(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 051 064**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **16 54122**

(51) Int Cl[8] : ***G 06 Q 20/34*** *(2017.01), G 06 F 21/31*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 09.05.16.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 10.11.17 Bulletin 17/45.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *OBERTHUR TECHNOLOGIES Société anonyme* — FR.

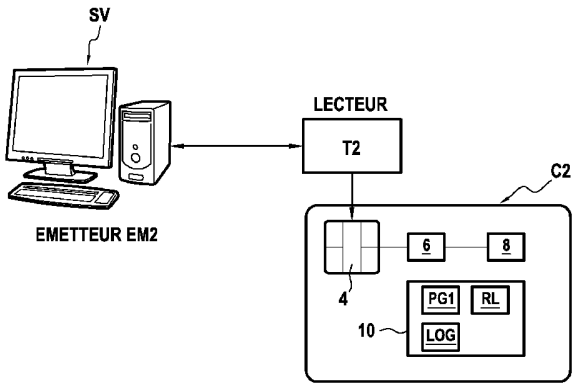
(72) **Inventeur(s) :** CHAMBEROT FRANCIS et DE OLIVEIRA MARCO.

(73) **Titulaire(s) :** OBERTHUR TECHNOLOGIES Société anonyme.

(74) **Mandataire(s) :** CABINET BEAU DE LOMENIE.

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

(57) L'invention concerne un procédé de sécurisation mis en oeuvre par un dispositif électronique (C2), le procédé comprenant : réception d'une commande requérant une modification d'un paramètre de fonctionnement du dispositif électronique (C2) ; détection de si ledit paramètre de fonctionnement est un paramètre prédéfini en tant que paramètre sensible ; dans l'affirmative, détermination de si la modification requise par la commande entraîne, si elle est appliquée, une dégradation de la sécurité du dispositif électronique (C2) en comparant l'état initial du paramètre à réception de la commande avec un nouvel état à affecter au paramètre de fonctionnement en réponse à la commande ; et, en cas de dégradation de la sécurité du dispositif électronique (C2), déclenchement d'une opération de sécurisation du dispositif électronique (C2) en réponse à ladite première commande.



FR 3 051 064 - A1

Arrière-plan de l'invention

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

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

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

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

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

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

critères de vérification préenregistrés pour décider si la transaction doit être autorisée ou refusée.

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, les cartes à puce font aujourd'hui face à un type d'attaque malveillante pour lequel aucune protection satisfaisante n'a été à ce jour développée. Cette attaque consiste à envoyer, depuis l'entité émettrice de la carte à puce, une commande, dite « commande de script », destinée à modifier un ou plusieurs paramètres de fonctionnement de la carte. La modification porte généralement sur des paramètres de fonctionnement sensibles de la carte tels que des niveaux de compteurs internes ou des seuils limites à respecter (limites de paiement hors ligne etc.). La commande peut encore porter sur une mise à jour de la configuration de la carte à puce causant un changement sensible dans le traitement des transactions par la carte à puce.

Dans le cadre d'une telle attaque, les commandes de script envoyées sont authentiques dans le sens où elles présentent toutes les caractéristiques d'une commande de script valide générée et envoyée par l'émetteur de la carte pour modifier l'un ou plusieurs de ses paramètres de fonctionnement. Ces commandes de script sont cependant frauduleuses dans l'intention dans le sens où ces commandes sont envoyées sans l'autorisation préalable de l'émetteur (de la banque par exemple).

Dans la mesure où ces commandes de script présentent en tout point les caractéristiques d'une commande valide (cryptogramme MAC authentique etc.), elles sont normalement exécutées par les cartes à puce.

De telles commandes de script frauduleuses peuvent notamment être envoyées avec la complicité d'une personne malveillante ayant accès à l'interface de communication de l'émetteur. Il peut s'agir par exemple d'un employé mal intentionné de la banque émettrice de la carte à puce ou encore d'un tiers ou d'un programme ayant accès aux infrastructures permettant l'envoi de telles commandes. C'est pourquoi, ce type d'attaque est parfois désignée sous la dénomination anglo-saxonne « *insider attack* » (ou « attaque de l'intérieur ») car l'envoi de ces commandes frauduleuses émanera généralement de l'entité émettrice de la carte à puce concernée.

Les risques en termes de sécurité sont donc particulièrement élevés en raison du caractère sensible des paramètres de fonctionnement susceptibles d'être modifiés frauduleusement dans une carte à puce lors d'une telle attaque. Ce risque est encore accru par le fait qu'un grand nombre de commandes de script frauduleuses peut être envoyé massivement à de multiples cartes à puce.

Il existe donc aujourd'hui un besoin pour sécuriser les cartes à puce (de type EMV notamment) et, plus généralement, les dispositifs électroniques aptes à coopérer avec un

terminal externe pour mettre en œuvre une transaction. En particulier, aucune solution satisfaisante n'existe aujourd'hui pour pallier aux risques de sécurité liés à une attaque de type « *insider attack* » telle qu'expliquée ci-avant.

Objet et résumé de l'invention / Résumé

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

- réception d'une première commande requérant une modification d'au moins un paramètre de fonctionnement du dispositif électronique ;
- détection de si ledit au moins un paramètre de fonctionnement est un paramètre prédéfini en tant que paramètre sensible dans le dispositif électronique ;
- dans l'affirmative, détermination de si ladite modification requise par la première commande entraîne, si elle est appliquée, une dégradation de la sécurité du dispositif électronique en comparant l'état initial dudit au moins un paramètre à réception de ladite première commande avec un nouvel état à affecter audit au moins un paramètre de fonctionnement en réponse à la première commande ; et
- en cas de dégradation de la sécurité dudit dispositif électronique, déclenchement d'au moins une opération de sécurisation du dispositif électronique en réponse à ladite première commande.

L'invention permet avantageusement de réaliser une sécurisation appropriée du dispositif électronique lorsque ce dernier détecte qu'une modification de l'un de ses paramètres de fonctionnement sensibles est requise par une commande de script. Il est ainsi possible d'adapter le traitement, par le dispositif électronique, des commandes de script visant à modifier un paramètre de fonctionnement, de façon à limiter les risques encourus par ledit dispositif en termes de sécurité.

L'invention permet notamment de protéger efficacement le dispositif électronique face à une potentielle attaque de type « *insider attack* » telle que décrite précédemment, dans le cas où une commande de script frauduleuse est reçue par le dispositif en question. Le dispositif électronique peut adapter sa réponse sécuritaire à une commande de script reçue en réalisant une opération de sécurisation spécifique et ce, même si la vérification de l'authenticité et de l'intégrité de ladite commande de script est passée avec succès par le dispositif électronique.

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

Selon un mode de réalisation particulier, le dispositif électronique détecte que ledit paramètre de fonctionnement est un paramètre prédéfini en tant que paramètre sensible

si la première commande comprend l'un parmi une liste d'au moins un identifiant prédéfini.

Selon un mode de réalisation particulier, si ledit au moins un paramètre est détecté comme étant un paramètre prédéfini en tant que paramètre sensible, la détermination, à partir dudit au moins un paramètre de fonctionnement, d'une vérification à réaliser,

le dispositif électronique réalisant ladite vérification lors de ladite détermination pour déterminer si ladite modification requise entraîne, si elle est appliquée, une dégradation de la sécurité du dispositif.

Selon un mode de réalisation particulier, le dispositif électronique vérifie si ledit nouvel état est supérieur ou inférieur à l'état initial dudit au moins un paramètre,

et détermine, à partir de ladite vérification, si ladite modification requise entraîne, si elle est appliquée, une dégradation de la sécurité du dispositif électronique.

Selon un mode de réalisation particulier, le dispositif électronique détermine que ladite modification requise par la première commande entraîne, si elle est appliquée, une dégradation de la sécurité du dispositif électronique, si l'écart de valeur entre le nouvel état et l'état initial dudit au moins un paramètre atteint une valeur seuil prédéfinie.

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

- enregistrement d'un message à envoyer, ledit message informant de la réception de ladite première commande ;
- envoi dudit message ;
- enregistrement de l'état initial dudit au moins un paramètre de fonctionnement ;
- application de ladite modification audit au moins un paramètre de fonctionnement de sorte à passer son état de l'état initial au nouvel état ; et
- enregistrement, dans un fichier d'historisation, d'une donnée représentative de la réception de ladite première commande.

Selon un mode de réalisation particulier, suite audit enregistrement de l'état initial et à l'application de la modification causant le passage dudit au moins un paramètre de fonctionnement de l'état initial au nouvel état, le dispositif électronique restaure l'état initial ou un état prédéfini dudit au moins un paramètre de fonctionnement en réponse à une commande de restauration. Dans un exemple particulier, l'état prédéfini est un état par défaut différent du nouvel état.

Selon un mode de réalisation particulier, le dispositif électronique reçoit ladite première commande lors d'une première transaction mise en œuvre par le dispositif électronique, et dans lequel le dispositif électronique reçoit la commande de restauration lors d'une seconde transaction mise en œuvre par le dispositif électronique, ladite seconde transaction étant subséquente à la première transaction.

Selon un mode de réalisation particulier, la première commande comprend un cryptogramme de type MAC.

Selon un mode de réalisation particulier, la première commande est une commande PUT DATA selon la norme ISO 7816, ladite première commande commandant l'affectation du nouvel état audit au moins un paramètre de fonctionnement.

Selon un mode de réalisation particulier, le dispositif électronique est une carte à puce apte à mettre en œuvre une transaction en coopération avec un terminal de lecture.

Selon un mode de réalisation particulier, le dispositif électronique est une carte EMV, l'une au moins parmi les première commande et deuxième commande étant une commande de script reçue, lors d'une transaction EMV, après l'envoi, par ladite carte EMV, d'un message ARQC conforme à la norme EMV.

Selon un mode de réalisation particulier, la première commande inclut le nouvel état à affecter audit au moins un paramètre de fonctionnement.

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

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

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

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

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

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

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

L'invention concerne également un dispositif électronique comprenant :

- un module de réception d'une première commande requérant une modification d'au moins un paramètre de fonctionnement du dispositif électronique ;
- un module de détection pour détecter si ledit au moins un paramètre de fonctionnement est un paramètre prédéfini en tant que paramètre sensible dans le dispositif électronique ;
- un module de détermination configuré, en cas de résultat positif de ladite détection par le module de détection, pour déterminer si ladite modification requise par la première commande entraîne, si elle est appliquée, une dégradation de la sécurité du dispositif électronique en comparant l'état initial dudit au moins un paramètre à réception de ladite première commande avec un nouvel état à affecter audit au moins un paramètre de fonctionnement en réponse à la première commande ; et
- un module de sécurisation configuré, en cas de résultat positif de ladite détermination par le module de détermination, pour déclencher au moins une opération de sécurisation prédéfinie du dispositif électronique en réponse à ladite première commande.

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

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

Brève description des dessins

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

- la figure 1 est un diagramme représentant schématiquement les étapes réalisées par une carte à puce, un terminal externe et l'émetteur de la carte à puce dans la mise en œuvre d'une transaction EMV ;
- la figure 2 représente schématiquement la structure d'une carte à puce conforme à un mode de réalisation particulier de l'invention ;

- la figure 3 représente schématiquement des modules mis en œuvre dans la carte à puce illustrée en figure 2, selon un mode de réalisation particulier ;
- la figure 4 représente schématiquement des règles prédéfinies enregistrées dans la carte à puce illustrée en figure 2, selon un mode de réalisation particulier ;
- la figure 5 représente schématiquement un fichier d'historisation enregistré dans la carte à puce illustrée en figure 2, selon un mode de réalisation particulier ;
- la figure 6 représente schématiquement, sous forme d'un organigramme, les étapes d'un procédé de sécurisation mise en œuvre selon un mode de réalisation particulier de l'invention ;
- la figure 7 représente schématiquement, sous forme d'un organigramme, les étapes d'un procédé de sécurisation mise en œuvre selon un mode de réalisation particulier de l'invention ; et
- la figure 8 représente schématiquement, sous forme d'un organigramme, les étapes d'un procédé de sécurisation mise en œuvre selon un mode de réalisation particulier de l'invention.

Description détaillée de plusieurs modes de réalisation

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

L'invention propose de sécuriser les carte à puce contre les attaques de type « *insider attack* », et plus particulièrement contre les commandes de script frauduleuses telles que décrites précédemment.

La **figure 1** représente un exemple d'une transaction de paiement conforme au protocole EMV, à l'aide d'une carte à puce C1. Dans cet exemple, la carte C1 est une carte EMV.

Lors de la mise en œuvre d'une transaction, le protocole EMV s'articule en trois phases, des variantes étant toutefois possibles. On comprendra que certains éléments et opérations généralement mis en œuvre lors d'une transaction EMV ont été volontairement omis car ils ne sont pas nécessaires à la compréhension de la présente invention.

Lors d'une première phase destinée à authentifier la carte à puce C1 utilisée, le terminal T1 et la carte C1 s'échangent un message RESET (RST) en S2 puis une réponse ATR en S4.

En S6, le porteur de la carte sélectionne via le terminal T1 le mode de transaction souhaité, déclenchant ainsi l'envoi d'une commande « *SELECT* » à la carte C1 afin d'initier le début de la transaction EMV.

Une fois la phase d'authentification de carte achevée, le protocole EMV procède à une phase d'authentification (non représentée) du porteur de la carte C1. Le terminal T2 détermine le procédé d'authentification du porteur à appliquer et détermine en particulier si la transaction est effectuée en mode avec vérification de code ou en mode sans vérification de code. Si le mode avec vérification de code est sélectionné, la carte à puce C1 vérifie la validité du code PIN entré par le porteur sur le terminal T1. Si en revanche le mode sans vérification de code est sélectionné, aucune vérification de code PIN n'est réalisée. Ce cas se produit par exemple lorsque le terminal est dans l'incapacité de prendre en charge la vérification d'un code PIN. Dans ce cas, la signature manuscrite du porteur peut éventuellement être requise pour authentifier ce dernier.

Une fois la phase d'authentification du porteur achevée, le protocole EMV initie la phase de vérification de la transaction. Pour ce faire, le terminal T1 envoie (S8) à la carte à puce C1 une première commande APDU dite GENERATE AC ou GAC (notée ici GAC1). Cette commande bien connue comprend des informations sur la transaction en cours telles que le montant de la transaction, la devise utilisée, le type de transaction, etc.

La carte EMV réalise alors une vérification de la transaction selon des critères de vérification prédéfinis puis envoie (S10), en réponse, un cryptogramme (ou certificat cryptographique) comprenant un code d'authentification de message (ou MAC pour « *Message Authentification Code* » en anglais). Ce code d'authentification MAC est par exemple crypté à partir d'une clé cryptographique mémorisée dans la carte C1. La réponse de la carte C1 dans le message ARQC dépend notamment du paramétrage de la carte effectué par l'entité émettrice (dit « émetteur ») de ladite carte.

Plus précisément, dans l'exemple de la **figure 1**, la carte à puce C1 envoie en S10 un message de type ARCQ (« *Autorisation Request Cryptogram* ») indiquant que la carte souhaite poursuivre la transaction en ligne avec, par exemple, un serveur distant de l'émetteur EM1 de la carte C1 utilisée (mode en ligne). Le terminal T1 transmet (S12) alors le cryptogramme ARQC à l'émetteur EM1 qui réalise à distance un certain nombre de vérifications afin de s'assurer que la transaction est valide. Le terminal T1 reçoit (S14)

ensuite, en réponse, un message crypté de type ARPC indiquant la décision de l'émetteur EM1. En S14, le terminal T1 peut en outre recevoir de l'émetteur EM1 une ou des commandes, dites « commandes de script », chacune requérant la modification dans la carte à puce C1 d'au moins un paramètre de fonctionnement. Dans cet exemple, deux commandes de script SC1 et SC2 sont envoyées en S14 par l'émetteur EM1.

Le terminal T1 transmet alors le message ARPC (S16) et chacune des commandes de script SC1 et SC2 (S18, S22) à la carte C1.

Plus particulièrement, dans l'exemple représenté en **figure 1**, le terminal T1 envoie en S18 la commande de script SC1 à la carte C1. En réponse à cette commande SC1, la carte à puce C1 modifie au moins un paramètre de fonctionnement de façon appropriée. Le terminal T1 envoie ensuite en S20 à la carte à puce C1 une deuxième commande APDU bien connue de type GENERATE AC ou GAC (notée ici GAC2). Si la carte C2 accepte la transaction, celle-ci envoie, en réponse à la commande GAC2, un cryptogramme de type TC (transaction acceptée) au terminal T1. Dans le cas contraire, la carte C1 envoie un cryptogramme de type AAC au terminal T1 (refus de la transaction). En outre, toujours dans cet exemple, le terminal T1 envoie ensuite en S22 la commande de script SC2 à la carte C1. En réponse à cette commande SC2, la carte C1 modifie au moins un paramètre de fonctionnement de façon appropriée.

Chaque commande de script SC1, SC2 provenant de l'émetteur EM1 peut être reçue en cours de transaction, avant ou après la réception de la commande GAC2, et peut donner lieu à un échange de données entre la carte C1 et le terminal T1. Le nombre et la nature des commandes de script reçues ainsi que la manière dont celles-ci sont traitées par la carte C1 peut varier selon le cas.

Comme indiqué ci-avant, dans le cadre d'une attaque de type « *insider attack* », des commandes de script SC1, SC2 peuvent être envoyées par une personne ou entité malveillante, par exemple depuis l'interface de communication de l'émetteur EM1 (depuis l'un de ses serveurs par exemple).

La présente invention propose un procédé de sécurisation mis en œuvre par un dispositif électronique pour palier notamment à ce type d'attaque malveillante.

Selon différents modes de réalisation, le procédé de l'invention, mis en œuvre par un dispositif électronique tel qu'une carte à puce par exemple, comprend : la réception d'une commande requérant une modification d'un (ou d'une pluralité de) paramètre de fonctionnement du dispositif électronique, cette commande incluant un nouvel état à affecter audit paramètre de fonctionnement ; la détection de si le paramètre de

fonctionnement est un paramètre prédéfini en tant que paramètre sensible dans le dispositif électronique ; dans l'affirmative, la détermination de si la modification requise entraîne, si elle est appliquée, une dégradation de la sécurité du dispositif électronique en comparant l'état initial du paramètre à réception de ladite commande avec le nouvel état à affecter audit paramètre ; et en cas de dégradation de la sécurité dudit dispositif électronique, le déclenchement d'une opération de sécurisation du dispositif électronique en réponse à ladite commande.

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

Dans le présent exposé, des exemples de mises en œuvre de l'invention sont décrits en relation avec une carte à puce de type EMV. On comprendra que l'invention ne se limite par exclusivement aux cartes EMV mais s'applique plus généralement à tout dispositif apte à mettre en œuvre une transaction, y compris des dispositifs autre que des cartes à puce et qui utilisent le standard EMV, et des dispositifs électroniques qui utilisent d'autres standards de transaction.

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

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

La **figure 2** représente, de manière schématique, la structure d'une carte à puce C2, conforme à un mode de réalisation particulier.

On comprendra que certains éléments généralement présents dans une carte à puce ont été volontairement omis car ils ne sont pas nécessaires à la compréhension de la présente invention. A noter également que la carte à puce C2 représentée en **figure 1** n'est qu'un exemple de réalisation, d'autres mises en œuvre étant possibles dans le cadre de l'invention. L'homme du métier comprendra en particulier que certains éléments de la

carte à puce C2 ne sont décrits ici que pour faciliter la compréhension de l'invention, ces éléments n'étant pas nécessaires pour mettre en œuvre l'invention.

La carte à puce C2 est apte à coopérer avec un terminal (ou lecteur) T2 afin de réaliser une transaction, telle qu'une transaction financière ou bancaire (transaction de paiement ou autre) dans le cas présent.

Le terminal T2 est apte à faire l'interface entre la carte à puce C2 et un serveur distant SV. Dans le cas présent, le serveur SV est un serveur de l'entité émettrice EM2 (i.e., une institution bancaire par exemple) de la carte à puce C2. Dans cet exemple, la carte C2 est apte, via le terminal T2, à communiquer avec le serveur distant SV afin de mettre en œuvre, selon le protocole EMV, une transaction dite « en ligne », c'est-à-dire impliquant un échange avec l'émetteur EM1.

Plus précisément, la carte à puce C2 comprend dans cet exemple des contacts externes aptes à coopérer avec le lecteur T2, au moins un processeur 6, une mémoire volatile réinscriptible (de type RAM) 8 et une mémoire non volatile réinscriptible 10 (de type Flash par exemple).

La mémoire 10 constitue dans un cet exemple un support d'enregistrement (ou support d'informations) conforme à un mode de réalisation particulier, lisible par le la carte à puce C2, et sur lequel est enregistré un programme d'ordinateur 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 sécurisation selon un mode de réalisation particulier. Les principales étapes de ce procédé sont représentées, dans des modes de réalisation particuliers de l'invention, sur les **figures 6**, **7** et **8** décrites ultérieurement.

Dans un exemple particulier, la carte à puce C2 est conforme à la norme ISO 7816. Dans ce cas, les contacts externes 4 présentent des caractéristiques conformes à cette norme. On comprendra toutefois que d'autres modes de réalisation sont possibles. La carte à puce C2 peut par exemple coopérer avec le lecteur T2 en mode sans contact via une antenne RF intégrée dans la carte C2.

Toujours dans l'exemple considéré ici, un fichier d'historisation LOG (appelé aussi « *Log* » en anglais) et au moins une règle prédéfinie RL sont enregistrés dans la mémoire non volatile réinscriptible 10 de la carte C2. Dans l'exemple considéré ici, les règles RL comprennent quatre règles prédéfinies RL1, RL2, RL3 et RL4, d'autres exemples étant possibles dans le cadre de l'invention. Les règles prédéfinis RL et le fichier d'historisation

LOG seront décrits plus en détail ci-après en référence aux **figures 4** et **5** respectivement.

Le processeur 6 piloté par le programme d'ordinateur PG1, met ici en œuvre un certain nombre de modules représentés en **figure 3**, à savoir : un module de réception MD2, un module de détection MD4, un module de détermination MD6 et un module de sécurisation MD8.

Dans cet exemple, le module de réception MD2 est apte à recevoir une commande (ou « commande de script ») notée ici CMD, cette commande requérant une modification d'au moins un paramètre de fonctionnement PR de la carte à puce C2. Des exemples d'une telle commande de script CMD seront décrits ultérieurement.

Selon un exemple particulier, ladite commande CMD inclut un nouvel état V2 (ou une nouvelle valeur) à affecter audit au moins un paramètre de fonctionnement PR de la carte C2. Grâce à l'envoi d'une telle commande CMD, il est ainsi possible de commander à la carte à puce C2 la modification d'un paramètre de fonctionnement PR de sorte à faire passer son état d'un ancien état (ou « état initial ») V1 à un nouvel état V2 spécifié dans la commande.

Le module de détection MD4 est configuré pour détecter si ledit au moins un paramètre de fonctionnement PR, dont une modification est requise par la commande CMD reçue par le module de réception MD2, est un paramètre prédéfini en tant que paramètre sensible dans la carte à puce C2.

Selon un exemple particulier illustré en **figure 4**, une liste LT d'au moins un paramètre sensible PR est enregistrée dans la mémoire 10. A partir d'une telle liste LT, il est possible de déterminer, pour chaque paramètre de fonctionnement PR de la carte à puce C2, s'il s'agit ou non d'un paramètres sensible (ou non sensible). La définition des paramètres de fonctionnement dits sensibles est par exemple réalisée lors de la personnalisation de la carte à puce C2. Comme expliqué par la suite, divers manières sont possibles pour définir, à partir d'une telle liste LT, le ou les paramètres de fonctionnement dit sensibles dans la carte à puce C2.

Selon un exemple particulier, la commande de script CMD reçue par le module de réception MD2 présente une structure TLV pour « *Tag Length Value* » en anglais. Dans le cas présent, le tag TG inclus dans la commande CMD définit la zone mémoire de destination où le paramètre de fonctionnement PR correspondant doit être modifié dans la mémoire 10 de la carte C2. Dans cet exemple, le module de détection MD4 est configuré

pour déterminer si le tag TG de la commande CMD reçue est enregistré dans la liste LT comme identifiant un paramètre PR sensible de la carte C2.

Dans l'exemple illustré en **figure 4**, la liste LT identifie quatre tags (ou identifiants) TG1, TG2, TG3 et TG4, chacun de ces tags correspondant à un paramètre de fonctionnement respectif PR1, PR2, PR3 et PR4.

On suppose par exemple que le paramètre de fonctionnement PR1 n'est pas un paramètre prédéfini en tant que paramètre sensible dans la carte C2 et que les paramètres de fonctionnement PR2, PR3 et PR4 sont chacun prédéfinis en tant que paramètre sensible dans la carte C2.

Dans le cas où ledit au moins un paramètre de fonctionnement PR, dont une modification est requise par la commande CMD reçue, est détecté comme étant un paramètre sensible dans la carte à puce C2, le module de détermination MD6 est configuré pour déterminer si ladite modification requise par la commande CMD cause, si elle est appliquée, une dégradation (ou baisse) de la sécurité de la carte à puce C2. Pour ce faire, le module de détermination MD6 compare l'état initial V1 dudit au moins un paramètre PR à réception de ladite commande CMD avec le nouvel état V2 à affecter audit au moins un paramètre PR en réponse à la commande CMD reçu (ce nouvel état étant par exemple inclus dans la commande la commande CMD).

Selon un exemple de réalisation particulier, si ledit au moins un paramètre PR est détecté en tant que paramètre sensible, le module de détermination MD6 est configuré pour déterminer, à partir dudit au moins un paramètre PR, une vérification à réaliser. Le module de détermination MD6 est alors configuré pour déterminer si ladite commande de script CMD entraîne une dégradation de la carte C2 en réalisant ladite vérification précédemment déterminée. Comme expliqué par la suite, ladite vérification à réaliser peut varier selon le cas. Cette vérification permet de réaliser un contrôle de sécurité supplémentaire lorsque la modification d'un paramètre de fonctionnement sensible est requise par la commande de scripte CMD reçue. Dans un exemple particulier, cette vérification est une fonction de vérification F prédéfinie exécutable par la carte C2.

Dans l'exemple illustré en **figure 4**, une fonction de vérification F1, F2, F3 et F4 est enregistrée dans les règles prédéfinies RL en association avec respectivement le tag TG1, TG2, TG3 et TG4. Ces fonctions de vérification F1-F4 seront décrites plus en détail ci-après dans un exemple de réalisation particulier illustré en **figures 6**, **7** et **8**. Ces fonctions F définissent ici si le paramètre de fonctionnement PR correspondant est sensible ou non.

Par ailleurs, toujours en référence à la **figure 3**, le module de sécurisation MD8 est configuré, si une dite dégradation de la sécurité de la carte C2 est détectée comme décrit ci-avant, pour déclencher au moins une opération de sécurisation prédéfinie du dispositif électronique en réponse à la commande de script CMD reçue. Chaque opération de sécurisation est destinée à sécuriser la carte à puce C2 en réponse à la commande de script CMD. Des exemples de telles opérations sont décrits ci-après en référence aux **figures 6**, **7** et **8**.

La **figure 5** représente schématiquement le fichier d'historisation LOG selon un mode de réalisation particulier. Ce fichier d'historisation, stocké ici dans la mémoire non-volatile 10, est apte à enregistrer, pour chaque paramètre de fonctionnement PR1-PR4, l'état (ou valeur) initiale V1 dudit paramètre PR à réception d'une commande de script CMD reçue par le module de réception MD2 et le nouvel état V2, spécifier dans la commande de script CMD reçue, à affecter audit paramètre PR. L'exemple particulier de fichier d'historisation LOG illustré en **figure 5** sera décrit plus en détail ultérieurement.

Les étapes réalisées par la carte à puce C2 lors d'un procédé de sécurisation selon un mode de réalisation particulier sont à présent décrites en référence à la **figure 6**. Pour ce faire, la carte à puce C2 exécute le programme d'ordinateur PG1.

Au cours d'une étape A2 de réception, la carte à puce C2 reçoit une commande de script CMD requérant une modification d'au moins un paramètre PR de fonctionnement de la carte à puce C2. Dans cet exemple, ladite commande CMD inclut le nouvel état (ou valeur) V2 à affecter audit au moins un paramètre de fonctionnement PR, bien que d'autres exemples de réalisation sont possibles selon lesquels le nouvel état (ou valeur) V2 n'est pas inclus dans la commande de script CMD.

La commande de script CMD est par exemple reçue lors d'une transaction EMV en cours mise en œuvre par la carte à puce C2 en coopération avec le terminal T2. Cette commande de script CMD peut être reçue à divers moment lors de la transaction EMV, comme déjà décrit en référence à la **figure 1**.

Selon un exemple particulier, cette commande de script CMD est émise par l'émetteur EM2 de la carte à puce C2 (par exemple depuis un serveur distant). Cette commande CMD comprend un identifiant MAC permettant à la carte à puce C2 de vérifier l'authenticité et l'intégrité de ladite commande CMD.

Cette commande CMD peut être une commande APDU, par exemple une commande « PUT DATA » selon la norme ISO 7816, cette commande commandant l'affectation d'un nouvel état V2 audit au moins un paramètre de fonctionnement PR dans la carte à puce

C2. Grâce à l'envoi d'une telle commande CMD, il est ainsi possible de commander à la carte à puce C2 la modification d'un paramètre de fonctionnement PR de sorte à faire passer son état d'un ancien état V1, dit « état initial », à un nouvel état V2 spécifié dans la commande CMD.

La nature du ou des paramètres de fonctionnement PR, dont une modification est requise par la commande de script CMD, peut varier selon le cas. D'une manière générale, un paramètre de fonctionnement PR configure la manière dont la carte à puce C2 traite une transaction avec un terminal extérieur, tel que le lecteur T2 dans cet exemple.

Le paramètre de fonctionnement PR à modifier peut, par exemple, être un compteur enregistré dans la carte à puce C2. Un tel compteur peut par exemple représenter un nombre de transactions hors ligne déjà réalisées par la carte à puce C2, ou encore le montant cumulé de transactions hors ligne déjà réalisées par la carte à puce C2. Le paramètre PR peut par ailleurs porter sur une valeur seuil d'un tel compteur. Le paramètre PR peut également commander une mise à jour de la configuration de la carte à puce C2 causant un changement dans le traitement des transactions par la carte à puce.

Dans un exemple particulier, une fois la commande de script CMD reçue, la carte à puce C2 vérifie en outre, en A2, l'authenticité de la commande CMD. L'authentification est par exemple réalisée par la carte C2 à partir de l'identifiant MAC inclus dans la commande CMD. La carte C2 est configurée pour procéder à l'étape A4 qui suit uniquement si cette authentification en A2 est passée avec succès. Si l'authentification de la commande CMD échoue, le procédé prend fin (la carte C2 décline par exemple la demande de modification du paramètre PR requise par la commande CMD). Autrement dit, la carte à puce C2 poursuit le procédé seulement si cette commande de script CMD est déterminée comme étant « authentique » en A2. Comme expliqué ci-avant, une commande de script peut être authentique dans le sens où elle a bien été émise par l'émetteur EM2 mais potentiellement frauduleuse dans l'intention dans le sens où cette commande a été envoyée sans autorisation préalable de l'émetteur (par exemple par un employé mal intentionné).

Au cours d'une étape A4 de détection, la carte à puce C2 détecte si ledit au moins un paramètre de fonctionnement PR, dont une modification est requise par la commande CMD reçue en A2, est un paramètre prédéfini en tant que paramètre sensible dans la carte à puce C2. Comme déjà indiqué, il est possible d'adapter, selon le cas d'usage, les

paramètres de fonctionnement PR considérés par la carte à puce C2 comme étant sensibles ou non.

Pour ce faire, dans l'exemple considéré ici, la carte à puce C2 consulte la liste LT dans laquelle est spécifié au moins un paramètre de fonctionnement sensible de la carte à puce C2.

Selon un exemple particulier, une donnée (ou fonction) est enregistrée dans la carte à puce C2 en association avec chaque paramètre PR de la liste LT, ladite donnée indiquant si le paramètre PR correspondant est sensible ou non. L'utilisation d'une telle donnée (ou fonction) sera décrite plus en détail dans un exemple particulier en référence à la **figure 7**.

Selon un exemple de réalisation particulier, chaque paramètre PR identifié dans la liste LT est un paramètre sensible. Selon encore un autre exemple de réalisation, chaque paramètre PR identifié dans la liste est un paramètre non sensible. Selon ces variantes, la carte à puce C2 peut ainsi déterminer si un paramètre PR donné est sensible ou non à partir de la liste LT, sans qu'il soit nécessaire d'enregistrer une donnée (ou fonction) associée indiquant le caractère sensible ou non du paramètre PR en question.

Au cours d'une étape A6 de détermination, en cas de résultat positif de la détection A4 (c.-à-d. si ledit au moins un paramètre PR à modifier est prédéfini en tant que caractère sensible), la carte à puce C2 détermine si ladite modification requise par la commande de script CMD reçue cause, si elle est appliquée, une dégradation de la sécurité de ladite carte à puce C2. Pour ce faire, la carte à puce C2 compare l'état initial V1 dudit au moins un paramètre PR à réception de ladite commande CMD avec le nouvel état V2 à affecter audit au moins un paramètre PR, ce nouvel état V2 étant (dans cet exemple) inclus dans la commande CMD reçue en A2. Autrement dit, la carte à puce C2 compare l'ancienne valeur V1 dudit au moins un paramètre PR avec sa nouvelle valeur V2 dans l'hypothèse où la modification requise par la commande CMD est appliquée.

A noter qu'une telle dégradation de sécurité peut résulter d'une réelle attaque malveillante à l'encontre de la carte C2 ou d'une situation jugée à risque en termes de sécurité par la carte C2.

Selon un exemple de réalisation particulier, si ledit au moins un paramètre PR est détecté en tant que paramètre sensible en A4, la carte à puce C2 détermine (A6), à partir dudit au moins un paramètre PR, une vérification à réaliser. La carte à puce C2 détermine alors en A6 si ladite commande de script CMD entraîne une dégradation de la carte C2 en réalisant la vérification ainsi déterminée. Dans un exemple particulier, cette vérification

est une fonction de vérification F prédéfinie comme expliqué plus en détail dans l'exemple de réalisation illustré en **figure 7**. Il est ainsi possible varier la manière dont la dégradation de sécurité est évaluée en fonction du paramètre de sécurité sensible concerné.

Selon un exemple de réalisation particulier, lors de la détermination A6, la carte à puce C2 vérifie si ledit nouvel état V2 est supérieur ou inférieur à l'état initial V1 dudit au moins un paramètre PR à modifier, puis détermine, à partir de cette vérification, si ladite modification requise par la commande CMD reçue entraîne, si elle est appliquée, une dégradation de la sécurité de la carte à puce C2. Selon la configuration choisie dans la carte à puce C2, la détection d'une augmentation (ou, respectivement, réduction) de la valeur d'un paramètre PR sensible causée par la commande de script CMD peut ainsi être considérée comme constituant une dégradation de la sécurité de ladite carte C2.

Selon un exemple de réalisation particulier, lors de la détermination A6, la carte à puce C2 détermine que ladite modification requise par la commande de script CMD entraîne, si elle est appliquée, une dégradation de la sécurité du dispositif électronique si l'écart de valeur entre le nouvel état V2 et l'état initial V1 dudit au moins un paramètre PR à modifier atteint au moins une valeur seuil prédéfinie. La carte à puce C2 peut par exemple être configurée pour détecter (A6) une dégradation de sécurité si la modification requise par la commande CMD requiert une augmentation d'au moins une valeur prédéfinie de l'un de ses paramètres de fonctionnement PR.

Au cours d'une étape de déclenchement A8, en cas de résultat positif de ladite détermination A6 (c'est-à-dire si une dite dégradation de la sécurité de la carte C2 est détectée en A6), la carte à puce C2 déclenche au moins une opération de sécurisation prédéfinie en réponse à la commande de script CMD reçue. Chaque opération de sécurisation vise à sécuriser ladite carte à puce C2 vis-à-vis de la commande de script CMD reçue en A2. Le nombre et la nature de ces opérations de sécurisation peuvent varier selon le cas d'usage.

Selon un mode de réalisation particulier, ladite au moins une opération de sécurisation A8 comprend au moins l'un quelconque parmi :

- l'enregistrement d'un message à envoyer, ledit message informant de la réception A2 de ladite commande de script CMD, et éventuellement l'envoi dudit message (ce message pouvant inclure un indicateur représentatif du type d'évènement, d'attaque ou de problème de sécurité rencontré par la carte à puce C2 suite à la réception A2 de la commande CMD) ;

- l'enregistrement dans le fichier d'historisation LOG de l'état initial V1 dudit au moins un paramètre de fonctionnement PR, et l'application de ladite modification requise par la commande CMD audit au moins un paramètre de fonctionnement PR de sorte à passer son état de l'état initial V1 au nouvel état V2 spécifié dans la commande de script CMD reçue ; et
- l'enregistrement, dans le fichier d'historisation LOG, d'une donnée représentative de la réception A2 de ladite commande de script CMD.

D'autres opérations de sécurisation A8 sont possibles telles que la restauration de la de l'état initial V1 du paramètre de fonctionnement PR postérieurement à l'application de la modification requise par la commande de script CMD, comme décrit par exemple plus en détail dans le mode de réalisation illustré en **figure 8**.

L'invention permet avantageusement de réaliser une sécurisation supplémentaire de la carte à puce C2 lorsque cette dernière détecte qu'une modification de l'un de ses paramètres de fonctionnement sensibles est requise par une commande de script. Il est ainsi possible d'adapter le traitement, par la carte à puce, des commandes de script visant à modifier un paramètre de fonctionnement, de façon à limiter les risques encourus par ladite carte en termes de sécurité.

L'invention permet notamment de protéger efficacement la carte à puce face à une potentielle attaque de type « *insider attack* » telle que décrite précédemment, dans le cas où une commande de script frauduleuse est reçue par la carte en question. La carte à puce C2 peut adapter sa réponse sécuritaire à une commande de script reçue en réalisant une opération de sécurisation spécifique et ce, même si la vérification de l'authenticité et de l'intégrité de ladite commande de script est passée avec succès par la carte à puce.

Un mode de réalisation particulier du procédé décrit en référence à la **figure 6** est à présent décrit en référence notamment à la **figure 7**. On suppose que la carte à puce C2 met en œuvre un procédé de sécurisation en exécutant le programme PG1.

On suppose en premier lieu qu'une transaction EMV (notée TR1) est en cours (A20), cette transaction étant mise en œuvre de façon quelconque par la carte à puce C2 en coopération avec le terminal T2, ce dernier faisant l'interface entre la carte C2 et le serveur distant SV de l'émetteur EM2. Il s'agit ici d'une transaction en ligne dans le sens où l'émetteur EM2 intervient dans la mise en œuvre de la transaction TR1.

En C1, le serveur SV envoie une commande de script CMD1 au terminal T2 qui la reçoit en B1. Le terminal T2 transmets (B2) ensuite cette commande CMD1 à la carte à puce C2 qui la reçoit en A2.

On suppose ici que la commande CMD1 requiert une modification d'un unique paramètre de fonctionnement PR de la carte à puce C2, bien que d'autres implémentations soient possibles.

La commande de script CMD1 comprend un identifiant MAC permettant de vérifier que la commande CMD1 est bien authentique.

De plus, dans l'exemple considéré ici, la commande de script CMD1 présente une structure TLV comme déjà mentionnée ci-avant. La commande CMD1 comprend en particulier un tag (noté TG) définissant la zone mémoire de destination où le paramètre de fonctionnement PR en question doit être modifié dans la mémoire 10 de la carte C2.

On suppose dans cet exemple que la commande de script CMD1 est une commande APDU de type « PUT DATA » selon la norme ISO 7816, cette commande commandant l'affectation d'un nouvel état V2 au paramètre de fonctionnement PR dans la carte à puce C2. Comme déjà indiqué, une telle commande CMD permet de demander à la carte à puce C2 la modification d'un paramètre de fonctionnement PR de sorte à faire passer son état d'un état initial V1 à un nouvel état V2 spécifié dans la commande CMD1. Dans cet exemple particulier, le nouvel état (ou valeur) V2 à affecter au paramètre de fonctionnement PR concerné est inclus dans la commande de script PUT DATA CMD1, bien que d'autres exemples de réalisation sont possibles selon lesquels le nouvel état (ou valeur) V2 n'est pas inclus dans la commande de script.

Dans un exemple particulier déjà décrit ci-avant, une fois la commande de script CMD1 reçue, la carte à puce C2 vérifie en outre, en A2, l'authenticité de la commande CMD1. Dans cet exemple, l'authentification est réalisée par la carte C2 à partir de l'identifiant MAC inclus dans la commande CMD1 reçue en A2. La carte C2 est configurée pour procéder à l'étape A4 qui suit uniquement si cette authentification en A2 est passée avec succès. Si l'authentification de la commande CMD1 échoue, le procédé prend fin (la carte C2 décline par exemple la demande de modification du paramètre PR requise par la commande CMD1). Autrement dit, la carte à puce C2 poursuit le procédé seulement si cette commande de script CMD1 est déterminée comme étant « authentique » en A2.

Comme déjà expliqué ci-avant en référence à la **figure 6**, la carte à puce détecte en A4 si le paramètre de fonctionnement PR à modifier est un paramètre prédéfini en tant que paramètre sensible. Dans cet exemple particulier représenté en **figure 7**, cette détermination est réalisée à partir de la liste LT dans laquelle sont enregistrés les tags TG1, TG2, TG3 et TG4 correspondant respectivement aux paramètres de fonctionnement PR1, PR2, PR3 et PR4 (figure 4). Lors de la détection A4, la carte à puce C2 détermine si

le tag TG inclus dans la commande CMD reçue en A2 est enregistré dans la liste LT comme identifiant un paramètre PR sensible de la carte C2.

Dans l'exemple illustré en **figure 4**, les fonctions de vérification F1, F2, F3 et F4 (notées collectivement F) sont en outre enregistrées dans les règles prédéfinies RL (notées RL1 à RL4) en association avec respectivement le tag TG1, TG2, TG3 et TG4. Chaque fonction F indique si le paramètre de fonctionnement PR1-PR4 correspondant est sensible ou non.

Dans cet exemple particulier, la fonction de vérification F1 renvoie la valeur « 0 » (F1 = 0) ce qui signifie que le paramètre PR1 associé au tag TG1 est prédéfini en tant que paramètre non sensible dans la carte C2. Toujours dans cet exemple, les fonctions de vérification F2, F3 et F4 sont telles que :

- la fonction de vérification F2(TG2, V21, V22) associée au paramètre de fonctionnement PR2 prend comme entrées le tag TG2, la valeur initiale V21 du paramètre PR2 et la nouvelle valeur V22 à affecter au paramètre PR2 ;
- la fonction de vérification F3(TG3, V31, V32) associée au paramètre de fonctionnement PR3 prend comme entrées le tag TG3, la valeur initiale V31 du paramètre PR3 et la nouvelle valeur V32 à affecter au paramètre PR3 ;
- la fonction de vérification F4(TG4, V41, V42) associée au paramètre de fonctionnement PR4 prend comme entrées le tag TG2, la valeur initiale V41 du paramètre PR4 et la nouvelle valeur V42 à affecter au paramètre PR4.

Selon un exemple particulier, deux au moins parmi les fonctions F2, F3 et F4 sont identiques.

Selon un exemple particulier, l'une au moins parmi les fonctions F ne prend pas de tag TG en entrée.

Selon un exemple particulier, chaque règle RL enregistre, en lieu et place des fonctions F, un indicateur spécifiant si le paramètre de fonctionnement PR associé est sensible ou non.

Dans l'exemple considéré ici, la carte à puce C2 détermine en A4 si le paramètre PR à modifier est sensible ou non en comparant le tag TG inclus dans la commande CMD1 avec les tag TG1-TG4 identifié dans la liste LT et en déterminant la fonction de vérification F enregistrée (le cas échéant) dans une règle RL en association avec le tag TG inclus dans la commande CMD1. La carte à puce C2 détermine (A4) alors, à partir de la fonction F associée au tag TG inclus dans la commande CMD1, si le paramètre de fonctionnement PR correspondant est sensible ou non pour la carte à puce C2. On suppose par exemple

que la carte à puce détecte en A4 que le tag TG inclus dans la commande CMD1 est le tag TG2 et détermine, en exécutant la fonction de vérification F2, que le tag TG correspond à un paramètre de fonctionnement sensible de la carte à puce C2.

Comme déjà expliqué ci-avant en référence à la **figure 6**, la carte à puce détermine (A6 ; **figure 7**) ensuite si ladite modification requise par la commande de script CMD1 entraîne, si elle est appliquée, une dégradation de la sécurité de la carte à puce C2 en comparant l'état initial V1 du paramètre sensible PR concerné à réception de la commande CMD1 avec le nouvel état V2 (inclus dans cet exemple dans la commande CMD1) à affecter au paramètre sensible PR en question. Pour ce faire, la carte à puce C2 exécute ici la fonction de vérification F spécifiée dans la règle RL concernée en association avec le tag TG inclus dans la commande CMD1 reçue.

Dans cet exemple, l'exécution de la fonction de vérification F applicable cause la réalisation successive de l'étape A24 de comparaison et de l'étape A26 de détermination telles que décrites ci-après.

On comprendra que l'exécution ci-dessous de la fonction F ne constitue qu'un exemple non limitatif et que la manière dont l'évaluation de la potentielle dégradation de sécurité peut être adaptée en modifiant la fonction F en conséquence. L'exécution de cette fonction permet de réaliser un contrôle de sécurité supplémentaire lorsque la modification d'un paramètre de fonctionnement sensible est requise par la commande de scripte reçue.

En A24, la carte à puce C2 compare l'état initial V1 du paramètre sensible PR à modifier (c'est-à-dire l'état actuel du paramètre PR au moment de la réception de ladite commande CMD) avec le nouvel état V2, inclus ici dans la commande CMD1 reçue, à affecter audit paramètre sensible PR.

Dans cet exemple, la carte à puce C2 vérifie en A24 si la nouvelle valeur V2 du paramètre sensible PR à modifier est supérieur (ou, respectivement, inférieur) à la valeur initiale V1 dudit paramètre sensible PR à modifier. Autrement dit, la carte à puce C2 détermine en A24 si la modification requise par la commande de script CMD1 cause l'augmentation (ou, respectivement, la diminution) de l'état du paramètre sensible PR en question. Dans l'exemple considéré ici, si la carte à puce détecte en A24 que V2 > V1, le procédé continue en A26. Dans le cas contraire, le procédé prend fin.

En A26, la carte à puce C2 détermine si l'écart de valeur entre le nouvel état V2 et l'état initial V1 du paramètre sensible PR à modifier atteint au moins une valeur seuil

prédéfinie Lmax. Le paramètre sensible PR à modifier est par exemple l'un quelconque parmi :

- un compteur du nombre de transactions hors ligne réalisées par la carte à puce C2 ;
- le montant cumulé de transactions hors ligne réalisées par la carte à puce C2 ; et
- une valeur seuil d'un tel compteur.

Si la carte à puce C2 détermine en A26 que l'écart entre V1 et V2 est au moins égal à la valeur seuil limite Lmax, une dégradation de la sécurité de la carte à puce C2 est détectée et le procédé continue en A8. Dans le cas contraire, le procédé prend fin.

Comme déjà expliqué ci-avant en référence à la **figure 6**, la carte à puce C2 déclenche en A8 (**figure 7**) au moins une opération de sécurisation de la carte à puce C2 en réponse à la commande de script CMD1 reçue. Comme déjà indiqué, le nombre et la nature de ces opérations (ou actions) de sécurisation peuvent varier selon le cas d'usage.

La carte à puce C2 peut ainsi mettre en œuvre une réponse sécuritaire adaptée en fonction du problème de sécurité rencontré.

Dans l'exemple représenté en **figure 7**, la carte à puce C2 réalise les opérations de sécurisation A30 et A32 telles que décrites ci-après.

En A30, la carte à puce C2 envoie un message MSG à destination du serveur SV de l'émetteur EM2. Le terminal T2 reçoit le message MSG en B30 et transmet celui-ci au serveur SV en B31. Le serveur SV reçoit le message MSG en C31.

Ce message MSG comprend une donnée représentative de la dégradation de sécurité détectée en A6. Ce message permet avantageusement à la carte à puce C2 d'informer le serveur SV (et éventuellement aussi le terminal T2, si ce dernier prend en compte cette information) du type de problème de sécurité rencontré par la carte à puce C2 suite à la réception A2 de la commande CMD1.

L'envoi A30 du message MSG par la carte à puce C2 peut être réalisé au cours de la transaction TR1, par exemple avant ou après la réception d'un message GAC2 tel que décrit ci-avant en référence à la **figure 1**.

Dans un exemple particulier, le message MSG est un message de transaction EMV tel que défini par le protocole EMV, ce message comprenant ladite donnée représentative de la dégradation de sécurité détectée en A6.

Dans un exemple particulier, le message MSG est envoyé en A30 au cours d'une nouvelle transaction EMV subséquente à la transaction TR1.

Par ailleurs, la carte à puce C2 enregistre en A32 l'état (ou la valeur) initial V1 du paramètre sensible PR à modifier, c'est-à-dire l'état que présente ledit paramètre PR à réception par la carte à puce C2 de la commande de scripte CMD1. Dans cet exemple, comme représenté en **figure 5**, l'état initial V1 est enregistré (A32) dans le fichier d'historisation LOG en association avec le paramètre sensible PR correspondant.

En outre, toujours en A32, la carte à puce C2 applique la modification du paramètre sensible PR requise par la commande de script CMD1. Pour ce faire, la carte à puce C2 exécute dans cet exemple la commande PUT DATA en affectant audit paramètre sensible PR le nouvel état V2 requis par la commande CMD1. La carte à puce C2 peut éventuellement également enregistrer le nouvel état V2 dans le fichier d'historisation LOG en association au paramètre sensible PR et à l'état initial V1 correspondants.

Dans le mode de réalisation décrit ici, la carte à puce C2 exécute donc la commande de script CMD1 reçue bien qu'un risque de sécurité ait été détecté. Par précaution, la carte à puce C2 en informe toutefois l'émetteur EM2 et stocke en mémoire l'état initial V1 du paramètre sensible PR afin que la carte à puce C2 et/ou une entité extérieure (telle que l'émetteur EM2 par exemple) puisse y accéder ultérieurement. L'enregistrement A32 de l'état initial V1 permet le cas échéant à la carte à puce C2 de restaurer l'état initial V1 du paramètre sensible PR correspondant, comme expliqué dans un exemple particulier ci-après.

La **figure 8** représente un mode de réalisation particulier selon lequel, suite à l'étape A32 décrite ci-avant en référence à la **figure 7**, la carte à puce C2 met en œuvre une transaction EMV (notée TR2) subséquent à la transaction TR1. Le terminal T2 fait ici aussi l'interface entre la carte à puce C2 et le serveur distant SV de l'émetteur EM2.

En cours de cette nouvelle transaction TR2, la carte à puce C2 restaure l'état initial V1 du paramètre sensible PR modifié en A32, en réponse à une commande de restauration CMD2 envoyée par le serveur SV.

Plus précisément, suite à l'initiation de la transaction TR2, le serveur SV envoie C40 la commande de restauration CMD2 au terminal T2 qui la reçoit en B40. Le terminal T2 transmet (B42) ensuite cette commande CMD2 à la carte à puce C2 qui la reçoit en A42.

En A44, la carte à puce C2 restaure l'état du paramètre sensible PR modifié en A32 en lui affectant l'état initial V1 enregistré dans le fichier d'historisation LOG (dans cet exemple, V1 est différent de V2).

Dans un exemple particulier, la commande de restauration CMD2 comprend un identifiant du paramètre sensible PR à restaurer de façon à ce que la carte à puce C2 détermine le paramètre sensible PR à restaurer.

Alternativement, la commande CMD2 ne comprend pas un tel identifiant et la carte à puce C2 est configurée pour restaurer l'état d'un ou d'une pluralité de paramètres selon une règle prédéfinie. En réponse à la commande CMD2, la carte à puce C2 restaure par exemple l'état d'au moins un paramètre sensible PR prédéfini. Cette restauration est, par exemple, réalisée à partir du contenu du fichier d'historisation LOG.

On notera que la restauration de l'état initial du paramètre sensible PR modifié en A32 ne fait pas nécessairement intervenir un fichier d'historisation tel qu'illustré par exemple en **figure 5**. Selon un exemple particulier, en réponse à une commande de restauration CMD2, la carte à puce C2 est configurée pour affecter un état (ou valeur) prédéfini par défaut, cet état pouvant être différent de l'état initial V2 du paramètre sensible PR en question. Dans cet exemple, l'état (ou valeur) prédéfini par défaut est différent du nouvel état V2.

Selon un exemple particulier, en réponse à une commande de restauration CMD2, la carte à puce C2 restaure l'état de tous les paramètres sensibles PR définis en tant que tels dans la liste LT, de sorte que soit affecter à chacun de ces paramètres PR l'état initial V1 à réception A2 de la commande CMD1 ou un état prédéfini par défaut comme expliqué ci-avant.

Ce mode de réalisation particulier permet avantageusement à une entité externe, telle que l'émetteur EM2 par exemple, de déclencher la restauration à distance d'un paramètre sensible PR dont une modification avait précédemment causé une dégradation de la sécurité de la carte à puce C2. L'émetteur EM2 peut ainsi monitorer les messages MSG envoyer par chacune de ses cartes à puce et déclencher ultérieurement la restauration d'un paramètre sensible s'il le juge nécessaire.

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

REVENDICATIONS

1. Procédé de sécurisation mis en œuvre par un dispositif électronique (C2), ledit procédé comprenant :

- réception (A2) d'une première commande (CMD ; CMD1) requérant une modification d'au moins un paramètre (PR) de fonctionnement du dispositif électronique ;
- détection (A4) de si ledit au moins un paramètre de fonctionnement est un paramètre prédéfini en tant que paramètre sensible dans le dispositif électronique ;
- dans l'affirmative, détermination (A6) de si ladite modification requise par la première commande entraîne, si elle est appliquée, une dégradation de la sécurité du dispositif électronique en comparant l'état initial (V1) dudit au moins un paramètre (PR) à réception de ladite première commande avec un nouvel état (V2) à affecter audit au moins un paramètre de fonctionnement en réponse à la première commande ; et
- en cas de dégradation de la sécurité dudit dispositif électronique, déclenchement (A8) d'au moins une opération de sécurisation du dispositif électronique en réponse à ladite première commande.

2. Procédé selon la revendication 1, dans lequel le dispositif électronique détecte que ledit paramètre de fonctionnement (PR) est un paramètre prédéfini en tant que paramètre sensible si la première commande comprend l'un parmi une liste d'au moins un identifiant (TG2-TG4) prédéfini.

3. Procédé selon la revendication 1 ou 2, comprenant, si ledit au moins un paramètre (PR) est détecté comme étant un paramètre prédéfini en tant que paramètre sensible, la détermination (A22), à partir dudit au moins un paramètre de fonctionnement (PR), d'une vérification (F) à réaliser,

le dispositif électronique réalisant ladite vérification lors de ladite détermination (A6) pour déterminer si ladite modification requise entraîne, si elle est appliquée, une dégradation de la sécurité du dispositif.

4. Procédé selon l'une quelconque des revendications 1 à 3, dans lequel, le dispositif électronique vérifie (A24) si ledit nouvel état (V2) est supérieur ou inférieur à l'état initial (V1) dudit au moins un paramètre (PR),

et détermine (A6), à partir de ladite vérification, si ladite modification requise entraîne, si elle est appliquée, une dégradation de la sécurité du dispositif électronique.

5. Procédé selon la revendication 4, dans lequel le dispositif électronique détermine (A26) que ladite modification requise par la première commande entraîne, si elle est appliquée, une dégradation de la sécurité du dispositif électronique, si l'écart de valeur entre le nouvel état (V2) et l'état initial (V1) dudit au moins un paramètre (PR) atteint une valeur seuil prédéfinie (Lmax).

6. Procédé selon l'une quelconque des revendications 1 à 5, dans lequel ladite au moins une opération de sécurisation comprend au moins l'un quelconque parmi :

- enregistrement d'un message (MSG1) à envoyer, ledit message informant de la réception de ladite première commande (CMD1) ;
- envoi (A30) dudit message (MSG1) ;
- enregistrement (A32) de l'état initial (V1) dudit au moins un paramètre de fonctionnement (PR) ;
- application (A32) de ladite modification audit au moins un paramètre de fonctionnement de sorte à passer son état de l'état initial (V1) au nouvel état (V2) ; et
- enregistrement, dans un fichier d'historisation, d'une donnée représentative de la réception de ladite première commande (CMD1).

7. Procédé selon la revendication 6, dans lequel, suite audit enregistrement (A32) de l'état initial (V1) et à l'application (A32) de la modification causant le passage dudit au moins un paramètre de fonctionnement (PR) de l'état initial (V1) au nouvel état (V2), le dispositif électronique (C2) restaure l'état initial (V1) ou un état prédéfini dudit au moins un paramètre de fonctionnement en réponse à une commande de restauration (CMD2).

8. Procédé selon la revendication 7, dans lequel le dispositif électronique reçoit ladite première commande (CMD1) lors d'une première transaction (TR1) mise en œuvre par le dispositif électronique, et dans lequel

le dispositif électronique reçoit la commande de restauration (CMD2) lors d'une seconde transaction (TR2) mise en œuvre par le dispositif électronique, ladite seconde transaction étant subséquente à la première transaction.

9. Procédé selon l'une quelconque des revendications 1 à 8, dans lequel la première commande (CMD1) comprend un cryptogramme de type MAC.

10. Procédé selon l'une quelconque des revendications 1 à 9, dans lequel la première commande (CMD1) est une commande PUT DATA selon la norme ISO 7816, ladite première commande commandant l'affectation du nouvel état (V2) audit au moins un paramètre de fonctionnement (PR).

11. Procédé selon l'une quelconque des revendications 1 à 10, dans lequel le dispositif électronique (C2) est une carte à puce apte à mettre en œuvre une transaction (TR1, TR2) en coopération avec un terminal de lecture (T2).

12. Procédé selon la revendication 11, dans lequel le dispositif électronique est une carte EMV,

l'une au moins parmi les première commande et deuxième commande (CMD1, CMD2) étant une commande de script reçue (A2), lors d'une transaction EMV (TR1), après l'envoi, par ladite carte EMV, d'un message ARQC conforme à la norme EMV.

13. Procédé selon l'une quelconque des revendications 1 à 12, dans lequel ladite première commande inclut le nouvel état (V2) à affecter audit au moins un paramètre de fonctionnement.

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

15. Dispositif électronique (C2), comprenant :

- un module de réception (MD2) d'une première commande (CMD ; CMD1) requérant une modification d'au moins un paramètre de fonctionnement (PR) du dispositif électronique ;
- un module de détection (MD4) pour détecter si ledit au moins un paramètre de fonctionnement est un paramètre prédéfini en tant que paramètre sensible dans le dispositif électronique ;
- un module de détermination (MD6) configuré, en cas de résultat positif de ladite détection par le module de détection (MD4), pour déterminer si ladite modification requise par la première commande entraîne, si elle est appliquée, une dégradation de la sécurité du dispositif électronique en comparant l'état initial (V1) dudit au moins un paramètre (PR) à réception de ladite première commande avec un nouvel état (V2) à affecter audit au moins un paramètre de fonctionnement en réponse à la première commande ; et

- un module de sécurisation (MD8) configuré, en cas de résultat positif de ladite détermination par le module de détermination (MD6), pour déclencher au moins une opération de sécurisation prédéfinie du dispositif électronique en réponse à ladite première commande.

5

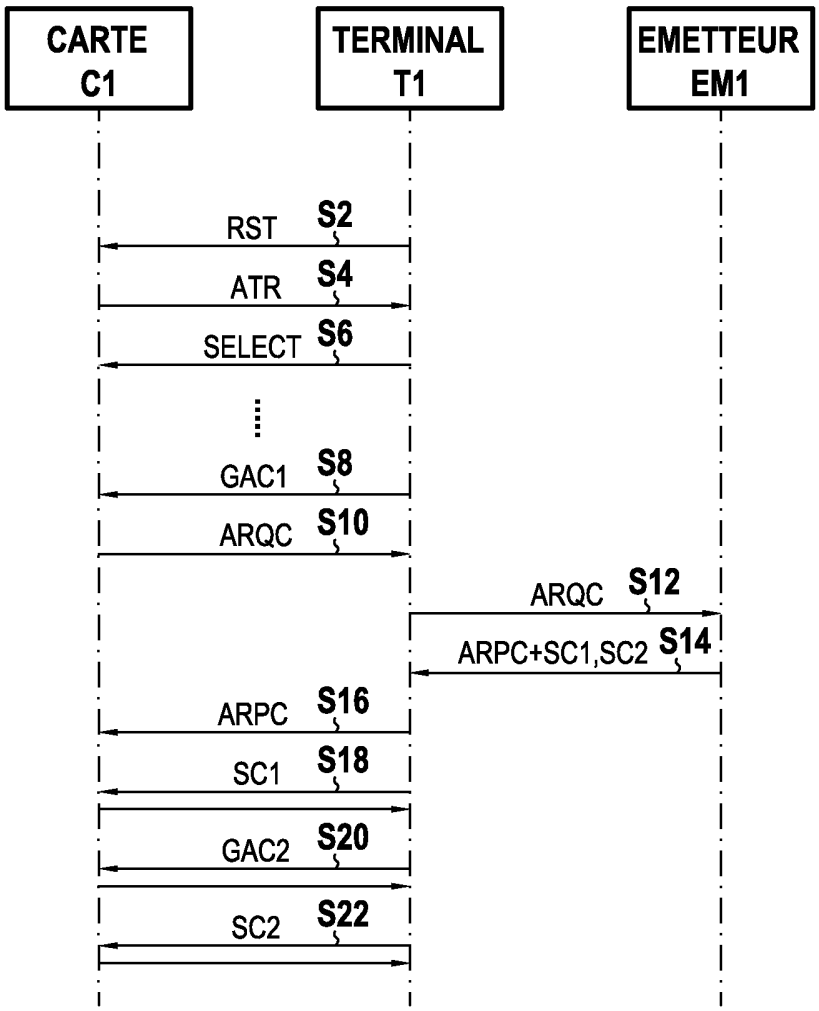

CARTE C1
TERMINAL T1
EMETTEUR EM1
RST S2
ATR S4
SELECT S6
GAC1 S8
ARQC S10
ARQC S12
ARPC+SC1,SC2 S14
ARPC S16
SC1 S18
GAC2 S20
SC2 S22

FIG.1

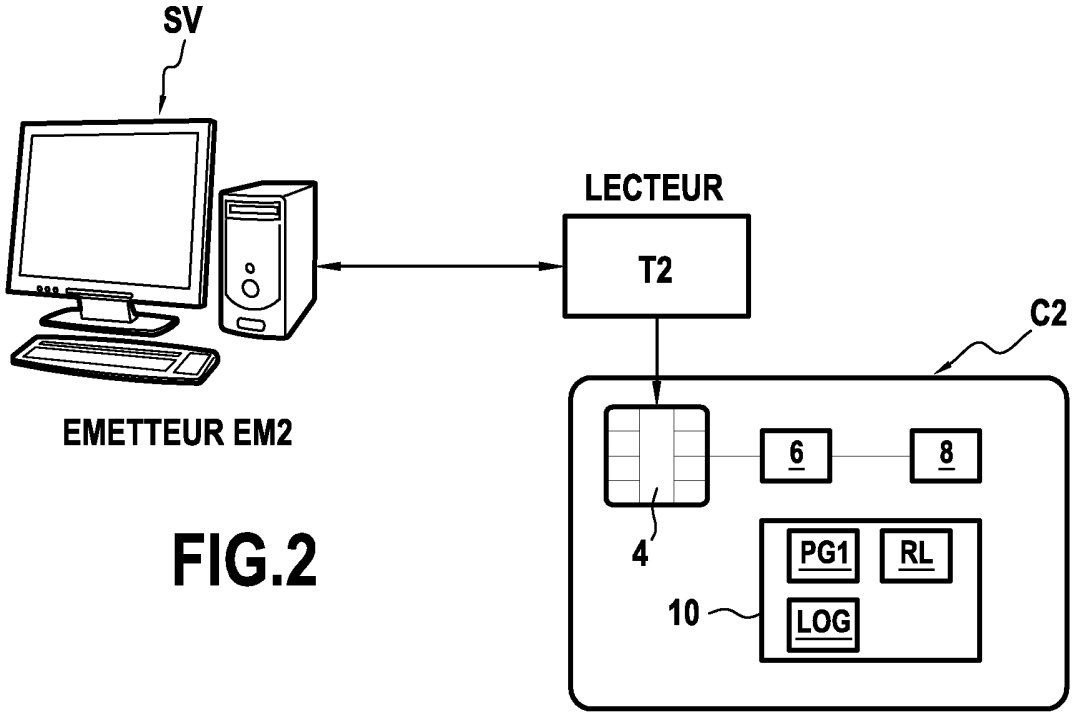

SV
LECTEUR
T2
C2
EMETTEUR EM2
6
8
4
PG1
RL
10
LOG

FIG.2

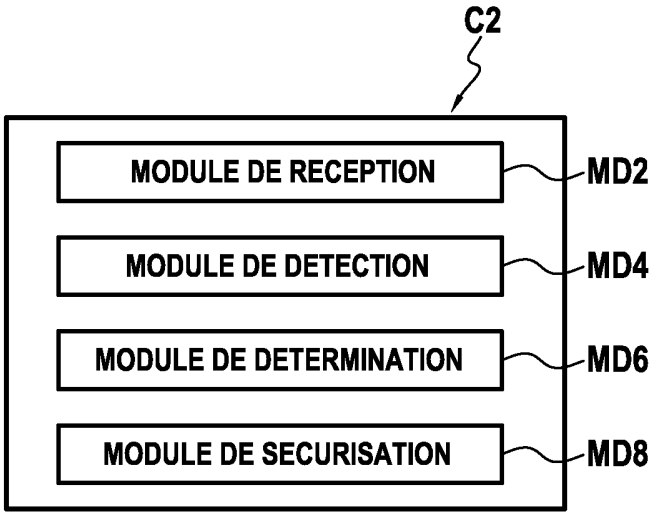


FIG.3

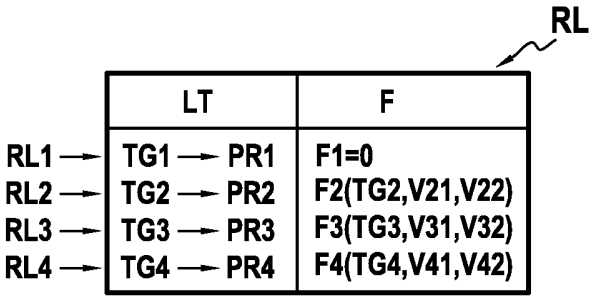


FIG.4

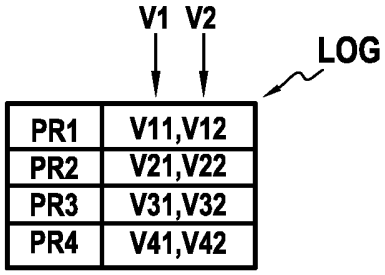


FIG.5

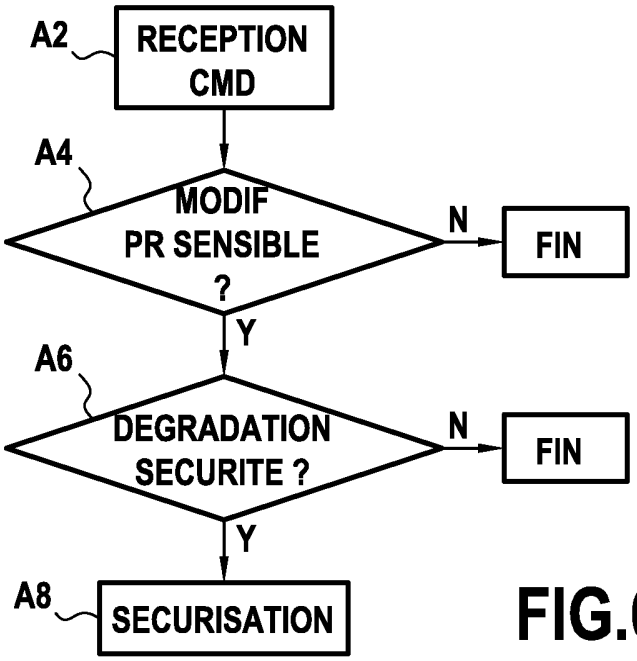


FIG.6

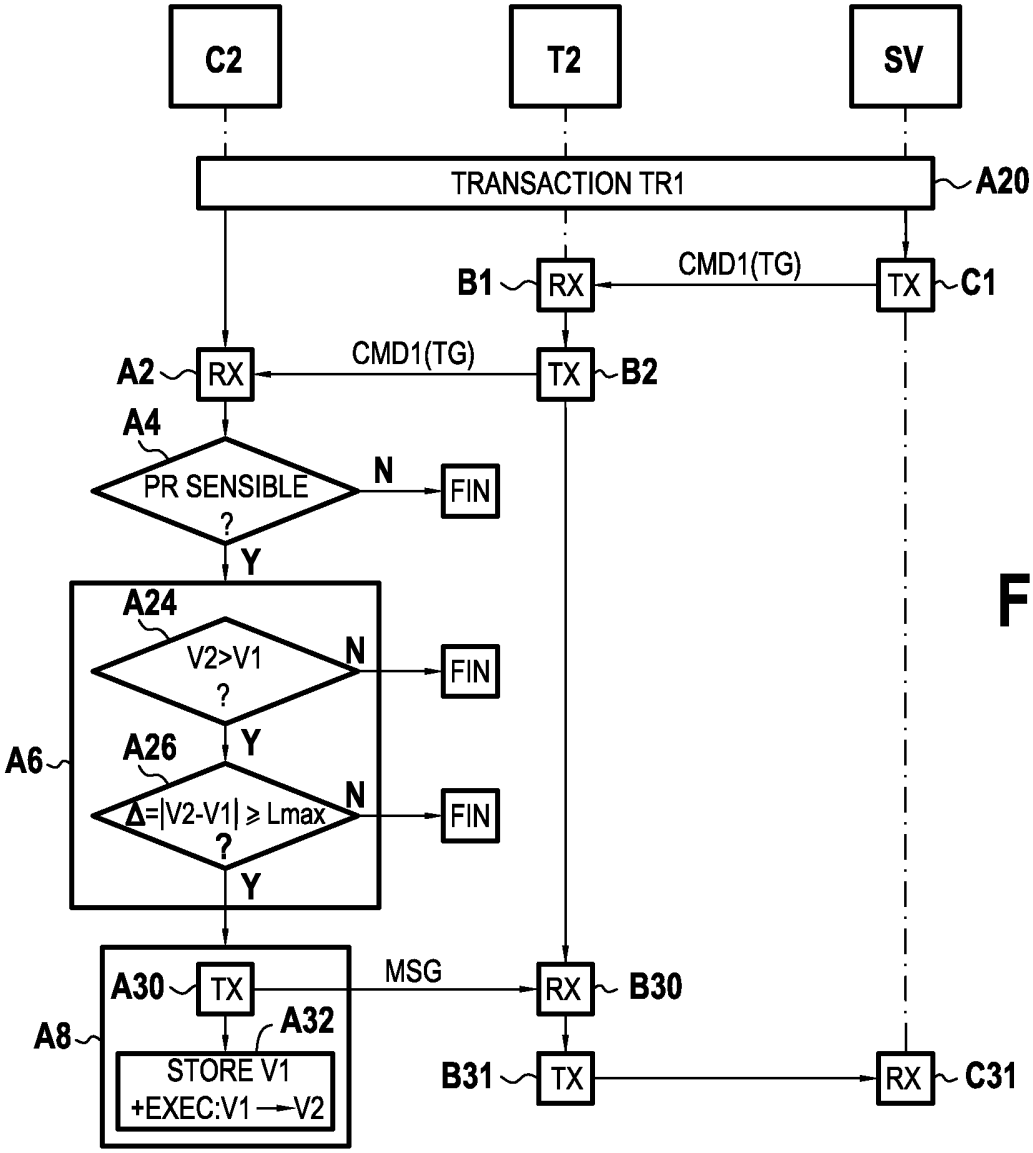

C2
T2
SV
TRANSACTION TR1
A20
B1
RX
CMD1(TG)
TX
C1
A2
RX
CMD1(TG)
TX
B2
A4
PR SENSIBLE ?
N
FIN
Y
A24
V2>V1 ?
N
FIN
Y
A6
A26
Δ=|V2-V1| ≥ Lmax ?
N
FIN
Y
A30
TX
MSG
RX
B30
A8
A32
STORE V1
+EXEC:V1→V2
B31
TX
RX
C31

FIG.7

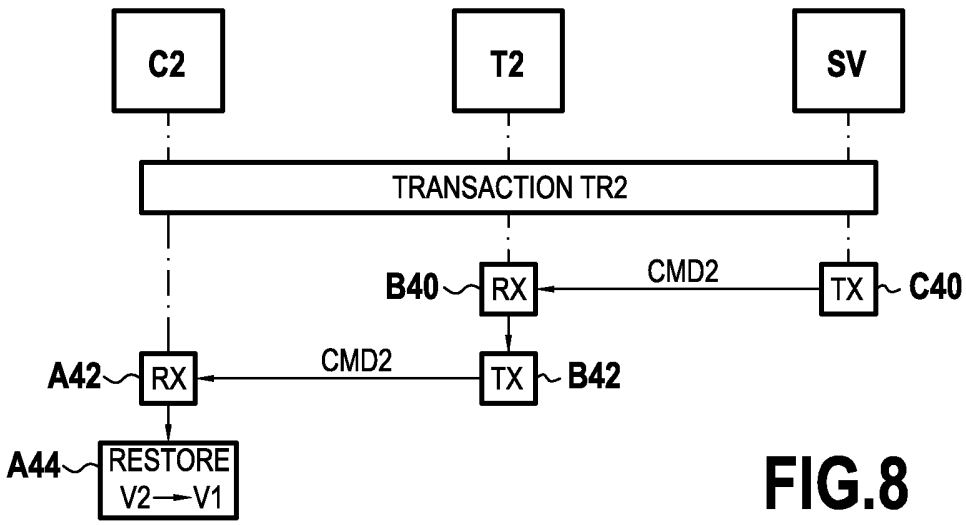

C2
T2
SV
TRANSACTION TR2
B40
RX
CMD2
TX
C40
A42
RX
CMD2
TX
B42
A44
RESTORE
V2→V1

FIG.8

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 827643
FR 1654122

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	US 2014/324698 A1 (DOLCINO LUC [CA] ET AL) 30 octobre 2014 (2014-10-30) * abrégé * * alinéas [0003] - [0013] * * alinéas [0034] - [0040] * * alinéa [0074]; figures 8a,8b * -----	1-15	G06Q20/34 G06F21/31
A	US 2013/119130 A1 (BRAAMS HARM [NL]) 16 mai 2013 (2013-05-16) * abrégé * * alinéas [0005] - [0037] * * alinéas [0047] - [0062]; figure 1 * * alinéas [0085], [0086] * * alinéa [0095] * -----	1-15	
A	WO 2010/070539 A1 (NXP BV [NL]; LAM ALISTER [GB]) 24 juin 2010 (2010-06-24) * abrégé * * page 1, ligne 1 - page 4, ligne 31 * * page 5, ligne 18 - page 14, ligne 7 * -----	1-15	
A	US 2011/185435 A1 (CHANG CHING-WEN [TW]) 28 juillet 2011 (2011-07-28) * abrégé * * alinéas [0008] - [0019] * * alinéas [0079] - [0085]; figure 6 * -----	1,14,15	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06Q G07F
A	WO 02/39222 A2 (WAVE SYS CORP [US]) 16 mai 2002 (2002-05-16) * abrégé * * page 2, ligne 29 - page 5, ligne 10 * -----	1,14,15	
A	EP 2 407 920 A1 (XIRING [FR]; CIRRA [FR]; MONECAM [FR]) 18 janvier 2012 (2012-01-18) * abrégé * * alinéas [0001] - [0013] * -----	1,14,15	
	-/--		

1

Date d'achèvement de la recherche	Examinateur
10 janvier 2017	Dedek, Frédéric

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 827643
FR 1654122

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	US 2009/259588 A1 (LINDSAY JEFFREY DEAN [US]) 15 octobre 2009 (2009-10-15) * abrégé * * alinéa [0009] * * alinéas [0019] - [0064] * * alinéas [0191] - [0194]; figure 15 * * alinéa [0297] * -----	1,14,15	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)

Date d'achèvement de la recherche	Examinateur
10 janvier 2017	Dedek, Frédéric

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

1

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1654122 FA 827643

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 10-01-2017
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2014324698 A1	30-10-2014	AU 2013225577 A1	25-09-2014
		CA 2860987 A1	06-09-2013
		CA 2881429 A1	06-09-2013
		CN 104145285 A	12-11-2014
		EP 2820601 A1	07-01-2015
		JP 2015513738 A	14-05-2015
		KR 20140137400 A	02-12-2014
		RU 2014138935 A	20-04-2016
		US 2014324698 A1	30-10-2014
		US 2016132861 A1	12-05-2016
		WO 2013126996 A1	06-09-2013
US 2013119130 A1	16-05-2013	CN 104040555 A	10-09-2014
		EP 2780854 A2	24-09-2014
		RU 154072 U1	10-08-2015
		RU 2014124198 A	27-12-2015
		US 2013119130 A1	16-05-2013
		WO 2013074631 A2	23-05-2013
WO 2010070539 A1	24-06-2010	CN 102257540 A	23-11-2011
		EP 2380149 A1	26-10-2011
		US 2011251955 A1	13-10-2011
		WO 2010070539 A1	24-06-2010
US 2011185435 A1	28-07-2011	TW 201126530 A	01-08-2011
		US 2011185435 A1	28-07-2011
		US 2012331218 A1	27-12-2012
WO 0239222 A2	16-05-2002	AU 2018202 A	21-05-2002
		AU 3950002 A	03-06-2002
		BR 0107346 A	09-02-2005
		BR 0114768 A	09-12-2003
		CN 1439136 A	27-08-2003
		CN 1470112 A	21-01-2004
		EP 1327321 A2	16-07-2003
		EP 1328891 A2	23-07-2003
		JP 2004513585 A	30-04-2004
		JP 2004515117 A	20-05-2004
		US 2002087860 A1	04-07-2002
		US 2002107804 A1	08-08-2002
		WO 0239222 A2	16-05-2002
		WO 0243309 A2	30-05-2002
EP 2407920 A1	18-01-2012	EP 2407920 A1	18-01-2012
		FR 2962830 A1	20-01-2012

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1654122 FA 827643

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 10-01-2017
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2009259588 A1	15-10-2009	US 2007250920 A1	25-10-2007
		US 2009259588 A1	15-10-2009

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 827643
FR 1654122

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	US 2014/324698 A1 (DOLCINO LUC [CA] ET AL) 30 octobre 2014 (2014-10-30) * abrégé * * alinéas [0003] - [0013] * * alinéas [0034] - [0040] * * alinéa [0074]; figures 8a,8b * -----	1-15	G06Q20/34 G06F21/31
A	US 2013/119130 A1 (BRAAMS HARM [NL]) 16 mai 2013 (2013-05-16) * abrégé * * alinéas [0005] - [0037] * * alinéas [0047] - [0062]; figure 1 * * alinéas [0085], [0086] * * alinéa [0095] * -----	1-15	
A	WO 2010/070539 A1 (NXP BV [NL]; LAM ALISTER [GB]) 24 juin 2010 (2010-06-24) * abrégé * * page 1, ligne 1 - page 4, ligne 31 * * page 5, ligne 18 - page 14, ligne 7 * -----	1-15	
A	US 2011/185435 A1 (CHANG CHING-WEN [TW]) 28 juillet 2011 (2011-07-28) * abrégé * * alinéas [0008] - [0019] * * alinéas [0079] - [0085]; figure 6 * -----	1,14,15	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06Q G07F
A	WO 02/39222 A2 (WAVE SYS CORP [US]) 16 mai 2002 (2002-05-16) * abrégé * * page 2, ligne 29 - page 5, ligne 10 * -----	1,14,15	
A	EP 2 407 920 A1 (XIRING [FR]; CIRRA [FR]; MONECAM [FR]) 18 janvier 2012 (2012-01-18) * abrégé * * alinéas [0001] - [0013] * -----	1,14,15	
	-/--		

1

Date d'achèvement de la recherche	Examinateur
10 janvier 2017	Dedek, Frédéric

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 827643
FR 1654122

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	US 2009/259588 A1 (LINDSAY JEFFREY DEAN [US]) 15 octobre 2009 (2009-10-15) * abrégé * * alinéa [0009] * * alinéas [0019] - [0064] * * alinéas [0191] - [0194]; figure 15 * * alinéa [0297] * -----	1,14,15	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)

Date d'achèvement de la recherche	Examinateur
10 janvier 2017	Dedek, Frédéric

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

1

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1654122 FA 827643

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 10-01-2017
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2014324698 A1	30-10-2014	AU 2013225577 A1	25-09-2014
		CA 2860987 A1	06-09-2013
		CA 2881429 A1	06-09-2013
		CN 104145285 A	12-11-2014
		EP 2820601 A1	07-01-2015
		JP 2015513738 A	14-05-2015
		KR 20140137400 A	02-12-2014
		RU 2014138935 A	20-04-2016
		US 2014324698 A1	30-10-2014
		US 2016132861 A1	12-05-2016
		WO 2013126996 A1	06-09-2013
US 2013119130 A1	16-05-2013	CN 104040555 A	10-09-2014
		EP 2780854 A2	24-09-2014
		RU 154072 U1	10-08-2015
		RU 2014124198 A	27-12-2015
		US 2013119130 A1	16-05-2013
		WO 2013074631 A2	23-05-2013
WO 2010070539 A1	24-06-2010	CN 102257540 A	23-11-2011
		EP 2380149 A1	26-10-2011
		US 2011251955 A1	13-10-2011
		WO 2010070539 A1	24-06-2010
US 2011185435 A1	28-07-2011	TW 201126530 A	01-08-2011
		US 2011185435 A1	28-07-2011
		US 2012331218 A1	27-12-2012
WO 0239222 A2	16-05-2002	AU 2018202 A	21-05-2002
		AU 3950002 A	03-06-2002
		BR 0107346 A	09-02-2005
		BR 0114768 A	09-12-2003
		CN 1439136 A	27-08-2003
		CN 1470112 A	21-01-2004
		EP 1327321 A2	16-07-2003
		EP 1328891 A2	23-07-2003
		JP 2004513585 A	30-04-2004
		JP 2004515117 A	20-05-2004
		US 2002087860 A1	04-07-2002
		US 2002107804 A1	08-08-2002
		WO 0239222 A2	16-05-2002
		WO 0243309 A2	30-05-2002
EP 2407920 A1	18-01-2012	EP 2407920 A1	18-01-2012
		FR 2962830 A1	20-01-2012

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1654122 FA 827643

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 10-01-2017
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2009259588 A1	15-10-2009	US 2007250920 A1	25-10-2007
		US 2009259588 A1	15-10-2009

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82