ou mot de passe. En somme, au lancement de l'application 11, de manière
25 automatique, notamment avant ou au moment de la réception de l'image 8 lors de sa dépose, ou bien par une action volontaire dudit utilisateur 7, une fenêtre d'authentification s'ouvre pour permettre à audit utilisateur 7 de s'authentifier localement avec des informations connues de lui seul, tel un
30 code confidentiel de type code PIN (pour « Personal Identification Number »). Cette étape permet d'authentifier localement avec certitude l'utilisateur 7.

De plus, cette authentification locale permet à l'utilisateur 7 d'accéder à des données, en particulier des
35 données d'authentification ou des données personnelles, comme un certificat numérique 17 ou une clef privée propre à ladite

application 11 ou audit utilisateur 7, ses coordonnées bancaires, etc.

De telles informations peuvent être utiles pour déchiffrer les données 5 reçues, vérifier la signature du serveur 2, 5 signer 19 des données en retour, ainsi que l'une et/ou l'autre des étapes susmentionnées dans les différents modes de réalisation.

Avantageusement, le système sécurisé de transmission selon l'invention peut comprendre un dispositif 18 amovible pour la 10 sécurisation de la transmission desdites données 5.

Un tel dispositif amovible 18 de transmission de données numériques comprend des moyens de connexion à un terminal, en particulier le terminal client 1.

Selon le mode de réalisation préférentiel, ledit 15 dispositif 18 peut se présenter sous la forme d'une clef équipée d'une connectique universelle, comme le standard USB (pour « Universal Serial Bus »).

De plus, ledit dispositif 18 comprend des moyens de 20 stockage de données personnelles à un utilisateur 7, lesdits moyens de stockage se présentant sous forme d'une mémoire. Cette dernière peut se présenter sous la forme, d'une part, d'une carte à puce contenant des données sensibles et personnelles relatives audit utilisateur et qui nécessitent une authentification locale dudit utilisateur (notamment par saisie 25 d'un code PIN) pour y avoir accès et, d'autre part, un espace mémoire distinct, notamment sous forme de mémoire dite « FLASH ». Plus particulièrement, ladite mémoire, notamment l'espace de stockage « FLASH », comprend au moins une application 11 de mise en œuvre du procédé selon l'invention. 30 En somme, le dispositif intègre l'application 11 nécessaire pour décaspuler ladite image et récupérer les données.

Pour ce faire, au moment de la connexion du dispositif 18 sur le terminal client 1, l'application 11 qu'il contient s'exécute automatiquement ou sous l'action de l'utilisateur 7.

35 Dès lors, le traitement de la transaction par ladite application 11 ne laisse aucune trace sur le terminal client 1

utilisé. L'utilisateur 7 conserve avec lui toutes ses données personnelles et sensibles, en emportant le dispositif amovible 18 avec lui.

5 A ce titre, ladite application 11 peut prévoir de conserver une copie de la transaction effectuée, à savoir l'image 8 envoyée par ledit serveur 2 contenant les données 5 signées par ce dernier, ou bien directement les données signées, ou tout autre résumé de ladite transaction.

10 De plus, l'accès auxdites données contenues sur ledit dispositif 18 amovible peuvent être restreint, notamment à l'authentification locale de l'utilisateur 7 précédemment évoquée. De plus, les données peuvent être chiffrées et cryptées pour en limiter l'accès à tout tiers qui prendrait possession dudit dispositif.

15 En somme, un tel dispositif 18 consiste en des moyens d'authentification personnel et propre audit utilisateur 7. Il est prévu nomade, au travers de son aspect amovible, pour être emporté et conservé en possession de son utilisateur.

20 On notera que ladite application 11 peut aussi être directement installée et s'exécuter sur le terminal client.

Ainsi, le système sécurisé de transmission de données selon l'invention propose une application 11 tierce distincte entièrement dédiée à la sécurité, s'affranchissant des risques liés à l'intervention d'un navigateur 4 qui n'est utilisé alors
25 qu'en tant que simple média de transmission, n'affichant qu'une image 8 et non les données 5 sensibles qu'elle véhicule. Selon différents protocoles de cryptographie connus, l'origine, l'intégrité et la confidentialité de ses données peuvent être assurées.

30 L'invention trouvera également une application particulière dans la récupération de données habilitant un utilisateur 7 (c'est-à-dire lui conférant des droits/privilèges), temporairement ou de façon permanente, à un accès ou à une utilisation réciproquement d'un logiciel ou
35 service, local ou distant. Dans ce cas particulier, ladite application peut être dédiée audit logiciel ou service, local

ou distant. On notera qu'un logiciel ou service distant peut être hébergé et accessible au travers dudit réseau 3 vers un serveur identique ou distinct dudit serveur 2.

REVENDEICATIONS

1. Procédé de transmission de données numériques (5), dans lequel :
- 5 - un utilisateur (7) se connecte depuis un terminal client (1) vers un serveur (2) au travers d'un réseau de communication (3), notamment informatique, par l'intermédiaire d'un navigateur (4) s'exécutant sur ledit terminal client (1) ;
- ledit terminal client (1) initie une transaction ;
- 10 - ledit serveur (2) transmet audit terminal client (1) des données numériques (5) relatives à ladite transaction ;
- caractérisé en ce que :
- ledit serveur (2) encapsule lesdites données (5) sous forme d'image (8) ;
- 15 - ledit serveur (2) transmet ladite image (8) vers ledit terminal client (1) ;
- ladite image (8) est affichée par ledit navigateur (4) au niveau dudit terminal client (1) ;
- ledit utilisateur (7) effectue une action de glisser-déposer (10) de ladite image (8) affichée vers une application
- 20 distincte (11) ;
- ladite application (11) récupère à partir de ladite image (8) lesdites données encapsulées (5).
2. Procédé selon la revendication 1 caractérisé par le
- 25 fait que l'encapsulation consiste à introduire lesdites données (5) au sein d'un fichier de type image.
3. Procédé selon la revendication 2, caractérisé par le fait que l'encapsulation consiste préalablement à signer numériquement au moins en partie lesdites données (5).
- 30 4. Procédé sécurisé selon l'une des revendications 2 ou 3, caractérisé par le fait que l'encapsulation consiste préalablement à chiffrer au moins en partie lesdites données (5).
5. Procédé selon l'une quelconque des revendications
- 35 précédentes, caractérisé en ce que ladite application (11) est exécutée sur ledit terminal client (1) et comprend une étape

d'authentification locale dudit utilisateur (7), notamment par saisie d'un code ou mot de passe.

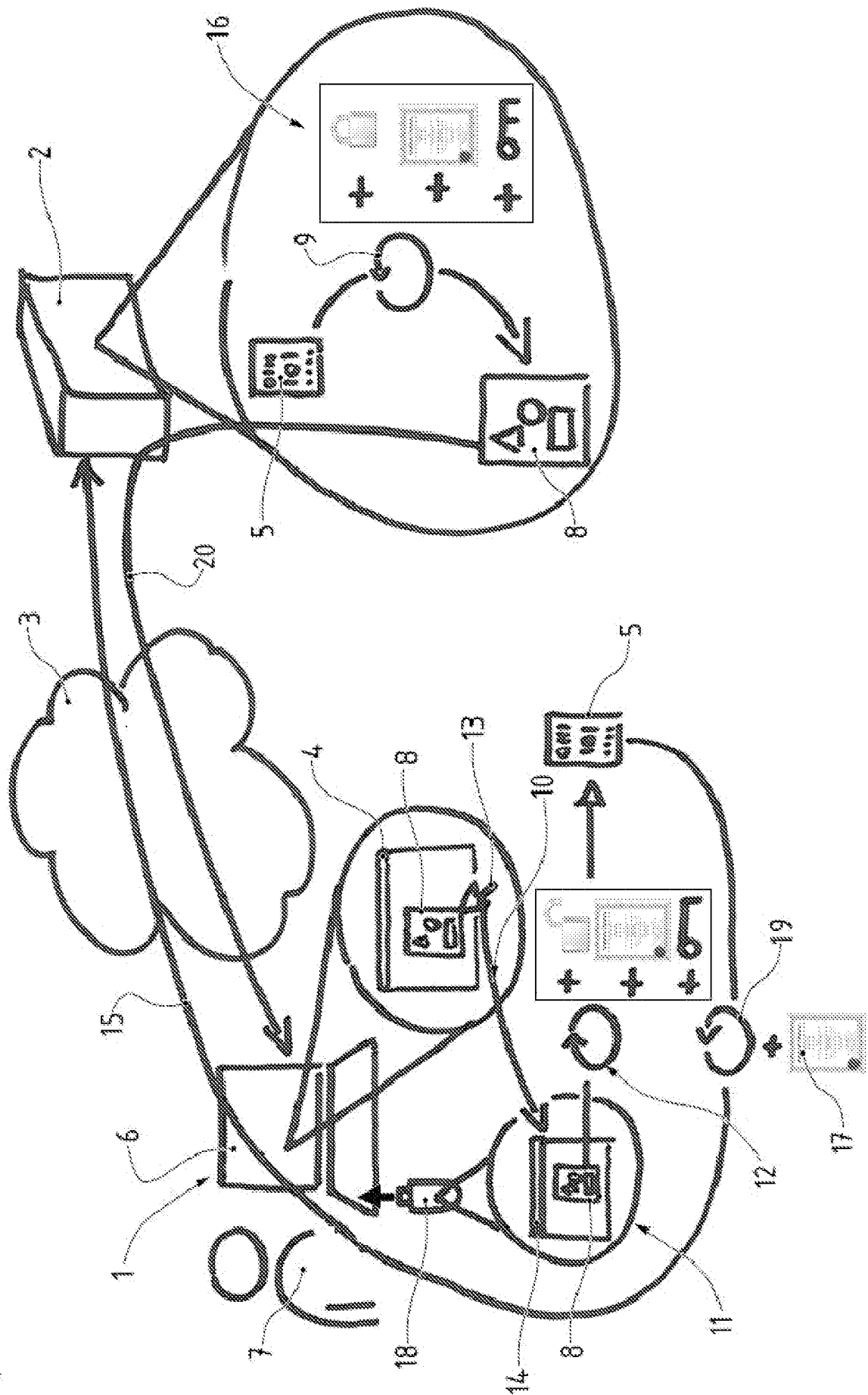
5 6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que ladite application (11) affiche lesdites données (5) récupérées, ledit utilisateur (7) valide lesdites données (5) affichées et ladite application (11) renvoie (15) les données (5) validées directement audit serveur (2).

10 7. Procédé selon la revendication 6, caractérisé en ce qu'il consiste à signer numériquement lesdites données (5) validées avant leur renvoi (15) par ladite application (11).

8. Procédé selon l'une quelconque des revendications 6 ou 7, caractérisé en ce qu'à réception et validation des données reçues (5), ledit serveur (2) modifie l'état du
15 navigateur (4) au niveau dudit terminal client (1).

9. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que lesdites données (5) sont des données habilitant ledit utilisateur (7), temporairement ou de façon permanente, à un accès ou une utilisation d'un
20 logiciel ou service, local ou distant.

10. Dispositif (18) amovible de transmission de données numérique, comprenant des moyens de connexion à un terminal et des moyens de stockage de données personnelles à un utilisateur (7), lesdits moyens de stockage se présentant sous
25 forme d'une mémoire, caractérisé par le fait que ladite mémoire comprend au moins une application (11) de mise en œuvre du procédé selon l'une quelconque des revendications précédentes.





RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 748150
FR 1059291

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	US 2009/288012 A1 (HERTEL PHILIPP FRANK HERMANN UDO [CA] ET AL) 19 novembre 2009 (2009-11-19) * alinéas [0253], [0259], [276] - [0277], [283] - [0284], [0409]; figures 32,35 *	1-10	G06F21/24 G06Q30/00 H04L9/00 G06F21/22
X	US 2008/130940 A1 (WHITELAW JAMES E [CA]) 5 juin 2008 (2008-06-05) * alinéas [0002] - [0004], [0 30], [0037] - [0040], [0 45] - [0046]; figures 7-8 *	1-10	
X	US 2009/187764 A1 (ASTAKHOV PAVEL [RU] ET AL) 23 juillet 2009 (2009-07-23) * le document en entier *	1-10	
A	US 2009/106556 A1 (HAMID LAURENCE [CA]) 23 avril 2009 (2009-04-23) * le document en entier *	1-10	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06F G06Q
Date d'achèvement de la recherche		Examineur	
8 juillet 2011		Veillas, Erik	
CATÉGORIE DES DOCUMENTS CITÉS		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	
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			

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1059291 FA 748150**

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 **08-07-2011**

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
US 2009288012 A1	19-11-2009	AU 2009249272 A1	26-11-2009
		CA 2728136 A1	26-11-2009
		EP 2294539 A1	16-03-2011
		WO 2009143084 A1	26-11-2009
		US 2011145049 A1	16-06-2011

US 2008130940 A1	05-06-2008	AUCUN	

US 2009187764 A1	23-07-2009	WO 2009091421 A1	23-07-2009

US 2009106556 A1	23-04-2009	AU 2008314461 A1	23-04-2009
		CA 2701055 A1	23-04-2009
		WO 2009049412 A1	23-04-2009
		EP 2213044 A1	04-08-2010
