



(51) Classification internationale des brevets :
G06F 21/52 (2013.01) *G06F 21/77* (2013.01)

(21) Numéro de la demande internationale :
PCT/FR2015/053630

(22) Date de dépôt international :
18 décembre 2015 (18.12.2015)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1462781 18 décembre 2014 (18.12.2014) FR

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

(72) Inventeurs : CHAMBEROT, Francis; c/o Oberthur Technologies, Département Propriété Intellectuelle, 420 rue d'Estienne d'Orves, 92700 Colombes (FR). VAURES, Pierre; c/o Oberthur Technologies, Département Propriété Intellectuelle, 420 rue d'Estienne d'Orves, 92700 Colombes (FR). VILAIN, Antoine; c/o Oberthur Technologies, Département Propriété Intellectuelle, 420 rue d'Estienne d'Orves, 92700 Colombes (FR).

(74) Mandataires : 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, 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, KN, KP, KR, 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.

(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))

(54) Title : METHOD OF DISPATCHING AN ITEM OF SECURITY INFORMATION AND ELECTRONIC DEVICE ABLE TO IMPLEMENT SUCH A METHOD

(54) Titre : PROCEDE D'ENVOI D'UNE INFORMATION DE SECURITE ET DISPOSITIF ELECTRONIQUE APTE A METTRE EN OEUVRE UN TEL PROCEDE

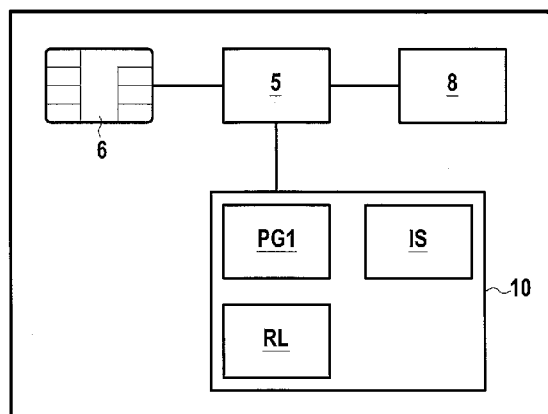


FIG.2

(57) Abstract : The invention relates to a method of dispatching an item of security information (IS) implemented by an electronic device (4), the method comprising the following steps: - detection of an event encountered by the electronic device (4); - recording, in a secure memory (10) of the device, of an item of security information (IS) representative of the event; - starting, following the recording, of a transaction with an external terminal; and - dispatching to the external terminal of the item of security information (IS) in a transaction message during said transaction. The invention furthermore relates to an electronic device able to implement such a method of dispatch.

(57) Abrégé : L'invention concerne un procédé d'envoi d'une information de sécurité (IS) mis en œuvre par un dispositif électronique (4), le procédé comprenant les étapes suivantes : - détection d'un événement rencontré par le dispositif électronique (4); - enregistrement, dans une mémoire sécurisée (10) du dispositif, d'une information de sécurité (IS) représentative de l'événement; - démarrage, suite à l'enregistrement, d'une transaction avec un terminal externe; et - envoi au terminal externe de l'information de sécurité (IS) dans un message de transaction lors de ladite transaction. L'invention concerne en outre un dispositif électronique apte à mettre en œuvre un tel procédé d'envoi.

Titre : Procédé d'envoi d'une information de sécurité et dispositif électronique apte à mettre en œuvre un tel procédé.

5

Arrière-plan de l'invention

La présente invention se situe dans le domaine général des dispositifs électroniques aptes à coopérer avec un terminal externe afin de réaliser une opération, telle qu'une transaction par exemple.

10

L'invention concerne en particulier la remontée d'informations utiles par de tels dispositifs électroniques vers le terminal externe afin de réaliser un traitement approprié.

L'invention s'applique plus particulièrement, mais de manière non exclusive, aux cartes à puce cartes (ou cartes à microcircuit), conformes par exemple à la norme ISO7816. L'invention vise notamment l'utilisation d'une carte à puce fonctionnant selon le

15

protocole EMV (pour « Europay Mastercard Visa ») pour remonter des informations de sécurité à un terminal externe (ou lecteur).

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 des transactions de paiement ou d'authentification du porteur, par exemple. Les cartes à puce pour applications bancaires (carte de crédit, carte de débit etc.), par exemple, sont aptes à communiquer avec des terminaux de paiement.

20

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

25

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.

30

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 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.

35

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.

Il a par exemple été développé des cartes à puce EMV aptes à détecter des attaques, de type optique ou autre, réalisées à leur rencontre par des personnes ou entités malveillantes. Sur détection d'une telle attaque, la carte à puce efface les données sensibles qu'elle contient en mémoire et se rend volontairement inopérante. Si un dialogue EMV est initié avec un lecteur, la carte répond à un message RESET (RST) par une réponse ATR (ANSWER TO RESET) modifiée indiquant que la transaction ne peut avoir lieu. Peu ou pas d'information est cependant inclus dans cette réponse ATR de sorte qu'il est difficile du côté lecteur de déterminer la cause de l'échec du dialogue.

Il n'existe pas aujourd'hui de mécanisme satisfaisant permettant de remonter efficacement des informations de sécurité depuis une carte à puce (ou plus généralement depuis un dispositif électronique) vers un lecteur afin de permettre une meilleure évaluation des risques de sécurité, d'identifier de possibles attaques rencontrées par la carte à puce ou encore de réaliser des traitements en fonction de certains comportements observés au niveau de la carte.

Les possibilités de suivi des comportements d'un porteur d'une carte à puce (ou équivalents) ou des opérations réalisées par cette carte sont aujourd'hui limitées et appelées à de nouveaux mécanismes de remonter d'information de la carte vers le lecteur, voire vers un tiers distant tel que l'émetteur de la carte à puce par exemple.

Il existe en particulier un besoin pour une solution permettant de remonter de tels informations sans modifier en profondeur les protocoles de communication actuels (de type EMV par exemple) mis en œuvre collectivement par les dispositifs électroniques et les lecteurs associés.

Objet et résumé de l'invention

A cet effet, la présente invention concerne un procédé d'envoi d'une information de sécurité mis en œuvre par un dispositif électronique, ledit procédé comprenant les étapes suivantes :

- détection d'un événement rencontré par le dispositif électronique ;
- enregistrement, dans une mémoire sécurisée du dispositif, d'une information de sécurité représentative dudit événement ;
- démarrage, suite audit enregistrement, d'une transaction avec un terminal externe ; et

- envoi au terminal externe de l'information de sécurité dans un message de transaction lors de ladite transaction.

Selon un mode de réalisation particulier, l'évènement détecté par le dispositif électronique comprend au moins l'un parmi :

- 5 - une anomalie rencontrée par le dispositif électronique ; et
- une attaque à l'encontre du dispositif électronique.

Selon un mode de réalisation particulier, l'évènement est détecté par le dispositif électronique à partir de la valeur courante d'un compteur.

- 10 Selon un mode de réalisation particulier, l'évènement est une anomalie ou attaque, ladite anomalie ou attaque étant détectée par le dispositif électronique en comparant la valeur courante du compteur avec une valeur seuil.

Selon un mode de réalisation particulier, le compteur représente au moins l'un parmi :

- un nombre consécutif d'essais manqués de saisie d'un code secret ; et
- 15 - un nombre total de transactions incomplètes réalisées par le dispositif électronique.

Selon un mode de réalisation particulier, l'information de sécurité comprend la valeur courante dudit compteur enregistré dans la mémoire sécurisée.

- 20 Selon un mode de réalisation particulier, le dispositif électronique détecte, en tant qu'évènement lors de ladite détection, un intervalle de temps entre :

- l'envoi d'une réponse, par ledit dispositif électronique, à une commande du terminal externe ; et
- la réception d'une commande subséquente du terminal externe.

- 25 Selon un mode de réalisation particulier, ledit dispositif électronique est configuré pour décider, à partir d'une comparaison entre ledit intervalle de temps et une valeur seuil prédéterminée, si une donnée représentative dudit intervalle de temps doit être enregistrée lors de l'étape d'enregistrement.

Selon un mode de réalisation particulier, ledit évènement satisfait au moins l'une des conditions suivantes :

- 30 - l'évènement cause une réinitialisation du dispositif électronique ; et
- l'évènement comprend l'exécution par le dispositif électronique d'une opération affectant un code confidentiel stocké dans une mémoire sécurisée du dispositif électronique.

- 35 Selon un mode de réalisation particulier, un comportement anormal du dispositif électronique ou une attaque à l'encontre dudit dispositif électronique est détecté si au moins une condition préenregistrée dans le dispositif électronique est satisfaite.

Selon un mode de réalisation particulier, la transaction et le message de transaction comportant l'information de sécurité sont conformes au protocole EMV.

5 Selon un mode de réalisation particulier, le procédé d'envoi comprend un envoi au terminal externe, dans un message AFL, d'une donnée de référencement permettant au terminal externe de lire l'information de sécurité dans la mémoire sécurisée du dispositif électronique ;

l'information de sécurité étant envoyée au terminal externe en réponse à une commande de lecture reçue du terminal externe suite à l'envoi du message AFL.

10 Selon un mode de réalisation particulier, le procédé d'envoi comprend l'envoi au terminal externe, dans un message ATR, d'une donnée de référencement lui permettant de lire l'information de sécurité dans la mémoire sécurisée du dispositif électronique.

Selon un mode de réalisation particulier, l'information de sécurité est envoyée au terminal externe en tant que donnée non interprétable par le terminal externe en réponse à un message GENERATE AC reçu du terminal externe.

15 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 (ou d'enregistrement), ce programme étant susceptible d'être mis en œuvre dans un dispositif électronique telle qu'une carte à puce ou un ordinateur, ce
20 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.

25 L'invention concerne également un procédé de traitement mise en œuvre par un terminal externe à un dispositif électronique, ledit procédé comprenant les étapes suivantes :

- démarrage d'une transaction avec le dispositif électronique ;
- réception, en provenance du dispositif électronique, d'un message de transaction
30 contenant une information de sécurité lors de la transaction, ladite information de sécurité étant représentative d'un évènement détecté par le dispositif électronique ; et
- traitement de l'information de sécurité.

Selon un mode de réalisation particulier, ledit traitement comprend au moins l'un
35 parmi :

- réalisation d'une analyse de risque associée à ladite transaction à partir de l'information de sécurité ; et
- envoi de l'information de sécurité à un serveur distant du terminal externe.

L'invention comprend corrélativement un dispositif électronique comprenant :

- 5 - un module de détection d'un évènement rencontrée par le dispositif électronique ;
- un module d'obtention d'une information de sécurité représentative dudit évènement ;
- un module d'enregistrement, dans une mémoire sécurisée du dispositif, de l'information de sécurité;
- 10 - un module d'exécution apte à démarrer, suite à l'enregistrement de l'information de sécurité, une transaction avec le terminal externe ; et
- un module d'envoi au terminal externe de l'information de sécurité dans un message de transaction lors de ladite transaction.

15 Les différents modes de réalisation et variantes définis ci-avant en référence au procédé d'envoi s'appliquent de manière analogue au dispositif électronique de l'invention.

 Selon un mode de réalisation particulier, le module d'exécution est apte à poursuivre jusqu'à son terme la transaction une fois l'information de sécurité envoyée au terminal externe.

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

 Selon un mode de réalisation particulier, le module de détection comprend au moins l'un parmi :

- 25 - un premier module de traitement apte à détecter ledit évènement à partir d'une commande reçue d'une l'entité externe par un module d'interface du dispositif électronique, ledit module d'interface permettant établir une communication entre le dispositif électronique et ladite entité électronique ; et
- un capteur apte à détecter une attaque survenant à l'encontre du dispositif électronique et un deuxième module de traitement apte à détecter ledit évènement à partir de l'attaque détectée.

30 L'invention concerne également un terminal externe à un dispositif électronique, ledit terminal comprenant :

- un module d'exécution apte à démarrer une transaction avec le dispositif électronique ;
- 35 - un module de réception apte à recevoir du dispositif électronique un message de transaction contenant une information de sécurité lors de la transaction, ladite

information de sécurité étant représentative d'un événement détecté par le dispositif électronique ; et

- un module de traitement de l'information de sécurité.

Selon un mode de réalisation particulier, ladite transaction et ledit message de transaction sont conformes au protocole EMV, le terminal comprenant :

un module d'extraction apte à extraire, d'un message ATR reçu du dispositif électronique lors de la transaction, une donnée de référencement permettant au terminal de lire l'information de sécurité dans une mémoire sécurisée du dispositif électronique.

A noter que les programme d'ordinateur mentionnés dans le présent exposé peuvent 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.

De plus, les supports d'enregistrement (ou d'information) mentionnés dans le présent exposé peuvent 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, les supports d'enregistrement peuvent correspondre à 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, les supports d'enregistrement peuvent correspondre à 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.

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 sous forme d'un organigramme un exemple de coopération entre une carte à puce et un terminal externe conformément au protocole EMV ;
- la figure 2 représente, de manière schématique, l'architecture matérielle d'une carte à puce conforme à une mise en œuvre particulière de l'invention ;

- la figure 3 représente schématiquement des modules mis en œuvre par la carte à puce de la figure 2 ;
- la figure 4 représente, de manière schématique, l'architecture matérielle d'un lecteur de carte conforme à une mise en œuvre particulière de l'invention, ce lecteur étant apte à coopérer avec la carte à puce représentée en figures 2 et 3 ;
- la figure 5 représente schématiquement des modules mis en œuvre par le lecteur de carte de la figure 4 ;
- la figure 6 représente, sous forme d'un organigramme, un procédé d'envoi réalisé par la carte à puce de la figure 2 conformément à une mise en œuvre particulière de l'invention ;
- la figure 7 représente, sous forme d'un organigramme, un procédé d'envoi et un procédé de traitement conformes à un premier mode de réalisation de l'invention ;
- la figure 8 représente, sous forme d'un organigramme, un procédé d'envoi et un procédé de traitement conformes à un deuxième mode de réalisation de l'invention ; et
- la figure 9 représente, sous forme d'un organigramme, un procédé d'envoi et un procédé de traitement conformes à un troisième mode de réalisation de l'invention.

Description détaillée de plusieurs modes de réalisation

Comme indiqué ci-avant, la présente invention se situe dans le domaine général des dispositifs électroniques aptes à coopérer avec un terminal externe (ou lecteur) afin de réaliser une opération telle qu'une transaction par exemple.

L'invention concerne en particulier la remontée d'informations de sécurité par de tels dispositifs électroniques vers le terminal externe afin de permettre une évaluation optimale de certains risques de sécurité, d'identifier de possibles attaques rencontrées par le dispositif électronique ou encore de réaliser des traitements en fonction de certains comportements observés au niveau du dispositif électronique.

La présente invention est décrite dans l'exposé qui suit dans le cadre d'une carte à puce (conforme par exemple à la norme ISO7816) de type EMV, cette carte étant apte à remonter des informations de sécurité à un lecteur externe lors d'une transaction EMV. On comprendra toutefois que d'autres types de protocole peuvent être envisagés dans le cadre de l'invention.

L'invention vise plus généralement un dispositif électronique destiné à coopérer avec un terminal externe (ou lecteur) pour réaliser une opération, typiquement une transaction (de paiement par exemple). Ce dispositif électronique est en particulier apte à fournir une information de sécurité au lecteur après avoir démarré une transaction avec celui-ci.

5 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. L'invention est décrite ici dans le cadre d'une carte de paiement destinée à réaliser des transactions bancaires. On comprendra que d'autres types de transactions ou opérations sont envisageables dans
10 le cadre de l'invention.

On notera également que, dans les exemples de réalisation qui suivent, la carte à puce coopère en mode contact avec le lecteur. L'invention s'applique toutefois également au cas où la carte à puce communique en mode sans contact avec le lecteur.

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

Afin de faciliter la compréhension de l'invention, on décrit à présent, en référence à la **figure 1**, un exemple d'une transaction de paiement conforme au protocole EMV, à l'aide
20 d'une carte à puce 1 coopérant avec un lecteur (ou terminal) externe 2. Le lecteur 2 est apte à communiquer avec un serveur bancaire 3 associé à l'émetteur de la carte à puce 1. Dans cet exemple, la carte à puce 1 est une carte de paiement et le lecteur 2 est un terminal de paiement.

25 Comme indiqué ci-après, la carte à puce 1 fonctionne ici en mode avec vérification du code secret bien que l'on puisse envisager des variantes selon lesquelles la carte à puce 1 ne procède pas à la vérification du code secret (mode sans vérification du code secret).

30 Une carte à puce EMV de paiement contient généralement différentes applications bancaires permettant par exemple de fonctionner en mode « carte de crédit » ou « carte de débit » dans un point de vente ou encore d'interagir avec un guichet automatique bancaire.

On suppose ici que le porteur insert la carte à puce 1 dans le lecteur 2.

35 Le protocole EMV comprend une phase préliminaire PHP destinée à préparer la carte à puce 1 et le lecteur 2 à la mise en œuvre à suivre de la transaction TR elle-même. Différents messages conformes au protocole EMV sont échangés entre la carte à puce 1, le lecteur 2 et (dans cet exemple) le serveur bancaire 3 au cours de la phase PHP puis de la transaction TR.

Plus précisément, lors de la phase préliminaire PHP, le lecteur 2 envoie (E2) tout d'abord un message RESET (RST) à la carte de paiement 1. La carte de paiement 1 répond (E4) à l'aide d'un message ANSWER TO RESET (ATR).

Une fois ce premier dialogue effectué, le lecteur 2 tente de choisir l'application appropriée sur la carte de paiement 1. Pour ce faire, le lecteur 2 envoie (E6) à la carte 1 une commande SELECT FILE afin de demander à la carte de paiement 1 les applications que cette dernière est capable d'exécuter. Cette commande SELECT FILE contient typiquement en paramètre l'identifiant d'application (AID pour « Application Identifier ») « 1PAY.SYS.DDF01 ». En réponse, la carte 1 fournit (E8) au lecteur 2 une liste des différentes applications qu'elle peut mettre en œuvre. Le porteur peut alors sélectionner via le lecteur 2 le mode de transaction souhaité, déclenchant ainsi l'envoi (E10) vers la carte 1 d'une commande SELECT APPLICATION avec en paramètre l'identifiant AID de l'application sélectionnée. A noter qu'il existe divers variantes pour sélectionner l'application appropriée dans la carte à puce 1.

Le lecteur 2 envoie (E10) en outre une commande GET PROCESSING OPTIONS (GPO) à la carte à puce 1 afin d'initier le début de la transaction. L'envoi de cette commande GPO marque le début de la transaction EMV.

Au cours de cette transaction TR, la carte de paiement 1 envoie (E14) au lecteur 2 une première série d'informations, telles que l'AIP (Application Interchange Profile) qui indique au lecteur 2 les différentes opérations à faire pour mener à bien une transaction. La carte 1 envoie (E16) également un message AFL (Application File Locator) qui indique la liste des données disponibles au niveau de l'application dans la carte 1 et que le lecteur 2 doit aller lire pour pouvoir réaliser la transaction TR. Le lecteur 2 lit (E18-E20) ainsi les informations spécifiées dans l'AFL. Pour ce faire, le lecteur 2 envoie (E18) une ou plusieurs commandes de lecture READ RECORD à la carte de paiement 1 et reçoit (E20) en retour les informations demandées (appelés RECORDS).

A noter que les étapes E14 et E16 peuvent être réalisées au cours de l'envoi d'un même message depuis la carte à puce 4.

Les informations lues (E18-E20) par le lecteur 2 dans la carte 1 comprennent par exemple la date d'expiration de la carte à puce 1, le numéro de compte associé, une signature numérique pour authentifier la carte 1, des paramètres de contrôle à utiliser par la suite pour réaliser la transaction, ou encore des listes d'objets dites listes CDOL (pour Card Data Object List).

Divers modes de réalisation sont envisageables. Dans cet exemple, le lecteur 2 réalise (E22) ensuite une étape d'analyse à partir des informations fournies (E20) par la carte de paiement 1. Si l'authentification associée à la carte de paiement 1 échoue, si une

anomalie est détectée ou encore si un risque trop important est détecté, le lecteur 2 peut refuser la transaction. On suppose ici que l'analyse E22 est passée avec succès.

Le protocole EMV se poursuit ici avec une phase d'authentification du porteur de la carte à puce 1 selon l'une des méthodes listées et supportées par ladite carte. Le lecteur
5 2 détermine le procédé d'authentification du porteur à appliquer en fonction des informations précédemment reçues dans les paramètres de contrôle. Cette phase permet en particulier au terminal de paiement de déterminer si la transaction est effectuée en mode avec vérification de code ou en mode sans vérification de code.

Dans cet exemple, où le mode avec vérification de code est mis en œuvre, le porteur
10 est invité à saisir son code PIN à l'aide du clavier dont est généralement muni le lecteur 2. Le lecteur 2 envoie (E24) alors à la carte de paiement 1 une requête VERIFY de vérification du code PIN saisi par le porteur. La carte de paiement 1 compare (E26) alors le code PIN saisi par le porteur avec le code PIN authentique inclus dans sa mémoire et en déduit si le porteur est authentique ou non.

15 Si le code PIN saisi est bon, la carte de paiement 1 envoie (E28) un message OK de type 0x9000 au terminal. Dans le cas contraire, la carte envoie (E28) un message de refus de type 0x63Cx au terminal, dans lequel x est le nombre de tentatives de code PIN restantes avant que la carte 1 bloque la transaction en cours (et les transactions à venir). On ne s'intéresse ici qu'au cas d'une vérification de code PIN hors ligne, c'est-à-dire sans
20 que le lecteur 2 fasse appel à l'émetteur de la carte dans le processus de vérification du code PIN, bien que cela soit également possible.

Une fois le porteur authentifié, le protocole EMV se poursuit avec une phase de vérification de la transaction. Plus précisément, le lecteur 2 génère puis envoie (E28) à la carte 1 une commande GAC (pour GENERATE AC). Cette commande contient différentes
25 données demandées préalablement par la carte de paiement 1 dans une liste CDOL reçue à l'étape E20 par le lecteur 2. Typiquement, la commande GAC contient des informations telles que le montant de la transaction en cours, la devise utilisée, le type de transaction, etc.

En réponse à la commande GAC, la carte 1 réalise (E32) une étape d'analyse
30 comprenant un certain nombre de vérifications de critères. Le nombre et la nature de ces vérifications ne sont pas normalisés par le protocole EMV et peuvent varier selon le cas.

A l'issue de l'analyse E32, la carte de paiement 1 répond au lecteur 2 en envoyant (E34) un cryptogramme (ou certificat cryptographique) qui comprend un code d'authentification de message (ou MAC pour Message Authentication Code), ce dernier
35 étant typiquement crypté à partir d'une clé cryptographique mémorisée dans la carte à

puce 1. La réponse de la carte dépend notamment du paramétrage de la carte 1 effectué par la banque émettrice.

Dans cet exemple, la carte à puce 1 envoie (E34) un cryptogramme ARQC (Autorisation Request Cryptogram) indiquant que la carte 1 souhaite poursuivre la transaction en ligne avec le serveur bancaire 3 de l'émetteur de la carte. La carte de paiement 1 peut en outre envoyer (E34) le cas échéant des informations IDD (pour Issuer Discretionary Data) au lecteur 2 en plus du cryptogramme.

Le lecteur 2 transmet (E36) ainsi le cryptogramme ARQC (et le cas échéant les informations IDD) au serveur bancaire 3 au niveau duquel est réalisé (E38) une nouvelle analyse à partir des informations reçues. Cette analyse E38 comprend typiquement un certain nombre de vérifications afin de s'assurer que la transaction est valide. Le lecteur 2 reçoit (E40) en réponse un message crypté ARPC indiquant la décision de l'émetteur. Le lecteur 2 transmet (E42) ce message ARPC à la carte de paiement 1 afin de lui indiquer la décision prise par l'émetteur.

Si la carte 1 accepte la transaction, celle-ci envoie (E44) en réponse un cryptogramme de type TC (transaction acceptée) au lecteur 2. Dans le cas contraire, la carte 1 envoie (E44) un cryptogramme de type AAC indiquant le refus de la transaction.

Chacun des messages ci-dessus échangés selon le protocole EMV pendant la transaction TR, en particulier entre la carte à puce 1 et le lecteur 2, constitue des exemples de messages de transaction au sens de l'invention.

Il convient de rappeler ici que le déroulement du protocole EMV décrit ci-dessus en référence à la **figure 1** ne constitue qu'un exemple non limitatif. Le protocole EMV offre en effet de nombreuses alternatives. Il incombe aux intégrateurs de faire les choix nécessaires pour adapter l'exécution du protocole selon les besoins (méthode d'authentification du porteur, transaction en ligne ou hors ligne etc.).

La **figure 2** représente, de manière schématique, l'architecture matérielle d'une carte à puce 4 conforme à un mode de réalisation particulier de l'invention. La carte 4 est dans cet exemple une carte EMV conforme à la norme ISO 7816.

Plus particulièrement, la carte à puce 4 comprend ici un microprocesseur 5 couplé à des contacts externes 6 (ports d'entrées/sorties), une mémoire volatile réinscriptible (de type RAM) 8 et une mémoire non volatile réinscriptible 10 (de type Flash par exemple). La carte 4 peut également comprendre une mémoire morte (de type ROM) non représentée ici.

On considère ici que la mémoire 10 est sécurisée, en faisant appel à un mécanisme de sécurité classique bien connu de l'homme du métier et qui ne sera donc pas décrit ici.

La mémoire 10 constitue ici un support d'enregistrement (ou d'information) conforme à un mode de réalisation de l'invention, lisible par la carte à puce 4, et sur lequel est enregistré un programme d'ordinateur PG1 conforme à un mode de réalisation de l'invention. Le programme PG1 comporte des instructions pour l'exécution des étapes d'un
5 procédé d'envoi d'une information de sécurité IS pouvant également être stockée dans la mémoire 10, conformément à un mode de réalisation de l'invention. Des exemples de réalisation de ce procédé sont représentés sur les **figures 6 à 9** décrites ultérieurement.

Dans l'exemple considéré ici, la mémoire 10 de la carte à puce 4 comporte en outre au moins une règle prédéfinie RL qui sera décrite ultérieurement.

10 Les contacts externes 6 constituent ici un module d'interface permettant à la carte à puce 4 (et plus particulièrement au microprocesseur 5) d'établir une communication, par contact dans cet exemple, avec une entité externe telle que le terminal 30 décrit ci-après en référence à la **figure 4**. On comprendra que d'autres types de module d'interface peuvent toutefois être envisagés comme un module d'interface permettant d'établir une
15 communication sans contact (comportant une antenne radiofréquence par exemple) entre la carte à puce et un terminal externe.

Dans un exemple particulier, la carte à puce 4 comporte au moins un capteur (non représenté sur les figures) apte à détecter une attaque survenant à l'encontre du dispositif électronique. Ce capteur peut être par exemple un capteur optique et/ou
20 électromagnétique. Ce capteur permet par exemple de détecter une attaque de type optique (attaque par laser par exemple) et/ou électromagnétique.

La **figure 3** représente schématiquement des modules pouvant être mis en œuvre par le microprocesseur 5 exécutant le programme PG1, à savoir : un module de détection 14 d'un évènement EVT, un module d'obtention 16 d'une information de sécurité IS, un
25 module d'enregistrement 18 d'une telle information de sécurité, un module d'exécution 20 permettant notamment le démarrage d'une transaction EMV et un module 22 apte à envoyer l'information de sécurité IS lors d'une transaction EMV.

Dans un exemple particulier, le module de détection 14 comprend au moins l'un parmi :

- 30
- un premier module de traitement (non représenté) apte à détecter l'évènement EVT à partir d'une commande (de type APDU par exemple) reçue d'une entité externe (telle que le terminal 30 représenté en **figure 4**) par le module d'interface 6 de la carte à puce 4 ; et
 - un capteur (non représenté) apte à détecter une attaque survenant à l'encontre
35 de la carte à puce 4, et un deuxième module de traitement (non représenté) apte à détecter l'évènement EVT à partir de l'attaque détectée.

La commande (de type APDU ou autre) est par exemple reçue par la carte à puce 4 lors d'une transaction donnée (de type EMV par exemple) avec un terminal externe, cette commande étant reçue du terminal externe via les contacts externes 6.

Par ailleurs, comme déjà expliqué, le capteur mentionné ci-avant peut par exemple
5 être un capteur optique et/ électromagnétique apte à détecter une attaque optique et/ou magnétique rencontrée par la carte à puce 4, cette attaque étant par exemple perpétrée par une personne ou un dispositif malveillant.

La **figure 4** représente, de manière schématique, l'architecture matérielle d'un terminal externe 30 (ici un lecteur de carte) selon un mode de réalisation particulier de
10 l'invention. Ce lecteur de carte 30 est ici apte à coopérer selon le protocole EMV avec la carte à puce 4.

Plus particulièrement, le lecteur de carte 30 comprend un microprocesseur 32, une mémoire morte (de type ROM) 34, une mémoire non volatile réinscriptible 36, une interface homme/machine 38 permettant à un utilisateur d'interagir avec le lecteur 30, un
15 connecteur 40 compatible avec les contacts externes de la carte à puce 4, et une interface de communication 42 permettant au lecteur 30 de communiquer avec une entité externe telle que le serveur distant 45 dans le cas d'espèce. Le serveur distant 45 est ici associé à l'émetteur (typiquement une banque) de la carte à puce 4.

La mémoire 36 constitue dans cet exemple un support d'informations conforme à un
20 mode de réalisation de l'invention, lisible par le lecteur 30, et sur lequel est enregistré un programme d'ordinateur PG2 conforme à un mode de réalisation de l'invention. Ce programme PG2 comporte des instructions pour l'exécution des étapes d'un procédé de traitement selon un mode de réalisation de l'invention. Des exemples de réalisation de ce procédé sont représentés ci-après en référence aux **figures 7 à 9**.

La **figure 5** représente schématiquement des modules pouvant être mis en œuvre
25 par le microprocesseur 32 du lecteur 30 exécutant le programme PG2, à savoir : un module d'exécution 48 permettant de démarrer une transaction TR avec la carte à puce 4 (envoi d'un message GPO), un module de réception 50 apte à recevoir une information de sécurité IS contenue dans un message de transaction provenant de la carte à puce 4, un
30 module de traitement 52 apte à réaliser un traitement à partir de l'information de sécurité IS reçue et, éventuellement, un module d'extraction 54 apte à extraire une donnée de référence DRF d'un message reçu de la carte à puce 4 comme décrit plus en détail ultérieurement.

Une mise en œuvre particulière de l'invention est à présent décrite en référence à la
35 **figure 6**. Plus précisément, la carte à puce 4 met en œuvre un procédé d'envoi en exécutant le programme PG1.

La carte à puce 4 détecte (S2) en premier lieu un évènement EVT. Cet évènement est par exemple représentatif d'une anomalie rencontrée par la carte à puce 4 ou d'une attaque à l'encontre de la carte à puce 4.

5 Dans l'exemple décrit ici, la détection S2 de l'évènement EVT est réalisée par le module de détection 14 illustré en **figure 3**.

Dans un cas particulier, l'évènement EVT satisfait au moins l'une des conditions suivantes :

- l'évènement EVT cause une réinitialisation de la carte à puce 4 ; et
- l'évènement EVT comprend l'exécution par la carte à puce 4 d'une commande ou
10 d'une opération affectant un code PIN (code secret) stocké dans une mémoire sécurisée de la carte à puce 4. Les commandes CHANGE PIN ou UNBLOCK PIN sont des exemples d'une telle commande.

15 Plus généralement, l'évènement EVT détecté (S2) par la carte à puce 4 peut être un quelconque évènement rencontré par la carte à puce 4 et que celle-ci juge digne d'intérêt, ce jugement étant éventuellement réalisé à partir d'au moins une condition préenregistrée dans une règle RL.

L'évènement EVT ainsi détecté par la carte à puce 4 peut correspondre à un ou à une pluralité d'évènements.

20 La détection de l'évènement EVT intervient par exemple lors d'une interaction avec un lecteur ou un terminal externe (lors d'une transaction par exemple). Dans un exemple particulier, une commande (de type APDU par exemple) d'un terminal externe est reçue par la carte à puce 4 via les contacts externes 6. Le module de détection 14 (ou plus particulièrement, un premier module de traitement compris dans le module de détection 14) détecte alors l'évènement EVT à partir de la commande reçue ou, éventuellement, à
25 partir d'un traitement réalisé par le premier module de traitement à partir de ladite commande.

Alternativement, l'évènement EVT peut être une attaque (de type optique et/ou électromagnétique) à l'encontre de la carte à puce 4, cette attaque étant détectée par le module de détection 14, ce dernier utilisant en particulier un capteur apte à détecter
30 l'attaque et un deuxième module de traitement apte à détecter l'évènement EVT à partir de l'attaque détectée. Dans ce cas, l'attaque n'est donc pas détectée en utilisant les contacts externes 6 (ou tout autre module d'interface de la carte à puce apte à communiquer avec un terminal externe) mais grâce à un capteur approprié de la carte à puce 4, comme déjà expliqué ci-avant.

35 Sur détection de l'évènement EVT, la carte à puce 4 obtient (S4) une information de sécurité IS représentative de cet évènement. Pour ce faire, la carte à puce 4 applique par

exemple une règle RL contenue en mémoire 10, cette règle spécifiant pour au moins un évènement donné une information IS à générer.

Dans l'exemple décrit ici, l'obtention S4 de l'information de sécurité IS est réalisée par le module d'obtention 16 illustré en **figure 3**.

5 La carte à puce 4 enregistre (S6) ensuite cette information de sécurité IS en mémoire 10. La carte à puce 4 crée par exemple un fichier (appelé ici fichier LOG) comprenant chaque information de sécurité IS obtenue.

Dans l'exemple décrit ici, l'enregistrement S6 est réalisé par le module d'enregistrement 18 illustré en **figure 3**.

10 On suppose que, après l'enregistrement S6, une transaction de type EMV est démarrée (S8) entre la carte à puce 4 et le lecteur externe 30. Ceci intervient typiquement lorsque la carte 4 est introduite par l'utilisateur dans le lecteur 30 en vue de réaliser une opération bancaire (consultation de compte, paiement, transfert...).

15 Comme déjà indiqué, le protocole EMV est ici mis en œuvre. Par conséquent, la carte à puce 4 et le lecteur 30 réalisent ensemble la phase préliminaire PHP (échange des messages RST et ATR etc.) déjà décrite en référence à la **figure 1**. Comme déjà indiqué, la réception par la carte à puce 4 du message GPO provenant du lecteur 30 marque ensuite le début S8 de la transaction EMV.

20 Dans l'exemple décrit ici, c'est le module d'exécution 20 illustré en **figure 3** qui réalise la phase préliminaire PHP et qui procède au début S8 de la transaction TR (réception du GPO) avec le lecteur externe 30.

25 Conformément à l'invention, la carte à puce 4 envoie (S10) au lecteur 30 l'information de sécurité IS dans un message de transaction lors de la transaction TR. Divers messages de transaction EMV peuvent être utilisés pour transporter l'information de sécurité IS jusqu'au lecteur 30, comme expliqué plus en détail en référence aux **figures 7 à 9**.

Dans l'exemple décrit ici, l'envoi S10 de l'information de sécurité IS est réalisée par le module d'envoi 22 illustré en **figure 3**.

30 Dans une mise en œuvre particulière, la carte à puce 4 prend la décision d'envoyer ou non (S10) au lecteur 30, pendant la transaction, une information de sécurité IS stockée en mémoire dans la carte 4, cette décision étant prise en appliquant une règle RL prédéfinie (stockée en mémoire 10) définissant au moins une condition préenregistrée. La carte à puce 4 décide d'envoyer une information de sécurité IS seulement si une condition préenregistrée associée à l'information IS est satisfaite.

35 Dans un exemple particulier, la carte à puce 4 n'est pas capable de poursuivre la transaction TR avec le lecteur 30 une fois l'envoi S10 de l'information de sécurité IS effectué, en raison par exemple d'une attaque ou d'une anomalie rencontrée par la carte.

Selon une variante, la carte à puce est apte à poursuivre la transaction TR normalement selon le protocole EMV une fois l'information de sécurité IS envoyée (S10) au lecteur 30.

Comme déjà indiqué, la nature de l'évènement EVT détecté en S2 par la carte à puce 4 peut varier selon le cas. Il en va de même pour l'information de sécurité IS pouvant être
5 remontée au terminal 30.

Selon un exemple particulier, l'évènement EVT est détecté (S2) par la carte à puce 4 à partir de la valeur courante d'un compteur enregistrée dans la carte à puce 4. Ce compteur représente par exemple un nombre consécutif d'essais manqués de saisie d'un code secret. Ce code secret peut être un code PIN à saisir par l'utilisateur sur le lecteur de
10 carte 30 coopérant avec la carte à puce 4 afin d'authentifier l'utilisateur lors d'une transaction. La carte à puce 4 est par exemple configurée pour détecter une anomalie (en tant qu'évènement EVT) en comparant la valeur courante de ce compteur d'essais manqués de saisie d'un code secret avec une valeur seuil. Par exemple, si la valeur courante atteint une valeur seuil prédéfinie, la carte à puce 4 le détecte en tant
15 qu'évènement EVT. Dans un exemple particulier, la carte à puce 4 est configurée pour enregistrer la valeur courante dudit compteur.

Selon un exemple particulier, l'évènement EVT est une erreur de transaction détectée par la carte à puce 4 lors d'une transaction. La carte à puce 4 est par exemple apte à détecter une erreur de transaction à partir d'au moins une information de transaction
20 reçue et enregistrée dans la carte à puce 4 lors d'une transaction (de type EMV par exemple). La carte à puce 4 est par exemple configuré pour remonter en S10 l'information de transaction au terminal 30.

Selon un exemple particulier, la carte à puce 4 détecte en tant qu'évènement EVT le fait qu'un compteur enregistré dans la carte à puce 4 dépasse une valeur seuil
25 prédéterminée. Le compteur représente par exemple un nombre total de transactions incomplètes réalisées par la carte à puce 4. L'information de sécurité IS envoyée en S10 par la carte à puce 4 au terminal 30 peut comprendre ledit compteur du nombre total de transactions incomplètes. Dans un exemple particulier, le compteur comprend une pluralité de composantes, le compteur pouvant indiquer un type d'attaque mise en œuvre
30 contre la carte à puce, ou encore quel type de défaillance présente la carte à puce.

Selon un exemple particulier, la carte à puce détecte, en tant qu'évènement EVT, un intervalle de temps entre (1) l'envoi d'une réponse, par la carte à puce 4, à une commande du terminal externe 30 ; et (2) la réception d'une commande subséquente du terminal externe 30. La carte à puce 4 est alors configurée pour enregistrer puis envoyer,
35 en tant qu'information de sécurité IS, une donnée représentative dudit l'intervalle de temps, lors des étapes S6 et S10 respectivement. Dans un exemple particulier, la carte à

puce 4 décide si elle doit enregistrer à l'étape S6 une donnée représentative d'un tel intervalle de temps, à partir d'une comparaison entre ledit intervalle de temps détecté et une valeur seuil prédéterminée.

Comme déjà décrit, divers types d'information de sécurité IS peuvent être envisagés dans le cadre de l'invention.

Dans un exemple particulier, l'information de sécurité IS comprend une donnée représentant la valeur courante d'un compteur enregistrée dans la carte à puce 4. Ce compteur peut comprendre au moins l'un des compteurs décrits ci-avant. En particulier, le compteur représente par exemple au moins l'un parmi :

- un nombre consécutif d'essais manqués de saisie d'un code secret ; et
- un nombre total de transactions incomplètes réalisées par la carte à puce 4 .

Dans un exemple particulier, l'information de sécurité IS comprend ladite valeur courante elle-même ou encore un paramètre indiquant que la valeur courante du compteur a atteint une valeur seuil prédéfinie.

Selon un exemple particulier, la donnée de sécurité IS est représentative d'une erreur de transaction détectée et enregistrée par la carte à puce 4 lors d'une transaction.

La remontée de l'information de sécurité IS lors d'une transaction permet d'informer le lecteur 30, et éventuellement le serveur bancaire 45, de l'occurrence d'un événement relatif par exemple à une attaque survenue à l'encontre de la carte à puce 4, à un risque de sécurité associé à la carte à puce 4 et/ou à son porteur, ou encore à un comportement observé antérieurement au niveau de la carte à puce 4.

A partir de l'information de sécurité IS reçue, le lecteur 30 est capable de réaliser un traitement particulier comme par exemple évaluer un risque lié à la transaction en cours ou transmettre l'information de sécurité IS au serveur distant 45.

Plusieurs modes de réalisation du procédé d'envoi mis en œuvre par la carte à puce 4 et du procédé de traitement mis en œuvre par le lecteur 30 sont à présent décrits en référence aux **figures 7 à 9**.

On suppose dans les modes de réalisation illustrés en **figures 7 à 9** que la carte à puce 4 a déjà réalisé les étapes S2 à S8 lorsqu'elle reçoit (E2) un message RST du lecteur 30. Comme indiqué par la suite, on peut toutefois envisager des variantes selon lesquelles au moins l'une des étapes S2 à S6 est réalisée par la carte à puce 4 après la réception par cette dernière du message RST, voire même après le début de la transaction S8.

Selon un premier mode de réalisation illustré en **figure 7**, la carte à puce 4 et le lecteur 30 coopère selon le protocole EMV.

Le déroulement du protocole EMV diffère ici de l'exemple décrit en **figure 1** en ce que le message RST envoyé par la carte à puce 4 est utilisé pour permettre au lecteur 30 de lire l'information de sécurité IS dans la mémoire de la carte à puce 4 lors de la transaction TR.

5 Dans cet exemple, le lecteur reçoit (E2) un message RST du lecteur 30. En réponse, la carte à puce 4 envoie (E4a) un message ATR modifié, ce message contenant une donnée de référence DRF permettant au lecteur 30 de lire l'information de sécurité IS dans la mémoire sécurisée 10 de la carte à puce 4.

10 Au cours d'une étape E5, le lecteur 30 extrait la donnée de référence DRF du message ATR.

Les étapes E6 à E16 sont réalisées comme déjà décrites en référence à la **figure 1**.

En réponse au message EFL envoyé (E16) par la carte à puce 4, le lecteur 30 réalise la lecture (E18-E20a) dans la mémoire de la carte à puce 4 des informations spécifiées dans le message AFL. Dans ce premier mode de réalisation, le lecteur 30 lit en outre
15 l'information de sécurité IS stockée dans la mémoire 10 de la carte à puce 4 en utilisant la donnée de référence DRF. Cette donnée DRF renseigne par exemple sur une adresse mémoire où est stockée l'information de sécurité IS.

Le lecteur 30 réalise ensuite un traitement approprié à partir de l'information de sécurité IS reçue.

20 Dans cet exemple, les étapes E24 à E34 sont réalisées comme déjà décrites en référence à la **figure 1**. Le lecteur 30 transmet (E36a) ensuite, au serveur distant 45, le message ARQC (préalablement reçu de la carte à puce 4 à l'étape E34) ainsi que l'information de sécurité IS.

25 Le serveur distant 45 (ou un autre terminal associé) réalise (E38) ensuite une analyse à partir des informations reçues, y compris si nécessaire l'information de sécurité IS.

Le lecteur 30 peut également réaliser (E38a) une analyse à partir de l'information de sécurité IS. Suite à cette analyse, le lecteur peut si besoin adapter le traitement de la transaction TR en cours, afin par exemple de rejeter la transaction ou de mettre en œuvre des mécanismes de sécurité supplémentaires.

30 Les étapes E40 à E44 sont réalisées comme déjà décrites en référence à la **figure 1**.

Selon une variante de ce premier mode de réalisation, la carte à puce 30 transmet la donnée de référence DRF non pas dans le message ATR (E4) mais dans le message APPLICATIONS en E8.

35 On notera que, dans ce premier mode de réalisation, le lecteur 30 est modifié afin d'être capable de reconnaître la donnée de référence DRF incluses dans le message ATR

(ou APPLICATIONS) en tant que telle, et de l'utiliser afin de récupérer l'information de sécurité IS de la carte à puce 4.

Selon un deuxième mode de réalisation illustré en **figure 8**, la carte à puce 4 et le lecteur 30 coopère également selon le protocole EMV.

5 Le déroulement du protocole EMV diffère ici du premier mode de réalisation décrit en référence à la **figure 7** en ce que la carte à puce 4 transmet (E16a) la donnée de référence DRF directement dans le message de transaction AFL.

10 Le lecteur 30 lit ensuite dans la carte à puce 4 les informations nécessaires, à savoir celles spécifiées dans l'AFL. Pour ce faire, le lecteur 30 envoie (E18b) une ou plusieurs commandes en lecture à la carte à puce 4 à laquelle celle-ci répond en fournissant (E20b) au lecteur 30 les informations demandées. Le lecteur 30 lit en particulier l'information de sécurité IS stockée dans la mémoire 10 de la carte à puce 4 à l'aide de la donnée de référence DRF.

15 Le lecteur 30 transmet (E36b) l'information de sécurité IS au serveur distant 45 et/ou réalise (E38b) une analyse à partir de l'information de sécurité IS de façon analogue aux étapes respectives E36a et E38a précédemment décrites.

Selon un troisième mode de réalisation illustré en **figure 9**, la carte à puce 4 et le lecteur 30 coopère également selon le protocole EMV.

20 Le déroulement du protocole EMV diffère ici des premier et deuxième modes de réalisation décrit en référence aux **figures 7 et 8** en ce que la carte à puce 4 transmet (E34c) au lecteur 30, après l'analyse E32, l'information de sécurité IS en tant que IDD (Issuer Discretionary Data). Cette donnée IDD (comme toutes données IDD) n'est pas interprétable par le lecteur 30 qui se contente de la transmettre (E36c) au serveur distant 45.

25 Ce troisième mode de réalisation met à profit la possibilité offerte par le protocole EMV de fournir des informations en tant que IDD au lecteur puis au serveur distant.

Une analyse peut ensuite être réalisée au niveau du serveur distant 45 à partir des informations reçues, y compris de l'information de sécurité IS.

30 Dans ce troisième mode de réalisation, le lecteur 30 réalise (E38c) en outre une analyse à partir de l'information de sécurité IS de façon analogue à l'analyse E38a ou E38b mentionnée ci-avant.

35 On notera que dans les deuxième et troisième modes de réalisation décrit ci-avant en référence aux **figures 8 et 9**, le lecteur 30 réalise le procédé de traitement de l'invention sans qu'il y ait besoin de modifier le protocole EMV. On utilise en effet le message de transaction AFL ou les informations IDD pour transmettre l'information de sécurité IS au lecteur 30.

De plus, dans les premier et deuxième modes de réalisation décrits ci-avant en référence aux **figures 7** et **8**, le lecteur 30 envoie une commande de lecture à la carte à puce 4 indiquant que le lecteur 30 souhaite accéder à l'information de sécurité 30. Dans le troisième mode de réalisation, en revanche, le lecteur 30 ne sollicite pas l'envoi par la

5 carte à puce 4 de l'information de sécurité IS, et transmet celle-ci en tant que IDD au serveur distant 45 comme déjà indiqué.

Selon une mise en œuvre particulière, au moins l'une parmi l'étape de détection S2, l'étape d'obtention S4 de l'information de sécurité IS et l'étape de stockage S6 de l'information de sécurité IS est réalisée par la carte à puce 4 pendant la phase

10 préliminaire PHP (i.e. après la réception par la carte du message RST provenant du lecteur 30), voire même pendant la transaction TR en cours (i.e. après la réception par la carte du message GPO provenant du lecteur 30).

Dans un cas particulier, la carte à puce 4 choisit la méthode de transmission de l'information de sécurité IS parmi plusieurs disponibles (par exemple parmi au moins deux

15 des méthodes décrites ci-avant) en fonction du moment où la carte à puce 4 détecte qu'elle a une information de sécurité IS à transmettre au lecteur. Le choix de la méthode d'envoi peut être réalisé par exemple à l'aide d'au moins une règle RL préenregistrée en mémoire dans la carte à puce 4.

Selon un exemple particulier, la carte à puce 4 détecte à un instant T1 qu'elle détient

20 une information de sécurité IS à transmettre, et transmet alors l'information de sécurité IS comme suit :

- si T1 est avant l'envoi par la carte à puce 4 de l'ATR, la carte transmet l'information de sécurité IS au lecteur 30 en mettant en œuvre le premier mode de réalisation illustré en **figure 7** (utilisation de l'ATR puis envoi de IS pendant

25 la transaction TR) ;
- si T1 est après l'envoi de l'ATR mais avant l'envoi du message APPLICATIONS, la carte 4 fournit la donnée de référence DRF au lecteur 30 en utilisant le message APPLICATIONS et envoie par la suite IS pendant la transaction TR (variante du premier mode de réalisation) ;
- 30 - si T1 est après l'envoi de APPLICATIONS mais avant la réception de GPO, la carte 4 envoie la donnée de référence DRF dans le message AFL et envoie par la suite IS pendant la transaction TR (deuxième mode de réalisation illustré en **figure 8**) ; et
- si T1 est après la réception de GPO mais avant la réception de GAC, la carte 4

35 envoie l'information de sécurité IS au lecteur 30 en tant qu'IDD en réponse au GAC (troisième mode de réalisation illustré en **figure 9**).

La présente invention permet avantageusement de remonter efficacement des informations de sécurité depuis une carte à puce (ou plus généralement depuis un dispositif électronique) vers un lecteur (ou terminal) externe afin de permettre la réalisation d'un traitement approprié par le lecteur et, le cas échéant, par un tiers tel que l'émetteur de la carte à puce par exemple.

La remontée de telles informations de sécurité permet notamment d'évaluer des risques de sécurité associés à la carte à puce et/ou à la transaction en cours (voire même à une transaction passée), d'identifier de possibles attaques rencontrées dans le passé par la carte à puce ou encore de réaliser des traitements en fonction de certains comportements observés dans le passé au niveau de la carte.

Si, par exemple, une commande visant à modifier le code PIN de la carte a été exécutée par la carte à puce ou si cette dernière s'est réinitialiser suite à un évènement donné, l'invention prévoit dans un cas particulier de stocker dans la carte à puce une information de sécurité représentative de cet évènement et de transférer de la carte à puce au lecteur ladite information afin d'en informer ensuite l'émetteur de la carte à puce. L'émetteur, typiquement la banque émettrice de cette carte, peut ainsi analyser le ou les évènements rencontrés par la carte et prendre si besoin les mesures nécessaires comme par exemple contacter le propriétaire de la carte, bloquer la carte ou encore refuser la transaction en cours.

L'invention offre un mécanisme souple et efficace pour mettre en œuvre des analyses de risque et/ou de comportement à partir d'évènements détectés par la carte à puce.

L'invention est avantageuse en ce qu'il est possible de mettre en œuvre la remontée d'information de sécurité vers le lecteur, voire vers le serveur distant sans qu'il soit nécessaire de modifier le déroulement général d'un protocole de type EMV par exemple.

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 combinaison des variantes et modes de réalisation décrits ci-avant afin de répondre à un besoin bien particulier.

REVENDEICATIONS

1. Procédé d'envoi d'une information de sécurité (IS) mis en œuvre par un dispositif électronique (4), ledit procédé comprenant les étapes suivantes :

- 5 - détection (S2) d'un événement rencontré par le dispositif électronique ;
- enregistrement (S6), dans une mémoire sécurisée (10) du dispositif, d'une information de sécurité (IS) représentative dudit événement ;
- démarrage (S8), suite audit enregistrement, d'une transaction (TR) avec un terminal externe (30) ; et
- 10 - envoi (S10) au terminal externe de l'information de sécurité (IS) dans un message de transaction (E20a ; E20b ; E34c) lors de ladite transaction (TR).

2. Procédé selon la revendication 1, dans lequel l'événement détecté par le dispositif électronique (4) comprend au moins l'un parmi :

- 15 - une anomalie rencontrée par le dispositif électronique ; et
- une attaque à l'encontre du dispositif électronique.

3. Procédé selon la revendication 1 ou 2, dans lequel l'événement est détecté par le dispositif électronique (4) à partir de la valeur courante d'un compteur.

20

4. Procédé selon la revendication 3, dans lequel l'événement (EVT) est une anomalie ou attaque détectée par le dispositif électronique (4) en comparant la valeur courante du compteur avec une valeur seuil.

25 5. Procédé selon la revendication 3 ou 4, dans lequel le compteur représente au moins l'un parmi :

- un nombre consécutif d'essais manqués de saisie d'un code secret ; et
- un nombre total de transactions incomplètes réalisées par le dispositif électronique (4).

30

6. Procédé selon l'une quelconque des revendications 3 à 5, dans lequel l'information de sécurité (IS) comprend la valeur courante dudit compteur enregistré dans la mémoire sécurisée.

7. Procédé selon l'une quelconque des revendications 1 ou 2, dans lequel le dispositif électronique (4) détecte, en tant qu'évènement (EVT) lors de ladite détection (S2), un intervalle de temps entre :

- 5 - l'envoi d'une réponse, par ledit dispositif électronique, à une commande du terminal externe (30) ; et
- la réception d'une commande subséquente du terminal externe (30).

8. Procédé selon la revendication 7, dans lequel ledit dispositif électronique (4) est configuré pour décider, à partir d'une comparaison entre ledit intervalle de temps et une
10 valeur seuil prédéterminée, si une donnée représentative dudit intervalle de temps doit être enregistrée lors de l'étape d'enregistrement.

9. Procédé selon l'une quelconque des revendications 1 à 8, dans lequel ledit évènement satisfait au moins l'une des conditions suivantes :

- 15 - l'évènement cause une réinitialisation du dispositif électronique (4) ; et
- l'évènement comprend l'exécution par le dispositif électronique (4) d'une opération affectant un code confidentiel stocké dans une mémoire sécurisée du dispositif électronique.

20 10. Procédé selon l'une quelconque des revendications 1 à 9, dans lequel un comportement anormal du dispositif électronique ou une attaque à l'encontre dudit dispositif électronique est détecté si au moins une condition préenregistrée dans le dispositif électronique est satisfaite.

25 11. Procédé selon l'une quelconque des revendications 1 à 10, dans lequel la transaction (TR) et le message de transaction comportant l'information de sécurité (IS) sont conformes au protocole EMV.

30 12. Procédé selon la revendication 11, comprenant un envoi au terminal externe, dans un message AFL, d'une donnée de référencement (DRF) permettant au terminal externe (3) de lire l'information de sécurité (IS) dans la mémoire sécurisée (10) du dispositif électronique ;

 l'information de sécurité (IS) étant envoyée (S10, E20a) au terminal externe en réponse à une commande de lecture (E18a) reçue du terminal externe suite à l'envoi du
35 message AFL.

12. Procédé selon la revendication 11, comprenant l'envoi au terminal externe (30), dans un message ATR, d'une donnée de référencement (DRF) lui permettant de lire l'information de sécurité (IS) dans la mémoire sécurisée (IS) du dispositif électronique.

5 12. Procédé selon la revendication 11, l'information de sécurité étant envoyée (S10, E34c) au terminal externe (30) en tant que donnée non interprétable (IDD) par le terminal externe en réponse à un message GENERATE AC reçu (E30) du terminal externe.

10 13. Programme d'ordinateur (PG1) comportant des instructions pour l'exécution des étapes d'un procédé d'envoi selon l'une quelconque des revendications 1 à 12 lorsque ledit programme est exécuté par un processeur (5).

15 14. Support d'enregistrement (10) lisible par un processeur (5) sur lequel est enregistré un programme d'ordinateur (PG1) comportant des instructions pour l'exécution des étapes d'un procédé d'envoi selon l'une quelconque des revendications 1 à 12.

15. Procédé de traitement mise en œuvre par un terminal externe (30) à un dispositif électronique (4), ledit procédé comprenant les étapes suivantes :

- 20 - démarrage (E12) d'une transaction (TR) avec le dispositif électronique (4) ;
- réception (E20a ; E20b ; E34c), en provenance du dispositif électronique, d'un message de transaction contenant une information de sécurité (IS) lors de la transaction (TR), ladite information de sécurité étant représentative d'un événement détecté par le dispositif électronique ; et
- traitement (E36a, E38a ; E36b, E38b ; E36c, E38c) de l'information de sécurité.

25 16. Procédé de traitement selon la revendication 15, dans lequel ledit traitement comprend au moins l'un parmi :

- réalisation (E38c) d'une analyse de risque associée à ladite transaction à partir de l'information de sécurité ; et
- 30 - envoi (E36c) de l'information de sécurité à un serveur distant (45) du terminal externe.

17. Dispositif électronique (4) comprenant :

- 35 - un module de détection (14) d'un événement rencontrée par le dispositif électronique ;

- un module d'obtention (16) d'une information de sécurité représentative dudit évènement ;
- un module d'enregistrement (18), dans une mémoire sécurisée du dispositif, de l'information de sécurité;
- 5 - un module d'exécution (20) apte à démarrer, suite à l'enregistrement de l'information de sécurité, une transaction avec le terminal externe ; et
- un module d'envoi (22) au terminal externe de l'information de sécurité dans un message de transaction lors de ladite transaction.

10 18. Dispositif selon la revendication 17, dans lequel le module d'exécution (20) est apte à poursuivre jusqu'à son terme la transaction une fois l'information de sécurité envoyée au terminal externe.

15 19. Dispositif électronique selon la revendication 17 ou 18, le dispositif électronique étant une carte à puce.

20 20. Dispositif électronique selon l'une quelconque des revendications 17 à 19, le module de détection comprenant au moins l'un parmi :

- un premier module de traitement apte à détecter ledit évènement à partir d'une commande reçue d'une l'entité externe par un module d'interface du dispositif électronique, ledit module d'interface permettant établir une communication entre le dispositif électronique et ladite entité électronique ; et
- un capteur apte à détecter une attaque survenant à l'encontre du dispositif électronique et un deuxième module de traitement apte à détecter ledit évènement à partir de l'attaque détectée.

25 21. Terminal (30) externe à un dispositif électronique (4), ledit terminal comprenant :

- un module d'exécution (48) apte à démarrer une transaction (TR) avec le dispositif électronique ;
- 30 - un module de réception (50) apte à recevoir du dispositif électronique un message de transaction contenant une information de sécurité (IS) lors de la transaction, ladite information de sécurité étant représentative d'un évènement détecté par le dispositif électronique (4) ; et
- un module de traitement (52) de l'information de sécurité.

22. Terminal (30) selon la revendication 21, dans lequel ladite transaction (TR) et ledit message de transaction sont conformes au protocole EMV, le terminal comprenant :
- un module d'extraction (54) apte à extraire, d'un message ATR reçu du dispositif électronique (4) lors de la transaction (TR), une donnée de référencement (DRF)
- 5 permettant au terminal de lire l'information de sécurité (IS) dans une mémoire sécurisée (10) du dispositif électronique.

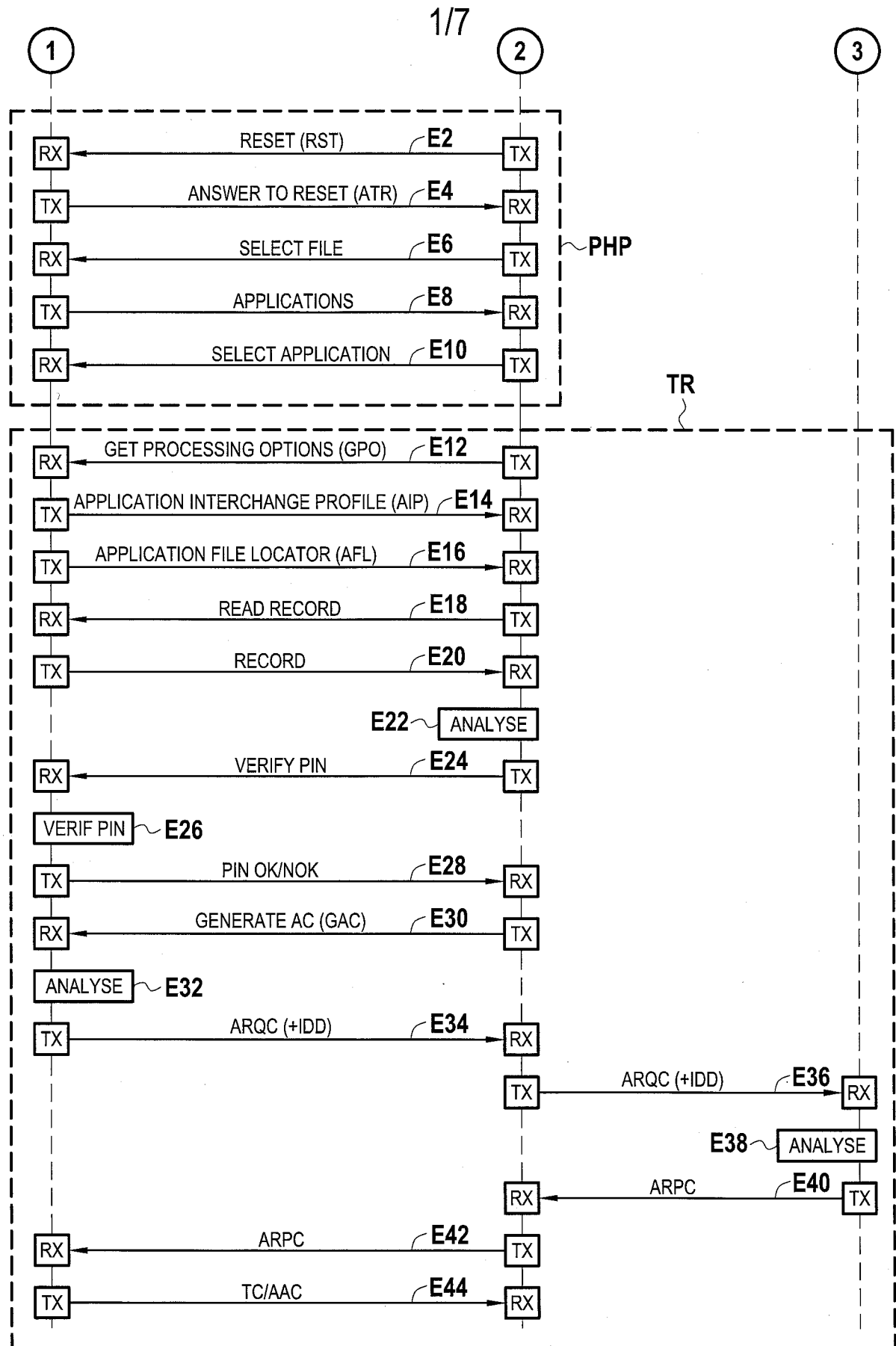


FIG.1

2/7

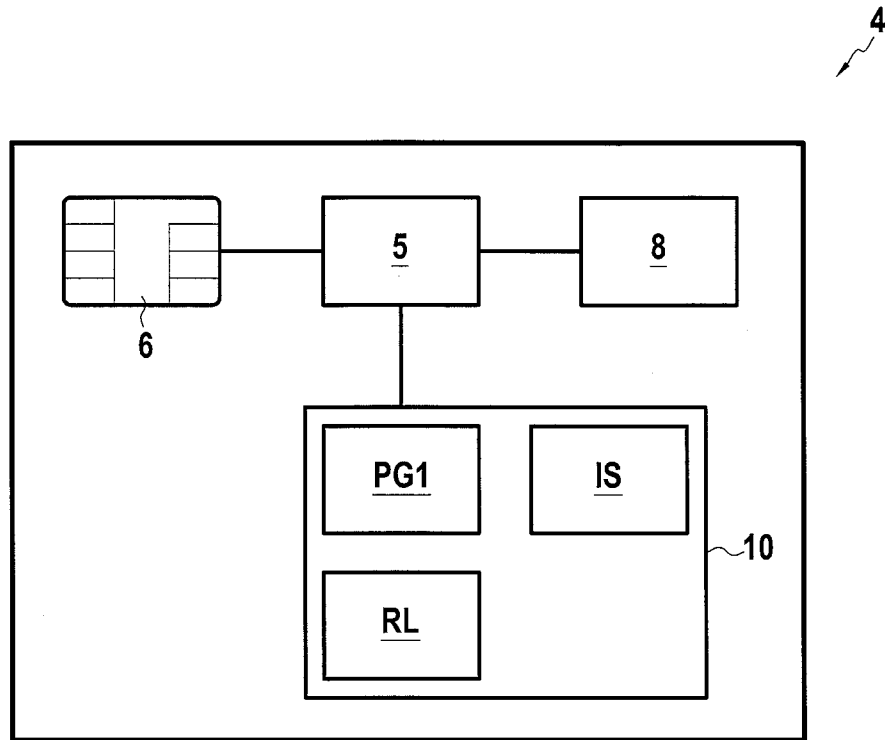


FIG.2

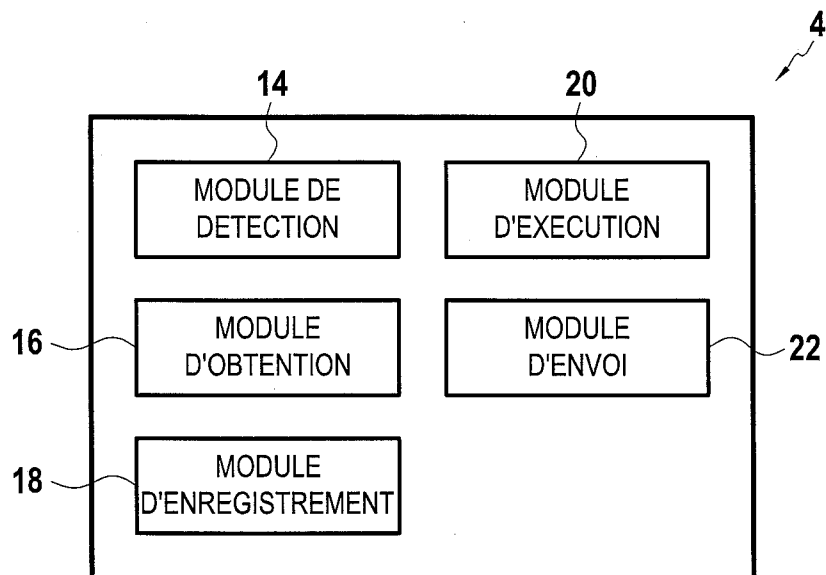


FIG.3

3/7

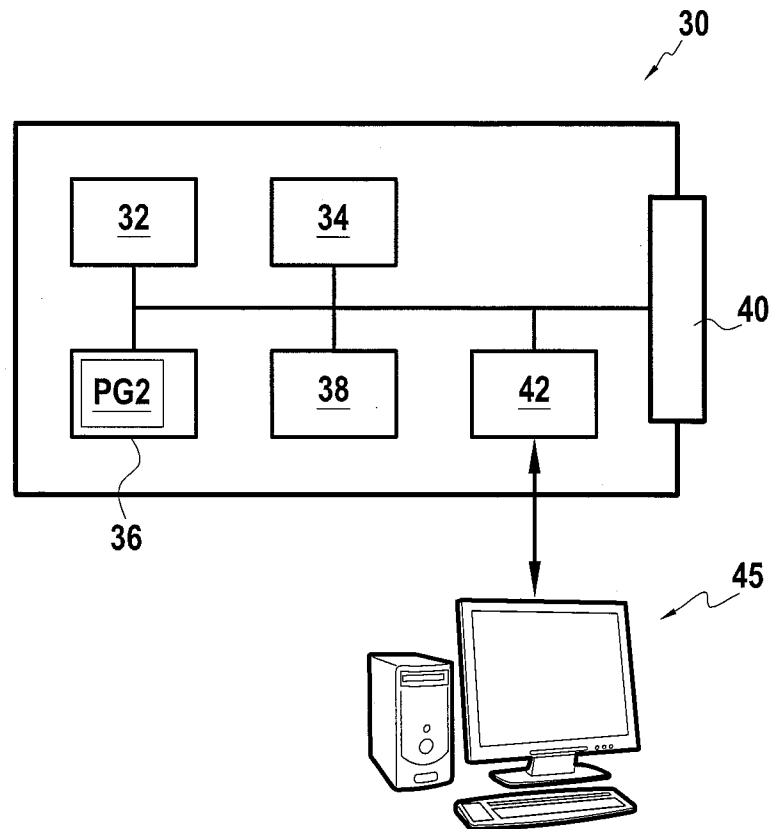


FIG.4

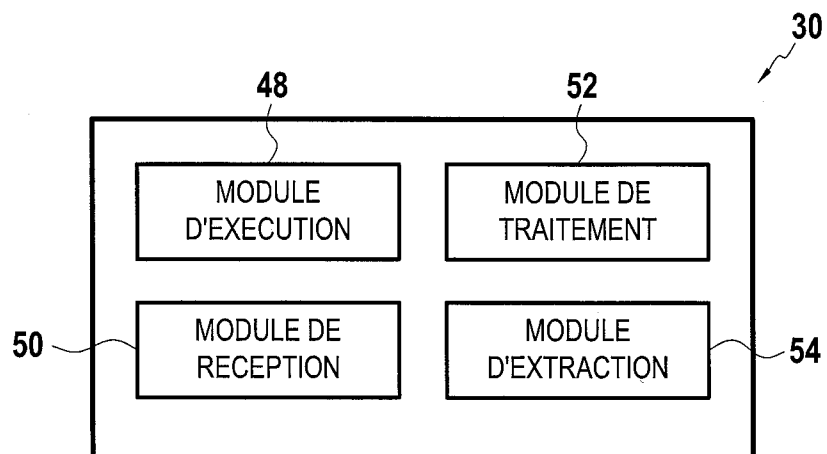


FIG.5

4/7

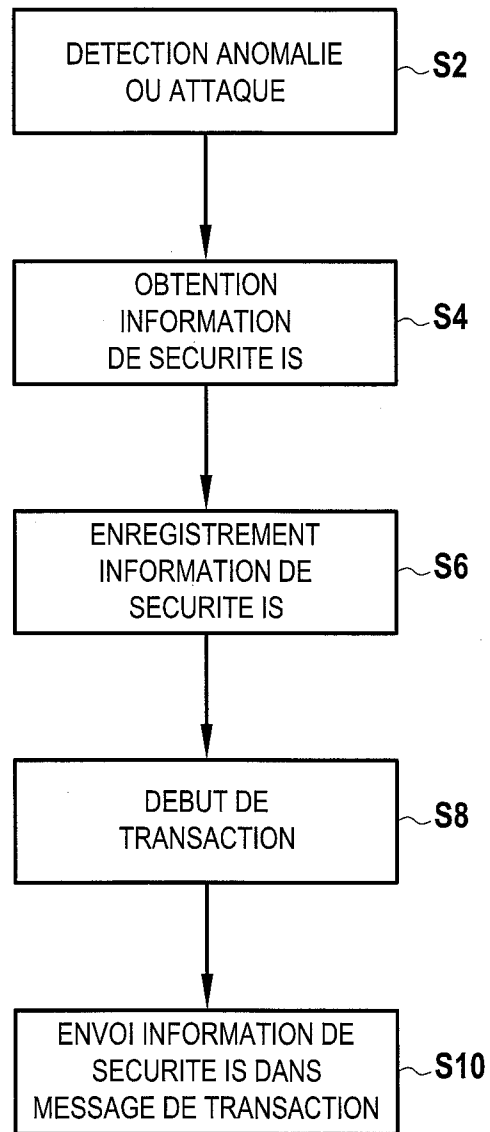
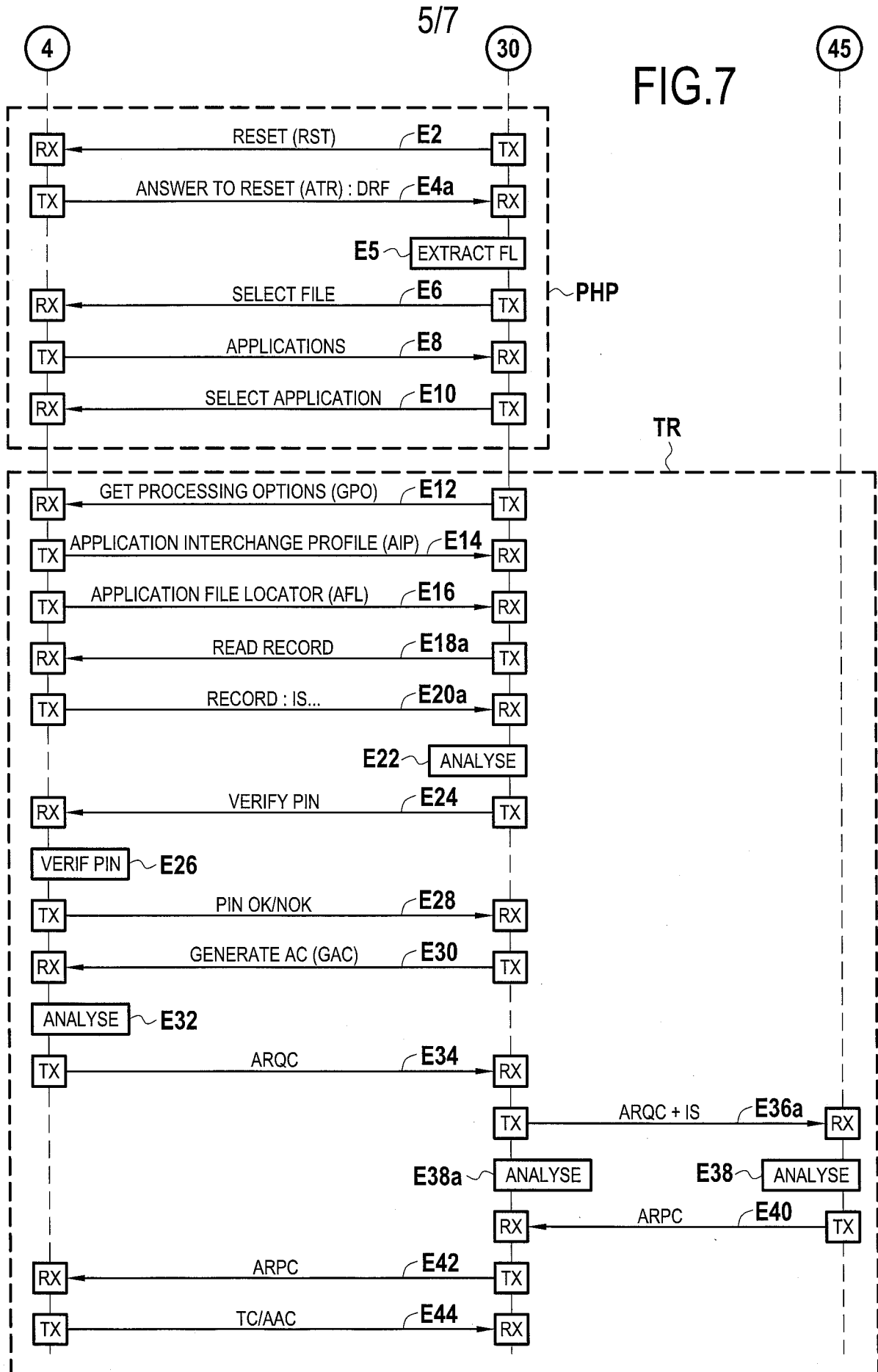


FIG.6



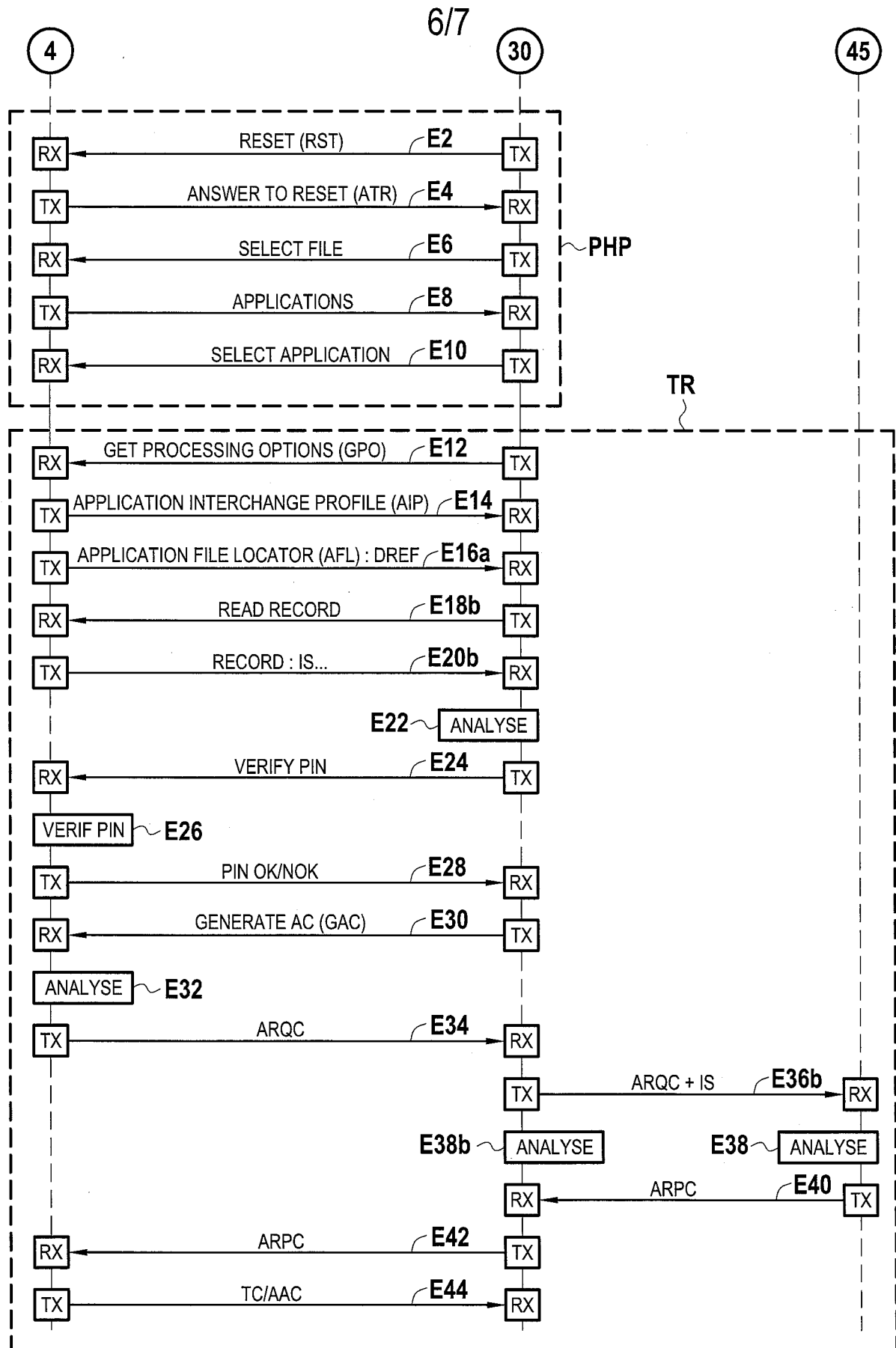


FIG.8

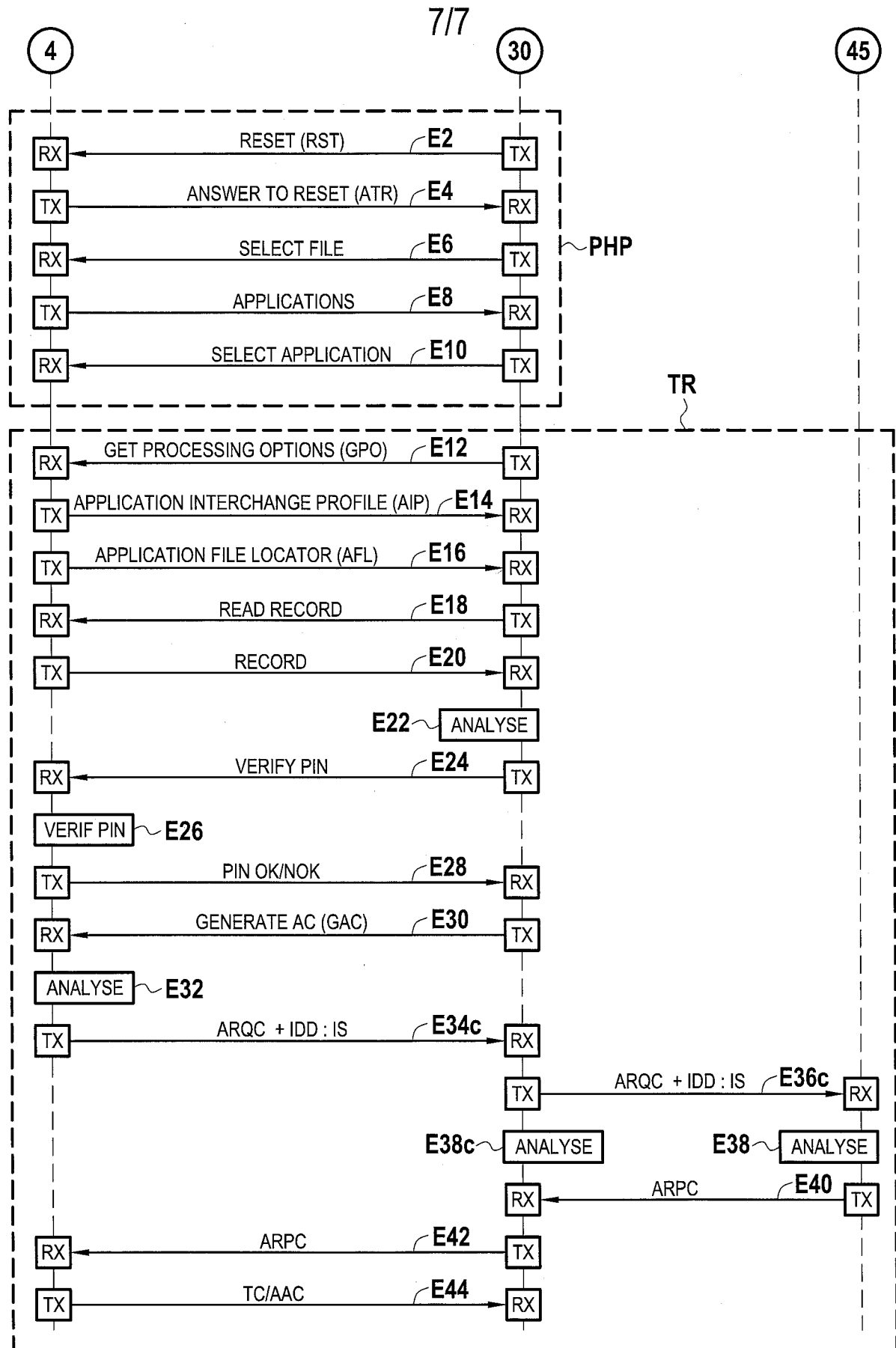


FIG.9

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/053630

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/52 G06F21/77
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)
G06F

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CONSTANTINOS MARKANTONAKIS ED - BRUCE SCHNEIER ET AL: "Secure Log File Download Mechanisms for Smart Cards", 1 January 2006 (2006-01-01), SMART CARD. RESEARCH AND APPLICATIONS LECTURE NOTES IN COMPUTER SCIENCE;;LNCS, SPRINGER, BERLIN, DE, PAGE(S) 285 - 304, XP019048907, ISBN: 978-3-540-67923-3	1,13-19, 21
Y	*1 Introduction* *2 Applications* *3 Model of SmRT Card Environment* * 4.4 Using an ALSS in a Remote Location* ----- -/-	2-12,20, 22



Further documents are listed in the continuation of Box C.



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

18 February 2016

Date of mailing of the international search report

26/02/2016

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Chabot, Pedro

INTERNATIONAL SEARCH REPORT

International application No

PCT/FR2015/053630

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	B. ROBISSON ET AL: "Management of the security in smart secure devices", SMART SYSTEMS INTEGRATION, DRESDEN, 22 - 23 MARCH 2011, 1 January 2011 (2011-01-01), XP055064434, Germany ISBN: 978-3-80-073324-8 * 1 Introduction * * 2.1 Misuse/Anomaly detection* *3.4.1 Security sensors* -----	2-12,20, 22

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/FR2015/053630

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. G06F21/52 G06F21/77 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) G06F		
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		
C. DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	CONSTANTINOS MARKANTONAKIS ED - BRUCE SCHNEIER ET AL: "Secure Log File Download Mechanisms for Smart Cards", 1 janvier 2006 (2006-01-01), SMART CARD. RESEARCH AND APPLICATIONS LECTURE NOTES IN COMPUTER SCIENCE;;LNCS, SPRINGER, BERLIN, DE, PAGE(S) 285 - 304, XP019048907, ISBN: 978-3-540-67923-3	1,13-19, 21
Y	*1 Introduction* *2 Applications* *3 Model of SmRT Card Environment* * 4.4 Using an ALSS in a Remote Location* ----- -/--	2-12,20, 22
☒ Voir la suite du cadre C pour la fin de la liste des documents ☐ 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 18 février 2016		Date d'expédition du présent rapport de recherche internationale 26/02/2016
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Fonctionnaire autorisé Chabot, Pedro

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	B. ROBISSON ET AL: "Management of the security in smart secure devices", SMART SYSTEMS INTEGRATION, DRESDEN, 22 - 23 MARCH 2011, 1 janvier 2011 (2011-01-01), XP055064434, Germany ISBN: 978-3-80-073324-8 * 1 Introduction * * 2.1 Misuse/Anomaly detection* *3.4.1 Security sensors* -----	2-12,20, 22