(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 831 361**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **01 14075**

(51) Int Cl[7] : **H 04 L 9/30,** G 06 F 17/60

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 24.10.01.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 25.04.03 Bulletin 03/17.

(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) :** *GEMPLUS Société anonyme* — FR.

(72) **Inventeur(s) :** MERRIEN LIONEL et CARRARA JEAN LOUIS.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :**

(54) JETON INFORMATIQUE.

(57) Un procédé d'échange sécurisé d'informations lors de transactions de services ou de produits, impliquant un utilisateur, un vendeur et un fournisseur de services. L'utilisateur fournit au vendeur un jeton chiffré contenant les informations personnelles nécessaires à la transaction souhaitée. Le vendeur transmet ce jeton au fournisseur de services qui est en mesure de le déchiffrer et de le valider. L'utilisateur génère le jeton chiffré au moyen d'un dispositif électronique.

FR 2 831 361 - A1

JETON INFORMATIQUE

La présente invention a trait à un jeton informatique. Plus spécifiquement, la présente invention concerne un jeton informatique permettant de transmettre de façon confidentielle des informations personnelles.

Parallèlement à l'essor de l'utilisation de l'Internet comme outil de transaction de services et de produits, la protection des informations confidentielles devient une préoccupation importante des utilisateurs. En effet, il est de pratique courante, que ce soit pour accéder à un service ou pour acheter un produit sur l'Internet, que l'utilisateur doive remplir un formulaire en ligne et fournir un certain nombre de renseignements d'ordre personnel, tels que : adresse de courrier électronique, adresse postale, numéro de carte de débit ou de crédit, numéro de téléphone, numéro de sécurité sociale et autres informations personnelles du même type.

Il arrive fréquemment qu'une fois entrées en ligne afin d'obtenir un service ou pour effectuer un achat, ces informations se trouvent distribuées dans des bases de données, essentiellement sans que l'utilisateur n'ait aucun contrôle sur cette diffusion. C'est ainsi, par exemple, que l'utilisateur se voit figurer sur des listes de distribution promotionnelle ou autres, à son insu. De façon plus inquiétante, des informations confidentielles peuvent être ainsi disponibles sur le réseau Internet, exposées aux risques de piratage informatique et susceptibles d'utilisations non autorisées.

En règle générale, les étapes du processus de transaction de services ou de produits sur l'Internet sont les suivantes :

le vendeur demande à l'utilisateur d'entrer certaines informations personnelles, puis il les enregistre dans une base de données locale pour un usage ultérieur. Le moment voulu, le vendeur peut ainsi retrouver ces informations dans cette base de données et les transmettre à un fournisseur de services, par exemple une société de livraison de colis ou une institution bancaire. Celui-ci, à son tour, utilise alors les informations personnelles afin de procéder au service requis, puis détruit ces informations personnelles.

Une telle façon d'effectuer des transactions électroniques a l'avantage que le vendeur demande à l'utilisateur les informations dont il a besoin seulement une seule fois, lors de la première transaction. Par la suite, l'utilisateur n'a pas à fournir ces informations de nouveau à chaque nouvelle transaction. Cependant, ce faisant, l'utilisateur n'a aucun contrôle sur l'utilisation de ces données, une fois que le vendeur les a acquises.

Cette méthode de transactions consistant à fournir des informations personnelles, voire confidentielles, à un vendeur sur le réseau Internet, en perdant tout contrôle sur leur diffusion, n'est pas sans inquiéter de nombreux utilisateurs potentiels. Une méthode permettant l'échange sécurisé d'informations sur l'Internet contribuerait grandement à rassurer et convaincre ces utilisateurs inquiets.

Ainsi, une méthode, par laquelle le vendeur aurait la possibilité d'utiliser seulement une fois les informations dont il a besoin pour effectuer la transaction désirée par l'utilisateur, et qui garantit à l'utilisateur le contrôle des informations personnelles qui le concernent sur le réseau, renforcerait le développement des transactions électroniques.

Un objet de la présente invention est donc de présenter un jeton informatique permettant de transmettre de façon confidentielle des informations personnelles de l'utilisateur.

Selon l'invention, il est présenté un procédé d'échange sécurisé d'informations lors d'une transaction impliquant un utilisateur, un vendeur et un fournisseur de services, caractérisé en ce qu'il comprend les étapes suivantes :

création par l'utilisateur d'un jeton électronique chiffré contenant des informations nécessaires à la transaction, ces informations étant sélectionnées parmi un ensemble d'informations concernant l'utilisateur;

transmission du jeton électronique au fournisseur de services; et

déchiffrage et validation du jeton électronique par le fournisseur de services.

Également, selon l'invention, il est prévu un dispositif électronique permettant l'échange sécurisé d'informations lors d'une transaction, caractérisé en ce que le dispositif électronique permet à un utilisateur de sélectionner, parmi un ensemble d'informations contenues dans le dispositif électronique, des informations nécessaires à la transaction et de générer un jeton électronique chiffré contenant les informations et destiné à un fournisseur de service afin de procéder à la transaction.

Tel qu'il sera évident à l'homme de métier, dans la présente description et dans les revendications annexées, le terme " utilisateur " désigne un individu effectuant une transaction avec un vendeur, dans le but d'acheter un produit ou d'obtenir un service. De façon similaire, le terme " vendeur " désigne l'entité qui offre des

services ou des produits sur un site Internet et l'expression " fournisseur de services " désigne l'entité qui effectue la service à la demande du vendeur de façon à répondre à la requête de l'utilisateur; il peut s'agir, suivant le type de service ou de produit désiré par l'utilisateur, d'un serveur de courrier électronique, d'un service de courrier, ou d'une passerelle de paiement, par exemple. Le terme " internet " doit être entendu comme ayant une définition englobant tous type de réseaux informatiques, incluant les réseaux téléphonique ou autres en télécommunication.

D'autres particularités et avantages de la présente invention apparaîtront clairement dans la description suivante, relative à des modes de réalisations préférentiels, non limitatifs, et faite en regard des figures annexées.

La Figure 1 représente un schéma fonctionnel illustrant les étapes générales d'un échange sécurisé d'informations selon un mode de réalisation préférentielle de la présente invention;

La Figure 2 représente un schéma fonctionnel illustrant les étapes de l'achat d'un produit et du paiement de celui-ci par carte de crédit;

La Figure 3 représente un schéma fonctionnel illustrant les étapes de l'achat d'un produit et du transport de celui-ci;

La Figure 4 représente un schéma fonctionnel illustrant les étapes de la transmission sécurisée de l'adresse de courrier électronique;

La Figure 5 représente un schéma fonctionnel illustrant les étapes de la transmission sécurisée d'un numéro de téléphone;

La Figure 6 représente un dispositif électronique permettant la génération d'un jeton électronique selon une première variante de mode de réalisation de la présente invention;

La Figure 7 représente un dispositif électronique permettant la génération d'un jeton électronique selon une seconde variante de mode de réalisation de la présente invention; et

La Figure 8 représente un dispositif électronique permettant la génération d'un jeton électronique selon une troisième variante de mode de réalisation de la présente invention.

Un mode préféré de réalisation de la présente invention sera maintenant décrit à titre purement illustratif.

La Figure 1 illustre le concept général de la présente invention permettant le transfert sécurisé d'informations personnelles de l'utilisateur. Tel qu'entendu dans le présent document, une transaction électronique implique généralement un utilisateur, un vendeur et un fournisseur de services.

Dans une première étape 10, l'utilisateur entre en contact avec un vendeur, par exemple par l'intermédiaire du site Internet de celui-ci, dans le but d'acheter un produit ou d'obtenir un service offert par le vendeur.

Sollicité par l'utilisateur, le vendeur lui demande des informations personnelles, sélectionnées parmi une liste d'informations possibles, en fonction du type de produit ou de service désiré par l'utilisateur (étape 12). La liste des informations possibles peut inclure, par exemple, l'adresse, le numéro de téléphone, le numéro de carte de

crédit, le numéro du compte bancaire le numéro de sécurité sociale et l'adresse de courrier électronique.

L'utilisateur, au moyen d'un appareil électronique qui contient préalablement les informations personnelles de l'utilisateur ou qui peut les recevoir directement de l'utilisateur, sélectionne et enregistre les informations personnelles requises dans un jeton électronique (étape 14). Le jeton électronique est chiffré, et contient, en plus des informations demandées par le vendeur afin de procéder à la transaction, des conditions d'utilisation de ces informations, tel que décrit ultérieurement. Le jeton peut également contenir des mécanismes d'intégrité empêchant un tiers de modifier celui-ci et des mécanismes de non-duplication, telle qu'une identité unique, par exemple.

À l'étape 16, l'utilisateur transmet au vendeur non pas les informations personnelles elles-mêmes, mais le jeton électronique qu'il vient de constituer sur mesure aux fins de la transaction désirée. Il est à noter que ces informations personnelles ne sont pas directement accessibles par le vendeur puisqu'elles sont chiffrées.

À l'étape 18, le vendeur fournit à un fournisseur de services, sélectionné en fonction de la requête de l'utilisateur, le jeton électronique accompagné d'une description de la transaction désirée.

À la réception du jeton et de la description de la transaction désirée, le fournisseur de services déchiffre et valide le jeton puis en extrait les données nécessaires à la transaction décrite (étape 20).

Une fois la validation terminée, le fournisseur de services peut optionnellement transmettre une confirmation de transaction à

l'utilisateur et au vendeur (étape 22). Il est alors prêt à effectuer le service demandé.

Il est à noter que dans le scénario général présenté ci-dessus, le vendeur n'a aucun accès à l'information personnelle de l'utilisateur. Ceci est avantageux pour l'utilisateur puisqu'il peut ainsi déterminer quel fournisseur de services mérite sa confiance. En effet, l'information personnelle de l'utilisateur peut être déchiffrée uniquement par des fournisseurs de services choisis par l'utilisateur.

À titre d'exemple d'application de la présente invention, les étapes de l'achat d'un produit et du paiement de celui-ci par carte de crédit sont illustrées à la Figure 2.

La transaction implique dans ce cas particulier un utilisateur, un vendeur, un fournisseur de service, qui dans ce cas est une banque ou un serveur d'autorisation de crédit, tel qu'il sera décrit plus loin.

À l'étape 110, l'utilisateur prend contact avec le vendeur dans le but d'acheter un produit, spécifiant qu'il désire payer par carte de crédit.

Le vendeur, à l'étape 112, demande alors à l'utilisateur des informations personnelles, notamment son numéro de carte de crédit.

L'utilisateur, au moyen d'un appareil électronique, crée un jeton électronique chiffré comprenant son numéro de carte de crédit, ainsi que les conditions d'utilisation de ce numéro (étape 114). Par exemple, une condition d'utilisation peut porter sur le montant maximal créditable et sur le nombre de fois que le jeton peut être

utilisé. Il est à noter que les conditions d'utilisation peuvent être modifiées par l'utilisateur lors de la création du jeton ou peuvent être génériques au type de jeton et au type d'informations qui y sont contenues.

À l'étape suivante (étape 116), l'utilisateur transmet le jeton électronique chiffré ainsi créé au vendeur.

Le vendeur transmet alors celui-ci, accompagné d'une description de la transaction voulue, à la banque émettrice de la carte de crédit de l'utilisateur (étape 118), cette banque étant le fournisseur de service pour ce type de transaction.

La banque déchiffre et valide le jeton électronique puis fait l'extraction des données nécessaires à la transaction, contenues dans le jeton (étape 120). Le jeton, par exemple, n'est validé que si le montant de la transaction ne dépasse pas la limite prédéterminée par le jeton et si l'utilisateur est bien le détenteur de la carte de crédit. Bien entendu, d'autre conditions d'utilisation pourraient être intégrées au jeton et validées par la banque. Par exemple, le nom du vendeur pourrait être inscrit dans le jeton.

Lorsque la validation est effectuée, la banque émettrice transmet une confirmation de transaction à l'utilisateur et au vendeur (étape 122) et peut effectuer le paiement au vendeur tout en débitant le montant du compte de l'utilisateur.

Il est à noter que le fournisseur de service peut être autre que la banque émettrice de la carte de crédit utilisée par l'utilisateur. Le cas échéant, le fournisseur de services valide et déchiffre le jeton et, moyennant que le jeton s'avère valide, sollicite l'autorisation de paiement de la banque émettrice. Par exemple, un serveur

d'autorisation de crédit pourrait être utilisé pour valider les informations du jeton.

Un second exemple d'application de la présente invention sera maintenant décrit en relation avec la Figure 3. Cet exemple implique le transfert de l'adresse de l'utilisateur dans le but de réception d'un colis provenant du vendeur.

L'utilisateur entre en contact avec un vendeur dans le but d'acheter un produit (étape 210). S'ensuit un échange entre l'utilisateur et le vendeur selon les étapes présentées à la Figure 2 pour effectuer le paiement du produit (étape 212).

Dans le cours de la transaction, le vendeur demande à l'utilisateur des données personnelles, incluant l'adresse de livraison du produit (étape 214).

L'utilisateur, via un appareil électronique, crée un jeton électronique chiffré comprenant son adresse ainsi que les conditions d'utilisation de cette adresse (étape 216). Par exemple, une condition portant sur le montant maximal des frais de livraison et une indication que le jeton ne peut être utilisé que par le vendeur en question peuvent être contenues dans le jeton.

Le jeton électronique chiffré ainsi créé est transmis au vendeur (étape 218). Le vendeur fait suivre celui-ci, accompagné d'une description de la transaction voulue, à un service de livraison (étape 220). Le service de livraison déchiffre et valide le jeton électronique, puis extrait les données nécessaires à la transaction (étape 222). Ainsi, par exemple, le jeton ne peut être validé que si le montant de la livraison ne dépasse pas la limite prédéterminée par le jeton.

Lorsque la validation est effectuée, le service de livraison transmet une confirmation de transaction à l'utilisateur et au vendeur (étape 224) et peut effectuer le service demandé, i.e., la livraison.

Il est à noter que plusieurs variations de la méthode présentée ci-dessus peuvent être envisagées.

Par exemple, à l'étape 46, au lieu de transmettre le jeton électronique au service de livraison, le vendeur peut transmettre un jeton encodé sous la forme d'un code à barres imprimé sur une étiquette placée sur le colis. La validation et le déchiffrement de l'information concernant l'adresse de l'utilisateur peuvent ainsi être effectués directement par un livreur assurant le transport du produit, à l'aide d'un appareil électronique adéquat. Le livreur pourrait donc connaître l'adresse de livraison sans que celle-ci soit directement imprimée sur le colis.

Une autre variation à la méthode illustrée à la Figure 3 consisterait à transmettre le jeton électronique directement au service de livraison, sans transiger par le vendeur. Dans ce cas, le vendeur transmettrait de l'information pertinente au service de livraison de façon à permettre le lien entre le colis et le jeton. De cette façon, le vendeur n'est jamais en possession du jeton électronique, ce qui rend la transaction encore plus sécuritaire pour l'utilisateur.

Il est à noter que les informations relatives au paiement du produit et les informations relatives à la livraison de celui-ci à l'utilisateur pourraient être contenues dans le même jeton électronique transmis au vendeur (étape 218). Si tel est le cas, le même jeton pourrait être transmis aux deux fournisseurs de services (banque et service de livraison) qui ne pourraient déchiffrer que la portion du jeton

leur étant nécessaire. Alternativement, une tierce partie, qui aurait la confiance de l'utilisateur et du vendeur, pourrait être utilisée pour déchiffrer ce jeton en entier et transmettre à la banque et au service de livraison les informations qui leur sont nécessaires.

En référence plus spécifique à la Figure 4, les étapes d'une transaction impliquant l'échange sécurisé de l'adresse de courrier électronique de l'utilisateur vont être décrites.

L'utilisateur interagit avec un vendeur dans le but d'obtenir un service (étape 310). Dans ce cas particulier, la transaction consiste en l'envoi d'informations du vendeur vers l'utilisateur, par voie électronique, donc essentiellement sous la forme de messages électroniques adressés à l'adresse de courrier électronique de l'utilisateur.

S'ensuit un échange entre l'utilisateur et le vendeur tel que présenté à la Figure 2 pour effectuer le paiement du service (étape 312).

Le vendeur demande à l'utilisateur des données personnelles (étape 314). Dans le présent exemple, ces données personnelles incluent l'adresse de courrier électronique à laquelle l'information demandée doit être envoyée.

L'utilisateur, via un appareil électronique, crée un jeton électronique chiffré comprenant son adresse de courrier électronique ainsi que les conditions d'utilisation de cette adresse (étape 316). Une condition d'utilisation peut être, par exemple, que le jeton n'est utilisable que par le vendeur en question. Le jeton électronique chiffré ainsi créé est transmis au vendeur à l'étape 318.

Le vendeur transmet alors le jeton électronique, accompagné de l'information demandée, à un service de transmission de courrier électronique (étape 320).

Le service de transmission de courrier électronique déchiffre et valide le jeton électronique, puis extrait les données nécessaires à la transaction (étape 322). Ainsi, le jeton n'est validé, par exemple, que si le vendeur est bien autorisé à utiliser le jeton.

Lorsque la validation est effectuée, le service de transmission de courrier électronique peut acheminer l'information demandée à l'adresse de courrier électronique contenue dans le jeton (étape 324), et transmettre une confirmation de transaction à l'utilisateur et au vendeur.

Encore une fois, plusieurs variations de la méthode de la Figure 4 peuvent être envisagées. Par exemple, l'envoi du jeton vers le service de transmission de courrier électronique et l'envoi de l'information à transmettre à l'utilisateur pourraient s'effectuer en deux étapes distinctes.

Un dernier exemple est décrit en référence à la Figure 5. Cet exemple consiste en une transaction impliquant l'échange sécurisé du numéro de téléphone de l'utilisateur.

L'utilisateur prend contact avec un vendeur (étape 410). Le vendeur demande à l'utilisateur des données personnelles, incluant son numéro de téléphone (étape 412).

À l'étape 414, l'utilisateur, via un appareil électronique, crée un jeton électronique chiffré comprenant son numéro de téléphone ainsi que les conditions d'utilisation de ce numéro. Les

conditions d'utilisation peuvent inclure, par exemple, l'identification du vendeur autorisé à utiliser le jeton ainsi que le nombre d'utilisations possibles du jeton. Le jeton peut prendre la forme d'un code numérique pouvant être entré directement sur un téléphone conventionnel. Le jeton électronique chiffré ainsi créé est transmis au vendeur à l'étape 416.

Le vendeur, à l'étape 418, compose, sur son téléphone, le numéro correspondant au jeton, se reliant ainsi à une centrale d'appel.

La centrale d'appel déchiffre et valide le jeton électronique, puis en extrait le numéro de téléphone (étape 420). Le jeton n'est validé, par exemple, que si le vendeur est bien autorisé à utiliser le jeton, et si le nombre maximal d'utilisations n'est pas dépassé.

Lorsque la validation est effectuée, la centrale d'appel peut composer le numéro de téléphone de l'utilisateur et mettre le vendeur en contact avec l'utilisateur (étape 422).

Tel que mentionné précédemment, le jeton généré par l'utilisateur au moyen du dispositif électronique contient les informations nécessaires à la transaction désirée, tels que le numéro de carte de crédit, l'adresse de courrier électronique, le nom et le mot de passe de l'utilisateur, etc. Il est possible de lui ajouter, par exemple, une condition d'expiration qui ne le rende utilisable qu'un nombre de fois prédéterminé. Ce type de condition est encodé au moyen du dispositif électronique. Une méthode possible peut être du type <identification carte><compteur>, où <identification carte> constitue une identification unique du dispositif dans le système, et <compteur>

représente un compteur interne. De façon similaire, le jeton peut contenir une condition du type date d'expiration, montant maximum débité etc., toutes conditions qui doivent être remplies pour que le jeton soit validé par le fournisseur de services.

Se référant maintenant aux Figures 6 à 8, trois variantes d'un dispositif électronique permettant la génération d'un jeton électronique tel que décrit ci-dessus va être présenté.

La Figure 6 illustre un ordinateur conventionnel 500 comprenant un moniteur 502, un clavier 504 et une unité centrale de traitement 506. L'ordinateur 500 est également pourvu d'un lecteur de carte à puce 508 qui peut recevoir une carte à puce conventionnelle 510.

La carte à puce 510 contient toutes les informations personnelles de l'utilisateur, soit, par exemple, l'adresse de courrier électronique, l'adresse postale, le numéro de carte de débit ou de crédit, le numéro du compte bancaire, le numéro de téléphone, et d'autres informations personnelles du même type.

Lorsque la carte 510 est insérée dans le lecteur 508, l'utilisateur peut demander à la carte 510 de générer un jeton électronique contenant certaines des informations personnelles contenues dans la carte 510. Puisque la carte à puce 510 comprend une puce électronique lui permettant d'effectuer des opérations mathématiques, le chiffrement des informations personnelles peut être effectué directement sur la carte 510.

Lorsque le jeton est généré par la carte 510, il peut ensuite être transmis par le réseau Internet (voir flèche 512) vers le vendeur sous la forme d'un signal électronique. Il est à noter que

d'autres méthodes, telles que discutées ci-dessus, pourraient être utilisées pour transférer le jeton de l'utilisateur au vendeur.

Un avantage d'utiliser un système tel qu'illustré à la Figure 6 consiste à permettre la génération et le transfert du jeton électronique pendant que l'utilisateur visite le site Internet du vendeur, par exemple.

La Figure 7 illustre un PDA (Personnal Digital Assistant) 600 pourvu d'une connection sans fil (voir flèche 602) et d'un lecteur de carte à puce (non montré) pouvant accepter une carte à puce 604.

L'utilisation du dispositif électronique constitué par le PDA 600 et la carte à puce 604 est très similaire à l'utilisation décrite ci-dessus. Encore une fois, le lien sans fil 602 permet le transfert du jeton électronique généré directement par la carte à puce 604.

Finalement, la Figure 8 illustre un téléphone cellulaire 700 conventionnellement pourvu d'une carte à puce 702 et d'une communication bi-directionnelle avec une centrale téléphonique.

La carte à puce conventionnelle 702 du téléphone 700 a été modifiée pour contenir les informations personnelles de l'utilisateur telles que décrites ci-dessus. La carte 702 peut donc, à la demande de l'utilisateur, générer un jeton électronique et le transmettre par communication cellulaire conventionnelle au vendeur ou au fournisseur de services.

Il est à noter que l'utilisation d'une carte à puce dans le dispositif électronique n'est pas nécessaire, par exemple, les informations personnelles pourraient être contenues directement dans

l'ordinateur 500 de la Figure 6 et chiffrées sur demande par un logiciel de cet ordinateur.

Le dispositif électronique permet de créer un jeton chiffré. Le chiffrement peut être effectué, par exemple, au moyen d'un algorithme de chiffrement asymétrique qui utilise une clé publique du fournisseur de services, clé qui est préalablement enregistrée dans le dispositif électronique. Le chiffrement garantit la confidentialité des informations.

La procédure de validation du jeton par le fournisseur de services implique généralement plusieurs actions. D'abord, le fournisseur de services doit déchiffrer le jeton. Dans le cas d'un chiffrement par algorithme asymétrique, le défrichement est effectué à l'aide d'une clé privée du fournisseur de service. Dans un second temps, le fournisseur de services vérifie que les conditions d'utilisation contenues dans le jeton sont rencontrées.

Bien entendu, d'autres systèmes de chiffrement, tel un algorithme à clé symétrique, peuvent également être utilisés.

Il va de soi que la présente invention fut décrite à titre purement indicatif et qu'elle peut recevoir plusieurs autres aménagements et variantes sans pour autant dépasser le cadre de la présente invention tel que délimité par les revendications qui suivent.

REVENDICATIONS

1. Procédé d'échange sécurisé d'informations lors d'une transaction impliquant un utilisateur, un vendeur et un fournisseur de services, caractérisé en ce qu'il comprend les étapes suivantes :

création par l'utilisateur d'un jeton électronique chiffré contenant des informations nécessaires à la transaction, ces informations étant sélectionnées parmi un ensemble d'informations concernant l'utilisateur;

transmission du jeton électronique au fournisseur de services; et

déchiffrage et validation du jeton électronique par le fournisseur de services.

2. Procédé selon la revendication 1, caractérisé en ce que ladite étape de création d'un jeton électronique chiffré est effectuée au moyen d'un dispositif électronique contenant un ensemble d'informations concernant l'utilisateur.

3. Procédé selon la revendication 1, caractérisé en ce que ladite étape de création d'un jeton électronique chiffré utilise un algorithme de chiffrement sélectionné parmis un groupe incluant le chiffrement asymétrique et le chiffrement symétrique.

4. Procédé selon la revendication 1, caractérisé en ce que ladite étape de création d'un jeton électronique comprend l'inclusion d'au moins une condition d'utilisation.

5. Procédé selon la revendication 4, caractérisé en ce que ladite étape de création d'un jeton électronique comprend l'inclusion d'une date d'expiration du jeton électronique.

7. Procédé selon la revendication 1, caractérisé en ce que ladite étape de création d'un jeton électronique comprend l'inclusion de l'identification du vendeur autorisé à utiliser le jeton électronique.

8. Procédé selon la revendication 1, caractérisé en ce que ladite étape de transmission du jeton électronique au fournisseur de services, comprend l'étape intermédiaire de transmission du jeton électronique au vendeur.

9. Procédé selon la revendication 1, caractérisé en ce que ladite étape de transmission du jeton électronique au fournisseur de services, comprend l'étape intermédiaire d'une inclusion d'une description de la transaction souhaitée par l'utilisateur.

10. Procédé selon la revendication 1, caractérisé en ce que ladite étape de transmission du jeton électronique au fournisseur de services comprend les étapes intermédiaires suivantes :

transmission du jeton électronique à un vendeur; et

inclusion par le vendeur d'une description de la transaction souhaitée par l'utilisateur.

11. Procédé selon la revendication 1, caractérisé en ce que ladite étape de déchiffrage du jeton électronique par le fournisseur de services utilise un algorithme de déchiffrage asymétrique.

12. Procédé selon la revendication 1, caractérisé en ce que ladite validation du jeton électronique par le fournisseur de

services nécessite que toute condition d'utilisation contenue dans le jeton électronique soit satisfaite.

13. Procédé selon la revendication 1, caractérisé en ce qu'il comprend une étape de confirmation de la transaction à l'utilisateur et au vendeur.

14. Procédé selon la revendication 1, caractérisé en ce que ladite transaction implique au moins un service.

15. Procédé selon la revendication 1, caractérisé en ce que ladite transaction implique au moins un produit.

16. Procédé selon la revendication 1, caractérisé en ce que ledit jeton électronique a la forme d'un code à barres sur un colis.

17. Procédé selon la revendication 1, caractérisé en ce que ledit jeton électronique a la forme d'un numéro de téléphone.

18. Procédé selon la revendication 1, caractérisé en ce que ledit jeton électronique a la forme d'un signal électronique.

19. Dispositif électronique permettant l'échange sécurisé d'informations lors d'une transaction, caractérisé en ce que ledit dispositif électronique permet à un utilisateur de sélectionner, parmi un ensemble d'informations contenues dans ledit dispositif électronique, des informations nécessaires à ladite transaction et de générer un jeton électronique chiffré contenant lesdites informations et destiné à un fournisseur de service afin de procéder à ladite transaction.

20. Dispositif selon la revendication 19, caractérisé en ce que ledit jeton électronique contient l'identification d'un vendeur

autorisé, intermédiaire entre ledit utilisateur et ledit fournisseur de services.

21. Dispositif selon la revendication 19, caractérisé en ce qu'il contient un ensemble d'informations personnelles concernant ledit utilisateur.

22. Dispositif selon la revendication 21, caractérisé en ce qu'il permet la sélection, parmi ledit ensemble d'informations qu'il contient, et le chiffrement desdites informations nécessaires à ladite transaction.

23. Dispositif selon la revendication 19, caractérisé en ce qu'il permet le chiffrement desdites informations nécessaires à ladite transaction au moyen d'un algorithme asymétrique.

24. Dispositif selon la revendication 19, caractérisé en ce que ledit dispositif est une carte à puce.

25. Dispositif selon la revendication 24, caractésiré en ce que ladite carte à puce peut être insérée dans le lecteur de carte à puce d'un ordinateur.

26. Dispositif selon la revendication 24, caractérisé en ce que ladite carte à puce peut être insérée dans le lecteur de carte à puce d'un PDA.

27. Dispositif selon la revendication 24, caractésiré en ce que ladite carte à puce peut être insérée dans le lecteur de carte à puce d'un téléphone cellulaire.

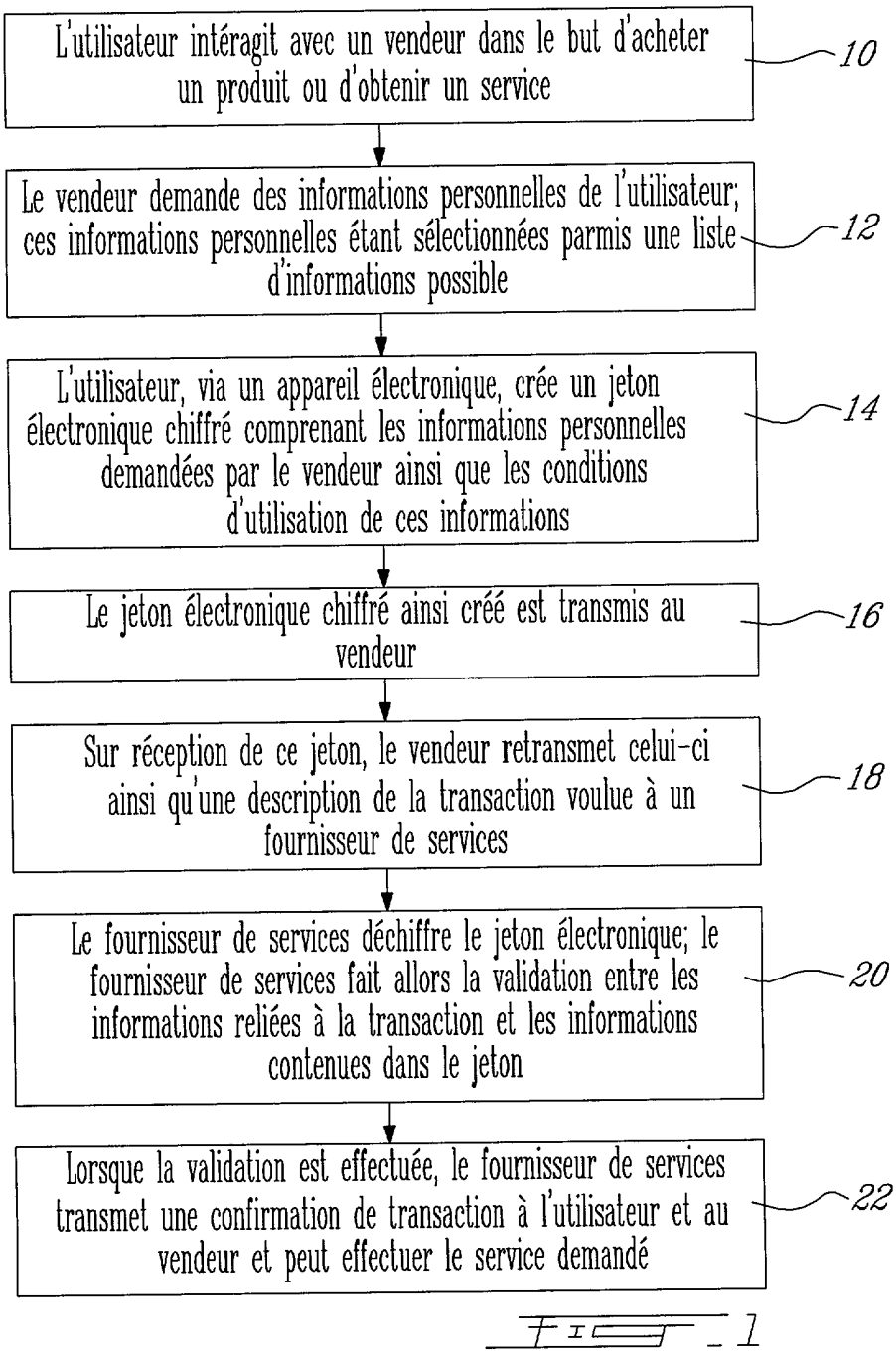
L'utilisateur intéragit avec un vendeur dans le but d'acheter un produit ou d'obtenir un service
10
Le vendeur demande des informations personnelles de l'utilisateur; ces informations personnelles étant sélectionnées parmis une liste d'informations possible
12
L'utilisateur, via un appareil électronique, crée un jeton électronique chiffré comprenant les informations personnelles demandées par le vendeur ainsi que les conditions d'utilisation de ces informations
14
Le jeton électronique chiffré ainsi créé est transmis au vendeur
16
Sur réception de ce jeton, le vendeur retransmet celui-ci ainsi qu'une description de la transaction voulue à un fournisseur de services
18
Le fournisseur de services déchiffre le jeton électronique; le fournisseur de services fait allors la validation entre les informations reliées à la transaction et les informations contenues dans le jeton
20
Lorsque la validation est effectuée, le fournisseur de services transmet une confirmation de transaction à l'utilisateur et au vendeur et peut effectuer le service demandé
22

Fig 1

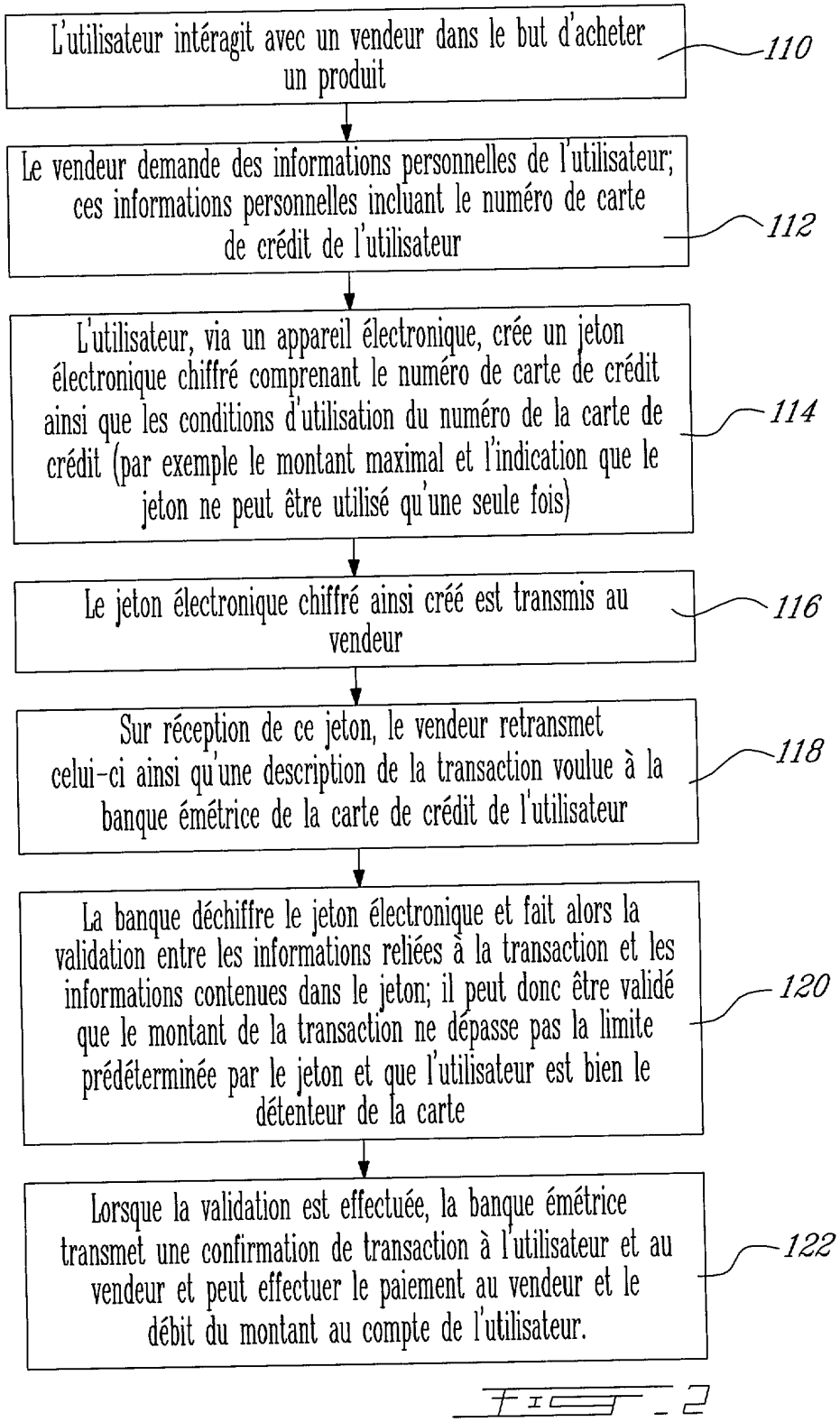
L'utilisateur intéragit avec un vendeur dans le but d'acheter un produit
110
Le vendeur demande des informations personnelles de l'utilisateur; ces informations personnelles incluant le numéro de carte de crédit de l'utilisateur
112
L'utilisateur, via un appareil électronique, crée un jeton électronique chiffré comprenant le numéro de carte de crédit ainsi que les conditions d'utilisation du numéro de la carte de crédit (par exemple le montant maximal et l'indication que le jeton ne peut être utilisé qu'une seule fois)
114
Le jeton électronique chiffré ainsi créé est transmis au vendeur
116
Sur réception de ce jeton, le vendeur retransmet celui-ci ainsi qu'une description de la transaction voulue à la banque émétrice de la carte de crédit de l'utilisateur
118
La banque déchiffre le jeton électronique et fait alors la validation entre les informations reliées à la transaction et les informations contenues dans le jeton; il peut donc être validé que le montant de la transaction ne dépasse pas la limite prédéterminée par le jeton et que l'utilisateur est bien le détenteur de la carte
120
Lorsque la validation est effectuée, la banque émétrice transmet une confirmation de transaction à l'utilisateur et au vendeur et peut effectuer le paiement au vendeur et le débit du montant au compte de l'utilisateur.
122

FIG_2

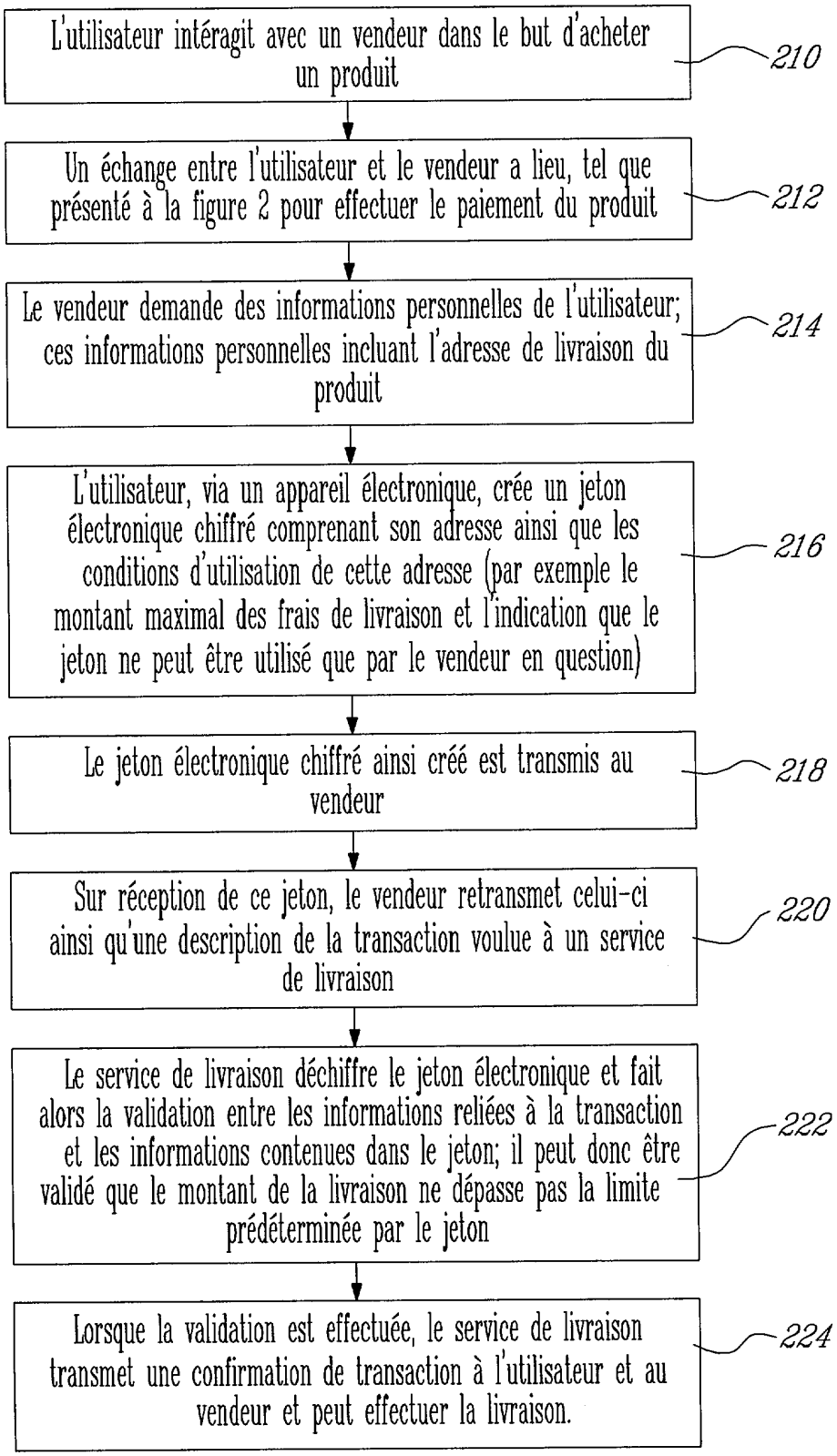
L'utilisateur intéragit avec un vendeur dans le but d'acheter un produit
210
Un échange entre l'utilisateur et le vendeur a lieu, tel que présenté à la figure 2 pour effectuer le paiement du produit
212
Le vendeur demande des informations personnelles de l'utilisateur; ces informations personnelles incluant l'adresse de livraison du produit
214
L'utilisateur, via un appareil électronique, crée un jeton électronique chiffré comprenant son adresse ainsi que les conditions d'utilisation de cette adresse (par exemple le montant maximal des frais de livraison et l'indication que le jeton ne peut être utilisé que par le vendeur en question)
216
Le jeton électronique chiffré ainsi créé est transmis au vendeur
218
Sur réception de ce jeton, le vendeur retransmet celui-ci ainsi qu'une description de la transaction voulue à un service de livraison
220
Le service de livraison déchiffre le jeton électronique et fait alors la validation entre les informations reliées à la transaction et les informations contenues dans le jeton; il peut donc être validé que le montant de la livraison ne dépasse pas la limite prédéterminée par le jeton
222
Lorsque la validation est effectuée, le service de livraison transmet une confirmation de transaction à l'utilisateur et au vendeur et peut effectuer la livraison.
224

FIG. 3

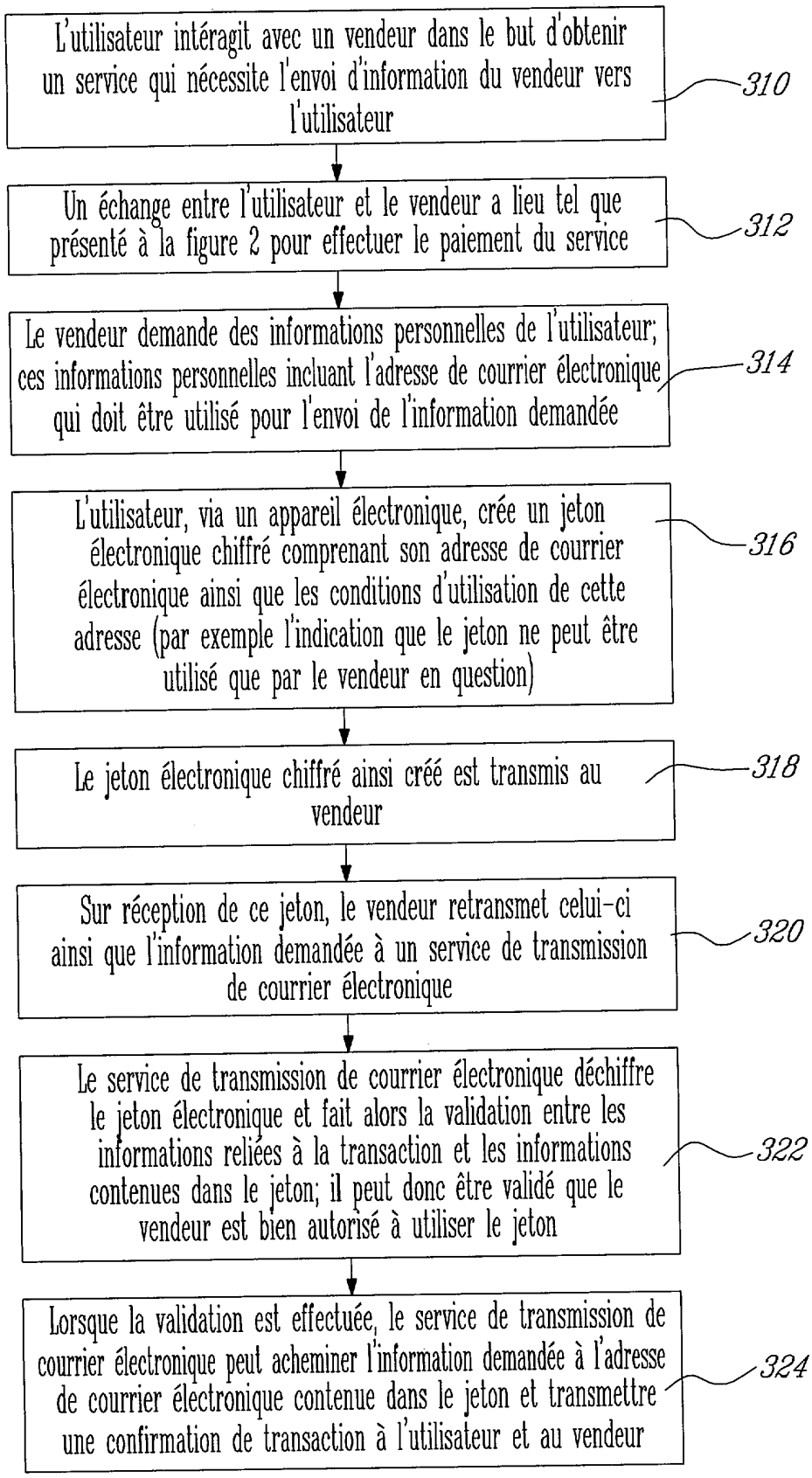
L'utilisateur intéragit avec un vendeur dans le but d'obtenir un service qui nécessite l'envoi d'information du vendeur vers l'utilisateur
310
Un échange entre l'utilisateur et le vendeur a lieu tel que présenté à la figure 2 pour effectuer le paiement du service
312
Le vendeur demande des informations personnelles de l'utilisateur; ces informations personnelles incluant l'adresse de courrier électronique qui doit être utilisé pour l'envoi de l'information demandée
314
L'utilisateur, via un appareil électronique, crée un jeton électronique chiffré comprenant son adresse de courrier électronique ainsi que les conditions d'utilisation de cette adresse (par exemple l'indication que le jeton ne peut être utilisé que par le vendeur en question)
316
Le jeton électronique chiffré ainsi créé est transmis au vendeur
318
Sur réception de ce jeton, le vendeur retransmet celui-ci ainsi que l'information demandée à un service de transmission de courrier électronique
320
Le service de transmission de courrier électronique déchiffre le jeton électronique et fait alors la validation entre les informations reliées à la transaction et les informations contenues dans le jeton; il peut donc être validé que le vendeur est bien autorisé à utiliser le jeton
322
Lorsque la validation est effectuée, le service de transmission de courrier électronique peut acheminer l'information demandée à l'adresse de courrier électronique contenue dans le jeton et transmettre une confirmation de transaction à l'utilisateur et au vendeur
324

FIG. 4

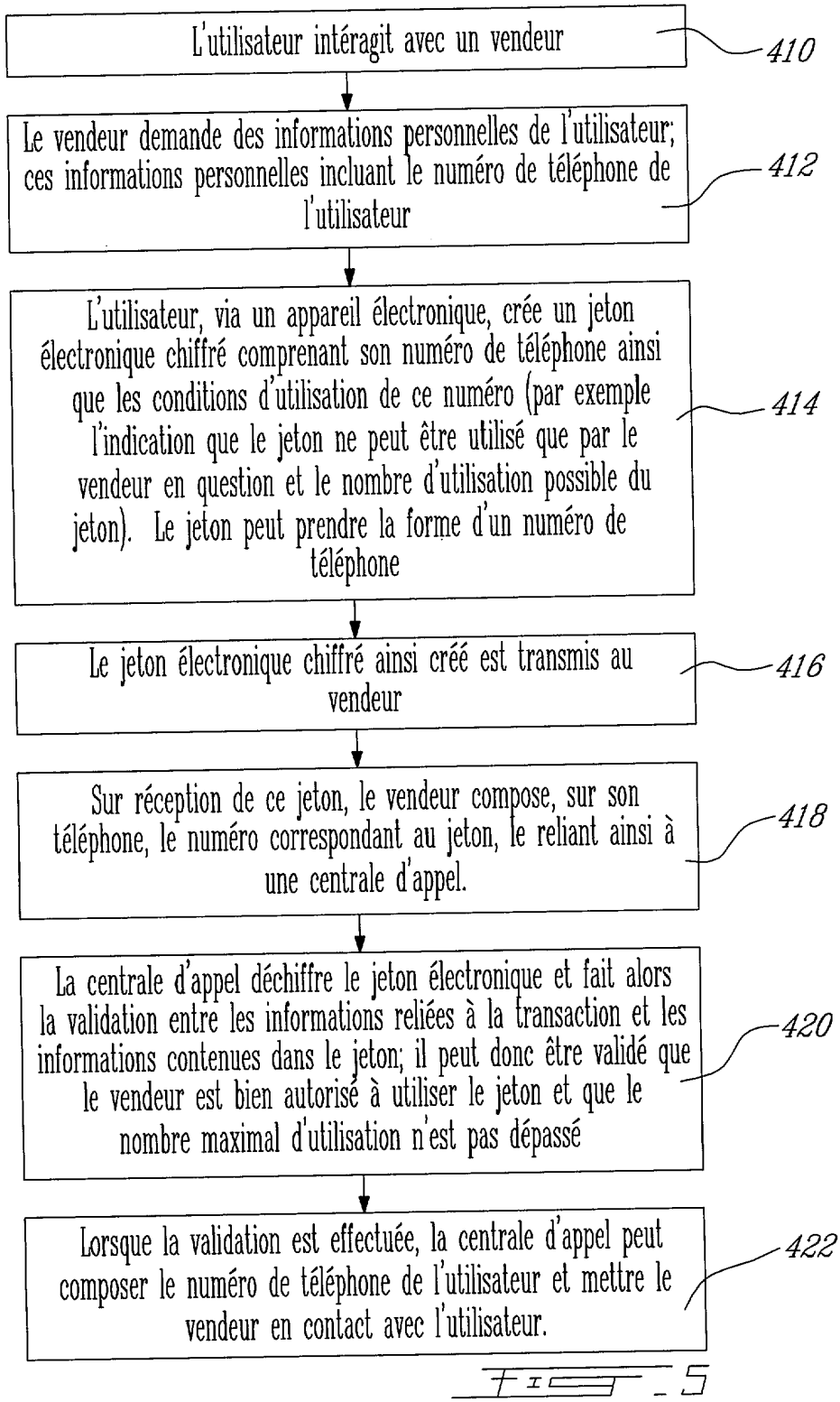
L'utilisateur intéragit avec un vendeur
410
Le vendeur demande des informations personnelles de l'utilisateur; ces informations personnelles incluant le numéro de téléphone de l'utilisateur
412
L'utilisateur, via un appareil électronique, crée un jeton électronique chiffré comprenant son numéro de téléphone ainsi que les conditions d'utilisation de ce numéro (par exemple l'indication que le jeton ne peut être utilisé que par le vendeur en question et le nombre d'utilisation possible du jeton). Le jeton peut prendre la forme d'un numéro de téléphone
414
Le jeton électronique chiffré ainsi créé est transmis au vendeur
416
Sur réception de ce jeton, le vendeur compose, sur son téléphone, le numéro correspondant au jeton, le reliant ainsi à une centrale d'appel.
418
La centrale d'appel déchiffre le jeton électronique et fait alors la validation entre les informations reliées à la transaction et les informations contenues dans le jeton; il peut donc être validé que le vendeur est bien autorisé à utiliser le jeton et que le nombre maximal d'utilisation n'est pas dépassé
420
Lorsque la validation est effectuée, la centrale d'appel peut composer le numéro de téléphone de l'utilisateur et mettre le vendeur en contact avec l'utilisateur.
422

FIG. 5

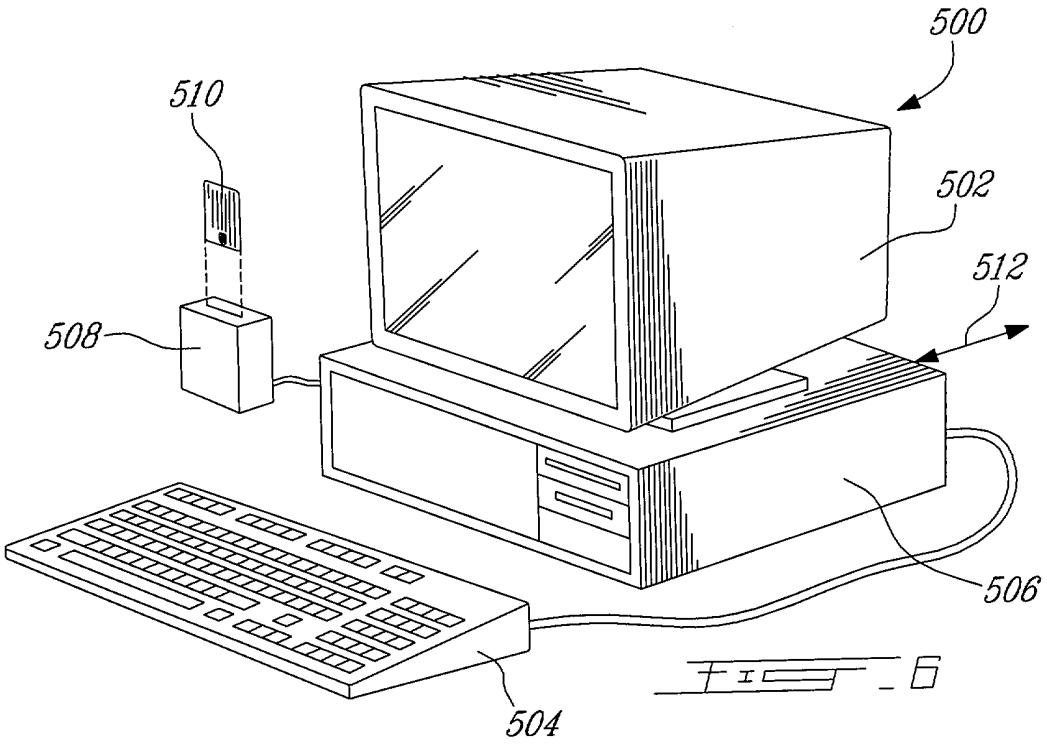

Fig. 6

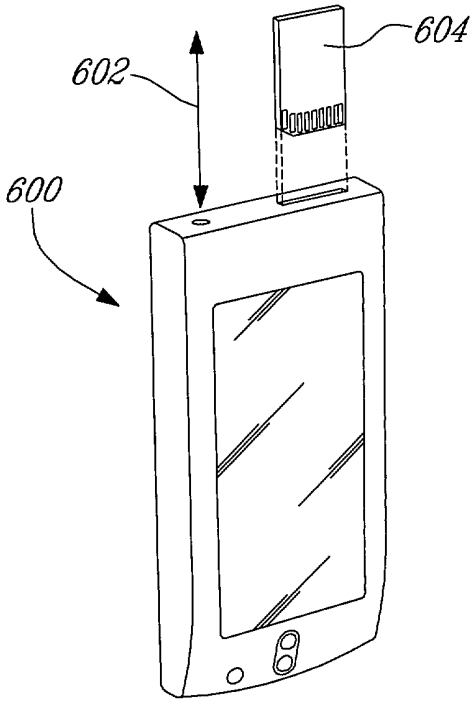

Fig. 7

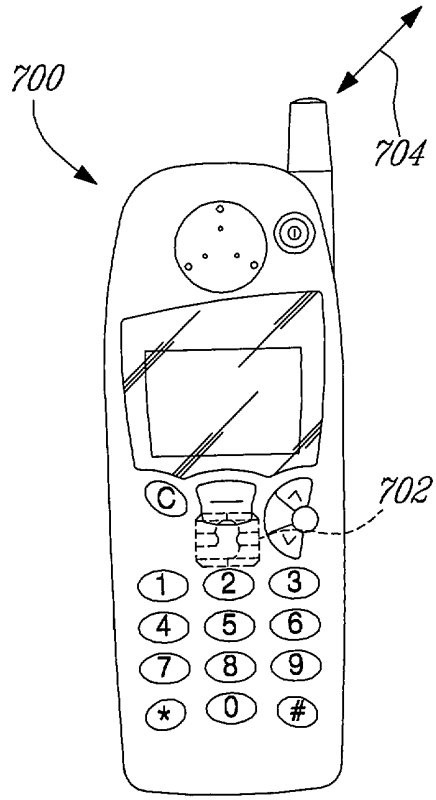

Fig. 8

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2831361

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 613553
FR 0114075

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	WO 01 71627 A (QUALCOMM INC) 27 septembre 2001 (2001-09-27)	1-4,9, 12-15, 18,19, 21,22	H04L9/30 G06F17/60
Y	* page 6, ligne 10 - page 8, ligne 5 * * page 8, ligne 30 - page 10, ligne 12 * * page 11, ligne 11 - page 12, ligne 11 * * page 13, ligne 4 - ligne 28 * * figures 1-5 *	7,11,20, 23,26,27	
X	WO 98 32260 A (COMMW BANK OF AUSTRALIA ;MAPSON MICHAEL JOSEPH (AU)) 23 juillet 1998 (1998-07-23) * page 5, ligne 1 - page 7, ligne 3 * * figures 1,2 *	1-3,7,9, 13,19, 21,22	
Y	US 6 175 922 B1 (WANG YNJIUN P) 16 janvier 2001 (2001-01-16)	7,11,20, 23,26,27	
A	* colonne 4, ligne 48 - colonne 6, ligne 24; figures 2-4,7A,7B,8 * * colonne 8, ligne 29 - ligne 49 * * revendications 1,11-13,17 *	1,19	
A	US 6 038 551 A (BARLOW DOUG ET AL) 14 mars 2000 (2000-03-14) * colonne 4, ligne 60 - colonne 5, ligne 33; figures 1-3,6-12 *	1,19	

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

G06F
G07F

1

Date d'achèvement de la recherche	Examinateur
4 septembre 2002	Paraf, E

CATÉGORIE DES DOCUMENTS CITÉS

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

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

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0114075 FA 613553

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 04-09-2002
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0171627	A	27-09-2001	AU	4766901 A	03-10-2001
			WO	0171627 A2	27-09-2001
WO 9832260	A	23-07-1998	AU	7998898 A	07-08-1998
			WO	9832260 A1	23-07-1998
			ZA	9800250 A	13-07-1998
US 6175922	B1	16-01-2001	US	6282656 B1	28-08-2001
			US	5917913 A	29-06-1999
			AU	2059701 A	24-09-2001
			WO	0169388 A1	20-09-2001
			US	2002023215 A1	21-02-2002
			AU	5383198 A	29-06-1998
			WO	9825371 A1	11-06-1998
US 6038551	A	14-03-2000	AUCUN		

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82