(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 045 896**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **15 62797**

(51) Int Cl[8] : ***G 06 Q 20/40*** *(2017.01)*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 18.12.15.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 23.06.17 Bulletin 17/25.

(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) :** *ORANGE Société anonyme* — FR.

(72) **Inventeur(s) :** BELLEE ARNAUD et DUMANOIS ANTOINE.

(73) **Titulaire(s) :** ORANGE Société anonyme.

(74) **Mandataire(s) :** REGIMBEAU.

(54) PROCEDE DE SECURISATION D'UNE TRANSACTION DEPUIS UN TERMINAL MOBILE.

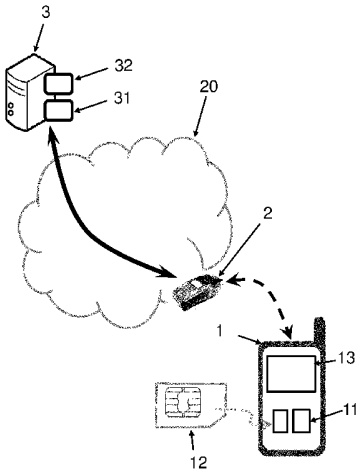
(57) La présente invention concerne un procédé de mise en oeuvre d'une transaction depuis un terminal mobile (1) comprenant un module de traitement de données (11) et un élément de sécurité (12) sur lequel sont stockés une pluralité de modules de transaction, chaque module de transaction étant associé à une carte électronique, et adapté pour autoriser une transaction pour le compte de ladite carte électronique lorsqu'il est activé sur présentation d'un code confidentiel associé,

Le procédé étant caractérisé en ce qu'il comprend la mise en oeuvre par l'élément de sécurité (12) d'étapes de :

(a) réception d'une requête de transaction visant un module de transaction de ladite pluralité ;

(b) réception par un module d'authentification également stocké sur l'élément de sécurité (12) d'un code d'authentification unique valide obtenu via une interface (13) du terminal (1), le module d'authentification stockant les codes confidentiels associés à chacun des modules de transaction, et étant lui-même activable sur présentation dudit code d'authentification ;

(c) Activation par le module d'authentification du module de transaction visé, et émission d'une autorisation de transaction en réponse à ladite requête de transaction.



FR 3 045 896 - A1

PROCEDE DE SECURISATION D'UNE TRANSACTION DEPUIS UN TERMINAL MOBILE

DOMAINE TECHNIQUE GENERAL

La présente invention concerne le domaine des transactions au moyen de terminaux mobiles.

Plus précisément, elle concerne un procédé pour la mise en œuvre d'une transaction depuis un premier terminal mobile sur lequel est dématérialisée une carte électronique.

ETAT DE L'ART

Des systèmes de paiement dits « dématérialisés » (ou « virtualisés ») sont apparus récemment, pour effectuer des transactions (en particulier des paiements) grâce à une carte bancaire dématérialisée sur un support électronique, par exemple un terminal mobile, apte à effectuer un paiement à distance ou en proximité avec une borne de paiement, par exemple de type sans contact (NFC).

La méthode de virtualisation utilisée par ces systèmes de paiement est par exemple la suivante : le client, ou porteur de la carte, entre les informations bancaires inscrites sur sa carte dans une application du terminal contrôlée par un agrégateur, ou fournisseur, du service de paiement. Par exemple, selon une méthode connue, le porteur photographie sa carte bancaire et renseigne le cryptogramme visuel (le code de sécurité qui se situe typiquement au verso). Alternativement, il entre manuellement ces informations, essentielles à l'identification du porteur de la carte lors d'une transaction.

La banque qui est responsable du compte bancaire associé à la carte valide la virtualisation si elle estime que la personne qui a rentré les informations est réellement le client titulaire de la carte, ou porteur. Le cas échéant, sont chargées au niveau du terminal des données de virtualisation correspondant à la carte, ou jeton (en anglais « token »), chiffrées à l'aide de clés de chiffrage connues uniquement par l'organisme bancaire responsable de la carte (ou par l'organisme gérant le schéma bancaire en délégation de l'organisme bancaire responsable de la carte).

On note que pour une carte bancaire dématérialisée, peuvent être disponibles plusieurs modules de transaction dans le token, en particulier si cette carte est associée en même temps à plusieurs réseaux de paiement, par exemple Visa® et CB® en France, tout comme pour une carte bancaire physique.

Les données d'un module de transaction d'un token (données de virtualisation d'une carte bancaire) comprennent :

- Un identifiant,
- Un code supplémentaire (en général le cryptogramme visuel) ;
- Un PIN, c'est-à-dire un code confidentiel personnel, en général à 4 chiffres.

Le troisième doit être connu de l'utilisateur, il lui sera en effet demandé pour valider toute transaction utilisant la carte dématérialisée (en tous cas à partir d'une certaine valeur).

Pour faciliter la gestion d'une pluralité de cartes dématérialisées, il a été proposé l'utilisation d'applications de portefeuille électronique unifié, appelées « wallet ». Une telle application est par exemple décrite dans le document US2015235212. Si l'utilisateur souhaite utiliser l'une de ses cartes pour une transaction, il lui suffit d'ouvrir le wallet comme seule application de paiement, et ce dernier lui propose de choisir entre les cartes (et plus particulièrement entre les modules de transactions des cartes) celle qu'il souhaite utiliser, il n'a plus qu'à saisir le code PIN associé. Les wallets permettent également des fonctions supplémentaires telle que le changement de code PIN.

On constate que le nombre de codes PIN à mémoriser peut être assez élevé s'il a dématérialisé plusieurs cartes. De plus, comme une seule carte peut être associée à plusieurs modules d'un token, cela peut devenir complexe si l'utilisateur veut changer de code PIN. Ce dernier peut par mégarde mettre des codes PIN différents pour plusieurs modules associés à la même carte, et ne pas comprendre pourquoi son code ne marche plus s'il réalise un achat par exemple via Visa au lieu de CB ou inversement.

C'est d'autant plus critique que si l'utilisateur se trompe trois fois de code PIN cela bloque le module associé (et donc bloque partiellement sa carte, ce qui peut être très troublant pour l'utilisateur), et il est alors nécessaire de recommencer toute une procédure de génération de données cryptographique après vérification de l'identité du client (ce dernier doit en général se déplacer à la banque).

Il serait par conséquent souhaitable de disposer d'une nouvelle solution de contrôle des modules des tokens permettant de faciliter la gestion des codes PIN.

PRESENTATION DE L'INVENTION

La présente invention se rapporte ainsi selon un premier aspect à un procédé de mise en œuvre d'une transaction depuis un terminal mobile comprenant un module de traitement de données et un élément de sécurité sur lequel sont stockés une pluralité de modules de transaction, chaque module de transaction étant associé à une carte

électronique, et adapté pour autoriser une transaction pour le compte de ladite carte électronique lorsqu'il est activé sur présentation d'un code confidentiel associé,

Le procédé étant caractérisé en ce qu'il comprend la mise en œuvre par l'élément de sécurité d'étapes de :

(a) réception d'une requête de transaction visant un module de transaction de ladite pluralité ;

(b) réception par un module d'authentification également stocké sur l'élément de sécurité d'un code d'authentification unique valide obtenu via une interface du terminal, le module d'authentification stockant les codes confidentiels associés à chacun des modules de transaction, et étant lui-même activable sur présentation dudit code d'authentification ;

(c) Activation par le module d'authentification du module de transaction visé, et émission d'une autorisation de transaction en réponse à ladite requête de transaction.

L'utilisation d'un élément de sécurité tel qu'une carte d'identification d'abonné pour la mise en d'œuvre d'un module d'authentification qui chapeaute les modules de transaction permet de garder le niveau de sécurité maximal en s'affranchissant de la nécessité de gestion de PINs multiple.

De plus on évite le risque de blocage de modules d'un token en cas de mauvaise saisie d'un code confidentiel, et on évite des failles de sécurité liées à l'utilisateur : ce dernier ne connait plus nécessairement le ou les codes confidentiel, qui restent donc secrets, et qui prévient des vols de carte.

Selon d'autres caractéristiques avantageuses et non limitatives :

- le module de traitement de données met en œuvre un module de gestion des modules de transaction, l'étape (b) comprenant la réception par le module d'authentification d'une requête d'activation du module de transaction visé par la requête de transaction, ladite requête d'activation étant émise par ledit module de gestion.

Le présent procédé s'utilise astucieusement avec un module de gestion de type « wallet » facilitant la mise en œuvre de transactions par l'utilisateur.

- l'étape (b) comprend l'émission préalable par le module de transaction visé, à destination du module de gestion, d'une requête de présentation du code confidentiel associé.

Le module de gestion permet ainsi la mise en œuvre du module d'authentification en tant que « wallet companion » sans avoir à modifier les modules de transaction.

- le module de gestion est configuré pour requérir et obtenir via l'interface ledit code d'authentification.

En particulier, le module de gestion peut simplement contrôler le module d'authentification en remplaçant la requête de présentation du code confidentiel par une requête de présentation du code unique d'authentification, et ce de façon complètement transparente.

- ladite requête d'activation comprend un identifiant du module de transaction visé, et le code d'authentification obtenu via l'interface ;
- l'étape (c) comprend l'émission par le module d'authentification du code confidentiel associé au module de transaction visé en réponse à la requête d'activation.
- l'étape (c) comprend également la réception par le module de transaction visé du code confidentiel associé.

Dans ce premier mode, le module d'authentification fournit le code confidentiel au module de transaction visé de sorte à simuler un fonctionnement classique.

- l'étape (b) comprend la réception par le module d'authentification d'une requête d'activation du module de transaction visé par la requête de transaction, ladite requête d'activation étant émise par ledit module de transaction visé.
- le module d'authentification est configuré pour requérir et obtenir via l'interface ledit code d'authentification.

Dans ce deuxième mode, le module d'authentification et le module de transaction communiquent uniquement au sein de l'élément de sécurité, ce qui prévient physiquement toute attaque visant à intercepter les requêtes de codes.

- l'étape (b) comprend l'émission par le module d'authentification d'une commande d'activation du module de transaction visé en réponse à la requête d'activation.

Dans ce troisième mode, le module d'authentification contrôle complètement le module de transaction, ce qui permet d'éviter la complexité (et donc les aléas de sécurité) associés à une communication au sein de l'OS mobile.

- le module de transaction visé est associé à une carte bancaire, la requête de transaction étant reçue à l'étape (a) depuis un terminal de paiement électronique en communication sans fil avec le terminal, l'autorisation de transaction étant émise à l'étape (c) à destination du terminal de paiement électronique.
- Le procédé comprend en outre une étape (d) de transmission de l'autorisation de transaction à un serveur bancaire associé à ladite carte bancaire via un réseau.

Un terminal mobile configuré en mode NFC peut simuler une carte bancaire disposant de la même fonctionnalité. Il suffit à l'utilisateur de poser son terminal sur le TPE pour autoriser un paiement avec la carte dématérialisée.

- l'élément de sécurité est choisi parmi une carte d'identification d'abonné et un espace d'exécution sécurisé du module de traitement de données du terminal.

Ces éléments de sécurité sont très communs sur les terminaux mobiles, et très fiables.

- le procédé comprend la mise en œuvre préalable d'une digitalisation d'au moins une carte électronique, comprenant la mise en œuvre d'étapes par l'élément de sécurité de :
  - Réception depuis un serveur de données représentatives de ladite carte électronique, lesdites données comprenant un code confidentiel par module de transaction, de sorte à installer le(s) module(s) de transaction adapté(s) pour autoriser une transaction pour le compte de ladite carte électronique ;
  - Réception par le module d'authentification depuis le serveur dudit code confidentiel et d'un identifiant du module de transaction installé ;
  - Association par le module d'authentification du code confidentiel audit module de transaction installé, et stockage.

Une telle digitalisation est fiable et ne nécessite aucune intervention de l'utilisateur. Ce dernier peut alors directement utiliser le module d'authentification.

- le procédé comprend préalablement à la réception depuis le serveur de données représentatives de ladite carte électronique :
  - L'émission par le module de gestion à destination du serveur d'une requête de digitalisation d'au moins une carte électronique comprenant au moins un identifiant de ladite carte électronique ;
  - La génération par le serveur des données représentatives de ladite carte électronique.

Dans le mode de réalisation utilisant un module de gestion de type wallet, celui-ci peut se charger de la configuration automatique du wallet companion, avec une sécurité optimale.

Selon un deuxième aspect, l'invention concerne un élément de sécurité sur lequel sont stockés une pluralité de modules de transaction, chaque module de transaction étant associé à une carte électronique, et adapté pour autoriser une transaction pour le compte de ladite carte électronique lorsqu'il est activé sur présentation d'un code confidentiel associé,

L'élément de sécurité étant configuré pour :

- Recevoir une requête de transaction visant un module de transaction de ladite pluralité ;
- Recevoir au niveau d'un module d'authentification également stocké sur l'élément de sécurité un code d'authentification unique valide obtenu via une interface d'un terminal, le module d'authentification stockant les codes confidentiels associés à

chacun des modules de transaction, et étant lui-même activable sur présentation dudit code d'authentification ;

- activer au moyen du module d'authentification le module de transaction visé, et pour émission d'une autorisation de transaction en réponse à ladite requête de transaction.

Selon d'autres caractéristiques avantageuses et non limitatives est proposé le terminal mobile comprenant un module de traitement de données et l'élément de sécurité selon le deuxième aspect.

Selon un troisième aspect, l'invention concerne un produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé selon le premier aspect de l'invention de mise en œuvre d'une transaction depuis un terminal mobile.

Selon un quatrième aspect, l'invention concerne un moyen de stockage lisible par un équipement informatique sur lequel on trouve ce produit programme d'ordinateur.

PRESENTATION DES FIGURES

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description qui va suivre d'un mode de réalisation préférentiel. Cette description sera donnée en référence aux dessins annexés dans lesquels :

- la figure 1 est un schéma d'une architecture générale de réseau pour la mise en œuvre de l'invention ;
- la figure 2 représente un mode de réalisation de mise en œuvre d'une transaction via le procédé selon l'invention ;
- la figure 3 représente un mode de réalisation de digitalisation d'une carte électronique via le procédé selon l'invention.

DESCRIPTION DETAILLEE

Architecture

En référence à la **figure 1**, l'invention propose un procédé pour la mise en œuvre d'une transaction depuis un terminal mobile 1, en particulier une transaction utilisant une carte dématérialisée sur le terminal 1, i.e. une transaction reproduisant l'utilisation d'une

carte électronique. On verra également plus loin le procédé préalable associé de dématérialisation de la carte électronique sur le terminal 1.

La transaction est typiquement une transaction de paiement (c'est-à-dire que la carte dématérialisée sur le terminal 1 est une carte bancaire), en particulier une transaction de proximité initiée par un terminal de paiement électronique (TPE) 2 tel que l'on trouve dans la plupart des points de vente (par exemple de type EFTPOS). Les TPE possèdent en effet pour la plupart des moyens de communication en champ proche (NFC) à l'origine destinés à interagir avec une carte bancaire physique disposant de cette technologie, mais leur permettant également d'interagir avec le terminal mobile 1.

Le TPE 2 est donc avantageusement d'une part connecté via une liaison sans-fil (NFC, mais aussi Wi-Fi ou Bluetooth) au terminal mobile 1, et d'autre part connecté à au moins un serveur bancaire 3 via un réseau 20 (par exemple Internet).

Alternativement, le paiement peut être à distance (i.e. pas de communication en champ proche avec un TPE 2), le terminal mobile 1 pouvant par exemple être connecté via internet (grâce un réseau de communication mobile, typiquement 4G) à un équipement de paiement éloigné.

On comprendra toutefois que le présent procédé n'est pas limité à des transactions de paiement, mais peut concerner toute transaction reproduisant l'utilisation d'une carte électronique sur le terminal 1, et notamment des télétransmissions de feuilles de soins via Carte Vitale, des validations d'actes médicaux via Carte de Professionnel de Santé, des transmission sécurisée de documents en ligne (par exemple dépôt d'une demande de brevet par carte à puce de mandataire OEB), etc.

Dans la suite de la présente demande, on prendra l'exemple de la transaction de paiement, et l'homme du métier saura transposer à d'autres applications.

Le terminal mobile 1 peut être de n'importe quel type, en particulier smartphone ou des tablettes tactiles. Il comprend un module de traitement de données 11 (un processeur), un module de stockage de données 12, une interface utilisateur (IHM) 13 comprenant par exemple des moyens de saisie et des moyens d'affichage (par exemple un écran tactile, on verra plus loin d'autres alternatives).

Le terminal 1 comprend en outre un élément de sécurité 12. De façon préférée, il s'agit d'un élément adapté pour autoriser une connexion du terminal 1 à un réseau de communication mobile, en particulier une carte d'identification d'abonné. Par « carte d'identification d'abonné », on entend tout circuit intégré capable d'assurer les fonctions d'identification d'un abonné à un réseau via des données qui y sont stockées, et tout particulièrement une carte « SIM » (de l'anglais « Subscriber Identity Module »), ou une

carte « e-UICC » (pour « (embedded)-Universal Integrated Circuit Card ») comprenant des moyens de traitement de données sous la forme d'un microcontrôleur et de la mémoire de type « EEPROM » (pour « Electrically-Erasable Programmable Read-Only Memory »), ou flash. L'invention n'est pas limitée à ce type de module de sécurité. Ainsi, dans un autre exemple de réalisation, le module de sécurité 12 est une zone mémoire sécurisée du terminal mobile tel un composant « TEE » (de l'anglais « Trusted Execution Environment ») embarqué dans le module de traitement de données 11, ou un élément matériel dédié du terminal 1 (par exemple un microcontrôleur, une puce « eSE » pour « (embedded)-Secure Element » ou n'importe quel « Secure Component GP (GlobalPlatform) »), voire un composant amovible de type microSD (« SD » pour Secure Digital).

Le serveur 3 du réseau 20 désigne une plateforme de gestion des transactions, et comprend un module de traitement de données 31, par exemple un processeur et un module de stockage de données 32 tel qu'un disque dur ou de façon préférée un HSM (pour « Hardware Security Module »).

Comme l'on verra plus loin, on comprendra que la notion de « serveur 3 » peut englober une pluralité de serveurs bancaires distincts connectés et adaptés pour communiquer ensemble.

Elément de sécurité

De façon connue, sont stockés sur l'élément de sécurité 12 une pluralité de modules de transaction, chaque module de transaction étant associée à une carte électronique (i.e. un ou plusieurs modules de transaction constituent une version dématérialisée de la carte électronique), et adapté pour autoriser une transaction pour le compte de ladite carte électronique lorsqu'il est activé sur présentation d'un code confidentiel associé. Plus précisément, les modules de transaction sont avantageusement organisés en un ou plusieurs ensembles chacun représentatif d'une carte électronique. En d'autres termes, chaque ensemble regroupe les modules de transaction associés à la même carte électronique.

Dans le cas de transactions de paiement, les cartes électroniques sont des cartes bancaires, et les ensembles de modules de transaction constituent des « tokens » comme évoqué, chaque token étant ainsi représentatif d'une carte de bancaire. Dans la suite de la présente description, on prendra l'exemple de modules de tokens.

Dans le cas d'autres types de transactions, d'autres types de cartes électroniques peuvent être dématérialisées, et de façon générale toute carte à puce permettant une authentification forte, c'est-à-dire dont la possession associée à la connaissance d'un code confidentiel permet de valider l'identité de l'utilisateur et son autorisation à réaliser une action.

De façon générale, un module de transaction contient (entre autres):

- un identifiant de la carte dématérialisée,
- le cas échéant un code supplémentaire (par exemple le cryptogramme visuel),
- un code confidentiel.

Un module de transaction partie d'un token, une fois installé (voir plus loin) présente un identifiant applicatif en deux parties : un préfixe désignant l'origine de l'instance (Visa®, CB®, Mastercard®, Amex®, etc.) et un suffixe unique.

La présente solution se distingue en ce qu'est également stocké sur l'élément de sécurité 12 un module d'authentification stockant les codes confidentiels associés à chacun des modules de transaction, et étant lui-même activable sur présentation d'un code d'authentification.

Plus précisément, le module d'authentification est un « porte-clé » contenant les codes confidentiels, qui agit comme broker vis-à-vis des modules de transaction. Comme on va le voir, cela permet en toute sécurité de gérer une pluralité de modules de transaction avec une clé unique, y compris des modules de transactions avec des fonctionnements différents : les différents codes confidentiels peuvent avoir des longueurs différentes, des spécifications différentes, etc. De plus il permet d'éviter par exemple tout risque de bloquer un module de transaction en cas de trois faux codes : en effet, le module d'authentification ne peut pas se tromper de code. Si l'utilisateur se trompe de code d'authentification, alors le module d'authentification peut être bloqué, cela n'impose pas de refaire la carte (aucun module de transaction n'est bloqué) : il suffit par exemple d'aller en boutique de l'opérateur et de présenter une pièce d'identité pour obtenir ce déblocage selon un mode très sécurisé de réinitialisation à distance, bien connu de l'homme du métier.

On note par ailleurs qu'un module de sécurité, tel qu'une carte d'identification d'abonné est un dispositif physique de confiance quasi-impossible à infecter par un Cheval de Troie, car l'installation d'applications dans ces cartes est limitée à des entités bien identifiées, et contrôlées par l'opérateur et/ou ou l'émetteur du service en lien avec le fabricant de l'élément de sécurité 12.

Dans un mode de réalisation préféré, le module de traitement de données 11 (processeur « non-sécurisé ») du terminal 1 met en œuvre un module de gestion de type « wallet », que complète très astucieusement le module d'authentification 1 appelé alors « wallet companion ». On verra plus loin leurs interactions.

Procédé de mise en œuvre de la transaction

En référence à la **figure 2** va être décrit un exemple de réalisation du présent procédé selon l'invention. On comprendra que cet exemple, dans lequel un utilisateur a dématérialisé trois cartes pour un total de six modules de transaction, n'est qu'illustratif.

Dans une première étape (a), l'élément de sécurité 12 reçoit une requête de transaction visant un module de transaction de ladite pluralité, par exemple émise depuis un TPE 2 en connexion avec le terminal 1, en particulier une fois que l'utilisateur ait signalé vouloir mettre en œuvre une transaction via une carte de paiement dématérialisée qu'il a choisi par exemple sur son wallet. Cette étape est référencée 1. sur la figure 2.

On note que le TPE 2 peut dans cette étape interroger la matrice des moyens de paiement actifs, de sorte à sélectionner (à l'aide d'un filtre) l'instance (le module de transaction) qui sera en charge de la transaction. Par exemple, à supposer que l'utilisateur ait dématérialisé une carte EMV (Entropay MasterCard Visa) associée à la banque B3, il peut disposer de deux modules de transaction associés (référencés T3a/T3c), par exemple respectivement associés à Visa® et CB®. Si le TPE 2 est un terminal étranger n'acceptant que Amex® et Visa®, il choisit ce dernier et vise le module T3a en émettant une GPO (« Get Processing Option ») précisant l'action qu'il souhaite utiliser (ici le paiement d'un montant donné).

Dans une étape (b), le module d'authentification reçoit le code d'authentification unique valide obtenu via une interface 13 du terminal 1. Cette étape peut faire l'objet de plusieurs modes de réalisation.

Dans un premier mode conforme à la figure 2 où est installé sur le terminal 1 (et exécuté via son module de traitement classique 11) un wallet, c'est-à-dire un module de gestion des modules de transaction, c'est ce module de gestion qui sollicite le module d'authentification en lui envoyant une requête d'activation du module de transaction visé par la requête de transaction. De façon préférée, les communications entre le module de gestion et le module d'authentification (et de façon générale les communications entre le module de gestion et tous les modules présents sur l'élément de sécurité 12) sont

sécurisées (chiffrées) de sorte à prévenir toute interception ou manipulation des données échangées.

L'étape (b) comprend alors une sous-étape 2. préalable d'émission par le module de transaction visé d'une requête de présentation du code confidentiel adressée au module de gestion (wallet), de façon totalement naturelle et habituelle.

Toutefois, au lieu de demander à l'utilisateur le code confidentiel associé au module de transaction ayant émis la requête (comme il le ferait habituellement), le module de gestion demande le code d'authentification du module d'authentification. En d'autres termes, le module de gestion est configuré pour requérir et obtenir via l'interface 13 ledit code d'authentification. Il est à noter que le code peut être saisi directement via un clavier (notamment tactile) de l'interface 13, mais qu'également le code peut être généré suite à la vérification de l'identité de l'utilisateur sur le terminal 1, par exemple via un lecteur d'empreintes digitales, un module de reconnaissance vocale, ou autre. A ce titre, le code d'authentification peut être seulement une commande sous une forme sécurisée (par exemple un message contenant une clé), représentative de l'identité vérifiée de l'utilisateur, et donc de l'autorisation à activer le module d'authentification.

Le module de gestion génère alors ladite requête d'activation, cette dernière comprenant avantageusement un identifiant du module de transaction visé (reçu depuis ce dernier via la requête de présentation de son code confidentiel), et le code d'authentification obtenu via l'interface 13. Il s'agit de la sous-étape 3. représentée sur la figure 2.

On note que le présent mode de réalisation permet d'utiliser des modules de transactions d'origine (tel que fournis par un serveur 3 par exemple), ces derniers ne sachant même pas qu'ils sont contrôlés par un module d'authentification. Il suffit juste de configurer adéquatement le module de gestion. Comme expliqué, ce mode de réalisation supporte n'importe quelles exigences des modules de transaction, et en particulier des structures et des longueurs variées de codes confidentiels. Aucune normalisation n'est nécessaire.

Alternativement, dans un second mode de réalisation, le module de transaction et le module d'authentification peuvent communiquer en direct, en particulier au sein de l'élément sécurisé 12 (en d'autres termes le module d'authentification reçoit la requête d'activation du module de transaction visé par la requête de transaction, ladite requête d'activation étant émise par ledit module de transaction visé et remplaçant la requête de présentation du code confidentiel associé), cela impliquant que le module d'authentification soit lui-même configuré pour requérir et obtenir via l'interface 13 ledit code d'authentification.

On note que sont possibles des configurations hybrides utilisant un module de gestion par lequel ne transitent que certaines des requêtes (par exemple celle de présentation du code confidentiel associé au module de transaction visé, tout en ayant le module d'authentification requérant lui-même son code d'authentification).

Sur réception du code d'authentification valide (sinon il renvoie un message d'erreur, et de façon préférée se bloque au bout de trois erreurs) le module d'authentification s'active, et dans une étape (c) il active le module d'authentification du module de transaction visé, de sorte que ce dernier émette in fine une autorisation de transaction en réponse à ladite requête de transaction.

Dans le premier mode de réalisation, le module d'authentification émet le code confidentiel associé au module de transaction visé en réponse à la requête d'activation, soit à destination du module de gestion de type wallet qui le renvoie au module de transaction (sous-étape 4. représenté à la figure 2), soit directement au module de transaction.

Alternativement (en particulier dans le second mode de réalisation où le module de transaction et le module d'authentification communiquent directement de sorte qu'il n'y a pas nécessairement de requête de présentation d'un code), le module d'authentification émet d'une commande d'activation du module de transaction visé (plutôt que le code seul) en réponse à la requête d'activation, commande qui comprend le cas échéant le code confidentiel associé, ce qui permet d'améliorer encore la sécurité d'un cran. Toute interception de requêtes et manipulation de l'élément de sécurité 12 devient impossible.

Le module de transaction activé peut alors finir la mise en œuvre de la transaction de manière classique. De façon préférée, dans le cas de paiements, le procédé comprend à ce titre en outre une étape (d) de transmission de l'autorisation de transaction à un serveur bancaire 3 associé à ladite carte bancaire via le réseau 20. Typiquement, dans la sous-étape 5. l'autorisation de paiement est transférée au TPE 2 de sorte que ce dernier puisse rapporter auprès du serveur 3 dans une sous-étape 6.

Plus précisément, il est généralement prévu que :

- lors de l'émission de la GPO, le TPE 2 a gardé un contexte pour la transaction et s'est mis en attente d'une nouvelle présentation de du terminal 1 pour terminer le paiement en cours ;
- suite à l'entrée du code d'authentification, l'utilisateur est invité à présenter le terminal 1 à nouveau au TPE 2 ;

- reconnaissant le terminal 1, le TPE 2 émet à nouveau la même GPO qu'attend l'instance déverrouillée (le module de transaction visé à présent activé). Cette double émission correspond à des spécifications officielle pour s'assurer de la sureté de la transaction ;
- le module de transaction peut alors insérer des informations de paiement et signer l'ensemble dans sa réponse vers le TPE 2 ;
- le TPE 2 peut ensuite finir la transaction via les serveurs de paiement 3.

Procédé de digitalisation d'une carte électronique

En référence à la **figure 3**, la présente invention concerne également un procédé de digitalisation d'une carte électronique avantageusement mis en œuvre préalablement au procédé de mise en œuvre d'une transaction tel que précédemment décrit.

Si c'est la première carte dématérialisée au niveau du terminal 1, ce deuxième procédé peut commencer par une étape 0. d'initialisation par le module de gestion du module d'authentification. Par exemple, l'utilisateur défini son code d'authentification.

La dématérialisation d'une carte est avantageusement initiée au niveau du module de gestion, qui requiert auprès d'un serveur 3 la digitalisation d'au moins une carte électronique, la requête associée comprenant au moins un identifiant de ladite carte électronique.

Dans le cas des cartes bancaires, cette étape est bien connue : on peut par exemple prendre en photo la carte physique. Le serveur destinataire 3 est plus particulièrement un TRQ « Token Requestor », qui peut être par exemple de type SPS « Shared Payment Server », partagé entre plusieurs opérateurs (d'où le Shared). Il joue le rôle de requérir des tokens, à savoir qu'il est mandaté par des clients finaux pour aller demander à un organisme bancaire de lui fournir un moyen technique virtualisé de paiement avec des caractéristiques qu'il précise.

Pour cela il contacte un TSP (étape 1. de la figure 3) qui est lui-même en communication avec les serveurs bancaires évoqués précédemment. Le TSP est un Token Service Provider qui est lui en charge de fournir un moyen technique de paiement virtualisé précédemment discuté avec les caractéristiques demandées et un certain nombre de contraintes d'utilisation relatives à la politique de sécurité qu'il décide. Il est aussi en charge d'analyser la légitimité de la demande puisque c'est lui qui génère le moyen de paiement virtualisé.

Plus précisément, sur réception de la requête de digitalisation de la carte électronique, le TRQ contacte le TSP correspondant au type de carte (étape 2. de la figure

3). Il aide le TSP à déterminer la légitimité de la demande, ce dernier le cas échéant accepte la dématérialisation, génère des données représentatives de ladite carte électronique, et les renvoie au TRQ.

A partir de là l'élément de sécurité 12 du terminal 1 met en œuvre des étapes de :

- Réception depuis le serveur 3 (en l'espèce le TRQ) des données représentatives de ladite carte électronique, lesdites données comprenant un ou plusieurs code(s) confidentiel(s) (étape 3.), de sorte à installer le(s) module(s) de transaction adapté(s) pour autoriser une transaction pour le compte de ladite carte électronique (i.e. l'ensemble des modules de transaction représentatifs de la carte) ;
- Réception par le module d'authentification depuis le serveur 3 desdit code(s) confidentiel(s) et d'un identifiant du/des module(s) de transaction installé(s) (étape 4.) ; et
- Association par le module d'authentification du/des code(s) confidentiel(s) au(x)dit(s) module(s) de transaction installé(s), et stockage.

Le module d'authentification est alors configuré pour la mise en œuvre du procédé de mise en œuvre d'une transaction via le terminal mobile 1, en utilisant la carte nouvellement dématérialisée.

Elément de sécurité et terminal

Selon un deuxième aspect, l'invention concerne l'élément de sécurité 12 pour la mise en œuvre du procédé selon le premier aspect.

Sur ce dernier sont stockés une pluralité de modules de transaction, chaque module de transaction étant associé à une carte électronique (et l'ensemble de modules de transaction associés à une même carte étant représentatif de ladite carte), et adapté pour autoriser une transaction pour le compte de ladite carte électronique lorsqu'il est activé sur présentation d'un code confidentiel associé.

L'élément de sécurité 12 est configuré pour :

- Recevoir une requête de transaction visant un module de transaction de ladite pluralité (et le cas échéant émettre depuis le module de transaction visé une requête de présentation du code confidentiel associé) ;
- Recevoir au niveau d'un module d'authentification également stocké sur l'élément de sécurité 12 (au sein d'une requête d'activation comprenant également un identifiant du module de transaction visé) un code d'authentification unique valide

obtenu via une interface 13 d'un terminal 1, le module d'authentification stockant les codes confidentiels associés à chacun des modules de transaction, et étant lui-même activable sur présentation dudit code d'authentification ;

- activer au moyen du module d'authentification le module de transaction visé, et pour émission d'une autorisation de transaction en réponse à ladite requête de transaction.

Est également proposé le terminal mobile 1 comprenant un module de traitement de données 11 et un tel élément de sécurité 12, avantageusement sous la forme d'une carte d'identification d'abonné, mais également sous la forme d'un TEE ou d'un composant externe éventuellement amovible, etc.

Produit programme d'ordinateur

Selon un troisième et un quatrième aspects, l'invention concerne un produit programme d'ordinateur comprenant des instructions de code pour l'exécution (en particulier sur l'élément de sécurité 12 du terminal 1) d'un procédé selon le premier aspect de l'invention de mise en œuvre d'une transaction depuis le terminal mobile 1, ainsi que des moyens de stockage lisibles par un équipement informatique (une mémoire de l'élément de sécurité 12) sur lequel on trouve ce produit programme d'ordinateur.

REVENDICATIONS

1. Procédé de mise en œuvre d'une transaction depuis un terminal mobile (1) comprenant un module de traitement de données (11) et un élément de sécurité (12) sur lequel sont stockés une pluralité de modules de transaction, chaque module de transaction étant associé à une carte électronique, et adapté pour autoriser une transaction pour le compte de ladite carte électronique lorsqu'il est activé sur présentation d'un code confidentiel associé,

Le procédé étant caractérisé en ce qu'il comprend la mise en œuvre par l'élément de sécurité (12) d'étapes de :

(a) réception d'une requête de transaction visant un module de transaction de ladite pluralité ;

(b) réception par un module d'authentification également stocké sur l'élément de sécurité (12) d'un code d'authentification unique valide obtenu via une interface (13) du terminal (1), le module d'authentification stockant les codes confidentiels associés à chacun des modules de transaction, et étant lui-même activable sur présentation dudit code d'authentification ;

(c) Activation par le module d'authentification du module de transaction visé, et émission d'une autorisation de transaction en réponse à ladite requête de transaction.

2. Procédé selon la revendication 1, dans lequel le module de traitement de données (11) met en œuvre un module de gestion des modules de transaction, l'étape (b) comprenant la réception par le module d'authentification d'une requête d'activation du module de transaction visé par la requête de transaction, ladite requête d'activation étant émise par ledit module de gestion.

3. Procédé selon la revendication 2, dans lequel l'étape (b) comprend l'émission préalable par le module de transaction visé, à destination du module de gestion, d'une requête de présentation du code confidentiel associé.

4. Procédé selon la revendication 3, dans lequel le module de gestion est configuré pour requérir et obtenir via l'interface (13) ledit code d'authentification.

5. Procédé selon la revendication 4, dans lequel ladite requête d'activation comprend un identifiant du module de transaction visé, et le code d'authentification obtenu via l'interface (13).

6. Procédé selon l'une des revendications 2 à 5, dans lequel l'étape (c) comprend l'émission par le module d'authentification du code confidentiel associé au module de transaction visé en réponse à la requête d'activation.

7. Procédé selon la revendication 6, dans lequel l'étape (c) comprend également la réception par le module de transaction visé du code confidentiel associé.

8. Procédé selon la revendication 1, dans lequel l'étape (b) comprend la réception par le module d'authentification d'une requête d'activation du module de transaction visé par la requête de transaction, ladite requête d'activation étant émise par ledit module de transaction visé.

9. Procédé selon la revendication 8, dans lequel le module d'authentification est configuré pour requérir et obtenir via l'interface (13) ledit code d'authentification.

10. Procédé selon l'une des revendications 2 à 5 et 8 à 9, dans lequel l'étape (b) comprend l'émission par le module d'authentification d'une commande d'activation du module de transaction visé en réponse à la requête d'activation.

11. Procédé selon l'une des revendications 1 à 10, dans lequel le module de transaction visé est associé à une carte bancaire, la requête de transaction étant reçue à l'étape (a) depuis un terminal de paiement électronique (2) en communication sans fil avec le terminal (1), l'autorisation de transaction étant émise à l'étape (c) à destination du terminal de paiement électronique (2).

12. Procédé selon la revendication 11, comprenant en outre une étape (d) de transmission de l'autorisation de transaction à un serveur bancaire (3) associé à ladite carte bancaire via un réseau (20).

13. Procédé selon l'une des revendications 1 à 12, dans lequel l'élément de sécurité (12) est choisi parmi une carte d'identification d'abonné et un espace d'exécution sécurisé du module de traitement de données (11) du terminal (1).

14. Procédé selon l'une des revendications 1 à 13, dans lequel ladite pluralité de modules de transaction est organisée en un ou plusieurs ensembles tels que tous les modules de transaction d'un ensemble sont associés à la même carte électronique, de sorte que chaque ensemble de modules de transaction est représentatif de ladite carte électronique.

15. Procédé selon l'une des revendications 1 à 13, comprenant la mise en œuvre préalable d'une digitalisation d'au moins une carte électronique, comprenant la mise en œuvre d'étapes par l'élément de sécurité (12) de :

- Réception depuis un serveur (3) de données représentatives de ladite carte électronique, lesdites données comprenant un ou plusieurs codes confidentiels, de sorte à installer le ou les modules de transaction adaptés pour autoriser une transaction pour le compte de ladite carte électronique ;
- Réception par le module d'authentification depuis le serveur (3) dudit code confidentiel et d'un identifiant du module de transaction installé ;
- Association par le module d'authentification du code confidentiel audit module de transaction installé, et stockage.

16. Procédé selon la revendication 15 en combinaison avec la revendication 2, comprenant préalablement à la réception depuis le serveur (3) de données représentatives de ladite carte électronique :

- L'émission par module de gestion à destination du serveur (3) d'une requête de digitalisation d'au moins une carte électronique comprenant au moins un identifiant de ladite carte électronique ;
- La génération par le serveur (3) des données représentatives de ladite carte électronique.

17. Elément de sécurité (12) sur lequel sont stockés une pluralité de modules de transaction, chaque module de transaction étant associé à une carte électronique, et adapté pour autoriser une transaction pour le compte de ladite carte électronique lorsqu'il est activé sur présentation d'un code confidentiel associé,
l'élément de sécurité (12) étant configuré pour :

- Recevoir une requête de transaction visant un module de transaction de ladite pluralité ;

- Recevoir au niveau d'un module d'authentification également stocké sur l'élément de sécurité (12) un code d'authentification unique valide obtenu via une interface (13) d'un terminal (1), le module d'authentification stockant les codes confidentiels associés à chacun des modules de transaction, et étant lui-même activable sur présentation dudit code d'authentification ;
- activer au moyen du module d'authentification le module de transaction visé, et pour émission d'une autorisation de transaction en réponse à ladite requête de transaction.

18. Terminal mobile (1) comprenant un module de traitement de données (11) et un élément de sécurité selon la revendication 17.

19. Produit programme d'ordinateur comprenant des instructions de code pour l'exécution d'un procédé selon l'une des revendications 1 à 16 de mise en œuvre d'une transaction depuis un terminal mobile (1), lorsque ledit programme est exécuté par un ordinateur.

20. Moyen de stockage lisible par un équipement informatique sur lequel un produit programme d'ordinateur comprend des instructions de code pour l'exécution d'un procédé selon l'une des revendications 1 à 16 de mise en œuvre d'une transaction depuis un terminal mobile (1).

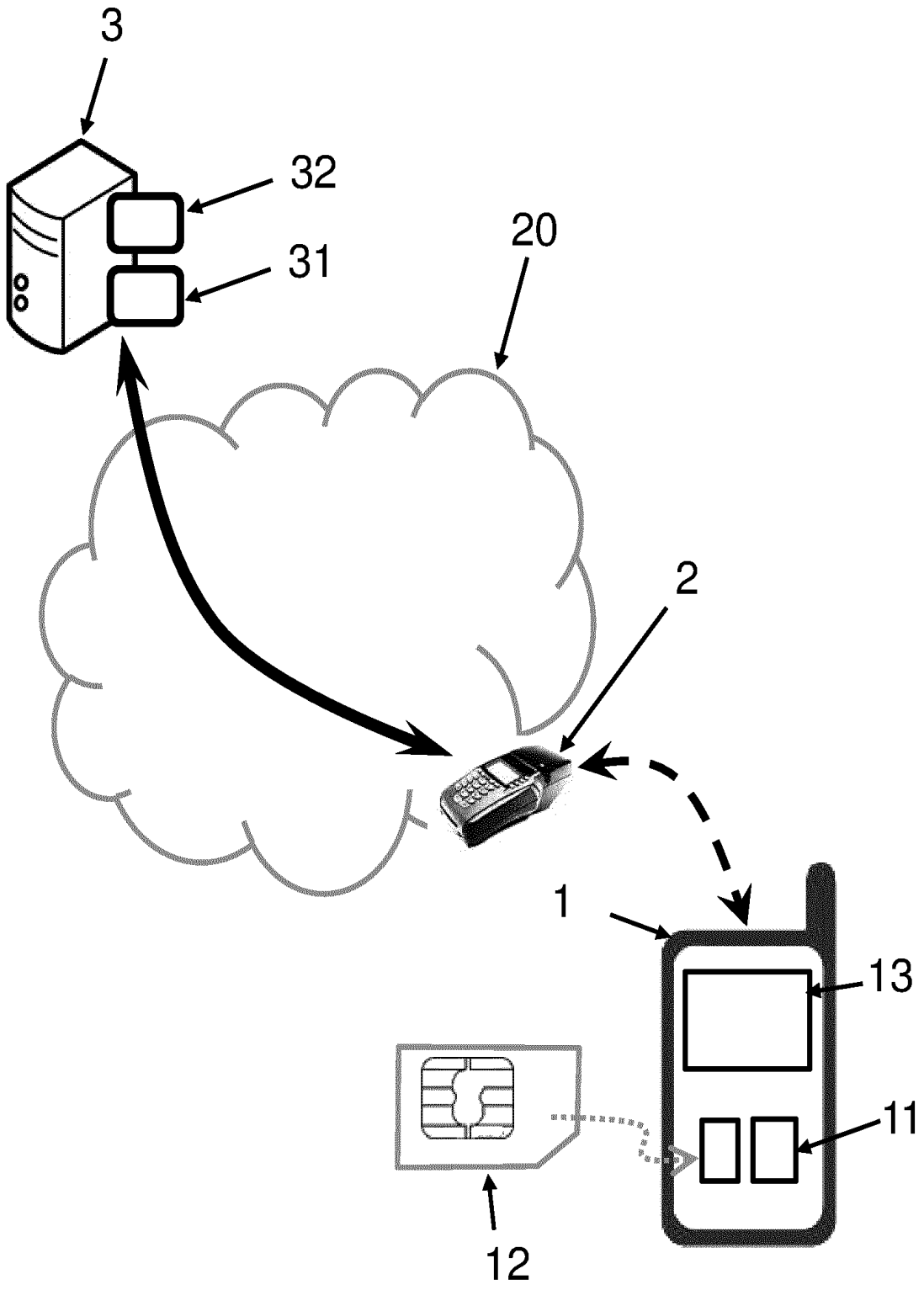


FIG. 1

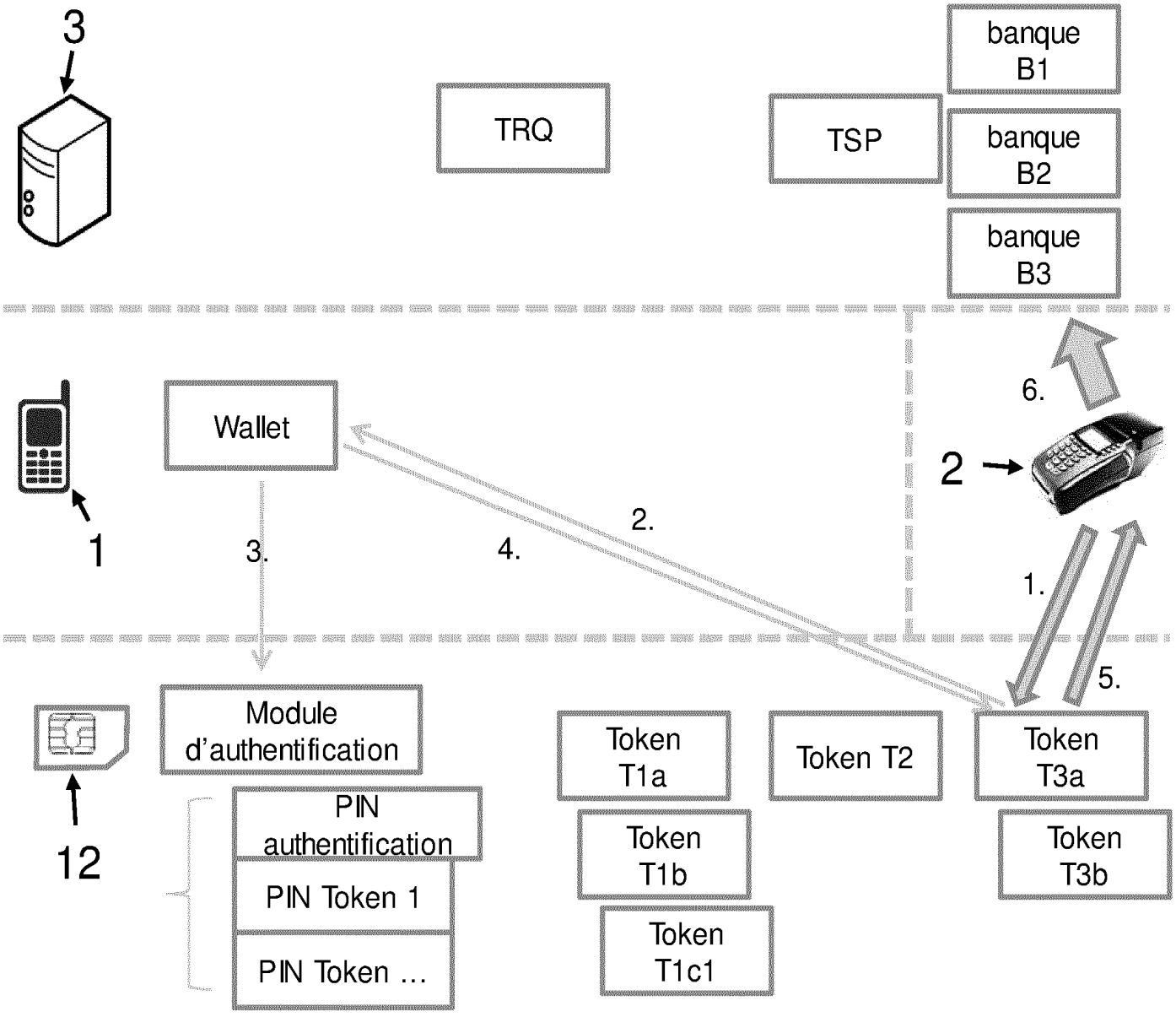

3
TRQ
TSP
banque B1
banque B2
banque B3
6.
Wallet
2
2.
3.
4.
1.
5.
1
12
Module d'authentification
PIN authentification
PIN Token 1
PIN Token ...
Token T1a
Token T1b
Token T1c1
Token T2
Token T3a
Token T3b

FIG. 2

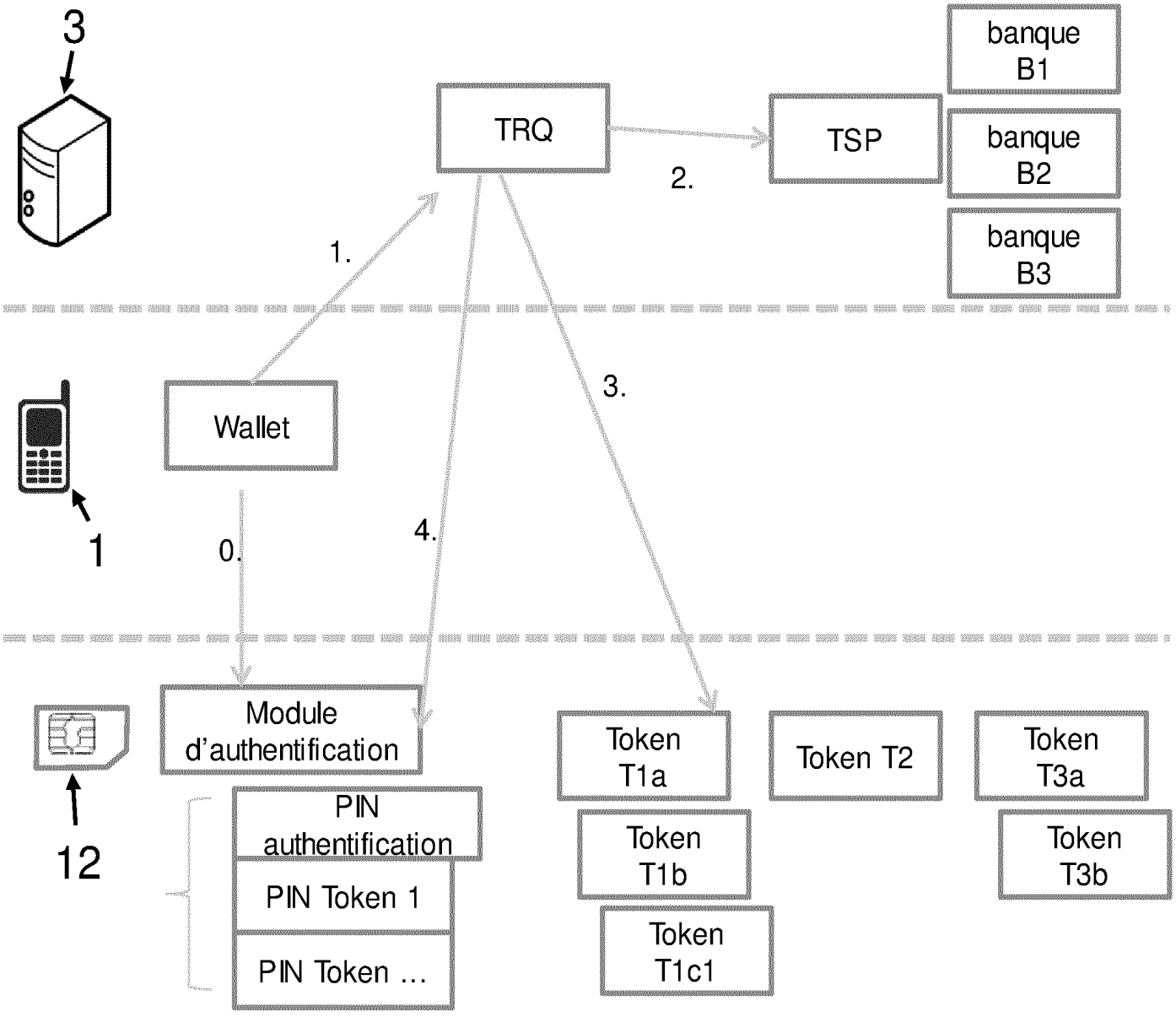

3
banque B1
TRQ
TSP
banque B2
banque B3
2.
1.
3.
Wallet
1
0.
4.
Module d'authentification
PIN authentification
PIN Token 1
PIN Token ...
12
Token T1a
Token T2
Token T3a
Token T1b
Token T3b
Token T1c1

FIG. 3

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 821855
FR 1562797

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	WO 2013/092796 A1 (MORPHO [FR]) 27 juin 2013 (2013-06-27) * le document en entier * -----	1-20	G06Q20/40
A	CN 104 602 224 A (ZHEJIANG RONGCHUANG INFORMATION INDUSTRY CO LTD) 6 mai 2015 (2015-05-06) * le document en entier * -----	15,16	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06Q

Date d'achèvement de la recherche	Examinateur
23 mai 2016	Aupiais, Brigitte

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)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1562797 FA 821855

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 23-05-2016
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
WO 2013092796 A1	27-06-2013	CN 104115173 A	22-10-2014
		EP 2795551 A1	29-10-2014
		FR 2985063 A1	28-06-2013
		JP 2015504207 A	05-02-2015
		KR 20140103153 A	25-08-2014
		RU 2014125072 A	10-02-2016
		US 2015020160 A1	15-01-2015
		WO 2013092796 A1	27-06-2013
CN 104602224 A	06-05-2015	AUCUN	

EPO FORM P0465