(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 099 272***

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

(21) **N° d'enregistrement national :** **19 08410**

(51) Int Cl[8] : ***G 06 Q 20/40*** *(2019.01), G 06 Q 20/16, 20/34, G 06 F 21/44*

(12) **DEMANDE DE BREVET D'INVENTION** **A1**

(22) **Date de dépôt :** 24.07.19.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 29.01.21 Bulletin 21/04.

(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) :** *IDEMIA FRANCE Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** TRUBERT Rozenn et DE OLIVEIRA Marco.

(73) **Titulaire(s) :** IDEMIA FRANCE Société par actions simplifiée.

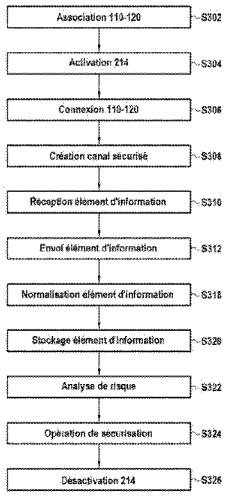
(74) **Mandataire(s) :** Cabinet Beau de Loménie.

(54) **Procédé de sécurisation, et dispositif électronique associé.**

(57) P rocédé de sécurisation, et dispositif électronique associé

L'invention concerne essentiellement un procédé de sécurisation, mis en œuvre par un premier dispositif électronique, ledit procédé comprenant les étapes suivantes : - réception (S310) d'au moins un élément d'information concernant une transaction passée mise en œuvre par un deuxième dispositif électronique, envoyé par le deuxième dispositif électronique, - analyse de risque (S322) à partir dudit au moins un élément d'information, afin de détecter une utilisation anormale du premier dispositif électronique et du deuxième dispositif électronique, et - dans l'affirmative, déclenchement (S324) d'au moins une opération de sécurisation du premier dispositif électronique.

Figure pour l'abrégé : Fig. 3.



FR 3 099 272 - A1

Description

Titre de l'invention : Procédé de sécurisation, et dispositif électronique associé

Domaine technique

[0001] La présente invention se rapporte au domaine de la sécurisation de transactions mises en œuvre par des dispositifs électroniques, et concerne plus particulièrement un procédé de sécurisation mis en œuvre par 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.

[0002] 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 de transactions réalisées par une carte à puce fonctionnant selon le protocole EMV (pour « Europay Mastercard Visa »).

Technique antérieure

[0003] De manière générale, une carte à puce est conçue pour communiquer avec un dispositif externe à cette carte, autrement appelé terminal ou lecteur. Les cartes à puce 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.

[0004] De façon connue, certains mécanismes permettent de détecter des comportements anormaux d'utilisation d'une carte à puce en utilisant un historique de transactions de cette carte, et permettent alors de protéger la carte contre ces comportements anormaux. Il est ainsi possible de détecter un nombre de retrait bancaire important pendant une durée limitée, et de réagir en fonction du nombre de retrait. Par exemple, une alerte peut être émise si trois retraits sont réalisés en moins de cinq minutes, un retrait peut être refusé si cinq retraits sont réalisés pendant cette durée, et/ou toute transaction peut être bloquée si dix retraits sont réalisés pendant cette durée.

[0005] Cependant, certaines utilisations anormales ne peuvent être détectées efficacement par ces mécanismes, telles que par exemple des utilisations impliquant plusieurs cartes à puces. Il est en effet courant que plusieurs cartes à puce soient liées, en étant associées à un même compte bancaire et/ou un même porteur de carte. Ces cartes peuvent alors être utilisées de manière alternative pour la réalisation de plusieurs transactions.

[0006] Un comportement frauduleux de commerçant difficilement détectable consiste par

exemple à déclarer qu'une première transaction impliquant une première carte a échoué alors que cela n'est pas le cas, de sorte à forcer la réalisation d'une deuxième transaction au moyen d'une deuxième carte liée à la première.

[0007] Un autre comportement frauduleux difficilement détectable consiste par exemple à réaliser plusieurs transactions avec des cartes différentes suite au vol de ces cartes, par exemple suite au vol d'un portefeuille contenant ces cartes. Des transactions sans contact ou avec contact peuvent par exemple être réalisées, ou des tentatives de transactions avec contact durant lesquelles plusieurs codes PIN sont soumis.

[0008] L'invention vise à pallier les problèmes et inconvénients mentionnés ci-dessus et vise plus généralement à protéger efficacement un dispositif électronique contre des comportements d'utilisation anormaux ou frauduleux, c'est-à-dire à protéger le dispositif électronique contre de tels comportements sans baisser la sécurité des données personnelles de l'utilisateur du dispositif, avec un coût relativement faible et un minimum d'intervention de l'utilisateur, et en limitant l'impact de la protection sur le temps de transaction.

Exposé de l'invention

[0009] La présente invention concerne un procédé de sécurisation, mis en œuvre par un premier dispositif électronique, ledit procédé comprenant les étapes suivantes :

- réception d'au moins un élément d'information concernant une transaction passée mise en œuvre par un deuxième dispositif électronique, envoyé par le deuxième dispositif électronique,
- analyse de risque à partir dudit au moins un élément d'information, afin de détecter une utilisation anormale du premier dispositif électronique et du deuxième dispositif électronique, et
- dans l'affirmative, déclenchement d'au moins une opération de sécurisation du premier dispositif électronique.

[0010] L'invention permet ainsi de protéger efficacement le premier dispositif électronique contre des comportements d'utilisation anormaux tels que des utilisations frauduleuses.

[0011] Dans un mode de réalisation particulier, ledit au moins un élément d'information est reçu directement depuis le deuxième dispositif électronique.

[0012] Dans un mode de réalisation particulier, le procédé comprend en outre l'étape suivante :

- création d'un canal sécurisé entre le premier dispositif électronique et le deuxième dispositif électronique,

ledit au moins un élément d'information étant reçu via le canal sécurisé.

[0013] La création d'un canal sécurisé permet de protéger encore plus efficacement le premier dispositif électronique.

[0014] Dans un mode de réalisation particulier, le procédé comprend en outre l'étape suivante :

- activation d'une interface de communication suite à un événement d'activation.

[0015] Dans un mode de réalisation particulier, le procédé comprend en outre l'étape suivante :

- désactivation de l'interface de communication à la fin d'une durée prédéfinie décomptée à partir d'un événement de désactivation.

[0016] Cette gestion particulière de l'interface de communication permet par exemple au premier dispositif électronique de détecter le deuxième dispositif électronique lors d'une transaction, mais aussi pendant une durée supplémentaire après la transaction, cette durée supplémentaire étant prédéfinie en fonction de cas d'utilisations anormales. Cela permet de protéger au mieux le premier dispositif électronique et le deuxième dispositif électronique. En outre, la désactivation de l'interface de communication à la fin de la durée prédéfinie permet d'économiser de l'énergie.

[0017] Dans un mode de réalisation particulier, le procédé comprend en outre l'étape suivante, mise en œuvre avant l'étape de réception dudit au moins un élément d'information :

- stockage d'un identifiant du deuxième dispositif électronique, de sorte à associer le premier dispositif électronique et le deuxième dispositif électronique.

[0018] L'association du premier dispositif électronique et du deuxième dispositif électronique permet de protéger encore plus efficacement le premier dispositif électronique et le deuxième dispositif électronique, puisqu'elle permet de cibler des dispositifs ayant un lien entre eux.

[0019] Dans un mode de réalisation particulier, le procédé comprend en outre l'étape suivante, mise en œuvre avant l'étape de réception dudit au moins un élément d'information :

- envoi au deuxième dispositif électronique d'une requête d'obtention d'information de transaction passée.

[0020] Dans un mode de réalisation particulier, le procédé comprend en outre l'étape suivante :

- envoi d'au moins un élément d'information concernant une transaction passée mise en œuvre par le premier dispositif électronique, au deuxième dispositif électronique.

[0021] Cet envoi permet de synchroniser les deux dispositifs de sorte que chaque dispositif soit apte à détecter une utilisation anormale, et permet ainsi d'améliorer l'efficacité de la protection de chaque dispositif.

[0022] Dans un mode de réalisation particulier, chaque opération de sécurisation est une des opérations parmi les opérations suivantes :

- envoi d'un message informant de ladite utilisation anormale détectée,

- modification d'au moins un paramètre de fonctionnement du premier dispositif électronique,
- envoi d'un message de modification d'au moins un paramètre de fonctionnement,
- enregistrement, dans un historique de transactions du premier dispositif électronique, d'une donnée de sécurité représentative de ladite utilisation anormale détectée, et
- refus de mettre en œuvre une transaction courante au moyen du premier dispositif électronique.

[0023] Dans un mode de réalisation particulier, le procédé est mis en œuvre après une initialisation d'une transaction courante mise en œuvre par le premier dispositif électronique, dans lequel :

- ledit élément d'information concernant la transaction passée provient d'un historique de transactions du deuxième dispositif électronique, et comprend une date de la transaction passée,
- l'analyse de risque comprend la comparaison de la date de la transaction passée à une date courante, une utilisation anormale étant détectée si la durée entre la date de la transaction passée et la date courante est inférieure à une durée prédéfinie.

[0024] Dans un mode de réalisation particulier, le procédé comprend en outre les étapes suivantes :

- réception d'une donnée de configuration,
- modification d'un paramètre de configuration du premier dispositif électronique en fonction de ladite donnée de configuration.

[0025] L'invention concerne de plus un dispositif électronique apte à mettre en œuvre le procédé de sécurisation tel que décrit ci-dessus et/ou le procédé de sécurisation tel que décrit ci-dessous.

[0026] Dans un mode particulier de réalisation, les différentes étapes du procédé tel que décrit ci-dessus sont déterminées par des instructions de programmes d'ordinateur.

[0027] 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 par un serveur 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 décrit ci-dessus et/ou le procédé de sécurisation tel que décrit ci-dessous.

[0028] 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 particulièrement compilée, ou dans n'importe quelle autre forme souhaitable.

[0029] L'invention vise aussi un support d'information (ou support d'enregistrement) lisible par un serveur ou plus généralement par un ordinateur, et comportant des instructions

d'un programme d'ordinateur tel que mentionné ci-dessus.

[0030] 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 mémoire non volatile réinscriptible (de type « EEPROM » ou « Flash NAND » par exemple), ou 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.

[0031] 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.

[0032] 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.

[0033] L'invention concerne en outre un procédé de sécurisation mis en œuvre par un deuxième dispositif électronique, ledit procédé comprenant l'étape suivante :

- envoi d'au moins un élément d'information concernant une transaction passée mise en œuvre par le deuxième dispositif électronique,

de sorte que le premier dispositif électronique soit apte mettre en œuvre une analyse de risque à partir dudit au moins un élément d'information, afin de détecter une utilisation anormale du premier dispositif électronique et du deuxième dispositif électronique, et, dans l'affirmative, déclencher d'au moins une opération de sécurisation du premier dispositif électronique.

Brève description des dessins

[0034] D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent un exemple de réalisation dépourvu de tout caractère limitatif. Sur les figures :

[0035] [fig.1] La figure 1 représente, de manière schématique, un système comprenant un premier dispositif électronique conforme à un exemple de mode de réalisation de l'invention ;

[0036] [fig.2] La figure 2 représente, de manière schématique, le premier dispositif électronique du système de la figure 1 ;

[0037] [fig.3] La figure 3 représente, sous forme d'un organigramme, les principales étapes d'un procédé de sécurisation conforme à un exemple de mode de réalisation de l'invention ;

[0038] [fig.4] La figure 4 représente, de manière schématique, un exemple de structure de données utilisée par le premier dispositif électronique de la figure 2 ;

[0039] [fig.5A] La figure 5A représente, de manière schématique, des étapes d'un procédé de sécurisation conforme à un exemple de mode de réalisation de l'invention ;

[0040] [fig.5B] La figure 5B représente, de manière schématique, des étapes d'un procédé de sécurisation conforme à un exemple de mode de réalisation de l'invention ;

[0041] [fig.6] La figure 6 représente, de manière schématique, un exemple de mise en œuvre d'un procédé de sécurisation conforme à un exemple de mode de réalisation de l'invention.

Description des modes de réalisation

[0042] La **figure 1** représente, de manière schématique, un système 100 comprenant un premier dispositif électronique 110 conforme à un exemple de mode de réalisation de l'invention, apte à mettre en œuvre un procédé de sécurisation conforme à un exemple de mode de réalisation, par exemple un des procédés décrits en référence aux figures 3 à 6.

[0043] Le système 100 comprend en outre un deuxième dispositif électronique 120 conforme à un exemple de mode de réalisation de l'invention, apte à mettre en œuvre un procédé de sécurisation conforme à un exemple de mode de réalisation, par exemple un des procédés décrits en référence aux figures 3 à 6.

[0044] Le premier dispositif électronique 110 et le deuxième dispositif électronique 120 sont typiquement aptes à communiquer entre eux au moyen d'un premier réseau de télécommunications 130.

[0045] Le premier réseau de télécommunications 130 est typiquement un réseau Bluetooth, un réseau Bluetooth à basse consommation (BLE pour « Bluetooth Low Energy », en terminologie anglo-saxonne), un réseau NFC (acronyme de « Near Field Communication », en terminologie anglo-saxonne), ou encore un réseau LoRaWAN (acronyme de « Long Range Wide-Area Network », en terminologie anglo-saxonne).

[0046] Chacun des premier et deuxième dispositifs électroniques 110, 120 est apte à coopérer avec un terminal 140 de transaction (ou lecteur) afin de traiter une transaction.

[0047] La transaction peut être une transaction bancaire (i.e. une transaction de paiement, un prélèvement, etc.), par exemple selon le protocole EMV, ou encore une authentification de l'utilisateur du dispositif (par exemple un contrôle d'accès).

[0048] Le premier dispositif électronique 110 et le terminal 140 sont typiquement aptes à communiquer entre eux via un deuxième réseau de télécommunications 150, ou directement au moyens de contacts lorsque le premier dispositif électronique 110 est inséré dans le terminal 140. De même, le deuxième dispositif électronique 120 et le terminal 140 peuvent communiquer entre eux via le deuxième réseau de télécommunications 150, ou directement au moyens de contacts lorsque le deuxième dispositif

électronique 120 est inséré dans le terminal 140.

[0049] Le deuxième réseau de télécommunication 150 est typiquement un réseau de courte portée, tel qu'un réseau NFC. Le deuxième réseau de télécommunications 150 et le premier réseau de télécommunications 130 peuvent former un même réseau de télécommunications, ou être deux réseaux distincts.

[0050] Chaque dispositif électronique 110, 120 peut être une carte à puce, par exemple une carte bancaire (ou carte de paiement) de format ID-1 spécifiée dans la norme ISO/IEC 7810, présentant les dimensions 85,6 millimètres par 53,98 millimètres par 0,76 millimètres.

[0051] La carte à puce 110, 120 peut être une carte à puce avec contacts dont les caractéristiques sont détaillées dans la norme ISO/IEC 7816, et/ou une carte à puce sans contact dont les caractéristiques sont détaillées dans la norme ISO/IEC 14443 ou NFC/ISO 15693.

[0052] Chaque dispositif électronique 110, 120 peut être en variante toute carte (une carte de transport, une carte d'accès, une carte d'assurance maladie, une carte d'identité, une carte de vote, une carte de permis de conduire, etc.) configurée pour stocker des données sensibles (par exemple des données d'identité, des données bancaires) et pour réaliser des transactions impliquant de telles données (e.g. une transaction pour effectuer un vote électronique, une transaction permettant l'accès à des données d'identité du dispositif électronique, une transaction pour obtenir un accès physique ou logique, etc.).

[0053] Chaque dispositif électronique 110, 120 peut aussi être un terminal fixe ou mobile tel qu'un téléphone portable, par exemple de type « smartphone », une tablette numérique, ou un ordinateur personnel.

[0054] Comme le montre la **figure 2**, le premier dispositif électronique 110 comprend une première puce électronique 211 connectée électriquement à une première interface de communication 212. Le premier dispositif électronique 110 peut aussi comprendre une deuxième puce électronique 213 connectée électriquement à une deuxième interface de communications 214, et éventuellement à une batterie 215.

[0055] La deuxième puce électronique 213 est connectée électriquement, directement ou indirectement à la première puce électronique 211. La communication entre la première puce électronique 211 et la deuxième puce électronique 213 peut être mise en œuvre via un canal de communication sécurisé.

[0056] La première puce électronique 211 est notamment apte à mettre en œuvre une transaction sécurisée, typiquement selon le protocole EMV, en communiquant avec le terminal 140 de transaction via la première interface de communications 212. La communication peut être une communication sans contact via le deuxième réseau de télécommunications 150, la première interface de communication 212 comprenant alors

une antenne radiofréquence, ou une communication par contact, la première interface de communication 212 comprenant alors des plages de contacts positionnés sur la surface externe du premier dispositif électronique 110.

[0057] La première puce électronique 211 comprend un premier processeur 216 et une première mémoire 217 non-volatile.

[0058] La première mémoire 217 est une mémoire non-volatile réinscriptible, cette première mémoire 217 constituant un support d'enregistrement (ou support d'informations) conforme à un mode de réalisation particulier, lisible par le premier processeur 216, et sur lequel est enregistré un premier programme d'ordinateur P1 conforme à un mode de réalisation particulier. En variante, le premier programme P1 est enregistré dans une mémoire morte (ROM) (non représentée) de la première puce électronique 211.

[0059] En outre, une structure de données SD, un premier historique de transactions HT1 et éventuellement un deuxième historique de transactions HT2 peuvent être stockés dans la première mémoire 217 du premier dispositif électronique 110. La structure de données SD prend par exemple la forme d'une table.

[0060] Le premier historique de transactions HT1 est typiquement un fichier cyclique conforme à la norme ISO/IEC 7816-4. Le premier historique de transactions HT1 peut comprendre une ou plusieurs données de transaction concernant une ou plusieurs transactions mises en œuvre au moyen du premier dispositif électronique 110. Le contenu du premier historique de transactions HT1 peut être configurable.

[0061] Plus précisément, le premier historique de transactions HT1 peut comprendre un ou plusieurs ensembles de données (dits « records »), chaque ensemble concernant une transaction différente, et comprenant une ou plusieurs données de la transaction telles que le montant de la transaction, la monnaie utilisée pour la transaction, la date de la transaction comprenant l'heure de la transaction, le CVR (pour « Card Verification Result », en terminologie anglo-saxonne), et une donnée « Merchant data ».

[0062] Le CVR est une donnée structurée qui contient les résultats de toutes les vérifications faites par le premier dispositif électronique 110 lors de la transaction (e.g. PIN vérifié).

[0063] La donnée « Merchant data » indique par exemple le nom du marchand et/ou sa localisation et/ou le numéro SIRET. La donnée « Merchant data » prend par exemple la forme d'une donnée propriétaire master card dont l'identifiant est 9F7C (appelée « merchant custom data »), une donnée dont l'identifiant EMV est 9F4E (appelée « merchant name and location », ou encore une donnée dont l'identifiant EMV est 9F16 (appelée « merchant ID »).

[0064] En outre, chaque ensemble concernant une transaction peut comprendre des données sécuritaires concernant par exemple le blocage d'une interface, du code PIN ou d'une application, par exemple parmi les données suivantes qui peuvent être définies par la norme EMV :

- Identifiant de carte (PAN),
- Type d'application bancaire (VISA, MChip, CB…),
- L'identifiant de l'application (e.g. l'AID définie dans la norme ISO/IEC 7816)
- 9F01 Acquirer Identifier,
- 9F40 Additional Terminal Capabilities,
- 9F02 Amount, Authorised,
- 9F03 Amount, Other,
- 8A Authorization Response Code,
- 9F36 Application Transaction Counter (ATC),
- DF52 Card Verification Result,
- 9F27 Cryptogram Information Data,
- 9F34 CVM Results,
- DF3E Interface Identifier,
- 9F10 Issuer Application Data,
- 9F37 Issuer Authentication Data,
- 9F16 Merchant Identifier,
- 9F4E Merchant Name and Location,
- 9F33 Terminal Capabilities,
- 9F1A Terminal Country Code,
- 9F1C Terminal ID,
- 9F35 Terminal Type,
- 95 Terminal Verification Results (TVR),
- 5F2A Transaction Currency Code,
- 5F36 Transaction Currency Exponent,
- 9A Transaction Date,
- 9F41 Transaction Sequence Counter,
- 9B Transaction Status Information,
- 9F21 Transaction Time,
- 9C Transaction Type,
- 9F37 Unpredictable Number.

[0065] Le premier historique de transactions HT1 peut être ordonné de façon à ce que le premier ensemble de données corresponde à la transaction la plus récente et le dernier ensemble de données corresponde à la transaction la plus ancienne. Le premier historique de transactions HT1 est ainsi utilisé pour détecter un comportement suspicieux au niveau du premier dispositif électronique 110 et envoyer une alerte, par exemple à l'organisme émetteur du premier dispositif électronique 110 (tel qu'un établissement bancaire).

[0066] Le deuxième historique de transactions HT2 est une structure de données pouvant

aussi prendre la forme d'un fichier cyclique. Le deuxième historique de transactions HT2 peut comprendre une ou plusieurs données de transaction concernant une ou plusieurs transactions mises en œuvre par un ou plusieurs dispositifs électroniques autres que le premier dispositif électronique 110, par exemple le deuxième dispositif électronique 120. Les données peuvent être regroupées par ensembles de données, chaque ensemble de données correspondant à une transaction différente. Chaque ensemble de données peut alors comprendre l'identifiant du dispositif électronique au moyen duquel la transaction a été réalisée (ou mise en œuvre).

[0067] En variante, la première mémoire 217 stocke le premier historique de transactions HT1, le deuxième historique de transactions HT2, et un ou plusieurs autres historiques de transaction, de sorte que chaque historique de transactions soit associé à un dispositif électronique différent, chaque historique de transactions pouvant alors comprendre une ou plusieurs données de transaction concernant une ou plusieurs transactions mises en œuvre au moyen du dispositif électronique associé.

[0068] La deuxième puce électronique 213 est notamment apte à échanger des données avec le deuxième dispositif électronique 120, au moyen de la deuxième interface de communication 214, la batterie 215 et du premier réseau de télécommunications 130. La communication peut être une communication sans contact, la deuxième interface de communication 214 comprenant alors une antenne radiofréquence.

[0069] La deuxième puce électronique 213 comprend un deuxième processeur 218 et une deuxième mémoire 219 non-volatile.

[0070] La deuxième mémoire 219 est une mémoire non-volatile réinscriptible, cette deuxième mémoire 219 constituant un support d'enregistrement (ou support d'informations) conforme à un mode de réalisation particulier, lisible par le deuxième processeur 218, et sur lequel peut être enregistré un deuxième programme d'ordinateur P2 conforme à un mode de réalisation particulier. En variante, le deuxième programme P2 est enregistré dans une mémoire morte (ROM) (non représentée) de la deuxième puce électronique 213.

[0071] Le premier programme d'ordinateur P1 et le deuxième programme d'ordinateur P2 comportent ainsi collectivement des instructions pour l'exécution des étapes d'un procédé de sécurisation selon un mode de réalisation particulier, typiquement un des procédés décrits en référence aux figures 3 à 6.

[0072] La batterie 215 du premier dispositif électronique 110 est typiquement un supercondensateur, une pile ou une batterie rechargeable.

[0073] En variante, le premier dispositif électronique 110 ne comprend pas la deuxième puce électronique 213, la deuxième mémoire 219 et/ou la batterie 215. La première puce électronique 111 est alors apte à échanger des données avec le deuxième dispositif électronique 120 au moyen de la deuxième interface de communication 214.

[0074] Le deuxième dispositif électronique 120 peut présenter la même architecture matérielle que le premier dispositif électronique 110. La description de cette architecture faite en référence à la figure 2 pour le premier dispositif électronique 110 s'applique donc au deuxième dispositif électronique 120.

[0075] En outre, le terminal 120 peut aussi présenter l'architecture conventionnelle d'un ordinateur, et peut ainsi comporter un processeur, une mémoire morte (de type « ROM »), une mémoire non volatile réinscriptible (de type « EEPROM » ou « Flash NAND » par exemple), une mémoire volatile réinscriptible (de type « RAM »), et une interface de communication (non représenté).

[0076] Dans l'exemple de la figure 1, le système 100 comprend deux dispositifs électroniques 110 et 120 et un terminal 140. On comprendra cependant que, pour la mise en œuvre de l'invention, le système peut comprendre un ou plusieurs autres dispositifs électroniques et/ou terminaux.

[0077] La **figure 3** représente un procédé de sécurisation conforme à un exemple de mode de réalisation de l'invention, pouvant être mis en œuvre par le premier dispositif électronique 110.

[0078] Dans une étape S302, le premier dispositif électronique 110 peut obtenir un identifiant ID2 du deuxième dispositif électronique 120, puis stocker l'identifiant ID2 du deuxième dispositif électronique 120, de sorte à associer (ou lier) le premier dispositif électronique 110 et le deuxième dispositif électronique 120. Cette étape S302 est typiquement mise en œuvre par la première puce électronique 211 du premier dispositif électronique 110.

[0079] L'identifiant ID2 du deuxième dispositif électronique 120 est typiquement stocké dans la structure de données SD. L'identifiant ID2 du deuxième dispositif électronique 120 peut prendre la forme d'un index, c'est-à-dire d'un identifiant court, afin de minimiser l'espace de stockage et faciliter la recherche dans la structure de données SD.

[0080] L'identifiant ID2 du deuxième dispositif électronique 120 peut être stocké en association avec une ou plusieurs informations dans la structure de données SD, chaque information pouvant aussi être obtenue à l'étape S302. Ainsi, l'identifiant ID2 du deuxième dispositif électronique 120 peut être stocké en association avec (voir **figure 4**) :

- un statut ST2 décrivant l'état du lien d'association entre le premier dispositif électronique 110 et le deuxième dispositif électronique 120 (par exemple actif, désactivé, etc.),
- un identifiant (une adresse) AD2 du deuxième dispositif électronique sur le premier réseau de télécommunications 130,
- une ou plusieurs clés K2 de chiffrage et/ou signature et/ou authentification, ou un

ou plusieurs identifiants de clés de chiffrage et/ou signature et/ou authentification, utilisées pour la communication entre le premier dispositif électronique 110 et le deuxième dispositif électronique 120,
- des métadonnées ML2 qualifiant le type de lien d'association entre le premier dispositif électronique 110 et le deuxième dispositif électronique 120, et/ou
- des métadonnées MD2 définissant les droits d'accès aux données associées à l'identifiant du deuxième dispositif électronique 120.

[0081] Les métadonnées ML2 qualifiant le type de lien entre le premier dispositif électronique 110 et le deuxième dispositif électronique 120 indique par exemple si :
- le premier dispositif électronique 110 et le deuxième dispositif électronique 120 sont associés à un même compte bancaire, et/ou
- le premier dispositif électronique 110 et le deuxième dispositif électronique 120 sont associés à un même utilisateur, ou
- le premier dispositif électronique 110 et le deuxième dispositif électronique 120 sont associés à deux utilisateurs différents mais ayant un lien entre eux (lien familial, de tuteur ou encore de curatelle).

[0082] En outre, les métadonnées MD2 définissant les droits d'accès aux données associées à l'identifiant ID2 du deuxième dispositif électronique 120 indiquent par exemple si l'utilisateur du premier dispositif électronique 110 a le droit de lire et/ou modifier une ou plusieurs informations stockées en association avec l'identifiant ID2, et/ou de supprimer ou encore ajouter une association.

[0083] La structure de données SD peut bien entendu permettre de stocker un ou plusieurs identifiant, chaque identifiant correspondant à un dispositif électronique différent, et pouvant être en association avec une ou plusieurs informations susmentionnées.

[0084] L'identifiant ID2 du deuxième dispositif électronique 120 et la ou les éventuelles informations associées peuvent être obtenus pendant une phase de fabrication du premier dispositif électronique 110 dite de personnalisation, via une commande STORE DATA. La commande STORE DATA est par exemple définie par la norme EMV CPS (EMV Common Personnalisation Specification) et la norme Global Platform Card Specification.

[0085] L'organisme émetteur du premier dispositif électronique 110 peut ainsi, à la sortie de l'usine, définir des liens d'association entre dispositifs électroniques et des clés de chiffrage utilisées pour la communication des dispositifs électroniques liés.

[0086] En variante, l'identifiant ID2 du deuxième dispositif électronique 120 et la ou les éventuelles informations associées peuvent être obtenus pendant une transaction. La structure de données SD est alors créée lors de l'obtention ou lors d'une mise-à-jour.

[0087] Par exemple, lorsque la transaction est réalisée au moyen d'un lecteur spécifique tel qu'un distributeur automatique de billets ou un lecteur en agence bancaire, l'identifiant

ID2 du deuxième dispositif électronique 120 et la ou les éventuelles informations associées dont la ou les clés K2 peuvent être obtenus via une commande de scripts.

[0088] En variante, la ou les clés K2 peuvent être définies lors de la phase de personnalisation, puis l'identifiant ID2 du deuxième dispositif électronique 120 et une ou plusieurs éventuelles informations associées sont obtenus lors d'une transaction.

[0089] En variante, l'utilisateur du premier dispositif électronique 110 peut créer ou modifier, au moins en partie, le contenu de la structure de données SD, par exemple au moyen d'une application permettant typiquement de gérer les dispositifs électroniques associés à l'utilisateur. L'application peut ainsi lire et/ou modifier une ou plusieurs données de la structure de données SD, au moyen de commandes propriétaires, après avoir authentifié l'utilisateur.

[0090] L'application peut ne pas pouvoir accéder, en lecture ou en écriture, à une ou plusieurs autres données de la structure de données SD, les droits étant typiquement définis par l'organisme émetteur du premier dispositif électronique 110.

[0091] Par exemple, l'organisme émetteur peut bloquer l'ajout d'un dispositif électronique n'appartenant pas à l'utilisateur, typiquement en comparant la valorisation de l'objet Cardholder Name (défini par la norme EMV avec le tag 5F20) ou de l'objet Cardholder Name Extended (défini par la norme EMV avec le tag 9F0B).

[0092] En variante, il est possible de stocker dans une première structure de données les données auxquelles l'application a accès, et de stocker dans une deuxième structure de données les données auxquelles l'application n'a pas accès.

[0093] L'application peut être une application du premier dispositif électronique 110, ou une application d'un autre dispositif électronique apte à accéder à la structure de données SD, tel qu'un téléphone portable.

[0094] En revenant à la figure 3, le procédé peut en outre comprendre une étape S304 d'activation de la deuxième interface de communication 214 du premier dispositif électronique 110, suite à un événement d'activation.

[0095] L'événement d'activation peut être la réception d'une commande de transaction émise (envoyée) par un terminal de transaction tel que le terminal 140 de transaction, ou une action effectuée par un utilisateur du premier dispositif électronique 110.

[0096] Lorsque le premier dispositif électronique 110 est une carte à puce, l'événement d'activation est par exemple l'activation de la carte à puce 110 lors de l'insertion de la carte à puce 110 dans le terminal 140. L'événement d'activation peut aussi être l'activation du premier dispositif électronique 110 par un champ NFC, typiquement à un moment où le premier dispositif électronique 110 est approché du terminal 140 afin de procéder à une transaction.

[0097] En variante, l'événement d'activation est l'appui de l'utilisateur sur un bouton d'activation du premier dispositif électronique 110, ou encore la présentation d'une

empreinte de l'utilisateur au niveau du premier dispositif électronique 110.

[0098] En variante, l'événement d'activation est la réception d'une première commande de transaction, ou d'une commande SELECT définie par la norme ISO/IEC 7816-4. Dans le cas où le premier dispositif électronique 110 comprend plusieurs applications et qu'une partie seulement de ces applications est apte à utiliser le procédé de sécurisation, la commande SELECT permet l'activation que si une application apte à utiliser le procédé de sécurisation est sélectionnée par le premier dispositif électronique 110. Ainsi la batterie 215 n'est typiquement pas sollicitée quand le premier dispositif électronique 110 est utilisé en exécutant les autres applications, ce qui permet de limiter la consommation d'énergie du premier dispositif électronique 110.

[0099] L'étape d'activation est typiquement mise en œuvre par la première puce électronique 211. Suite à l'évènement d'activation, la première puce électronique 211 peut par exemple activer la batterie 215, de sorte que la batterie 215 puisse fournir l'énergie nécessaire au fonctionnement de la deuxième puce électronique 213 et donc au fonctionnement de la deuxième interface de communication 214.

[0100] Suite à l'étape S304 d'activation, le premier dispositif électronique 110 peut rechercher, afin de s'y connecter via la deuxième interface de communication 214 (étape S306), le ou les dispositifs associés au premier dispositif électronique 110 tels que le deuxième dispositif électronique 120, en utilisant le ou les identifiants de dispositifs électroniques sur le premier réseau de télécommunications 130 enregistrés dans la structure de données SD. L'étape S306 est typiquement mise en œuvre par la deuxième puce électronique 213.

[0101] Le premier dispositif électronique peut par exemple rechercher le deuxième dispositif électronique 120 en utilisant l'identifiant AD2 du deuxième dispositif électronique 120, et trouver le deuxième dispositif électronique 120 si la deuxième interface de communications du deuxième dispositif électronique 120 est activée.

[0102] Si le premier dispositif électronique 110 ne parvient pas à se connecter à un dispositif électronique associé, la deuxième interface de communication 214 peut alors émettre périodiquement des informations d'identification à tous les dispositifs électroniques présents sur le premier réseau de télécommunications 130 et attendre la connexion d'un des dispositifs électroniques associés (mode de fonctionnement dit « advertising » de la deuxième interface de communication 214).

[0103] En variante, suite à l'étape S304 d'activation, la deuxième interface de communication 214 peut écouter le premier réseau de télécommunications 130 afin de tenter de détecter un dispositif électronique compatible avec le premier dispositif électronique 110 (mode de fonctionnement dit « scanning » de l'interface de communication 218).

[0104] Si, à la fin d'une durée prédéterminé (e.g. de 25 secondes), le premier dispositif élec-

tronique 110 ne parvient pas à se connecter à un dispositif électronique associé, la deuxième interface de communication 214 peut alors émettre périodiquement des informations d'identification à tous les dispositifs électroniques présents sur le réseau et attend la connexion d'un de ces dispositifs électroniques (mode de fonctionnement dit « advertising » de la deuxième interface de communication 214).

[0105] En variante, le premier dispositif électronique 110 ne recherche pas un dispositif électronique associé, mais n'importe quel dispositif électronique. L'étape S302 d'association peut alors ne pas être mise en œuvre.

[0106] On considère maintenant que le premier dispositif électronique 110 est connecté au deuxième dispositif électronique 120. Un canal de communication sécurisé peut alors être établi entre le premier dispositif électronique 110 et le deuxième dispositif électronique 120, dans une étape S308, afin de permettre le chiffrage et/ou signature de tout message envoyé par le premier dispositif électronique 110 ou par le deuxième dispositif électronique 120. L'étape S308 comprend typiquement une double authentification du premier dispositif électronique 110 et du deuxième dispositif électronique au moyen de clés , notamment par exemple au moyen de la ou les clés K2 de la structure de données SD.

[0107] L'organisme émetteur peut en effet définir une clé de chiffrage et/ou une clé de signature et/ou une clé d'authentification pour tous les dispositifs électroniques associé à cet organisme, afin de s'assurer que tous ces dispositifs électroniques puissent s'authentifier entre eux et partager des informations.

[0108] Dans le cas d'une connexion entre dispositifs associés à des organismes émetteurs différents, le lien d'association peut être configuré par l'organisme émetteur à la demande de l'utilisateur d'un des dispositifs (dans ce cas les deux organismes émetteurs peuvent négocier une ou plusieurs clés de chiffrage et/ou signature et/ou authentification du canal). En variante, le lien d'association peut être configuré via l'application permettant de gérer les dispositifs électroniques associés à l'utilisateur (c'est alors le dispositif électronique sur lequel est installée l'application qui fait office d'intermédiaire pour la négociation d'une clé de chiffrage pour le canal).

[0109] Dans une étape S310, le premier dispositif électronique 110 reçoit, via la deuxième interface de communications 214, au moins un élément d'information concernant une transaction passée mise en œuvre par le deuxième dispositif électronique 120, envoyé par le deuxième dispositif électronique 120. L'étape S310 est typiquement déclenchée par une commande GET_PROCESSING_OPTIONS, définie par la norme EMV, par exemple dans sa version 4.3 book 3.

[0110] Chaque élément d'information concernant une transaction passée mise en œuvre par le deuxième dispositif électronique 120 est typiquement un ensemble de données (« record ») concernant une transaction passée mise en œuvre par le deuxième

dispositif électronique 120, stocké dans le premier historique de transactions du deuxième dispositif électronique 120.

[0111] Le ou les éléments d'information peuvent être reçus directement depuis le deuxième dispositif électronique 120, le ou les éléments d'information ne transitant alors pas par un autre dispositif électronique. Ainsi, le ou les éléments d'information peuvent être reçus via le canal sécurisé créé à l'étape S308.

[0112] En variante, le ou les éléments d'information peuvent être envoyés par le deuxième dispositif électronique 120 au terminal 140, le terminal 140 les transmettant ensuite au premier dispositif électronique 110, le terminal 140 jouant ainsi un rôle de mémoire tampon.

[0113] Le premier dispositif électronique 110 peut en outre envoyer au deuxième dispositif électronique 120, via la deuxième interface de communications 214, au moins un élément d'information concernant une transaction passée mise en œuvre par le premier dispositif électronique 110 (étape S312). On peut alors parler de synchronisation des éléments d'information concernant des transactions passées entre le premier dispositif électronique 110 et le deuxième dispositif électronique 120.

[0114] Chaque élément d'information concernant une transaction passée mise en œuvre par le premier dispositif électronique 110 est typiquement un des ensembles de données (« record ») concernant une transaction passée réalisée par le premier dispositif électronique 110, stocké dans le premier historique de transactions HT1 du premier dispositif électronique 110.

[0115] Comme le montre la **figure 5A**, l'étape S310 et/ou l'étape S312 peuvent être précédées d'une étape de réception S502, par le premier dispositif électronique 110 et via la deuxième interface de communications 214, d'une indication concernant le format du premier historique de transactions HT3 du deuxième dispositif électronique 120. L'indication concernant le format est par exemple la donnée « Log Format » décrite par la norme EMV.

[0116] De la même manière, le premier dispositif électronique 110 peut envoyer au deuxième dispositif électronique 120, via la deuxième interface de communications 214, une indication concernant le format du premier historique HT1 de transaction du premier dispositif électronique 110 (étape S504).

[0117] L'étape S310 et/ou l'étape S312 peuvent aussi être précédées d'une étape S506 d'envoi, par le premier dispositif électronique 110, au deuxième dispositif électronique 120 et via la deuxième interface de communications 214, d'au moins une indication permettant de déterminer le nombre d'éléments d'information à envoyer par le deuxième dispositif électronique 120 au premier dispositif électronique 110, parmi les indications suivantes :

- le nombre maximum d'élément(s) d'information pouvant être reçu(s) par le premier

dispositif électronique 110,
- le nombre minimum d'élément(s) d'information pouvant être reçu(s) par le premier dispositif électronique 110,
- la date de la dernière transaction mise en œuvre par le deuxième dispositif électronique 120 et associée à un ensemble de données stocké par le premier dispositif électronique 110 dans le deuxième historique de transactions HT2.1 du premier dispositif électronique 110 (i.e. associée à un élément d'information ayant déjà été envoyé par le deuxième dispositif électronique 120),
- la valeur d'un compteur de transactions, associée à la dernière transaction mise en œuvre par le deuxième dispositif électronique 120 et associée à un ensemble de données stocké par le premier dispositif électronique 110 dans le deuxième historique de transactions HT2.1 du premier dispositif électronique 110.

[0118] Le compteur de transactions est incrémenté à chaque transaction réalisée au moyen du deuxième dispositif électronique 120 et permet ainsi d'identifier de façon unique une transaction réalisée au moyen du deuxième dispositif électronique 120. Le compteur de transactions est par exemple le compteur ATC (pour « Application Transaction Counter », en terminologie anglo-saxonne) défini par la norme EMV.

[0119] Le deuxième dispositif électronique 120 peut alors déterminer, à partir du ou des indications reçues, le nombre d'éléments d'information à envoyer au premier dispositif électronique 110, puis envoyer le ou les éléments d'information de sorte que le premier dispositif électronique 110 les reçoive à l'étape S310.

[0120] Le premier dispositif électronique 110 peut aussi recevoir (étape S508), via la deuxième interface de communications 214, au moins une indication permettant de déterminer le nombre d'éléments d'information à envoyer par le premier dispositif électronique 110 au deuxième dispositif électronique 120, parmi les indications suivantes :
- le nombre maximum d'élément(s) d'information pouvant être reçu(s) par le deuxième dispositif électronique 120,
- le nombre minimum d'élément(s) d'information pouvant être reçu(s) par le deuxième dispositif électronique 120,
- la date de la dernière transaction mise en œuvre par le premier dispositif électronique 110 et associée à un ensemble de données stocké par le deuxième dispositif électronique 120 dans le deuxième historique de transactions HT4.1 du deuxième dispositif électronique 120 (i.e. associée à un élément d'information ayant déjà été envoyé par le premier dispositif électronique 110),
- la valeur d'un compteur de transactions, associée à la dernière transaction mise en œuvre par le premier dispositif électronique 110 et associée à un ensemble de données stocké par le deuxième dispositif électronique 120 dans le deuxième historique de transactions HT4.1 du deuxième dispositif électronique 120.

[0121] Le premier dispositif électronique 110 peut alors déterminer, à partir du ou des indications reçues, le nombre d'éléments d'information concernant des transactions passées à envoyer au deuxième dispositif électronique 120, puis envoyer le ou les éléments d'information concernant des transactions passées de sorte que le deuxième dispositif électronique 120 les reçoive à l'étape S312.

[0122] Suite à l'étape S310 de réception, le premier dispositif électronique 110 peut déterminer, à partir de l'indication concernant le format du premier historique de transactions HT3 du deuxième dispositif électronique 120, si chaque élément d'information reçu à l'étape S310 doit être normalisé, de sorte à être compatible avec le deuxième historique de transactions HT2 du premier dispositif électronique 110 (étape S318). Les opérations suivantes de normalisation peuvent être effectuées, typiquement en utilisant une table de conversion :

- déplacement de données si l'ordre des données n'est pas le même,
- transformation (conversion) d'au moins une donnée si cette donnée doit être stockée sous un format différent dans le deuxième historique de transactions HT2,
- suppression d'au moins une données si celle-ci ne peut pas être stockée dans le deuxième historique de transactions HT2,
- ajout d'au moins une valeur par défaut si cette valeur n'est pas présente dans les données de l'élément d'information reçu.

[0123] Chaque élément d'information reçu est ensuite stocké dans le deuxième historique de transactions HT2.2 du premier dispositif électronique 110, dans une étape S320.

[0124] De même, le deuxième dispositif électronique 120 peut normaliser chaque élément d'information reçu à l'étape S312 avant de stocker chaque élément d'information dans le deuxième historique de transactions HT4.2 du deuxième dispositif électronique 120.

[0125] En variante, comme le montre la **figure 5B**, les étapes S506 et/ou S508 ne sont pas mises en œuvre. A la place, le premier dispositif électronique 110 envoie, via la deuxième interface de communication 214 et au deuxième dispositif électronique 120, une requête d'obtention d'information de transaction passée (étape S510).

[0126] Sous réception de la requête, le deuxième dispositif électronique 120 envoie l'élément d'information concernant la dernière transaction mise en œuvre au moyen du deuxième dispositif électronique 120 (étape S512).

[0127] Le premier dispositif électronique 110 vérifie alors que cet élément d'information n'est pas déjà stocké dans le deuxième historique de transactions HT2. Si cela est le cas, le premier dispositif électronique 110 stocke l'élément d'information dans le deuxième historique de transactions HT2, après l'avoir éventuellement normalisé.

[0128] Le premier dispositif électronique 110 détermine ensuite s'il est possible de stocker un autre élément d'information dans le deuxième historique de transactions HT2, en utilisant par exemple les indications susmentionnées. Si cela est le cas, le premier

dispositif électronique 110 envoie, via la deuxième interface de communication 214 et au deuxième dispositif électronique 120, une nouvelle requête d'obtention d'information de transaction passée (étape S514).

[0129] Sous réception de la nouvelle requête, le deuxième dispositif électronique 120 envoie l'élément d'information concernant l'avant dernière transaction mise en œuvre au moyen du deuxième dispositif électronique 120 (étape S516). Le premier dispositif électronique 110 vérifie alors que cet élément d'information n'est pas déjà stocké dans le deuxième historique de transactions HT2. Si cela est le cas, le dispositif électronique 110 stocke l'élément d'information dans le deuxième historique de transactions HT2, après l'avoir éventuellement normalisé.

[0130] Les étapes S514 et S516 peuvent être réitérées jusqu'à ce que le premier dispositif électronique 110 détermine qu'il n'est plus possible de stocker un élément d'information supplémentaire dans le deuxième historique de transactions HT2. A chaque réitération, le deuxième dispositif électronique 120 envoie l'élément d'information concernant la transaction précédant la transaction associée à l'élément d'information ayant été envoyé par le deuxième dispositif électronique à l'itération précédente.

[0131] De même, le deuxième dispositif électronique 120 peut envoyer des requêtes d'obtention d'information de sorte à obtenir des éléments d'information concernant des transactions mises en œuvre par le premier dispositif électronique 110, jusqu'à ce que cela ne soit plus nécessaire. La description des étapes S510 à S516 peut s'appliquer en échangeant les termes relatifs au premier dispositif électronique 110 et les termes relatifs au deuxième dispositif électronique 120.

[0132] D'autres informations peuvent être échangées par le premier dispositif électronique 110 et le deuxième dispositif électronique 120. Le premier dispositif électronique 110 peut par exemple recevoir et/ou envoyer une liste de terminaux à risque, pour lesquels des mesures de sécurité doivent être prises lorsqu'une transaction est réalisée. Un horodatage est typiquement ajouté à la liste reçue afin de pouvoir déterminer la liste la plus récente. La liste de terminaux à risque (appelée « Blacklist Commerçant ») est typiquement une liste « Terminal ID » 9F1C définie par la norme EMV, ou une liste « Merchant Name and Location » 9F4E définie par la norme EMV.

[0133] Le premier dispositif électronique 110 peut aussi recevoir et/ou envoyer une ou plusieurs commandes de script, pour mettre à jour des données internes du dispositif électronique (par exemple pour mettre à jour les limites et/ou la configuration d'une application de transaction) et/ou pour bloquer le dispositif électronique ou l'application de transaction.

[0134] A la réception d'une telle commande de script, le premier dispositif électronique 110 peut stocker la commande de script avec un code d'authentification de message (MAC

pour « Message Authentication Code », en terminologie anglo-saxonne) dans la première mémoire 217 du premier dispositif électronique 110, lorsque le premier dispositif électronique 110 détermine que cette commande de script doit être propagée à d'autres dispositifs électroniques. Par exemple, le premier dispositif électronique 110 détermine si la commande de script doit être propagée au moyen d'une table permettant de déterminer en fonction de la commande reçue et d'une application sélectionnée vers quel dispositif électronique la commande doit être transférée.

[0135] Le premier dispositif électronique 110 peut aussi recevoir et/ou envoyer des informations sur des alertes concernant des évènements de sécurité informatique.

[0136] Le premier dispositif électronique 110 peut aussi recevoir et/ou envoyer une ou plusieurs données de configuration, de sorte à assurer une cohérence des politiques de sécurités entre les dispositifs électroniques et ainsi améliorer leur sécurité. La configuration associée aux données de configuration peut comprendre :

- la possibilité de refuser des transactions pendant une durée prédéterminée,
- le déblocage ou le blocage d'applications sur le dispositif électronique, typiquement en fonction de conditions prédéterminées, telles que par exemple un montant total de transaction supérieur à un seuil prédéterminé pour des transactions réalisées pendant une durée prédéterminée,
- la possibilité de ne pas propager un blocage vers un autre dispositif électronique après une authentification réussie (typiquement au moyen d'un code tel qu'un code PUK ou par empreinte digitale) par exemple réalisée par le dispositif électronique,
- le changement de code PIN sur le dispositif électronique,
- l'activation ou la désactivation de la communication sans contact du dispositif électronique,
- la synchronisation de structures de données contenant des conditions considérées comme suspicieuses et les contremesures associées, telle que la structure de données appelée « Extended CRM » utilisée dans le domaine de la sécurité informatique, permettant de gérer des comportements non prévus dans les spécifications bancaires et d'adopter également des réactions non prévues dans ces spécifications, et/ou
- les vérifications à effectuer à l'étape S322 d'analyse de risque décrite ci-dessous, et les opérations de sécurisation pouvant être déclenchées à l'étape S324 décrite ci-dessous.

[0137] La synchronisation de la structure de données « Extended CRM » est réalisée au moyen d'un numéro de version attribué au contenu de la structure de données, permettant de déterminer quelle est la version la plus récente. L'ensemble des données de la structure de données, ou une partie de ces données, peut être synchronisée.

[0138] Dans une étape S322, le premier dispositif électronique 110 réalise une analyse de risque à partir du ou des éléments d'information reçus à l'étape S310, afin de détecter

une utilisation anormale du premier dispositif électronique 110 et du deuxième dispositif électronique 120. Cette analyse de risque est typiquement déclenchée par une commande GENERATE_AC, définie par la norme EMV, par exemple dans sa version 4.3 book 3.

[0139] Par exemple, lorsque l'étape S322 est mise en œuvre après l'initialisation d'une transaction courante mise en œuvre par le premier dispositif électronique 110, le premier dispositif électronique 110 obtient, en consultant l'élément d'information concernant la dernière transaction mise en œuvre au moyen du deuxième dispositif électronique 120 stocké dans le deuxième historique de transactions HT2, la date de transaction de la dernière transaction mise en œuvre au moyen du deuxième dispositif électronique 120, cette transaction étant une transaction passée, c'est-à-dire terminée.

[0140] L'analyse de risque peut alors comprendre une comparaison de la date de la dernière transaction passée à une date courante, c'est-à-dire la date de la transaction courante mise en œuvre par le premier dispositif électronique 110. La date de chaque transaction comprend typiquement l'heure de la transaction.

[0141] Si la durée entre la date de la dernière transaction passée et la date courante est inférieure à une durée prédéfinie, le premier dispositif électronique 110 détecte une utilisation anormale du premier dispositif électronique 110 et du deuxième dispositif électronique 120.

[0142] En variante, lorsque l'étape S322 est mise en œuvre après l'initialisation d'une transaction courante mise en œuvre par le premier dispositif électronique 110, le premier dispositif électronique obtient, en consultant les éléments d'information stockés dans le deuxième historique de transactions HT2 concernant les transactions mises en œuvre par le deuxième dispositif électronique 120, les dates de ces transactions. Le premier dispositif électronique 110 peut aussi obtenir les dates de transaction de tous les éléments d'information stockés dans le deuxième historique de transactions HT2, les transactions pouvant alors être mises en œuvre par le deuxième dispositif électronique 120 et/ou par un autre dispositif électronique.

[0143] Le premier dispositif électronique 110 détermine ensuite, pendant l'analyse de risque, le nombre de transactions ayant été réalisé pendant une durée prédéterminée se terminant à la date de transaction courante. La durée prédéterminée est typiquement de 5 à 10 minutes. Lorsque le nombre de transactions est supérieur ou égal à un seuil prédéterminé, par exemple de trois transactions, le premier dispositif électronique 110 détecte une utilisation anormale du premier dispositif électronique 110 et du deuxième dispositif électronique 120.

[0144] Lorsque le premier dispositif électronique 110 détecte une utilisation anormale du premier dispositif électronique 110 et du deuxième dispositif électronique 120 à l'étape S322 d'analyse de risque, le premier dispositif électronique 110 déclenche, dans une

étape S324, au moins une opération de sécurisation du premier dispositif électronique 110.

[0145] Chaque opération de sécurisation peut être une opération parmi les opérations suivantes :

- envoi d'un message informant de l'utilisation anormale détectée,
- modification d'au moins un paramètre de fonctionnement du premier dispositif électronique 110,
- envoi d'un message de modification d'au moins un paramètre de fonctionnement,
- enregistrement, dans le premier historique de transactions HT1 du premier dispositif électronique 110, d'une donnée de sécurité représentative de ladite utilisation anormale détectée, et
- refus de mettre en œuvre la transaction courante au moyen du premier dispositif électronique 110.

[0146] Le message informant de l'utilisation anormale détectée peut être envoyé au deuxième dispositif électronique 120 et/ou à un ou plusieurs autres dispositifs électroniques, par exemple les dispositifs électroniques associés au premier dispositif électronique 110. Le dispositif électronique recevant le message peut alors choisir la réaction qu'il doit adopter suite à l'utilisation anormale détectée par le premier dispositif électronique 110.

[0147] Le message de modification d'au moins un paramètre de fonctionnement peut être envoyé au deuxième dispositif électronique 120, cet envoi étant typiquement une commande de script. Le deuxième dispositif électronique 120 peut alors modifier le paramètre de fonctionnement du deuxième dispositif électronique 120. Ainsi, le premier dispositif électronique 110 peut imposer au moins une partie de la réaction du deuxième dispositif électronique 120 devant être adoptée suite à l'utilisation anormale détectée par le premier dispositif électronique 110.

[0148] Le premier dispositif électronique 110 peut ainsi ne pas se contenter d'informer le deuxième dispositif électronique 120 d'une utilisation anormale mais peut aussi par exemple bloquer le deuxième dispositif électronique 120 ou inhiber une interface de paiement sans contact du deuxième dispositif électronique 120.

[0149] En variante ou en complément, le message de modification d'au moins un paramètre de fonctionnement peut être envoyé à un ou plusieurs autres dispositifs électroniques, par exemple les dispositifs électroniques associés au premier dispositif électronique 110.

[0150] Bien entendu, le premier dispositif électronique 110 peut aussi déclencher une opération de sécurisation du premier dispositif électronique 110 lorsqu'il détecte une utilisation anormale du premier dispositif électronique 110 à partir du premier historique de transactions HT1.

[0151] Le premier dispositif électronique 110 peut en outre déclencher une opération de sécurisation dudit premier dispositif électronique 110 s'il ne reçoit pas d'élément d'information du deuxième dispositif électronique 120, par exemple au-delà d'un certain nombre d'itérations de mise en œuvre de transactions au moyen du premier dispositif électronique 110, ou si la durée entre la transaction en cours et la date de la dernière réception d'éléments d'information du deuxième dispositif électronique 120 est supérieure à une durée prédéfinie.

[0152] Dans une étape S326, le premier dispositif électronique 110 désactive la deuxième interface de communication 214. Cette étape S326 est typiquement mise en œuvre à la fin d'une durée prédéfinie, décomptée à partir d'un événement de désactivation.

[0153] L'événement de désactivation peut être la fin de la transaction entre le premier dispositif électronique 110 et le terminal de transaction 140 (par exemple le blocage de la transaction), ou une inactivité de la deuxième interface de communication 214 suite à son activation, pendant une durée supérieure à un seuil prédéfini.

[0154] L'étape de désactivation est typiquement mise en œuvre par la première puce électronique 211. A la fin d'une durée prédéfinie décomptée à partir de l'événement de désactivation, la première puce électronique 211 peut par exemple désactiver la batterie 215, de sorte que l'énergie nécessaire au fonctionnement de la deuxième puce électronique 213 et donc au fonctionnement de la deuxième interface de communication 214 ne soit plus fournie.

[0155] Cette gestion particulière de la deuxième interface de communication 214, peut permettre au premier dispositif électronique 110 de communiquer avec le deuxième dispositif électronique 120 lors d'une transaction, mais aussi pendant une durée supplémentaire après la transaction, cette durée supplémentaire étant prédéfinie en fonction de cas d'utilisations anormales (e.g. plusieurs transactions en peu de temps).

[0156] Ainsi, en cas d'utilisation du premier dispositif électronique 110 puis du deuxième dispositif électronique 120, le deuxième dispositif électronique 120 peut communiquer avec le premier dispositif électronique 110 afin d'obtenir un ou plusieurs éléments d'information concernant les transactions passées mise en œuvre par le premier dispositif électronique 110, et ainsi détecter une potentielle utilisation anormale.

[0157] En effet, les étapes S302, S304, S306, S308, S310, S312, S502, S504, S506, S508, S510, S512, S514, S516, S318, S320, S322, S324 et/ou S326 peuvent être mises en œuvre par le deuxième dispositif électronique 120. La description de chacune de ces étapes peut s'appliquer en échangeant les termes relatifs au premier dispositif électronique 110 et les termes relatifs au deuxième dispositif électronique 120.

[0158] Le deuxième dispositif électronique 120 peut ainsi lui aussi détecter une utilisation anormale du premier dispositif électronique 110 et du deuxième dispositif électronique 120 et déclencher au moins une opération de sécurisation du deuxième dispositif élec-

tronique 120.

[0159] La **figure 6** représente un exemple de mise en œuvre du procédé de sécurisation, dans le cadre de deux transactions mises en œuvre au moyen du premier dispositif électronique 110 et du deuxième dispositif électronique 120, les deux dispositifs électroniques 110, 120 prenant par exemple la forme de cartes à puce.

[0160] Plus précisément, une première transaction T1 est mise en œuvre par la deuxième carte à puce 120 et le terminal 140 de transaction, puis une deuxième transaction T2 est mise en œuvre par le premier dispositif électronique 110 et le terminal 140.

[0161] Suite à l'activation S602 de la deuxième carte à puce 120 par le terminal 140 lors l'initialisation de la première transaction T1, la première puce électronique 611 de la deuxième carte à puce 120 active la deuxième puce électronique 613 de la deuxième carte à puce 120 et donc la deuxième interface de communication de la deuxième carte à puce 120 (étape S304).

[0162] La deuxième interface de communication 214 de la première carte à puce 110 n'étant pas activée, la deuxième carte à puce 120 réalise la première transaction T1 sans se connecter à la première carte à puce 110.

[0163] Ensuite, lors de l'initialisation de la deuxième transaction T2, la première carte à puce 110 est activée (étape S622) par le terminal 140, et la première puce électronique 211 de la première carte à puce 110 active deuxième interface de communication 214 en activant la deuxième puce électronique 213 de la première carte à puce 110 (étape S304).

[0164] La deuxième interface de communication de la deuxième puce électronique 120 n'ayant pas encore été désactivée, la première carte à puce 110 peut se connecter S306 à la deuxième carte à puce 120, puis un canal de communication sécurisé peut être établi S308 entre les deux cartes à puce 110, 120.

[0165] Ensuite, la première carte à puce 110 peut recevoir (étape S310) l'élément d'information concernant la première transaction T1 mise en œuvre par la deuxième carte à puce 120. Cette réception est typiquement déclenchée par une commande GET_PROCESSING_OPTIONS (GPO).

[0166] L'élément d'information reçu est ensuite stocké dans le deuxième historique de transactions HT2.2 de la première carte à puce 110 (étape S320), typiquement après avoir été normalisé.

[0167] La première carte à puce 110 peut alors réaliser une analyse de risque à partir de cet élément d'information, afin de détecter une utilisation anormale des cartes 110, 120 (étape S322). Cette analyse de risque est typiquement déclenchée par une commande GENERATE_AC.

[0168] Par exemple, la première carte à puce 110 peut comparer la date de la première transaction T1 et la date courante de la deuxième transaction T2. Si la durée entre de la

première transaction T1 et la date courante de la deuxième transaction T2 est inférieure à une durée prédéfinie, la première carte à puce 110 détecte une utilisation anormale, et peut alors déclencher une opération de sécurisation (étape S324). Lorsque l'opération de sécurisation est l'envoi d'un message de modification d'au moins un paramètre de fonctionnement à la deuxième carte à puce 120, cette opération de sécurisation est typiquement une commande de script.

[0169] Dans une étape S326, la première carte à puce 110 désactive la deuxième interface de communication 214 de la première carte à puce 110. De même, la deuxième carte à puce 120 désactive la deuxième interface de communication de la deuxième carte à puce 120.

Revendications

[Revendication 1] Procédé de sécurisation, mis en œuvre par un premier dispositif électronique (110), ledit procédé comprenant les étapes suivantes :
- réception (S310) d'au moins un élément d'information concernant une transaction passée mise en œuvre par un deuxième dispositif électronique (120), envoyé par le deuxième dispositif électronique (120),
- analyse de risque (S322) à partir dudit au moins un élément d'information, afin de détecter une utilisation anormale du premier dispositif électronique (110) et du deuxième dispositif électronique (120), et
- dans l'affirmative, déclenchement (S324) d'au moins une opération de sécurisation du premier dispositif électronique (110).

[Revendication 2] Procédé de sécurisation selon la revendication 1, dans lequel ledit au moins un élément d'information est reçu directement depuis le deuxième dispositif électronique (120).

[Revendication 3] Procédé de sécurisation selon la revendication 2, comprenant en outre l'étape suivante :
- création (S308) d'un canal sécurisé entre le premier dispositif électronique (110) et le deuxième dispositif électronique (120),
ledit au moins un élément d'information étant reçu via le canal sécurisé.

[Revendication 4] Procédé selon l'une quelconque des revendications 1 à 3, comprenant en outre l'étape suivante :
- activation (S304) d'une interface de communication (214) suite à un événement d'activation.

[Revendication 5] Procédé selon la revendication 4, comprenant en outre l'étape suivante :
- désactivation (S326) de l'interface de communication (214) à la fin d'une durée prédéfinie décomptée à partir d'un événement de désactivation.

[Revendication 6] Procédé de sécurisation selon l'une quelconque des revendications 1 à 5, comprenant en outre l'étape suivante, mise en œuvre avant l'étape (S310) de réception dudit au moins un élément d'information :
- stockage d'un identifiant (ID2) du deuxième dispositif électronique (120), de sorte à associer (S302) le premier dispositif électronique (110) et le deuxième dispositif électronique (120).

[Revendication 7] Procédé de sécurisation selon l'une quelconque des revendications 1 à 6, comprenant en outre l'étape suivante, mise en œuvre avant l'étape (S310) de réception dudit au moins un élément d'information :

- envoi (S514) au deuxième dispositif électronique (120) d'une requête d'obtention d'information de transaction passée.

[Revendication 8] Procédé de sécurisation selon l'une quelconque des revendications 1 à 7, comprenant en outre l'étape suivante :
- envoi (S312) d'au moins un élément d'information concernant une transaction passée mise en œuvre par le premier dispositif électronique (110), au deuxième dispositif électronique (120).

[Revendication 9] Procédé de sécurisation selon l'une quelconque des revendications 1 à 8, dans lequel chaque opération de sécurisation est une des opérations parmi les opérations suivantes :
- envoi d'un message informant de ladite utilisation anormale détectée,
- modification d'au moins un paramètre de fonctionnement du premier dispositif électronique (110),
- envoi d'un message de modification d'au moins un paramètre de fonctionnement,
- enregistrement, dans un historique de transactions (HT1) du premier dispositif électronique (110), d'une donnée de sécurité représentative de ladite utilisation anormale détectée, et
- refus de mettre en œuvre une transaction courante au moyen du premier dispositif électronique (110).

[Revendication 10] Procédé de sécurisation selon l'une quelconque des revendications 1 à 9, mis en œuvre après une initialisation d'une transaction courante mise en œuvre par le premier dispositif électronique (110), dans lequel :
- ledit élément d'information concernant la transaction passée provient d'un historique de transactions du deuxième dispositif électronique (120), et comprend une date de la transaction passée,
- l'analyse de risque (S322) comprend la comparaison de la date de la transaction passée à une date courante, une utilisation anormale étant détectée si la durée entre la date de la transaction passée et la date courante est inférieure à une durée prédéfinie.

[Revendication 11] Procédé de sécurisation selon l'une quelconque des revendications 1 à 10, comprenant en outre les étapes suivantes :
- réception d'une donnée de configuration,
- modification d'un paramètre de configuration du premier dispositif électronique en fonction de ladite donnée de configuration.

[Revendication 12] Procédé de sécurisation mis en œuvre par un deuxième dispositif électronique, ledit procédé comprenant l'étape suivante :
- envoi d'au moins un élément d'information concernant une transaction

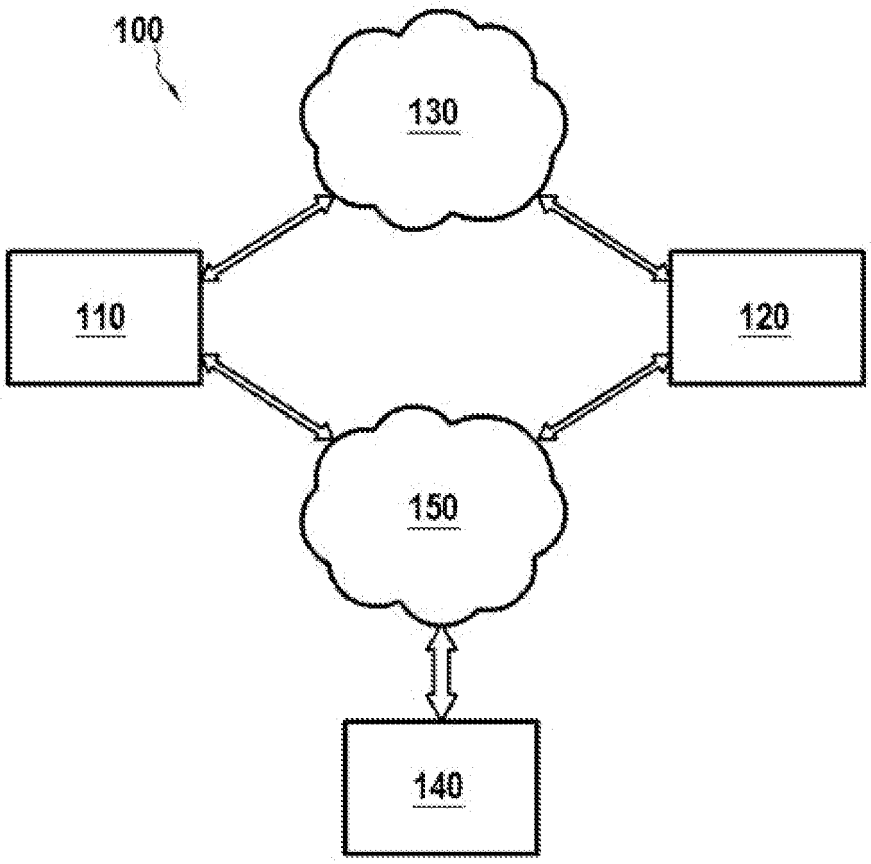
passée mise en œuvre par le deuxième dispositif électronique, de sorte que le premier dispositif électronique soit apte mettre en œuvre une analyse de risque à partir dudit au moins un élément d'information, afin de détecter une utilisation anormale du premier dispositif électronique et du deuxième dispositif électronique, et, dans l'affirmative, déclencher d'au moins une opération de sécurisation du premier dispositif électronique.

[Revendication 13] Dispositif électronique apte à mettre en œuvre un procédé de sécurisation selon l'une quelconque des revendications 1 à 12.

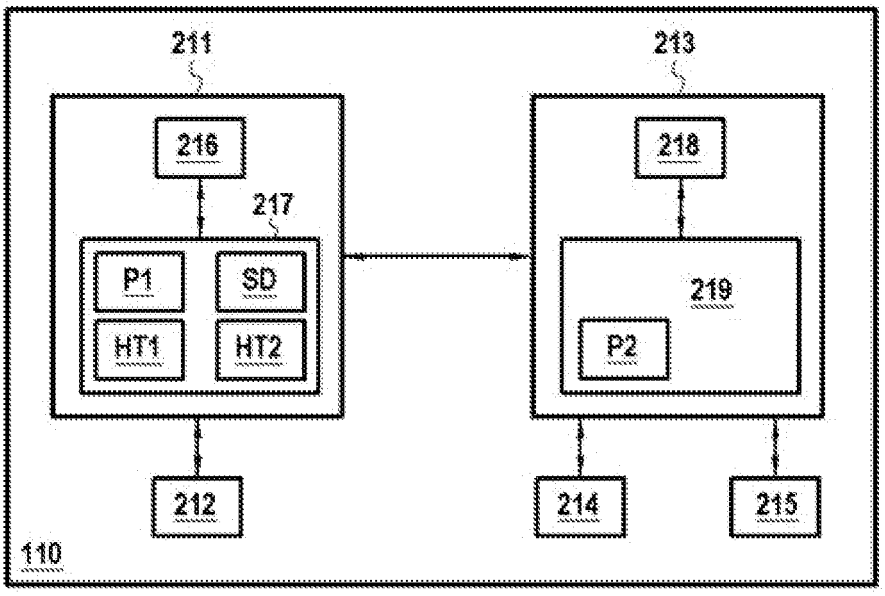
[Revendication 14] Programme d'ordinateur comportant des instructions pour l'exécution des étapes du procédé de sécurisation selon l'une quelconque des revendications 1 à 12 lorsque ledit programme est exécuté par un ordinateur.

[Revendication 15] Support d'enregistrement lisible par un ordinateur sur lequel est enregistré un programme d'ordinateur comprenant des instructions pour l'exécution des étapes du procédé selon l'une quelconque des revendications 1 à 12.

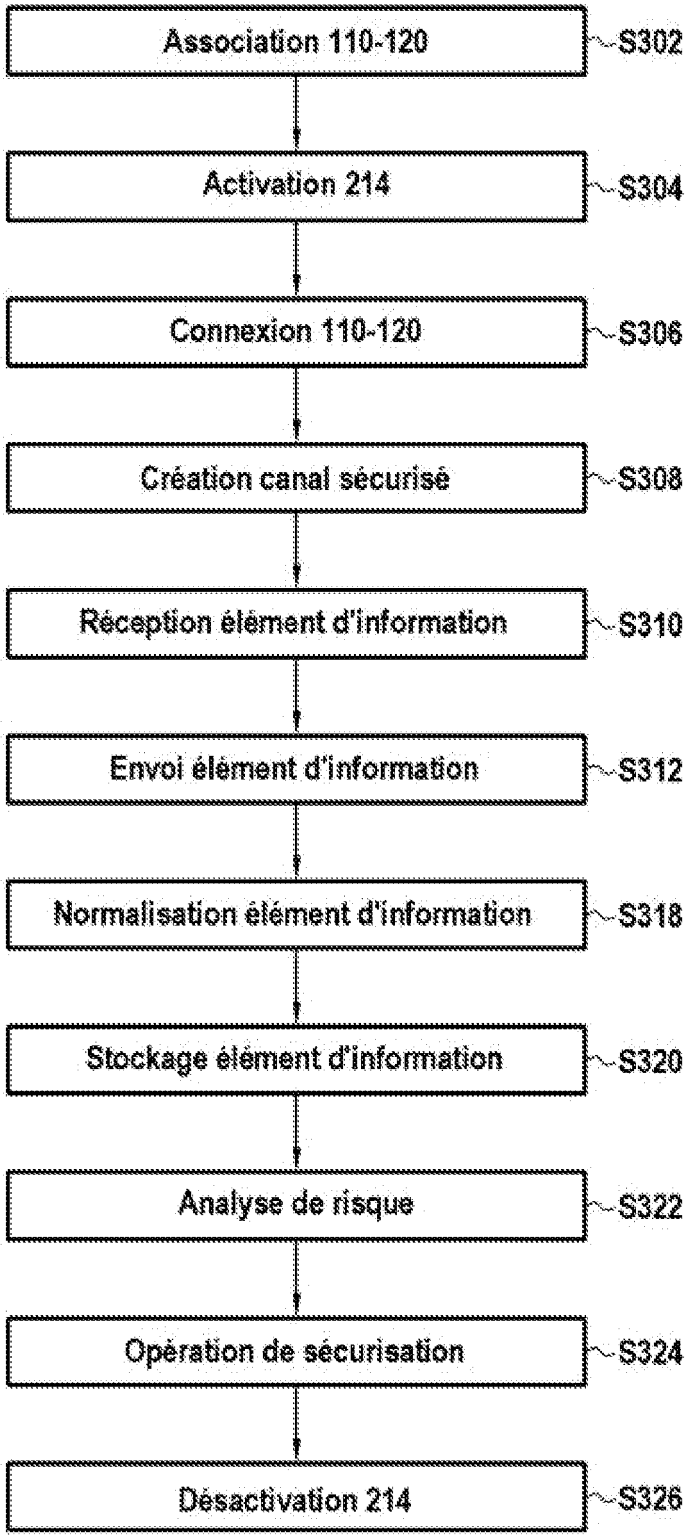
[Fig. 1]


100
130
110
120
150
140

[Fig. 2]


211
213
216
218
217
P1
SD
HT1
HT2
219
P2
212
214
215
110

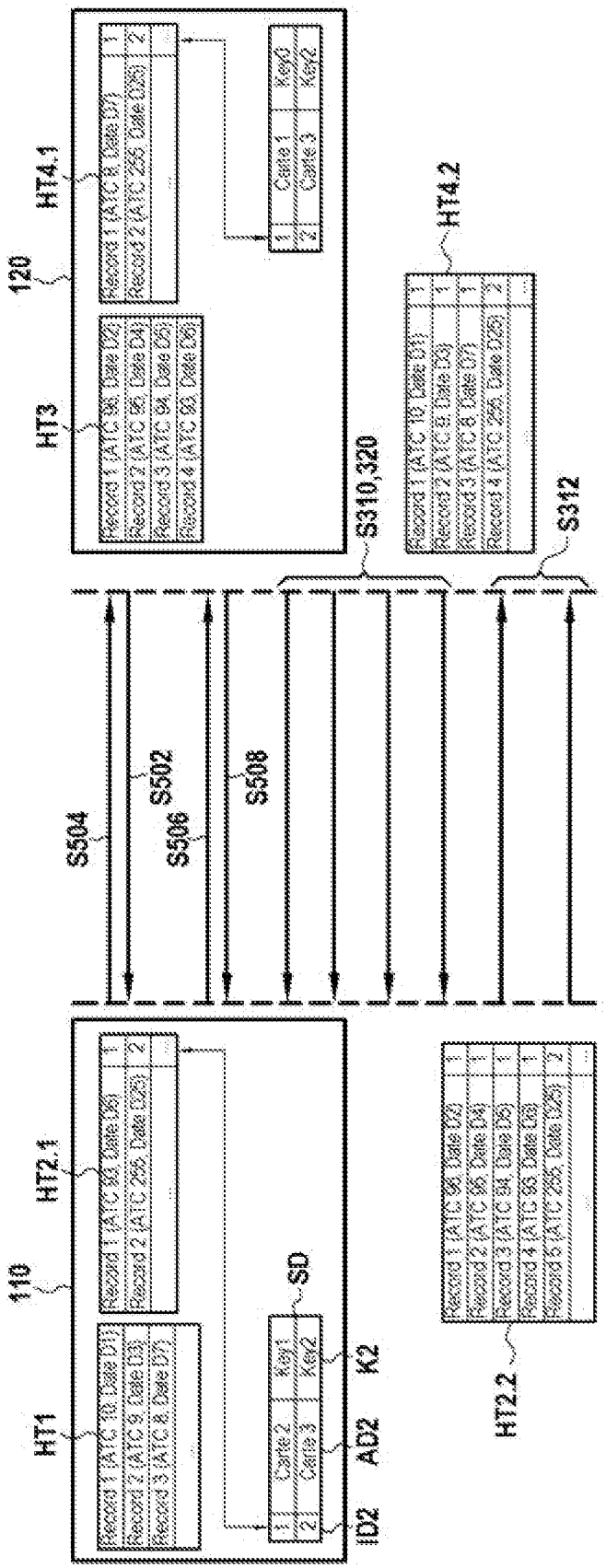
[Fig. 3]


Association 110-120
S302
Activation 214
S304
Connexion 110-120
S306
Création canal sécurisé
S308
Réception élément d'information
S310
Envoi élément d'information
S312
Normalisation élément d'information
S318
Stockage élément d'information
S320
Analyse de risque
S322
Opération de sécurisation
S324
Désactivation 214
S326

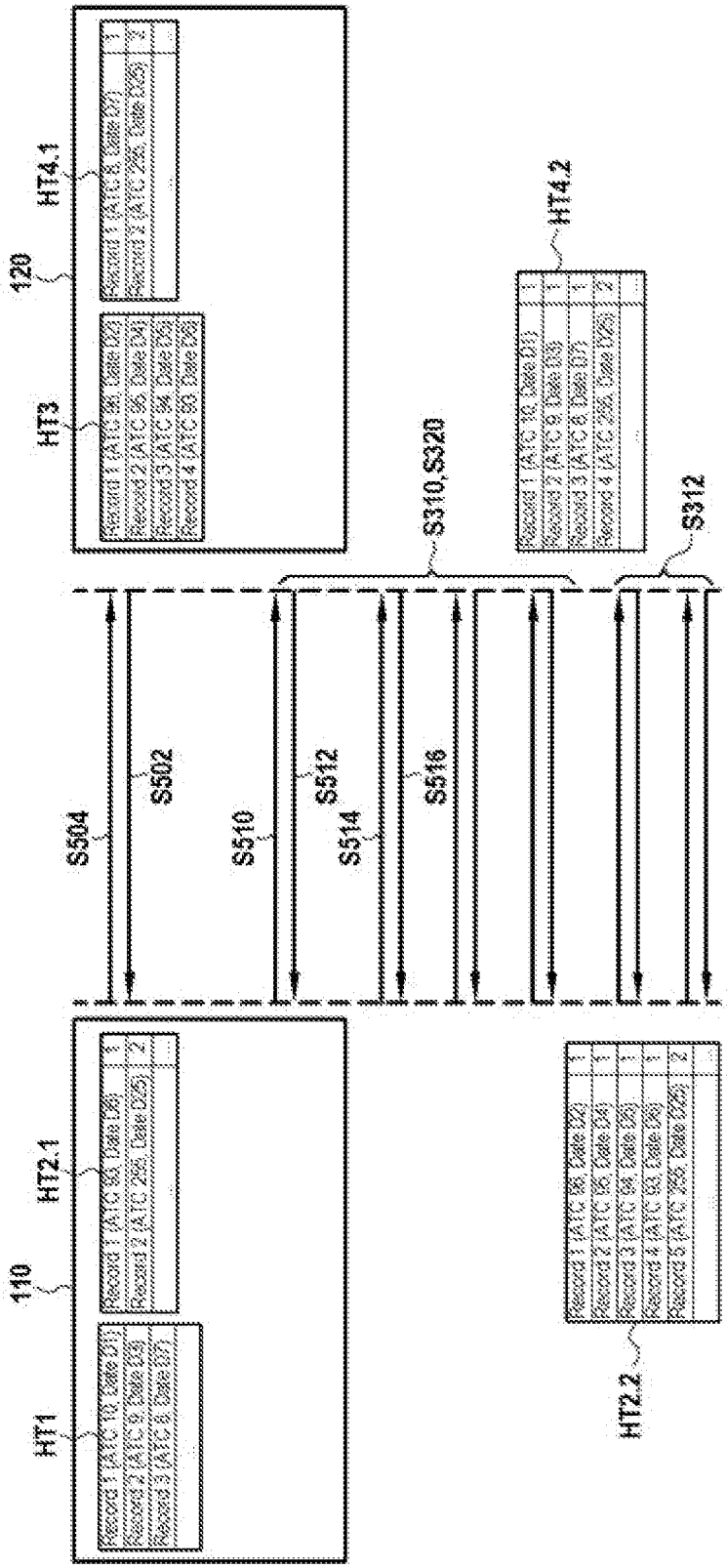
[Fig. 4]

Index	Statut	@	Clé	Métadonnées lieu	Métadonnées droits d'accès
Disp 1	Actif	@ 1	Clé 1	Utilisateur 1	r/w
⋮	⋮	⋮	⋮	⋮	⋮
Disp n	Inactif	@ n	Clé n	Utilisateur n	r/w
ID2	ST2	AD2	K2	ML2	MD2

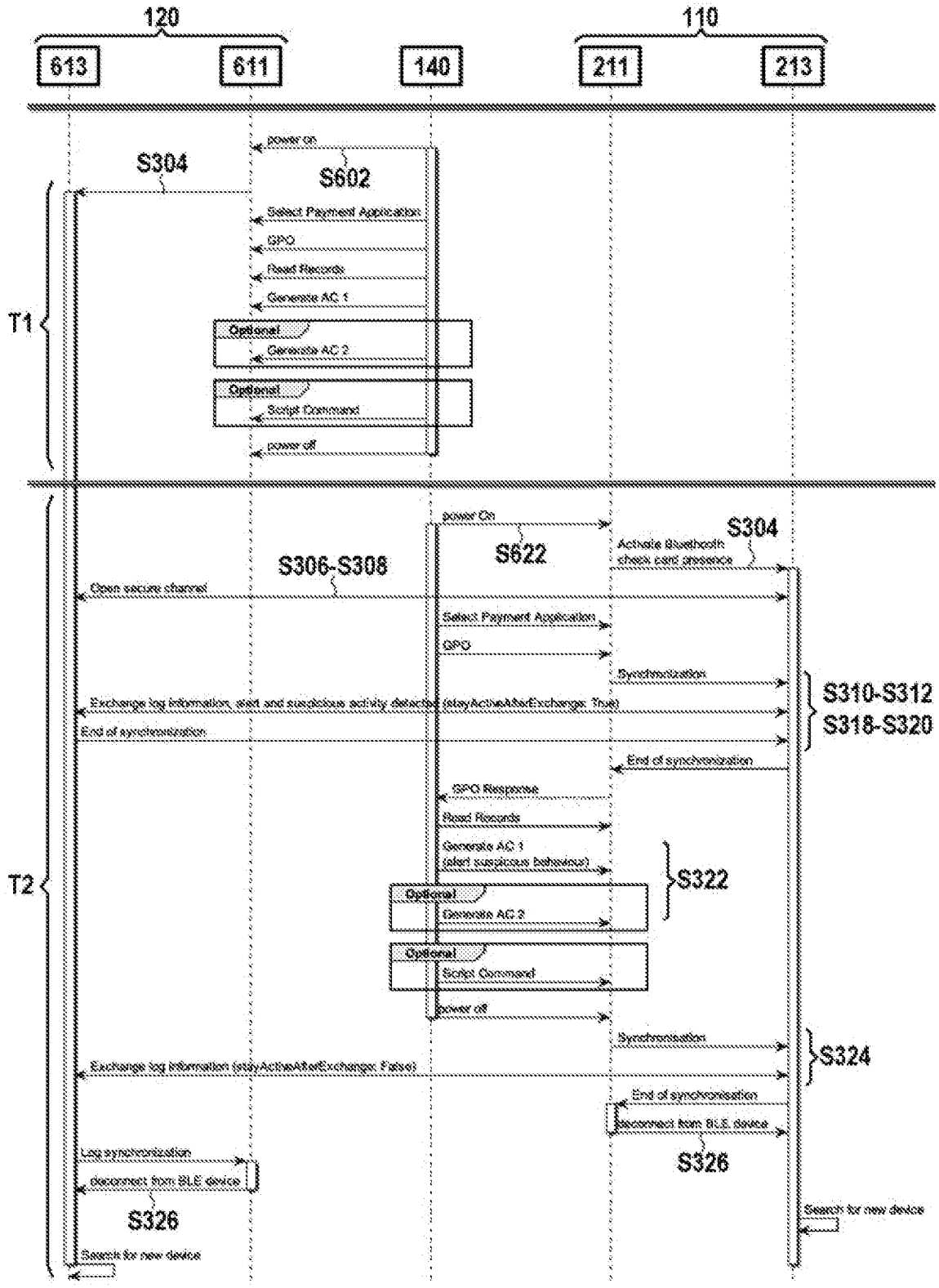
[Fig. 5A]


120
HT4.1
HT3
HT4.2
S310,320
S312
S504
S502
S506
S508
110
HT2.1
HT1
SD
K2
AD2
ID2
HT2.2

[Fig. 5B]


HT4.1
120
HT3
HT4.2
S310,S320
S312
S504
S502
S510
S512
S514
S516
HT2.1
110
HT1
HT2.2

[Fig. 6]


120
110
613
611
140
211
213
power on
S602
S304
Select Payment Application
GPO
Read Records
Generate AC 1
Optional
Generate AC 2
Optional
Script Command
power off
T1
power On
S622
S304
Activate Bluetooth
check card presence
S306-S308
Open secure channel
Select Payment Application
GPO
Synchronization
S310-S312
S318-S320
Exchange log information, alert and suspicious activity detected (stayActiveAfterExchange: True)
End of synchronization
End of synchronization
GPO Response
Read Records
Generate AC 1
(alert suspicious behaviour)
S322
Optional
Generate AC 2
Optional
Script Command
power off
Synchronization
S324
Exchange log information (stayActiveAfterExchange: False)
End of synchronization
Disconnect from BLE device
S326
Log synchronization
disconnect from BLE device
S326
Search for new device
Search for new device
T2

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 871893
FR 1908410

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		
X	EP 2 493 144 A1 (RESEARCH IN MOTION LTD [CA]) 29 août 2012 (2012-08-29) * alinéa [0009] - alinéa [0034] * * figure 1 * -----	1-15	G06Q20/40 G06Q20/16 G06Q20/34 G06F21/44
X	WO 2017/203146 A1 (OBERTHUR TECHNOLOGIES [FR]) 30 novembre 2017 (2017-11-30) * abrégé * * page 3, ligne 33 - page 7, ligne 17 * * page 10, ligne 7 - page 15, ligne 17 * * page 16, ligne 11 - page 20, ligne 20 * * figures 1-5, 8 * -----	1-15	
A	WO 2017/109434 A1 (OBERTHUR TECHNOLOGIES [FR]) 29 juin 2017 (2017-06-29) * abrégé * * page 1, ligne 14 - ligne 30 * * page 14, ligne 21 - page 15, ligne 7 * -----	1-15	
A	WO 2016/142612 A1 (CPMIX SARL [FR]) 15 septembre 2016 (2016-09-15) * page 1, ligne 33 - page 3, ligne 3 * * figures 1, 2 * -----	1-15	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06Q G07F G07G
A	US 2016/267486 A1 (MITRA RAJESHWAR D [US] ET AL) 15 septembre 2016 (2016-09-15) * figures 9, 21 * -----	1-15	

1

Date d'achèvement de la recherche	Examinateur
14 avril 2020	Nicoli, Félix

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

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1908410 FA 871893

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 14-04-2020
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
EP 2493144	A1	29-08-2012	CA 2769086	A1	28-08-2012
			EP 2493144	A1	29-08-2012
			US 2012221464	A1	30-08-2012
WO 2017203146	A1	30-11-2017	EP 3465584	A1	10-04-2019
			FR 3051579	A1	24-11-2017
			WO 2017203146	A1	30-11-2017
WO 2017109434	A1	29-06-2017	EP 3394796	A1	31-10-2018
			FR 3046279	A1	30-06-2017
			WO 2017109434	A1	29-06-2017
WO 2016142612	A1	15-09-2016	EP 3265954	A1	10-01-2018
			FR 3033437	A1	09-09-2016
			RU 2017135010	A	05-04-2019
			SG 11201708163P	A	29-11-2017
			WO 2016142612	A1	15-09-2016
US 2016267486	A1	15-09-2016	AU 2016233536	A1	21-09-2017
			CA 2978327	A1	22-09-2016
			GB 2551932	A	03-01-2018
			JP 2018508091	A	22-03-2018
			US 2016267486	A1	15-09-2016
			US 2019303945	A1	03-10-2019
			WO 2016149156	A1	22-09-2016

EPO FORM P0465