Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2946143 A1 2015/10/22

(21) 2 946 143

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) **Date de dépôt PCT/PCT Filing Date:** 2015/04/10
(87) **Date publication PCT/PCT Publication Date:** 2015/10/22
(85) **Entrée phase nationale/National Entry:** 2016/10/14
(86) **N° demande PCT/PCT Application No.:** EP 2015/057836
(87) **N° publication PCT/PCT Publication No.:** 2015/158618
(30) **Priorité/Priority:** 2014/04/18 (FR1453568)

(51) **Cl.Int./Int.Cl.** ***G06Q 20/08*** (2012.01), ***G06Q 20/32*** (2012.01), ***G06Q 20/34*** (2012.01)

(71) **Demandeur/Applicant:**
INGENICO GROUP, FR

(72) **Inventeur/Inventor:**
QUENTIN, PIERRE, FR

(74) **Agent:** GOUDREAULT, DOMINIC

(54) **Titre : PROCEDE DE TRAITEMENT DE DONNEES TRANSACTIONNELLES, DISPOSITIF ET PROGRAMME CORRESPONDANT**
(54) **Title: METHOD FOR PROCESSING TRANSACTION DATA, DEVICE AND CORRESPONDING PROGRAM**

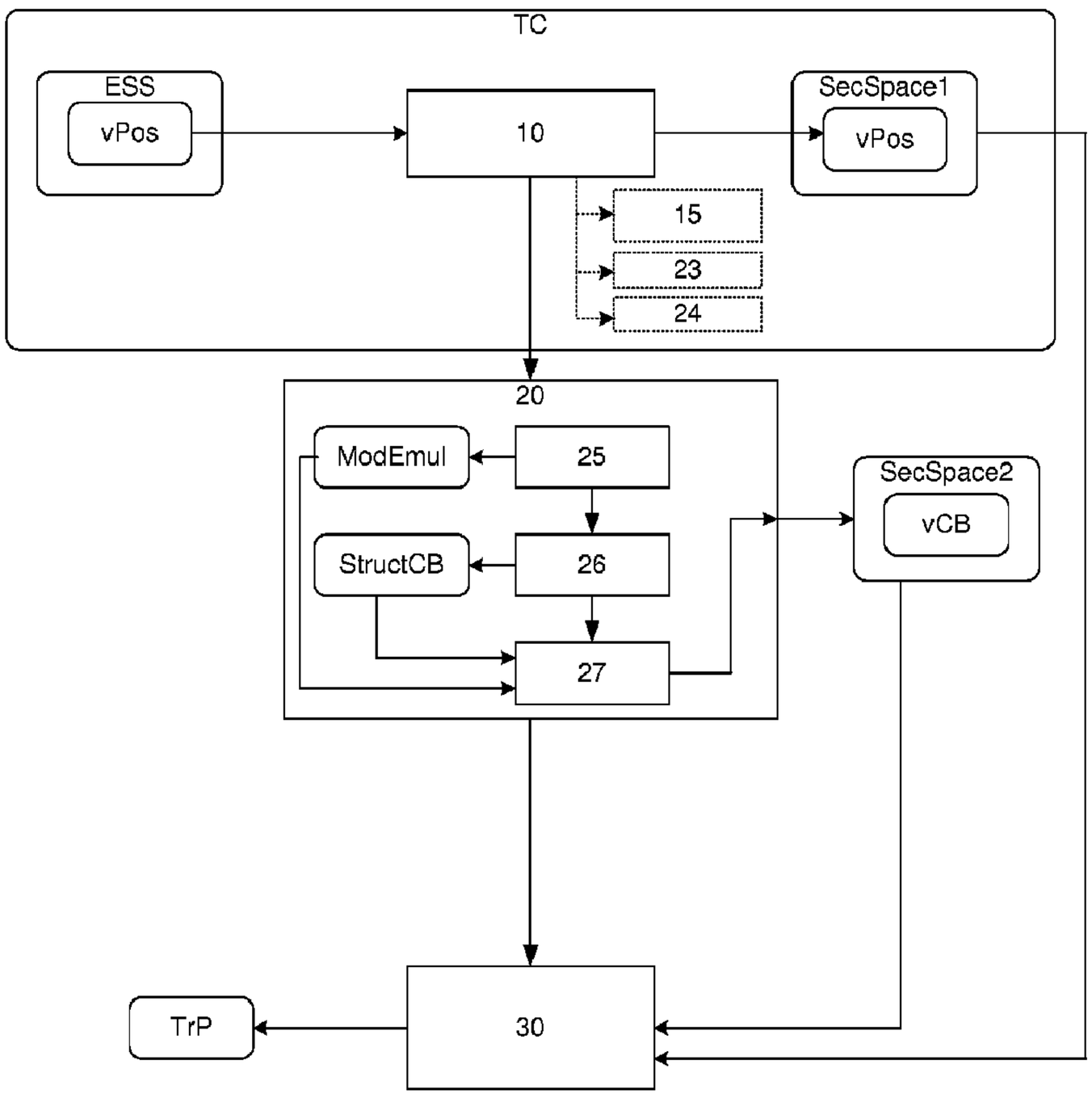

Figure 1

(57) **Abrégé/Abstract:**
L'invention se rapporte à un procédé de traitement de données transactionnelles représentatives d'un paiement effectué par un utilisateur à partir d'un terminal de communication (TC). Selon l'invention un tel procédé comprend: - une étape de chargement

(21) **2 946 143**

(13) **A1**

(57) **Abrégé(suite)/Abstract(continued):**
(10) d'un terminal de paiement virtuel (vPos), au sein d'un premier espace mémoire sécurisé (SecSpace1) du terminal de communication (TC), ledit terminal virtuel (vPos) se présentant sous la forme d'un module logiciel enregistré au sein d'un espace de stockage sécurisé du terminal de communication (TC); - une étape de chargement (20), au sein d'un deuxième espace sécurisé (SecSpace2), d'au moins une carte de paiement virtuelle (vCB); - une étape de traitement (30) par le terminal de paiement virtuel (vPos) d'une transaction de paiement à l'aide de ladite au moins une carte de paiement virtuelle (v CB).

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
22 octobre 2015 (22.10.2015)

WIPO | PCT

(10) Numéro de publication internationale
WO 2015/158618 A1

(51) Classification internationale des brevets :
G06Q 20/02 (2012.01) *G06Q 20/34* (2012.01)
G06Q 20/32 (2012.01)

(21) Numéro de la demande internationale :
PCT/EP2015/057836

(22) Date de dépôt international :
10 avril 2015 (10.04.2015)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1453568 18 avril 2014 (18.04.2014) FR

(71) Déposant : **INGENICO GROUP** [FR/FR]; 28/32 Boulevard de Grenelle, 75015 Paris (FR).

(72) Inventeur : **QUENTIN, Pierre**; 26 rue Paul Delinge, F-95880 Enghien-les-bains (FR).

(74) Mandataire : **VIDON BREVETS & STRATÉGIE**; 90333, B, Technopôle Atalante, 16B rue de Jouanet, F-35703 Rennes Cedex 7 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

(54) **Title** : METHOD FOR PROCESSING TRANSACTION DATA, DEVICE AND CORRESPONDING PROGRAM

(54) **Titre** : PROCÉDÉ DE TRAITEMENT DE DONNÉES TRANSACTIONNELLES, DISPOSITIF ET PROGRAMME CORRESPONDANT

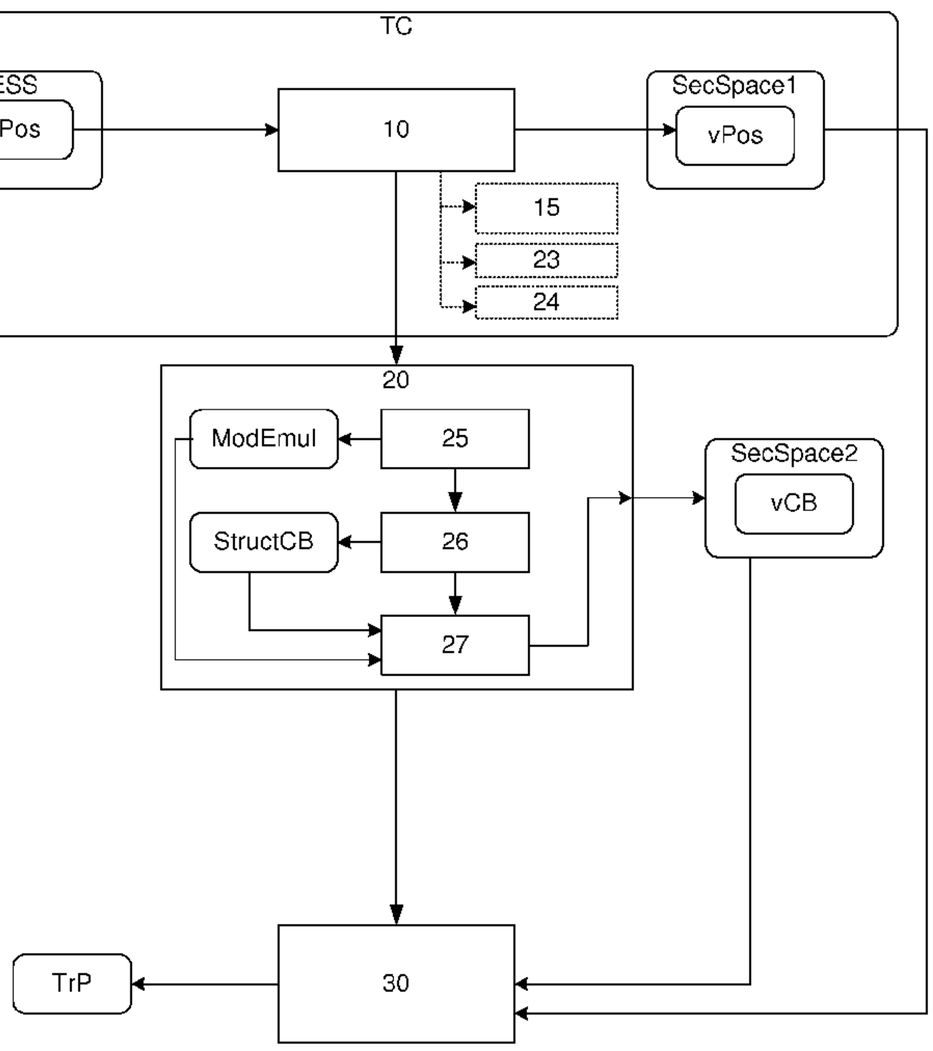

Figure 1

(57) Abstract : The invention relates to a method for processing transaction data representing a payment made by a user from a communication terminal (TC). According to the invention, such a method comprises: a step of loading (10) a virtual payment terminal (vPos) in a first secure memory space (SecSpace1) of the communication terminal (TC), said virtual terminal (vPos) being provided in the form of a software module stored in a secure storage space of the communication terminal (TC); a step of loading (20), in a second secure space (SecSpace2), at least one virtual payment card (vCB); a step of processing (30), by the virtual payment terminal (vPos), of a payment transaction by means of said at least one virtual payment card (vCB).

(57) Abrégé : L'invention se rapporte à un procédé de traitement de données transactionnelles représentatives d'un paiement effectué par un utilisateur à partir d'un terminal de communication (TC). Selon l'invention un tel procédé comprend: - une étape de chargement (10) d'un terminal de paiement virtuel (vPos), au sein d'un premier espace mémoire sécurisé (SecSpace1) du terminal de communication (TC), ledit terminal virtuel (vPos) se présentant sous la forme d'un module logiciel enregistré au sein d'un espace de

[Suite sur la page suivante]

WO 2015/158618 A1

WO 2015/158618 A1

stockage sécurisé du terminal de communication (TC); - une étape de chargement (20), au sein d'un deuxième espace sécurisé (SecSpace2), d'au moins une carte de paiement virtuelle (vCB); - une étape de traitement (30) par le terminal de paiement virtuel (vPos) d'une transaction de paiement à l'aide de ladite au moins une carte de paiement virtuelle (v CB).

Procédé de traitement de données transactionnelles, dispositif et programme correspondant

1. Domaine de l'invention

L'invention se rapporte au domaine des terminaux de paiement. La technique se rapporte plus particulièrement à des terminaux de paiement pouvant être mis en œuvre à l'aide d'un terminal d'utilisateur (tel qu'un terminal de communication de type smartphone, tablette, PDA ou ordinateur personnel).

L'invention s'inscrit dans un nouveau paradigme de mise en œuvre d'un paiement. Plus particulièrement, l'invention s'inscrit dans un système de paiement dans lequel l'utilisateur est muni d'un dispositif de paiement. Il s'agit de permettre à l'utilisateur de réaliser des paiements à l'aide d'un dispositif en sa possession afin de garantir un paiement de type "card present" même pour des paiements effectués pour des services en ligne.

2. Art Antérieur

De nombreuses solutions ont été proposées pour permettre à des utilisateurs d'effectuer des paiements à l'aide d'un terminal de communication tout en utilisant physiquement une carte de paiement (c'est à dire en utilisant les informations disponibles sur une puce ou sur une bande magnétique). Un tel type de paiement est appelé paiement de type "card present", qui diffère d'un paiement de type "card non present" dans lequel ce sont les informations inscrites sur la carte (numéro de carte, non du titulaire, date de validité) qui sont utilisées. Il est communément admis que des paiements (des transactions) qui sont effectuées en utilisant les données de la puce ou de la bande magnétique ont un degré de sécurisation supérieur aux paiements effectués en utilisant les informations inscrites sur la carte elle-même. Il est donc préférable que tout paiement puisse soit réalisé en mode "card present". L'essor des paiements en ligne a mis en évidence un besoin important. En effet, le nombre de paiements frauduleux effectués sur Internet a permis de prendre conscience de la nécessité de sécuriser ce type de paiement afin de juguler les fraudes.

Ainsi, par exemple, le dispositif de paiement décrit dans le brevet US2005/0236480 permet de se connecter à un terminal de communication de type téléphone. Un tel dispositif assure en théorie que le paiement ne puisse pas être répudié. C'est à dire que le paiement, dans la mesure où il a été effectué en utilisant une carte bancaire appartenant à l'utilisateur du terminal de communication et du dispositif adjoint, ne puisse pas ultérieurement faire l'objet d'une contestation de la part de l'utilisateur. Un tel dispositif de paiement est intéressant d'un point de vue théorique : il permet en effet à l'utilisateur de connecter un dispositif complémentaire à son

téléphone pour le transformer en terminal de paiement. Malheureusement, en pratique, un tel dispositif se heurte à de nombreux problèmes. Le premier est que ce dispositif est adapté à un modèle de terminal particulier. Il est nécessaire de prévoir un modèle de dispositif pour chaque modèle de terminal. Compte tenu de nombre très important de modèles de téléphones, une telle solution n'est pas économiquement viable. En second lieu, un tel dispositif peut être aisément compromis. Cela signifie qu'il est relativement aisé de subtiliser temporairement un tel dispositif, de le modifier (par exemple pour introduire un module de fraude) et d'utiliser par la suite les données obtenues par le module de fraude pour cloner une carte. En troisième lieu, un tel dispositif n'est pas adapté à une utilisation contemporaine des moyens de paiement. En effet, un dispositif de ce type nécessite une transmission d'une transaction de paiement par l'intermédiaire d'un SMS (de l'anglais pour "Short Message Service") ou d'un autre type de message équivalent (i.e. utilisant une architecture de téléphonie 2G). Or, actuellement, des moyens de réception et de transmission de données basés sur des protocoles Web sont largement plébiscités, notamment de fait de leur universalité.

Ainsi, il existe un besoin de fournir une technique qui permette de réaliser un paiement de type "card present" tout en étant adapté d'une part à des impératifs de passage à l'échelle, de sécurisation des données de la carte bancaire et des transactions.

3. Résumé de l'invention

L'invention ne pose pas ces problèmes de l'art antérieur. Plus particulièrement, l'invention apporte une solution simple à la problématique préalablement identifiée. L'invention se rapporte ainsi à une mise en œuvre, au sein d'un terminal de communication d'un utilisateur, d'un terminal de paiement virtuel. Plus spécifiquement, le terminal de paiement virtuel est mis en œuvre au sein d'un espace sécurisé du terminal de communication, lequel espace sécurisé comprend une zone de mémorisation inviolable pouvant être mise en œuvre pour exécuter des transactions, et notamment des transactions de paiement.

Plus particulièrement l'invention porte sur un procédé de traitement de données transactionnelles représentatives d'un paiement effectué par un utilisateur à partir d'un terminal de communication. Selon l'invention un tel procédé comprend :

- une étape de chargement d'un terminal de paiement virtuel , au sein d'un premier espace mémoire sécurisé du terminal de communication , ledit terminal virtuel se présentant sous la forme d'un module logiciel enregistré au sein d'un espace de stockage sécurisé du terminal de communication ;

- une étape de chargement , au sein d'un deuxième espace sécurisé , d'au moins une carte de paiement virtuelle ;
- une étape de traitement par le terminal de paiement virtuel d'une transaction de paiement à l'aide de ladite au moins une carte de paiement virtuelle.

Selon une caractéristique particulière, l'étape de chargement d'une carte de paiement virtuelle comprend :

- une étape de de chargement d'un module logiciel d'émulation de carte de paiement virtuelle ;
- une étape d'obtention d'une structure de données de carte de paiement
- une étape d'instanciation, au sein du deuxième espace sécurisé, de la carte de paiement virtuelle à l'aide du module logiciel d'émulation et de la structure de données de carte de paiement.

Ainsi, l'invention permet de réaliser des transactions de manière sécurisée, en maintenant les principes de non répudiation propres aux transactions réalisées en mode « card present » et en évitant la nécessité de disposer d'un terminal physique et d'une carte physique.

Selon une caractéristique particulière, l'étape de chargement d'une carte de paiement virtuelle comprend :

- une étape d'affichage sur un écran du terminal de communication, d'un ensemble de cartes de paiement virtuelles associées à l'utilisateur ;
- une étape de sélection, d'une carte de paiement virtuelle parmi l'ensemble de cartes de paiement affichée.

Ainsi, l'utilisateur peut disposer de plusieurs cartes de paiement virtuelles et effectuer une transaction de paiement avec la carte qui lui convient.

Selon un mode de réalisation particulier, ledit procédé comprend, postérieurement à l'étape de chargement du terminal de paiement virtuel, une étape d'affichage sur un écran du terminal de communication, d'une donnée représentative d'un passage en mode sécurisé.

Selon un mode de réalisation particulier, l'étape de chargement d'une carte de paiement virtuelle comprend :

- une étape d'identification par ledit terminal de paiement virtuel , du deuxième espace sécurisé au sein duquel la carte de paiement virtuelle doit être chargée ; et

- lorsque le deuxième espace sécurisé est situé sur un serveur connecté au terminal de communication par l'intermédiaire d'un réseau de communication, une étape de chargement, au sein du premier espace mémoire sécurisé, d'un module d'encapsulation.

Ainsi, la technique proposée permet de garantir la mise en œuvre d'un paiement quand bien même la carte virtuelle ne serait pas enregistrée sur le terminal de communication lui-même, mais sur un serveur distant.

Selon un mode de réalisation particulier, le procédé comprend, lorsque le deuxième espace sécurisé est situé sur un serveur connecté au terminal de communication, et ce pour au moins certaines des données échangées entre ledit terminal de paiement virtuel et ladite carte de paiement virtuelle, au moins une étape de transmission d'une commande audit serveur comprenant :

- une étape de création d'un entête de trame comprenant au moins un identifiant du terminal de paiement virtuel et un identifiant de la carte de paiement virtuelle ;
- une étape de remplissage d'une trame ledit entête, ladite commande, suivant un protocole d'échange de données déterminé,
- une étape de transmission de la trame à destination dudit serveur.

L'invention se rapporte également à un dispositif de traitement de données transactionnelles représentatives d'un paiement effectué par un utilisateur à partir d'un terminal de communication. Selon l'invention un tel dispositif comprend :

- des moyens de chargement d'un terminal de paiement virtuel , au sein d'un premier espace mémoire sécurisé du terminal de communication , ledit terminal virtuel se présentant sous la forme d'un module logiciel enregistré au sein d'un espace de stockage sécurisé du terminal de communication ;
- des moyens de chargement, au sein d'un deuxième espace sécurisé, d'au moins une carte de paiement virtuelle ;
- des moyens de traitement par le terminal de paiement virtuel d'une transaction de paiement à l'aide de ladite au moins une carte de paiement virtuelle.

L'invention se rapporte bien entendu à un terminal de communication qui intègre un dispositif de traitement de données transactionnelles tel que décrit précédemment.

Selon une implémentation préférée, les différentes étapes des procédés selon l'invention sont mises en œuvre par un ou plusieurs logiciels ou programmes d'ordinateur, comprenant des

instructions logicielles destinées à être exécutées par un processeur de données d'un module relais selon l'invention et étant conçu pour commander l'exécution des différentes étapes des procédés.

En conséquence, l'invention vise aussi un programme, susceptible d'être exécuté par un ordinateur ou par un processeur de données, ce programme comportant des instructions pour commander l'exécution des étapes d'un procédé tel que mentionné ci-dessus.

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

L'invention vise aussi un support d'informations lisible par un processeur de données, et comportant des instructions d'un programme tel que mentionné ci-dessus.

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

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

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

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

Un composant logiciel correspond à un ou plusieurs programmes d'ordinateur, un ou plusieurs sous-programmes d'un programme, ou de manière plus générale à tout élément d'un programme ou d'un logiciel apte à mettre en œuvre une fonction ou un ensemble de fonctions, selon ce qui est décrit ci-dessous pour le module concerné. Un tel composant logiciel est exécuté par un processeur de données d'une entité physique (terminal, serveur, passerelle, routeur, etc.) et est susceptible d'accéder aux ressources matérielles de cette entité physique (mémoires,

supports d'enregistrement, bus de communication, cartes électroniques d'entrées/sorties, interfaces utilisateur, etc.).

De la même manière, un composant matériel correspond à tout élément d'un ensemble matériel (ou hardware) apte à mettre en œuvre une fonction ou un ensemble de fonctions, selon ce qui est décrit ci-dessous pour le module concerné. Il peut s'agir d'un composant matériel programmable ou avec processeur intégré pour l'exécution de logiciel, par exemple un circuit intégré, une carte à puce, une carte à mémoire, une carte électronique pour l'exécution d'un micrologiciel (firmware), etc.

Chaque composante du système précédemment décrit met bien entendu en œuvre ses propres modules logiciels.

Les différents modes de réalisation mentionnés ci-dessus sont combinables entre eux pour la mise en œuvre de l'invention.

4. Dessins

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation préférentiel, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- la figure 1 présente un synoptique de la technique proposée ;
- la figure 2 présente un synoptique de la technique proposée, ... ;
- la figure 3 décrit un dispositif de mise en œuvre de la technique proposée ;
- la figure 4 décrit un serveur comprenant une pluralité de cartes de paiement virtuelles.

5. Description

5.1. Rappel du principe général

Comme explicité préalablement, le principe général de la technique proposée consiste à introduire, au sein du terminal de communication de l'utilisateur, un terminal de paiement virtuel (vPos). Un tel terminal de paiement virtuel se différentie d'un terminal de paiement physique en ce qu'il met en œuvre le processeur du terminal de communication qui lui est affecté. Par ailleurs, le terminal de paiement virtuel dispose d'un accès à une zone de mémoire sécurisée au sein de laquelle il est en mesure de réaliser des opérations cryptographiques. Un tel terminal de paiement comprend une interface de réception de commandes en provenance du terminal de communication, pour effectuer des transactions. De ce point de vue, le terminal de communication se comporte comme une sorte de caisse enregistreuse qui est apte à transmettre, au terminal de paiement virtuel, des commandes pour le paiement (par exemple un montant de transaction).

Lorsqu'il reçoit une commande d'activation et un montant de transaction, le terminal de paiement virtuel (vPos) est apte à mettre en œuvre une transaction de paiement, selon au moins deux modes de réalisation décrit ultérieurement.

On présente, en relation avec la figure 1 et la figure 2, les étapes générales du procédé de la présente technique. Un tel procédé de traitement de données transactionnelles représentatives d'un paiement effectué par un utilisateur à partir d'un terminal de communication (TC) comprend :

- une étape de chargement (10) d'un terminal de paiement virtuel (vPos), au sein d'un premier espace mémoire sécurisé (SecSpace1) du terminal de communication (TC), ledit terminal virtuel (vPos) se présentant sous la forme d'un module logiciel enregistré au sein d'un espace de stockage sécurisé (ESS) du terminal de communication (TC) ;
- une étape de chargement (20), au sein d'un deuxième espace sécurisé (SecSpace2), d'au moins une carte de paiement virtuelle (vCB) ;
- une étape de traitement (30) par le terminal de paiement virtuel (vPos) d'une transaction de paiement (TrP) à l'aide de ladite au moins une carte de paiement virtuelle (vCB).

L'étape que l'étape de chargement (20) d'une carte de paiement virtuelle (vCB) comprend :

- une étape de de chargement (25) d'un module logiciel d'émulation (modEmul) de carte de paiement virtuelle ;
- une étape d'obtention (26) d'une structure de données de carte de paiement (StructCB)
- une étape d'instanciation (27), au sein du deuxième espace sécurisé (SecSpace2), de la carte de paiement virtuelle (vCB) à l'aide du module logiciel d'émulation (modEmul) et de la structure de données de carte de paiement (StructCB).

En d'autres termes, selon la technique proposée, le terminal de paiement virtuel est mis en œuvre de la façon suivante :

- l'utilisateur utilise son terminal de communication pour effectuer un achat auprès d'un service en ligne (un site web). Il sélectionne un ou plusieurs articles et débute les opérations de paiement (généralement par l'utilisation d'un bouton de type "effectuer paiement" dans une page Web ou dans une application dédiée (par exemple l'application Amazon(tm), alibaba, ebay, etc.).
- le service ou l'application détecte que le terminal dispose d'un terminal de paiement virtuel. Au lieu de requérir la saisie de données relatives à une carte de paiement (numéros de carte, nom du titulaire, date de validité), le service ou l'application déclenche la mise en œuvre du terminal virtuel selon la technique proposée.

- le terminal virtuel est chargé en mémoire (de préférence en mémoire sécurisée SecSpace1 afin que son fonctionnement soit garanti). Alternativement il est sorti de veille (cas ou le terminal de paiement virtuel est chargé au démarrage du terminal de communication ou cas où le terminal de paiement a déjà été chargé préalablement).
- de manière optionnelle, un message d'avertissement est adressé (15) à l'utilisateur, l'informant qu'une opération sensible est sur le point d'être réalisée;
- le terminal virtuel requiert la saisie d'un code d'identification personnel de la part de l'utilisateur; ce code d'identification personnel correspond par exemple au code secret d'une carte de paiement (aussi appelé code PIN). Alternativement, ce code d'identification personnel peut également correspondre à un schéma devant être tracé par l'utilisateur ou encore à une signature d'une empreinte digitale devant être produite (si le terminal de communication comprend un lecteur d'empreinte digitales) ou encore à une saisie de zone de ;
- Pour la suite on suppose que le code saisi par l'utilisateur est correct. En cas de mauvais code, un nombre maximal d'essais est autorisé. Lorsque ce nombre d'essais est atteint ou dépassé (par exemple trois), le terminal de paiement virtuel se met hors fonction : cette mise hors fonction provoque l'effacement de la mémoire sécurisée ainsi que la suppression du terminal de paiement virtuel et/ou la suppression de données sensibles du terminal virtuel. Le terminal de communication ne peut alors plus opérer de terminal de paiement virtuel jusqu'à ce que ce terminal de paiement virtuel soit à nouveau installé sur le terminal de communication.
- La carte de paiement virtuelle est par la suite chargée dans un deuxième espace sécurisé. Il peut s'agir d'un espace local, présent sur le terminal de communication (SecSpace2, figure 1) ou d'un espace distant, présent sur un serveur auquel le terminal de communication est connecté (SecSpace2, figure 2) Dan ce deuxième cas, des étapes d'identification (21) et de chargement (22) d'une module de communication réseaux sont mise en œuvre afin d'échanger des trames de commande (APPDU) du protocole 7816 sur le réseau de communication (par exemple encapsulées dans des trames IP).
- de manière complémentaire, lorsque cela est envisageable, le terminal virtuel requiert une sélection, par l'utilisateur, d'un moyen de paiement à utiliser (c'est par exemple le cas lorsque plusieurs cartes de paiement peuvent être utilisées par l'utilisateur comme une carte de paiement pour un premier établissement bancaire et une carte de paiement pour

un deuxième établissement bancaire). Par ailleurs, il peut être envisagé de requérir une nouvelle saisie d'un code d'identification personnel spécifiquement attaché au moyen de paiement sélectionné, afin de renforcé la sécurisation (ceci est explicité par la suite dans le cadre d'une mise en œuvre EMV). De manière optionnelle, donc, un message d'avertissement est affiché (23) à l'utilisateur, afin qu'il sélectionne (24) une carte de paiement parmi une pluralité de cartes de paiements disponibles;

- une vérification de la concordance du code d'identification personnel relativement au moyen de paiement sélectionné est réalisée par un mécanisme explicité par la suite.
- la terminal de paiement virtuel met alors en œuvre le paiement en construisant une transaction de paiement, par exemple selon l'ensemble de protocoles SEPA et/ou EMV.
- Deux cas de figure se présentent par la suite :
- la transaction est correctement menée et un récapitulatif de paiement est affiché à l'écran du terminal de communication et/ou enregistré au sein de celui-ci;
- la transaction échoue (par exemple suite à un refus de l'établissement bancaire), et un message d'échec de transaction est affiché à l'écran puis le terminal de paiement virtuel est fermé (ou passé en mémoire cache sécurisée si cela est possible)).

Ainsi, au lieu d'utiliser un terminal complémentaire qui doit être apparié au terminal de communication, on utilise une zone de mémoire sécurisée du terminal de communication pour y exécuter un terminal de paiement virtuel. Comme on peut le noter, deux phases peuvent être décrites de manière complémentaire : l'installation de ce terminal de paiement virtuel au sein du terminal de communication et l'utilisation d'un moyen de paiement pour effectuer une transaction de paiement. L'installation du terminal de paiement virtuel au sein du terminal de communication est liée à une présence, au sein de ce terminal, d'une zone mémoire sécurisée. Une telle zone mémoire sécurisée est remarquable en ce qu'elle n'est accessible qu'à partir d'une portion sécurisée du système d'exploitation du terminal de communication, seule habilité à accéder à cette zone. L'installation de ce terminal de paiement virtuel passe donc par une utilisation de cette portion du système d'exploitation. Elle n'est pas détaillée plus avant, cette installation étant dépendante du système d'exploitation en tant que tel et des caractéristiques techniques de cette zone de mémoire sécurisée.

En revanche, la réalisation de la transaction à partir du moyen de paiement sélectionné fait pleinement partie de la présente technique. Une telle réalisation est effectuée d'au moins deux manières différentes :

- l'utilisation d'une carte de paiement virtuelle, accessible au sein du terminal de communication;
- l'utilisation d'une carte de paiement virtuelle, accessible par l'intermédiaire d'un réseau de communication sécurisé.

5.2. Utilisation d'une carte de paiement virtuelle, accessible au sein du terminal de communication

Dans ce mode de réalisation, en conjonction avec l'utilisation d'un terminal de communication comprenant un terminal de paiement virtuel, une ou plusieurs cartes bancaires virtuelles sont mises en œuvre. Le principe général est d'exécuter, au sien de la zone de mémorisation sécurisée ou à l'aide de celle-ci, une machine virtuelle reproduisant le comportement d'une carte de paiement. Cette machine virtuelle peut être perçue comme un émulateur, permettant de reproduire le comportement d'une carte bancaire à puce de type EMV. En outre, les données nécessaires à la réalisation de transactions sont également placées dans cette zone de mémoire sécurisée. Cette technique est présentée en relation avec la figure 2.

La machine virtuelle de la carte bancaire (MVC) est placée dans une zone mémoire sécurisée (ZMS) accessible en lecture seule afin de garantir l'absence de modification de celle-ci. Cette zone de mémoire sécurisée comprend (ZMS) en outre une (Expliciter architecture de la carte bancaire EMV). Principalement, l'organisation de cette zone de mémoire sécurisée consiste à reproduire une architecture d'une carte bancaire au standard EMV. La zone de mémoire sécurisée est donc organisée pour permettre un comportement identique ou similaire à une carte EMV réelle, qui serait par exemple insérée dans le terminal. La machine virtuelle émule donc la présence d'une carte bancaire de type EMV. Les données de personnalisation de cette carte virtuelle EMV (Certificats, Applications, Authentification du porteur, etc.) sont insérées à l'aide d'un protocole d'insertion spécifique.

Lorsqu'une carte virtuelle est instanciée au sein de la zone de mémoire sécurisée, la technique de mise en œuvre de cette carte virtuelle est la suivante : le terminal de paiement virtuel (vPos) transmet des commandes EMV à la carte de paiement virtuelle. Ces commandes respectent la norme 7816 et sont échangées selon le protocole APDU. La carte de paiement répond aux commandes transmises par le terminal de paiement virtuel selon le même principe. La transaction est menée entre le terminal de paiement virtuel et la carte de paiement virtuelle en utilisant l'enchainement suivant:

- Sélection de l'application EMV de la carte de paiement virtuelle (CB, VISA...)

- Initialisation de l'application
- Lecture des données de l'application
- Lecture des restrictions d'utilisation
- Authentification des données hors ligne
- Identification du porteur (saisie du code d'identification personnel)
- Gestion du risque du côté du terminal de paiement virtuel
- Analyse du risque par le terminal de paiement virtuel et action du terminal de paiement virtuel (Paiement accepté hors ligne, refusé hors ligne, Autorisation requise)
- Première analyse du risque du côté de la carte de paiement virtuelle
- Demande d'autorisation en ligne (le cas échéant)
- Deuxième analyse du risque du côté de la carte de paiement virtuelle
- Exécution du script final de l'émetteur de la carte de paiement virtuelle (établissement bancaire concerné) (mise à jour des paramètres carte, blocage...)

L'avantage de ce mode de réalisation est le suivant : contrairement aux solutions existantes, il n'est pas nécessaire de construire un dispositif de lecture de carte particulier (à connecter au terminal de communication de l'utilisateur) pour pouvoir effectuer des actions en mode Card Present à partir du terminal. Par ailleurs Il n'est pas nécessaire de modifier la mise en œuvre des protocoles existants. L'utilisateur peut ainsi utiliser son terminal de communication pour réaliser des achats. Au moins deux type de sous système de sécurisation interne au terminal de communication sont utilisés :

- TPM (de l'anglais pour "trusted platform module") pour les terminaux de communication de type ordinateur personnel. Des composants TPM peuvent être présents sur de tels terminaux. Lorsqu'une terminal possède un composant de ce type, la technique proposée est mise en œuvre par l'intermédiaire de ce composant;
- un composant de sécurisation dédié : un tel composant peut être inséré directement au sein du terminal de communication afin d'offrir un support physique pour la mise en œuvre de la technique proposée;

Dans un mode de réalisation complémentaire, une carte SIM insérée au sein du terminal de communication est utilisée en lieu et place de la zone de mémoire sécurisée afin de contenir les données de la carte bancaire virtuelle. Plus particulièrement, dans une première variante, la carte SIM du terminal de communication (par exemple un smartphone ou une tablette) est utilisée pour enregistrées les données de la carte bancaire virtuelle. Dans ce cas, la zone de mémoire sécurisé

est celle de la carte SIM. Dans cette première variante, l'émulateur de carte bancaire virtuel reste exécuté sur le terminal de communication. Ainsi, un procédé d'obtention des données enregistrées sur la carte SIM est mis en œuvre, en passant par l'interface d'échange de données de la carte SIM (Il s'agit également d'échanger des APDU). En revanche, l'échange de ces données ne vise qu'à obtenir les données nécessaires à la simulation de la carte bancaire par le terminal de communication : il s'agit donc d'un coffre-fort numérique déporté sur la carte SIM. Ainsi, l'émulateur de carte bancaire virtuel comprend un module d'accès aux données de la carte SIM, ce module étant apte à échanger des données avec cette carte SIM par l'intermédiaire des protocoles 7816-x.

Dans une deuxième variante, la carte SIM intègre directement une fonction bancaire et est donc apte à agir comme une carte bancaire lorsqu'elle est sollicitée en ce sens par le terminal de paiement virtuel. Plus particulièrement cette carte SIM fonctionne, lorsqu'elle est accédée en mode "bancaire" comme une carte bancaire classique. Cependant, à la différence de cartes SIM multi-tenants, celle-ci n'est pas destinée à offrir un paiement avec n'importe quel type de terminal de paiement. Le mode "bancaire" de cette carte n'est accessible que par l'intermédiaire du terminal de paiement virtuel installé au sein du terminal de communication. Dès lors, pour accéder au mode "bancaire" de cette carte SIM, une méthode d'accès spécifique est mise en œuvre (non détaillée). Cette méthode requiert l'authentification du terminal de paiement virtuel, lequel doit transmettre, par l'intermédiaire d'un APDU spécifique, une preuve de son authentification à la carte SIM fonctionnant en mode "bancaire". Plus particulièrement, cette preuve d'authentification peut par exemple consister en une donnée d'authentification de terminal virtuel obtenue postérieurement à une phase d'authentification réalisée avec un serveur d'authentification auquel le terminal de communication de l'utilisateur aura été connecté au moment de (ou postérieurement à) l'installation du terminal de paiement virtuel. Par ailleurs, l'obtention d'une telle donnée d'authentification peut être commune à l'ensemble des modes de réalisation de la présente technique.

Le procédé mis en œuvre est le suivant :

- le terminal de paiement virtuel transmet à la carte SIM une instruction de bascule en mode bancaire; pour ce faire, le terminal de paiement virtuel transmet sa donnée d'authentification (il s'agit par exemple d'une commande APDU de type BC,C0 avec la donnée d'authentification en paramètre);

- en fonction de l'application codée dans la carte SIM, un tel APDU provoque une mise en œuvre d'une fonction de vérification dans la carte SIM et la transmission d'une réponse normée (champs SW1 et champs SW2).

5.3. Utilisation d'une carte de paiement virtuelle, accessible par l'intermédiaire d'un réseau de communication sécurisé

Comme explicité préalablement, les protocoles 7816 définissent les APDU qui sont transmises une carte connectée à un lecteur de carte en mode contact. Dans ce mode de réalisation, on ne déroge pas à cette mise en œuvre des protocoles 7816, ce qui en fait justement une caractéristique intéressante. Dans le cadre d'un terminal de paiement virtuel et connecté à une ferme de cartes bancaires, le terminal de paiement virtuel doit interroger une carte lors de la réalisation d'une transaction. Dans ce mode de réalisation, on propose donc une utilisation d'une carte bancaire virtuelle, dont les données sont stockées sur un serveur. Par ailleurs, dans ce mode de réalisation, le serveur peut avantageusement stocker et protéger une pluralité de cartes de paiement virtuelles appartenant à une pluralité de titulaires. On dispose ainsi, sur ce serveur, d'une "ferme" de cartes de paiement. Cette ferme permet de centraliser les cartes de paiement virtuelles.

Ainsi, dans ce mode de réalisation, les APDU sont transmis par l'intermédiaire du réseau de communication auquel le terminal de communication et le serveur sont connectés. On suppose, comme un prérequis, que le terminal de communication et le serveur ont établi une communication sécurisée entre eux et que les échanges ne peuvent pas être interceptés.

Dès lors le terminal de paiement virtuel comprend un module de transmission et de réception de commandes APDU qui fonctionne en conjonction avec un module d'encapsulation (également sécurisé et fonctionnant en zone de mémoire sécurisé) en charge de l'encapsulation et de la désencapsulation des commandes APDU. Ce module d'encapsulation permet de générer des trames (par exemple des trames IP) comprenant un ou plusieurs champs de données (dont la taille est variable en fonction de la MTU). Le serveur qui gère la ferme de carte de paiement virtuel comprend également un module d'encapsulation similaire destiné à effectuer des opérations similaires depuis le serveur

Typiquement, un champ de données d'une trame IP encapsulant des commandes APDU comprend trois parties:

- La première partie, dite entête, comprend les champs suivants :

- Identifiant Serveur de cartes: l'identifiant du serveur à l'origine de la demande de transaction ;
- Identifiant vPos : identification du terminal virtuel. Cet identifiant doit permettre de remonter jusqu'à la version logicielle, l'opérateur du vPos, etc. ;
- Numéro de trame vPos : numéro de la trame envoyée par vPos, permettant à la ferme de traiter les trames dans l'ordre. Ce numéro est incrémenté uniquement par le vPos, et uniquement recopié dans les trames venant de la ferme ;
- Identification carte : token permettant d'identifier la carte dans la ferme ;
- Numéro de trame ferme : numéro de la trame échangée depuis la ferme, permettant au vPos de traiter les trames dans l'ordre ; A l'inverse, ce numéro est incrémenté par la ferme, et recopié par le vPos dans les trames retour ;
- Champs propriétaire : champs constitué d'une longueur et d'un nombre d'octet à usage particulier ;
- Longueur : longueur totale de la trame complète ;

- La deuxième partie comprend une trame iso7816 sans modification, que ce soit APDU ou TPDU.
- La troisième partie comprend une fin de trame qui est constituée d'un caractère de fin de trame spécifique.

Les avantages de ce mode de réalisation sont multiples. En premier lieu, il n'est pas nécessaire de disposer d'une espace de stockage sécurisé sur le terminal de communication. Ceci est avantageux car évite qu'une compromission du terminal de communication entraine un vol des données bancaires de la carte virtuelle stockée sur le terminal de communication. En second lieu, ce mode de réalisation permet de sécuriser fortement l'accès au serveur qui centraliser les cartes de paiement virtuelles. Par ailleurs, ceci évite de devoir faire fonctionner une machine virtuelle simulant le fonctionnement de la carte de paiement virtuelle sur le terminal de communication. Dès lors cette simulation de fonctionnement de carte virtuelle est effectuée sur le serveur qui est un lieu de traitement plus sûr.

5.4. Autres caractéristiques et avantages

On décrit, en relation avec la figure 3, un dispositif mis en œuvre pour réaliser des opérations de paiement à partir d'un terminal de communication tout en opérant en mode « card present », selon le procédé décrit préalablement.

Par exemple, le dispositif comprend une mémoire 31 constituée d'une mémoire tampon, une unité de traitement 32, équipée par exemple d'un microprocesseur, et pilotée par le programme d'ordinateur 33, mettant en œuvre un procédé de traitement de données transactionnelles.

À l'initialisation, les instructions de code du programme d'ordinateur 33 sont par exemple chargées dans une mémoire avant d'être exécutées par le processeur de l'unité de traitement 32. L'unité de traitement 32 reçoit en entrée au moins une donnée représentative d'un identifiant d'un terminal de communication. Le microprocesseur de l'unité de traitement 32 met en œuvre les étapes du procédé de traitement, selon les instructions du programme d'ordinateur 33 pour effectuer un chargement, en zone mémoire sécurisée, d'un terminal de paiement virtuel (zone mémoire utiliser pour exécuter le terminal de paiement virtuel sur le terminal de communication : il s'agit par exemple d'un TMP pour un ordinateur personnel ou d'un « Embedded secure element » au sein d'un téléphone).

Pour cela, le dispositif comprend, outre la mémoire tampon 31, des moyens de communications, tels que des modules de communication réseau, des moyens de transmission de donnée et éventuellement un processeur de chiffrement.

Ces moyens peuvent se présenter sous la forme d'un processeur particulier implémenté au sein du dispositif, ledit processeur étant un processeur sécurisé. Selon un mode de réalisation particulier, ce dispositif met en œuvre une application particulière qui est en charge de la réalisation des transactions, cette application étant par exemple fournie par le fabricant du processeur en question afin de permettre l'utilisation dudit processeur. Pour ce faire, le processeur comprend des moyens d'identification uniques. Ces moyens d'identification uniques permettent d'assurer l'authenticité du processeur.

Par ailleurs, le dispositif comprend les moyens de chargement d'un terminal de paiement virtuel (vPos), au sein d'un premier espace mémoire sécurisé (SecSpace1) du terminal de communication (TC), ledit terminal virtuel (vPos) se présentant sous la forme d'un module logiciel enregistré au sein d'un espace de stockage sécurisé du terminal de communication (TC) ; les moyens de chargement, au sein d'un deuxième espace sécurisé (SecSpace2), d'au moins une carte de paiement virtuelle (vCB), lorsque les cartes virtuelles sont également gérées par le dispositif ; des moyens de traitement par le terminal de paiement virtuel (vPos) d'une transaction de paiement à l'aide de ladite au moins une carte de paiement virtuelle (vCB). Ces moyens se présentent également comme des interfaces de communications permettant d'échanger des

données sur des réseaux de communication, des moyens d'interrogations et de mise à jour de base de données, ...

On décrit, en relation avec la figure 4, un serveur mis en œuvre pour réaliser des opérations de paiement à partir d'un terminal de communication tout en opérant en mode « card present », selon le procédé décrit préalablement.

Par exemple, le serveur comprend une mémoire 41 constituée d'une mémoire tampon, une unité de traitement 42, équipée par exemple d'un microprocesseur, et pilotée par le programme d'ordinateur 43, mettant en œuvre un procédé de traitement de données transactionnelles.

À l'initialisation, les instructions de code du programme d'ordinateur 43 sont par exemple chargées dans une mémoire avant d'être exécutées par le processeur de l'unité de traitement 42. L'unité de traitement 42 reçoit en entrée au moins une donnée représentative d'un identifiant d'un terminal de paiement virtuel et d'une carte de paiement virtuelle à utiliser. Le microprocesseur de l'unité de traitement 42 met en œuvre des étapes du procédé de traitement, selon les instructions du programme d'ordinateur 43 pour effectuer un chargement, d'un module logiciel d'émulation (modEmul) de carte de paiement virtuelle ; obtenir une structure de données de carte de paiement (StructCB) en fonction de l'identifiant de carte qui lui est fourni ; instancier au sein du deuxième espace sécurisé (SecSpace2), la carte de paiement virtuelle (vCB) et effectuer l'encapsulation et la des encapsulation des APDU et des RPDU destinés à cette carte de paiement virtuelle afin de mettre en œuvre la transaction (au moyen d'un module d'encapsulation).

Pour cela, le serveur comprend, outre la mémoire tampon 41, des moyens de communications, tels que des modules de communication réseau, des moyens de transmission de donnée et éventuellement un processeur de chiffrement.

Ces moyens peuvent se présenter sous la forme d'un processeur particulier implémenté au sein du serveur, ledit processeur étant un processeur sécurisé. Selon un mode de réalisation particulier, ce serveur met en œuvre une application particulière qui est en charge de la réalisation des transactions, cette application étant par exemple fournie par le fabricant du processeur en question afin de permettre l'utilisation dudit processeur. Pour ce faire, le processeur comprend des moyens d'identification uniques. Ces moyens d'identification uniques permettent d'assurer l'authenticité du processeur.

Revendications

1. Procédé de traitement de données transactionnelles représentatives d'un paiement effectué par un utilisateur à partir d'un terminal de communication (TC), procédé caractérisé en ce qu'il comprend :

- une étape de chargement (10) d'un terminal de paiement virtuel (vPos), au sein d'un premier espace mémoire sécurisé (SecSpace1) du terminal de communication (TC), ledit terminal virtuel (vPos) se présentant sous la forme d'un module logiciel enregistré au sein d'un espace de stockage sécurisé du terminal de communication (TC) ;
- une étape de chargement (20), au sein d'un deuxième espace sécurisé (SecSpace2), d'au moins une carte de paiement virtuelle (vCB) ;
- une étape de traitement (30) par le terminal de paiement virtuel (vPos) d'une transaction de paiement à l'aide de ladite au moins une carte de paiement virtuelle (vCB).

2. Procédé de traitement de données transactionnelles selon la revendication 1, caractérisé en ce que l'étape de chargement (20) d'une carte de paiement virtuelle (vCB) comprend :

- une étape de de chargement (25) d'un module logiciel d'émulation (modEmul) de carte de paiement virtuelle ;
- une étape d'obtention (26) d'une structure de données de carte de paiement (StructCB)
- une étape d'instanciation (27), au sein du deuxième espace sécurisé (SecSpace2), de la carte de paiement virtuelle (vCB) à l'aide du module logiciel d'émulation (modEmul) et de la structure de données de carte de paiement (StructCB).

3. Procédé de traitement de données transactionnelles selon la revendication 1, caractérisé en ce que l'étape de chargement (20) d'une carte de paiement virtuelle (vCB) comprend :

- une étape d'affichage (23) sur un écran du terminal de communication, d'un ensemble de cartes de paiement virtuelles associées à l'utilisateur ;
- une étape de sélection (24), d'une carte de paiement virtuelle parmi l'ensemble de cartes de paiement affichée.

4. Procédé selon la revendication 1, caractérisé en ce qu'il comprend, postérieurement à l'étape de chargement (10) du terminal de paiement virtuel (vPos), une étape d'affichage (15) sur un écran du terminal de communication, d'une donnée représentative d'un passage en mode sécurisé.

5. Procédé de traitement de données transactionnelles selon la revendication 1, caractérisé en ce que l'étape de chargement (20) d'une carte de paiement virtuelle (vCB) comprend :

- une étape d'identification (21) par ledit terminal de paiement virtuel (vPos), du deuxième espace sécurisé (SecSpace2) au sein duquel la carte de paiement virtuelle (vCB) doit être chargée ; et
- lorsque le deuxième espace sécurisé (SecSpace2) est situé sur un serveur (SrvVCB) connecté au terminal de communication (TC) par l'intermédiaire d'un réseau de communication (Ntwk), une étape de chargement (22), au sein du premier espace mémoire sécurisé (SecSpace1), d'un module d'encapsulation (ModEncaps).

6. Procédé de traitement de données transactionnelles selon la revendication 5, caractérisé en ce qu'il comprend, lorsque le deuxième espace sécurisé (SecSpace2) est situé sur un serveur (SrvVCB) connecté au terminal de communication (TC), et ce pour au moins certaines des données échangées entre ledit terminal de paiement virtuel (vPos) et ladite carte de paiement virtuelle (vCB), au moins une étape de transmission d'une commande (APDU) audit serveur (SrvVCB) comprenant :

- une étape de création d'un entête de trame comprenant au moins un identifiant du terminal de paiement virtuel (vPos) et un identifiant de la carte de paiement virtuelle (vCB) ;
- une étape de remplissage d'une trame ledit entête, ladite commande, suivant un protocole d'échange de données déterminé,
- une étape de transmission de la trame à destination dudit serveur.

7. Dispositif de traitement de données transactionnelles représentatives d'un paiement effectué par un utilisateur à partir d'un terminal de communication (TC), dispositif caractérisé en ce qu'il comprend :

- des moyens de chargement d'un terminal de paiement virtuel (vPos), au sein d'un premier espace mémoire sécurisé (SecSpace1) du terminal de communication (TC), ledit terminal virtuel (vPos) se présentant sous la forme d'un module logiciel enregistré au sein d'un espace de stockage sécurisé du terminal de communication (TC) ;
- des moyens de chargement, au sein d'un deuxième espace sécurisé (SecSpace2), d'au moins une carte de paiement virtuelle (vCB) ;
- des moyens de traitement par le terminal de paiement virtuel (vPos) d'une transaction de paiement à l'aide de ladite au moins une carte de paiement virtuelle (vCB).

8. Terminal de communication caractérisé en ce qu'il intègre un dispositif de traitement de données transactionnelles selon la revendication 7.

9. Produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution d'un procédé de traitement de données transactionnelles selon la revendication 1, lorsqu'il est exécuté sur un ordinateur.

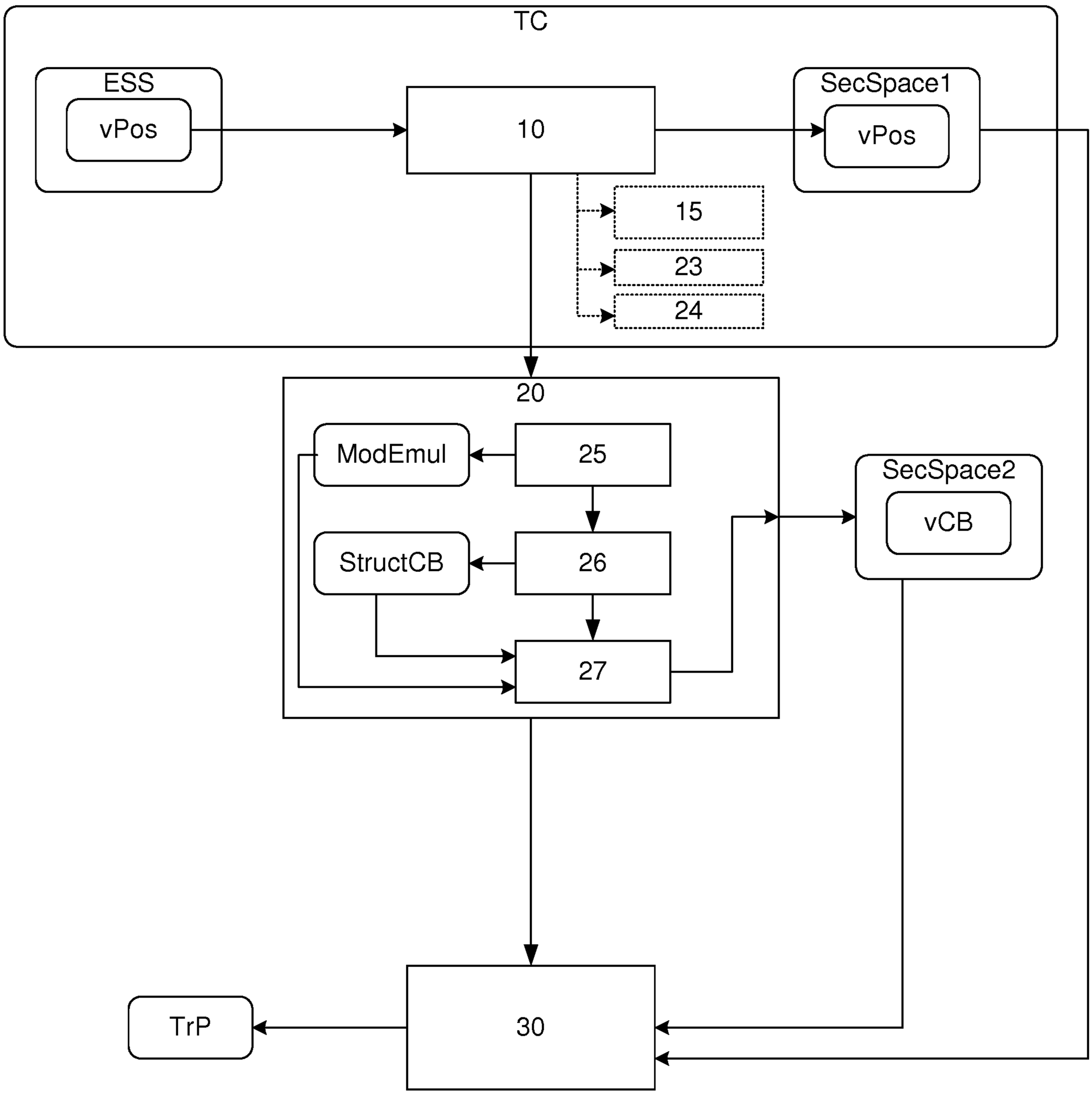
TC
ESS
vPos
10
SecSpace1
vPos
15
23
24
20
ModEmul
25
StructCB
26
27
SecSpace2
vCB
TrP
30

Figure 1

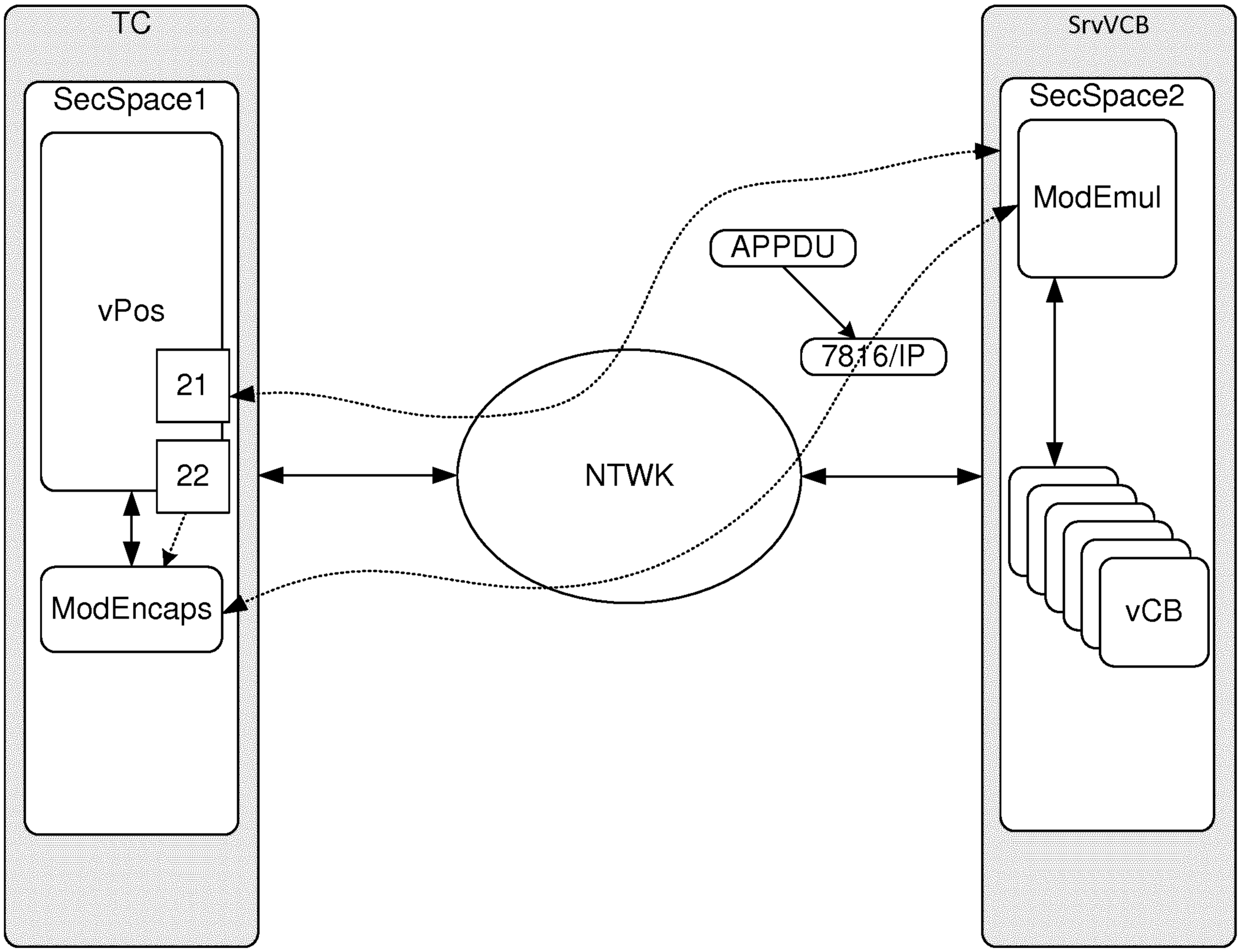
TC
SecSpace1
vPos
21
22
ModEncaps
NTWK
APPDU
7816/IP
SrvVCB
SecSpace2
ModEmul
vCB

Figure 2

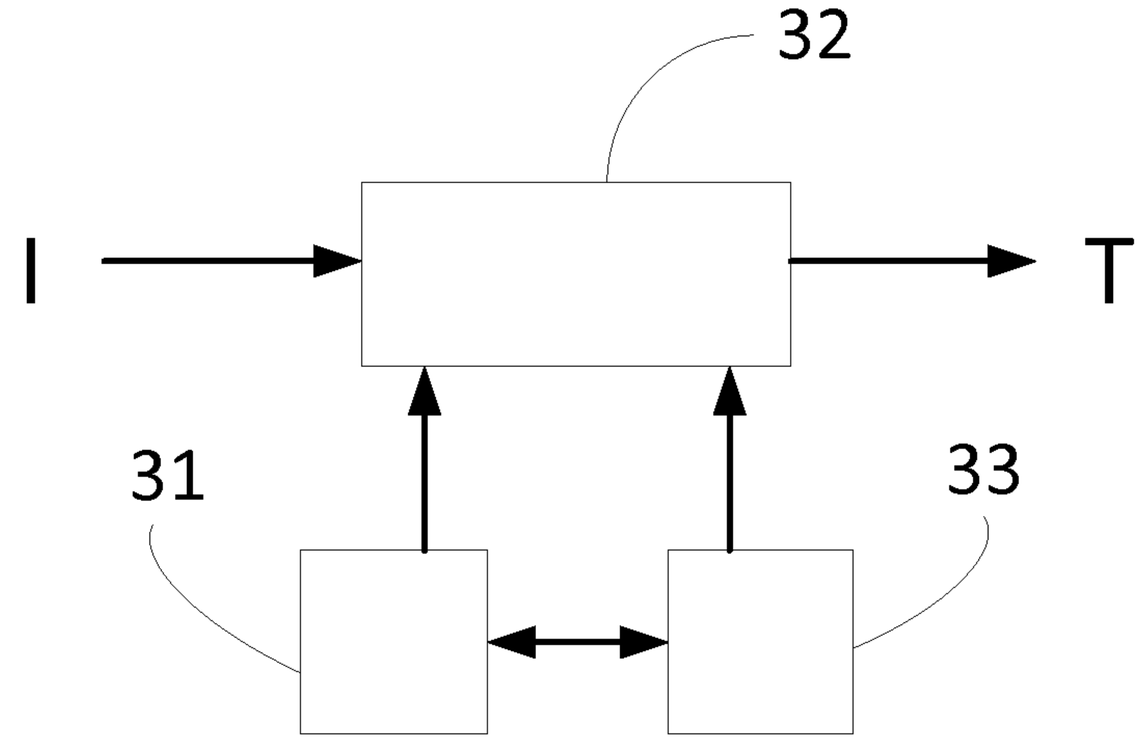

Figure 3

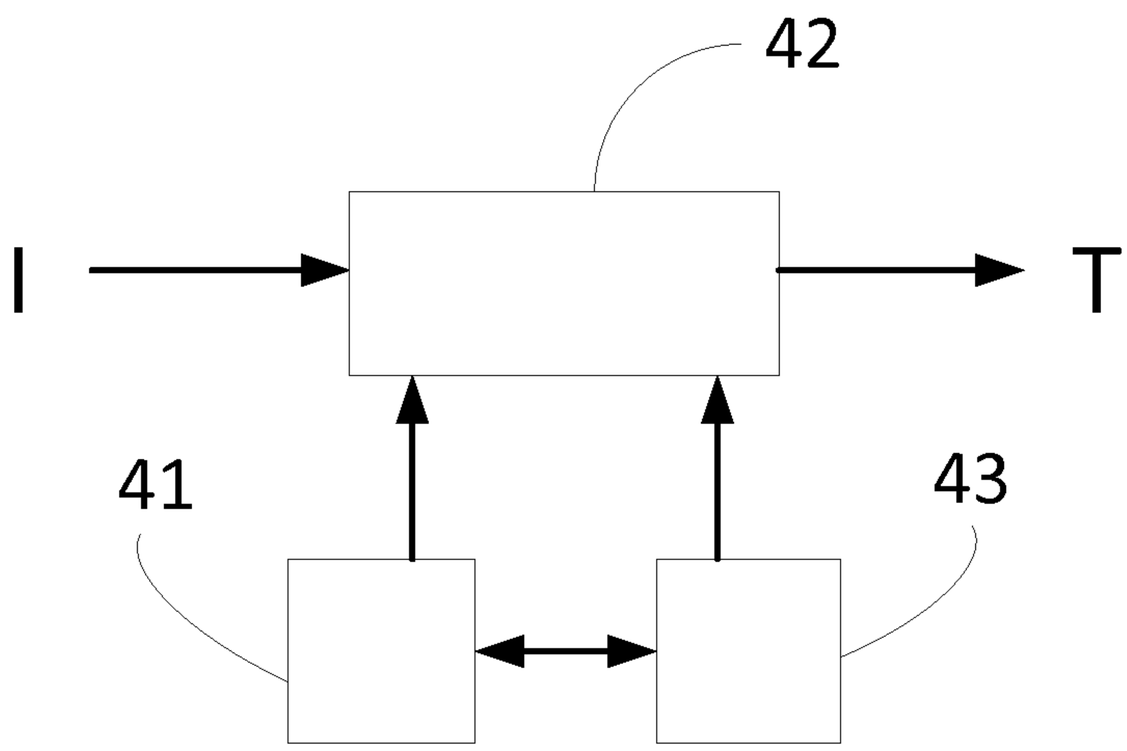

Figure 4

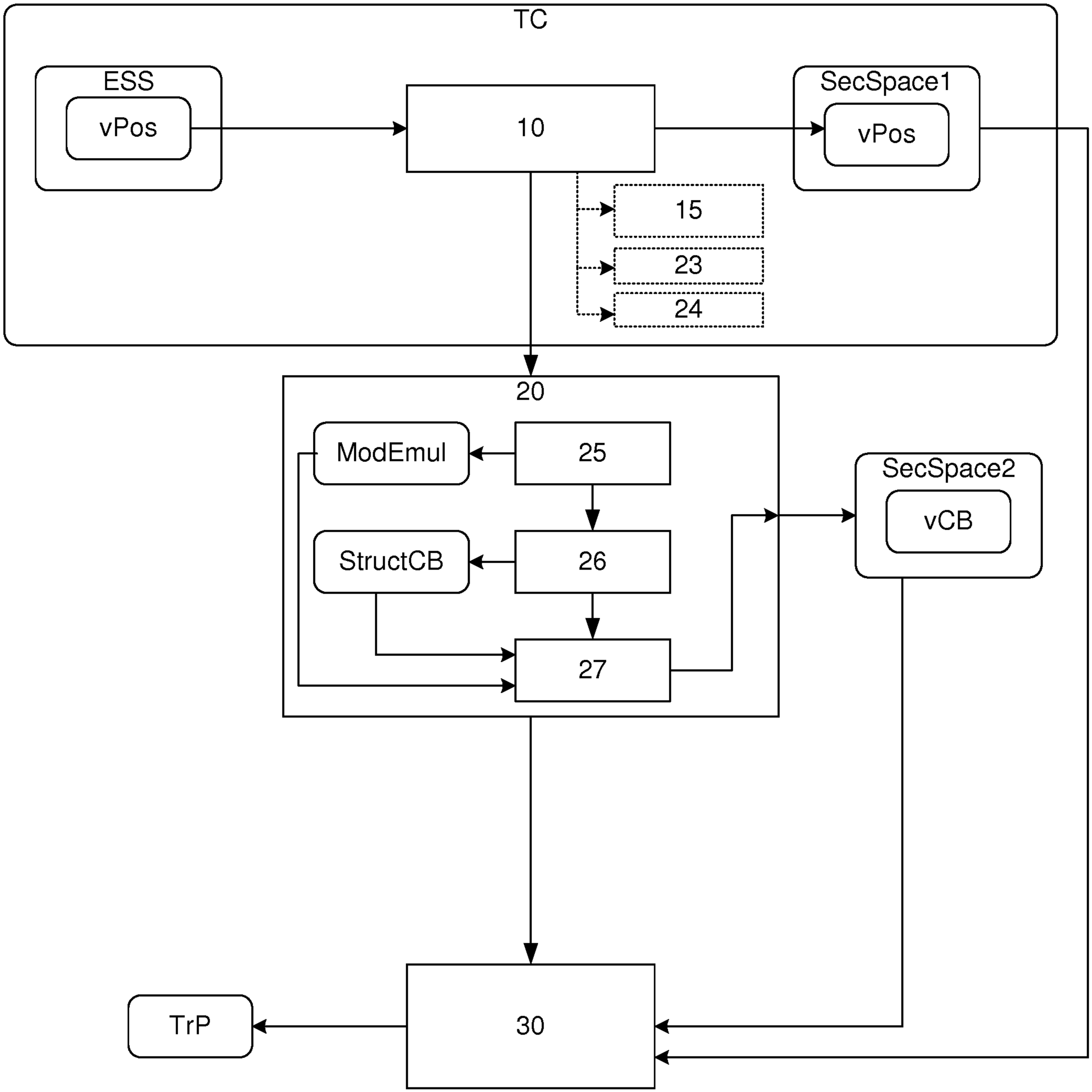
TC
ESS
vPos
10
SecSpace1
vPos
15
23
24
20
ModEmul
25
StructCB
26
27
SecSpace2
vCB
TrP
30

Figure 1