(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
18 janvier 2018 (18.01.2018)

WIPO | PCT

(10) Numéro de publication internationale
WO 2018/011514 A1

(51) Classification internationale des brevets :
G06Q 20/32 (2012.01) *G06Q 20/40* (2012.01)

(21) Numéro de la demande internationale :
PCT/FR2017/051897

(22) Date de dépôt international :
11 juillet 2017 (11.07.2017)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1656622 11 juillet 2016 (11.07.2016) FR

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

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

CLIMEN, Bruno ; c/o OBERTHUR TECHNOLOGIES, Département Propriété Intellectuelle, 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, JO, 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, 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.

WO 2018/011514 A1

(54) Title: METHOD FOR CONTROLLING AN ELECTRONIC DEVICE FOR PROCESSING A TRANSACTION

(54) Titre : PROCÉDÉ DE CONTRÔLE D'UN DISPOSITIF ÉLECTRONIQUE POUR TRAITER UNE TRANSACTION

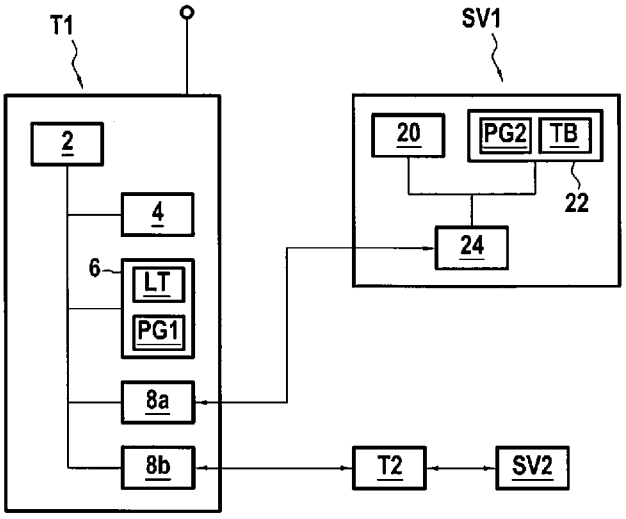

FIG.1

(57) Abstract: The invention relates to a method for controlling an electronic device (T1), said method comprising the following steps during transaction processing with the aid of a terminal (T2): receiving, from the terminal (T2), an identifier of said terminal; consulting a list (LT) of terminal identifiers in order to determine whether the identifier that was received is featured on said list (LT); and processing the transaction depending on the result of this consultation.

(57) Abrégé : L'invention propose un procédé de contrôle d'un dispositif électronique (T1), le procédé comprenant, lors d'une transaction en cours de traitement en coopération avec un terminal (T2), la réception, en provenance du terminal (T2), d'un identifiant dudit terminal; la consultation d'une liste (LT) d'identifiants de terminal pour déterminer si l'identifiant reçu est inclus dans la liste (LT); et le traitement de la transaction en fonction du résultat de la consultation.

[Suite sur la page suivante]

(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))*

Procédé de contrôle d'un dispositif électronique pour traiter une transaction

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 ou un terminal mobile par exemple, configuré 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 s'applique également aux terminaux, notamment les terminaux mobiles tels que les téléphones portables par exemple, configurés pour coopérer avec un terminal (ou lecteur) externe pour traiter une transaction.

L'invention vise notamment la sécurisation d'un tel dispositif électronique dans le traitement d'une transaction selon 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.

Des solutions alternatives à la carte à puce ont également été développées comme notamment des solutions logicielles mises en œuvre sur des terminaux pour permettre à un utilisateur d'effectuer une transaction avec un terminal externe. Une solution mobile consiste par exemple à installer une application sur un terminal mobile (un téléphone portable par exemple) pour traiter une transaction de façon similaire à une carte à puce.

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 ou solutions mobiles.

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.

De nombreux mécanismes de sécurité ont récemment été développés afin de sécuriser autant que possible l'usage croissant des cartes à puce, de type EMV notamment.

Cependant, certains terminaux de paiement peuvent présenter des faiblesses d'implémentation (nombre imprédictible non aléatoire, signature non supportée...) susceptibles d'être exploitées à mauvais escient par un tiers ou entité malveillant pour réaliser une transaction frauduleuse. Ces terminaux sont cependant fonctionnels et constituent donc un risque sécuritaire élevé pour une carte à puce, ou plus généralement pour un dispositif électronique destiné à traiter une transaction comme indiqué ci-avant.

Ces terminaux sensibles au sens sécuritaire, sont généralement connus des banques. Il n'existe toutefois pas aujourd'hui de solution satisfaisante pour sécuriser les transactions réalisées entre un dispositif électronique, tel qu'une carte à puce ou un terminal mobile par exemple, et un terminal sensible comme décrit ci-dessus.

Un besoin existe en particulier pour sécuriser le traitement d'une transaction hors ligne entre un dispositif électronique et un terminal à risque, dans la mesure où la banque n'est pas en mesure de faire de contrôles spécifiques pour s'assurer de la validité de la transaction.

Objet et résumé de l'invention / Résumé

A cet effet, la présente invention concerne un procédé de contrôle d'un dispositif électronique, ledit procédé comprenant, lors d'une transaction en cours de traitement en coopération avec un terminal, les étapes suivantes :

- réception, en provenance du terminal, d'un identifiant dudit terminal ;
- consultation d'une première liste d'au moins un identifiant de terminal pour déterminer si l'identifiant dudit terminal est inclus dans ladite première liste ; et
- traitement de la transaction en fonction du résultat de ladite consultation.

L'invention permet avantageusement à un dispositif électronique de déterminer si le terminal avec lequel il coopère lors d'une transaction présente un risque sécuritaire particulier et, dans l'affirmative, d'adapter le traitement de la transaction en conséquence afin, par exemple, de sécuriser d'avantage la transaction.

Selon un mode de réalisation particulier, le procédé comprend, préalablement à ladite étape de consultation, l'enregistrement de la première liste d'au moins un identifiant de terminal dans une mémoire du dispositif électronique. Le dispositif électronique dispose ainsi d'une liste lui permettant d'identifier le ou les terminaux à risque avec lesquels il est susceptible de coopérer lors d'une transaction.

Selon un mode de réalisation particulier, ledit procédé comprend, préalablement à ladite étape de consultation :

- envoi, à un serveur distant, d'une donnée permettant au serveur distant de déterminer la localisation du dispositif électronique ; et
- réception, en réponse audit envoi, de la première liste d'au moins un identifiant de terminal, ladite première liste étant fonction de ladite localisation du dispositif électronique.

L'invention permet ainsi avantageusement au dispositif électronique de recevoir une liste de terminaux présentant un risque sécuritaire particulier, cette liste étant adaptée à la localisation dudit dispositif électronique. De façon avantageuse, il est ainsi possible d'envoyer au dispositif électronique une liste de taille limitée adaptée à la zone géographique dans laquelle se trouve le dispositif électronique, ce qui permet un gain en termes d'espace mémoire et de ressources utilisés au niveau du dispositif électronique. En outre, l'invention permet de s'assurer que le dispositif électronique est capable de déterminer si les terminaux susceptibles d'être situés à proximité présentent un risque particulier ou non.

Selon un mode de réalisation particulier, ladite donnée est une donnée de localisation représentative de la localisation du dispositif électronique.

Selon un mode de réalisation particulier, le procédé comprend, préalablement à son envoi, la détermination de ladite donnée de localisation à partir d'au moins l'un parmi :

- des coordonnées GPS représentatives de la localisation géographique du dispositif électronique ; et
- des données de réseau représentatives de la localisation du dispositif électronique dans un réseau de communication.

Selon un mode de réalisation particulier, s'il est déterminé lors de ladite consultation que l'identifiant dudit terminal est inclus dans la liste d'au moins un identifiant de terminal, l'étape de traitement de la transaction comprend le déclenchement d'au moins une opération prédéfinie de sécurisation de la transaction.

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

- envoi d'une requête demandant le traitement en ligne de la transaction en cours ;
- enregistrement, dans un fichier d'historisation, d'une donnée d'historisation prédéfinie ; et
- configuration d'au moins un paramètre de fonctionnement du dispositif électronique.

Selon un mode de réalisation particulier, la transaction en cours est de type EMV. L'identifiant du terminal est par exemple reçu dans un message de transaction EMV de type GAC.

Selon un mode de réalisation particulier, le procédé comprend les étapes suivantes :

- réception, lors de la transaction en cours, d'une commande spécifiant une deuxième liste d'au moins un identifiant de terminal ; et
- en réponse à ladite commande, enregistrement de ladite deuxième liste dans une mémoire du dispositif électronique en remplacement de ladite première liste.

L'invention permet ainsi avantageusement de mettre à jour la liste détenue par le dispositif électronique.

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

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans un dispositif électronique tel qu'un terminal mobile, ou plus généralement dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de contrôle tel que défini ci-dessus.

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

L'invention concerne aussi un procédé d'envoi mis en œuvre par un serveur, comprenant les étapes suivantes :

- réception d'une donnée en provenance d'un dispositif électronique configuré pour coopérer avec un terminal pour mettre en œuvre une transaction ;
- détermination de la localisation du dispositif électronique à partir de ladite donnée ;
- sélection, à partir de la localisation du dispositif électronique, d'une liste d'au moins un identifiant de terminal ; et
- envoi de ladite liste à destination du dispositif électronique de sorte à configurer le traitement, par le dispositif électronique, d'une transaction.

Selon un mode de réalisation particulier, la donnée reçue est l'une parmi :

- une donnée de localisation représentative de la localisation du dispositif électronique ; et
- un identifiant d'un terminal avec lequel le dispositif électronique coopère pour traiter une transaction en cours.

Selon un mode de réalisation particulier, le serveur envoie la liste d'au moins un identifiant de terminal au dispositif électronique dans un message de transaction EMV.

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

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans un serveur, ou plus généralement dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé d'envoi tel que défini ci-dessus.

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

L'invention concerne également un dispositif électronique comprenant, lors d'une transaction en cours avec un terminal, les étapes suivantes :

- un module de réception configuré pour recevoir, lors d'une transaction en cours avec un terminal, un identifiant dudit terminal ;

- un module de détermination configuré pour consulter une première liste d'au moins un identifiant de terminal pour déterminer si l'identifiant dudit terminal est inclus dans ladite première liste ; et
- un module de traitement configuré pour traiter la transaction en fonction du résultat de la consultation de la première liste par le module de consultation.

Le dispositif électronique est par exemple un terminal mobile tel qu'un téléphone mobile intelligent configuré pour coopérer avec un terminal externe pour réaliser une transaction (de type EMV par exemple). Le dispositif électronique peut également être une carte à puce, de type EMV par exemple.

L'invention concerne en outre un serveur comprenant :

- un module de réception configuré pour recevoir une donnée en provenance d'un dispositif électronique, ledit dispositif étant configuré pour coopérer avec un terminal pour mettre en œuvre une transaction ;
- un module de détermination configuré pour déterminer la localisation du dispositif électronique à partir de ladite donnée ;
- un module de sélection configuré pour sélectionner, à partir de la localisation du dispositif électronique, une liste d'au moins un identifiant de terminal ; et
- un module d'envoi configuré pour envoyer ladite liste à destination du dispositif électronique de sorte à configurer le traitement, par le dispositif électronique, d'une transaction.

A noter que les différents modes de réalisation définis ci-avant en relation avec le procédé de contrôle, d'une part, et avec le procédé d'envoi, d'autre part, ainsi que les avantages associés à ces procédés, s'appliquent par analogie au dispositif électronique et au serveur définis ci-avant.

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 représente schématiquement un terminal mobile apte à coopérer avec un serveur distant SV1 et avec un terminal externe T2, selon un mode de réalisation particulier de l'invention ;

- la figure 2 représente schématiquement des modules mis en œuvre dans le terminal mobile T1 et dans le serveur distant SV1 représentés en figure 1, selon un mode de réalisation particulier de l'invention ;
- la figure 3 représente schématiquement des procédés de contrôle mis en œuvre respectivement par le terminal mobile T1 et par le serveur distant SV1 représentés en figures 1 et 2, selon un mode de réalisation particulier de l'invention ;
- la figure 4a représente schématiquement un exemple d'une table TB contenant des listes LT d'au moins un identifiant de terminal, en association avec une zone géographique ;
- la figure 4b représente schématiquement un exemple d'une liste LT2 contenue dans la table TB représentée en figure 4a ;
- la figure 5 représente, sous forme d'un diagramme, les principales étapes de procédés de contrôle mis en œuvre respectivement par le terminal mobile T1 et par le serveur distant SV1 représentés en figures 1 et 2, selon un mode de réalisation particulier de l'invention ;
- la figure 6 représente schématiquement une carte à puce apte à coopérer avec un serveur distant SV3 par l'intermédiaire d'un terminal externe T3, selon à un mode de réalisation particulier de l'invention ;
- les figures 7a et 7b représentent schématiquement des modules mis en œuvre dans la carte à puce CD et dans le serveur distant SV3 représentés en figure 6, selon un mode de réalisation particulier de l'invention ; et
- la figure 8 représente, sous forme d'un diagramme, les principales étapes de procédés de contrôle mis en œuvre respectivement par la carte à puce CD et par le serveur distant SV3 représentés en figure 6, selon un mode de réalisation particulier de l'invention.

Description détaillée de plusieurs modes de réalisation

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

L'invention vise en particulier à sécuriser les transactions réalisées entre un dispositif électronique, tel qu'une carte à puce ou un terminal mobile par exemple, et un terminal externe présentant un risque sécuritaire élevé.

Dans le présent exposé, des exemples de mises en œuvre de l'invention sont décrits de façon non limitative en relation avec une transaction conforme au protocole EMV. On comprendra que l'invention s'applique plus généralement à tout dispositif électronique configuré pour mettre en œuvre une transaction, y compris selon un standard de transaction autre que le standard EMV.

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 de façon non limitative dans le cadre d'une transaction de paiement dans le domaine bancaire, d'autres types de transaction étant possibles 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 1** représente, selon un mode de réalisation particulier, un terminal (ou dispositif électronique) T1 configuré pour coopérer avec un serveur distant SV1 et un terminal externe (ou lecteur) T2. Le terminal T2 est configuré pour faire l'interface entre le terminal T1 et un serveur distant SV2. Dans un exemple particulier, les serveurs SV1 et SV2 forment un seul et même serveur.

On suppose ici que le terminal T1 est un terminal mobile, par exemple un téléphone portable, configuré pour traiter des transactions EMV en coopération avec le terminal T2, d'autres exemples de terminaux (mobiles ou fixes) étant toutefois possibles dans le cadre de l'invention. Le terminal T1 constitue dans cet exemple un terminal de paiement électronique.

On comprendra que certains éléments généralement présents dans un téléphone portable ou dans un serveur ont été volontairement omis car ils ne sont pas nécessaires à la compréhension de la présente invention. A noter également que le terminal mobile T1 et le serveur distant SV1 représentés en **figure 1** ne constituent que des exemples 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 du terminal mobile T1 et du serveur SV1 ne sont décrits ici que pour faciliter la compréhension de l'invention, ces éléments n'étant pas indispensables pour mettre en œuvre l'invention.

Plus précisément, le terminal mobile T1 comprend dans cet exemple un processeur 2, une mémoire volatile 4 (de type RAM), une mémoire non volatile réinscriptible 6, une première interface de communication 8a et une deuxième interface de communication 8b.

La mémoire non volatile réinscriptible 6 constitue ici un support d'enregistrement conforme à un mode de réalisation particulier, lisible par le terminal T1, et sur lequel est enregistré un programme d'ordinateur PG1 conforme à un mode de réalisation particulier. Ce programme d'ordinateur PG1 comporte des instructions pour l'exécution des étapes d'un procédé de contrôle selon un mode de réalisation particulier.

La mémoire 6 est par ailleurs configurée pour contenir une liste LT d'au moins un identifiant de terminal. Comme expliqué plus en détail par la suite, cette liste permet au terminal mobile T1 d'identifier des terminaux présentant un risque sécuritaire particulier. A partir de cette liste LT, le terminal T1 peut ainsi déterminer si le terminal T2, avec lequel il communique pour traiter une transaction EMV, est un terminal à risque ou non.

Les interfaces 8a, 8b permettent au terminal mobile T1 de communiquer respectivement avec le serveur distant SV1 et avec le terminal externe T2, comme expliqué ci-après.

Par ailleurs, le serveur SV1 comprend dans cet exemple un processeur 20, une mémoire non volatile réinscriptible 22 et interface de communication 24.

La mémoire non volatile réinscriptible 22 constitue ici un support d'enregistrement conforme à un mode de réalisation particulier, lisible par le serveur SV1, et sur lequel est enregistré un programme d'ordinateur PG2 conforme à un mode de réalisation particulier. Ce programme d'ordinateur PG2 comporte des instructions pour l'exécution des étapes d'un procédé de contrôle selon un mode de réalisation particulier.

La mémoire 22 est en outre configurée pour contenir une table TB contenant au moins une liste LT en association avec une zone géographique donnée, chaque liste LT contenant au moins un identifiant de terminal, comme expliqué ultérieurement dans un exemple particulier en référence aux **figures 4a** et **4b**. Selon une variante, la table TB est enregistrée dans une mémoire (par exemple une base de données) située hors du serveur SV1 et consultable par ce dernier.

Comme expliqué ci-après en référence à la **figure 2**, le terminal T1 est configuré pour coopérer avec le terminal externe T2 pour mettre en œuvre une transaction EMV. Lorsque le traitement de cette transaction EMV se fait en ligne, le terminal T2 est configuré pour coopérer avec le serveur distant SV2 pour permettre à ce dernier de vérifier et valider la transaction EMV en cours.

Dans l'exemple considéré ici, les serveurs SV1 et SV2 sont des serveurs contrôlés par l'émetteur (par exemple une banque) d'une application bancaire AP2 installée dans le terminal T1, comme illustré ci-après en **figure 2**.

Comme représenté en **figures 1** et **2**, le processeur 2 du terminal mobile T1 piloté par le programme d'ordinateur PG1 met ici en œuvre un certain nombre de modules, à savoir : un premier module de détermination MD2, un module d'envoi MD4, un premier module de réception MD6, un deuxième module de réception MD8, un deuxième module de détermination MD10 et un module de traitement MD12.

Dans cet exemple, le module d'envoi MD4 et le module de réception MD6 sont mis en œuvre par une première application AP1 installée dans le terminal T1 et exécutable par le processeur 2. De même, le module de réception MD8, le module de détermination MD10 et le module de traitement MD12 sont mis en œuvre par une autre application AP2 installée dans le terminal T1 et exécutable par le processeur 2. Dans cet exemple, les applications AP1 et AP2 sont des applications bancaires.

Plus précisément, le module de détermination MD2 est configuré pour déterminer une donnée de localisation DN représentative de la localisation du terminal mobile T1 à un instant donné. Dans l'exemple considéré ici, le module de détermination MD2 est configuré pour obtenir des coordonnées géographiques (par exemple des coordonnées GPS) indiquant la position géographique du terminal mobile T1, d'autres exemples de mise en œuvre étant toutefois envisageables.

Selon une variante, le module de détermination MD2 est apte à déterminer des données de réseau représentatives de la localisation du terminal mobile T2 dans un réseau de communication, tel qu'un réseau de téléphonie mobile par exemple. Selon cette variante, le module MD2 identifie par exemple au moins deux points d'accès (des antennes relais par exemple) au réseau de communication, ces points d'accès se situant à proximité du terminal mobile T1. A partir des points d'accès ainsi identifiés, le module de détermination MD2 est configuré pour déterminer la donnée de localisation DN, par exemple en utilisant une technique de repérage bien connue de triangularisation.

Le module d'envoi MD4 est configuré pour envoyer la donnée de localisation DN au serveur SV1.

Le module de réception MD6 est configuré pour recevoir, en réponse à la donnée DN envoyée par le module d'envoi MD4, une liste LT d'au moins un identifiant de terminal.

Le module de réception MD8 est configuré pour recevoir, lors d'une transaction EMV en cours avec le terminal externe T2, un identifiant IDX2 dudit terminal T2.

Le deuxième module de détermination MD10 est configuré pour consulter la liste LT reçue par le premier module de réception MD6 pour déterminer si l'identifiant IDX2 reçu par le deuxième module de réception MD8 est inclus dans ladite liste LT. Dans un exemple particulier, le module de réception MD6 est en outre configuré pour enregistrer la liste LT dans une mémoire du terminal mobile T1 (dans la mémoire 6 dans cet exemple).

Le module de traitement MD12 est configuré pour traiter la transaction EMV en cours en fonction du résultat de la consultation de la liste LT par le deuxième module de détermination MD10. Dans un exemple particulier, si le module de détermination MD10 détermine que l'identifiant IDX2 du terminal T2 est inclus dans la liste LT, le module de traitement MD12 est configuré pour déclencher au moins une opération prédéfinie de sécurisation de la transaction EMV en cours. Le module de traitement MD12 est par exemple configuré pour déclencher, en tant qu'opération de sécurisation, l'envoi d'un message RGAC requérant la poursuite de la transaction en mode en ligne, de façon à ce que le serveur distant SV2 de la banque puisse procéder aux vérifications nécessaires.

Par ailleurs, comme représenté en **figures 1** et **2**, le processeur 20 du serveur SV1 piloté par le programme d'ordinateur PG2 met ici en œuvre un certain nombre de modules, à savoir : un module de réception MD20, un module de détermination MD22, un module de sélection MD24 et un module d'envoi MD26.

Plus précisément, le module de réception MD20 est configuré pour recevoir la donnée de localisation DN émis par le module d'envoi MD4 du terminal mobile T1.

Le module de détermination MD22 est configuré pour déterminer la localisation, notée LOC, du terminal mobile T1 à partir de la donnée de localisation DN reçue. La donnée de localisation DN peut se présenter sous tout format approprié pouvant être interprété par le module de détermination MD22 du serveur SV1.

Le module de sélection MD24 est configuré pour sélectionner, en fonction de la localisation LOC du terminal mobile T1, une liste LT correspondante, c'est-à-dire une liste

LT d'au moins un identifiant de terminal, cette liste étant ainsi adaptée à la position géographique du terminal mobile T1. Comme expliqué par la suite, l'invention permet avantageusement au terminal T1 de déterminer si le ou les terminaux externes T2 avec lequel il est susceptible de coopérer présentent un risque sécuritaire particulier et, dans l'affirmative, d'adapter le traitement d'une transaction en conséquence.

Le module d'envoi MD26 du serveur SV1 est configuré pour envoyer la liste LT, sélectionnée par le module de sélection MD24, à destination du terminal mobile T1. De cette manière, il est possible de configurer la manière dont le terminal mobile T1 traite une ou des transactions EMV ultérieures.

Le fonctionnement des modules MD2-MD12 du terminal mobile T1 et des modules MD20-MD26 du serveur distant SV1 apparaîtra plus précisément dans les exemples de réalisation décrits ci-après en référence aux **figures 3**, **4a**, **4b** et **5**.

On comprendra que les modules MD2-MD26 tels que représentés en **figure 2** ne représentent qu'un exemple de mise en œuvre non limitatif de l'invention.

Des modes de réalisation particuliers sont à présent décrit sen référence aux **figures 3-5**. Plus précisément, le terminal mobile T1 et le serveur distant SV1 représentés en **figures 1** et **2** mettent chacun en œuvre un procédé de contrôle en exécutant respectivement les programmes d'ordinateur PG1 et PG2.

Comme représentées en **figures 1** et **4a**, trois listes LT (notées LT1, LT2 et LT3) sont ici enregistrées dans la mémoire 22 du serveur SV1 en association avec une zone géographique RG respective (notées RG1, RG2 er RG3). Cet enregistrement se présente ici sous la forme d'une table TB bien que d'autres représentations ou arrangements soient possibles.

Chaque zone géographique peut correspondre à un territoire, à une région ou encore à un site approprié. Dans un exemple particulier, une zone géographique correspond à un pays, à une ville ou encore à une zone de périmètre quelconque. La banque émettrice peut par exemple définir la taille et les emplacements des zones géographiques en fonction de critères de son choix (adresse postale du domicile du porteur du terminal mobile T1 etc.).

Plus précisément, dans l'exemple considéré ici, la table TB contient les listes LT1, LT2 et LT3 en association avec des identifiants respectifs IDR1, IDR2, IDR3 (notés collectivement IDR) correspondant aux zones géographiques RG1, RG2, RG3. Chaque

identifiant de zone IDR1-IDR3 identifie une zone géographique RG correspondante, en association avec une liste LT.

La **figure 4b** représente schématiquement la liste LT2 contenant par exemple ici les identifiants IDT notés IDT1 à IDT4, chaque identifiant IDT correspondant à un terminal externe (ou lecteur) respectif susceptible de coopérer avec le terminal mobile T1 pour traiter une transaction EMV.

Comme représenté en **figure 3**, le terminal mobile T1 détermine, au cours d'une étape A2, une donnée de localisation DN représentative de la localisation LOC du terminal mobile T1. Dans l'exemple décrit ici, cette donnée DN est déterminée à partir de coordonnées GPS obtenues par le module de détermination MD2, ces coordonnées GPS étant représentatives de la position géographique du terminal mobile 2. Comme déjà expliqué, d'autres techniques sont possibles pour déterminer la donnée de localisation DN. Le format de la donnée de localisation DN peut varier selon le cas. Dans un exemple particulier, la donnée de localisation DN comprend des coordonnées physiques (par exemple les coordonnées GPS) du terminal mobile T1.

En A4, le terminal mobile T1 envoie la donnée de localisation DN au serveur SV1 qui la reçoit en B6.

Le serveur SV1 détermine (B8) ensuite, à partir de la donnée de localisation DN reçue, la localisation LOC du terminal mobile T1.

En B10, le serveur SV1 consulte sa table TB et sélectionne, à partir de la localisation LOC (ou directement à partir des données de localisation DN), la liste LT correspondante. Pour ce faire, le serveur SV1 détermine par exemple dans quelle région RG spécifiée dans la table TB se trouve le terminal mobile T1 et en déduit la liste LT associée. On suppose dans cet exemple que le serveur SV1 détermine, à partir de la localisation LOC du terminal mobile T1, que ledit terminal T1 se trouve dans la zone géographique RG2 et, par conséquent, sélectionne (B10) la liste LT2 associée, illustrée en **figure 4b**.

En B12, le serveur SV1 envoie alors au terminal mobile T1 la liste LT2 sélectionnée en B10. Le terminal mobile T1 reçoit cette liste LT2 en A12. Dans un exemple particulier, le serveur SV1 envoie en B12 la liste LT2 sous forme chiffrée (ou cryptée). Le terminal mobile T1 est alors capable de déchiffrer la liste LT2 à partir d'une clé cryptographique dont il dispose.

En A14, le terminal mobile T1 enregistre la liste LT2 dans sa mémoire 6.

A l'issue des procédés de contrôle représentés en **figure 3**, le terminal mobile T1 dispose ainsi dans sa mémoire d'une liste d'au moins un terminal (ou lecteur) présentant un risque sécuritaire particulier, cette liste étant adaptée à la localisation du terminal mobile T1. De façon avantageuse, il est ainsi possible d'envoyer au terminal mobile T1 une liste de taille limitée adaptée à la zone géographique dans laquelle se trouve ledit terminal T1, ce qui permet un gain en termes d'espace mémoire et de ressources utilisés au niveau du terminal mobile T1. En outre, l'invention permet de s'assurer que le terminal mobile T1 est capable de déterminer si les terminaux externes T2 situés à proximité présentent un risque particulier ou non.

L'invention permet également de mettre à jour si nécessaire une liste LT déjà contenue en mémoire dans le terminal mobile T1. Différents modes de réalisation sont envisageables pour mettre à jour cette liste LT.

Selon un exemple particulier, préalablement à l'étape A2 représentée en **figure 3**, le terminal mobile T1 contient déjà en mémoire une liste LT, par exemple la liste LT1. En A14, le terminal mobile T1 est alors configuré pour effacer la liste LT1 existante et pour enregistrer, en tant que nouvelle liste, la liste LT2 reçue en A12. De cette façon, il est possible de limiter l'espace mémoire nécessaire dans le terminal mobile T1 pour stocker les identifiants IDT de terminaux à risque. Le terminal mobile T1 dispose ainsi des identifiants des terminaux externes qu'il est susceptible de rencontrer dans son voisinage.

Selon un mode de réalisation particulier, le serveur SV1 envoie également, en B12 (**figure 3**), au terminal mobile T1, des données DRG2 représentatives de la zone géographique RG2 associée à la liste LT2 sélectionnée (B12) par le serveur SV1. Ces données DRG2 définissent les limites de la zone géographique DRG2. En A14, le terminal mobile T1 enregistre les données DRG2 en association avec la liste LT2. Le terminal mobile T1 compare ensuite périodiquement, et/ou sur réception d'une commande, la position courante du terminal mobile T1 avec les limites de la zone géographique RG2 définies par les données DRG2. Le terminal mobile T1 envoie au serveur SV1 une demande de mise à jour de sa liste LT2 contenue dans sa mémoire s'il détecte que sa position courante est hors de la zone géographiques associée RG2. Cette demande de mise à jour comprend par exemple une donnée de localisation DN représentative de la nouvelle positon du terminal mobile T1. La mise à jour de la liste LT2 peut s'effectuer de la même manière que les procédés de contrôle illustrés en **figure 3** pour récupérer et stocker la liste LT2 dans la mémoire du terminal mobile T1. Ce mode de réalisation

permet avantageusement de limiter les ressources du réseau et du serveur SV1 nécessaires pour la mise à jour de la liste LT dans la mesure où les zones géographiques sont préétablies et le terminal mobile T1 envoie une requête de mise à jour seulement s'il détecte qu'il est positionné hors de la zone géographique associée à sa liste LT.

Selon une autre variante du procédé de contrôle représenté en **figure 3**, le terminal mobile T1 définit, en tant que position de référence PRef, la position dudit terminal mobile T1 correspondant à la donnée de localisation DN envoyée en A4. Après la réception A12 de la liste LT1, le terminal mobile T1 est alors configuré pour évaluer périodiquement, et/ou en réponse à une commande reçue, la distance entre la position courante du terminal mobile T1 et la position de référence PRef. Le terminal mobile T1 envoie au serveur SV1 une demande de mise à jour de sa liste LT s'il détecte que sa position courante se situe à une distance D supérieure ou égale à une distance limite prédéfinie Dlim vis-à-vis de la position de référence PRef. La mise à jour de la liste LT2 peut s'effectuer de la même manière que les procédés de contrôle illustrés en **figure 3** pour récupérer et stocker la liste LT2 dans la mémoire du terminal mobile T1. Ce mode de réalisation permet de limiter les ressources nécessaires au niveau du terminal mobile T1 dans la mesure où il n'est pas nécessaire que le terminal mobile T1 détermine les limites de la zone géographique associée à sa liste LT actuelle, ou qu'il compare ces limites avec sa position courante pour déterminer si une mise à jour de sa liste LT est nécessaire.

Selon un exemple de réalisation particulier, on suppose qu'après l'étape A14 d'enregistrement de la liste LT2 comme illustrée en **figure 3**, le terminal mobile T1 débute le traitement d'une transaction EMV notée TR1, comme illustré en **figure 5**. Pour ce faire, le terminal mobile T1 coopère avec le terminal externe T2 de façon connue selon le protocole EMV. Le terminal mobile T1 et le terminal externe T2 s'échangent divers messages normalisés de transaction EMV tels que, par exemple, les messages RST (« Reset »), ATR (« Answer to Reset »), SELECT FILE ou encore SELECT APPLICATION bien connus de l'homme du métier.

Comme illustré en **figure 5**, le terminal T2 envoie (C20) au terminal mobile T1 un identifiant IDX2 du terminal T2. Dans l'exemple considéré ici, l'identifiant IDX2 est envoyé en C20 dans un message de transaction MSG1 de type « GENERATE AC » (GAC) bien connu de l'homme du métier. La commande GAC contient des informations telles que, par exemple, le montant de la transaction en cours, la devise utilisée et/ou le type de transaction, etc.

Le terminal mobile T1 reçoit l'identifiant IDX2 du terminal externe T2 en A20 puis consulte en A22 la liste LT2, précédemment reçue en A12 (**figure 3**), pour déterminer si l'identifiant IDX2 est inclus dans ladite liste LT2.

Le terminal mobile T1 traite (A24) ensuite la transaction TR1 en fonction du résultat de la consultation A22. Dans l'exemple considéré ici, s'il est détecté en A22 que l'identifiant IDX2 est contenu dans la liste LT2 présente dans la mémoire 6, le terminal mobile T1 en déduit que le terminal externe T2 présente un risque sécuritaire élevé et adapte son traitement A24 de la transaction TR1 en conséquence afin de sécuriser la transaction TR1.

Selon un exemple particulier, s'il est déterminé lors de ladite consultation A22 que l'identifiant IDX2 du terminal T2 est inclus dans la liste LT2, le traitement A24 de la transaction par le terminal mobile T1 comprend le déclenchement d'au moins une opération prédéfinie de sécurisation de la transaction TR1. Le terminal mobile T1 réalise par exemple au moins l'une des opérations de sécurisation A26, A28 et A30 telles que décrites ci-après.

En A26, le terminal mobile T1 envoie une requête MSG2 au terminal T2 demandant le traitement en mode en ligne de la transaction TR1 en cours. Dans cet exemple particulier, la requête MSG2 est une requête de type ARQC (pour « Autorisation Request Cryptogram ») selon le protocole EMV, bien connue de l'homme du métier. Le terminal T2 reçoit la requête MSG2 en C26, puis transmet celle-ci au serveur distant SV2 en C28. Une fois la requête MSG2 reçue (B28), le serveur distant SV2 peut alors authentifier la transaction TR1 et effectuer les contrôles de sécurité appropriés.

En A28, le terminal mobile T1 enregistre, dans un fichier d'historisation (non représenté), une donnée d'historisation prédéfinie notée ici DNH. Cette donnée DNH est par exemple stockée dans une mémoire du terminal mobile T1. Dans un exemple particulier, cette donnée d'historisation DNH indique qu'une transaction TR1 a été traitée en coopération avec le terminal externe T2 présentant un risque sécuritaire élevé. Il est ainsi possible de garder un historique, dans le terminal mobile T1, des transactions à risque traiter avec un terminal externe sensible. Cette donnée d'historisation DNH pourra si besoin être consultée ultérieurement par la banque.

En A30, le terminal mobile T1 configure au moins un paramètre de fonctionnement PR du terminal mobile T1. Chaque paramètre de fonctionnement définit la manière dont le

terminal mobile T1 traite une transaction EMV. Ainsi, le terminal mobile T1 modifie par un compteur ou le seuil limite de ce dernier.

La présente invention permet avantageusement à un dispositif électronique (ici le terminal mobile T1) de déterminer si un terminal externe, avec lequel il coopère pour traiter une transaction en cours, présente un risque sécuritaire particulier. De manière avantageuse, le dispositif électronique peut vérifier si ce terminal externe est un terminal à risque lors d'une transaction hors ligne, c'est-à-dire sans l'intervention du serveur distant SV2 de l'émetteur. En fonction de si le terminal externe en question est identifié comme étant à risque ou non, le dispositif électronique est alors en mesure d'adapter son traitement de la transaction en cours. Si besoin, le dispositif électronique peut requérir la poursuite de la transaction en ligne avec l'aide du serveur distant SV2.

Dans un exemple particulier, la liste LT d'au moins un identifiant de terminal dont dispose le dispositif électronique est adaptée à la position dudit dispositif électronique (comme décrit ci-avant en référence à la **figure 3**). Cela permet avantageusement de s'assurer que le dispositif électronique est capable de déterminer si les terminaux externes T2 avec lesquels il est susceptible de coopérer présentent un risque sécuritaire particulier ou non.

En outre, l'identité de terminaux de paiement, par exemple, présentant une faiblesse de sécurité peut constituer une information sensible que les banques souhaitent protéger. L'invention permet avantageusement de limiter le nombre des terminaux sensibles qui sont identifiés dans de la liste transmise au dispositif électronique de l'invention, de sorte à réduire au maximum les risques en cas d'interception par un tiers ou une entité malveillante.

A noter que, dans ce mode de réalisation, le terminal mobile T1 reçoit la liste LT appropriée hors du cadre d'une transaction, de type EMV par exemple, avec un terminal externe. Il est ainsi possible de mettre à jour la liste LT d'identifiants de terminal du terminal mobile sans allonger la durée de traitement d'une transaction EMV ou autre.

Comme déjà indiqué, la mise en œuvre de l'invention n'est pas limitée à un terminal mobile et peut s'appliquer à divers dispositifs électroniques configurés pour traiter une transaction, de type EMV par exemple, avec un terminal externe (ou lecteur).

La **figure 6** représente, selon un autre mode de réalisation, une carte à puce EMV notée CD, cette carte CD étant configurée pour coopérer avec un terminal externe T3 pour traiter une transaction EMV. Le terminal T3 est configuré pour faire l'interface entre

la carte à puce CD et un serveur distant SV3, en particulier lorsqu'une transaction EMV est traitée en ligne. Dans l'exemple considéré ici, le serveur SV3 est contrôlé par l'émetteur (la banque par exemple) de la carte à puce CD.

On comprendra ici aussi que certains éléments généralement présents dans une carte à puce ou dans un serveur bancaire 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 et le serveur distant SV3 représentés en **figure 6** ne constituent que des exemples 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 CD et du serveur SV3 ne sont décrits ici que pour faciliter la compréhension de l'invention, ces éléments n'étant pas indispensables pour mettre en œuvre l'invention.

Plus précisément, la carte à puce CD comprend dans cet exemple un processeur 30, des contacts externes 32 configurés pour coopérer avec le lecteur T3 et une mémoire non volatile réinscriptible 34.

La mémoire 34 constitue dans un cet exemple un support d'enregistrement conforme à un mode de réalisation particulier, lisible par la carte à puce CD, et sur lequel est enregistré un programme d'ordinateur PG3 conforme à un mode de réalisation particulier. Ce programme d'ordinateur PG3 comporte des instructions pour l'exécution des étapes d'un procédé de contrôle selon un mode de réalisation particulier, comme décrit ci-après.

Dans un exemple particulier, la carte à puce CD est conforme à la norme ISO 7816. Dans ce cas, les contacts externes 32 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 T3 en mode sans contact via une antenne RF intégrée dans la carte CD.

Toujours dans l'exemple considéré ici, la mémoire 34 est configurée pour contenir une liste LT d'au moins un identifiant de terminal, de la même manière que la mémoire 6 représentée en **figure 1**.

Toujours en référence à la **figure 6**, le serveur SV3 présente dans cet exemple une structure similaire à celle du serveur SV1 illustrée en **figure 1**. Plus particulièrement, le serveur SV2 comprend dans cet exemple un processeur 40, une mémoire non volatile réinscriptible 42 et interface de communication 44.

La mémoire 42 constitue ici un support d'enregistrement conforme à un mode de réalisation particulier, lisible par le serveur SV3, et sur lequel est enregistré un programme

d'ordinateur PG4 conforme à un mode de réalisation particulier. Ce programme d'ordinateur PG4 comporte des instructions pour l'exécution des étapes d'un procédé de contrôle selon un mode de réalisation particulier.

La mémoire 42 est en outre configurée pour contenir une table TB identique à celle décrite ci-avant en référence aux **figures 4a, 4b**. Dans l'exemple considéré ici, la table TB contient ainsi les listes LT1 à LT3 en association avec les zones géographiques respectives RG1 à RG3 (ou plus particulièrement, en association avec les identifiants de zones IDR1 à IDR3). Selon une variante, la table TB est enregistrée dans une mémoire (par exemple une base de données) hors du serveur SV3 et consultable par ce dernier.

L'interface 44 permet au serveur SV3 de communiquer avec le terminal externe T3.

Par ailleurs, le processeur 30 de la carte CD, piloté par le programme d'ordinateur PG3, met ici en œuvre un certain nombre de modules représentés en **figure 7a**, à savoir : un premier module de réception MD40, un module de détermination MD42, un module de traitement MD44, un module d'envoi MD46 et un deuxième module de réception MD48.

Le premier module de réception MD40 est configuré pour recevoir un identifiant IDX3 du terminal externe T3, par exemple dans un message de transaction EMV. Dans un exemple particulier, le module de réception MD40 est en outre configuré pour enregistrer l'identifiant IDX3 reçue dans la mémoire 34 de la carte à puce CD.

Le module de détermination MD42 est configuré pour consulter la liste LT, présente dans la mémoire 34, pour déterminer si l'identifiant IDX3 reçu par le premier module de réception MD40 est inclus dans ladite liste LT.

Le module de traitement MD44 est configuré pour traiter une transaction EMV en cours en fonction du résultat de la consultation de la liste LT par le module de détermination MD42. Dans un exemple particulier, si le module de détermination MD42 détermine que l'identifiant IDX3 du terminal T3 est inclus dans la liste LT, le module de traitement MD12 est configuré pour déclencher au moins une opération prédéfinie de sécurisation de la transaction EMV en cours. Le module de traitement MD44 est par exemple configuré pour déclencher une opération de sécurisation prédéfinie de façon identique au module de traitement MD12 illustré en **figure 1**.

Le module d'envoi MD46 est configuré pour envoyer, par exemple dans un message de transaction EMV, l'identifiant IDX3 du terminal T3 au serveur SV3.

Le module de réception MD48 est configuré pour recevoir, en réponse à l'identifiant IDX3 envoyé par le module d'envoi MD46, une nouvelle liste LT d'au moins un identifiant de terminal. Cette nouvelle liste LT est par exemple reçue dans une commande, dite commande de script, provenant du serveur SV3.

Par ailleurs, le processeur 40 du serveur SV3, piloté par le programme d'ordinateur PG4, met ici en œuvre un certain nombre de modules représentés en **figure 7b**, à savoir : un module de réception MD60, un module de détermination MD62, un module de sélection MD64 et un module d'envoi MD66. Les modules MD60 à MD66 du serveur SV3 fonctionnent respectivement de façon analogue aux modules MD20 à MD26 du serveur SV1, tel que représentés en **figure 2**.

Plus précisément, le module de réception MD60 est configuré pour recevoir l'identifiant IDX3, du terminal T3, en provenance de la carte à puce CD.

Le module de détermination MD62 est configuré pour déterminer la localisation, notée LOC, de la carte à puce CD à partir de l'identifiant IDX3 reçue. Sachant quel terminal T3 coopère avec la carte CD, le serveur SV3 est en effet capable d'en déduire la position de la carte CD.

Le module de sélection MD64 est configuré pour sélectionner, à partir de la localisation LOC de la carte à puce CD, une liste LT correspondante, c'est-à-dire une liste LT d'au moins un identifiant IDT de terminal, cette liste étant adaptée à la position géographique de la carte à puce CD. Comme indiqué par la suite, cette liste permet ensuite à la carte à puce CD d'identifier le ou les terminaux externes T3 se trouvant dans son voisinage, et présentant un risque sécuritaire particulier.

Le module d'envoi MD66 du serveur SV3 est configuré pour envoyer la liste LT, sélectionnée par le module de sélection MD64, à destination de la carte à puce CD. Il est ainsi possible de configurer la manière dont la carte à puce CD traite une ou des transactions EMV ultérieures.

Le fonctionnement des modules MD40-MD48 de la carte à puce CD et des modules MD60-MD66 du serveur distant SV3 apparaîtra plus précisément dans les exemples de réalisation décrits ci-après en référence à la **figure 8**.

On comprendra que les modules MD40-MD48 de la carte à puce CD et les modules MD60-MD66 du serveur distant SV3, tels que représentés dans les **figures 7a** et **7b,** ne constituent qu'un exemple de mise en œuvre non limitatif de l'invention.

Un mode de réalisation particulier est à présent décrit en référence à la **figure 8**. Plus précisément, la carte à puce CD et le serveur distant SV3 représentés en **figure 6** mettent chacun en œuvre un procédé de contrôle en exécutant respectivement les programmes d'ordinateur PG3 et PG4.

Dans un état initial, on suppose que la liste LT2 telle que représentée en **figure 4b** est enregistrée dans la mémoire 34 de la carte à puce CD. Cette liste LT2 est par exemple enregistrée lors d'une phase de personnalisation de la carte à puce CD ou lors d'une mise à jour ultérieure de la carte à puce CD.

Comme déjà indiqué, la table TB du serveur SV3 contient les listes LT1, LT2 et LT3 (notées collectivement LT) en association avec respectivement les zones géographiques RG1, RG2 er RG3 (notées collectivement RG).

Comme illustré en **figure 8**, on suppose que la carte à puce CD a initié le traitement d'une transaction EMV notée TR2 avec le terminal externe T3. Pour ce faire, la carte à puce CD coopère avec le terminal externe T3 de façon connue selon le protocole EMV, La carte à puce CD et le terminal externe T3 s'échangent en particulier des messages normalisés de transaction EMV bien connus de l'homme du métier, tels que RST, ATR SELECT FILE etc. comme déjà expliqué en référence à la transaction TR1 en **figure 5**.

Au cours d'une étape d'envoi C40, le terminal externe T3 envoie l'identifiant IDX3 dudit terminal T3 à la carte à puce CD. Le message MSG4, dans lequel est envoyé l'identifiant IDX3 en C40, est dans cet exemple un message GAC conforme au standard EMV.

La carte à puce CD reçoit l'identifiant IDX3 du terminal externe T3 en A40 puis consulte en A42 la liste LT2, de façon analogue à la consultation A22 représentée en **figure 5**, pour déterminer si l'identifiant IDX3 est inclus dans ladite liste LT2.

La carte à puce CD traite (A43) ensuite la transaction TR2 en cours en fonction du résultat de la consultation A42. Dans l'exemple considéré ici, s'il est détecté en A42 que l'identifiant IDX3 est contenu dans la liste LT2 présente dans la mémoire 34, la carte à puce CD en déduit que le terminal externe T3 présente un risque sécuritaire élevé et adapte son traitement de la transaction TR2 en conséquence afin de sécuriser la transaction TR2, de façon analogue à l'étape A24 représentée en **figure 5**. Selon un exemple particulier, s'il est déterminé lors de ladite consultation A42 que l'identifiant IDX3 du terminal T3 est inclus dans la liste LT2, le traitement (A43) de la transaction par la carte à puce CD comprend le déclenchement d'au moins une opération prédéfinie de

sécurisation de la transaction TR2, comme par exemple au moins l'une des opérations A26, A28 et A30 représentées en **figure 5**.

L'invention permet ici à la carte à puce CD de déterminer, sans l'aide du serveur distant SV3 de l'émetteur (hors ligne), si le terminal externe T3 est sensible en termes de sécurité et ainsi d'adapter le traitement de la transaction EMV comme déjà expliqué ci-avant.

Dans un exemple particulier, on suppose à présent que la carte à puce CD a déterminé, lors de la consultation A42, que l'identifiant iDX3 du terminal T3 n'est pas présent dans la liste LT2. Au cours d'une étape A44 d'envoi, la carte à puce CD envoie l'identifiant IDX3 à destination du serveur distant SV3. Le message MSG5, dans lequel se trouve l'identifiant IDX3 du terminal T3, est dans cet exemple un message de transaction EMV de type ARPC (pour « authorization response cryptogram ») indiquant la décision de la banque.

On notera que la carte à puce CD ne dispose pas ici de moyens lui permettant de déterminer sa localisation. Aussi, elle n'est pas en mesure de fournir une donnée de localisation DN comme cela été décrit ci-avant dans les étapes A2-A4 représentées en **figure 3**. Comme indiqué par la suite, c'est ici l'identifiant IDX3 du terminal T3 fourni par la carte à puce CD qui permet au serveur SV3 de déterminer une liste LT adaptée à la position de la carte à puce CD.

Le terminal T3, faisant ici l'interface entre la carte à puce CD et le serveur SV3, reçoit l'identifiant IDX3 en C44 et transmet celui-ci au serveur SV3 en C46.

Le serveur SV1 évalue (B48) ensuite, à partir de l'identifiant IDX3 du terminal T3 reçu, la localisation LOC de la carte à puce CD. Pour ce faire, le serveur SV3 utilise par exemple une table (non représentée) indiquant la zone géographique RG associé au terminal externe T3. Dans le présent exemple, on suppose que la banque émettrice de la carte à puce CD est capable de déterminer, à partir de l'identifiant IDX3, la position géographique du terminal T3, et donc de la carte à puce CD se trouvant à proximité.

En B50, le serveur SV3 consulte ensuite sa table TB illustrée en **figure 4a** et sélectionne, à partir de la localisation LOC de la carte à puce CD, la liste LT correspondante. Pour ce faire, le serveur SV3 détermine par exemple dans quelle zone géographique RG spécifiée dans la table TB se trouve le terminal T3 (et donc la carte à puce CD) et en déduit la liste LT associée. On suppose dans cet exemple que le serveur SV3 détermine, à partir de la localisation LOC de la carte à puce CD, que la carte à puce

CD se trouve à présent dans la zone géographique RG3 et, par conséquent, sélectionne (B50) la liste LT3 associée.

En B52, le serveur SV3 envoie alors à la carte à puce CD la liste LT3 sélectionnée en B50. Dans cet exemple, le message MSG6 dans lequel est envoyée la liste LT3 en B52, est une commande de script conforme au standard EMV, cette commande requérant la mise à jour de la carte à puce CD à partir de la liste LT3.

La carte à puce CD reçoit en A54 la commande MSG6 contenant la nouvelle liste LT3 d'au moins un identifiant de terminal.

En A56, la carte à puce CD enregistre la nouvelle liste LT3 dans sa mémoire 34. Dans cet exemple, la carte à puce CD supprime (A56) en outre l'ancienne liste LT2 qui était jusqu'ici stockée dans la mémoire 34.

A l'issue des procédés de contrôle représentés en **figure 8**, la carte à puce CD dispose ainsi dans sa mémoire d'une liste d'au moins un terminal (ou lecteur) présentant un risque sécuritaire particulier, cette liste étant adaptée à la localisation de ladite carte CD. De façon avantageuse, il est ainsi possible d'envoyer à la carte à puce CD une liste de taille limitée adaptée à la zone géographique dans laquelle se trouve la carte à puce CD, ce qui permet un gain en termes d'espace mémoire et de ressources utilisés au niveau de la carte à puce CD. En outre, l'invention permet de s'assurer que la carte à puce CD est capable de déterminer si les terminaux externes T2 situés à proximité présentent un risque particulier ou non.

Dans les modes de réalisation et variantes décrits dans cet exposé, la liste LT fourni au dispositif électronique par le serveur distant est une liste « noire » dans le sens où elle identifie le ou les terminaux externes présentant un risque sécuritaire particulier. En variante, on peut envisager d'autres mises en œuvre dans lesquelles la liste LT est une liste « blanche » dans le sens où elle identifie le ou les terminaux externes ne présentant pas de risque sécuritaire particulier. Selon d'autres variantes, la liste LT identifie à la fois des terminaux en tant que terminaux à risque, et d'autres terminaux en tant que terminaux de confiance.

Selon un mode de réalisation particulier, outre la première liste LT variant en fonction de la position du dispositif électronique, ce dernier peut contenir en mémoire une deuxième liste LT d'au moins un identifiant de terminal qui ne varie pas en fonction de la position du dispositif électronique. Cette deuxième liste LT est par exemple associée à une zone géographique où le porteur du dispositif électronique est susceptible de se trouver

fréquemment (à proximité de son domicile, d'un lieu privilégié de son choix etc.). Le dispositif électronique est alors configuré pour consulter les première et deuxième listes LT lors des étapes A22 et A42 précédemment décrites.

A noter par ailleurs que, dans les modes de réalisation et variantes décrites ci-avant, chaque identifiant IDT de terminal correspond à un unique terminal externe susceptible d'interagir avec le dispositif électronique de l'invention. En variante, un identifiant IDT contenu dans une liste LT peut correspondre à un groupe d'au moins deux terminaux (IDT identifie par exemple un type ou modèle de terminal). Un identifiant IDT peut par exemple correspondre au nom du marchant impliqué dans une transaction de paiement.

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 contrôle d'un dispositif électronique (T1 ; CD), ledit procédé comprenant, lors d'une transaction de paiement (TR1 ; TR2) en cours de traitement en coopération avec un terminal de paiement (T2 ; T3), les étapes suivantes :
   - réception (A20 ; A40), en provenance du terminal de paiement, d'un identifiant (IDX2 ; IDX3) dudit terminal de paiement ;
   - consultation (A22 ; A42) d'une première liste (LT) d'au moins un identifiant (ID) de terminal pour déterminer si l'identifiant dudit terminal de paiement (T2 ; T3) est inclus dans ladite première liste ; et
   - traitement (A24 ; A43) de la transaction de paiement en fonction du résultat de ladite consultation.

2. Procédé de contrôle selon la revendication 1, comprenant, préalablement à ladite étape (A22 ; A42) de consultation, l'enregistrement de la première liste d'au moins un identifiant de terminal dans une mémoire du dispositif électronique.

3. Procédé de contrôle selon la revendication 1 ou 2, ledit procédé comprenant, préalablement à ladite étape (A22 ; A42) de consultation :
   - envoi (A4 ; A44), à un serveur distant (SV1 ; SV3), d'une donnée (DN ; IDX3) permettant au serveur distant de déterminer la localisation (LOC) du dispositif électronique ; et
   - réception (A12 ; A54), en réponse audit envoi, de la première liste (LT2 ; LT3) d'au moins un identifiant (IDT) de terminal, ladite première liste étant fonction de ladite localisation du dispositif électronique.

4. Procédé de contrôle selon la revendication 3, dans lequel ladite donnée est une donnée de localisation (DN) représentative de la localisation du dispositif électronique.

5. Procédé de contrôle selon la revendication 4, ledit procédé comprenant, préalablement à son envoi (A4), la détermination de ladite donnée de localisation (DN) à partir d'au moins l'un parmi :
   - des coordonnées GPS représentatives de la localisation géographique du dispositif électronique ; et

- des données de réseau représentatives de la localisation du dispositif électronique dans un réseau de communication.

6. Procédé de contrôle selon l'une quelconque des revendications 1 à 5, dans lequel, s'il est déterminé lors de ladite consultation (A22 ; A42) que l'identifiant dudit terminal de paiement est inclus dans la première liste (LT2 ; LT3) d'au moins un identifiant de terminal, l'étape de traitement (A24 ; A43) de la transaction de paiement comprend le déclenchement d'au moins une opération prédéfinie de sécurisation de la transaction de paiement.

7. Procédé de contrôle selon la revendication 6, dans lequel ladite au moins une opération prédéfinie de sécurisation comprend au moins l'un quelconque parmi :

- envoi (A26) d'une requête demandant le traitement en ligne de la transaction de paiement en cours ;
- enregistrement (A38), dans un fichier d'historisation, d'une donnée d'historisation prédéfinie ; et
- configuration (A30) d'au moins un paramètre de fonctionnement du dispositif électronique.

8. Procédé de contrôle selon l'une quelconque des revendications 1 à 7, dans lequel la transaction de paiement (TR1 ; TR2) en cours est de type EMV et l'identifiant (IDX2 ; IDX3) du terminal de paiement (T2 ; T3) est reçu dans un message de transaction EMV de type GAC.

9. Procédé de contrôle selon la revendication 8, comprenant :

- réception (A12 ; A54), lors de la transaction de paiement en cours, d'une commande spécifiant une deuxième liste (LT) d'au moins un identifiant de terminal ; et
- en réponse à ladite commande, enregistrement (A14 ; A56) de ladite deuxième liste dans une mémoire du dispositif électronique en remplacement de ladite première liste.

10. Procédé d'envoi mis en œuvre par un serveur (SV1 ; SV3), comprenant les étapes suivantes :

- réception (B6 ; B46) d'une donnée (DN ; IDX3) en provenance d'un dispositif électronique (T1 ; CD) configuré pour coopérer avec un terminal de paiement (T2 ; T3) pour mettre en œuvre une transaction de paiement ;
- détermination (B8 ; B48) de la localisation du dispositif électronique à partir de ladite donnée ;
- sélection (B10 ; B50), à partir de la localisation du dispositif électronique, d'une liste (LT) d'au moins un identifiant (IDT) de terminal ; et
- envoi (B12 ; B52) de ladite liste à destination du dispositif électronique de sorte à configurer le traitement, par le dispositif électronique, d'une transaction de paiement.

11. Procédé d'envoi selon la revendication 10, dans lequel la donnée reçue est l'une parmi :

- une donnée de localisation (DN) représentative de la localisation du dispositif électronique ; et
- un identifiant (IDX3) d'un terminal de paiement avec lequel le dispositif électronique coopère pour traiter une transaction de paiement en cours.

12. Procédé d'envoi selon la revendication 10 ou 11, dans lequel le serveur envoie la liste (LT) d'au moins un identifiant de terminal au dispositif électronique dans un message de transaction EMV.

13. Programme d'ordinateur (PG1 ; PG2) comportant des instructions pour l'exécution des étapes d'un procédé selon l'une quelconque des revendications 1 à 12 lorsque ledit programme est exécuté par un ordinateur.

14. Dispositif électronique (T1 ; CD) comprenant, lors d'une transaction de paiement (T2 ; T3) en cours avec un terminal de paiement, les étapes suivantes :

- un module de réception (MD8) configuré pour recevoir, lors d'une transaction de paiement en cours avec un terminal de paiement, un identifiant dudit terminal de paiement ;
- un module de détermination (MD10) configuré pour consulter une première liste d'au moins un identifiant de terminal pour déterminer si l'identifiant dudit terminal de paiement est inclus dans ladite première liste ; et

- un module de traitement (MD12) configuré pour traiter la transaction de paiement en fonction du résultat de la consultation de la première liste par le module de consultation.

15. Serveur (SV3) comprenant :
- un module de réception (MD60) configuré pour recevoir une donnée en provenance d'un dispositif électronique, ledit dispositif étant configuré pour coopérer avec un terminal de paiement pour mettre en œuvre une transaction de paiement ;
- un module de détermination (MD62) configuré pour déterminer la localisation du dispositif électronique à partir de ladite donnée ;
- un module de sélection (MD64) configuré pour sélectionner, à partir de la localisation du dispositif électronique, une liste d'au moins un identifiant de terminal ; et
- un module d'envoi (MD66) configuré pour envoyer ladite liste à destination du dispositif électronique de sorte à configurer le traitement, par le dispositif électronique, d'une transaction de paiement.

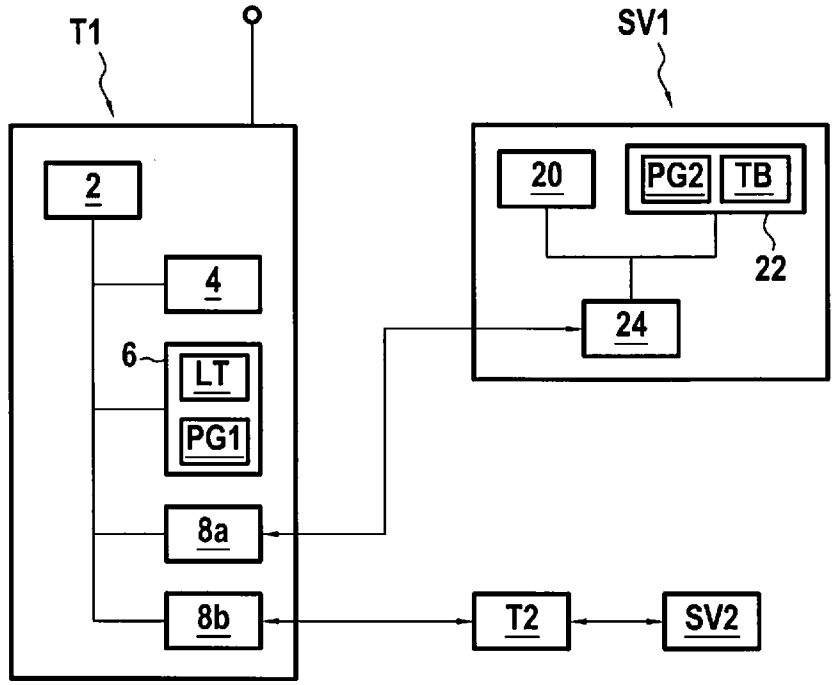
T1
SV1
2
20
PG2
TB
22
4
24
6
LT
PG1
8a
8b
T2
SV2

FIG.1

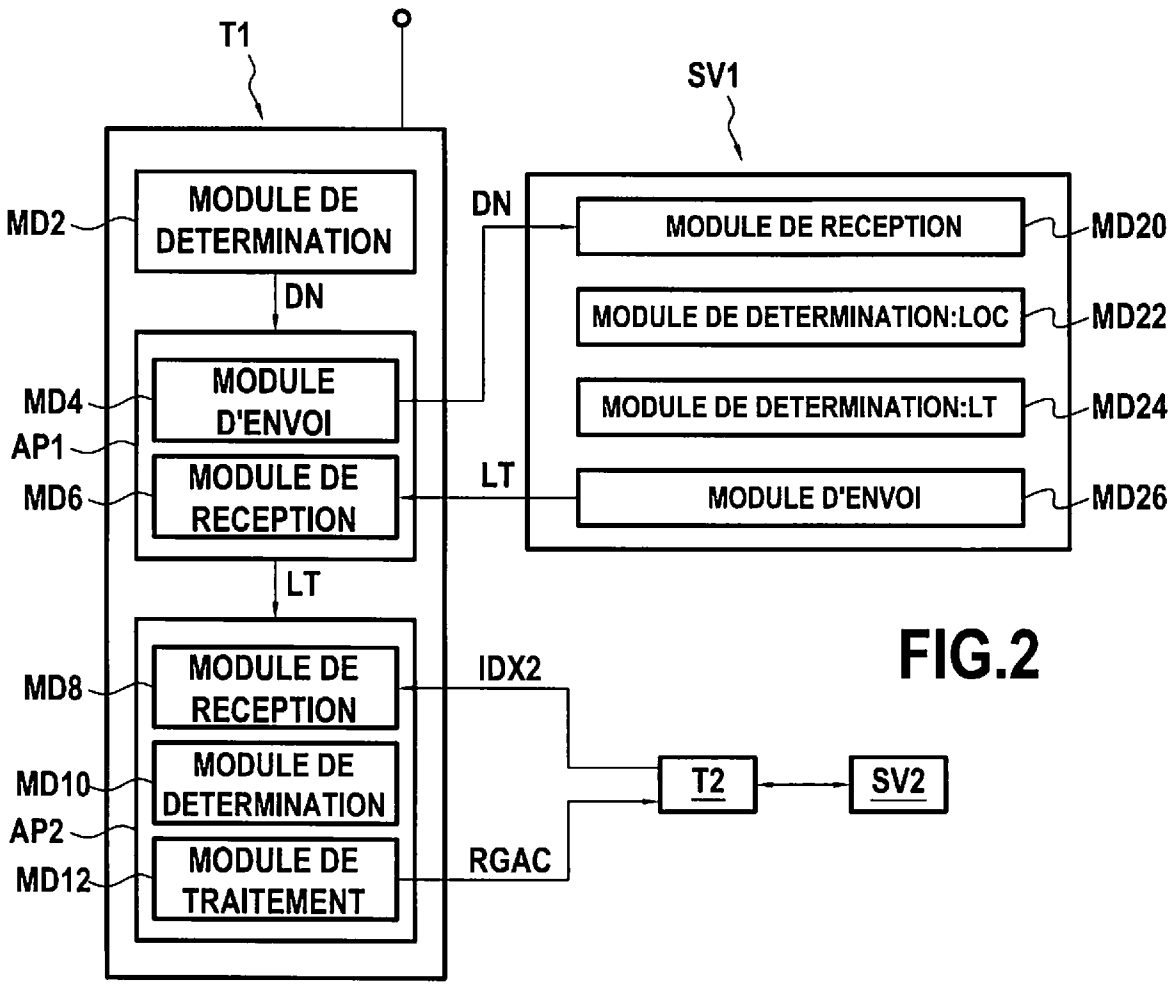
T1
SV1
MD2
MODULE DE DETERMINATION
DN
DN
MODULE DE RECEPTION
MD20
MODULE DE DETERMINATION:LOC
MD22
MD4
MODULE D'ENVOI
MODULE DE DETERMINATION:LT
MD24
AP1
MD6
MODULE DE RECEPTION
LT
LT
MODULE D'ENVOI
MD26
MD8
MODULE DE RECEPTION
IDX2
MD10
MODULE DE DETERMINATION
T2
SV2
AP2
MD12
MODULE DE TRAITEMENT
RGAC

FIG.2

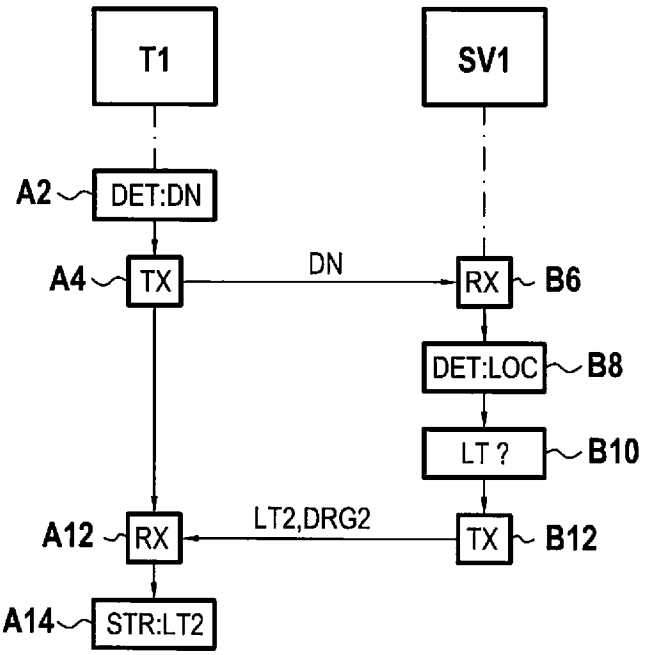

FIG.3

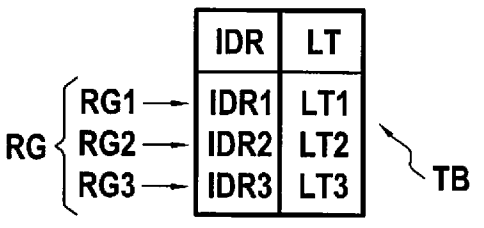

FIG.4a

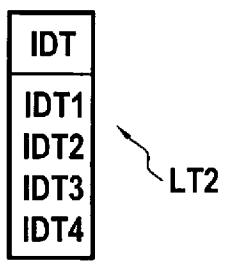

FIG.4b

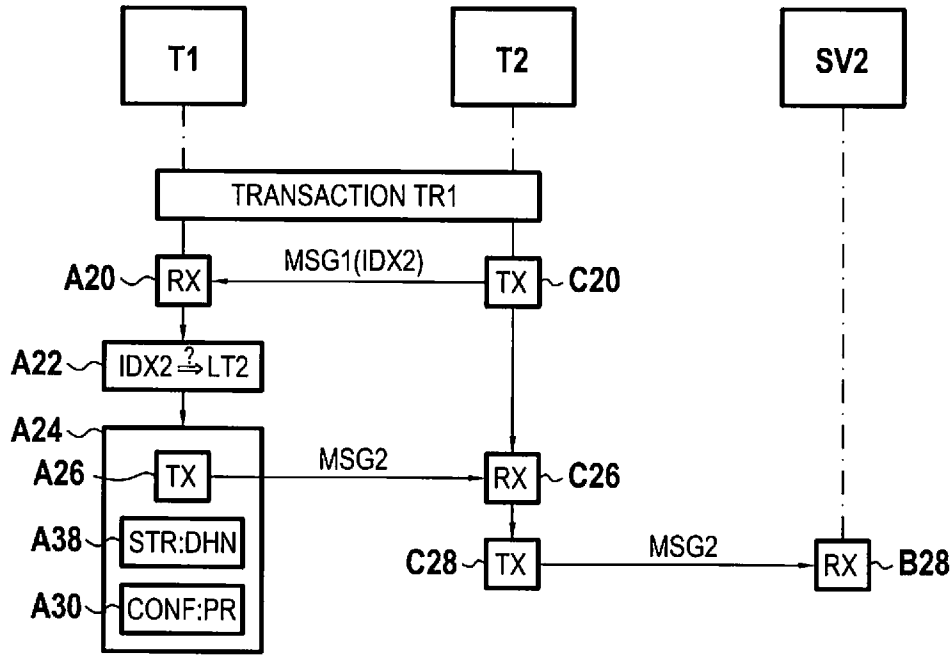
T1
T2
SV2
TRANSACTION TR1
A20
RX
MSG1(IDX2)
TX
C20
A22
IDX2 ? LT2
A24
A26
TX
MSG2
RX
C26
A38
STR:DHN
C28
TX
MSG2
RX
B28
A30
CONF:PR

FIG.5

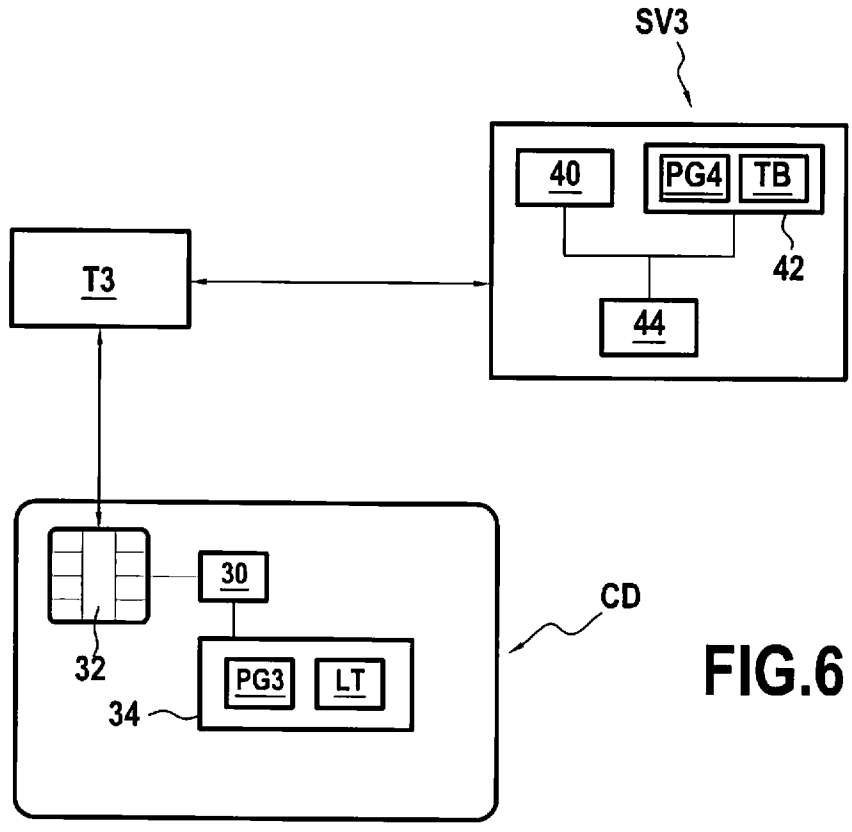
SV3
40
PG4
TB
42
T3
44
30
CD
32
PG3
LT
34

FIG.6

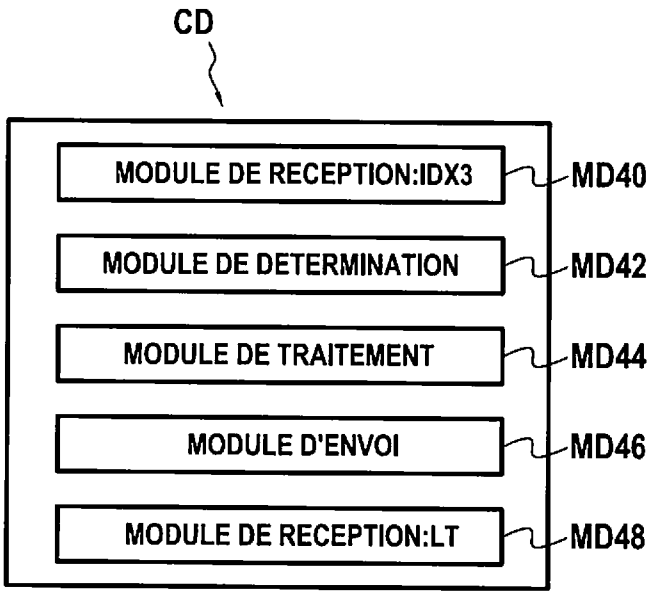
CD
MODULE DE RECEPTION:IDX3
MD40
MODULE DE DETERMINATION
MD42
MODULE DE TRAITEMENT
MD44
MODULE D'ENVOI
MD46
MODULE DE RECEPTION:LT
MD48

FIG.7a

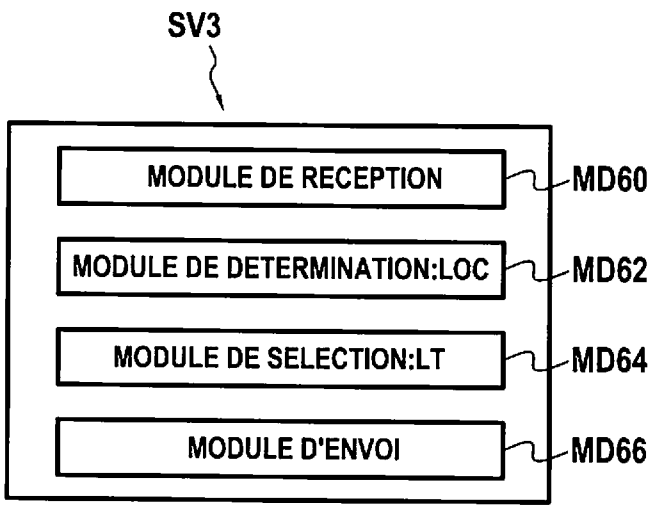
SV3
MODULE DE RECEPTION
MD60
MODULE DE DETERMINATION:LOC
MD62
MODULE DE SELECTION:LT
MD64
MODULE D'ENVOI
MD66

FIG.7b

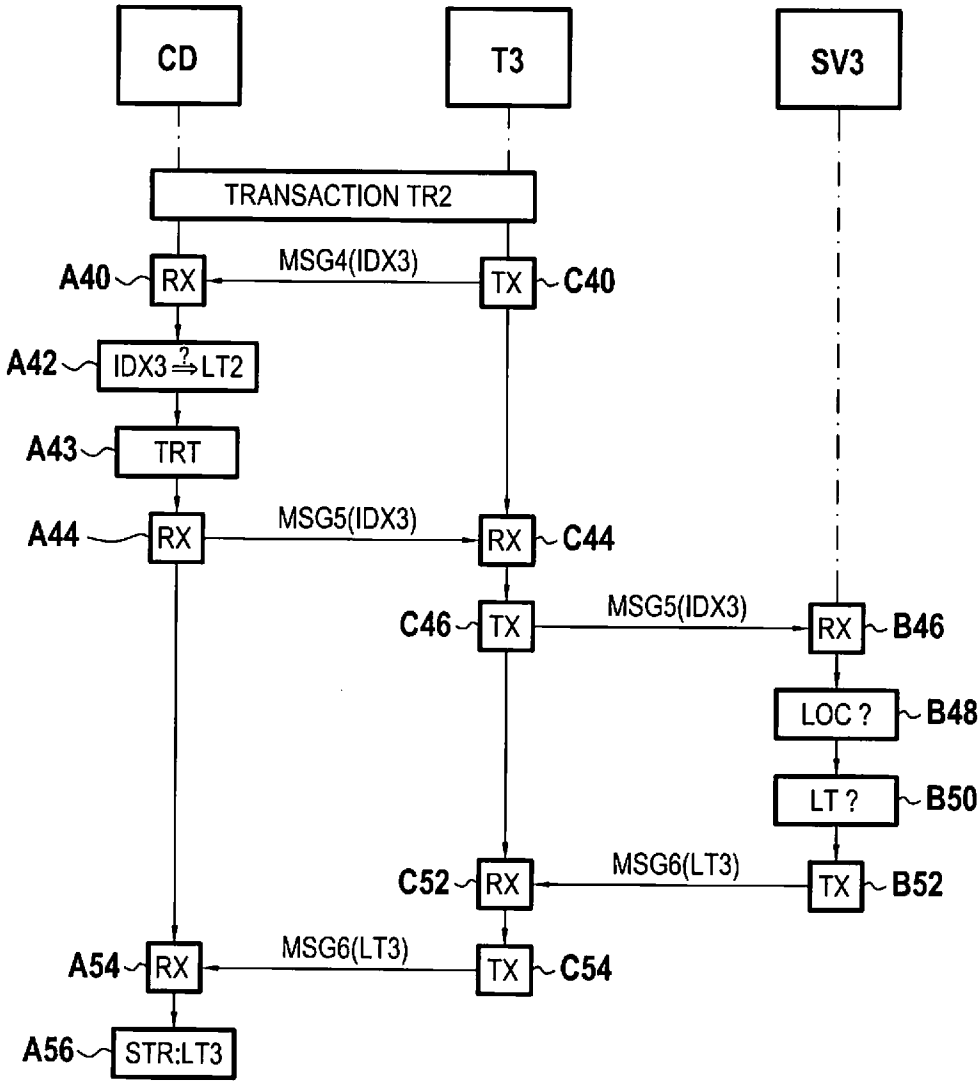
CD
T3
SV3
TRANSACTION TR2
A40
RX
MSG4(IDX3)
TX
C40
A42
IDX3 ? LT2
A43
TRT
A44
RX
MSG5(IDX3)
RX
C44
C46
TX
MSG5(IDX3)
RX
B46
LOC ?
B48
LT ?
B50
C52
RX
MSG6(LT3)
TX
B52
A54
RX
MSG6(LT3)
TX
C54
A56
STR:LT3

FIG.8

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/051897

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/32 G06Q20/40
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	MATEI CIOBANU MOROGAN ET AL: "Certificate Revocation System Based on Peer-to-Peer CRL Distribution", PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON DISTRIBUTEDMULTIMEDIA SYSTEMS, XX, XX , no. 9TH 1 January 2003 (2003-01-01), pages 587-592, XP002513671, Retrieved from the Internet: URL:http://citeseerx.ist.psu.edu/viewdoc/download	1-7, 10-15
Y	abstract; figures 1,2 3.1 Basic CRL Scheme; page 2 4. Techniques for Off-line verification of Revocation; page 3	8,9,12
	-/--	

[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
29 September 2017	13/10/2017

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	Bauer, Rodolphe

1

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

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	"4.1 Distribution points for Multiple CRLs"; page 3, right-hand column -----	
X	ABUGHAZALAH SARAH ET AL: "Secure Mobile Payment on NFC-Enabled Mobile Phones Formally Analysed Using CasperFDR", 2014 IEEE 13TH INTERNATIONAL CONFERENCE ON TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS, IEEE, 24 September 2014 (2014-09-24), pages 422-431, XP032724924, DOI: 10.1109/TRUSTCOM.2014.55	1-15
Y	abstract; figure 1; tables II, III page 422, right-hand column - page 424, right-hand column C. Protocol description, Authentication Phase, Payment Phase; page 425, right-hand column - page 428, left-hand column Mutual authentication between mobile & merchant; page 428, right-hand column Mutual authentication:...; page 430, left-hand column -----	8,9,12
A	WO 2006/136750 A2 (FRANCE TELECOM [FR]; LE ROUZIC JEAN-PIERRE [FR]; BARRE CHRISTIAN [FR];) 28 December 2006 (2006-12-28) abstract page 1, line 1 - page 2, line 31 page 3, line 30 - page 5, line 28 page 11, line 13ff page 8, line 5 - page 9, line 15 -----	1-15
A	BOND MIKE ET AL: "Chip and Skim: Cloning EMV Cards with the Pre-play Attack", 2014 IEEE SYMPOSIUM ON SECURITY AND PRIVACY, IEEE, 18 May 2014 (2014-05-18), pages 49-64, XP032686173, ISSN: 1081-6011, DOI: 10.1109/SP.2014.11 [retrieved on 2014-11-13] abstract; figures 2,6,7 IV The two variants of the pre-play attack; page 52 - page 53 B. Identifying vulnerable ATMs; page 53 - page 55 VI The deeper problem; pages 58-60 IX Conclusions; page 63 - page 64 ----- -/--	1-15

1

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/051897

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FR 2 958 770 A1 (OBERTHUR TECHNOLOGIES [FR]) 14 October 2011 (2011-10-14) abstract; figures 1,4 page 3, lines 23-31 page 5, lines 1-30 page 14, line 1 - page 19, line 17 -----	8,9,12

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2017/051897

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006136750 A2	28-12-2006	EP 1894342 A2	05-03-2008
		WO 2006136750 A2	28-12-2006
FR 2958770 A1	14-10-2011	FR 2958770 A1	14-10-2011
		US 2011251958 A1	13-10-2011

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2017/051897

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06Q20/32 G06Q20/40
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	MATEI CIOBANU MOROGAN ET AL: "Certificate Revocation System Based on Peer-to-Peer CRL Distribution", PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON DISTRIBUTEDMULTIMEDIA SYSTEMS, XX, XX , no. 9TH 1 janvier 2003 (2003-01-01), pages 587-592, XP002513671, Extrait de l'Internet: URL:http://citeseerx.ist.psu.edu/viewdoc/download	1-7, 10-15
Y	abrégé; figures 1,2 3.1 Basic CRL Scheme; page 2 4. Techniques for Off-line verification of Revocation; page 3	8,9,12

-/--

[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
29 septembre 2017	13/10/2017

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	Bauer, Rodolphe

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
	"4.1 Distribution points for Multiple CRLs"; page 3, colonne de droite -----	
X	ABUGHAZALAH SARAH ET AL: "Secure Mobile Payment on NFC-Enabled Mobile Phones Formally Analysed Using CasperFDR", 2014 IEEE 13TH INTERNATIONAL CONFERENCE ON TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS, IEEE, 24 septembre 2014 (2014-09-24), pages 422-431, XP032724924, DOI: 10.1109/TRUSTCOM.2014.55	1-15
Y	abrégé; figure 1; tableaux II, III page 422, colonne de droite - page 424, colonne de droite C. Protocol description, Authentication Phase, Payment Phase; page 425, colonne de droite - page 428, colonne de gauche Mutual authentication between mobile & merchant; page 428, colonne de droite Mutual authentication:...; page 430, colonne de gauche -----	8,9,12
A	WO 2006/136750 A2 (FRANCE TELECOM [FR]; LE ROUZIC JEAN-PIERRE [FR]; BARRE CHRISTIAN [FR];) 28 décembre 2006 (2006-12-28) abrégé page 1, ligne 1 - page 2, ligne 31 page 3, ligne 30 - page 5, ligne 28 page 11, ligne 13ff page 8, ligne 5 - page 9, ligne 15 -----	1-15
A	BOND MIKE ET AL: "Chip and Skim: Cloning EMV Cards with the Pre-play Attack", 2014 IEEE SYMPOSIUM ON SECURITY AND PRIVACY, IEEE, 18 mai 2014 (2014-05-18), pages 49-64, XP032686173, ISSN: 1081-6011, DOI: 10.1109/SP.2014.11 [extrait le 2014-11-13] abrégé; figures 2,6,7 IV The two variants of the pre-play attack; page 52 - page 53 B. Identifying vulnerable ATMs; page 53 - page 55 VI The deeper problem; pages 58-60 IX Conclusions; page 63 - page 64 ----- -/--	1-15

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
Y	FR 2 958 770 A1 (OBERTHUR TECHNOLOGIES [FR]) 14 octobre 2011 (2011-10-14) abrégé; figures 1,4 page 3, lignes 23-31 page 5, lignes 1-30 page 14, ligne 1 - page 19, ligne 17 -----	8,9,12

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2017/051897

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2006136750 A2	28-12-2006	EP 1894342 A2	05-03-2008
		WO 2006136750 A2	28-12-2006
FR 2958770 A1	14-10-2011	FR 2958770 A1	14-10-2011
		US 2011251958 A1	13-10-2011