(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
27 septembre 2012 (27.09.2012)

WIPO | PCT

(10) Numéro de publication internationale
WO 2012/127024 A2

(51) Classification internationale des brevets :
G06Q 20/00 (2012.01) *H04L 9/32* (2006.01)
G07F 7/08 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2012/055180

(22) Date de dépôt international :
23 mars 2012 (23.03.2012)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1152403 23 mars 2011 (23.03.2011) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **LE CHEQUE DEJEUNER CCR** [FR/FR]; 27-29 avenue des Louvresses, F-92230 Gennevilliers (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : **PASQUET, Marc** [FR/FR]; 43 Quai de Juillet, F-14000 Caen (FR).

(74) Mandataire : **DELPRAT, Olivier**; Bureau D.A. Casalonga & Josse, 8 Avenue Percier, F-75008 Paris (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

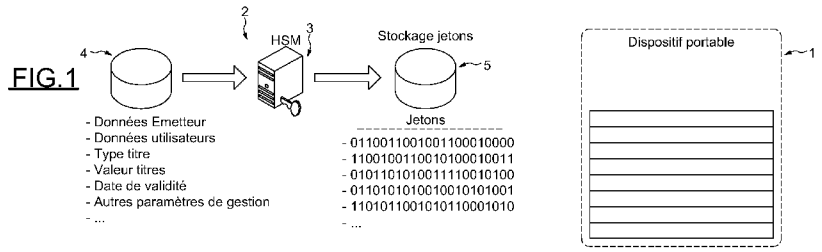
Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport (règle 48.2.g))*

(54) Title : METHOD FOR GENERATING AND USING A BOOK-ENTRY SECURITY IN A PORTABLE DEVICE AND CORRESPONDING SECURITY MANAGEMENT SYSTEM

(54) Titre : PROCEDE DE GENERATION ET D'UTILISATION D'UN TITRE DEMATERIALISE DANS UN DISPOSITIF PORTABLE ET SYSTÈME DE GESTION DE TITRES CORRESPONDANT

FIG.1



(57) Abstract : The invention relates to a method for generating and using a book-entry security in a portable device, including: a step comprising the selection of data relating to security management parameters; a step comprising the processing of said data, such as to generate a token; a step comprising the securement of the token by the processing means of a token issuing device; and a step comprising the storing of the secure token in a secure memory zone of the portable device.

(57) Abrégé : Procédé de génération et d'utilisation d'un titre dématérialisé dans un dispositif portable comportant : - une étape de sélection de données relatives à des paramètres de gestion de titre; - une étape de traitement desdites données de sorte à générer un jeton; - une étape de sécurisation dudit jeton par les moyens de traitement d'un dispositif d'émission de jetons, et - une étape de mémorisation dudit jeton sécurisé dans une zone de mémoire sécurisée dudit dispositif portable.

WO 2012/127024 A2

Procédé de génération et d'utilisation d'un titre dématérialisé dans un dispositif portable et système de gestion de titres correspondant

L'invention se rapporte à un procédé de génération et à un procédé d'utilisation d'un jeton stocké dans un dispositif portable, et à un système de gestion de jetons correspondant.

L'invention s'inscrit dans le domaine des transactions électroniques pouvant être effectuées à partir d'un dispositif portable.

Dans le cadre de systèmes transactionnels, des documents, ci-après nommés titres, susceptibles de conférer un droit, ne serait-ce que temporaire, sont délivrés à un utilisateur afin qu'il puisse bénéficier de l'obtention d'un service ou d'un bien auprès d'un organisme en échange de ce document.

Un tel titre se rapporte par exemple à un titre restaurant, un bon de réduction, un ticket de parking ou encore à un titre de paiement.

Le titre restaurant est par exemple matérialisé par des coupons papier sécurisés.

Dans le cadre de la gestion de ces titres et plus précisément pour ce qui concerne la gestion des titres restaurant, celle-ci est très contraignante.

En effet, un salarié a droit à un et un seul titre restaurant par jour de travail effectif, les jours d'absence du salarié en étant exclus, quel que soit le motif, et notamment pour cause de maladie ou de congés.

Dans un tel contexte, il apparaît inenvisageable dans la pratique, tant du point de vue de l'employeur que de celui du salarié, de distribuer quotidiennement un titre restaurant par salarié. Ainsi, dans la plupart des cas l'employeur commande des carnets de plusieurs titres restaurant afin qu'un ou plusieurs de ces carnets soient distribués à chaque salarié en début de mois. Dans ce mode de fonctionnement un titre restaurant ne peut être utilisé que par le salarié auquel il a été remis par l'employeur.

Cependant, un inconvénient majeur qui se pose dans la mise en œuvre d'un tel procédé est lié au fait que des contraintes obligent l'employeur à commander les carnets de titres par avance et à maintenir une liste des titres distribués à chaque salarié, tout en veillant à ne pas accumuler trop de carnets de titres, ceux-ci ayant de façon connue une période de validité déterminée. Un tel procédé n'est donc pas satisfaisant car il requiert des ressources matérielles et humains importantes.

Pour pallier cet inconvénient on connaît dans l'art antérieur des procédés permettant de gérer des documents de même nature que ceux précédemment évoqués mais sous une forme dématérialisée. De tels documents sont gérés habituellement sous formes de compteurs associés à des paramètres de gestion tel que le titre, la date de validité, la ou les valeurs, etc...

Dans de tels procédés, les mécanismes de dématérialisation de titres avec des compteurs sont gérés de deux manières différentes.

Selon une première technique, des compteurs correspondants aux différents titres utilisés sont implémentés dans une carte à puce d'authentification, cette carte à puce étant prévue pour être utilisée avec un terminal lecteur de cartes.

Ce terminal a pour fonction d'effectuer des opérations de débits de titres en mode non connecté en contrôlant le type, la validité et le ou les compteurs des titres, ainsi que de réaliser la décrémentation des compteurs, la génération des transactions de débit et, en mode connecté, la télécollecte périodique de ces transactions vers un serveur de gestion.

Ce terminal permet également de recharger la carte à puces en titres en mettant en œuvre des étapes d'authentification de la carte, de contrôle des compteurs et leurs paramètres respectifs, de connexion au serveur de gestion afin d'incrémenter les compteurs des nouveaux titres à disposition.

Une seconde manière consiste en ce que le terminal est cette fois-ci connecté au serveur de gestion des titres. Les opérations de débits des titres sont alors effectuées *via* le terminal par le serveur de

gestion des titres. Ainsi une fois la carte authentifiée, le terminal transmet le type de titre et le nombre de titres à décrémenter. Le serveur effectue un contrôle et décrémente les compteurs correspondant au type de titre et enregistre la transaction.

Le chargement des nouveaux titres est effectué directement sur le serveur de gestion des compteurs.

Un inconvénient majeur est qu'une telle solution comporte un certain nombre de contraintes liées à la gestion des compteurs implémentés dans la carte à puce d'authentification, et rend par conséquent difficile leur intégration et leur traitement dans la chaîne de gestion de compensation financière.

De plus, un autre inconvénient important se rapporte à la gestion des compteurs et des contraintes liées à leur cohérence en fonction d'un référentiel, qui peut être compris dans la carte à puce ou centralisé dans une base de données, et qui demande des contrôles permanents afin d'assurer l'intégrité de ces compteurs, lesdits contrôles requérant des ressources matérielles de façon importante et constante.

On pourra enfin se référer au document EP-A-1 411 482, qui décrit un système de gestion de tickets dématérialisés dans lequel un crédit de jetons alloués à des utilisateurs est mémorisé et géré de manière centralisée au sein d'une société émettrice et dans lequel des ordres de compensation financière sont directement transmis de l'utilisateur vers la société émettrice.

Cette solution nécessite une gestion lourde des jetons et est difficile à mettre en œuvre dans la mesure où elle nécessite l'établissement de plusieurs connexions pour le débit des jetons et la transmission des ordres de compensation financière.

L'invention propose d'améliorer l'interopérabilité et la portabilité des mécanismes de dématérialisation de titres, du type titre restaurant, de sorte à les rendre compatible avec les systèmes de gestion existant pour de tels titres.

De plus, la présente invention confère l'avantage de diminuer le temps d'occupation des ressources matérielles des dispositifs

sollicités lors de la mise en œuvre du procédé solution de cette invention, et donc la consommation énergétique qui en résulte.

L'invention permet également de ne plus requérir des contrôles de cohérence comme c'est le cas dans le cadre de la gestion de compteurs, et d'améliorer la sécurité dans de tels mécanismes de dématérialisation de titres.

L'invention a donc pour objet un procédé de génération d'un titre dématérialisé, comportant :

- une sélection de données relatives à des paramètres de gestion du titre ;
- un traitement desdites données de sorte à générer un jeton ;
- une sécurisation dudit jeton ;
- une transmission du jeton sécurisé vers un dispositif portable distant ; et
- une mémorisation dudit jeton sécurisé dans une zone de mémoire sécurisée du dispositif portable.

On comprendra que la mémorisation du jeton dans une zone sécurisée du dispositif portable offre l'avantage d'éviter qu'il ne puisse être subtilisé et/ou qu'il soit dupliqué.

Avantageusement, l'étape de sécurisation consiste à chiffrer ledit jeton à partir d'une clé cryptographique.

Dans un mode de mise en œuvre, les étapes de génération et de sécurisation du jeton sont mises en œuvre au sein d'un centre serveur centralisé. En outre, lors de l'étape de mémorisation, on établit une communication avec le dispositif portable distant.

Par exemple, le dispositif portable est un dispositif de stockage données, notamment de type carte à puce ou carte mémoire.

Le dispositif portable peut être un poste de télécommunication sans fil.

L'invention a également pour objet un procédé d'utilisation d'un titre dématérialisé stocké dans une zone mémoire d'un dispositif portable, comprenant les étapes suivantes :

- établissement d'un canal de communication sécurisé entre le dispositif portable et un dispositif tiers servant à la mise en œuvre d'une transaction pour le débit de titres ;

- transmission d'un titre vers le dispositif tiers ;

- établissement d'une communication entre le dispositif tiers et un centre de collecte ; et

- transfert dudit titre du dispositif tiers vers le centre de collecte.

Dans un mode de mise en œuvre, le dispositif comprend, stocké en mémoire, un ensemble de titres dématérialisés, le procédé comprenant en outre une étape de sélection automatique du titre à transmettre vers le dispositif tiers.

L'invention a encore pour objet un système de gestion de titres dématérialisés stockés dans des zones mémoires sécurisées d'un ensemble de dispositifs portables, comprenant une plateforme de gestion comprenant

- des moyens de stockage de données pour le stockage de données relatives à des paramètres de gestion des titres,

- un centre serveur de gestion comprenant des moyens de traitement pour gérer des jetons à partir des paramètres de gestion,

- des moyens de communication adaptés pour communiquer avec des moyens de communication correspondants des dispositifs portables pour la recharge des dispositifs en titres dématérialisés, et

- un réseau de dispositifs tiers servant à la mise en œuvre de transactions tendant à débiter les dispositifs en titres dématérialisés, et comprenant des premiers moyens de communication adaptés pour communiquer avec des moyens de communication correspondants des dispositifs pour établir un premier canal de communication sécurisé et avec les moyens de communication de la plateforme pour établir un deuxième canal de communication sécurisé.

Selon une autre caractéristique, la plateforme comporte une base de données de stockage des titres dématérialisés générés, raccordée au centre serveur.

Par exemple, un titre dématérialisé est un titre de paiement.

D'autres buts, caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante, donnée uniquement à titre d'exemple non limitatif, et fait en référence aux dessins annexés sur lesquels :

- la figure 1 est une représentation d'un système de gestion de titres selon l'invention illustrant la procédure de génération des jetons ;
- la figure 2 est une représentation du système de gestion de la figure 1, illustrant la procédure de stockage des titres dans le dispositif portable ; et
- la figure 3 est un procédé d'utilisation de titres selon un mode de mise en œuvre de l'invention.

Le système de gestion de titres dématérialisés illustré à la figure 1 est destiné à l'élaboration de titres dématérialisés destinés à être mémorisés et utilisés dans un dispositif portable 1.

Dans l'exemple de mise en œuvre, les titres dématérialisés se présentent sous la forme de jetons correspondant à des titres de paiement dématérialisés. Comme indiqué précédemment, il s'agit par exemple, mais de manière nullement limitative de titres de paiement, tels que des titres restaurants, des bons de réduction, des tickets de parking...

Ce titre dématérialisé est un objet numérique. Cet objet numérique correspond à un ensemble structuré de données, sur lequel une signature électronique est apposée à partir d'une clé privée émise par une autorité de confiance. Cet objet numérique correspond à un fichier numérique comportant cet ensemble structuré de données dont notamment les paramètres de gestion de titre.

L'entité qui joue le rôle de tiers de confiance est l'émetteur de la carte, qui peut se fournir en certificat maître auprès d'une autorité de confiance reconnue pour la délivrance de ces certificats.

Comme on le voit sur la figure 1, le système de gestion comporte essentiellement une plateforme de gestion 2 centralisée, assurant l'élaboration proprement dite des jetons, comprenant un dispositif émetteur de jetons 3, une première base de données 4 dans

laquelle sont stockées des informations servant à l'élaboration des jetons, et une deuxième base de données 5 dans laquelle sont stockés les jetons, après avoir été générés.

Le dispositif émetteur de jetons 3, dénommé serveur HSM, comprend un centre serveur de gestion associé à un dispositif HSM (acronyme de « Hardware Security Module », qui signifie Module Matériel de Sécurité), sous la forme d'un jeton sécurisé à partir d'algorithmes cryptographiques. Ce jeton avant d'être sécurisé est alors généré à partir de paramètres de gestion contenus dans la première base de données 4 reliée à ce serveur HSM.

Les paramètres de gestion entrant dans la réalisation du jeton comportent les caractéristiques du titre en question à savoir, et de manière non exhaustive : numéro de série, nom de société ou collectivité employeur de l'utilisateur, valeur du titre, millésime, date de validité, etc....

L'ensemble de ces paramètres est signé avec des algorithmes tels que RSA, DES, 3xDES, SHA, AES, etc....

Ce serveur HSM comporte des moyens pour sécuriser l'objet numérique, donc le jeton. Le jeton sécurisé ainsi obtenu étant ensuite archivé dans une base de données.

Le mode de sécurisation utilisé pour les jetons, est de signer, à l'aide d'une clef cryptographique utilisée par le HSM, les éléments constitutifs du jeton. Le jeton selon les cas peut être aussi chiffré à l'aide d'une clé privée du HSM.

Dans le présent mode de réalisation et de manière non limitative, la clé cryptographique est associée à l'émetteur de la carte.

La sécurisation est effectuée suite à la réception d'une commande de génération de jeton par la société employeur de l'utilisateur.

Ce serveur HSM est un appareil qui stocke des clefs et effectue des calculs cryptographiques dans une enceinte considérée comme inviolable. Il s'agit, plus particulièrement d'un matériel électronique offrant un service de sécurité qui consiste à signer et chiffrer des

jetons sous la forme de certificats. Ces jetons sont stockés dans la base de données 5.

Le serveur HSM comporte des moyens de traitement tels qu'un processeur et des moyens de mémoire (mémoire vive et une mémoire morte). Ces moyens de traitement sont aptes à mettre en œuvre un programme d'ordinateur, archivé dans les moyens de mémoire, comportant des instructions visant la génération de jetons sécurisés. Les variables nécessaires à l'exécution de ce programme sont mémorisées au besoin dans la mémoire sécurisée. Ces variables se rapportent par exemple aux paramètres de gestion.

La plateforme de gestion 2 est par ailleurs pourvue d'un module de communication comprenant des moyens de communication (non représentés) capables de communiquer avec des moyens de communication correspondants prévus dans le dispositif portable 1. Ces moyens de communication peuvent être constitués par des moyens de télécommunication sans fil ou des moyens de télécommunication filaires. Toutefois, dans un mode de réalisation avantageux, ces moyens de communication sont prévus dans la plateforme de gestion, d'une part, et dans le dispositif portable, d'autre part, sont aptes à communiquer via les réseaux mobiles ou Internet et ce, de manière sécurisée.

En outre, comme cela sera décrit en détail par la suite, la plateforme de gestion 2 est dotée de moyens de communication capables de communiquer avec des dispositifs tiers, de type terminaux de paiement, de manière à établir un canal de communication sécurisé.

Le serveur HSM comporte également des moyens d'accès aux bases de données 4 et 5, dont l'une comporte des données utilisées par le serveur HSM pour l'élaboration des jetons sécurisés et l'autre pour archiver ces jetons.

Le serveur HSM est également relié à un centre de collecte se rapportant à des serveurs aptes à émettre des commandes nécessaires au déclenchement de la création de jetons sécurisés par ce serveur HSM.

Ce serveur HSM ainsi que les bases de données sont disposés dans la plateforme technique de gestion gérée par une entité qui peut être par exemple une entreprise d'émission de titres matériels, ou encore une entreprise d'émission de titres restaurant sous forme papier.

En ce qui concerne le jeton, celui-ci comporte un certificat contenant, notamment, les données suivantes :

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 41 (00x29)
Signature Algorithm: sha1WithRSSAEncryptio n
Issuer: CC=FR, ST=FRANCE, L=Saint-lo, O=CEV, OU=CEV,
Validity
Not Before: Mar 22 17:56:55 2010 GMT
Not After: Mar 22 17:56:55 2011 GMT
Subject: C=FR, ST= FRANCE, O =CEV, CN=ssqfdsqgfqsdgghdfqsdhqgssdghs
Subject Public Key Innfo:
Public Key Algorithm: rsaEncrryption
RSA Public Key: (512 bit)
Modulus (512 bit):
00:bd:55:a00:f9:e0:fb:355:83:fe:97:e6 :41:59:e7:
e0:f4:b1:688:36:63:6a:c55:ff:c8:95:d4 :42:29:a5:
25:ae:94:b22:b3:69:b7:773:21:36:4b:fff:72:89:ca:
65:e4:72:100:4e:dd:91:777:2d:90:02:665:3d:f6:89:
e6:2f:7b:000:61
Exponent: 655537 (0x100011)
Signature Algorithm: sha1WithRSAEncryption

7a:69:4ee:83:4d:9b:a99:ff:2a:59:0f:03:16:9d:16 :b7:05:bc:
af:ca:09:f2:a9:89:8a::1c:ff:9d:4d:000:ab:a7:96:33f:1e:53:
f6:3a:62:22:6a:58:9f::63:18:94:51 :9c:ba:93:fb::e2:68:0e:
75:b0:811:9f:cd:ad:6f::0c:25:25:61 :8c:39:62:399:2d:82:de:

8f:f6:fc:446:27:3c:c7:bb1:b2:b7:d6:229:42:39:c7: e2:97:f2:
57:13:977:30:1d:71:a33:54:0f:bf:277:10:81:71:0f :7f:f0:8a:
b6:0b:211:ef:0e:69:733:c5:58:8d:800:45:3b:f6:a55:dd:57:05:
79:17:5dd:64:37:83:5ff:ea:a0:c2:8f:e5:a2:1c:6f::41:25:88:
2b:c4:1bb:cd:b5:13:288:6e:04:f9:a44:d9:67:77:a11:af:b3:4c:
cc:1e:d22:0f:90:78:6e :43:43:1f:51 :05:8d:19:477:c4:a1:0c:
de:78:f4:db:44:a0:166:80:5b:b9:822:66:a8:23:9ff:d3:8a:ed:
34:b1:b44:87:eb:ef:4cc:b2:28:7c:d11:44:fb:4d:044:9a:e1:7b:
82:31:811:6d:f5:20:833:8d:14:ff:6f:dd2:f3:c5:83:eef:80:f7:
73:fb:29:13:c9:3a:300:3e:02:e5:b33:77:c0:0a:c88:28:57:83:
76:f7:dd:aa

Contrairement au document dématérialisé selon l'état de la technique qui est implémenté sous la forme d'un compteur, le jeton est dans la présente invention complètement autonome du fait qu'il comporte les éléments tels que les paramètres de gestion du titre dématérialisé, notamment, type de titre, date de validité, valeur, numéro de série du titre, identifiant de l'émetteur, identifiant, ... et la signature de l'ensemble.

Le jeton après avoir été généré est archivé dans une zone sécurisée du dispositif portable 1.

On notera que le dispositif portable 1 peut être réalisé de diverses manières.

Dans un premier mode de réalisation, le dispositif portable 1 est réalisé sous la forme d'un support de stockage de données, de type carte à puce, contenant un microcontrôleur et de la mémoire, de type carte à microcircuit, carte SIM, ..., ou de type carte à mémoire amovible de stockage de données, de type carte micro SD, SDHC, ...

Le dispositif portable 1 peut encore comporter un support de stockage de données de type périphérique, comme par exemple clé USB ou une clé Firewire.

Dans ce mode de réalisation, le dispositif portable est prévu pour être inséré dans un équipement ou terminal informatique ou de télécommunication.

Dans un autre mode de réalisation, le dispositif portable peut être constitué par un équipement de communication mobile ou portable comportant une zone mémoire dans laquelle peuvent être stockés les jetons, et capable de communiquer par voie d'onde via un réseau de communication mobile ou cellulaire et un réseau local sans fil du type WLAN, Wifi, Bluetooth, Wimax ou Infrarouge.

En d'autres termes, le dispositif portable peut être soit un support de stockage de données amovible et comporter des moyens de raccordement, notamment un connecteur, capables de coopérer avec des moyens de raccordement d'un équipement informatique ou de télécommunication, pour utiliser ses moyens de communication, notamment en vue de sa recharge, ou être constitué par un équipement de communication intégrant dès lors de tels moyens de communication.

En d'autres termes, lorsque le dispositif portable 1 est constitué par un support de stockage de données amovible, il peut être connecté notamment à un ordinateur fixe ou portable, à une tablette numérique et multimédia, à un terminal de paiement électronique, ou encore à tout autre équipement informatique portable ou non pouvant accueillir un tel dispositif et intégrant des moyens de communication lui permettant d'établir une communication notamment avec la plateforme.

Lorsque le dispositif portable est constitué par un terminal de communication il incorpore de tels moyens de communication. Il peut s'agir d'un téléphone mobile, d'un assistant personnel numérique (ou PDA, ou encore « Smartphone »), d'une tablette numérique multimédia,...

En effet, comme indiqué précédemment, les moyens de communication du dispositif portable ou, en variante de l'équipement dans lequel il vient se monter, sont adaptés pour établir un canal de communication sécurisé avec la plateforme de gestion 2 pour le téléchargement des jetons stockés dans la base de données 5. Ainsi, ce téléchargement peut s'effectuer soit en établissant une communication directe entre la plateforme et le dispositif, soit en insérant le

dispositif dans un équipement hôte pour récupérer, par son intermédiaire, les jetons stockés dans la base 5.

Ainsi, le dispositif portable ou le terminal dans lequel il vient se raccorder peut être constitué par tout équipement comprenant :

- des moyens de traitement comprenant au moins un microprocesseur,
- de la mémoire volatile et/ou non volatile et/ou de masse,
- des moyens de saisie, tel qu'un clavier et/ou une souris et/ou écran tactile ou encore à des moyens de commande vocale,
- des moyens d'affichage,
- des moyens de communication, et
- un élément de lecture/écriture de dispositif portable (par exemple : lecteur de carte mémoire ou de carte SIM).

Les moyens de communication considérés ici se rapportent par exemple aux technologies et/ou normes suivantes :

- Bluetooth et/ou IrDA (Infrared Data Association), et/ou WI-FI (abbreviation de wireless fidelity) et/ou Wimax, et GPRS (General Packet Radio Service), GSM, UMTS, HSDPA ou IMS (IP Multimedia Subsystem).
- ou encore Ethernet.

Le système de gestion comporte encore un ensemble de terminaux de paiement 6 (figure 3) destinés à être utilisés pour effectuer une transaction tendant à débiter le dispositif portable d'un jeton.

Ces terminaux de paiement comportent des moyens de traitement et des moyens de communication capables de coopérer avec les moyens de communication du dispositif portable, en établissant un premier canal de communication sécurisé, et avec les moyens de communication de la plateforme pour établir un deuxième canal de communication sécurisé.et des moyens de traitement.

Les moyens de traitement du dispositif portable sont aptes à mettre en œuvre un programme d'ordinateur, archivé dans les moyens de mémoires, comportant des instructions aptes effectuer les

traitements nécessaires pour réaliser les étapes de rechargement de jetons, et de transaction avec les terminaux de paiement.

Les étapes de rechargement peuvent s'effectuer soit en établissant une communication entre le dispositif portable et le serveur, soit par l'intermédiaire des terminaux de paiement.

Dans le cas où le dispositif portable est un terminal mobile, celui-ci dans le cadre de l'étape de rechargement établit une connexion avec la plateforme 2.

Le module de communication de la plateforme comporte des moyens de communication aptes à envoyer les jetons sécurisés du dispositif portable directement *via* le réseau mobile ou le réseau Internet.

Le protocole de rechargement du dispositif portable comporte les étapes suivantes :

- étape de connexion du dispositif portable, et d'établissement d'un canal de communication sécurisé avec authentification mutuelle (utilisant des clés symétrique ou asymétrique) entre le dispositif portable et le module de communication de la plateforme, garantissant ainsi la confidentialité et l'intégrité des échanges ;
- étape d'authentification de l'utilisateur par le dispositif portable, exemple par saisie d'un code PIN ;
- étape d'envoi d'une première commande du dispositif portable *via* le réseau de communication (réseau Internet ou mobile), à destination du serveur HSM 3 ladite première commande se rapportant à une demande de chargement de jetons (c'est-à-dire le ou les titres restaurant devant être émis pour l'utilisateur) ;
- étape d'identification par le serveur HSM 3 du nombre de jetons à disposition pouvant être envoyé au dispositif portable en fonction de l'entité à laquelle appartient l'utilisateur, et/ou une étape dans laquelle le serveur HSM identifie les utilisateurs et les caractéristiques des jetons à émettre pour ces utilisateurs ;
- étape d'échange des jetons par un protocole garantissant l'unicité du jeton (présence du jeton valide dans un endroit unique à un instant donné) ;

- étape de paramétrage du dispositif portable en fonction du contexte (règles de gestion des jetons, ...), et

- étape de fin chargement, fin de la session du canal de communication sécurisé et déconnexion.

On notera que, lors de l'étape de recharge du dispositif portable, plusieurs jetons peuvent être associés chacun à des informations relatives à leur mode d'utilisation. Il peut s'agir, par exemple, d'informations de validité ou d'informations relatives à des établissements dans lesquels ils sont autorisés à être utilisés.

En effet, chaque jeton est émis pour un individu donné appartenant à une entité donnée. Ces éléments que sont l'individu et l'entité sont définis respectivement par un identifiant qui est compris dans les paramètres de gestion du titre dématérialisé, fait partie de l'objet numérique.

Ainsi, contrairement à l'état de l'art, il n'est plus nécessaire que le terminal mette en œuvre un programme d'ordinateur afin de réaliser des calculs et contrôles de cohérence de gestion du ou des compteurs. Et, par voie de conséquence, les attaques pouvant être réalisées contre ces compteurs par des pirates informatiques dans l'optique de modifier ces compteurs ne sont plus possibles.

En effet, dans le cas de dispositifs portables selon l'état de la technique comportant des compteurs, le terminal envoie des commandes de mise à jour des compteurs et enregistre la transaction de mise à jour. Après la télécollecte des transactions, ces données sont intégrées dans les bases de données de gestions, qui comportent les montants crédités ou débités et les soldes des compteurs du dispositif portable pour qu'ensuite le serveur de gestion intègre et compare les compteurs de la carte et des comptes client dans la base. Périodiquement des traitements de contrôle des historiques des transactions doivent être effectués afin de contrôler la cohérence de gestion du ou des compteurs réalisés au cours d'une période donnée.

Dans la présente invention, grâce à la gestion de jeton mise en œuvre en tant qu'objet numérique unique, leur gestion, ne consiste

qu'au seul contrôle de comparaison entre les jetons générés et téléchargés avec les jetons effectivement utilisés.

On va maintenant décrire en référence à la figure 3, un exemple d'utilisation d'un dispositif portable, ici un poste téléphonique mobile, dans lequel ont été chargés un certain nombre de jetons.

Comme indiqué précédemment, lors d'une transaction, une communication est établie avec un dispositif tiers, constitué ici par un terminal de paiement.

Il s'agit par exemple du terminal de paiement d'un restaurant qui accepte les titres restaurant dématérialisés du type jeton.

Ce terminal de paiement comporte une architecture matérielle d'un ordinateur.

Ce terminal de paiement comporte un module SAM 7 (acronyme anglais de « Security Access Module » pour Module d'Accès Sécurisé). Ce module SAM permet de sécuriser les échanges de données entre le dispositif portable et lui même. Le mécanisme choisi pour cette sécurisation, est l'établissement d'un canal sécurisé avec authentification mutuelle (utilisant des clés symétriques ou asymétrique), garantissant la confidentialité et l'intégrité des échanges.

Ce terminal de paiement est apte à fournir les moyens de communication sans fil courte portée (de type NFC ou encore IrFA, Bluetooth, etc..), nécessaire à l'établissement des connexions entre le SAM et le dispositif portable.

Ce terminal de paiement est également apte à fournir les moyens de communication longue distance (Ethernet, IP, RTC, etc..), nécessaires à l'établissement des connexions entre le SAM et le centre de collecte, permettant ainsi la collecte des jetons transmis par le dispositif portable via le terminal mobile. Ce centre de collecte se rapporte à des serveurs ayant émis les commandes nécessaires pour déclenchement de la création de jetons sécurisés par le serveur HSM.

Dans le mode de réalisation décrit ici, les moyens de communication utilisés par le dispositif portable, et le terminal de

paiement permettent d'établir un canal de communication sécurisé compatible avec le mode de transmission de données utilisé (NFC, IRdA, etc..).

Dans le cas où le terminal de paiement ne comporte pas de module SAM, ce terminal de paiement est relié à un serveur apte à avoir un rôle similaire à celui du module SAM.

Une fois le montant de la transaction saisi sur le terminal de paiement et lorsque l'utilisateur du terminal mobile souhaite utiliser un titre restaurant, il approche son téléphone mobile typiquement à quelques centimètres du terminal de paiement de sorte que les moyens de communication sans fil et de ces appareils soient à portée l'un de l'autre.

Il autorise, via un menu de l'interface homme-machine de son terminal, l'établissement d'une communication sans fil courte portée entre ces équipements et la transmission du jeton au terminal de paiement.

L'établissement d'un canal sécurisé avec authentification mutuelle (utilisant des clés symétriques ou asymétrique) entre dispositif portable du terminal mobile et Le SAM du terminal de paiement (ou le module de communication dans le cas d'un terminal ne comportant pas de SAM), garantie la confidentialité et l'intégrité des échanges.

L'application exécutée par les moyens de traitement du terminal mobile détermine et sélectionne automatiquement le jeton parmi les jetons archivés dans le dispositif portable à transmettre au terminal de paiement à partir des caractéristiques liées aux jetons.

Ainsi, le SAM indique au dispositif portable les caractéristiques des jetons acceptés et le dispositif portable lui retourne les jetons correspondants dans la limite de leur validité et de leur valeur.

Par la suite, le débit de jetons est réalisé par le transfert du ou des jetons du dispositif portable vers la carte SAM après vérification de l'authenticité du ou des jetons, via le canal de communication

sécurisé. Le dispositif portable transmet également la valeur totale des jetons débités.

On notera que l'échange des jetons est effectué par un protocole garantissant l'unicité du jeton (présence du jeton valide dans un endroit unique à un instant donné).

Ainsi, il est entendu que l'invention n'est pas limitée aux exemples de réalisation décrits et illustrés. Elle n'est en outre pas limitée à ces exemples d'exécution et aux variantes décrites et peut être mis en œuvre dans tout système dans lequel un document tel qu'un titre de paiement – titre de restaurant ; un bon de réduction ; un ticket de parking ; ticket de spectacle ou divertissement - est nécessaire pour réaliser une transaction.

REVENDICATIONS

1. Procédé de génération d'un titre dématérialisé, caractérisé en ce qu'il comporte :

- une sélection de données relatives à des paramètres de gestion du titre ;
- un traitement desdites données de sorte à générer un jeton ;
- une sécurisation dudit jeton ;
- une transmission du jeton sécurisé vers un dispositif portable distant ; et
- une mémorisation dudit jeton sécurisé dans une zone de mémoire sécurisée du dispositif portable.

2. Procédé selon la revendication 1, dans lequel l'étape de sécurisation consiste à chiffrer ledit jeton à partir d'une clef cryptographique.

3. Procédé selon l'une des revendications 1 et 2, dans lequel les étapes de génération et de sécurisation du jeton sont mises en œuvre au sein d'un centre serveur centralisé (3), et dans lequel, lors de l'étape de mémorisation, on établit une communication avec le dispositif portable distant (1).

4. Procédé selon l'une quelconque des revendications 1 à 3, dans lequel le dispositif portable comprend un dispositif de stockage de données, notamment de carte à puce ou carte à mémoire.

5. Procédé selon l'une quelconque des revendications 1 à 3, dans lequel le dispositif portable est un poste de télécommunication sans fil.

6. Système de gestion de titres dématérialisés stockés dans des zones mémoire sécurisées dans un ensemble de dispositifs portables, caractérisé en ce qu'il comporte une plateforme de gestion (2) comprenant des moyens de stockage de données (4) pour le stockage de données relatives à des paramètres de gestion des titres, un centre serveur de gestion (3) comprenant des moyens de traitement pour générer des jetons à partir des paramètres de gestion, et des moyens de communication adaptés pour communiquer avec des moyens de

communication correspondants des dispositifs portables pour la recharge des dispositifs en titre dématérialisés, et

un réseau de dispositifs tiers servant à la mise en œuvre de transactions tendant à débiter les dispositifs en titres dématérialisés, et comprenant des moyens de communication aptes à communiquer avec des moyens de communication correspondants desdits dispositifs pour établir un premier canal de communication et avec les moyens de communication de la plateforme pour établir un deuxième canal de communication sécurisé.

7. Système selon la revendication 6, caractérisé en ce que la plateforme comporte en outre une base de données (5) de stockage des titres dématérialisés générés, raccordée au centre serveur (3).

8. Système selon l'une des revendications 6 et 7, caractérisé en ce que le titre dématérialisé est un titre de paiement.

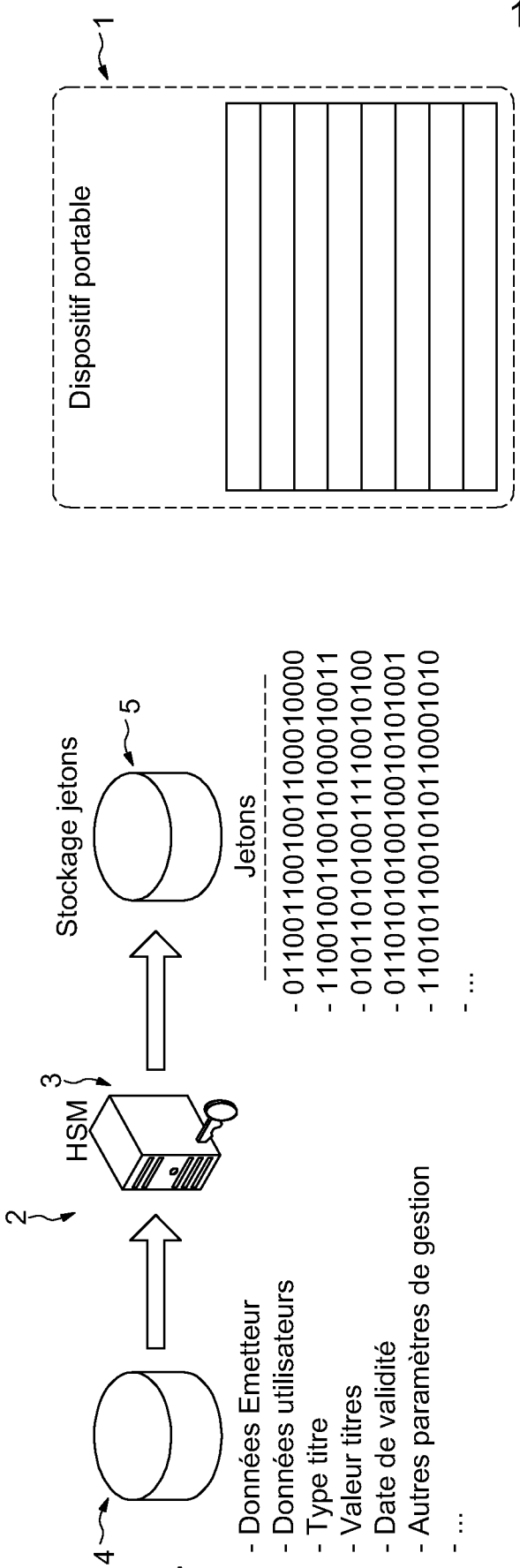

1
Dispositif portable
Stockage jetons
5
Jetons
- 0110011001001100010000
- 1100100110010100010011
- 0101101010011110010100
- 0110101001001010101001
- 1101011001010110001010
- ...
3
HSM
2
4
- Données Emetteur
- Données utilisateurs
- Type titre
- Valeur titres
- Date de validité
- Autres paramètres de gestion
- ...

FIG.1

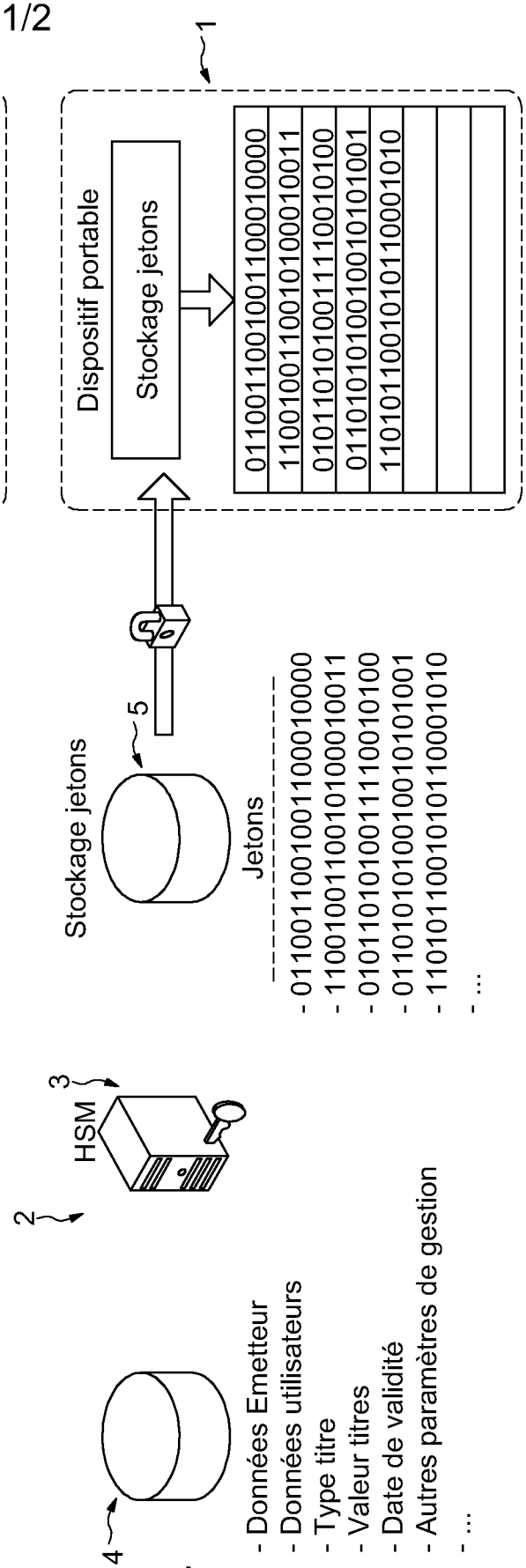
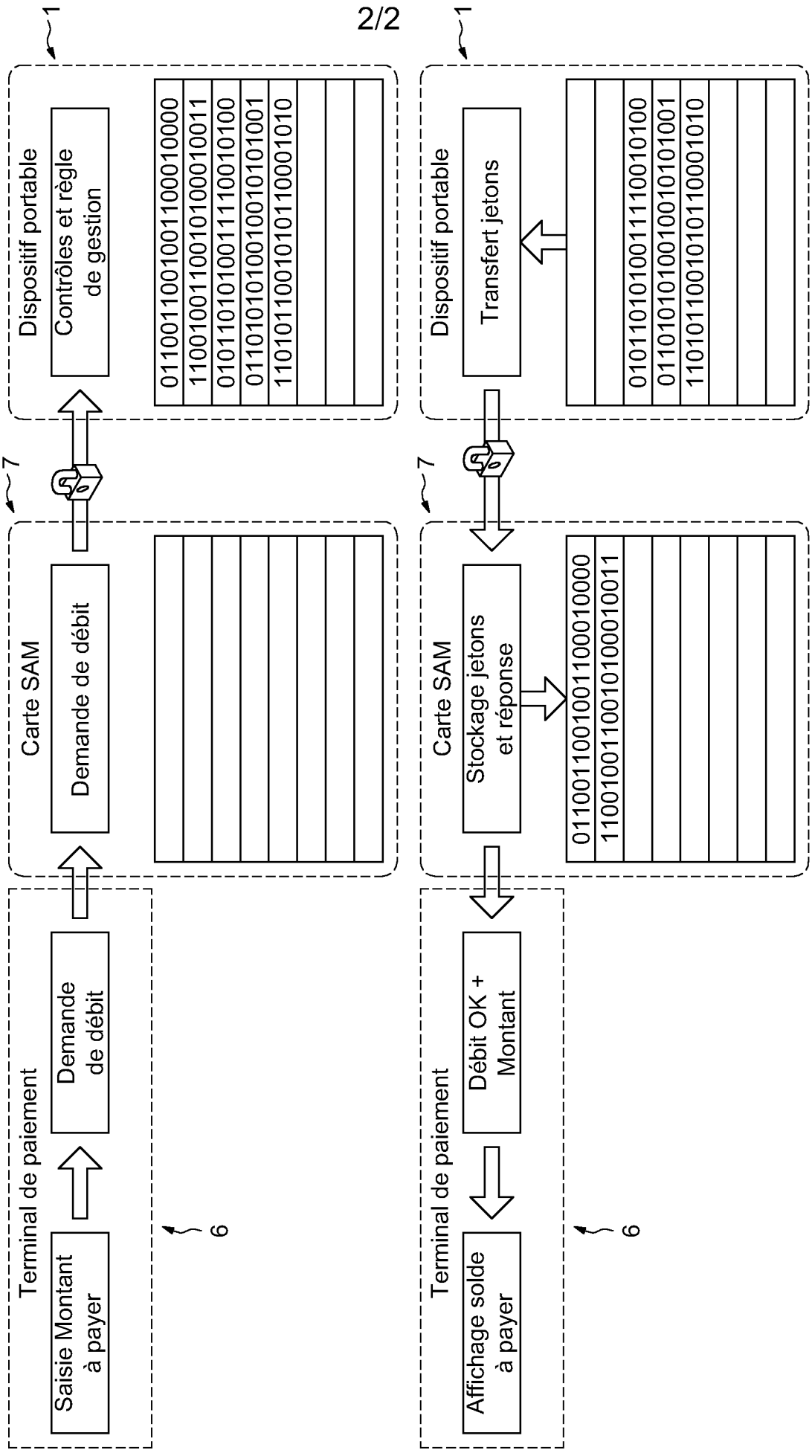

1
Dispositif portable
Stockage jetons
0110011001001100010000
1100100110010100010011
0101101010011110010100
0110101001001010101001
1101011001010110001010
5
Stockage jetons
Jetons
- 0110011001001100010000
- 1100100110010100010011
- 0101101010011110010100
- 0110101001001010101001
- 1101011001010110001010
- ...
3
HSM
2
4
- Données Emetteur
- Données utilisateurs
- Type titre
- Valeur titres
- Date de validité
- Autres paramètres de gestion
- ...

FIG.2

FIG.3


Terminal de paiement
Saisie Montant à payer
Demande de débit
Carte SAM
Demande de débit
Dispositif portable
Contrôles et règle de gestion
0110011001001100010000
1100100110010100010011
0101101010011110010100
0110101010010010101001
1101011001010110001010
6
7
1
Terminal de paiement
Affichage solde à payer
Débit OK + Montant
Carte SAM
Stockage jetons et réponse
Dispositif portable
Transfert jetons
0110011001001100010000
1100100110010100010011
0101101010011110010100
0110101010010010101001
1101011001010110001010
6
7
1