(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
30 novembre 2017 (30.11.2017)

WIPO | PCT

(10) Numéro de publication internationale
WO 2017/203146 A1

(51) Classification internationale des brevets :
G06Q 20/34 (2012.01)

(21) Numéro de la demande internationale :
PCT/FR2017/051254

(22) Date de dépôt international :
22 mai 2017 (22.05.2017)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1654572 23 mai 2016 (23.05.2016) FR

(71) Déposant : **OBERTHUR TECHNOLOGIES** [FR/FR] ; 420 rue d'Estienne d'Orves, 92700 COLOMBES (FR).

(72) Inventeurs : **CHAMBEROT, Francis** ; c/OBERTHUR TECHNOLOGIES, 420 rue d'Estienne d'Orves, 92700 COLOMBES (FR). **DE OLIVEIRA, Marco** ; c/OBERTHUR TECHNOLOGIES, 420 rue d'Estienne d'Orves, 92700 COLOMBES (FR).

(74) Mandataire : **COUGARD, Jean-Marie** et al. ; Cabinet BEAU DE LOMENIE, 158 rue de l'Université, 75340 PARIS Cedex 07 (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA,

(54) Title: METHOD FOR SECURING AN ELECTRONIC DEVICE AND CORRESPONDING ELECTRONIC DEVICE

(54) Titre : PROCEDE DE SECURISATION D'UN DISPOSITIF ELECTRONIQUE, ET DISPOSITIF ELECTRONIQUE CORRESPONDANT

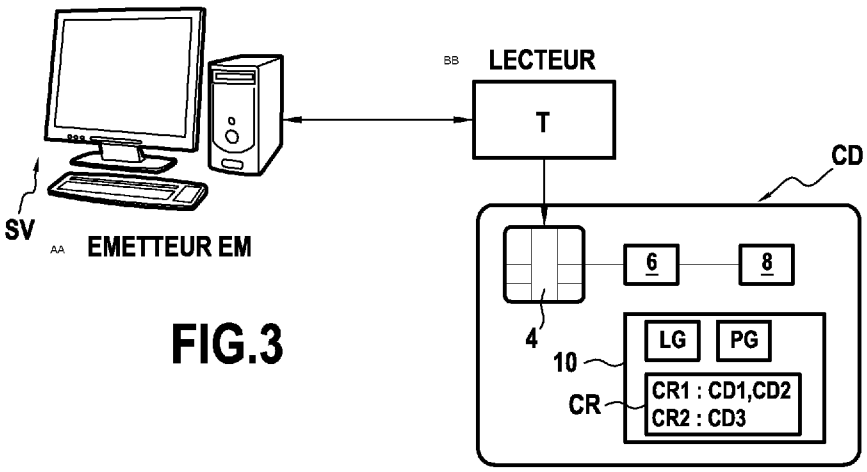

FIG.3

AA TRANSMITTER EM
BB READER

(57) Abstract: The invention relates to a security method implemented by an electronic device (CD), the method comprising: determining a current point in time during which a current transaction is being implemented; selecting, in an archive file (LG) in which at least one past transaction is recorded, each transaction implemented by said electronic device (CD) in a predefined period of time ending at the current point in time; a risk analysis, based on at least one item of archive data recorded in the archive file in association with each transaction selected, in order to detect whether an anomalous use of the electronic device (CD) occurred during said predefined time period; and, if so, triggering at least one security operation of the electronic device (CD) in response to the current transaction.

(57) Abrégé : L'invention propose un procédé de sécurisation mis en œuvre par un dispositif électronique (CD), le procédé comprenant : une détermination d'un point courant dans le temps au cours duquel une transaction courante est mise en œuvre; une sélection, dans un fichier d'historisation (LG) dans lequel est enregistrée au moins une transaction passée, de chaque transaction mise en œuvre par

[Suite sur la page suivante]

WO 2017/203146 A1

PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, 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, KM, ML, MR, NE, SN, TD, TG).

Publiée:

— *avec rapport de recherche internationale (Art. 21(3))*

ledit dispositif électronique (CD) dans une période de temps prédéfinie terminant au point courant dans le temps; une analyse de risque, à partir d'au moins une donnée d'historisation enregistrée dans le fichier d'historisation en association avec chaque transaction sélectionnée, pour détecter si une utilisation anormale du dispositif électronique (CD) s'est produite pendant ladite période de temps prédéfinie; et dans l'affirmative, un déclenchement d'au moins une opération de sécurisation du dispositif électronique (CD) en réponse à ladite transaction courante.

Procédé de sécurisation d'un dispositif électronique, et dispositif électronique correspondant.

Arrière-plan de l'invention

La présente invention se situe dans le domaine général des dispositifs électroniques et concerne plus particulièrement un dispositif électronique, tel qu'une carte à puce par exemple, configurée pour coopérer avec un terminal externe pour réaliser une transaction, dans le domaine bancaire par exemple.

L'invention s'applique plus particulièrement, mais de manière non exclusive, aux cartes à puce (ou cartes à microcircuit), conformes par exemple à la norme ISO7816. L'invention vise notamment la sécurisation d'une carte à puce fonctionnant selon le protocole EMV (pour « *Europay Mastercard Visa* »).

De manière générale, une carte à puce est conçue pour communiquer avec un dispositif externe à cette carte, autrement appelé terminal ou lecteur. Ces cartes permettent d'effectuer divers types de transactions, telles que par exemple des transactions de paiement, de prélèvement ou encore d'authentification du porteur. Les cartes à puce pour applications bancaires (carte de crédit, carte de débit etc.), par exemple, sont aptes à coopérer avec des terminaux de paiement ou des distributeurs automatiques de billets (DAB) pour réaliser divers opérations financières.

EMV est le protocole standardisé utilisé aujourd'hui majoritairement dans le monde pour sécuriser notamment les transactions de paiement effectuées par des cartes à puce.

Le protocole EMV a été conçu pour diminuer les risques de fraudes lors d'une transaction de paiement en permettant notamment l'authentification à la fois de la carte à puce et de son porteur. Ce processus d'authentification fait appel à une combinaison de cryptogrammes (ou clés cryptées) et de signatures numériques et nécessite éventuellement la saisie d'un code secret (appelé communément code PIN) par le porteur de la carte.

Suivant le type de carte utilisé, la situation, ou encore le montant considéré, une carte EMV peut fonctionner en ligne ou hors ligne. En mode en ligne, la carte EMV peut communiquer, via le lecteur, avec l'entité émettrice correspondante (la banque à l'origine de la carte, par exemple) afin de vérifier en particulier que la transaction en cours est légitime. En revanche, si la carte EMV fonctionne en mode hors ligne, celle-ci applique des critères de vérification préenregistrés pour décider si la transaction doit être autorisée ou refusée.

La **figure 1** représente un exemple de mise en œuvre d'une transaction de paiement conforme au protocole EMV, à l'aide d'une carte à puce EMV 100. Certains aspects d'une transaction EMV ont été omis par souci de simplicité.

Lors de la mise en œuvre d'une transaction, le protocole EMV s'articule en trois phases, des variantes étant toutefois possibles. Lors d'une première phase destinée à authentifier la carte à puce 100 utilisée, le terminal 110 et la carte 100 s'échangent un certain nombre de messages dont un message RESET (RST) en S2 puis une réponse ATR en S4. En S6, le porteur de la carte sélectionne via le terminal 110 le mode de transaction souhaité, déclenchant ainsi l'envoi d'une commande « *SELECT* » à la carte 100 afin d'initier le début de la transaction EMV.

Une fois la phase d'authentification de carte achevée, le protocole EMV procède à une phase d'authentification (non représentée) du porteur de la carte 100. Le terminal 110 détermine le procédé d'authentification du porteur à appliquer et détermine en particulier si la transaction doit être effectuée en mode avec vérification de code ou en mode sans vérification de code. Si le mode avec vérification de code est sélectionné, la carte à puce 100 vérifie la validité du code PIN saisi par le porteur sur le terminal 110. Si en revanche le mode sans vérification de code est sélectionné, aucune vérification de code PIN n'est réalisée.

Une fois la phase d'authentification du porteur achevée, le protocole EMV initie la phase de vérification de la transaction. Pour ce faire, le terminal 110 envoie (S8) à la carte à puce 100 une première commande APDU dite GENERATE AC ou GAC (notée ici GAC1). Cette commande bien connue comprend des informations sur la transaction en cours telles que le montant de la transaction, la devise utilisée, le type de transaction, etc. La carte EMV réalise (S9) alors une vérification de la transaction selon des critères de vérification prédéfinis puis envoie (S10), en réponse au GAC1, un cryptogramme (ou certificat cryptographique) comprenant un code d'authentification de message (ou MAC pour « *Message Authentification Code* » en anglais). La réponse de la carte 100 dans le message ARQC dépend notamment du paramétrage de la carte effectué par l'entité émettrice 120 (dit « émetteur ») de ladite carte.

Si le mode en ligne est choisi, comme représenté dans l'exemple de la **figure 1**, la carte à puce 100 envoie en S10 un message de type ARCQ (« *Autorisation Request Cryptogram* ») indiquant que la carte 100 souhaite poursuivre la transaction en ligne avec, par exemple, un serveur distant de l'émetteur 120 (mode en ligne). Le cryptogramme ARQC est transmis par le terminal 110 à l'émetteur 120 qui peut ainsi réaliser (S13) un certain nombre de vérifications afin de s'assurer que la transaction est valide. L'émetteur 120 envoie (S14) ensuite, en réponse au message ARCQ reçu, un message crypté de type ARPC indiquant la décision de l'émetteur 120. Ce message ARPC est transmis par le terminal 110 à la carte 100 en S16.

La carte 100 détermine si elle accepte ou non la transaction à partir de la réponse ARPC reçue en S16. Si la carte 100 accepte la transaction, celle-ci envoie (S18) en réponse un cryptogramme de type TC (transaction acceptée) au terminal 110. Dans le cas contraire, la carte 100 envoie (S18) un cryptogramme de type AAC indiquant le refus de la transaction.

La réalisation en ligne d'une transaction permet donc de mettre en œuvre des mécanismes de sécurité permettant d'identifier des situations à risque et de déclencher une réponse sécuritaire appropriée. L'émetteur de la carte à puce peut par exemple détecter un comportement anormal lors d'une transaction en ligne et décliner la transaction ou déclencher des contrôles de vérification supplémentaires.

Les cartes EMV actuelles sont généralement configurées de façon à pouvoir réaliser un certain nombre de transaction hors ligne, de sorte qu'il n'est pas possible pour l'entité émettrice de la carte d'effectuer de contrôle de sécurité à distance au cours de la transaction hors ligne. Certaines cartes EMV sont par exemple configurées pour fonctionner hors ligne si le montant de la transaction en cours n'atteint pas un montant minimum prédéfini.

Les cartes à puce, EMV notamment, sont donc particulièrement vulnérables aux attaques et comportement malveillants (ou anormaux) lorsqu'elles fonctionnent hors ligne. En cas par exemple de vol d'une carte EMV, l'auteur du vol peut alors réaliser de multiples transactions successives portant toutes sur des montants modérés de sorte à ne pas déclencher le fonctionnement en ligne de la carte et ainsi échapper à la vigilance de l'émetteur de la carte.

Il existe donc aujourd'hui un besoin pour un mécanisme de sécurité permettant de protéger efficacement les cartes à puce, par exemple de type EMV, contre les comportements anormaux et/ou suspects survenant notamment lors des transactions hors ligne. Une sécurisation renforcée est en particulier nécessaire pour protéger les cartes à puce contre les utilisations frauduleuses, en cas de vol par exemple. Un besoin existe plus généralement pour mieux contrôler l'utilisation d'un dispositif électronique tel qu'une carte à puce par exemple (de type EMV ou autre), y compris lorsque ce dispositif fonctionne hors ligne pour mettre en œuvre une transaction.

Objet et résumé de l'invention

A cet effet, la présente invention concerne un procédé de sécurisation mis en œuvre par un dispositif électronique, ledit procédé comprenant :

- détermination d'un point courant dans le temps au cours duquel une transaction courante est ou doit être mise en œuvre par le dispositif électronique ;
- sélection, dans un fichier d'historisation dans lequel est enregistrée au moins une transaction passée, d'au moins une (ou de chaque) transaction mise en œuvre

par ledit dispositif électronique dans une période de temps prédéfinie terminant au point courant dans le temps ;

- analyse de risque, à partir d'au moins une donnée d'historisation enregistrée dans le fichier d'historisation en association avec chaque transaction sélectionnée, pour détecter si une utilisation anormale dudit dispositif électronique s'est produite pendant ladite période de temps prédéfinie ; et
- dans l'affirmative, déclenchement d'au moins une opération de sécurisation du dispositif électronique en réponse à ladite transaction courante

La période de temps prédéfinie est ici une période de temps glissante se terminant au point courant dans le temps.

La présente invention permet avantageusement de protéger de façon efficace les dispositifs électroniques, notamment les cartes à puce (de type EMV ou autre), configurés pour coopérer avec un terminal pour mettre en œuvre une transaction (une transaction bancaire ou autre).

L'invention permet en particulier de sécuriser de tels dispositifs électroniques contre les comportements anormaux ou suspects survenant lors des transactions hors ligne.

Selon un mode de réalisation particulier, le point courant dans le temps comprend au moins l'un parmi la date courante et l'heure courante de la transaction courante.

Selon un mode de réalisation particulier, la détermination du point courant comprend une réception, depuis un terminal avec lequel coopère le dispositif électronique, d'une donnée temporelle représentative du point courant dans le temps.

Selon un mode de réalisation particulier, ladite sélection comprend un calcul du point dans le temps du début de la période de temps prédéfinie, à partir du point courant dans le temps et d'une durée prédéfinie attribuée à ladite période de temps prédéfinie,

chaque transaction sélectionnée étant postérieure au point dans le temps du début de la période de temps prédéfinie.

Selon un mode de réalisation particulier, lors de ladite sélection, le dispositif électronique :

- détermine, à partir du fichier d'historisation, en tant que transaction de référence, la transaction la plus récente dans la période de temps prédéfinie qui satisfait au moins une première condition prédéfinie ; et
- sélectionne uniquement chaque transaction mise en œuvre par ledit dispositif électronique postérieurement à ladite transaction de référence dans la période de temps prédéfinie.

Selon un mode de réalisation particulier, ladite au moins une première condition prédéfinie comprend au moins l'une des conditions suivantes :

- la transaction de référence est une transaction dite « en ligne » ayant été réalisée en coopération avec une entité émettrice du dispositif électronique ; et
- la transaction de référence est une dite transaction en ligne qui a été authentifiée avec succès par l'entité émettrice du dispositif électronique.

Selon un mode de réalisation particulier, lors de ladite sélection, le dispositif électronique filtre les transactions enregistrées dans le fichier d'historisation pour ne sélectionner que chaque transaction satisfaisant au moins une deuxième condition prédéfinie.

Selon un mode de réalisation particulier, la deuxième condition prédéfinie comprend une condition sur le type du terminal avec lequel le dispositif électronique a coopéré lors de ladite transaction.

Selon un mode de réalisation particulier, lors de ladite analyse de risque, le dispositif électronique détecte si une utilisation anormale dudit dispositif électronique s'est produite pendant ladite période de temps prédéfinie à partir d'au moins l'un parmi :

- le nombre de transactions sélectionnées ; et
- le montant cumulé de chaque transaction sélectionnée.

Selon un mode de réalisation particulier, dans lequel, lors de ladite analyse de risque, le dispositif électronique détecte qu'une utilisation anormale s'est produite pendant ladite période de temps prédéfinie si au moins l'une des troisièmes conditions prédéfinies suivantes est satisfaite :

- le nombre de transactions sélectionnées lors de ladite sélection atteint une première valeur seuil prédéfinie ; et
- le montant cumulé de chaque transaction sélectionnée lors de ladite sélection atteint une deuxième valeur seuil prédéfinie.

Selon un mode de réalisation particulier, ladite au moins une opération de sécurisation comprend au moins l'un parmi :

- envoi d'un message informant de ladite utilisation anormale détectée ;
- modification d'au moins un paramètre de fonctionnement du dispositif électronique ;
- enregistrement, dans le fichier d'historisation, d'une donnée de sécurité représentative de ladite utilisation anormale détectée ; et
- refus de mettre en œuvre ladite transaction courante.

Selon un mode de réalisation particulier, le dispositif électronique est une carte à puce.

Dans un mode particulier de réalisation, les différentes étapes du procédé de sécurisation sont déterminées par des instructions de programmes d'ordinateurs.

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations (ou support d'enregistrement), ce programme étant susceptible d'être mis en œuvre dans un dispositif électronique tel qu'une carte à puce, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de sécurisation tel que défini ci-dessus.

Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

L'invention vise aussi un support d'informations (ou support d'enregistrement) lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

Alternativement, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

L'invention concerne également un dispositif électronique comprenant :

- un module de détermination pour déterminer un point courant dans le temps au cours duquel une transaction courante est ou doit être mise en œuvre par le dispositif électronique ;
- un module de sélection pour sélectionner, dans un fichier d'historisation dans lequel est enregistrée au moins une transaction passée, au moins une (ou chaque) transaction mise en œuvre par ledit dispositif électronique dans une période de temps prédéfinie terminant au point courant dans le temps ;
- un module d'analyse de risque pour détecter, à partir d'au moins une donnée d'historisation enregistrée dans le fichier d'historisation en association avec chaque transaction sélectionnée, si une utilisation anormale dudit dispositif électronique s'est produite pendant ladite période de temps prédéfinie ; et

- un module de sécurisation configuré, en cas de résultat positif de ladite détection par le module d'analyse de risque, pour déclencher une opération de sécurisation du dispositif électronique en réponse à ladite transaction courante.

La période de temps prédéfinie est ici une période de temps glissante se terminant au point courant dans le temps.

Selon un mode de réalisation particulier, l'invention est mise en œuvre au moyen de composants logiciels et/ou matériels. Dans cette optique, le terme « module » peut correspondre dans ce document aussi bien à un composant logiciel, qu'à un composant matériel ou à un ensemble de composants matériels et logiciels.

Selon un mode de réalisation particulier, le dispositif électronique est une carte à puce, de type EMV par exemple. Dans un exemple particulier, la carte à puce est conforme à la norme ISO 7816.

Selon un mode de réalisation particulier, le dispositif électronique comprend une mémoire dans laquelle est enregistré le fichier d'historisation.

On notera que les différents modes de réalisation mentionnés ci-avant en relation avec le procédé de sécurisation de l'invention ainsi que les avantages associés s'appliquent de façon analogue au dispositif électronique de l'invention.

Brève description des dessins

D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent des exemples de réalisation dépourvus de tout caractère limitatif. Sur les figures:

- la figure 1 déjà décrite représente, de manière schématique, une transaction mise en œuvre selon le protocole EMV ;
- les figures 2A et 2B représentent schématiquement un premier mécanisme de sécurisation d'une carte à puce EMV ;
- la figure 3 représente schématiquement la structure d'une carte à puce conforme à un mode de réalisation particulier de l'invention ;
- la figure 4 représente schématiquement des modules mis en œuvre dans la carte à puce de la figure 3, selon à un mode de réalisation particulier de l'invention ;
- la figure 5 représente, sous forme d'un organigramme, les étapes d'un procédé de sécurisation selon un mode de réalisation particulier de l'invention ;
- la figure 6 représente un fichier d'historisation selon un mode de réalisation particulier de l'invention ;
- la figure 7 représente schématiquement des transactions mises en œuvre au fil du temps par la carte à puce de la figure 3, selon un exemple de réalisation particulier ; et

- la figure 8 représente, sous forme d'un organigramme, les étapes d'un procédé de sécurisation selon un mode de réalisation particulier de l'invention.

Description détaillée de plusieurs modes de réalisation

Comme indiqué précédemment, la présente invention concerne les dispositifs électroniques, tels que les cartes à puce par exemple, configurés pour coopérer avec un terminal externe pour réaliser une transaction, dans le domaine bancaire par exemple.

L'invention porte plus particulièrement sur la sécurisation des cartes à puce configurées, en particulier lorsque celles-ci sont configurées pour traiter une transaction hors ligne comme expliqué précédemment.

Les **figures 2A** et **2B** illustrent un premier mécanisme de sécurisation d'une carte à puce 130 de type EMV. Dans cet exemple, la carte à puce 130 est configurée pour calculer le montant cumulé de transactions TR qu'elle a réalisées avec succès lors d'une période de temps fixe CL, appelée « cycle », puis pour vérifier si ce montant cumulé atteint une valeur seuil maximale. Cette période de temps CL débute à une position (ou point) fixe DRef dans le temps, dite position de référence dans le temps, correspondant par exemple à la date d'une transaction TR1 donnée. La période de temps CL se termine également à une position fixe DF dans le temps.

Dans l'exemple illustré en **figure 1A**, la carte EMV 130 vérifie, au cours de la transaction TR4, le montant cumulé des transactions TR1, TR2 et TR3 réalisées précédemment au cours du même cycle CL, ainsi que le montant de la transaction TR4 en cours. Si ce montant cumulé atteint au moins la valeur seuil maximale, la carte 130 demande par exemple à poursuivre en mode en ligne. Par la suite, lorsque la carte 130 détecte qu'une nouvelle transaction se produit après l'instant DF, elle réinitialise le point de référence DRef afin d'initier un nouveau cycle de temps CL lui aussi fixe dans le temps.

Cette technique présente toutefois un inconvénient en ce qu'il n'est pas toujours possible de détecter notamment une augmentation importante, potentiellement anormale, des montants des transactions.

Comme illustré en **figure 2B**, on suppose par exemple que la carte à puce 130 est volée à l'instant V et que l'auteur du vol réalise des transactions successives TR1 – TR5 dans un intervalle de temps relativement restreint. Dans l'hypothèse où le montant de chaque transaction reste inférieur au seuil maximal autorisé en mode hors ligne, il n'est pas certain que la carte 130 soit capable de détecter le comportement anormal résultant du vol, et ce malgré le mécanisme de sécurité décrit en référence à la **figure 2A**.

La **figure 2B** illustre un exemple dans lequel la carte 130 réalise les transactions TR1 et TR2 lors d'un premier cycle CL1 puis initie un nouveau cycle CL2 au cours duquel elle réalise les transactions TR3 – TR5. Au cours de la transaction TR5, par exemple, la carte à puce 130 vérifie le montant cumulé des transactions TR3, TR4 et TR5 incluses dans le

cycle CL2 mais ne prend pas en compte les transactions TR1 et TR2 du fait que ces dernières ont été réalisées lors du cycle précédent CL1. La distribution dans le temps des transactions TR1 – TR5 sur deux cycles distincts CL1 – CL2 augmente ainsi les risques que ces transactions hors lignes ne soient pas identifiées par la carte 130 comme constituant un comportement anormal ou suspect.

L'invention propose de palier notamment ces inconvénients à l'aide d'un mécanisme de sécurité permettant de détecter efficacement des comportements anormaux ou suspects, y compris lorsque la carte à puce fonctionne en mode hors ligne, de sorte qu'une réponse sécuritaire appropriée puisse être apportée si nécessaire.

Selon différents modes de réalisation, le procédé de l'invention, mis en œuvre par un dispositif électronique tel qu'une carte à puce par exemple, comprend les étapes suivantes : détermination d'un point courant dans le temps au cours duquel une transaction courante est ou doit être mise en œuvre par le dispositif électronique ; sélection, dans un fichier d'historisation dans lequel est enregistrée au moins une transaction passée, de chaque transaction mise en œuvre par ledit dispositif électronique dans une période de temps prédéfinie terminant au point courant dans le temps ; analyse de risque, à partir d'au moins une donnée d'historisation enregistrée dans le fichier d'historisation en association avec chaque transaction sélectionnée, pour détecter si une utilisation anormale dudit dispositif électronique s'est produite pendant ladite période de temps prédéfinie ; et, dans l'affirmative, déclenchement d'une opération de sécurisation du dispositif électronique en réponse à ladite transaction courante.

L'invention porte également sur un tel dispositif électronique apte à mettre en œuvre un procédé de sécurisation comme défini ci-dessus.

D'autres aspects et avantages de la présente invention ressortiront des exemples de réalisation décrits ci-dessous en référence aux dessins mentionnés ci-avant.

Dans le présent exposé, des exemples de mises en œuvre de l'invention sont décrits en relation avec une carte à puce de type EMV. On comprend que l'invention ne se limite par exclusivement aux cartes EMV mais s'applique plus généralement à tout dispositif électronique configuré pour mettre en œuvre une transaction, y compris des dispositifs autre que des cartes à puce, ce dispositif pouvant utiliser le standard EMV ou d'autres standards de transaction.

Dans un exemple particulier, le dispositif électronique de l'invention est une carte à puce conforme à la norme ISO 7816.

A noter également que la notion de transaction est ici entendue au sens large et comprend par exemple, dans le domaine bancaire, aussi bien une transaction de paiement ou de transfert que d'une consultation d'un compte bancaire sur un terminal bancaire. Les divers modes de réalisation de l'invention sont ici décrits dans le cadre d'une carte de paiement configurée pour réaliser des transactions bancaires. On comprendra

que d'autres types de transactions ou opérations sont envisageables dans le cadre de l'invention.

Sauf indications contraires, les éléments communs ou analogues à plusieurs figures portent les mêmes signes de référence et présentent des caractéristiques identiques ou analogues, de sorte que ces éléments communs ne sont généralement pas à nouveau décrits par souci de simplicité.

La **figure 3** représente, de manière schématique, la structure d'une carte à puce CD, conforme à un mode de réalisation particulier de l'invention.

On comprendra que certains éléments généralement présents dans une carte à puce ont été volontairement omis car ils ne sont pas nécessaires à la compréhension de la présente invention. A noter également que la carte à puce CD représentée en **figure 3** ne constitue qu'un exemple de réalisation, d'autres mises en œuvre étant possibles dans le cadre de l'invention. L'homme du métier comprendra en particulier que certains éléments de la carte à puce CD ne sont décrits ici que pour faciliter la compréhension de l'invention, ces éléments n'étant pas nécessaires pour mettre en œuvre l'invention.

La carte à puce CD est configurée pour coopérer avec un terminal (ou lecteur) T afin de réaliser une transaction TR, telle qu'une transaction financière ou bancaire (transaction de paiement ou autre) dans le cas présent.

Le terminal T est configuré pour faire l'interface entre la carte à puce CD et un serveur distant SV. Dans le cas présent, le serveur SV est un serveur de l'entité émettrice EM (i.e., une institution bancaire par exemple) de la carte à puce CD. Dans cet exemple, la carte CD est apte à communiquer, via le terminal T, avec le serveur distant SV afin de mettre en œuvre, selon le protocole EMV, une transaction dite « en ligne », c'est-à-dire impliquant un échange avec l'émetteur EM comme déjà expliqué ci-avant.

Plus précisément, la carte à puce CD comprend dans cet exemple des contacts externes 4 aptes à coopérer avec le lecteur T, au moins un processeur 6, une mémoire volatile réinscriptible (de type RAM) 8 et une mémoire non volatile réinscriptible 10 (de type Flash par exemple).

La mémoire 10 constitue dans un cet exemple un support d'enregistrement (ou support d'informations) conforme à un mode de réalisation particulier, lisible par le la carte à puce C2, et sur lequel est enregistré un programme d'ordinateur PG conforme à un mode de réalisation particulier. Ce programme d'ordinateur PG comporte des instructions pour l'exécution des étapes d'un procédé de sécurisation selon un mode de réalisation particulier. Les principales étapes de ce procédé sont représentées, dans des modes de réalisation particuliers de l'invention, sur les **figures 5** et **8** décrites ultérieurement.

Dans un exemple particulier, la carte à puce CD est conforme à la norme ISO 7816. Dans ce cas, les contacts externes 4 présentent des caractéristiques conformes à cette

norme. On comprendra toutefois que d'autres modes de réalisation sont possibles. La carte à puce CD peut par exemple coopérer avec le lecteur T en mode sans contact via une antenne RF intégrée dans la carte CD.

Toujours dans l'exemple considéré ici, un fichier d'historisation LG (appelé aussi « *Log* » en anglais) et au moins un critère (ou paramètre) CR prédéfini sont enregistrés dans la mémoire non volatile réinscriptible 10 de la carte CD.

Dans cet exemple, au moins une transaction TR mise en œuvre dans le passé par la carte à puce CD est enregistrée dans le fichier d'historisation LG. En association avec chaque transaction TR, au moins une donnée d'historisation DLG est enregistrée dans le fichier d'historisation LG. Une donnée d'historisation DLG est par exemple une donnée de transaction caractérisant la transaction TR correspondante. Ce fichier d'historisation LG permet à la carte CD de garder en mémoire des données DLG utiles concernant les transactions qu'elle réalise, ces informations pouvant ensuite si besoin être consultées, traitées et/ou envoyées par la carte CD.

Un exemple particulier d'un tel fichier d'historisation LG dans lequel sont enregistrées des transactions TR (et, plus particulièrement, des données d'historisation associées à ces transactions) est décrit ultérieurement en référence à la **figure 6**. Les données d'historisation DLG pouvant être enregistrées dans le fichier d'historisation LG comprennent par exemple au moins l'un parmi : un identifiant de transaction ID, un point dans le temps PT (par exemple une date et/ou une heure) caractérisant à quel moment la transaction a été réalisée, un montant MT de la transaction, une donnée d'historisation DN1 indiquant si la transaction a été réalisée en ligne ou hors ligne, une donnée d'historisation DN2 indiquant si l'authentification (ou validation) en ligne par l'émetteur EM a été passée avec succès dans le cas d'une transaction en ligne, et une donnée d'historisation DN3 indiquant le type de terminal T ayant coopéré avec la carte CD lors de la transaction. Parmi les types de terminaux T possibles, on peut citer par exemple les distributeurs automatiques de billets (ou DAB) et les terminaux de paiement, d'autres types de terminaux étant possibles.

Par ailleurs, le ou les critères CR enregistrés dans la mémoire 10 peuvent comprendre au moins un critère de sélection CR1 et/ou au moins un critère d'analyse CR2. Les critères de sélection et d'analyse CR1, CR2 configurent, le cas échéant, la manière dont la carte met en œuvre le procédé de l'invention, comme expliqué ultérieurement. Dans l'exemple représenté en **figure 3**, les critères CR enregistrés dans la mémoire 10 comprennent deux conditions prédéfinies CD1 et CD2 constituant chacune un critère de sélection CR1, ainsi qu'une condition CD3 constituant un critère d'analyse CR2. Comme déjà indiqué, d'autres exemples de réalisation sont possibles dans le cadre de l'invention, le nombre et la nature des critères de sélection et des critères d'analyse notamment pouvant varier selon le cas d'usage.

Les critères CR et le fichier d'historisation LOG seront décrits plus en détail ci-après selon un exemple de réalisation particulier en référence aux **figures 4-9**.

Dans un mode de réalisation particulier, le processeur 6 piloté par le programme d'ordinateur PG, met en œuvre un certain nombre de modules représentés en **figure 4**, à savoir : un module de détermination MD2, un module de sélection MD4, un module d'analyse MD6 et un module de sécurisation MD8.

Dans cet exemple particulier, le module de détermination MD2 est configuré pour déterminer un point (ou position) courant dans le temps, noté PC, au cours duquel une transaction courante est, ou doit être, mise en œuvre par la carte à puce CD. Par « point courant dans le temps », on entend un instant donné dans le temps où une transaction courante est, ou doit être, mise en œuvre par la carte à puce CD. Un point dans le temps peut être défini par exemple par une date et/ou une heure, et plus généralement par toutes données temporelles permettant de définir une position donnée dans le temps.

Différentes méthodes peuvent être utilisées pour permettre à la carte CD de déterminer le point courant PC dans le temps au cours duquel une transaction courante est, ou doit être, mises en œuvre par la carte CD. Dans un exemple décrit plus en détail ultérieurement, le module de détermination MD2 détermine le point courant PC dans le temps à partir d'une donnée temporelle reçue, provenant par exemple du terminal T. En variante, la carte à puce CD comprend une unité de calcul de la date et/ou de l'heure courante.

Dans cet exemple particulier, le module de sélection MD4 est configuré pour sélectionner, dans le fichier d'historisation LG dans lequel est enregistrée au moins une transaction TR passée, chaque (ou au moins une) transaction TR mise en œuvre par la carte à puce CD dans une période (ou fenêtre) de temps prédéfinie (notée PD) terminant au point courant dans le temps PC. La période de temps PD ayant une durée fixe, elle se déplace dans le temps de sorte à ce qu'elle se termine toujours au point courant dans le temps PC déterminé par le module de détermination MD2. Autrement dit, la période de temps prédéfinie PD est une période de temps glissante dont la borne de fin est définie par le point courant PC dans le temps déterminé par le module de détermination MD2. A chaque fois qu'un nouveau point courant PC dans le temps est déterminé par le module de détermination MD2, la période de temps PD glisse dans le temps de sorte à ce qu'elle se termine toujours par le point courant PC. Des exemples de réalisation seront décrits ultérieurement en référence notamment à la **figure 6**.

Dans un exemple particulier, le module de sélection MD4 est configuré pour sélectionner, parmi les transactions TR enregistrées dans le fichier d'historisation LG, toutes les transactions TR qui ont été mises en œuvre dans la période de temps prédéfinie PD.

Dans un exemple particulier, le module de sélection MD4 est configuré pour sélectionner, parmi les transactions TR enregistrées dans le fichier d'historisation LG, les transactions TR qui ont été mises en œuvre dans la période de temps prédéfinie PD et qui respectent en outre au moins un critère (ou condition) de sélection prédéfini CR1. Ces critères de sélection CR1 sont par exemple enregistrés dans la mémoire 10 de la carte CD. Comme déjà indiqué, la **figue 3** représente un exemple particulier où les critères de sélection CR1 comprennent deux conditions CD1 et CD2.

Le module d'analyse de risque MD6 est configuré pour détecter, à partir d'au moins une donnée d'historisation DLG enregistrée dans le fichier d'historisation LG en association avec chaque transaction TR sélectionnée par le module de sélection MD4, si une utilisation anormale (ou suspecte) de ladite carte CD s'est produite pendant ladite période de temps prédéfinie PD.

On entend ici par « utilisation anormale », toute utilisation de la carte à puce CD jugée, selon au moins un critère d'analyse prédéfini, comme étant potentiellement à risque, frauduleuse ou anormale.

Toujours dans cet exemple, le module de sécurisation MD8 est configuré, en cas de résultat positif de la détection par le module d'analyse de risque MD6 (c'est-à-dire si une utilisation anormale de la carte CD est détectée par le module d'analyse MD6), pour déclencher au moins une opération de sécurisation de la carte à puce CD en réponse à la transaction courante TR. Chaque opération de sécurisation est configurée pour sécuriser la carte à puce CD en réponse à la transaction courante TR. Des exemples de telles opérations sont décrits ci-après en référence aux **figures 5-9**.

Les étapes réalisées par la carte à puce CD lors d'un procédé de sécurisation selon un mode de réalisation particulier sont à présent décrites en référence à la **figure 5**. Pour ce faire, la carte à puce CD exécute le programme d'ordinateur PG.

On suppose ici que la carte à puce CD a initié, en coopération avec le terminal T, le traitement d'une transaction TR, dite transaction courante. Selon une variante, la transaction TR courante n'a pas encore été initiée.

Dans cet exemple, la transaction TR est conforme au protocole EMV.

Au cours d'une étape S30 de détermination, la carte à puce CD détermine un point courant PC dans le temps au cours duquel la transaction courante TR est, ou doit être, mise en œuvre par la carte à puce CD. Ce point courant PC comprend par exemple au moins l'un parmi la date (dite date courante) et l'heure (dite heure courante) de la transaction courante.

En S32, la carte à puce CD sélectionne, dans le fichier d'historisation LG dans lequel est enregistrée au moins une transaction TR passée, chaque (ou au moins une) transaction TR mise en œuvre par la carte à puce CD dans une période de temps prédéfinie PD terminant au point courant PC dans le temps. Comme déjà indiqué, cette

période PD est une fenêtre de temps glissante, de durée prédéfinie, dont la borne de fin est définie par la position courante dans le temps PC.

Dans un exemple particulier, le point courant PC dans le temps est défini par la date courante DC = [16 février 2016] et l'heure courante HC = [16.00], et la durée de la période de temps PD est fixée à 30 jours. Comme expliqué par la suite, la durée de la période de temps PD peut notamment être adaptée selon la configuration souhaitée au vu du type d'évènements ou de comportements que l'on souhaite surveiller au niveau de la carte à puce CD.

La carte à puce CD réalise ensuite en S34 une analyse de risque (ou une analyse de transaction), à partir d'au moins une donnée d'historisation DLG enregistrée dans le fichier d'historisation LG en association avec chaque transaction TR sélectionnée en S32, pour détecter si une utilisation anormale (ou suspecte) de la carte à puce CD s'est produite pendant la période de temps prédéfinie PD. En S34, la carte à puce CD détecte par exemple si une utilisation anormale de ladite carte CD s'est produite pendant la période de temps PD prédéfinie à partir d'au moins l'un parmi :

- le nombre de transactions TR sélectionnées en S32 ; et
- le montant cumulé (c.-à-d. le total des montants MT) de chaque transaction TR sélectionnée en S32.

Par exemple, lors de cette analyse de risque S34, la carte à puce CD détecte qu'une utilisation anormale s'est produite pendant la période de temps prédéfinie PD si au moins l'une des conditions prédéfinies suivantes est satisfaite :

- le nombre de transactions sélectionnées lors de la sélection S32 atteint au moins une première valeur seuil prédéfinie ; et
- le montant cumulé de chaque transaction TR sélectionnée lors de la sélection S32 atteint au moins une deuxième valeur seuil prédéfinie.

Si une utilisation anormale est détectée en S34, la carte à puce CD déclenche en S36 au moins une opération de sécurisation de la carte à puce CD en réponse à la transaction TR courante.

Chaque opération de sécurisation vise à sécuriser la carte à puce CD vis-à-vis de la transaction courante TR, et plus généralement, vis-à-vis de l'utilisation faite de la carte à puce CD sur la période de temps PD. Le nombre et la nature de ces opérations de sécurisation peuvent varier selon le cas d'usage.

Selon un mode de réalisation particulier, ladite au moins une opération de sécurisation S36 comprend au moins l'un quelconque parmi :

- envoi d'un message (par exemple au terminal T et/ou au serveur SV) informant de ladite utilisation anormale détectée en S34 ;
- modification d'au moins un paramètre de fonctionnement de la carte à puce CD ;

- enregistrement, dans le fichier d'historisation LG, d'une donnée de sécurité représentative de ladite utilisation anormale détectée en S34 ; et
- refus de mettre en œuvre la transaction TR courante.

La nature du ou des paramètres de fonctionnement PR à modifier le cas échéant en S36 peut varier selon le cas. D'une manière générale, un paramètre de fonctionnement PR configure la manière dont la carte à puce CD traite une transaction TR avec un terminal extérieur, tel que le lecteur T dans cet exemple. Le paramètre de fonctionnement PR à modifier peut, par exemple, être un compteur enregistré dans la carte à puce CD. Un tel compteur peut par exemple représenter un nombre de transactions hors ligne déjà réalisées par la carte à puce CD, ou encore le montant cumulé de transactions hors ligne déjà réalisées par la carte à puce CD. Le paramètre PR peut par ailleurs porter sur une valeur seuil d'un tel compteur. La modification du paramètre PR peut constituer une mise à jour de la configuration de la carte à puce CD causant un changement dans le traitement des transactions TR par la carte à puce CD.

Un mode de réalisation particulier est à présent décrit en référence aux **figures 6-8**. Plus précisément, la carte à puce CD met en œuvre un exemple de procédé de sécurisation en exécutant le programme d'ordinateur PG.

La **figure 7** représente, le long d'une ligne de temps, des transactions TR1 – TR5 ayant été successivement mises en œuvre dans le passé par la carte à puce CD selon le protocole EMV.

La **figure 6** représente l'enregistrement de ces transactions TR1 à TR5 dans le fichier d'historisation LG de la carte à puce CD. Plus particulièrement, des données d'historisation DLG sont enregistrées dans le fichier d'historisation LG en association avec chaque transaction TR1 – TR5. Ces données d'historisation DLG caractérisent les transactions TR1 – TR5 qui ont été déjà mises en œuvre par la carte à puce CD. Dans cet exemple particulier, les données d'historisation DLG enregistrées dans le fichier d'historisation LG comprennent, en association avec chaque transaction TR référencée, un identifiant de transaction ID, un point dans le temps PT (par exemple une date et/ou une heure) où la transaction a été réalisée et un montant MT de la transaction, et éventuellement au moins l'une parmi : une donnée d'historisation DN1 indiquant si la transaction a été réalisée en ligne ou hors ligne, une donnée d'historisation DN2 indiquant si l'authentification (ou validation) en ligne par l'émetteur EM a été passée avec succès dans le cas d'une transaction en ligne, et une donnée d'historisation DN3 indiquant le type de terminal T ayant coopéré avec la carte CD lors de la transaction. Parmi les types de terminaux T possibles, on peut citer par exemple les distributeurs automatiques de billets (ou DAB) et les terminaux de paiement, d'autres types de terminaux étant envisageables.

Comme illustré en **figure 7**, on suppose à présent que la carte à puce CD a initié, en coopération avec le terminal T, le traitement selon le protocole EMV d'une nouvelle

transaction TR6, dite transaction courante. La carte à puce CD est par exemple insérée dans le terminal T pour permettre la communication par contact. Dans un exemple particulier, on suppose que la carte à puce CD a reçu une première commande APDU de type GENERATE AC, notée GAC1, comme déjà expliqué ci-avant en référence à l'étape S8 en **figure 1**, et que la carte à puce CD met en œuvre le procédé de sécurisation selon un mode de réalisation particulier de l'invention en réponse à cette commande GAC1. Selon une variante, le procédé de sécurisation est mis en œuvre à un autre stade du protocole EMV. Selon encore une autre variante, la carte à puce CD met œuvre le procédé de sécurisation alors que le traitement de la transaction TR courante selon le protocole EMV n'a pas encore été initié.

Les étapes A4, A6, A12 et A14 décrites ci-après en référence à la **figure 8** correspondent respectivement aux étapes S30, S32, S34 et S36, représentées en **figure 5,** mises en œuvre dans un mode de réalisation particulier de l'invention.

Au cours d'une étape d'envoi B2, le terminal T envoie une donnée temporelle DNT à la carte à puce CD qui la reçoit en A2. La donnée temporelle DNT est représentative d'un point courant PC dans le temps. Cette donnée temporelle DNT peut présenter un quelconque format approprié et comprend ici par exemple la date courante DC et l'heure courante HC.

En A4, la carte à puce CD détermine, à partir de la donnée temporelle DNT reçue en A2, le point courant dans le temps PC au cours duquel la transaction courante TR6 doit être mise en œuvre. Dans cet exemple, le point courant PC est défini par la date courante DC et l'heure courante HC au moment de l'initiation du protocole EMV entre la carte à puce DC et le terminal T pour mettre en œuvre la transaction courante TR6. D'autres techniques pour déterminer la date et/ou l'heure courantes sont toutefois possibles.

La carte à puce CD sélectionne (A6) ensuite, dans le fichier d'historisation LG, chaque transaction TR mise en œuvre par la carte à puce CD dans la période de temps prédéfinie PD terminant au point courant PC dans le temps déterminé en A4. Dans cet exemple, la période de temps PD est une fenêtre de temps d'une durée prédéfinie DT. La valeur de DT peut être adaptée selon le but recherché comme expliqué ultérieurement.

Plus spécifiquement, au cours de la sélection A6, la carte à puce CD (plus particulièrement le module de sélection MD4) détermine dans cet exemple le point de référence dans le temps, noté PRef, correspondant au début de la période de temps prédéfinie PD (**figure 7**). Pour ce faire, dans cet exemple particulier, la carte à puce CD calcule le point de référence PRef dans le temps à partir du point courant PC dans le temps et de la durée prédéfinie DT attribuée à la période de temps PD. Plus précisément, la carte à puce CD calcule PRef tel que :

$$PRef = PC - DT$$

Dans cet exemple, le point de référence PRef comprend la date et l'heure du début de la période de temps PD.

Le point de référence PRef dans le temps peut correspondre à une transaction précédemment mise en œuvre par la carte à puce CD.

Toujours en A6, la carte à puce CD sélectionne (A10) ensuite chaque transaction TR, enregistrée dans le fichier d'historisation LG, qui est postérieure au point de référence PRef dans le temps. Selon un exemple particulier, la sélection A10 inclus la transaction TR mise en œuvre le cas échéant au point de référence PRef dans le temps (aucune transaction n'est enregistrée au point PRef dans cet exemple).

Dans cet exemple, la carte à puce CD détermine à quel moment a été mise en œuvre (ou traitée) une transaction TR référencée dans le fichier d'historisation LG à partir du point dans le temps PT enregistré dans le fichier d'historisation LG en association avec la transaction TR concernée. PT comprend par exemple la date et/ou l'heure de la transaction TR correspondante.

Dans cet exemple particulier, la carte à puce CD sélectionne en A10 les transactions TR2, TR3, TR4 et TR5 dont le point dans le temps PT (c.-à-d. la date et l'heure) est postérieur à la position de référence PRef dans le temps. La carte à puce CD sélectionne en outre en A10 la transaction TR6 en cours, bien que des variantes soient possibles dans lesquelles la transaction TR en cours n'est pas sélectionnée en A10.

La carte à puce CD peut en outre être configurée pour appliquer au moins un critère de sélection CR1 pour affiner la sélection réalisée en A10. Selon une variante, la carte à puce CD détermine par exemple en A10, à partir du fichier d'historisation LG, en tant que transaction de référence TRef, la transaction TR la plus récente dans la période de temps PD qui satisfait la première condition prédéfinie CD1. On entend ici par « plus récente » la transaction TR dont le point dans le temps PT est le plus proche du point courant PC. La carte à puce CD sélectionne alors en A10 uniquement chaque transaction TR mise en œuvre par ladite carte CD postérieurement à la transaction de référence TRef dans la période de temps prédéfinie PD. Selon un exemple de réalisation particulier, la première condition CD1 comprend au moins l'une des conditions suivantes :

- CD11 : la transaction de référence TRef est une transaction en ligne ayant été réalisée en coopération avec l'émetteur EM ; et
- CD12 : la transaction de référence TRef est une transaction en ligne réalisée en coopération avec l'émetteur EM et qui a été authentifiée (ou validée) avec succès par ledit émetteur EM.

Lorsque la condition CD11 ci-dessus est appliquée, la carte à puce CD détermine, pour chaque transaction TR dont le point dans le temps PT est postérieur à la transaction de référence TRef, et à partir de la donnée DN1 associée, si ladite transaction TR est une transaction en ligne.

Lorsque la condition CD12 ci-dessus est en outre appliquée, la carte à puce CD détermine, pour chaque transaction en ligne dont le point dans le temps PT est postérieur à la transaction de référence TRef, et à partir de la donnée DN2 correspondante dans le fichier d'historisation LG, si ladite transaction TR a été authentifiée (ou validée) avec succès par l'émetteur EM.

Dans un mode de réalisation particulier, la carte à puce CD applique la condition CD11 mais pas la condition CD12 en A10. Selon l'exemple représenté en **figure 6**, la transaction TR3 constitue alors la transaction de référence TRef (DN1 = ON LINE) de sorte que la carte à puce CD sélectionne en A10, conformément à la condition CD11, les transactions TR4 et TR5.

Selon un autre mode de réalisation, la carte à puce CD applique la condition CD12 ci-dessus. Selon l'exemple représenté en **figure 6**, la transaction TR3 constitue alors également la transaction de référence TRef car la donnée DN2 associée indique que cette transaction en ligne a été authentifiée (ou validée) avec succès par l'émetteur EM (DN2 = OK). En conséquence, la carte à puce CD sélectionne en A10, conformément à la condition CD12, les transactions TR4 et TR5.

Comme déjà indiqué, la carte à puce CD peut être configurée pour appliquer au moins un critère de sélection CR1 pour affiner la sélection réalisée en A10. Le nombre et la nature des critères de sélection CR1 peut varier selon le cas. Selon un exemple particulier, lors de la sélection A10, la carte à puce CD filtre les transactions TR enregistrées dans le fichier d'historisation LG pour ne sélectionner que chaque transaction TR satisfaisant au moins une deuxième condition prédéfinie CD2.

Dans un exemple particulier, la deuxième condition prédéfinie CD2 comprend une condition sur le type du terminal T avec lequel la carte à puce CD a coopéré lors de ladite transaction TR. Dans l'exemple représenté en **figure 6**, le fichier d'historisation LG enregistre en tant que donnée d'historisation DN3, pour chaque transaction TR, si ladite transaction a été réalisée en coopération avec un terminal T selon un premier type TY1 ou selon un deuxième type TY2. Dans un exemple particulier, les états TY1 et TY2 indiquent respectivement que le terminal T est un distributeur automatique de billets (DAB) et un terminal de paiement (un terminal mobile par exemple). Si par exemple la condition CD2 est appliquée, la carte à puce CD exclut de la sélection A10 les transactions TR qui sont dans la période prédéfinies PD et mais ne satisfont par l'état TY1 (la transaction TR5 est donc exclus dans cet exemple).

On comprendra qu'il est possible de configurer la carte à puce CD pour qu'elle applique au moins une première condition CD1 et/ou au moins une deuxième condition CD2 comme expliqué ci-avant.

On supposera dans la suite de cet exemple que la carte à puce CD applique la condition CD11 et sélectionne en conséquence en A10 les transactions TR4 et TR5.

Au cours d'une étape d'analyse A12, la carte à puce CD (plus particulièrement le module d'analyse de risque MD6), réalise une analyse de risque (ou analyse de transaction), à partir des données d'historisation DLG enregistrées dans le fichier d'historisation LG en association avec chaque transaction TR sélectionnée en A6 (à savoir TR4 et TR5 dans cet exemple), pour détecter si une utilisation anormale (ou suspecte) de la carte à puce CD s'est produite pendant la période de temps prédéfinie PD.

Dans cet exemple de réalisation, lors de ladite analyse A12, la carte à puce CD détecte si une utilisation anormale de ladite carte CD s'est produite pendant la période de temps prédéfinie PD à partir d'au moins l'un parmi :

- le nombre de transactions TR sélectionnées en A6 ; et
- le montant cumulé de chaque transaction TR sélectionnée en A6.

On suppose dans cet exemple que le nombre de transactions TR sélectionnées en A6 et le montant cumulé de chaque transaction TR sélectionnée en A6 sont pris en compte par la carte à puce CD lors de l'analyse de risque A12. Dans l'exemple considéré ici et comme représenté en **figure 6**, deux transactions (TR4 et TR5) sont sélectionnées en A6 et le montant cumulé des transactions TR4 et TR5 s'élève à MT4 + MT5.

Selon un exemple particulier, lors de l'analyse de risque A12, la carte à puce CD détecte si une utilisation anormale (ou suspecte) s'est produite pendant la période de temps prédéfinie PD selon au moins un critère d'analyse CR2, enregistré dans cet exemple dans la mémoire 10. Dans cet exemple, lors de l'analyse A12, la carte à puce CD applique, en tant que critères d'analyse CR2, les conditions prédéfinies CD3 suivantes :

- CD31 : le nombre de transactions sélectionnées lors de ladite sélection A6 atteint au moins une première valeur seuil prédéfinie Lmax1 ; et
- CD32 : le montant cumulé (TR4 + TR5 dans cet exemple) de chaque transaction TR sélectionnée en A6 atteint au moins une deuxième valeur seuil prédéfinie Lmax2.

Autrement dit, lors de l'analyse A12, la carte à puce CD détecte qu'une utilisation anormale ou suspecte s'est produite pendant la période de temps prédéfinie PD si les conditions CD32 et CD32 sont satisfaites. Les valeurs Lmax1 et Lmax2 sont fixées selon les besoins du cas d'espèce.

Selon une variante, seule l'une parmi les conditions prédéfinies CD31 et CD32 est appliquée par la carte à puce CD lors de l'analyse A12.

Si aucune utilisation anormale n'est détectée lors de l'analyse A12, le procédé de sécurisation prend fin. Dans ce cas, la carte à puce CD reprend par exemple un traitement normal de la transaction selon le protocole EMV.

Si, en revanche, une utilisation anormale est détectée en A12, la carte à puce CD déclenche en A14 au moins une opération de sécurisation de la carte à puce CD en réponse à la transaction courante TR6. Chaque opération de sécurisation est configurée

pour sécuriser la carte à puce CD vis-à-vis de la transaction courante TR, et plus généralement, vis-à-vis de l'utilisation faite de la carte à puce CD sur la période de temps PD. Le nombre et la nature de ces opérations de sécurisation peuvent varier selon le cas d'usage.

Dans cet exemple, la carte à puce CD réalise en A14 au moins l'une des opérations de sécurisation suivantes :

- envoi (A16) au terminal T d'un message MSG1 informant de ladite utilisation anormale ou suspecte détectée. Le terminal T peut le cas échéant transmettre (B17) le message MSG1 au serveur distant SV afin que l'émetteur SV soit informé de l'utilisation anormale ou suspecte détectée par la carte à puce CD ;
- modification d'au moins un paramètre de fonctionnement PR du dispositif électronique. Comme déjà indiqué, divers paramètres de fonctionnement PR de la carte à puce CD peuvent être modifiés selon les besoins. De manière générale, un paramètre de fonctionnement PR configure la manière dont la carte à puce CD traite une transaction TR avec le terminal T.
- enregistrement (A20), dans le fichier d'historisation LG, d'une donnée de sécurité DS représentative de ladite utilisation anormale ou suspecte détectée en A12 ; et
- refus (A22) d'autoriser la transaction courante. La carte CD à puce CD envoie par exemple un message de refus MSG2 qui est reçu par le terminal T en B22.

La présente invention permet avantageusement de protéger de façon efficace les cartes à puce, par exemple de type EMV, contre les comportements anormaux ou suspects survenant notamment lors des transactions hors ligne. Une carte à puce selon l'invention est ainsi capable de stocker en mémoire des données d'historisation relatives aux transactions traitées par ladite carte au fil du temps. A partir de ces données d'historisation, la carte à puce peut alors analyser l'utilisation qui est faite de la carte dans une fenêtre de temps pertinente, à savoir une fenêtre de temps correspondant ici à une période de temps qui précède immédiatement la transaction en cours. Il est ainsi possible de prendre en compte toutes les transactions pertinentes pour chaque analyse faite par la carte à puce, sans qu'il y ait un risque que certaines transactions soient exclues de l'analyse comme c'est le cas par exemple dans le mécanisme de sécurisation décrit précédemment en référence aux **figures 2A** et **2B**.

Il est possible de fixer la durée DT de la période de temps PD en fonction du type d'utilisation anormale ou non autorisée que l'on cherche à détecter. Afin de pallier les problèmes de vol précédemment décrits, on peut par exemple fixer la durée DT telle que DT = 10 minutes (ou une quelconque valeur inférieure à 60 ou 10 minutes). Si, en revanche, on cherche à détecter un comportement anormal du porteur authentique (par exemple un nombre et/ou un montant cumulé de dépense anormal ou suspect), on peut

par exemple régler la durée DT telle que DT = 30 jours. De cette manière, l'émetteur peut contrôler les habitudes de consommations du porteur authentique et, si besoin, contacter le porteur ou prendre toute autre mesure appropriée.

On peut ainsi configurer la carte à puce afin de déclencher une réponse sécuritaire adaptée à l'utilisation anormale détectée. Une sécurisation renforcée de la carte à puce contre les utilisations frauduleuses (en cas de vol par exemple) est par exemple possible.

De manière générale, l'invention permet de mieux contrôler l'utilisation d'une carte à puce, de type EMV notamment, y compris lorsque celle-ci fonctionne hors ligne.

Un homme du métier comprendra que les modes de réalisation et variantes décrits ci-avant ne constituent que des exemples non limitatifs de mise en œuvre de l'invention. En particulier, l'homme du métier pourra envisager une quelconque adaptation ou combinaison des modes de réalisation et variantes décrits ci-avant afin de répondre à un besoin bien particulier.

REVENDICATIONS

1. Procédé de sécurisation mis en œuvre par un dispositif électronique (CD), ledit procédé comprenant :

- détermination (S30 ; A4) d'un point courant dans le temps (PC) au cours duquel une transaction courante (TR) est ou doit être mise en œuvre par le dispositif électronique ;
- sélection (S32 ; A6), dans un fichier d'historisation (LG) dans lequel est enregistrée au moins une transaction (TR) passée, d'au moins une transaction mise en œuvre par ledit dispositif électronique dans une période de temps glissante d'une durée prédéfinie (PD), ladite période de temps glissante se terminant au point courant dans le temps ;
- analyse de risque (S34 ; A12), à partir d'au moins une donnée d'historisation (DLG) enregistrée dans le fichier d'historisation en association avec chaque transaction (TR) sélectionnée, pour détecter si une utilisation anormale dudit dispositif électronique s'est produite pendant ladite période de temps glissante ; et
- dans l'affirmative, déclenchement (S36 ; A14) d'au moins une opération de sécurisation (A16-A22) du dispositif électronique en réponse à ladite transaction courante.

2. Procédé selon la revendication 1, dans lequel le point courant dans le temps comprend au moins l'un parmi la date courante et l'heure courante de la transaction courante.

3. Procédé selon la revendication 1 ou 2, dans lequel la détermination du point courant comprend une réception, depuis un terminal avec lequel coopère le dispositif électronique, d'une donnée temporelle représentative du point courant dans le temps.

4. Procédé selon l'une quelconque des revendications 1 à 3, dans lequel ladite sélection comprend un calcul du point dans le temps du début de la période de temps glissante, à partir du point courant dans le temps et de la durée prédéfinie attribuée à ladite période de temps glissante,

chaque transaction sélectionnée étant postérieure au point dans le temps du début de la période de temps glissante.

5. Procédé selon l'une quelconque des revendications 1 à 4, dans lequel, lors de ladite sélection, le dispositif électronique :

- détermine, à partir du fichier d'historisation, en tant que transaction de référence, la transaction la plus récente dans la période de temps glissante qui satisfait au moins une première condition prédéfinie ; et
- sélectionne uniquement chaque transaction mise en œuvre par ledit dispositif électronique postérieurement à ladite transaction de référence dans la période de temps glissante.

6. Procédé selon la revendication 5, dans lequel ladite au moins une première condition prédéfinie comprend au moins l'une des conditions suivantes :

- la transaction de référence est une transaction dite « en ligne » ayant été réalisée en coopération avec une entité émettrice du dispositif électronique ; et
- la transaction de référence est une dite transaction en ligne qui a été authentifiée avec succès par l'entité émettrice du dispositif électronique.

7. Procédé selon l'une quelconque des revendications 1 à 6, dans lequel, lors de ladite sélection, le dispositif électronique filtre les transactions enregistrées dans le fichier d'historisation pour ne sélectionner que chaque transaction satisfaisant au moins une deuxième condition prédéfinie.

8. Procédé selon la revendication 7, dans lequel la deuxième condition prédéfinie comprend une condition sur le type du terminal avec lequel le dispositif électronique a coopéré lors de ladite transaction.

9. Procédé selon l'une quelconque des revendications 1 à 8, dans lequel, lors de ladite analyse de risque, le dispositif électronique détecte si une utilisation anormale dudit dispositif électronique s'est produite pendant ladite période de temps glissante à partir d'au moins l'un parmi :

- le nombre de transactions sélectionnées ; et
- le montant cumulé de chaque transaction sélectionnée.

10. Procédé selon la revendication 9, dans lequel, lors de ladite analyse de risque, le dispositif électronique détecte qu'une utilisation anormale s'est produite pendant ladite période de temps glissante si au moins l'une des troisièmes conditions prédéfinies suivantes est satisfaite :

- le nombre de transactions sélectionnées lors de ladite sélection atteint une première valeur seuil prédéfinie ; et
- le montant cumulé de chaque transaction sélectionnée lors de ladite sélection atteint une deuxième valeur seuil prédéfinie.

11. Procédé selon l'une quelconque des revendications 1 à 10, dans lequel ladite au moins une opération de sécurisation comprend au moins l'un parmi :

- envoi d'un message informant de ladite utilisation anormale détectée ;
- modification d'au moins un paramètre de fonctionnement du dispositif électronique ;
- enregistrement, dans le fichier d'historisation, d'une donnée de sécurité représentative de ladite utilisation anormale détectée ; et
- refus de mettre en œuvre ladite transaction courante.

12. Procédé selon l'une quelconque des revendications 1 à 11, dans lequel le dispositif électronique est une carte à puce.

13. Programme d'ordinateur (PG1) comportant des instructions pour l'exécution des étapes d'un procédé de sécurisation selon l'une quelconque des revendications 1 à 12 lorsque ledit programme est exécuté par un ordinateur.

14. Support d'enregistrement lisible par un ordinateur sur lequel est enregistré un programme d'ordinateur (PG1) comprenant des instructions pour l'exécution des étapes d'un procédé de sécurisation selon l'une quelconque des revendications 1 à 12.

15. Dispositif électronique comprenant :

- un module de détermination pour déterminer un point courant dans le temps au cours duquel une transaction courante est ou doit être mise en œuvre par le dispositif électronique ;
- un module de sélection pour sélectionner, dans un fichier d'historisation dans lequel est enregistrée au moins une transaction passée, au moins une transaction mise en œuvre par ledit dispositif électronique dans une période de temps glissante, d'une durée prédéterminée, terminant au point courant dans le temps ;
- un module d'analyse de risque pour détecter, à partir d'au moins une donnée d'historisation enregistrée dans le fichier d'historisation en association avec chaque transaction sélectionnée, si une utilisation anormale dudit dispositif électronique s'est produite pendant ladite période de temps glissante ; et

- un module de sécurisation configuré, en cas de résultat positif de ladite détection par le module d'analyse de risque, pour déclencher une opération de sécurisation du dispositif électronique en réponse à ladite transaction courante.

16. Dispositif électronique selon la revendication 15, comprenant une mémoire dans laquelle est enregistré le fichier d'historisation.

17. Dispositif électronique selon la revendication 15 ou 16, dans lequel le dispositif électronique est une carte à puce.

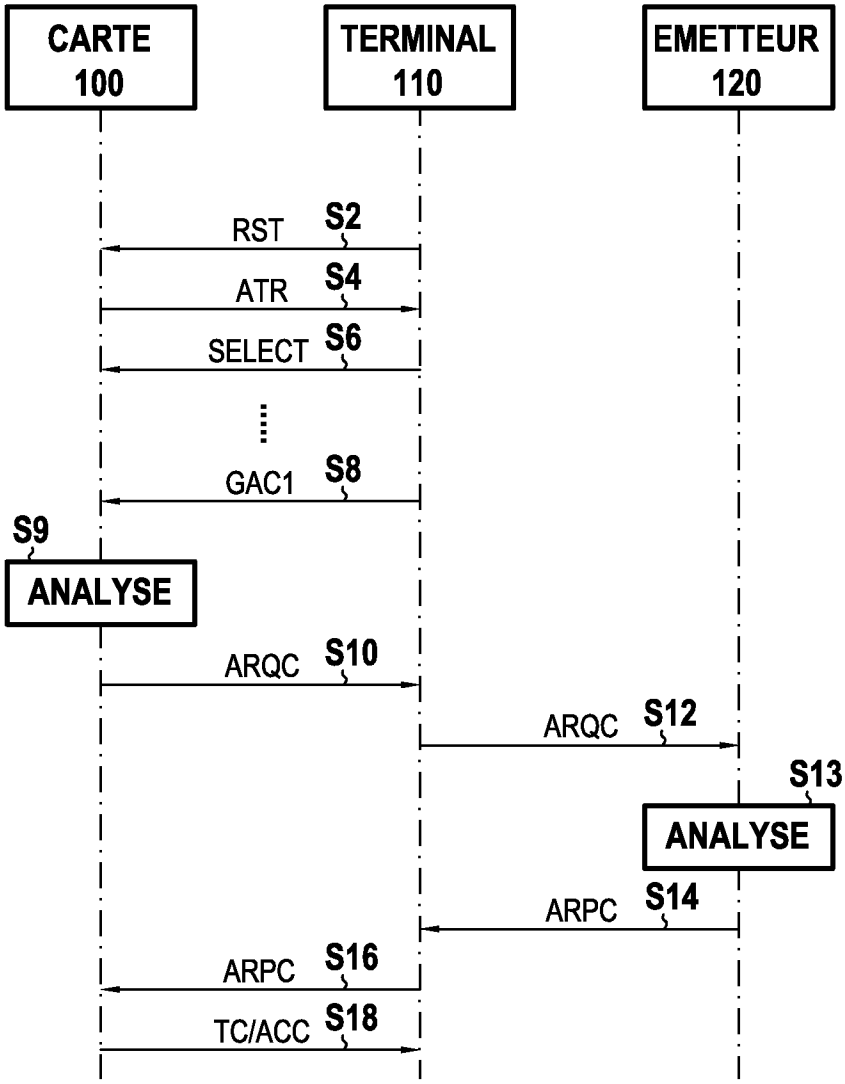

FIG.1

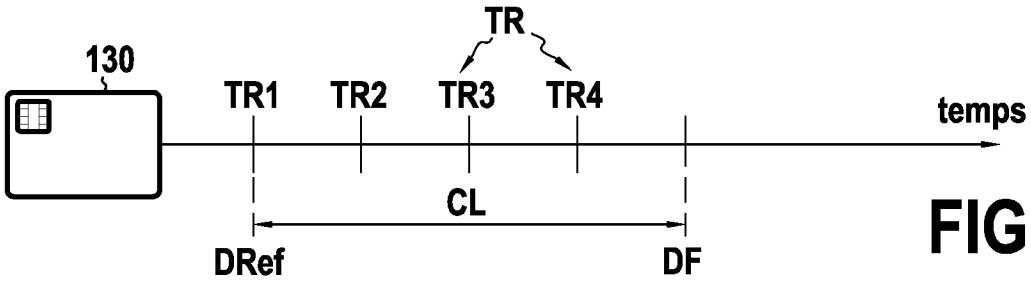

FIG.2A

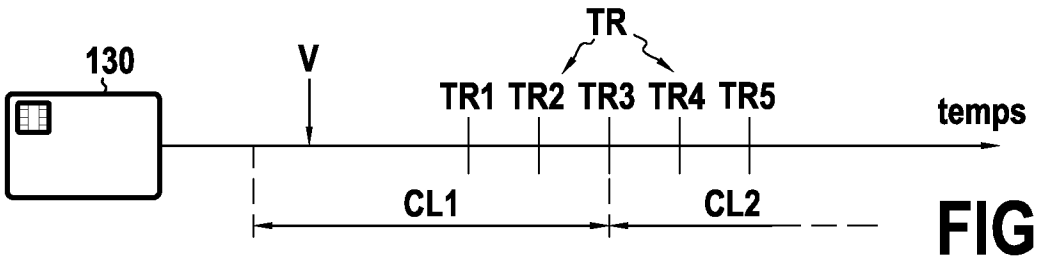

FIG.2B

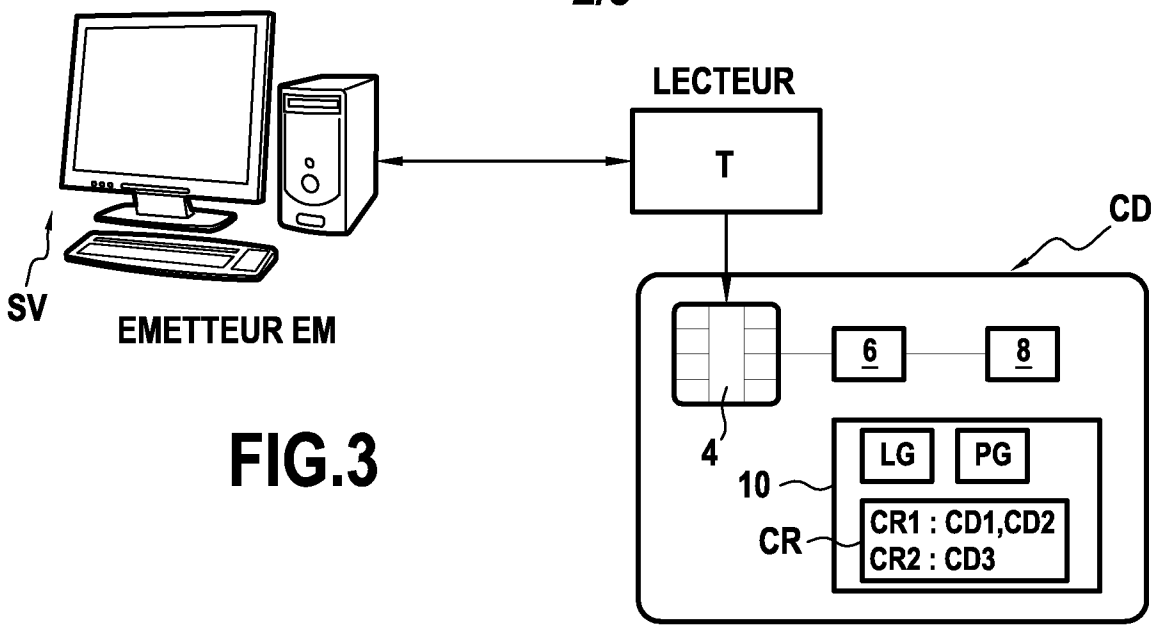

FIG.3

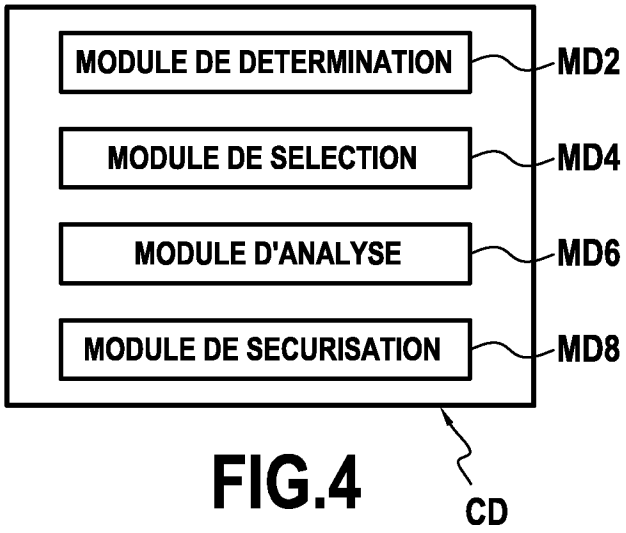

FIG.4

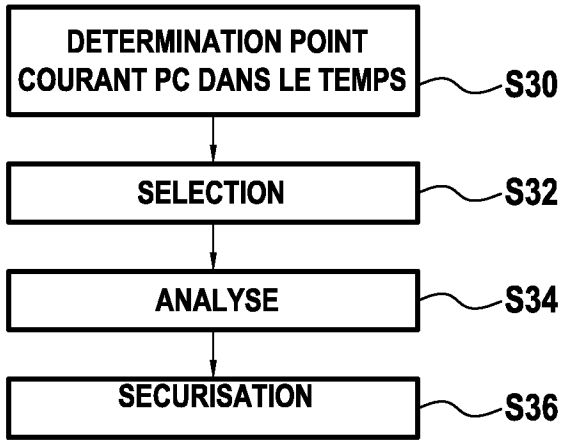

FIG.5

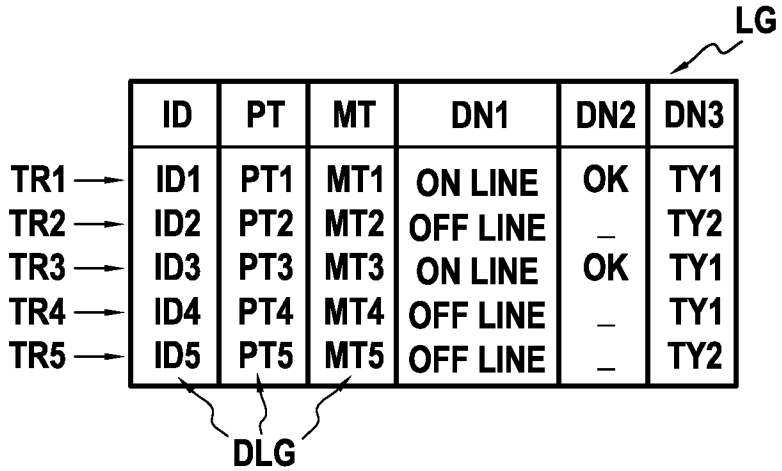

FIG.6

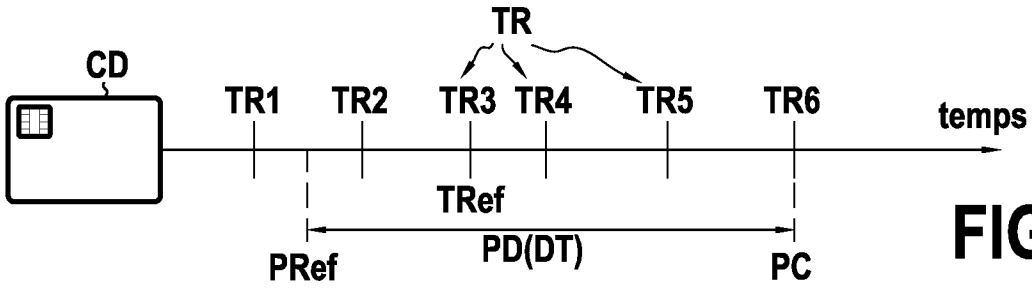
TR
CD
TR1
TR2
TR3
TR4
TR5
TR6
temps
TRef
PD(DT)
PRef
PC

FIG.7

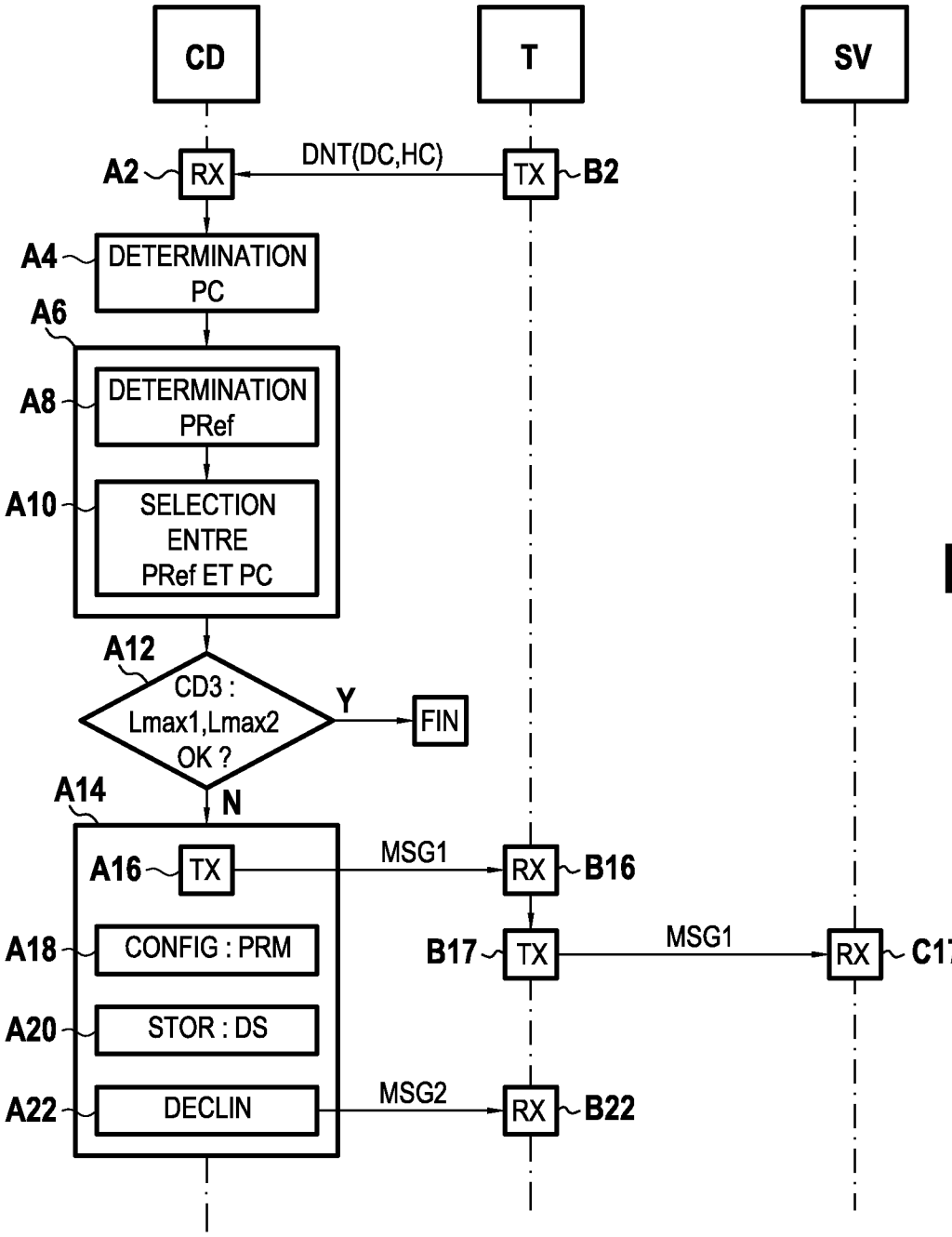
CD
T
SV
A2
RX
DNT(DC,HC)
TX
B2
A4
DETERMINATION PC
A6
A8
DETERMINATION PRef
A10
SELECTION ENTRE PRef ET PC
A12
CD3 : Lmax1,Lmax2 OK ?
Y
FIN
N
A14
A16
TX
MSG1
RX
B16
A18
CONFIG : PRM
B17
TX
MSG1
RX
C17
A20
STOR : DS
A22
DECLIN
MSG2
RX
B22

FIG.8

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/051254

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/34
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FR 2 958 770 A1 (OBERTHUR TECHNOLOGIES [FR]) 14 October 2011 (2011-10-14) abstract page 1, lines 9 -12; figure 2 page 12, line 7 - page 15, line 27; figure 4 -----	1-17
X	WO 2016/061093 A1 (PAYPAL INC [US]) 21 April 2016 (2016-04-21) abstract paragraphs [0032] - [0034] paragraphs [0042] - [0043]; figure 4 -----	1-17
A	FR 2 984 648 A1 (OBERTHUR TECHNOLOGIES [FR]) 21 June 2013 (2013-06-21) abstract page 8, lines 10-21; figure 3 ----- -/--	1-17

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 July 2017	19/07/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Dedek, Frédéric

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/051254

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2015/059389 A1 (ORANGE [FR]) 30 April 2015 (2015-04-30) abstract page 11, lines 5-19; figure 1A	1-17
A	WO 2007/078431 A2 (WELCOME REAL TIME PTE LTD [SG]; HADDAD ANEACE [FR]; MAYANCE FREDERIC [] 12 July 2007 (2007-07-12) abstract page 2, line 22 - page 6, line 33	1,13-15
A	WO 2015/095517 A1 (CAPITAL ONE FINANCIAL CORP [US]) 25 June 2015 (2015-06-25) paragraphs [0007] - [0012] paragraph [0029]	1,13-15

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2017/051254

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2958770 A1	14-10-2011	FR 2958770 A1	14-10-2011
		US 2011251958 A1	13-10-2011
WO 2016061093 A1	21-04-2016	US 2016110718 A1	21-04-2016
		WO 2016061093 A1	21-04-2016
FR 2984648 A1	21-06-2013	NONE	
WO 2015059389 A1	30-04-2015	FR 3012645 A1	01-05-2015
		WO 2015059389 A1	30-04-2015
WO 2007078431 A2	12-07-2007	AU 2006333425 A1	12-07-2007
		EP 1955269 A2	13-08-2008
		JP 2009517775 A	30-04-2009
		US 2009048934 A1	19-02-2009
		WO 2007078431 A2	12-07-2007
WO 2015095517 A1	25-06-2015	CA 2934342 A1	25-06-2015
		EP 3084702 A1	26-10-2016
		WO 2015095517 A1	25-06-2015

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2017/051254

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06Q20/34
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06Q

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	FR 2 958 770 A1 (OBERTHUR TECHNOLOGIES [FR]) 14 octobre 2011 (2011-10-14) abrégé page 1, lignes 9 -12; figure 2 page 12, ligne 7 - page 15, ligne 27; figure 4	1-17
X	WO 2016/061093 A1 (PAYPAL INC [US]) 21 avril 2016 (2016-04-21) abrégé alinéas [0032] - [0034] alinéas [0042] - [0043]; figure 4	1-17
A	FR 2 984 648 A1 (OBERTHUR TECHNOLOGIES [FR]) 21 juin 2013 (2013-06-21) abrégé page 8, lignes 10-21; figure 3	1-17

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
11 juillet 2017	19/07/2017

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Dedek, Frédéric

1

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 2015/059389 A1 (ORANGE [FR]) 30 avril 2015 (2015-04-30) abrégé page 11, lignes 5-19; figure 1A	1-17
A	WO 2007/078431 A2 (WELCOME REAL TIME PTE LTD [SG]; HADDAD ANEACE [FR]; MAYANCE FREDERIC [) 12 juillet 2007 (2007-07-12) abrégé page 2, ligne 22 - page 6, ligne 33	1,13-15
A	WO 2015/095517 A1 (CAPITAL ONE FINANCIAL CORP [US]) 25 juin 2015 (2015-06-25) alinéas [0007] - [0012] alinéa [0029]	1,13-15

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2017/051254

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2958770 A1	14-10-2011	FR 2958770 A1	14-10-2011
		US 2011251958 A1	13-10-2011
WO 2016061093 A1	21-04-2016	US 2016110718 A1	21-04-2016
		WO 2016061093 A1	21-04-2016
FR 2984648 A1	21-06-2013	AUCUN	
WO 2015059389 A1	30-04-2015	FR 3012645 A1	01-05-2015
		WO 2015059389 A1	30-04-2015
WO 2007078431 A2	12-07-2007	AU 2006333425 A1	12-07-2007
		EP 1955269 A2	13-08-2008
		JP 2009517775 A	30-04-2009
		US 2009048934 A1	19-02-2009
		WO 2007078431 A2	12-07-2007
WO 2015095517 A1	25-06-2015	CA 2934342 A1	25-06-2015
		EP 3084702 A1	26-10-2016
		WO 2015095517 A1	25-06-2015