(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 051 613**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **16 54400**

(51) Int Cl[8] : ***H 04 L 9/00*** *(2016.01), G 06 K 7/14, G 06 K 19/06, G 06 Q 20/32, G 06 Q 20/36, G 06 Q 20/40*

(12) **BREVET D'INVENTION** **B1**

(54) ÉCHANGE SÉCURISÉ DE DONNÉES SENSIBLES SUR UN RÉSEAU SUR LA BASE DE CODE-BARRES ET DE JETONS.

(22) **Date de dépôt :** 18.05.16.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 24.11.17 Bulletin 17/47.

(45) **Date de la mise à disposition du public du brevet d'invention :** 13.12.19 Bulletin 19/50.

(56) **Liste des documents cités dans le rapport de recherche :**

Se reporter à la fin du présent fascicule

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

(○) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *AMADEUS S.A.S. Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** APARICIO RUIZ PABLO, TAHON MATHIEU et ESPEJO MALAGON DANIEL.

(73) **Titulaire(s) :** AMADEUS S.A.S. Société par actions simplifiée.

(74) **Mandataire(s) :** SAMSON & PARTNER PATENTANWALTE MBB.

FR 3 051 613 - B1

ÉCHANGE SÉCURISÉ DE DONNÉES SENSIBLES SUR UN RÉSEAU SUR LA BASE DE CODE-BARRES ET DE JETONS

DOMAINE TECHNIQUE

[0001] L'invention concerne de façon générale des ordinateurs et des logiciels d'ordinateur, et en particulier des procédés, des systèmes, et des produits-programmes d'ordinateurs pour effectuer des échanges sécurisés de données sensibles sur un réseau.

CONTEXTE

[0002] En raison des nombreuses possibilités pour que des données sensibles, telles que des données de carte de crédit, soient compromises lors d'un paiement, il est impératif d'utiliser des dispositifs qui sont conformes à la norme de l'industrie en matière de sécurité applicable aux données de carte de paiement (PCI-DSS) permettant de réduire les vulnérabilités et de protéger les données du détenteur de carte. Cependant, il peut être extraordinairement difficile et coûteux de se conformer à la norme PCI-DSS. Dans une approche pour protéger des données sensibles, la substitution des données par un jeton ou un alias peut être utilisée en remplacement des données actuelles de la carte de crédit. Le jeton peut être utilisé à la place de la carte de crédit actuelle d'un individu lors d'une transaction de paiement. Par exemple, un utilisateur peut se servir de son smartphone ou d'un autre dispositif électronique portable pour régler un produit. De façon spécifique, l'utilisateur peut télécharger une application logicielle sur un smartphone. L'utilisateur peut ensuite saisir les informations relatives à une carte de crédit et envoyer les informations par un réseau à un groupe de serveurs. En réponse à la réception des informations associées à la carte de crédit de l'utilisateur, les serveurs peuvent générer un jeton correspondant aux informations de la carte de crédit de l'utilisateur. Les hommes de métier comprendront que les jetons, en eux-mêmes, n'ont pas de sens et ne peuvent donc pas être utilisés seuls. Par ailleurs, la génération de jetons peut s'avérer moins coûteuse et plus sécurisée qu'un cryptage de bout en bout.

[0003] Par exemple, les agents de réservation tiers (c.-à-d., les agents de voyage), ou les voyageurs peuvent utiliser des dispositifs informatiques afin de créer une réservation de voyage, ce qui ouvre des possibilités pour que les données de la carte de crédit du voyageur soient compromises lors du paiement. Parfois un voyageur peut avoir besoin, pendant son déplacement, de payer la réservation de voyage elle-même ou tout autre frais accessoire, tel que des frais de bagages. C'est-à-dire, que le voyageur peut avoir besoin de payer sur place, dans un aéroport ou dans un autre endroit, tel qu'une gare, des frais liés au voyage.

[0004] En plus des difficultés, mentionnées ci-dessus pour protéger les données du détenteur de carte, on remarquera que les voyageurs peuvent aussi être confrontés à d'autres problèmes en essayant

d'effectuer un paiement pour confirmer une réservation de voyage, dans un aéroport ou autre endroit similaire. Par exemple, l'utilisation d'un smartphone pour payer une réservation peut s'avérer problématique pour le voyageur lorsqu'il est de passage dans un pays étranger. Cela s'explique par le fait que de nombreux fournisseurs de services cellulaires n'offrent peut-être pas de tels services dans un autre pays, ou peuvent facturer des tarifs très élevés pour les données d'itinérance lorsque le voyageur est à l'étranger. Ainsi, l'acceptation de paiements de la part des voyageurs, même lorsque leur smartphone n'est pas connecté à un réseau, constitue un besoin. Par ailleurs, on remarquera qu'il peut aussi être incommode et fastidieux pour un voyageur de sortir sa carte de crédit de son portefeuille qui se trouve dans sa poche, surtout s'il est pressé et a beaucoup de bagages à porter pendant son déplacement. De la même manière, il peut aussi être incommode pour une voyageuse de fouiller dans son sac à main pour récupérer sa carte de crédit, surtout si ses mains sont déjà prises par des sacs à porter pendant son déplacement.

[0005] Ainsi, des procédés, des systèmes et des produits-programmes d'ordinateurs améliorés sont nécessaires pour permettre l'échange sécurisé de données sensibles sur un réseau.

RÉSUMÉ

[0006] Dans un mode de réalisation de l'invention, un système pour l'échange sécurisé d'un jeton d'une carte de crédit entre un premier ordinateur et un ordinateur externe pour acheter un produit. Le premier ordinateur inclut un ou plusieurs processeurs, une mémoire, et une caméra couplée à au moins un processeur. Le premier ordinateur numérise le code-barres à l'aide de la caméra. Le premier code-barres est publié sur un écran d'affichage de l'ordinateur externe et indique une pluralité de paramètres de paiement pour le paiement du produit. Le premier ordinateur décode le premier code-barres pour en extraire les paramètres de paiement. Le premier ordinateur publie les paramètres de paiement pour affichage à l'intention d'un utilisateur. Le premier ordinateur reçoit une première saisie dans laquelle la première saisie indique un numéro de carte de crédit pour l'achat d'un produit, et un jeton de carte de crédit correspondant au numéro de la carte de crédit est sauvegardé en mémoire. En réponse à la réception de la première saisie, le premier ordinateur génère un second code-barres qui contient les premières données cryptées de charge utile. Les premières données cryptées de charge utile incluent le jeton de carte de crédit. Le premier ordinateur publie le second code-barres pour affichage, ledit second code-barres étant lisible par un dispositif optique de l'ordinateur externe.

[0007] Dans certains modes de réalisation, le système comprend par ailleurs un troisième ordinateur et une chambre forte de jetons en communication avec l'ordinateur externe. L'ordinateur externe envoie le second code-barres au troisième ordinateur. Dans un mode de réalisation, le troisième ordinateur décode le second code-barres, valide le contenu des premières données cryptées de charge utile pour obtenir le jeton de la carte de crédit et récupère un numéro de carte de crédit originale dans la chambre forte de

jetons sur la base du jeton de la carte de crédit. Dans certains modes de réalisation, le troisième ordinateur communique avec un réseau de paiement pour déterminer la validité du numéro de la carte de crédit originale et, en réponse au numéro de la carte de crédit originale s'avérant valide, le réseau de paiement autorise le paiement du produit et envoie une approbation au troisième ordinateur. Dans certains modes de réalisation, l'ordinateur externe reçoit l'approbation du troisième ordinateur pour le paiement du produit, génère un troisième code-barres qui contient un reçu de paiement pour le produit et publie le troisième code-barres pour affichage. Le troisième code-barres est numérisé par la caméra.

[0008] Dans certains modes de réalisation, la pluralité des paramètres de paiement inclut au moins un montant monétaire, un type spécifique de devise sur lequel le montant monétaire est basé, une description du produit et une référence du paiement sous forme d'identifiant (ID).

[0009] Dans certains modes de réalisation, avant la numérisation du premier code-barres par la caméra, le premier ordinateur et un troisième ordinateur sont connectés à un réseau, le premier ordinateur reçoit une seconde saisie indiquant le numéro de la carte de crédit et, en réponse à la réception de la seconde saisie, le premier ordinateur génère des secondes données cryptées de charge utile qui contiennent le numéro de la carte de crédit. Dans certains modes de réalisation, le premier ordinateur transmet sur le réseau une demande de provisionnement de carte incluant les secondes données cryptées de charge utile, le troisième ordinateur reçoit la demande de provisionnement de carte sur le réseau et, en réponse à la réception de la demande de provisionnement de carte, le troisième ordinateur décrypte les secondes données cryptées de charge utile pour obtenir le numéro de la carte de crédit. Dans certains modes de réalisation, le troisième ordinateur envoie le numéro de la carte de crédit à une application de tokénisation et en réponse à la réception du numéro de la carte de crédit, l'application de tokénisation génère le jeton de la carte de crédit. Dans certains modes de réalisation, le jeton de la carte de crédit est sauvegardé dans une chambre forte de jetons et est aussi transmis par le troisième ordinateur au premier ordinateur via le réseau, et le premier ordinateur conserve le jeton de la carte de crédit sous forme d'une empreinte numérique (hash) en mémoire. Dans certains modes de réalisation, les processeurs font partie d'un dispositif électronique portable.

[0010] Selon un autre aspect, un procédé est révélé pour l'échange sécurisé d'un jeton de carte de crédit entre un premier ordinateur et un ordinateur externe dans le cadre de l'achat d'un produit. Le procédé inclut la numérisation d'un premier code-barres à l'aide d'une caméra d'un premier ordinateur dans lequel le premier code-barres est publié pour affichage sur un écran de l'ordinateur externe, et le premier code-barres indique une pluralité des paramètres de paiement du produit. Le procédé comprend par ailleurs le décodage du premier code-barres, par le premier ordinateur, pour en extraire les paramètres de paiement. Le procédé inclut aussi la publication des paramètres de paiement par le premier ordinateur, pour affichage sur l'écran d'un utilisateur. Le procédé inclut par ailleurs la réception d'une première saisie

par le premier ordinateur, dans laquelle la première saisie indique un numéro de carte de crédit pour l'achat du produit, et un jeton de carte de crédit, correspondant au numéro de la carte de crédit, est sauvegardé dans la mémoire du premier ordinateur. En réponse à la réception de la première saisie, le procédé inclut la génération, par le premier ordinateur, d'un second code-barres contenant les premières données cryptées de charge utile, dans lesquelles les premières données cryptées de charge utile incluent le jeton de la carte de crédit. Enfin, le procédé inclut la publication du second code-barres pour affichage sur l'écran du premier ordinateur, dans laquelle le second code-barres est lisible à l'aide d'un dispositif optique de l'ordinateur externe.

[0011] Dans certains modes de réalisation, l'ordinateur externe envoie le second code-barres à un troisième ordinateur via un réseau. Le troisième ordinateur décode le second code-barres, valide le contenu des premières données cryptées de charge utile pour obtenir le jeton de la carte de crédit et récupère un numéro de la carte de crédit originale dans une chambre forte de jetons sur la base du jeton de la carte de crédit. Dans certains modes de réalisation, le troisième ordinateur envoie une communication à un réseau de paiement. En réponse à la réception de la communication, le réseau de paiement détermine si le numéro de la carte de crédit originale est valide. En réponse au numéro de la carte de crédit originale s'avérant valide, le réseau de paiement autorise le paiement du produit via le réseau de paiement et envoie une autorisation au troisième ordinateur. Dans certains modes de réalisation, le troisième ordinateur reçoit l'autorisation pour le paiement du produit, envoie l'autorisation à l'ordinateur externe via le réseau, génère un troisième code-barres contenant un reçu de paiement du produit et publie le troisième code-barres pour affichage par l'ordinateur externe, dans lequel le troisième code-barres est numérisé par la caméra du premier ordinateur.

[0012] Dans certains modes de réalisation, le premier ordinateur et le troisième ordinateur sont connectés à un réseau avant la numérisation du premier code-barres par le premier ordinateur. Le premier ordinateur reçoit une seconde saisie indiquant le numéro de la carte de crédit et, en réponse à la réception de la seconde saisie, génère des secondes données cryptées de charge utile contenant le numéro de la carte de crédit. Le premier ordinateur transmet une demande de provisionnement de carte incluant les données cryptées de charge utile via le réseau. Le troisième ordinateur reçoit la demande de provisionnement de carte via le réseau et, en réponse à la réception de la demande de provisionnement de carte, décrypte les secondes données cryptées de charge utile pour obtenir le numéro de carte de crédit. Le troisième ordinateur envoie le numéro de carte de crédit à une application de tokénisation du troisième ordinateur et, en réponse à la réception du numéro de carte de crédit, génère le jeton de carte de crédit à l'aide de l'application de tokénisation. Dans certains modes de réalisation, le troisième ordinateur sauvegarde le jeton de carte de crédit dans une chambre forte de jetons et transmet le jeton de carte de crédit via le réseau. Le premier ordinateur reçoit le jeton de carte de crédit par le système via le réseau et conserve le

jeton de carte de crédit sous forme d'empreinte numérique dans la mémoire du système. Dans certains modes de réalisation, le premier ordinateur est un dispositif électronique portable.

[0013] Selon un autre aspect, un produit-programme d'ordinateur est fourni pour l'échange sécurisé d'un jeton de carte de crédit avec un ordinateur externe dans le cadre de l'achat d'un produit. Le produit programme d'ordinateur comprend un support de stockage durable lisible par ordinateur et un code de programme enregistré sur le support de stockage durable lisible par ordinateur qui, lorsqu'il est exécuté par un ou plusieurs processeurs, amène un ou plusieurs processeurs à numériser un premier code-barres à l'aide d'une caméra, dans lequel le premier code-barres est publié pour affichage sur un écran de l'ordinateur externe et le premier code-barres indique une pluralité des paramètres de paiement du produit. Les processeurs sont par ailleurs amenés à décoder le premier code-barres pour en extraire les paramètres de paiement. Les processeurs sont par la suite amenés à publier les paramètres de paiement pour affichage à l'intention d'un utilisateur. Puis les processeurs sont amenés à recevoir une première saisie, dans laquelle la première saisie indique un numéro de carte de crédit pour l'achat du produit et un jeton de carte de crédit correspondant au numéro de carte de crédit est sauvegardé dans la mémoire. En réponse à la réception de la première saisie, les processeurs sont ensuite amenés à générer un second code-barres qui contient les premières données cryptées de charge utile dans lesquelles les premières données cryptées de charge utile incluent le jeton de carte de crédit. Les processeurs sont par ailleurs amenés à publier le second code-barres pour affichage. Le second code-barres est lisible à l'aide d'un dispositif optique de l'ordinateur externe.

[0014] Le préambule ci-dessus est bref et simplifié pour permettre une compréhension basique de certains aspects des systèmes et/ou procédés décrits dans les présentes. Ce résumé n'est pas un aperçu extensif des systèmes et/ou procédés décrits dans les présentes. Il ne prétend ni identifier des éléments clés ou décisifs, ni définir l'étendue de tels systèmes et/ou procédés. Son seul but est de présenter certains concepts de façon simplifiée en guise de préface à la description plus détaillée qui est exposée par la suite.

BRÈVE DESCRIPTION DES DESSINS

[0015] Les dessins qui accompagnent font partie intégrante des spécifications ; ils illustrent des modes variés de réalisation de l'invention et, conjointement à la description générale de l'invention ci-dessus et la description détaillée des modes de réalisation donnée ci-après, servent à expliquer les modes de réalisation de l'invention.

[0016] FIG. 1 est une vue schématique d'un environnement d'exploitation exemplaire pour échanger un jeton de carte de crédit dans le cadre de l'achat d'un produit, dans lequel l'environnement d'exploitation inclut un dispositif client, un système commerçant et un serveur.

[0017] FIG. 2 et une vue schématique d'un système informatique exemplaire de la FIG. 1.

[0018] FIG. 3 est une vue schématique du dispositif client illustré dans la FIG 1. en cours de téléchargement d'une application logicielle.

[0019] FIG. 4 est une vue schématique du dispositif client et du système commerçant illustrés dans la FIG. 1, dans laquelle le dispositif client et le système commerçant peuvent afficher des codes-barres uniques.

DESCRIPTION DÉTAILLÉE

[0020] Faisant maintenant référence à la FIG. 1, un environnement d'exploitation 10, conforme à un mode de réalisation de l'invention, peut inclure un dispositif client 12, un système commerçant 14 et un ou plusieurs serveurs 16. Ainsi qu'expliqué de façon plus détaillée ci-dessous, le serveur 16 peut être en communication avec une chambre forte de jetons 18 ainsi qu'un serveur de paiement 20. Les hommes de métier comprendront que la chambre forte de jetons 18 est un serveur sécurisé où les jetons et le numéro principal de compte correspondant (Primary Account Number, ou (PAN)) sont conservés de façon sécurisée. Le PAN, qui comporte typiquement entre quatorze et seize chiffres, est un numéro de carte de crédit associé à la carte de crédit du détenteur d'un compte. La chambre forte de jetons 18 est la seule composante du système d'exploitation 10 où le jeton peut être mappé pour obtenir le PAN. Par ailleurs, on remarquera également que la chambre forte de jetons 18 répond aux spécifications relatives à la norme de l'industrie en matière de sécurité applicable aux données de carte de paiement (PCI-DSS). Chaque dispositif client 12, chaque système commerçant 14 et chaque serveur 16 peut communiquer par l'intermédiaire d'un réseau 26. Le réseau 26 peut inclure un ou plusieurs réseaux privés ou publics (par ex., Internet) qui permettent l'échange de données.

[0021] Le dispositif client 12 peut, par exemple, être une tablette numérique, un smartphone, ou tout autre dispositif informatique approprié. On remarquera que du fait que l'utilisateur final en déplacement durant un voyage peut éventuellement utiliser le dispositif client 12, le dispositif client 12 peut être un dispositif électronique portable. C'est-à-dire, que la taille du dispositif client 12 est telle que le dispositif client 12 peut être transporté dans le sac à main, un bagage cabine, un portefeuille, ou même dans la poche du voyageur. Ainsi qu'il le sera expliqué en détail ci-dessous, un utilisateur final peut se servir du dispositif client 12 pour confirmer et régler une réservation de voyage en accédant au système commerçant 14. Par exemple, le voyageur peut lancer une application de navigateur et utiliser l'application du navigateur pour effectuer le paiement d'une réservation de voyage. On remarquera que le voyageur peut d'abord télécharger une application 27 sur la mémoire du dispositif client 12 avant que le dispositif client 12 ne soit utilisé pour confirmer et payer la réservation de voyage.

[0022] Le dispositif client 12 peut inclure une caméra 22 ainsi qu'un écran 24. La caméra 22 est capable de capturer des images. Par ailleurs, on remarquera également que le dispositif client 12 est

capable de reconnaître et de décoder des codes-barres capturés par la caméra 22. Des exemples de codes-barres qui peuvent être capturés par la caméra 22 et décodés par le dispositif client 12 incluent, sans que ce soit limitatif, des codes à réaction rapide (QR codes). L'écran 24 du dispositif client 12 peut, par exemple, être un écran d'affichage à cristaux liquides (LCD) qui affichent électroniquement des graphiques, tels que des textes, des images, et des animations.

[0023] Le système commerçant 14 peut être associé à un fournisseur ou des fournisseurs de voyage spécifiques. Dans un mode de réalisation, le système commerçant 14 peut inclure une application commerçante 28, un dispositif optique 30 et un écran 32. Ainsi qu'il le sera expliqué de façon plus détaillée ci-dessous, l'application commerçante 28 peut être utilisée conjointement avec le dispositif client 12 afin de permettre l'échange sécurisé d'un jeton de carte de crédit dans le cadre de l'achat d'un produit. On remarquera que le système commerçant 14 peut aussi être mobile. Dans un mode de réalisation non limitatif, le produit peut être un produit de voyage tel que, par exemple, un voyage aérien, un voyage en train, un voyage en ferry, des chambres d'hôtel, des locations de voitures, du tourisme et d'autres activités liées au voyage. Le produit peut aussi inclure non seulement des produits de voyage, mais aussi d'autres dépenses liées au voyage telles que, par exemple, des frais de bagages qui peuvent survenir pendant les déplacements ou le surclassement d'une réservation de voyage existante. Le dispositif optique 30 peut être tout type de dispositif permettant la capture d'image tel que, par exemple, un scanner ou une caméra Web. De façon spécifique, le système commerçant 14 peut reconnaître et décoder les codes-barres qui sont affichés sur l'écran 24 du dispositif client 12. L'écran 32 du système commerçant 14 peut, par exemple, être un LCD qui affiche électroniquement des graphiques tels que du texte, des illustrations et des images animées.

[0024] Le serveur 16 peut être en communication avec la chambre forte de jetons 18 ainsi qu'avec le serveur de paiement 20 par l'intermédiaire du réseau 26. Le serveur de paiement 20 peut être en communication avec un réseau de paiement 34 et un fournisseur de services de paiement (PSP) 36 par l'intermédiaire du serveur de paiement 20. Ainsi qu'expliqué de façon plus détaillée ci-dessous, le serveur 16 peut récupérer un numéro de carte de crédit originale de la chambre forte de jetons 18 sur la base du jeton de carte de crédit. Le serveur 16 peut recevoir une autorisation en provenance du réseau de paiement 34 validant le numéro de la carte de crédit originale et confirmer avec le PSP 36 que le système commerçant 14 est bien autorisé à effectuer un paiement pour l'achat d'un produit particulier.

[0025] Faisant maintenant référence à la FIG. 2, le dispositif client 12, le système commerçant 14 et le serveur 16 de l'environnement d'exploitation 10 peuvent être implémentés sur un ou plusieurs dispositifs ou systèmes informatiques, tels que le système informatique exemplaire 40. Le système informatique 40 peut inclure un processeur 42, une mémoire 44, un dispositif de stockage de mémoire de masse 46, une interface saisie/sortie (I/O) 48 et une interface homme-machine (HMI) 50. Le système

informatique 40 peut aussi être couplé de façon fonctionnelle à une ou plusieurs ressources externes 52 par l'intermédiaire du réseau 26 ou de l'interface I/O 48. Les ressources externes peuvent inclure, mais de façon non exhaustive, des serveurs, des bases de données, des dispositifs de stockage de mémoire de masse, des dispositifs périphériques, des services de réseau cloud, ou toute autre ressource informatique appropriée qui peut être utilisée avec l'ordinateur 40.

[0026] Le processeur 42 peut inclure un ou plusieurs dispositifs sélectionnés : microprocesseurs, microcontrôleurs, processeurs de signal numérique, micro-ordinateurs, unités centrales de traitement, des réseaux de portes programmables, des dispositifs logiques programmables, des machines à état défini, des circuits logiques, des circuits analogiques, des circuits numériques, ou tout autre dispositif servant à manipuler des signaux (analogues ou numériques) sur la base des instructions de fonctionnement enregistrées dans la mémoire 44. La mémoire 44 peut inclure un seul dispositif ou une pluralité de dispositifs de mémoire, notamment, mais de façon non exhaustive, la mémoire à lecture seule (read-only memory (ROM)), la mémoire à accès aléatoire (random access memory (RAM)), la mémoire volatile, la mémoire non volatile, la mémoire vive statique (SRAM), la mémoire dynamique à accès aléatoire (DRAM), la mémoire flash, l'antémémoire (cache memory), ou tout autre dispositif capable de stocker des informations. Le dispositif de stockage de mémoire de masse 46 peut inclure des dispositifs de stockage de données tels qu'un disque dur, un disque optique, un dérouleur de bande magnétique, un circuit à l'état solide volatile ou non volatile, ou tout autre dispositif capable de stocker des informations.

[0027] Le processeur 42 peut fonctionner sous le contrôle d'un système d'exploitation 56 qui réside dans la mémoire 44. Le système d'exploitation 56 peut gérer les ressources informatiques de telle sorte que le code de programme de l'ordinateur intégré sous forme d'une ou de plusieurs applications logicielles, telles que l'application 58 qui réside dans la mémoire 44, puisse contenir des instructions exécutables par le processeur 42. Dans un mode de réalisation, le processeur 42 peut exécuter l'application 58 directement et dans ce cas le système d'exploitation 56 peut être omis. Une ou plusieurs structures de données 60 peuvent aussi résider dans la mémoire 44 et peuvent être utilisées par le processeur 42, le système d'exploitation 56 ou l'application 58 pour conserver ou manipuler des données.

[0028] L'interface I/O 48 peut fournir une interface machine qui couple de façon fonctionnelle le processeur 42 aux autres dispositifs et systèmes, tels que le réseau 26 ou la ressource externe 52. L'application 58 peut ainsi collaborer avec le réseau 26 ou la ressource externe 52 en communiquant par l'intermédiaire de l'interface I/O 48 afin de fournir une variété de caractéristiques, de fonctions, d'applications logicielles, de processus, ou de modules comprenant les modes de réalisation de l'invention. L'application 58 peut aussi avoir un code de programme exécutable par une ou plusieurs ressources externes 52, ou reposant autrement sur des fonctions ou signaux fournis par d'autres systèmes ou par des composants de réseaux externes au système informatique 40. En effet, au vu des configurations

matérielles et logicielles presque infinies possibles, les hommes de métier comprendront que les modes de réalisation de l'invention peuvent inclure des applications localisées extérieurement au système informatique 40, distribuées à des ordinateurs multiples et à d'autres ressources externes 52, ou apportées par des ressources informatiques (matérielles et logicielles) telles qu'un service de cloud computing, fournies comme services via le réseau 26.

[0029] Le HMI 50 peut être couplé de façon fonctionnelle au processeur 42 du système informatique 40 d'une façon connue pour permettre à un utilisateur d'interagir directement avec le système informatique 40. Le HMI 50 peut inclure des écrans vidéos ou alphanumériques, un écran tactile, un haut-parleur et tout autre indicateur visuel et audio capable de fournir des données à l'utilisateur. Le HMI 50 peut aussi inclure des dispositifs de saisie et des contrôles tels qu'un clavier alphanumérique, un périphérique de pointage, des claviers, des boutons poussoir, des boutons de commande, des microphones, etc., capables d'accepter des commandes ou des saisies de l'utilisateur, et de les transmettre au processeur 42.

[0030] Une base de données 50 peut résider sur le dispositif de mémoire de masse 46, et peut être utilisée pour recueillir et organiser les données utilisées par les différents systèmes et modules décrits dans les présentes. La base de données 54 peut inclure des données et des structures de données qui les supportent pour stocker et organiser les données. En particulier, la base de données 54 peut être agencée selon toute organisation ou structure de base de données incluant, mais de façon non exhaustive, une base de données relationnelle, une base de données de type hiérarchique, une base de données en réseau, ou des combinaisons de celles-là. Un système de gestion de base de données, sous forme d'une application logicielle d'ordinateur qui exécute les instructions du processeur 42, peut être utilisé pour accéder aux informations ou aux données stockées dans des enregistrements de la base de données 54 en réponse à une demande, lorsque la demande peut être déterminée de façon dynamique et exécutée par le système d'exploitation 56, les autres applications 58, ou un ou plusieurs modules.

[0031] Faisant maintenant référence à la FIG. 3, le dispositif client 12 peut télécharger l'application 27 en mémoire. De façon spécifique, le dispositif client 12 peut connecter un serveur d'applications 70 via le réseau 26 et télécharger l'application 27 sur la mémoire du dispositif client 12. Comme on le voit sur la FIG.3, un certificat public (certificat PubA) peut être associé à l'application 27. Une fois que l'application 27 a été téléchargée avec succès, un utilisateur final, tel qu'un voyageur, peut créer un mot de passe. Le mot de passe peut être exigé pour accéder à l'application 27. Dans un mode de réalisation, le mot de passe peut être saisi manuellement dans le dispositif client 12 en utilisant un clavier (non illustré). Cependant, les hommes de métier comprendront que d'autres approches peuvent aussi être utilisées pour saisir le mot de passe. Dans un mode de réalisation, il peut être nécessaire de saisir le mot de passe à deux reprises afin d'empêcher une saisie erronée. Une fois que le mot de passe est créé, le mot

de passe peut être conservé sous forme d'empreinte numérique dans la mémoire du dispositif client 12 pour un usage ultérieur. Les hommes de métier comprendront que le hachage de mots de passe consiste à créer, à partir d'un mot de passe de longueur variable, un mot de passe cryptique de longueur fixe, basé sur le mot de passe d'origine de longueur variable.

[0032] Le dispositif client 12 peut aussi générer une paire de clés asymétriques (PubP, PrivP). PubP représente la clé publique et PrivP représente une clé secrète. La cryptographie asymétrique, aussi désignée comme cryptographie de clé publique, est un système cryptographique qui utilise une paire de clés. Notamment, la clé publique (PubP) peut être largement disséminée et la clé secrète (PrivP) peut avoir un accès contrôlé grâce à l'utilisation du mot de passe. Les clés asymétriques sont enregistrées dans la mémoire du dispositif client 12.

[0033] Une fois que l'application 27 et les clés asymétriques sont enregistrées dans la mémoire du dispositif client 12, l'utilisateur final peut s'identifier sur l'application 27. Spécifiquement, l'utilisateur final peut s'identifier sur l'application 27 et saisir le mot de passe. Si le mot de passe haché saisi par l'utilisateur correspond à l'empreinte numérique sauvegardée précédemment dans la mémoire du dispositif client 12, l'accès à la clé secrète PrivP ainsi que l'accès à des transactions ultérieures sont accordés. Spécifiquement, l'utilisateur final peut maintenant enregistrer une ou plusieurs cartes de crédit qui peuvent être utilisées pour l'achat d'un produit, par exemple un billet d'avion, en utilisant l'application 27. Chaque carte de crédit est associée à un numéro de carte de crédit unique.

[0034] Faisant maintenant référence à la FIG. 1, on remarquera que le dispositif client 12 doit être connecté au réseau 26 avant que la carte de crédit ne soit enregistrée. L'enregistrement d'une carte de crédit unique à l'aide de l'application 27 du dispositif client 12 est maintenant expliquée. Tout d'abord, l'utilisateur final peut choisir une option pour enregistrer un nouveau numéro de carte de crédit à l'aide du dispositif client 12. Par exemple, l'utilisateur final peut choisir une option telle que, par exemple, « Enregistrer une carte », sur un menu qui est affiché sur l'écran 24 du dispositif client 12. L'utilisateur final peut ensuite saisir le numéro de carte de crédit et les autres détails liés à la carte de crédit à l'aide d'un clavier ou d'une autre interface utilisateur du dispositif client 12. Cependant, on remarquera que d'autres approches peuvent être utilisées également pour saisir les informations de la carte de crédit telles que, par exemple, la véritable carte de crédit prise en photo, puis son analyse à l'aide d'une technologie de reconnaissance optique de caractères (OCR). Des détails de carte de crédit incluent, par exemple, mais de façon non limitative, une date d'expiration associée à la carte, le nom du principal détenteur de la carte, l'adresse du principal détenteur de la carte, et la valeur de vérification de la carte (CVV) associée à la carte de crédit. Une fois que l'utilisateur final a saisi le numéro de la carte de crédit et les détails associés à la carte de crédit, une vérification de la carte de crédit peut être effectuée par l'application 27 pour confirmer la date d'expiration. L'application 27 peut aussi exécuter un algorithme de Luhn, qui consiste en

une formule de somme de contrôle, pour vérifier que le numéro de carte de crédit ne comporte pas de chiffres erronés.

[0035] Une fois que le numéro de carte de crédit et les détails associés à la carte de crédit sont vérifiés, l'application 27 et le dispositif client 12 peuvent construire des données cryptées de charge utile, désignées comme les données de charge utile de provisionnement de la carte. De façon spécifique, l'application 27 du dispositif client 12 peut obtenir le certificat public PubA. L'application 27 peut ensuite générer une clé symétrique S1 et son vecteur initial associé I1. La clé symétrique S1 et le vecteur initial I1 peuvent être concaténés et signés ensuite par la clé secrète (PrivP) afin d'obtenir $(S1, I1)^*_P$, dans lequel le « * » dénote que la valeur est signée. L'application 27 peut ensuite concaténer la clé symétrique S1, le vecteur initial I1 et $(S1, I1)^*_P$, puis crypter ces valeurs en utilisant le certificat public PubA sur la base d'un schéma de remplissage par cryptage asymétrique optique (Optical Asymmetric Encryption Padding, ou [OAEP]) pour obtenir $(S1, I1, (S1, I1)^*_P)'_A$, ou le « ' » dénote que la valeur est cryptée.

[0036] L'application 27 du dispositif client 12 peut ensuite signer le numéro de carte de crédit qui est dénoté dans les présentes comme N, à l'aide de la clé secrète PrivP pour obtenir la signature N^*_P. Le numéro de carte de crédit N peut ensuite être concaténé avec la signature N^*_P et crypté avec la clé symétrique S1 pour obtenir $(N, N^*_P)'_{S1}$. Enfin, l'application 27 du dispositif client 12 peut concaténer le certificat de la clé publique PubP, le résultat étant désigné comme certP, avec $(S1, I1, [S1, I1]^*_P) »_A$ et $(N, N^*_P) »_{S1}$. Le résultat donne les données de charge utile de provisionnement de la carte. Le dispositif client 12 peut envoyer les données de charge utile de provisionnement de la carte, comprises dans la demande de provisionnement de la carte, au serveur 16 via le réseau 26.

[0037] En réponse à la réception de la demande de provisionnement de la carte, le serveur 16 peut en extraire les données de charge utile de provisionnement et décrypter ensuite les données de charge utile de provisionnement de la carte pour obtenir le numéro de la carte de crédit N. De façon spécifique, le serveur 16 peut par la suite obtenir la clé symétrique S1, le vecteur initial I1 et $(S1, I1)^*_P$, et décrypter chacune des valeurs avec un certificat privé PrivA. Le certificat privé PrivA est la clé secrète associée au certificat public PubA, et le certificat public PubA ainsi que le certificat privé Priv A sont générés avant que l'application 27 ne soit sauvegardée sur le serveur d'applications 70. Le serveur 16 peut ensuite vérifier la signature de $(S1, I1)^*_P$ de la clé symétrique S1 et le vecteur initial I1 à l'aide du certificat concaténé de la clé publique certP. Le serveur 16 peut alors obtenir le numéro de la carte de crédit N et N^*_P et décrypter ces deux valeurs en utilisant la clé symétrique S1. Puis, la signature N^*_P du numéro de la carte de crédit N peut être vérifiée à l'aide du certificat concaténé de la clé publique certP.

[0038] Le serveur 16 peut ensuite envoyer le numéro de la carte de crédit N à une application de tokénisation74. L'application de tokénisation74 peut alors générer un jeton de carte de crédit T sur la base du numéro unique de carte de crédit N. Les hommes de métier comprendront que les jetons ne peuvent

pas être utilisés en dehors du contexte d'une transaction unique spécifique avec un commerçant spécifique. L'application de tokénisation74 peut ensuite renvoyer le jeton de carte de crédit T au serveur 16. L'application de tokénisation 74 peut aussi envoyer le jeton T ainsi que le numéro unique de la carte de crédit N à la chambre forte de jetons 18. La chambre forte de jetons 18 est le seul élément compris dans le système d'exploitation 10 où le jeton de la carte de crédit T est mappé sur le numéro unique de la carte de crédit N.

[0039] En réponse à la réception du jeton de carte de crédit T en provenance de l'application de tokénisation74, le serveur 16 peut ensuite générer une clé symétrique S2 et son vecteur initial I2. Dans un mode de réalisation, la clé symétrique S2 est basée sur la norme de cryptage 128 bits avancée utilisant le mode de cryptage avec enchainement de blocs de données (AES 128 CBC). Le serveur 16 peut ensuite concaténer la clé symétrique S2 et le vecteur initial I2, puis signer la valeur avec le certificat privé PrivA pour obtenir $(S2, I2)^*_A$. Le serveur 16 peut ensuite concaténer la clé symétrique S2, le vecteur initial I2 et $(S2, I2)^*_A$ et les crypter avec la clé publique PubP sur la base du schéma de remplissage OAEP pour obtenir $(S2, I2, [S2, I2]^*_A) \gg_P$. Le serveur 16 peut ensuite signer le jeton de la carte de crédit T avec le certificat privé PrivA pour obtenir un jeton signé T^*_A. Le serveur 16 peut ensuite concaténer le jeton T avec le jeton signé T^*_A, et crypter les deux valeurs avec la clé symétrique S2 pour obtenir $(T, T^*_A) \gg_{S2}$. Enfin, le serveur 16 peut concaténer $(S2, I2, [S2, I2]^*_A) \gg_P$ et $(T, T^*_A) \gg_{S2}$. Les données de charge utile qui en résultent sont renvoyées dans une réponse de provisionnement de carte 76 via le réseau 26 au dispositif client 12.

[0040] En réponse à la réception de la réponse de provisionnement de carte 76, l'application 27 du dispositif client 12 peut vérifier le certificat concaténé du certificat privé PrivA, désigné comme certA, avec des clés à numéro personnel d'identification (PIN). Les hommes de métier comprendront que les clés PIN sont des mécanismes de sécurité permettant de résister au piratage faisant usage de certificat frauduleux. L'application 27 du dispositif client 12 peut ensuite obtenir la clé symétrique S2, le vecteur initial I2 et la signature $(S2, I2)^*_A$ et décrypter ces valeurs avec la clé secrète PrivP. L'application du dispositif client 12 peut alors vérifier la signature $(S2, I2)^*_A$ de la clé symétrique S2 et le vecteur initial I2 avec le certificat concaténé du certificat privé certA. L'application 27 du dispositif client 12 peut ensuite obtenir le jeton de la carte de crédit T ainsi que le jeton signé T^*_A et décrypter ces valeurs à l'aide de la clé symétrique S2. Puis, l'application 27 du dispositif client 12 peut vérifier le jeton signé T^*_A du jeton de la carte de crédit T avec le certificat concaténé du certificat privé certA. Enfin, après la vérification du jeton signé T^*_A, le jeton de la carte de crédit T peut être conservé dans la mémoire du dispositif client 12.

[0041] On remarquera que le dispositif client 12 enregistre le jeton de la carte de crédit T dans sa mémoire respective et que le jeton de la carte de crédit peut être utilisé ultérieurement lors d'une transaction de paiement. Si l'utilisateur final voyage et qu'il se trouve dans un pays étranger ou un autre

endroit où le service cellulaire n'est pas disponible, ou qu'il est coûteux en raison des frais d'itinérance de données, l'utilisateur final n'a pas besoin de connectivité de réseau pour effectuer le paiement d'une réservation de voyage spécifique, puisque le jeton T de la carte de crédit de l'utilisateur final a déjà été enregistré en mémoire. Par ailleurs, en remarquera que plus d'un jeton de carte de crédit peut être sauvegardé en mémoire sur le dispositif client 12, chaque jeton de carte de crédit correspondant à une carte de crédit unique. Par exemple, en faisant référence à la FIG. 4, le dispositif client 12 publie le numéro de carte de crédit 80 sur l'écran 24. On remarquera que seuls les quatre derniers chiffres des numéros de carte de crédit 80 sont lisibles pour l'utilisateur final, et que le numéro intégral de la carte de crédit n'est pas conservé en mémoire sur le dispositif client 12.

[0042] Pendant son voyage, l'utilisateur final peut avoir besoin de payer une réservation de voyage et/ou d'autres frais accessoires afférents, tels que par exemple, des frais d'excédent de bagages. Dans le mode de réalisation exemplaire montrée sur la FIG. 4, l'utilisateur final peut avoir besoin de payer des frais d'excédent de bagages qui coûtent 50 euros. Cependant, on remarquera que le mode de réalisation illustré dans la FIG. 4 est purement de nature exemplaire et que divers autres produits et frais peuvent également faire l'objet d'un achat. Faisant maintenant référence aux deux FIGS. 1 et 4, un agent peut confirmer par la suite que l'utilisateur final souhaite payer le produit (par ex., les cinquante euros pour les frais d'excédent de bagages) en utilisant une des cartes de crédit ayant un jeton T de carte de crédit correspondant sauvegardé en mémoire sur le dispositif client 12. Une fois que cela est confirmé, l'agent peut ensuite utiliser un clavier ou un autre dispositif de saisie du système commerçant 14 (non illustré) pour indiquer que l'utilisateur final souhaite payer le produit à l'aide de son dispositif client 12.

[0043] En réponse à la réception d'une indication de l'agent, l'application commerçante 28 du système commerçant 14 peut envoyer une demande au serveur 16 via le réseau 26. La demande envoyée au serveur 16 est pour un code-barres 82, ou pour des données de charge utile, indiquant une pluralité des paramètres de paiement concernant le produit. Dans le mode de réalisation exemplaire illustré dans la FIG. 4 le code-barres 82 est un code QR ; cependant, on remarquera que d'autres types de code-barres peuvent aussi être générés. Dans un mode de réalisation, les paramètres de paiement peuvent inclure, de façon non exhaustive, un montant monétaire dû (par ex., cinquante euros), un type de devise spécifique sur lequel est basé le montant monétaire (par ex., l'Euro), une description du produit (par ex., frais d'excédent de bagages) et un identifiant de référence de paiement (ID).

[0044] En réponse à la réception d'une demande en provenance du système commerçant 14, le serveur 16 peut par la suite confirmer avec le PSP 36 que le système commerçant 14 est bien autorisé à effectuer un paiement en utilisant le code-barres 82. Si le système commerçant 14 est autorisé à effectuer un paiement à l'aide du code-barres 82, le PSP 36 peut alors générer le code-barres 82. Le code-barres 82 peut être encodé avec une paire temporaire de clés asymétriques. Le PSP 36 peut ensuite envoyer une

autorisation au serveur 16. L'autorisation inclut le code-barres 82. En réponse à la réception d'une autorisation en provenance du PSP 36, le serveur 16 peut ensuite envoyer le code-barres 82 via le réseau 26 au système commerçant 14. En réponse à la réception du code-barres 82, l'application 28 du système commerçant 14 peut publier le code-barres 82 sur l'écran 24 correspondant.

[0045] Une fois que le code-barres 82 est publié sur l'écran 24 du système commerçant 14, l'utilisateur final peut ensuite positionner le dispositif client 12 de sorte que la caméra 22 peut numériser le code-barres 82. On remarquera que l'utilisateur final s'est déjà identifié sur l'application 27 du dispositif client 12 et a saisi le mot de passe avec succès. Le dispositif client 12 peut ensuite décoder le code-barres 82 afin d'en extraire les paramètres de paiement. Le dispositif client 12 peut ensuite publier les paramètres de paiement sur son écran 24. Par exemple, comme on le voit sur la FIG. 4, les paramètres de paiement indiquent que 50 € sont exigés pour le paiement des frais d'excédent de bagages. Le dispositif client 12 peut alors publier les numéros des cartes de crédit 80 ayant des jetons de cartes de crédit correspondants sauvegardés en mémoire sur le dispositif client 12.

[0046] L'utilisateur final peut ensuite sélectionner ou saisir le numéro de carte de crédit 80 qui doit être utilisé pour l'achat du produit en utilisant le dispositif client 12. Dans un mode de réalisation, l'utilisateur final peut aussi utiliser un numéro de carte de crédit par défaut 80, présélectionné au moment du paiement, ou des règles plus complexes peuvent être utilisées pour une sélection automatique d'un numéro de carte de crédit spécifique. Dans l'éventualité où un numéro de carte de crédit unique 80 aurait un jeton T de carte de crédit correspondant sauvegardé en mémoire, l'utilisateur final peut alors simplement avoir besoin de confirmer l'utilisation du numéro unique de carte de crédit 80. En réponse à la réception d'une confirmation de la part de l'utilisateur final, l'application 17 du dispositif client 12 peut alors générer un autre code-barres 84. Dans le mode de réalisation exemplaire illustré dans la FIG. 4, le code-barres 84 est également un code QR ; cependant, on notera que d'autres types de code-barres peuvent aussi être utilisés. Le code-barres 84 inclut d'autres données cryptées de charge utile. La génération de ces données cryptées de charge utile est décrite ci-dessous.

[0047] L'application 27 du dispositif client 12 peut d'abord générer une clé symétrique S3 et son vecteur initial I3. L'application 27 du dispositif client 12 peut ensuite concaténer à la fois la clé symétrique S3 et le vecteur initial I3 et signer le résultat avec la clé secrète PrivP pour obtenir $(S3, I3)^*_P$. La clé symétrique S3, le vecteur initial I3 et $(S3, I3)^*_P$ peuvent ensuite être cryptés avec le certificat public PubA sur la base d'un schéma de remplissage OAEP pour obtenir $(S3, I3, [S3, I3]^*_P) »_A$. L'application 27 du dispositif client 12 peut ensuite construire des données de charge utile L. Spécifiquement, les données de charge utile L peuvent inclure $(S3, I3, [S3, I3]^*_P) »_A$ et le jeton T de la carte de crédit. Les données de charge utile L sont ensuite signées avec la clé secrète PrivP pour obtenir L^*_P. Les données de charge utile L et les données de charge utile signées L^*_P sont aussi signées avec la clé symétrique S3 pour obtenir

(L, L**P)'$_{S3}$. Enfin, le certificat concaténé de la clé publique certP, (S3, I3, [S3, I3]*P) » $_A$ et (L, L*$_P$) » $_{S3}$ sont concaténés pour créer les données cryptées de charge utile.

[0048] L'application 27 du dispositif client 12 peut ensuite publier le code QR 84 sur l'écran 24. Une fois que l'utilisateur final voit que le code QR 84 a été publié sur l'écran 24 du dispositif client 12, l'utilisateur final peut alors positionner le dispositif client 12 de sorte que le code QR 84 soit lu par le dispositif optique 30 du système commerçant 14 en utilisant la communication en lumière visible. Le système commerçant 14 peut ensuite envoyer le code QR 84 ou les données de charge utile du code QR via le réseau 26 au serveur 16. Le serveur 16 peut ensuite décoder et valider les données cryptées de charge utile contenues dans le code QR 84. En particulier, le serveur 16 peut valider les données cryptées de charge utile afin d'obtenir le jeton de lacarte de crédit T. On remarquera que la transaction peut être annulée avant la validation. Ainsi, aucun paiement ne peut être fait en utilisant la carte de crédit de l'utilisateur final.

[0049] Le serveur 16 peut valider les données cryptées de charge utile en obtenant la clé symétrique S3, le vecteur initial I3 et (S3, I3)*$_P$ et décrypter ces valeurs en utilisant le certificat privé PrivA. Le serveur 16 peut ensuite vérifier la signature (S3, I3)*$_P$ de la clé symétrique S3 et le vecteur initial I3 en utilisant le certificat concaténé de la clé publique certP pour obtenir les données de charge utile L et les données signées de charge utile L*$_P$. Les données signées de charge utile L*$_P$ sont ensuite vérifiées par le certificat concaténé de la clé publique certP. La validation des données cryptées de charge utile permet au serveur 16 de récupérer le numéro de la carte de crédit originale N de la chambre forte de jetons 18.

[0050] Une fois que le numéro de la carte de crédit originale a été récupéré, le serveur 16 peut ensuite effectuer une autorisation de paiement pour obtenir l'autorisation de l'émetteur de la carte de crédit. Spécifiquement, le serveur 16 peut envoyer une demande via le réseau 26 au réseau de paiement 34 pour déterminer si le numéro de la carte de crédit N est valide et si l'émetteur de la carte de crédit donne son accord pour le paiement. Le réseau de paiement 34 peut renvoyer l'autorisation au serveur 16 via le réseau 26. En réponse à la réception de l'autorisation de paiement du réseau de paiement, le serveur 16 peut ensuite envoyer une réponse au système commerçant 14 via le réseau 26. La réponse indique que le numéro de la carte de crédit N est valide et que le paiement a été confirmé par l'émetteur de la carte de crédit.

[0051] En réponse à la réception de la réponse du serveur 16, le système commerçant 14 peut générer un reçu de paiement. En particulier, l'application commerçante 28 du système commerçant 14 peut générer un reçu de paiement qui est contenu dans le code-barres (non illustré). Le code-barres peut être publié sur l'écran 32 du système commerçant 14. L'utilisateur final peut alors positionner le dispositif

client 12 de sorte que la caméra 22 peut numériser le code-barres publié sur l'écran 32 du système commerçant 14.

[0052] En se référant de façon générale aux dessins, le système divulgué apporte une approche commode et conviviale permettant au dispositif client de communiquer avec le système commerçant, même si le dispositif client a peu ou pas de connectivité à un réseau. On remarquera qu'il est possible que le voyageur ne puisse pas se connecter à Internet pendant son déplacement, et plus particulièrement lorsqu'il est de passage dans des pays étrangers ou des endroits dans le monde où la connectivité des réseaux est limitée ou inexistante. En effet, le système divulgué utilise le matériel existant sur un dispositif client (par ex., la caméra) pour numériser et décoder un code-barres qui est publié sur l'écran du système commerçant. Le système divulgué apporte une approche plus efficace pour le voyageur, lui permettant ainsi de payer une réservation de voyage sans avoir besoin de sa carte de crédit physique. En d'autres termes, les voyageurs n'ont plus besoin de chercher leur carte de crédit physique, qui peut être difficile à trouver, et notamment lorsque le voyageur porte de nombreux sacs pendant son déplacement. Enfin, les cartes d'entreprise, les cartes partagées, les points de fidélité, ou même les cartes de crédit virtuelles peuvent aussi être utilisées.

[0053] Généralement, les routines exécutées pour mettre en œuvre les modes de réalisation de l'invention, qu'elles soient implémentées dans le cadre d'un système d'exploitation ou d'une application spécifique, d'un composant, d'un programme, d'un objet, d'un module ou d'une séquence d'instructions, ou même un sous-ensemble de ceux-là, peuvent être désignées dans les présentes comme « code de programme informatique » ou simplement « code de programme. » Un code de programme comporte typiquement des instructions lisibles par ordinateur qui résident à divers moments dans divers dispositifs de mémoire et de stockage dans un ordinateur et qui, lorsqu'elles sont lues et exécutées par un ou plusieurs processeurs dans un ordinateur, amènent l'ordinateur à effectuer les opérations nécessaires à l'exécution d'opérations et/ou d'éléments propres à la mise en œuvre des aspects variés des modes de réalisation de l'invention. Les instructions d'un programme, lisibles par ordinateur, pour effectuer les opérations des modes de réalisation de l'invention peuvent être, par exemple, le langage d'assemblage, ou encore un code source ou un code objet écrit en combinaison avec un ou plusieurs langages de programmation.

[0054] Divers codes de programme décrits dans les présentes peuvent être identifiés selon l'application dans laquelle ils sont implémentés dans des modes de réalisation spécifiques de l'invention. Cependant, on remarquera que toute nomenclature d'un programme particulier dans ce qui suit est utilisée uniquement par commodité ; ainsi l'invention ne peut être limitée à un seul usage dans toute application spécifique identifiée et/ou sous-entendue par ladite nomenclature. Par ailleurs, au vu du nombre généralement infini de moyens par lesquels les programmes informatiques peuvent être organisés selon

des sous-programmes, procédures, procédés, modules, objets, et ainsi de suite, ainsi que les façons variées d'affecter les fonctionnalités d'un programme parmi diverses couches de logiciels qui sont résidents dans un ordinateur typique (par ex., les systèmes d'exploitation, les bibliothèques, les interfaces d'application de programme [API], les applications, les applications courtes [applets], etc.), on remarquera que les modes de réalisation de l'invention ne sont pas limités à l'organisation spécifique ou à l'affectation spécifique des fonctionnalités de programme telles qu'elles sont décrites dans les présentes.

[0055] Le code de programme mis en œuvre dans toute application/module décrit(e) dans les présentes peut être distribué individuellement ou collectivement comme un produit programme d'ordinateur sous une variété de formes. En particulier, le code de programme peut être distribué en utilisant un support de stockage lisible par ordinateur, disposant d'instructions de programme lisibles par ordinateur, permettant à un processeur d'effectuer des aspects des modes de réalisation de l'invention.

[0056] Les supports de stockage lisibles par machine étant intrinsèquement non transitoires, peuvent inclure des médias tangibles volatiles et non volatiles, amovibles et non amovibles, implémentés dans tout procédé ou technologie de stockage d'information, tels que des instructions de programme lisibles par machine, des structures de données, des modules de programme, ou autres données. Les supports de stockage lisibles par ordinateur peuvent aussi comprendre des mémoires RAM, ROM, EPROM (mémoire à lecture exclusivement, programmable et effaçable), une mémoire flash, ou toute technologie de support solide de mémoire, CD-ROM (disque compact portable doté d'une mémoire à lecture seule), ou tout autre stockage optique, bandes d'enregistrement magnétique, mémoire à disque magnétique, ou tout autre support pouvant être utilisé pour stocker l'information désirée, et apte à être lu par un ordinateur. Un support de stockage lisible par ordinateur ne peut être interprété comme « signaux transitoires » en soi (par exemple, des ondes radio ou toute autre onde électromagnétique se propageant à travers un support de transmission tel qu'un guide d'ondes, ou des signaux électriques transmis par câble). Les instructions de programme lisibles par ordinateur peuvent être téléchargées sur un ordinateur, un autre type d'appareil de traitement de données programmable ou sur tout autre dispositif de support de stockage lisible par machine, ou vers un ordinateur externe ou vers un dispositif de stockage externe via un réseau.

[0057] Les instructions de programme lisibles par ordinateur, enregistrées sur un support lisible par ordinateur, peuvent être utilisées pour amener un ordinateur, d'autres types d'appareil programmable de traitement de données, ou d'autres dispositifs, à fonctionner d'une façon particulière, de sorte que les instructions enregistrées sur un support lisible par ordinateur produisent un article de fabrication comprenant les instructions qui mettent en œuvre les fonctions, les actions et/ou les opérations spécifiées dans les organigrammes, diagrammes de séquence, et/ou diagrammes blocs. Les instructions de programme informatique peuvent être fournies à un ou plusieurs processeurs d'un ordinateur à usage général, un ordinateur dédié ou un autre appareil programmable de traitement de données pour produire

une machine, de sorte que les instructions, lorsqu'elles sont exécutées à l'aide du ou des processeurs, accomplissent une série de calculs pour mettre en œuvre les fonctions, actions, et/ou les opérations spécifiées dans les organigrammes, diagrammes séquentiels et/ou diagrammes blocs.

[0058] Dans certains autres modes de réalisation, les fonctions, les actions et/ou des opérations spécifiées dans les organigrammes, diagrammes de séquence, et/ou des diagrammes blocs peuvent être commandées à plusieurs reprises, traitées en série, et/ou traitées en même temps conformément aux modes de réalisation de l'invention. De plus, tout organigramme, diagramme séquentiel, et/ou diagramme bloc peut inclure plus ou moins de blocs que ceux illustrés tout en restant conformes aux modes de réalisation de l'invention.

[0059] La terminologie utilisée dans les présentes a pour but de décrire uniquement des modes de réalisation particuliers et n'est pas destinée à limiter les modes de réalisation de l'invention. Par ailleurs, les termes « comprend », « comprennent » et/ou « comprenant », lorsqu'ils sont utilisés dans ces spécifications, précisent la présence de caractéristiques, de nombres entiers, d'étapes, d'opérations, d'éléments, et/ou de composants, mais n'excluent pas la présence ou l'ajout d'un(e) ou de plusieurs caractéristiques, nombres entiers, étapes, éléments, composants et/ou groupes, en cela. De plus, dans la mesure où les formes verbales « inclut », « ayant », « a », ou des variantes, sont utilisés dans la description détaillée des revendications, ces termes sont censés être inclusifs de façon similaire au verbe « comprendre ».

[0060] Bien que l'invention soit illustrée par une description de divers modes de réalisation, et bien que ces modes de réalisation soient décrits de façon très détaillée, il n'est pas de l'intention du demandeur de restreindre ou de limiter, de quelque façon que ce soit, l'étendue des revendications des présentes à ces détails. Des avantages supplémentaires et des modifications possibles apparaîtront aisément aux hommes de métier. L'invention sous un angle plus large n'est donc pas limitée aux détails spécifiques, aux procédés et aux appareils représentatifs, ni aux illustrations montrées et décrites à titre d'exemple. Par conséquent, il est possible de s'éloigner de ces détails sans pour autant s'éloigner de l'esprit et de la portée du concept inventif général du demandeur.

REVENDICATIONS

1. Un système pour l'échange sécurisé d'un jeton de carte de crédit entre un premier ordinateur et un ordinateur externe pour l'achat d'un produit, le système comprenant :

l'ordinateur externe ;

le premier ordinateur avec un ou plusieurs processeurs, une caméra couplée à un ou plusieurs processeurs, et une mémoire couplée à un ou plusieurs processeurs, la mémoire stockant des données comprenant une base de données et un code de programme qui, lorsqu'il est exécuté par un ou plusieurs processeurs, amène le système à :

numériser le premier code-barres à l'aide de la caméra, dans lequel le premier code-barres est publié sur un écran d'affichage de l'ordinateur externe et le premier code-barres indique une pluralité de paramètres de paiement du produit ;

décoder le premier code-barres pour en extraire les paramètres de paiement ;

publier les paramètres de paiement pour affichage à l'intention de l'utilisateur ;

recevoir une première saisie, dans laquelle la première saisie indique un numéro de carte de crédit pour l'achat d'un produit;

en réponse à la réception de la première saisie, générer un second code-barres qui contient les premières données cryptées de charge utile, dans lesquelles les premières données cryptées de charge utile incluent un jeton de la carte de crédit correspondant au numéro de carte de crédit, dans lequel le jeton de la carte de crédit est sauvegardé dans la mémoire ; et

publier le second code-barres pour affichage dans lequel le second code-barres est lisible par un dispositif optique de l'ordinateur externe,

dans lequel le premier ordinateur et un troisième ordinateur sont connectés à un réseau avant la numérisation du premier code-barres par la caméra, dans lequel le premier ordinateur est configuré pour :

recevoir une seconde saisie indiquant le numéro de la carte de crédit ;

générer des secondes données cryptées de charge utile qui contiennent le numéro de la carte de crédit, en réponse à la réception de la seconde saisie ;

transmettre une demande de provisionnement de carte incluant les secondes données cryptées de charge utile via le réseau,

dans lequel le troisième ordinateur est configuré pour :

recevoir la demande de provisionnement de carte via le réseau,

décrypter les secondes données cryptées de charge utile, en réponse à la réception d'une demande de provisionnement de carte, pour récupérer le numéro de la carte de crédit, envoyer le numéro de la carte de crédit à une application de tokénisation, et

dans lequel, en réponse à la réception du numéro de carte de crédit, l'application de tokénisation génère un jeton de la carte de crédit, et

dans lequel le numéro de jeton de carte de crédit est sauvegardé dans une chambre forte de jetons et est également transmis via le réseau du troisième ordinateur au premier ordinateur, et dans lequel le premier ordinateur est configuré pour conserver le jeton de la carte de crédit en mémoire sous forme d'empreinte numérique.

2. Le système selon la revendication 1 comprenant par ailleurs :

un troisième ordinateur en communication avec l'ordinateur externe dans lequel l'ordinateur externe est configuré pour envoyer le second code-barres au troisième ordinateur ; et

une chambre forte de jetons en communication avec le troisième ordinateur ;

dans laquelle le troisième ordinateur est configuré pour décoder le second code-barres, pour valider le contenu des données cryptées de charge utile afin d'obtenir le jeton de la carte de crédit et pour récupérer un numéro d'une carte de crédit originale dans la chambre forte de jetons sur la base du jeton de la carte de crédit.

3. Le système selon la revendication 2 dans lequel le troisième ordinateur est configuré pour communiquer avec un réseau de paiement afin de déterminer si le numéro de la carte de crédit originale est valide, et en réponse au numéro de la carte de crédit originale s'avérant valide, le réseau de paiement autorise le paiement du produit et envoie une autorisation au troisième ordinateur.

4. Le système selon la revendication 3 dans lequel l'ordinateur externe est configuré pour recevoir l'autorisation de paiement pour le produit en provenance du troisième ordinateur, pour générer un troisième code-barres qui contient un reçu de paiement pour le produit, et pour publier le troisième code-barres pour affichage, dans lequel le troisième code-barres est numérisé à l'aide de la caméra.

5. Le système selon l'une quelconque des revendications 1 à 4 dans lequel un ou plusieurs processeurs font partie d'un dispositif électronique mobile.

6. Un procédé pour l'échange sécurisé d'un jeton de carte de crédit entre un premier ordinateur et un ordinateur externe dans le cadre de l'achat d'un produit, le procédé comprenant :

la numérisation d'un premier code-barres par une caméra d'un premier ordinateur, dans lequel le premier code-barres est publié sur un écran d'affichage de l'ordinateur externe et le premier code-barres indique une pluralité de paramètres de paiement du produit ;

le décodage du premier code-barres, par le premier ordinateur, pour en extraire les paramètres de paiement ;

la publication, par le premier ordinateur, des paramètres de paiement pour affichage à l'intention de l'utilisateur ;

la réception, par le premier ordinateur, d'une première saisie, dans laquelle la première saisie indique un numéro de carte de crédit pour l'achat d'un produit ;

en réponse à la réception d'une première saisie, la génération par le premier ordinateur, d'un second code-barres qui contient des premières données cryptées de charge utile, dans lesquelles les premières données cryptées de charge utile incluent un jeton de la carte de crédit correspondant au numéro de carte de crédit, dans lequel le jeton de la carte de crédit est sauvegardé dans une mémoire du premier ordinateur ; et

la publication par le premier ordinateur du second code-barres pour affichage, dans laquelle le second code-barres est lisible par un dispositif optique de l'ordinateur externe,

dans lequel le procédé comprenant par ailleurs :

avant la numérisation du premier code-barres par le premier ordinateur, la connexion du premier ordinateur et du troisième ordinateur au réseau ;

la réception, par le premier ordinateur, d'une seconde saisie indiquant le numéro de carte de crédit ;

en réponse à la réception de la seconde saisie, la génération, par le premier ordinateur, de secondes données cryptées de charge utile contenant le numéro de carte de crédit ;

la transmission, par le premier ordinateur, d'une demande de provisionnement de carte incluant les secondes données cryptées de charge utile, via le réseau ;

la réception, par le troisième ordinateur, de la demande de provisionnement de carte, en provenance du réseau ;

en réponse à la réception de la demande de provisionnement de carte, le décryptage, par le troisième ordinateur, des secondes données cryptées de charge utile pour récupérer le numéro de carte de crédit ;

l'envoi, par le troisième ordinateur, du numéro de carte de crédit à une application de tokénisation ; et

en réponse à la réception du numéro de carte de crédit, la génération, par l'application de tokénisation, du jeton de la carte de crédit, et

dans lequel le procédé comprenant par ailleurs :

la sauvegarde, par le troisième ordinateur, du jeton de carte de crédit dans une chambre forte de jetons ;

la transmission, par le troisième ordinateur, du jeton de carte de crédit, sur le réseau ;

la réception sur le réseau, par le premier ordinateur, du jeton de carte de crédit ; et

l'enregistrement du jeton de la carte de crédit, sous forme d'empreinte numérique, dans la mémoire du premier ordinateur.

7. Le procédé selon la revendication 6 comprenant par ailleurs :

l'envoi sur le réseau, par l'ordinateur externe, d'un second code-barres à un troisième ordinateur ;

le décodage du second code-barres par le troisième ordinateur ;

la validation du contenu des premières données cryptées de charge utile, par le troisième ordinateur, pour obtenir le jeton de la carte de crédit ; et

la récupération, par le troisième ordinateur, d'un numéro de la carte de crédit originale d'une chambre forte de jetons, sur la base du jeton de carte de crédit.

8. Le procédé selon la revendication 7 comprenant par ailleurs :

l'envoi, par le troisième ordinateur, d'une communication à un réseau de paiement ;

en réponse à la réception de la communication, le réseau de paiement détermine la validité du numéro de la carte de crédit originale ;

en réponse au numéro de la carte de crédit originale s'avérant valide, le réseau de paiement autorise le paiement pour le produit via le réseau de paiement ; et

l'envoi, via le réseau de paiement, d'une autorisation au troisième ordinateur.

9. La procédé selon la revendication 8 comprenant par ailleurs :

la réception, par le troisième ordinateur, de l'autorisation pour le paiement du produit ;

l'envoi de l'autorisation via le réseau à l'ordinateur externe ;

la génération, par l'ordinateur externe, d'un troisième code-barres qui contient un reçu de paiement pour le produit ; et

la publication, par l'ordinateur externe, du troisième code-barres pour affichage, dans lequel le troisième code-barres est numérisé par la caméra du premier ordinateur.

10. Le procédé selon l'une quelconque des revendications 6 à 9 dans lequel le premier ordinateur est un dispositif électronique portable.

11. Un produit-programme d'ordinateur pour l'échange sécurisé d'un jeton de carte de crédit avec un ordinateur externe dans le cadre de l'achat d'un produit, le produit-programme d'ordinateur comprenant :

des portions/moyens/instructions de code de programme enregistrées sur un support lisible par ordinateur pour mettre en œuvre les étapes du procédé selon l'une quelconque des revendications 6 à 10 lorsque ledit programme fonctionne sur un ordinateur.

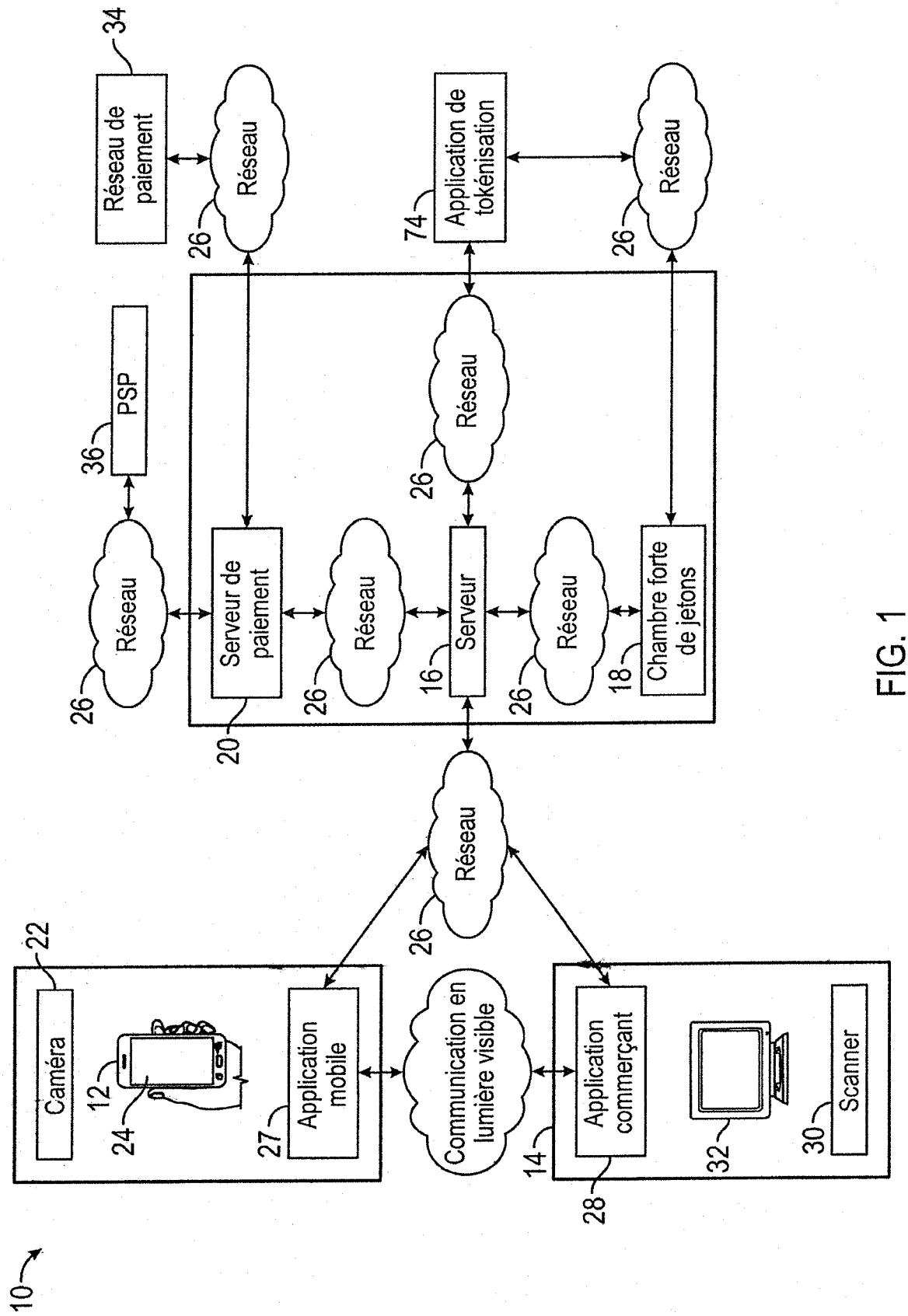
10
22
Caméra
12
24
27
Application mobile
Communication en lumière visible
14
Application commerçant
28
32
30
Scanner
26
Réseau
20
Serveur de paiement
16
Serveur
18
Chambre forte de jetons
36
PSP
34
Réseau de paiement
74
Application de tokénisation

FIG. 1

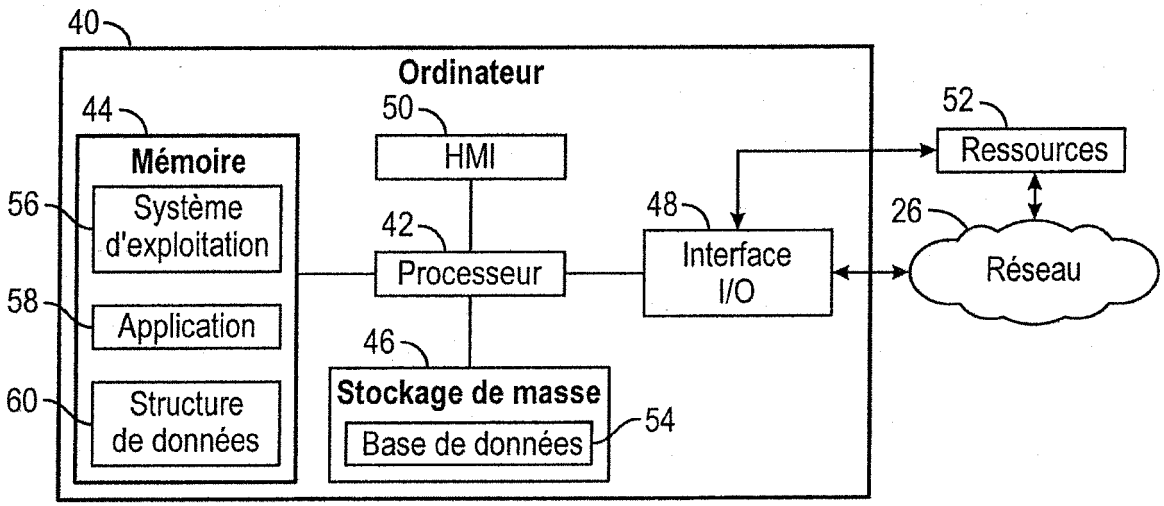
40
Ordinateur
44
Mémoire
56
Système d'exploitation
58
Application
60
Structure de données
50
HMI
42
Processeur
46
Stockage de masse
Base de données
54
48
Interface I/O
52
Ressources
26
Réseau

FIG. 2

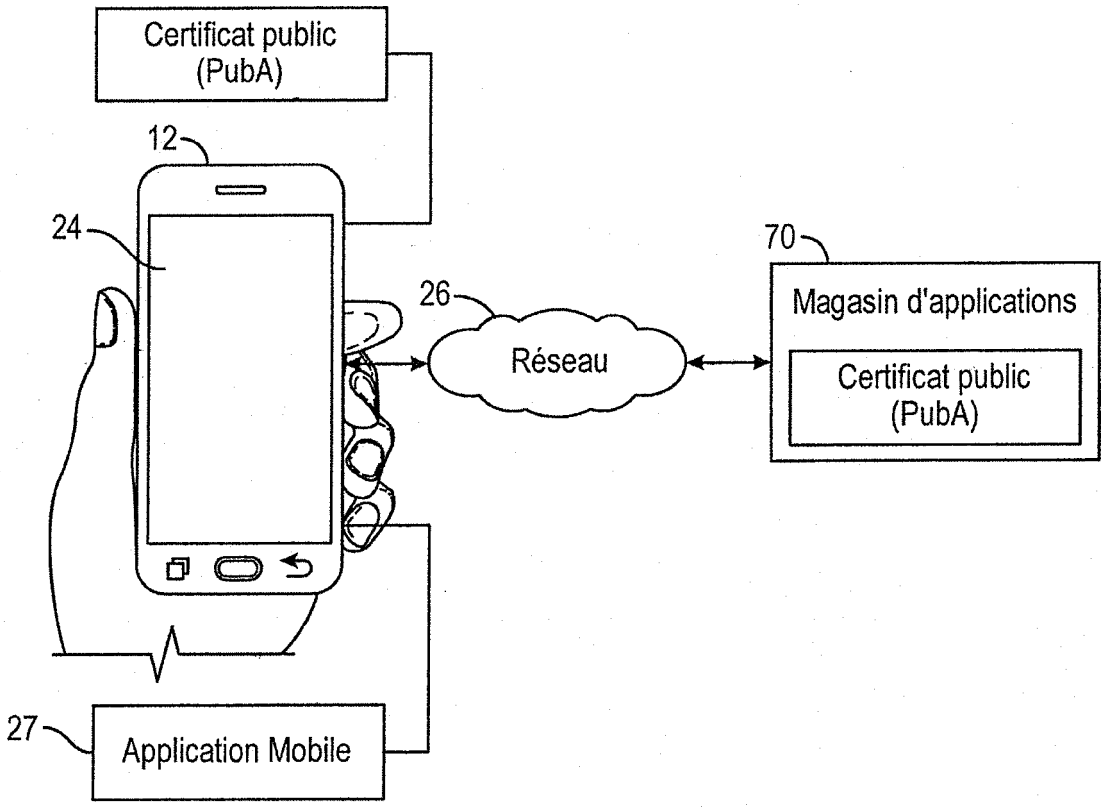
Certificat public (PubA)
12
24
26
Réseau
70
Magasin d'applications
Certificat public (PubA)
27
Application Mobile

FIG. 3

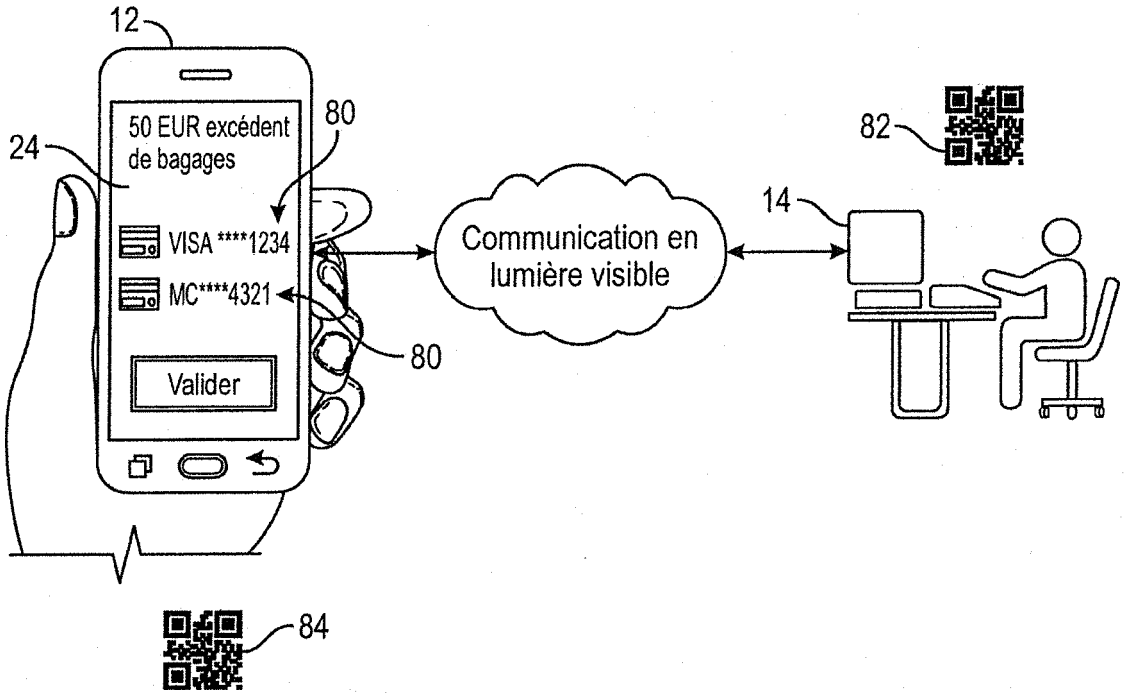
12
50 EUR excédent de bagages
24
80
VISA ****1234
MC****4321
80
Valider
Communication en lumière visible
82
14
84

FIG. 4

N° d'enregistrement national : FR1654400 N° de publication : FR3051613

RAPPORT DE RECHERCHE

articles L.612-14, L.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.
Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

[x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

☐ Le demandeur a maintenu les revendications.

[x] Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

[x] Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

☐ Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION
GB 2 478 712 A (JACKSON DAVID [GB]) 21 septembre 2011 (2011-09-21) EP 2 819 080 A1 (SAP SE [DE]) 31 décembre 2014 (2014-12-31) US 2013/262317 A1 (COLLINGE MEHDI [BE] ET AL) 3 octobre 2013 (2013-10-03) WO 2015/054697 A1 (VISA INT SERVICE ASS [US]) 16 avril 2015 (2015-04-16)
2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL
NEANT
3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES
NEANT