ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية
---

(12) FASCICULE DE BREVET

(11) N° de publication :
MA 29525 B1

(51) Cl. internationale :
G06Q 30/00

(43) Date de publication :
02.06.2008

(21) N° Dépôt :
30413

(22) Date de Dépôt :
22.11.2007

(30) Données de Priorité :
29.04.2005 FR 0504389

(86) Données relatives à l'entrée en phase nationale selon le PCT :
PCT/EP2006/061944 28.04.2006

(71) Demandeur(s) :
THALES, 45, RUE DE VILLIERS F-92200 NEUILLY SUR SEINE (FR)

(72) Inventeur(s) :
D'ATHIS, Thierry ; DAILLY, Philippe ; MORIN, Pascal ; RATIER, Denis

(74) Mandataire :
ABU-GHAZALEH INTELLECTUAL PROPERTY (TMP AGENTS)

(54) Titre : **TERMINAL NOMADE DE TRANSACTIONS ELECTRONIQUES SECURISE ET SYSTEME DE TRANSACTIONS ELECTRONIQUES SECURISE**

(57) Abrégé : LA PRÉSENTE INVENTION CONCERNE UN TERMINAL NOMADE DE TRANSACTIONS ÉLECTRONIQUES. ELLE CONCERNE ÉGALEMENT UN SYSTÈME DE TRANSACTIONS ÉLECTRONIQUES SÉCURISÉ COMPORTANT DES UN OU PLUSIEURS TERMINAUX NOMADES. LE TERMINAL (1) COMPORTE UN SUPPORT APPLICATIF (2) ET UN COUPLEUR (3) POUR RÉALISER LES OPÉRATIONS DE LECTURES ET D'ÉCRITURES SUR UN MÉDIA NÉCESSAIRES AUX TRANSACTIONS ÉLECTRONIQUES EN RELATION AVEC L'APPLICATIF. LE COUPLEUR (3) COMPORTE DES MOYENS POUR CRÉER UNE FENÊTRE TEMPORELLE D'ÉCRITURE ET UNE FENÊTRE TEMPORELLE DE LECTURE À PARTIR D'UN SIGNAL D'ENTRÉE SÉCURISÉ, TOUTE ÉCRITURE ET TOUTE LECTURE ÉTANT BLOQUÉE EN DEHORS DES FENÊTRES CORRESPONDANTES. L'INVENTION S'APPLIQUE NOTAMMENT POUR LA SÉCURISATION DE TERMINAUX OPÉRANT DES CONTRÔLES ET DES TRANSACTIONS CONTRACTUELLES SUR DES SUPPORTS ÉQUIPÉS DE PROCESSEURS ET DE MÉMOIRES, CES SUPPORTS POUVANT ÊTRE PAR DES CARTES À LECTURE ET ÉCRITURE SANS CONTACT COMPORTANT PAR EXEMPLE

DES TITRES DE TRANSPORT, DES MOYENS DE PAIEMENT OU TOUS AUTRES TITRES À FAIRE VALOIR.

ABREGE

Terminal nomade de transactions électroniques sécurisé et système de transactions électroniques sécurisé

La présente invention concerne un terminal nomade de transactions électroniques. Elle concerne également un système de transactions électroniques sécurisé comportant des un ou plusieurs terminaux nomades.

Le terminal (1) comporte un support applicatif (2) et un coupleur (3) pour réaliser les opérations de lectures et d'écritures sur un média nécessaires aux transactions électroniques en relation avec l'applicatif. Le coupleur (3) comporte des moyens pour créer une fenêtre temporelle d'écriture et une fenêtre temporelle de lecture à partir d'un signal d'entrée sécurisé, toute écriture et toute lecture étant bloquée en dehors des fenêtres correspondantes.

L'invention s'applique notamment pour la sécurisation de terminaux opérant des contrôles et des transactions contractuelles sur des supports équipés de processeurs et de mémoires, ces supports pouvant être par des cartes à lecture et écriture sans contact comportant par exemple des titres de transport, des moyens de paiement ou tous autres titres à faire valoir.

Figure 1

MA 29525B1

N°30413

E29525

02 JUIN 2008

TERMINAL NOMADE DE TRANSACTIONS ELECTRONIQUES SECURISE ET SYSTEME DE TRANSACTIONS ELECTRONIQUES SECURISE

La présente invention concerne un terminal nomade de transactions électroniques. Elle concerne également un système de transactions électroniques sécurisé comportant des un ou plusieurs terminaux nomades. L'invention s'applique notamment pour la sécurisation de terminaux opérant des contrôles et des transactions contractuelles sur des supports équipés de mémoires, ces supports pouvant être par des cartes à lecture et écriture sans contact comportant par exemple des titres de transport, des moyens de paiement ou tous autres titres à faire valoir.

Un exemple de transactions électroniques utilisant des cartes sans contact concerne les titres de transport. Ces cartes permettent aux usagers d'accéder aux moyens de transport en passant ces dernières en regard de lecteurs placés aux points d'entrée des stations ou à l'entrée des véhicules. Les titres sont dématérialisés et stockés dans la mémoire des cartes. Comme pour des moyens classiques, du type par exemple des cartes oranges en région parisienne, les titres stockés dans les cartes correspondent à différents types d'abonnement ou de contrats en fonction notamment de la zone géographique couverte, de la qualité de l'usager et de la durée. Le contrôle de la validité d'un abonnement nécessite des moyens particuliers contrairement à un titre classique en papier où les caractéristiques de l'abonnement sont visibles. Il faut notamment des moyens de lectures électroniques permettant de lire le contenu du contrat mémorisé dans une carte. Les agents en charge du contrôle des titres de transport doivent donc être équipés en permanence d'appareil de lecture de supports électroniques tels que des cartes à mémoire par exemple.

Ces agents, les contrôleurs, doivent aussi avoir la possibilité de délivrer des titres de transports ou de modifier les contrats, par exemple les abonnements. Leurs appareils doivent donc aussi être capable de lire et écrire les données inscrites dans la mémoire des cartes.

Ces appareils de lectures et d'écritures peuvent aussi être utilisés dans des points de ventes fixes par exemple chez des buralistes qui sont habilités à délivrer des titres de transport. En particulier les usagers doivent pouvoir faire recharger leurs cartes dans ces points de ventes fixes.

Le problème de la sécurité se pose pour les agents ou pour les points de ventes, chez les buralistes par exemple. Il faut en particulier empêcher l'exploitation de transactions électroniques en cas de vol de ces terminaux de lectures et d'écriture qui sont généralement de type nomade, qu'ils soient portés par des agents ou installés dans des points de vente.

Un but de l'invention est notamment d'empêcher toute utilisation malveillante ou frauduleuse d'un terminal de transactions électroniques. A cet effet, l'invention a pour objet un terminal nomade de transactions électroniques comportant un support applicatif et un coupleur pour réaliser les opérations de lectures et d'écritures sur un média nécessaires aux transactions électroniques en relation avec l'applicatif. Le coupleur comporte des moyens pour créer une fenêtre temporelle d'écriture et une fenêtre temporelle de lecture à partir d'un signal d'entrée sécurisé, toute écriture et toute lecture étant bloquée en dehors des fenêtres correspondantes.

Dans un mode de réalisation particulier, le coupleur comporte une horloge, un premier registre pour compter le temps de la fenêtre temporelle en lecture et un deuxième registre pour compter le temps de la fenêtre temporelle en écriture, les registres étant initialisés en fonction du signal sécurisé. La valeur du premier registre est comparée à une première valeur REG_R définissant la fenêtre temporelle de lecture et la valeur du deuxième registre est comparée à une deuxième valeur REG_W définissant la valeur temporelle d'écriture, la lecture étant bloquée lorsque la valeur du premier registre atteint la première valeur REG_R et l'écriture étant bloquée lorsque la valeur du deuxième registre atteint la deuxième valeur REG_W.

Avantageusement, la fenêtre temporelle de lecture et la fenêtre temporelle d'écriture ont des valeurs différentes. La fenêtre temporelle d'écriture est par exemple inférieure à la fenêtre temporelle de lecture.

Les échanges avec le coupleur se font par exemple selon deux canaux :

- le coupleur et le support applicatif communiquent entre-eux par une liaison confidentielle ;

- le coupleur communique avec un organe de contrôle extérieur (5) par une liaison sécurisée ;

la clé Kv permettant d'ouvrir la session confidentielle étant générée par le coupleur, l'ouverture d'une session confidentielle étant réalisée par identification mutuelle au moyen de la clé Kv. Avantageusement, cette clé Kv est fournie au support applicatif par l'intermédiaire de l'organe de contrôle extérieur.

La liaison entre le coupleur et l'organe de contrôle passe par exemple par le support applicatif qui comporte un programme de routage pour router les données du coupleur vers l'organe de contrôle.

Le signal sécurisé dont est issue l'initialisation des fenêtres temporelles d'écriture et de lecture est par exemple généré par l'ouverture d'une session de communication entre le coupleur et l'organe de contrôle. Une fenêtre temporelle peut par exemple être initialisée par un signal codé saisi sur le support applicatif. Avantageusement, seule la fenêtre temporelle d'écriture peut être initialisée par un signal saisi sur le support applicatif.

Avantageusement, le support applicatif et le coupleur comportent par exemple chacun un historique des transactions électroniques effectuées dans une période donnée, les historiques étant envoyés à un organe de contrôle qui effectue un rapprochement des historiques, un défaut de rapprochement révélant une transaction manquante ou falsifiée.

L'invention concerne également un système de transactions électroniques sécurisé composé d'un organe de contrôle et d'un ou plusieurs terminaux tel que celui décrit précédemment. Avantageusement, l'organe de contrôle et le coupleur communique sous forme de session sécurisée par authentification mutuelle basée sur une clé contenue dans l'organe de contrôle et dans le coupleur.

L'invention a pour principaux avantages qu'elle sécurise l'utilisation d'un terminal de transactions électroniques nomade, qu'elle permet de détecter des chargements de données ou de logiciels frauduleux sur ce type de

terminal et d'en empêcher l'utilisation, et qu'elle est adaptée à tous types d'applications de transactions électroniques.

D'autres caractéristiques et avantages de l'invention apparaîtront à l'aide de la description qui suit faite en regard de dessins annexés qui représentent :

- la figure 1, par un synoptique un terminal de transactions électroniques selon l'invention ;
- la figure 2, une illustration d'un mode de réalisation possible d'un système et d'un terminal selon l'invention ;
- la figure 3, un exemple de durées relatives d'une fenêtre temporelle d'écriture et d'une fenêtre temporelle de lecture.

La figure 1 présente par un synoptique un terminal nomade de transactions électroniques selon l'invention. Le terminal 1 comporte un support d'applicatif 2 et un coupleur 3. Le support 2 et le coupleur 3 échangent des données par une liaison 4. Le terminal peut dialoguer avec un serveur 5 par une liaison 6. L'applicatif porté par le support 2 traite par exemple toute une application billettique, allant par exemple du contrôle des titres à la délivrance des titres et à la génération ou modification de contrats d'abonnement. Le support 2 est par exemple du type ordinateur de poche plus communément appelé PDA. Le coupleur 3 comporte notamment la fonction de lecture du contenu d'un support électronique et/ou la fonction d'écriture sur ce même support. Ce support électronique est par exemple une carte intelligente sans contact avec possibilité de lecture et d'écriture. Le coupleur n'est pas dédié en tant que tel à une application particulière, c'est un simple périphérique de lecture et d'écriture d'une carte sans contact par exemple.
Dans la suite de la description et à titre d'exemple il sera fait référence à une application billettique. Le coupleur 3 sera appelé coupleur billettique et sera destiné à effectuer des opérations de lectures et d'écriture sur des cartes sans contact, ces dernières comportant les titres contrôlés ou délivrés par l'application. Toujours dans le cadre d'un exemple d'application, les titres en question seront des titres de transport et le support d'application sera du type PDA porté par un agent. Lorsqu'il sera en mission, cet agent sera donc équipé du PDA 2 et du coupleur billettique 3.

La figure 2 présente par un synoptique plus détaillé un exemple de réalisation d'un terminal 1 selon l'invention. Le terminal 1 est un appareil pour le contrôle et la vente de titres de transports dématérialisés, stockés sur des cartes à lecture sans contact. Il comporte un PDA 2 et un coupleur billettique 3. Le PDA 2 comporte le programme d'application billettique 21. Cette application traite par exemple le contrôle des titres de transport stockés dans les cartes sans contact ainsi que la délivrance de titres. Elle traite aussi des modifications ou des renouvellements de contrat d'abonnement. Un contrôle de titre se fait par une opération lecture de la carte. Une délivrance de titre ou de modification / renouvellement de contrat se fait par une opération de lecture et d'écriture sur la carte. La nature et la durée d'un abonnement sont stockés sur une carte par une opération d'écriture. Pour déterminer le prix à payer par l'usager une opération de lecture peut être nécessaire pour vérifier les caractéristiques de l'usager, ses droits à réduction par exemple. Pour traiter l'ensemble des opérations de billettique l'applicatif 21 contenu dans le PDA mémorise par exemple tous les types de contrats par types d'usager, par durées, par zones géographiques, par moyens de transport etc ...

Le PDA échangent des données avec le coupleur 3 par une liaison 4. Cette liaison peut être sans fil, du type « bluetooth » par exemple. A l'initialisation, l'application ou une partie de l'application billettique est chargée dans le coupleur par cette liaison 4 dans un espace mémoire 22 prévu à cet effet. Le terminal 1 comporte par ailleurs une liaison 6 avec un serveur 5.

La liaison 4 entre le PDA 2 et le coupleur 3 permet donc l'échange de données entre ces deux éléments. La confidentialité des échanges entre le coupleur et le PDA est assurée par une clé Kv qui sert d'identification mutuelle. La clé Kv sert d'identification mutuelle par exemple par échange de clés tirées aléatoirement. Elle est par exemple changée régulièrement sur l'initiative du coupleur ou de PDA. Dans un mode de fonctionnement, cette clé Kv est par exemple renouvelée aléatoirement par le coupleur et fournie au PDA. Ainsi, une clé Kv_{i+1} est par exemple envoyée au PDA chiffrée avec la clé de session précédente Kv_i. A cet effet, le coupleur 3 comporte un programme 23 de gestion de cette clé Kv, notamment de la génération

aléatoire des différentes clés Kv_i qui la composent. Le PDA n'étant pas réputé fiable, cette clé est simplement confidentielle.

Le coupleur 3 est l'élément sécurisé du terminal nomade 1. Il comporte par exemple une application billettique pour effectuer les lectures et écritures de titres, le traitement billettique étant mis en œuvre par ailleurs par PDA. Seul le coupleur 3 peut exécuter les opérations de lecture et d'écriture de cartes sans contact nécessaires aux transactions électroniques de billettique.

La liaison 6 entre le terminal 1 et le serveur 5 permet notamment l'échange de données entre le coupleur 3 et le serveur 5. La connexion entre le coupleur et le serveur est par exemple sécurisée par authentification mutuelle basée sur des clés Kab 24, 25 contenues dans le serveur 5 et dans le coupleur 3. L'authentification répond par exemple au protocole ISO 9798-2. Le coupleur et le serveur étant réputés fiables, ces clés sont secrètes. Le PDA 2 peut servir de relais de communication entre le coupleur et le serveur. Il comporte par exemple à cet effet un programme de routage 26. Les échanges qu'il route par l'intermédiaire de ce programme 26 sont donc cryptés par la clé Kab et ne sont donc connus que des extrémités de la chaîne, à savoir le coupleur 3 et le serveur 5.

Le coupleur 3 est considéré comme un périphérique du point de vue billettique. Cependant il n'est pas en tant que tel dédié à une application billettique. L'application dépend notamment du logiciel chargé dans la mémoire 22 du coupleur dédié à l'application. Il est possible de charger tous types d'application, en particulier autres que billettique.

Les transactions électroniques se font avec le coupleur. Il fait office de périphérique de lecture et d'écriture. En effet il lit les cartes et écrit sur les cartes nécessaires à l'application billettique, alors que le PDA traite ces applications de billettiques en particulier il effectue le traitement des titres de transport tels que les ventes ou délivrance de titres ou les ventes ou modifications d'abonnement par exemple.

Le coupleur communique avec le PDA et avec le serveur. Ses liaisons avec l'extérieur se font donc par deux canaux :

- sous forme de session sécurisée par la clé Kab avec le serveur 5 via la liaison 6 coupleur- serveur ;

- sous forme de session confidentielle par la clé Kv avec le PDA 2 via la liaison coupleur-PDA.

La session confidentielle empêche de faire fonctionner un coupleur non appairé avec un PDA. La session confidentielle est établie à travers la liaison 4 entre le coupleur et le PDA. Si le PDA ne connaît pas la clé Kv générée par le coupleur 3, l'ouverture de sessions entre le PDA et le coupleur n'est pas possible. Les deux éléments 2, 3 ne peuvent pas être appairés et le terminal 1 ne fonctionne pas.

La session sécurisée 6 est notamment la seule qui permette de recharger les données internes nécessaires au fonctionnement du coupleur, c'est-à-dire notamment l'applicatif. Elle permet donc de charger le logiciel d'application 22 propre au coupleur, dans le cas de l'exemple de la figure 2, et les autres données internes nécessaires. Par cette session sécurisée, le serveur 5 permet aussi d'appairer le coupleur et le PDA en fournissant au PDA la clé Kv, confidentielle, lorsque le coupleur la lui donne sous session sécurisée par clé Kab. En particulier dans le cas où le PDA a perdu sa clé Kv, le moyen de la retrouver est de se connecter au serveur d'une manière sécurisée par la liaison coupleur-serveur 6. Il en est ainsi notamment dans le cas de la première initialisation où le serveur recharge la clé Kv dans le PDA après en avoir pris connaissance de la part du coupleur sous session sécurisée obtenue avec la clé Kab.

Cette session sécurisée permet aussi d'ouvrir une fenêtre temporelle de fonctionnement du coupleur.

En particulier, le coupleur 3 comporte une horloge temps réel 27 et des registres de mémorisation de valeurs de fenêtres temporelles de lecture 10 et d'écriture 11. Le coupleur 3 comporte aussi des registres temporels 28, 29 associés à l'horloge 27 pour mesurer des intervalles de temps. Plus particulièrement un premier registre temporel 28 est affecté au comptage du temps de la fenêtre temporelle de lecture et un deuxième registre temporel 29 est affecté au comptage du temps de la fenêtre temporelle d'écriture. L'horloge et ses registres associés 28, 29 évoluent même hors tension. Lorsque la liaison est établie entre le serveur 5 et le coupleur 3 par authentification mutuelle, les registres 28, 29 sont initialisés à la valeur de l'horloge 27, égale à REG H.. A cet effet l'horloge 27 est par exemple un compteur incrémenté par des fronts d'un oscillateur à quartz. En

fonctionnement, le coupleur compare la valeur REG_R et REG_W de ces registres 28, 29 avec les données la valeur REG_H de l'horloge 27 majorée de respectivement T_R et T_W inscrits dans les registres 10, 11. Ces données T_R et T_W définissent respectivement la valeur de l'ouverture temporelle en lecture et de l'ouverture temporelle en écriture. Lorsque la valeur REG_W du registre 29 dédié à l'écriture dépasse par exemple la valeur REG_H + T_W le coupleur est bloqué en écriture. Il ne peut plus alors exécuter des opérations de vente de billets ou d'abonnement, ou encore de modification de contrat par exemple. Lorsque la valeur REG_R du registre 28 dédié à la lecture dépasse par exemple la valeur REG_H + T_R le coupleur est bloqué en lecture. Il ne peut plus alors exécuter des opérations de contrôle. T_W peut par exemple être fixé à un jour et T_R peut par exemple être fixé à une semaine.

La figure 3 illustre par deux chronogrammes un exemple de fenêtre temporelle 31 pour l'écriture et un exemple de fenêtre temporelle 32 pour la lecture. Grâce à l'horloge 27 le coupleur mémorise l'instant de la dernière initialisation des registres temporels 28, 29. Cette initialisation est effectuée à un instant t_0 lors d'une communication établie avec le serveur 5. A l'occasion de cette initialisation, le serveur peut aussi modifier les valeurs des registres 10, 11 de définition des fenêtres temporelles. En fait, lors d'une session de communication avec le serveur 5, les données suivantes peuvent être rechargées :

- un logiciel d'application, par exemple billettique ;
- les valeurs T_R et T_W des durées des fenêtres temporelles de lecture et d'écritures.

Ainsi à l'établissement d'une communication par authentification mutuelle entre le serveur 5 et le coupleur 3, une fenêtre temporelle en écriture est initialisée et une fenêtre en lecture est initialisée. Au-delà de la première fenêtre toute opération d'écriture est impossible et au-delà de la deuxième fenêtre toute opération de lecture est impossible. Un agent peut ainsi connecter le coupleur 3 au serveur 5 en début de mission par exemple. Puis il se déconnecte et part en mission. Si son terminal 1 est volé ou perdu, les opérations de ventes de billets ou de contrats d'abonnement ne pourront pas excéder 24 heures à compter de la connexion d'initialisation au serveur. De

même au-delà d'une semaine toute opération de lecture sera impossible. Ces durées de fenêtres temporelles de lecture et d'écriture peuvent bien sûr être paramétrées en fonction du type de mission.

Dans l'exemple de la figure 3 les durées des fenêtres temporelles n'ont pas la même durée pour l'écriture et la lecture. Pour certaines applications ces fenêtres pourraient être de mêmes durées. Un avantage apporté par des durées de fenêtres 31, 32 différentes est la souplesse d'utilisation. Le cas d'un agent de contrôle et de délivrance de titres de transport illustre notamment cet avantage. A l'instant t_0 l'agent connecte son terminal 1 au serveur. Plus particulièrement le coupleur 3 entre en communication avec le serveur 5. La fenêtre temporelle pour l'écriture est alors ouverte par exemple pour une durée 24 heures et la fenêtre temporelle pour la lecture est alors ouverte pour une durée d'une semaine. Dans ce cas on peut prévoir la possibilité de réarmer le registre temporel 29 prévu pour la fenêtre temporelle d'écriture un certain nombre de fois sans connexion directe au serveur. L'agent peut alors téléphoner à un service qui lui procure un code pour réarmer ce registre temporel 29, la fenêtre temporelle étant réinitialisée pour 24 heures. L'opération peut se répéter une semaine pendant la durée d'ouverture de la fenêtre temporelle de lecture 32. Cette fenêtre 32 nécessite une connexion au serveur 5 pour être réinitialisée. Avantageusement, un agent qui habite loin du lieu de stockage du serveur 5 n'a pas besoin de se déplacer tous les jours pour réinitialiser la fenêtre temporelle pour l'écriture auprès du serveur ou à proximité. Au-delà d'une semaine toute utilisation du terminal est néanmoins impossible car la fenêtre temporelle pour la lecture est fermée et elle ne peut être réactivée que par une connexion par authentification mutuelle sur le serveur. En cas dysfonctionnement de l'horloge ou des registres temporels, un système est par exemple prévu pour inhiber le fonctionnement du coupleur. Dans l'exemple de réalisation de la figure 2 l'initialisation des fenêtres temporelles d'écriture 31 et de lecture 32 se fait par une connexion sécurisée au serveur 5. Ainsi dans ce cas, les initialisations des fenêtres temporelles se font par un signal sécurisé provenant d'un serveur ou de tout autre organe extérieur. Toutefois il est possible de prévoir un autre mode d'initialisation, fonctionnant par exemple en parallèle. Ce signal sécurisé peut aussi être entré sous forme de code

saisi par un agent ou un utilisateur sur le coupleur, notamment et de façon avantageuse pour l'ouverture de la fenêtre d'écriture 31.

Le coupleur 3 comporte par exemple par ailleurs un registre 12 qui comporte l'historique des transactions effectuées par le coupleur 3 pendant une période donnée limitée ou non. Ce dernier mémorise dans cet historique 12 toutes les cartes qu'il a traitées. En particulier il peut mémoriser pour chaque transaction un numéro de séquence 121, un code d'opération 122 et un numéro physique de la carte 123 ou tout autre code d'identification de la carte. Cet historique est envoyé par session sécurisée au serveur 5, par exemple à chaque fois que le coupleur est mis en communication par authentification mutuelle avec le serveur. Comme indiqué précédemment la session sécurisée peut se faire par la liaison 6 entre le coupleur et le serveur par l'utilisation de la clé Kab.

Le PDA 2 comporte lui aussi un historique des transactions 13 pendant une période donnée, limitée ou non. Il s'agit des transactions effectuées par PDA lui-même. Les transactions mémorisées dans cet historique sont stockées à chaque transaction effectuée par le PDA 2. L'historique 13 du PDA comporte pour chaque transaction mémorisée le numéro de séquence 131 vu du PDA, le numéro 132 du PDA ou tout autre identifiant de celui-ci et le numéro physique 133 de la carte objet de la transaction ou tout autre code permettant d'identifier cette carte. L'identifiant de la carte est envoyé par le coupleur via la liaison 4. Les transactions mémorisées par le PDA correspondent aux transactions mémorisées par le coupleur.

Les historiques 12, 13 comportent par exemple l'instant de chaque transaction, l'instant étant par exemple fourni par l'horloge 27 du coupleur 3. L'historique 13 peut-être envoyé régulièrement au serveur 5, par exemple par l'intermédiaire de la liaison 6 entre le coupleur 3 et le serveur 5 qui transite par le PDA. L'historique 13 du PDA peut aussi être envoyé par tout autre moyen vers le serveur, par exemple par liaison téléphonique ou par réseau.

Le serveur dispose ainsi des deux historiques des transactions, l'historique 12 mémorisé par le coupleur et l'historique 13 mémorisé par le PDA. Théoriquement ces historiques concernent les mêmes transactions. Le serveur peut ainsi comporter une fonction de comparaison de ces deux

historiques 12, 13. Avantageusement ces deux historiques apportent un degré de sécurité supplémentaire au terminal 1. En particulier, cette sécurité permet de détecter des transactions frauduleuses. Une différence entre les deux historiques, par exemple une transaction qui manque dans l'historique 13 du PDA relève une fraude. Cette fraude peut-être due par exemple à une vente frauduleuse mémorisée dans l'historique 12 du coupleur mais non stockée dans l'historique 13 de PDA, ou vice versa. On peut ainsi détecter et identifier des transactions supprimées ou modifiées par un agent ou utilisateur malveillant.

Ainsi, le serveur 5 peut corréler les données des transactions qu'il reçoit du PDA 2, qui sont non fiables, avec les données des transactions, sûres, qu'il reçoit du coupleur 3 sous forme d'historique. Son rôle de surveillance s'étend à d'autres terminaux. Il vérifie notamment que ce qui été validé a bien été vendu et ce qui a été vendu a bien été payé. Il permet d'appairer un coupleur à un PDA en fournissant au PDA la clé Kv confidentielle lorsque le coupleur la lui donne sous session sécurisée par la clé Kab. Un système composé du serveur 5 et d'un ou plusieurs terminaux de transactions électroniques nomades tel que celui présenté précédemment forme alors un système de transactions électroniques sécurisé.

Le serveur 5 est le seul élément du système qui permette de recharger le coupleur puisque c'est le seul à connaître la clé Kab. Les historiques 12, 13 pourraient être envoyés à d'autres organes de contrôle que le serveur 5 pour effectuer leur rapprochement, avec les liaisons appropriées. Cet organe de contrôle 5 effectue un rapprochement des transactions mémorisées dans l'historique 12 du coupleur 3 de celles mémorisées dans l'historique 13 du PDA 2. Un défaut de rapprochement, c'est-à-dire une transaction présente dans un registre et non dans l'autre, relève une transaction erronée, frauduleuse ou non. Un exemple de rapprochement est la comparaison effectuée sur les données précitées121, 122, 123, 131, 132, 133 des historiques 12, 13. D'autres types de rapprochements des transactions mémorisées dans ces historiques 12, 13 sont possibles.

L'invention a été présentée pour une application billettique, plus particulièrement pour le traitement de titres de transport par un terminal nomade. Elle peut bien sûr s'appliquer à d'autres domaines et plus

généralement à d'autres types de transactions électroniques faisant appel à un terminal nomade nécessitant un certain niveau de sécurisation. Par ailleurs le média utilisé dans l'exemple d'application est une carte à lecture et écriture sans contact. Il est évidemment possible d'utiliser d'autres types de média. De même le support applicatif 2 a été décrit comme étant un PDA. Il est possible d'utiliser d'autres types de supports applicatif, par exemple un ordinateur portable, un téléphone portable ou tous autres types de d'interface homme-machine capable de se connecter à un serveur 5 et à un coupleur 3. La liaison 6 entre le coupleur 3 et le serveur 5 et la liaison 4 entre le coupleur et le PDA ont été décrite comme étant des liaisons sans fil, par exemple de type bluetooth. Ces liaisons ont l'avantage de rendre plus pratique l'utilisation du PDA. D'autres types de liaisons peuvent être utilisés.

Enfin le support applicatif 2 et le coupleur 3 ont été présentés comme deux composants ayant des supports physiques différents. Dans un autre mode de réalisation, le support applicatif 2 et le coupleur 3 pourraient être placés sur un même support physique. Néanmoins la séparation du support applicatif 1 et du coupleur 3, c'est-à-dire le fait de communiquer par une liaison confidentielle 4, apporte un élément de sécurité supplémentaire. En particulier le serveur 5 ou tout autre organe de contrôle extérieur permet seul d'appairer un coupleur 3 et un support applicatif 2. En effet la clé Kv par exemple qui permet d'ouvrir les sessions de communications entre le support applicatif 2 et le coupleur 3 est fournie par le serveur 5 au coupleur par liaison sécurisé, au moyen de la clé Kab par exemple. Le coupleur transmet ensuite cette clé Kv au support applicatif 2. Comme il a été indiqué précédemment cette clé peut-être renouvelée, par exemple de manière aléatoire.

REVENDICATIONS

1. Terminal nomade de transactions électroniques, caractérisé en ce qu'il comporte un support applicatif (2) et un coupleur (3) pour réaliser les opérations de lectures et d'écritures sur un média nécessaires aux transactions électroniques en relation avec l'applicatif, le coupleur (3) comportant des moyens pour créer une fenêtre temporelle d'écriture (31) et une fenêtre temporelle de lecture (32) à partir d'un signal d'entrée sécurisé, toute écriture et toute lecture étant bloquée en dehors des fenêtres correspondantes.

2. Terminal selon la revendication 1, caractérisé en ce que le coupleur (3) comporte une horloge (27), un premier registre (28) pour fixer la fenêtre temporelle en lecture et un deuxième registre (29) pour fixer la fenêtre temporelle en écriture, les registres (28, 29) étant initialisés en fonction du signal sécurisé, la fenêtre temporelle en lecture commençant à un instant REG_R du registre (28) et durant une durée T_R mémorisée dans un registre (10), la fenêtre temporelle en écriture commençant à un instant REG_W du registre (29) et durant une durée T_W mémorisée dans un registre (11), la lecture étant bloquée lorsque la valeur de l'horloge (27) atteint la valeur REG_R augmentée de la durée T_R et l'écriture étant bloquée lorsque la valeur de l'horloge (27) atteint la valeur REG_W augmentée de la durée T_W.

3. Terminal selon l'une quelconque des revendications précédentes, caractérisé en ce que la fenêtre temporelle de lecture (32) et la fenêtre temporelle d'écriture (31) ont des valeurs différentes.

4. Terminal selon la revendication 3, caractérisé en ce que la fenêtre temporelle d'écriture (31) est incluse dans la fenêtre temporelle de lecture (32).

5. Terminal selon l'une quelconque des revendications précédentes, caractérisé en ce que :

- le coupleur (3) et le support applicatif (2) communiquent entre-eux par une liaison confidentielle (4) ;

- le coupleur (3) communique avec un organe de contrôle extérieur (5) par une liaison sécurisée (6) ;

la clé (Kv) permettant d'ouvrir la session confidentielle étant générée par le coupleur (3), l'ouverture d'une session confidentielle étant réalisée par identification mutuelle au moyen de la clé (Kv), cette clé (Kv) étant fournie au support applicatif (2) par l'intermédiaire de l'organe de contrôle extérieur (5).

6. Terminal selon la revendication 5 caractérisé en ce que la liaison (6) entre le coupleur (3) et l'organe de contrôle (5) passe par le support applicatif (2) qui comporte un programme de routage (26) pour router les données du coupleur (3) vers l'organe de contrôle (5).

7. Terminal selon l'une quelconque des revendications précédentes caractérisé en ce que le signal sécurisé dont est issue l'initialisation des fenêtres temporelles d'écriture (31) et de lecture (32) est généré par l'ouverture d'une session de communication entre le coupleur (3) et l'organe de contrôle (5).

8. Terminal selon l'une quelconque des revendications précédentes caractérisé en ce qu'une fenêtre temporelle (31, 32) est initialisée par un signal codé saisi sur le support applicatif (2) et transmis au coupleur (3).

9. Terminal selon la revendication 8, caractérisé en ce que seule la fenêtre temporelle d'écriture peut être initialisée par un signal saisi sur le support applicatif (2) et transmis au coupleur (3).

10. Terminal selon l'une quelconque des revendications précédentes, caractérisé en ce que le support applicatif (2) et le coupleur (3) comportent chacun un historique (12, 13) des transactions électroniques effectuées dans une période donnée, les historiques étant envoyés à un organe de contrôle (5) qui effectue un rapprochement des historiques, un défaut de rapprochement révélant une transaction erronée.

11. Terminal selon l'une quelconque des revendications précédentes, caractérisé en ce que l'organe de contrôle (5) est un serveur.

12. Terminal selon l'une quelconque des revendications précédentes, caractérisé en ce que le support applicatif (2) est un ordinateur de poche du type PDA.

13. Terminal selon l'une quelconque des revendications précédentes, caractérisé en ce que le support applicatif (2) comporte une application de traitement billettique.

14. Terminal selon l'une quelconque des revendications précédentes, caractérisé en ce que le média est une carte à lecture sans contact.

15. Système de transactions électroniques caractérisé en ce qu'il comporte un organe de contrôle (5) et au moins un terminal selon l'une quelconque des revendications précédentes.

16. Système selon la revendication 15, caractérisé en ce que l'organe de contrôle (5) et le coupleur (3) communique sous forme de session sécurisée par authentification mutuelle basée sur une clé (Kab) contenue dans l'organe de contrôle (5) et dans le coupleur (3).

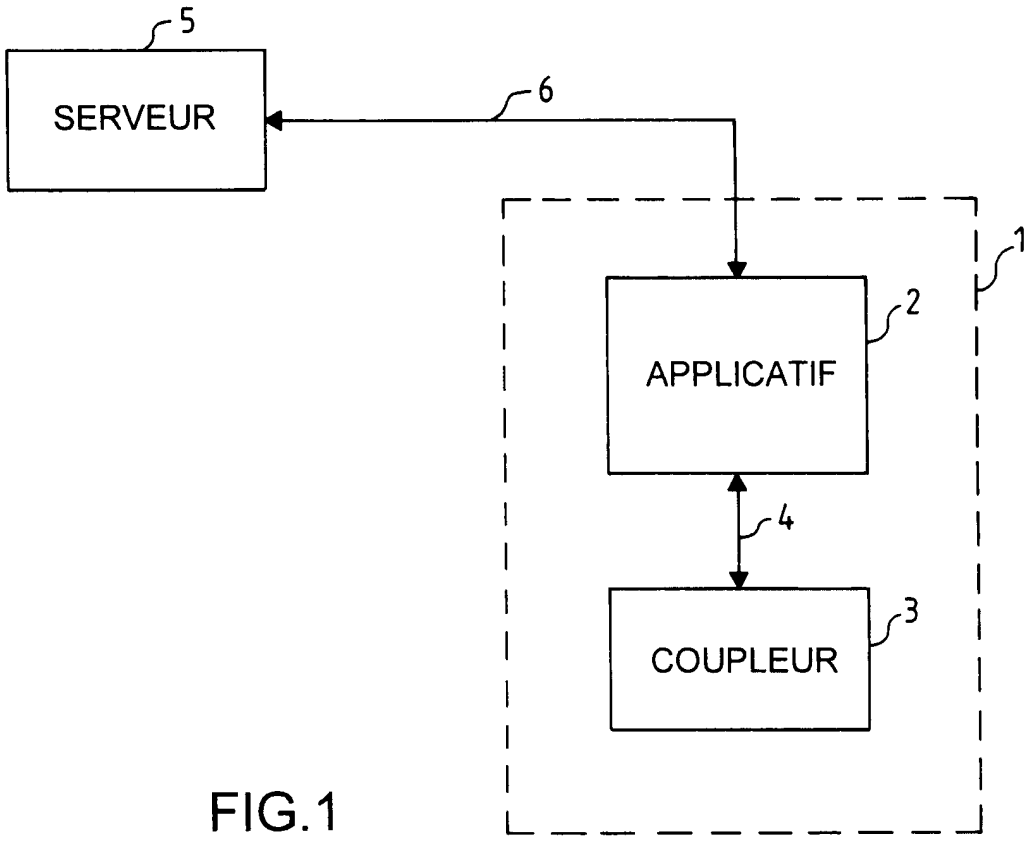

FIG.1

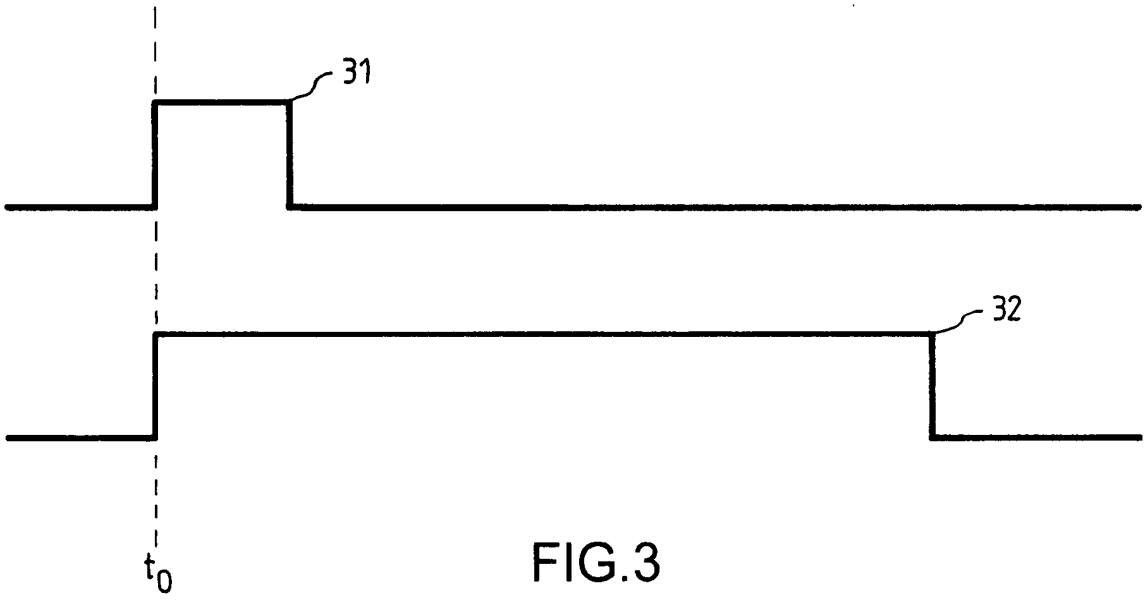

FIG.3

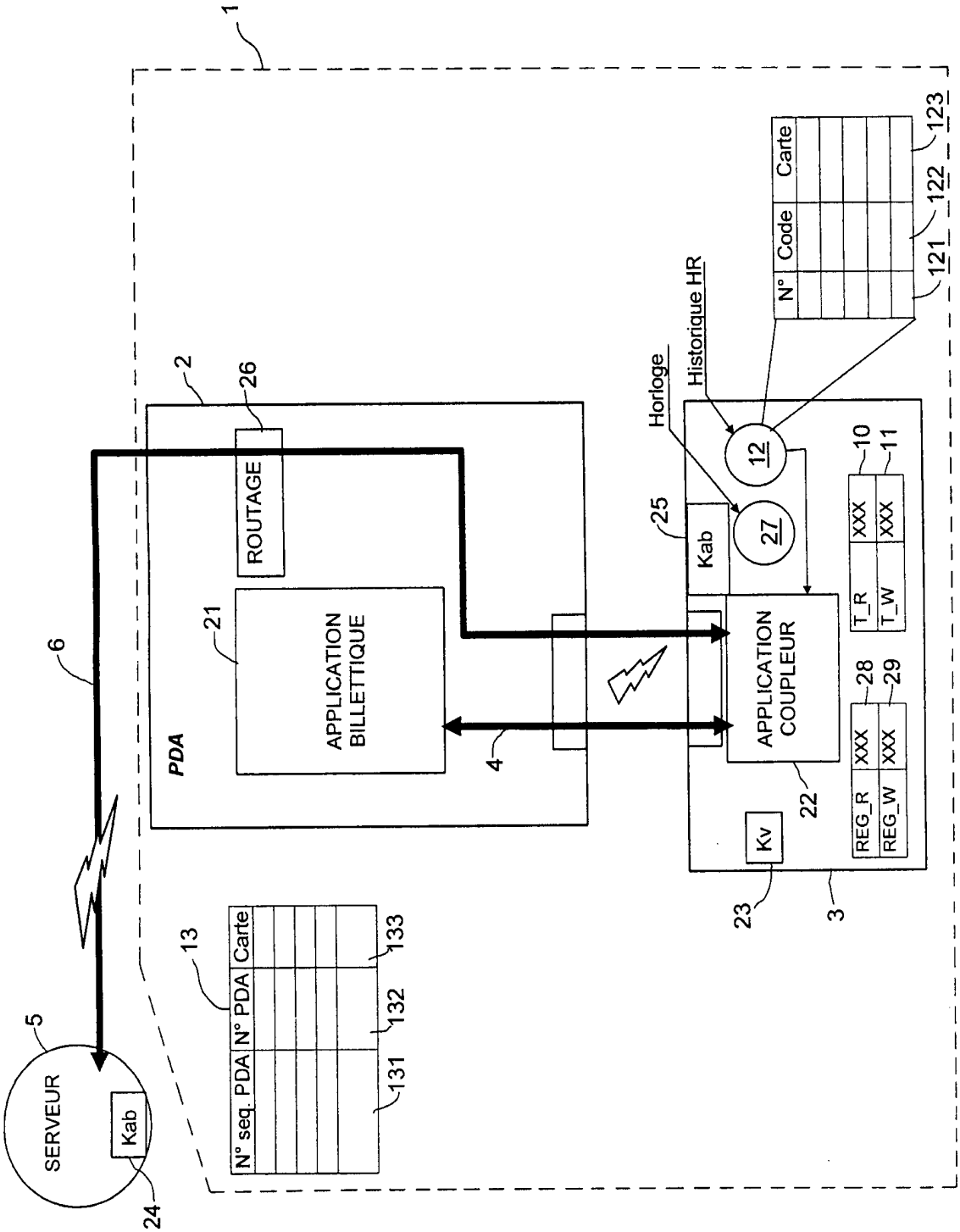
1
2
26
ROUTAGE
21
APPLICATION BILLETTIQUE
PDA
4
6
5
SERVEUR
Kab
24
13
N° seq. PDA
N° PDA
Carte
131
132
133
3
APPLICATION COUPLEUR
22
Kv
23
25
Kab
27
Horloge
12
Historique HR
N°
Code
Carte
121
122
123
T_R
T_W
10
11
XXX
XXX
REG_R
REG_W
28
29
XXX
XXX

FIG.2