Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 2946145 C 2023/02/28

(11)(21) **2 946 145**

(12) **BREVET CANADIEN**
CANADIAN PATENT

(13) **C**

(86) **Date de dépôt PCT/PCT Filing Date:** 2015/04/10
(87) **Date publication PCT/PCT Publication Date:** 2015/10/22
(45) **Date de délivrance/Issue Date:** 2023/02/28
(85) **Entrée phase nationale/National Entry:** 2016/10/14
(86) **N° demande PCT/PCT Application No.:** EP 2015/057837
(87) **N° publication PCT/PCT Publication No.:** 2015/158619
(30) **Priorité/Priority:** 2014/04/18 (FR1453569)

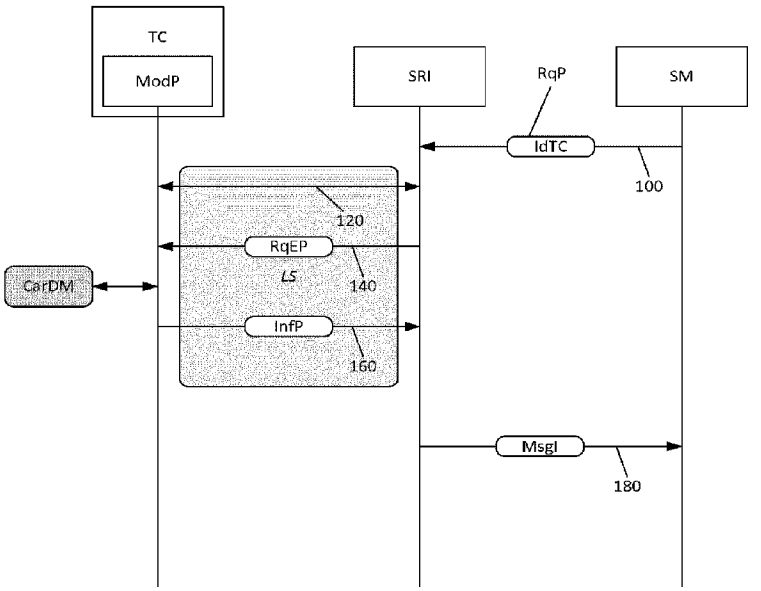
(51) **Cl.Int./Int.Cl.** ***G06Q 20/08*** (2012.01), ***G06Q 20/32*** (2012.01), ***G06Q 20/34*** (2012.01), ***G06Q 20/38*** (2012.01)

(72) **Inventeur/Inventor:**
SARRADIN, JEAN-LOUIS, FR

(73) **Propriétaire/Owner:**
BANKS AND ACQUIRERS INTERNATIONAL HOLDING, FR

(74) **Agent:** BCF LLP

(54) **Titre : PROCEDES DE TRAITEMENT DE DONNEES TRANSACTIONNELLES, DISPOSITIFS ET PROGRAMMES CORRESPONDANTS**
(54) **Title: METHODS FOR PROCESSING TRANSACTIONAL DATA, AND CORRESPONDING DEVICES AND PROGRAMS**



(57) **Abrégé/Abstract:**
L'invention se rapporte à un procédé de traitement de données transactionnelles, mis en oeuvre au sein d'un serveur intermédiaire sécurisé, connecté à un réseau de communication. Un tel procédé comprend : - une étape de réception (100), par le serveur intermédiaire sécurisé (SRI) d'une requête de paiement (RqP) comprenant une donnée représentative d' une identification (IdTC) d'un terminal de communication (TC) utilisé par un utilisateur pour effectuer une opération d'achat sur un serveur marchand (SM) connecté audit réseau de communication; - une étape d'établissement (120) d'une liaison sécurisée (LS) point à point avec un Module de paiement (ModP) du terminal de communication (TC); - une étape de transmission (140), audit Module de paiement (ModP), d'une requête d'exécution de paiement (RqEP); - une étape de réception (160) de la part du module de paiement (ModP), d'une information de paiement (InfP); - une étape de transmission (180), d'un message d'information (Msgl) au serveur marchand (SM).

(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 2015/158619 A1

(51) Classification internationale des brevets :
G06Q 20/02 (2012.01) *G06Q 20/34* (2012.01)
G06Q 20/32 (2012.01) *G06Q 20/40* (2012.01)

(21) Numéro de la demande internationale :
PCT/EP2015/057837

(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 :
1453569 18 avril 2014 (18.04.2014) FR

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

(72) Inventeur : **SARRADIN, Jean-Louis**; Bel-Air, F-07300 Etables (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** : METHODS FOR PROCESSING TRANSACTIONAL DATA, AND CORRESPONDING DEVICES AND PROGRAMS

(54) **Titre** : PROCÉDÉS DE TRAITEMENT DE DONNÉES TRANSACTIONNELLES, DISPOSITIFS ET PROGRAMMES CORRESPONDANTS

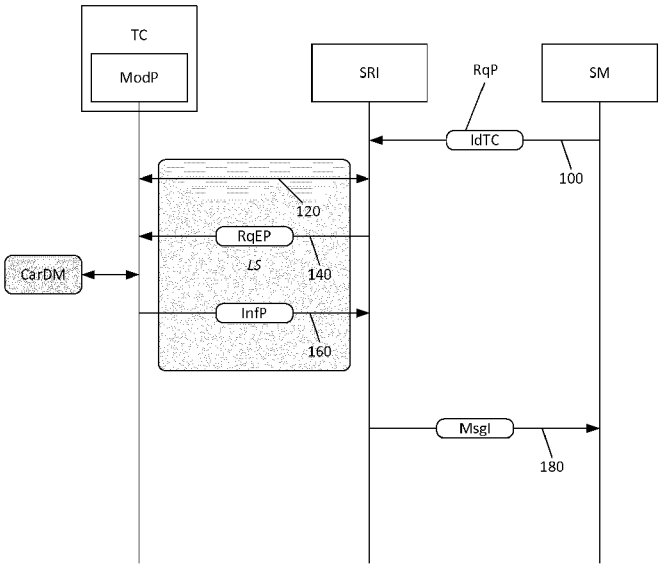


Figure 1

(57) Abstract : The invention relates to a method for processing transactional data, implemented on a secure intermediate server connected to a communication network. Such a method comprises: a step of receiving (100) a payment request (RqP), via the secure intermediate server (SRI), comprising data representing the identification (IdTC) of a communication terminal (TC) used by a user to perform a purchasing operation on a commercial server (SM) connected to said communication network; a step (120) of establishing a secure point-to-point connection (LS) to a payment module (ModP) of the communication terminal (TC); a step (140) of transmitting a payment execution request (RqEP) to said payment module (ModP); a step (160) of receiving payment information (InfP) from the payment module (ModP); and a step (180) of transmitting an information message (Msg1) to the commercial server (SM).

(57) Abrégé : L'invention se rapporte à un procédé de traitement de données transactionnelles, mis en œuvre au sein d'un serveur intermédiaire sécurisé, connecté à un réseau de communication. Un tel procédé comprend : - une étape de réception (100), par le serveur intermédiaire sécurisé (SRI) d'une requête de paiement (RqP) comprenant une donnée représentative

[Suite sur la page suivante]

WO 2015/158619 A1

WO 2015/158619 A1

d' une identification (IdTC) d'un terminal de communication (TC) utilisé par un utilisateur pour effectuer une opération d'achat sur un serveur marchand (SM) connecté audit réseau de communication; - une étape d'établissement (120) d'une liaison sécurisée (LS) point à point avec un Module de paiement (ModP) du terminal de communication (TC); - une étape de transmission (140), audit Module de paiement (ModP), d'une requête d'exécution de paiement (RqEP); - une étape de réception (160) de la part du module de paiement (ModP), d'une information de paiement (InfP); - une étape de transmission (180), d'un message d'information (Msgl) au serveur marchand (SM).

Procédés de traitement de données transactionnelles, dispositifs et programmes correspondants.

1. Domaine de l'invention

L'invention se rapporte au domaine du paiement. Plus particulièrement, l'invention se rapporte au paiement de biens et de services auprès de commerçants en ligne, par exemple par l'intermédiaire d'une plateforme de vente en ligne accessible depuis un réseau de communication.

2. Art antérieur

Le paiement de biens ou de services en ligne, par l'intermédiaire de plateformes commerciale, a facilité la vie des consommateurs. En règle générale, le paiement est effectué auprès d'un commerçant par l'intermédiaire d'une carte de paiement. Plus particulièrement, le paiement est effectué en utilisant les données inscrites sur la carte de paiement (nom du titulaire, numéro de carte, date de validité, cryptogramme visuel). Ces données sont saisies par l'utilisateur, dans un formulaire de saisie en ligne, qui lui est proposé lors de la validation de son achat. Ces données peuvent être complétées. En effet, le problème d'un paiement par carte bancaire en ligne est lié l'identification et l'authentification de la personne qui saisit les informations de la carte de paiement. Il est en effet très difficile de s'assurer que la personne qui saisit les données de la carte bancaire est réellement le titulaire de cette carte. Pour pallier ce problème, des systèmes ont été mis en œuvre. Parmi ces systèmes, le protocole 3D-Secure, qui a reçu le soutien de Visa et de MasterCard, vise à s'assurer que le titulaire de la carte est bien celui qui réalise la transaction. Usuellement, ce système comprend, pour l'utilisateur qui souhaite payer, une étape de saisie d'un code complémentaire. Ce code complémentaire n'est supposé être connu que de l'utilisateur lui-même, soit parce qu'il s'agit d'une donnée personnelle (comme sa date de naissance), soit parce qu'il s'agit d'une donnée dont il a seul connaissance (comme un code transmis par SMS). Ce type de solution, cependant, pose problème. D'une part il a été constaté que la mise ne œuvre d'une solution de type 3D-Secure avait un effet négatif sur les ventes, car cela complique le processus pour l'utilisateur. La baisse peut être située entre dix et quinze pour cent, ce qui est loin d'être négligeable. De ce fait, les commerçants ne sont pas réellement tenter d'adopter ce type de solutions.

Par ailleurs, ce type de solutions ne garantit en rien le paiement. En effet, du fait que le paiement est réalisé en mode "Card Non Present", c'est à dire sans présence réelle de la carte bancaire, la transaction est tout à fait répudiable par le titulaire de la carte : cela signifie que la transaction peut être annulée postérieurement à la livraison du bien ou du service acheté (par exemple en cas de fraude, la transaction est annulée par le titulaire de la carte postérieurement à la fraude). Dans le cas normal, sans 3D-Secure, le commerçant est complètement perdant lorsque la transaction est répudiée postérieurement à la livraison : il ne peut qu'intenter une action judiciaire sans grand espoir que celle-ci puisse le dédommager. Dans le cas d'une fraude avec 3D-Secure, c'est la banque qui accepte le risque de ne pas être réglée. En cas de fraude, c'est donc elle qui est perdante, avec les mêmes conséquences que pour le commerçant. Cela vient du fait de l'absence de présence de la carte.

Il existe donc un besoin de fournir une méthode permettant des achats en lignes non répudiables, méthode qui soit simple pour l'utilisateur et qui n'entraine pas de perte de chiffre d'affaire.

3. Résumé de l'invention

L'invention ne pose pas ces problèmes de l'art antérieur. Plus particulièrement, l'invention se rapporte à une méthode de traitement de données transactionnelles.

L'invention se rapporte à un procédé de traitement de données transactionnelles, mis en œuvre au sein d'un serveur intermédiaire sécurisé, connecté à un réseau de communication. Un tel procédé comprend :

- une étape de réception, par le serveur intermédiaire sécurisé d'une requête de paiement comprenant une donnée représentative d'une identification d'un terminal de communication utilisé par un utilisateur pour effectuer une opération d'achat sur un serveur marchand connecté audit réseau de communication ;
- une étape d'établissement d'une liaison sécurisée point à point avec un Module de paiement du terminal de communication ;
- une étape de transmission, audit module de paiement, d'une requête d'exécution de paiement ;
- une étape de réception de la part du module de paiement, d'une information de paiement ;
- une étape de transmission, d'un message d'information au serveur marchand.

Selon une caractéristique particulière, le procédé de traitement de données transactionnelles comprend préalablement à ladite étape d'établissement d'une liaison sécurisée :

- une étape de recherche, au sein d'une base de données, d'au moins une donnée représentative d'un identifiant d'un module de paiement attaché audit terminal de communication à l'aide de ladite donnée représentative d'une identification d'un terminal de communication ;
- une étape de vérification de la validité dudit module de paiement ;
- une étape d'obtention d'au moins une donnée permettant d'établir une liaison sécurisée avec ledit module de paiement lorsque ladite étape de vérification de la validité dudit module de paiement est positive.

Dans un autre mode de réalisation, côté terminal client, la technique se rapporte à un procédé de traitement de données transactionnelles, mis en œuvre au sein d'un module de paiement attaché à un terminal de communication et connecté à un réseau de communication. Un tel procédé comprend :

- une étape de réception, par le module de paiement et par l'intermédiaire du terminal de communication, d'une requête d'établissement d'une liaison sécurisée point à point avec un serveur intermédiaire sécurisé, en fonction d'une donnée représentative d'une identification dudit terminal de communication.
- une étape d'établissement de ladite liaison sécurisée à l'aide d'au moins une clé de chiffrement comprise dans ledit module de paiement ;
- une étape de réception, de la part du serveur intermédiaire sécurisé, d'une requête d'exécution de transaction de paiement ;
- une étape de calcul d'un certificat de transaction en utilisant des clés de chiffrement et au moins une donnée issue d'une carte à microcircuit présentée par un utilisateur pour effectuer la transaction ;
- une étape de transmission dudit certificat de transaction au serveur intermédiaire sécurisé ;
- une étape de réception d'un acquittement correspondant à la transaction en provenance dudit serveur intermédiaire sécurisé.

Selon une caractéristique particulière, ladite étape de calcul d'un certificat de transaction comprend une étape d'authentification de ladite la carte à microcircuit.

Selon une caractéristique particulière, le procédé de traitement de données transactionnelles comprend une étape de saisie, par ledit utilisateur, d'un code d'identification personnel attaché à ladite carte à microcircuit.

Ainsi, le module de traitement est apte à contrôler la validité de la saisie du code de l'utilisateur

Dans un autre mode de réalisation, la technique se rapporte à un serveur de traitement de données transactionnelles, dit serveur intermédiaire sécurisé, serveur pouvant être connecté à un réseau de communication. Un tel serveur comprend :

- des moyens de réception d'une requête de paiement comprenant une donnée représentative d'une identification d'un terminal de communication utilisé par un utilisateur pour effectuer une opération d'achat sur un serveur marchand connecté audit réseau de communication ;
- des moyens d'établissement d'une liaison sécurisée point à point avec un module de paiement du terminal de communication ;
- des moyens de transmission, audit module de paiement, d'une requête d'exécution de paiement ;
- des moyens de réception de la part du module de paiement, d'une information de paiement. ;
- des moyens de transmission, d'un message d'information au serveur marchand.

Selon un mode de réalisation spécifique, la technique proposée se rapporte à un module de paiement rattachable à un terminal de communication, terminal pouvant être connecté à un réseau de communication. Un tel module comprend :

- des moyens de réception, par l'intermédiaire du terminal de communication, d'une requête d'établissement d'une liaison sécurisée point à point avec un serveur intermédiaire sécurisé.
- des moyens d'établissement de ladite liaison sécurisée à l'aide d'au moins une clé de chiffrement comprise dans ledit module de paiement ;
- des moyens de réception, de la part du serveur intermédiaire sécurisé, d'une requête d'exécution de transaction de paiement ;
- des moyens de calcul d'un certificat de transaction en utilisant des clés de chiffrement et au moins une donnée issue d'une carte à microcircuit présentée par un utilisateur pour effectuer la transaction ;

- des moyens de transmission dudit certificat de transaction au serveur intermédiaire sécurisé ;
- des moyens de réception d'un acquittement correspondant à la transaction en provenance dudit serveur intermédiaire sécurisé.

D'une manière générale, la technique proposée se rapporte à un procédé de traitement de données transactionnelles, mis en œuvre au sein d'un système comprenant un serveur intermédiaire sécurisé, connecté à un réseau de communication et un module de paiement attaché à un terminal de communication connecté audit réseau de communication, procédé caractérisé en ce qu'il comprend :

- une étape de réception, par le serveur intermédiaire sécurisé d'une requête de paiement comprenant une donnée représentative d'une identification d'un terminal de communication utilisé par un utilisateur pour effectuer une opération d'achat sur un serveur marchand connecté audit réseau de communication ;
- une étape de réception, par le module de paiement et par l'intermédiaire du terminal de communication, d'une requête d'établissement d'une liaison sécurisée point à point avec le serveur intermédiaire sécurisé, en fonction de ladite donnée représentative d'une identification dudit terminal de communication.
- une étape d'établissement d'une liaison sécurisée point à point avec ledit module de paiement du terminal de communication ;
- une étape de transmission, audit module de paiement, par le serveur intermédiaire sécurisé, d'une requête d'exécution de paiement ;
- une étape de réception, de la part du serveur intermédiaire sécurisé, par ledit module de paiement, de ladite requête d'exécution de paiement ;
- une étape de calcul, par ledit module de paiement, d'un certificat de transaction en utilisant des clés de chiffrement et au moins une donnée issue d'une carte à microcircuit présentée par un utilisateur pour effectuer la transaction ;
- une étape de transmission dudit certificat de transaction au serveur intermédiaire sécurisé ;
- une étape de réception de la part du module de paiement, par le serveur intermédiaire sécurisé, d'une information de traitement de données ;
- une étape de transmission, d'un message d'information au serveur marchand ;

- une étape de réception, par ledit module de paiement, d'un acquittement correspondant à la transaction en provenance dudit serveur intermédiaire sécurisé.

Dans un autre mode de réalisation, la technique proposée se rapporte à un système de traitement de données transactionnelles comprenant un serveur intermédiaire sécurisé, connecté à un réseau de communication et un module de paiement attaché à un terminal de communication connecté audit réseau de communication, système caractérisé en ce qu'il comprend :

- des moyens de réception, par le serveur intermédiaire sécurisé d'une requête de paiement comprenant une donnée représentative d'une identification d'un terminal de communication utilisé par un utilisateur pour effectuer une opération d'achat sur un serveur marchand connecté audit réseau de communication ;
- des moyens de réception, par le module de paiement et par l'intermédiaire du terminal de communication, d'une requête d'établissement d'une liaison sécurisée point à point avec le serveur intermédiaire sécurisé, en fonction de ladite donnée représentative d'une identification dudit terminal de communication.
- des moyens d'établissement d'une liaison sécurisée point à point avec ledit module de paiement du terminal de communication ;
- des moyens de transmission, audit module de paiement, par le serveur intermédiaire sécurisé, d'une requête d'exécution de paiement ;
- des moyens de réception, de la part du serveur intermédiaire sécurisé, par ledit module de paiement, de ladite requête d'exécution de paiement ;
- des moyens de calcul, par ledit module de paiement, d'un certificat de transaction en utilisant des clés de chiffrement et au moins une donnée issue d'une carte à microcircuit présentée par un utilisateur pour effectuer la transaction ;
- des moyens de transmission dudit certificat de transaction au serveur intermédiaire sécurisé ;
- des moyens de réception de la part du module de paiement, par le serveur intermédiaire sécurisé, d'une information de traitement de données ;
- des moyens de transmission d'un message d'information au serveur marchand ;

- des moyens de réception, par ledit module de paiement, d'un acquittement correspondant à la transaction en provenance dudit serveur intermédiaire sécurisé.

Les procédés et dispositifs présentés sont bien entendu complémentaires.

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. Figures

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, du point de vue du serveur intermédiaire sécurisé ;
- la figure 2 présente un synoptique de la technique proposée, du point de vue du module de paiement ;
- la figure 3 décrit un serveur intermédiaire sécurisé de transaction ;
- la figure 4 décrit un module de paiement.

5. Description

Dans une transaction commerciale à distance classique l'utilisateur entre en relation avec un Site Marchand via un terminal de communication lui permettant d'échanger des données (traditionnellement un PC, tablette,… connectés localement ou à distance à internet) pour sélectionner le bien ou le service qu'il souhaite acheter. Lors du paiement du bien/service sélectionné, l'utilisateur qui souhaite payer par carte doit communiquer via le site marchant les données d'identification de sa carte (traditionnellement le PAN, la date de validité et le cryptogramme). Dans le meilleur des cas, le flux d'information est redirigé du site marchand vers un site sécurisé ce qui évite la transmission de données sensibles au site marchand. Dans d'autres cas, généralement des systèmes privatifs permettant le paiement entre un groupe d'abonnées, on ne communique pas ses données bancaires mais des données équivalentes permettant in fine le transfert d'argent entre le compte du Client et celui du commerçant. Dans tous ces cas, outre la notion de sécurisation des informations transmises par l'utilisateur, reste la problématique de la répudiation du paiement par l'utilisateur et donc la non-garantie du paiement au commerçant.

La présente technique, présentée en relation avec la figure 1, repose sur l'implémentation d'un principe de paiement de proximité par carte bancaire (sécurisé, garantie, non répudiable) pour réaliser un paiement à distance. On résout la problématique préalablement présentée en utilisant un Module de paiement (ModP) contenant des mécanismes de sécurité propres à un terminal de paiement classique et capable de traiter une transaction par carte à microcircuit. Ce Module de paiement (ModP) est connecté ou intégré au terminal de communication (TC) (PC, Tablette,…) de l'utilisateur.

Après la phase de transaction commerciale réalisée via des réseaux ouverts (ex Internet) entre le terminal de communication TC (PC/Tablette) et le Site Marchand SM, celui-ci déclenche la phase de paiement.

Cette phase de paiement débute par la réception (100), par un serveur intermédiaire sécurisé (SRI) (serveur passerelle), d'un message de demande de paiement (également appelée requête de paiement RqP). Ce message provient du site marchand SM (ou d'un des serveurs du site marchand). Ainsi, au lieu de transmettre des données bancaires de l'utilisateur (comme cela se fait traditionnellement), le Site Marchant SM

transmet des informations relatives à la transaction commerciale (montant à payer,...). La requête de paiement RqP comprend également une identification du terminal de communication (IdTC) utilisé par l'utilisateur (cette identification IdTC est explicitée par la suite).

Le Serveur intermédiaire sécurisé (SRI) établit (120) alors une liaison sécurisée (LS) point à point avec le Module de paiement (ModP) du terminal de communication (TC). Cette liaison est établie grâce à l'identification IdTC du terminal de communication TC. Lorsque la liaison sécurisée est établie, le Serveur intermédiaire sécurisé (SM) transmet (140) au Module de paiement (ModP), une requête d'exécution de paiement (RqEP). La transaction de paiement est réalisée par le module de paiement (ModP) avec la carte à microcircuit (CardM) de l'utilisateur en utilisant des mécanismes similaires à ceux utilisés sur un terminal de paiement classique chez un commerçant.

Lorsque la transaction est effectuée sans erreur, le Serveur intermédiaire sécurisé (SRI) reçoit (160) de la part du module de paiement (ModP), une information de paiement (InfP). Cette information de paiement InfP comprend au moins une donnée représentative de l'acceptation ou du refus de paiement. Le processus d'obtention de cette information est décrit par la suite.

La transaction se termine par une transmission (180), par le Serveur intermédiaire sécurisé (SRI) d'un message d'information (MsgI) au site marchand (SM). Ce message d'information (MsgI) comprend une information représentative du résultat de la transaction qui a été réalisée. Si la transaction a été réalisée avec succès, le site marchand peut délivrer le bien/service. Les mécanismes utilisés pour réaliser la transaction étant identiques à ceux d'un terminal de paiement chez un commerçant, l'utilisateur ne peut pas répudier la transaction au seul motif d'un paiement par vente à distance comme cela est le cas avec les solutions actuelles.

On établit ainsi un canal de communication sécurisé point à point entre le Serveur intermédiaire sécurisé d'une part et le Module de paiement d'autre part. Ce canal point à point autorise l'échange sécurisé de données relatives à la transaction financière entre deux entités elles-mêmes sécurisées, le Serveur intermédiaire sécurisé et le Module de paiement. Par ailleurs, cette méthode de traitement de données transactionnelles implique une séparation stricte des flux commerciaux d'une part (respectivement entre le terminal de communication et le serveur marchand) et d'autre part les flux de paiement

(respectivement entre le terminal de communication et le serveur intermédiaire sécurisé). On assure ainsi que le serveur marchand n'est pas en possession de données de carte bancaire de l'utilisateur. On assure également que le paiement ne peut pas être réalisé sans la possession physique de la carte à microcircuits.

L'établissement du canal de communication sécurisé entre le module de paiement et le serveur intermédiaire sécurisé repose, selon un mode de réalisation de la technique proposée, sur plusieurs éléments, dont le premier est l'identification du terminal de communication. Cette identification permet au serveur intermédiaire sécurisé de reconnaitre le terminal de communication et d'entrer en relation avec lui.

Dans un mode de réalisation basique, l'identification du terminal de communication est assurée par son adresse IP. Dans un mode de réalisation complémentaire, l'identification repose sur l'adresse MAC du module matériel utilisé par le terminal de communication pour réaliser la transmission des données (par exemple adresse MAC de du module matériel de communication WiFi ou adresse MAC de la carte réseau Ethernet). Dans un autre mode de réalisation, l'identification du terminal de communication est réalisée par un mécanisme de redirection d'URL depuis le serveur marchand vers le serveur intermédiaire sécurisé. Ce mécanisme de redirection est complété par la transmission, du serveur marchand vers le serveur intermédiaire, de données de session, ces données de session comprenant par exemple le nom et le prénom de l'utilisateur, une adresse IP, voire un numéro de compte client (chez le marchand). Sur la base des données transmises par le site marchand, le serveur intermédiaire sécurisé identifie le module de paiement dans une base de données, et transmet, sur une interface de communication spécifique (par exemple un port UDP/IP spécifique) du terminal de communication, une requête d'établissement d'un canal de communication sécurisé point à point. Comme cela est explicité infra, le module de paiement "écoute" cette interface spécifique et s'active lors de la réception de cette requête.

Le fonctionnement du module de paiement est décrit en relation avec la figure 2. Comme indiqué préalablement, le terminal de communication est équipé d'un module de paiement. Dans un premier mode de réalisation, ce module de paiement est un composant électronique programmable particulier, inséré au sein du terminal de communication (soudé sur une carte mère du terminal de communication). Ce module de

paiement physique comprend une unité de traitement indépendante, un espace de stockage sécurisé et des interfaces de communication. Plus particulièrement, le module de paiement, quelle que soit son implémentation, comprend une interface de communication avec un lecteur de données sans contact. Cette interface de communication, dite sans contact, permet de commander un module de lecture sans contact. Ce module de lecture sans contact est celui qui est utilisé pour dialoguer avec la carte à microcircuit (qui comprend donc des moyens de communication sans contact). Alternativement, le lecteur de données sans contact fait partie du module de paiement. Le module de paiement comprend alors une liaison vers une antenne sans contact implémentée au sein du terminal.

Ce module comporte également des mécanismes permettant d'assurer le stockage sécurisé des éléments de chiffrement qui sont utilisés, d'une part pour assurer la transmission sécurisée avec le Serveur intermédiaire sécurisé et d'autre part, pour assurer la transaction de paiement sécurisée avec la carte à microcircuit du Client. Les mécanismes garantissent par ailleurs la non accessibilité des données sensibles contenues dans le Module de paiement (clefs de chiffrement,...). Enfin, le module de paiement dispose de codes exécutables lui permettant d'assurer le traitement de la carte à microcircuit de l'utilisateur et les échanges avec le Serveur intermédiaire sécurisé.

Du point de vue du module de paiement, la phase de paiement débute par la réception (200), par le module de paiement (ModP) et par l'intermédiaire du terminal de communication (TC), d'une requête (RqLS) d'établissement d'une liaison sécurisée (LS) point à point avec le serveur intermédiaire sécurisé (SRI).

Pour établir (220) cette liaison sécurisée (LS), le module de paiement (ModP) utilise (225) des clés de chiffrement (KeyModP) pour d'une part authentifier (230) le serveur intermédiaire sécurisé (SRI) et générer (235) des certificats (CertLS) permettant l'établissement de la liaison sécurisée (LS).

Lorsque la liaison sécurisée (LS) est établie, le module de paiement (ModP) reçoit (240), de la part du serveur intermédiaire sécurisé (SRI), une requête d'exécution de transaction de paiement (RqTP). Sur réception de cette requête, le module de paiement (ModP) :

- vérifie (245) la carte à microcircuit : plus spécifiquement, vérifie que la carte sans contact est présente et que les informations qu'elle contient sont formées de manière valide;
- calcule (250) le certificat de transaction (CertT) en utilisant des clés de chiffrement (KeyModP);

Optionnellement, le module de paiement (ModP) requiert la saisie d'un code d'identification personnel sur le terminal de communication. Cette saisie est réalisée dans des conditions d'isolation de saisies particulières. Plus particulièrement, le module de paiement comprend des moyens d'interception des saisies réalisées sur le terminal de communication. Optionnellement, le module de paiement (ModP) requiert une autorisation auprès d'un centre de contrôle accessible par l'intermédiaire de la liaison sécurisée (LS).

Postérieurement au calcul du certificat de transaction, le module de paiement (ModP), transmet (260) ce certificat de transaction (CertT) au serveur intermédiaire sécurisé (SRI).

Le serveur intermédiaire sécurisé (SRI) reçoit le certificat de transaction, réalise le traitement financier de la transaction et transmet les acquittements nécessaires, notamment au module de paiement (ModP) et au site marchand (SM).

Le module de paiement (ModP) reçoit (280) l'acquittement correspondant à la transaction de paiement. Le module de paiement (ModP) démonte (300) la liaison sécurisée (LS).

On décrit, en relation avec la figure 3, un serveur intermédiaire sécurisé mis en œuvre pour réaliser les transactions, du point de vue du serveur, selon le procédé décrit préalablement.

Par exemple, le serveur 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 identifiant d'utilisateur et une donnée représentative

d'un montant de transaction. Le microprocesseur de l'unité de traitement 32 met en œuvre les étapes du procédé de traitement de données représentatives de transactions, selon les instructions du programme d'ordinateur 33 pour effectuer une validation de transaction (recherche du module de paiement, établissement de la liaison sécurisée, transmission des requêtes).

Pour cela, le serveur 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 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.

Par ailleurs, le serveur comprend en outre les moyens d'identification et de validation modules de paiement. 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, des moyens de comparaisons de données de localisation (par exemple sur la base des adresses IP des modules de paiement).

On décrit, en relation avec la figure 4, un module de paiement (module de traitement de données transactionnelles) mis en œuvre pour réaliser les transactions selon le procédé décrit préalablement.

Par exemple, le module de paiement 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, c'est-à-dire à la mise sous tension du terminal de communication auquel le module de paiement est connecté, 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'une requête d'initialisation d'une liaison sécurisée. Le microprocesseur de l'unité de traitement 42 met en œuvre les étapes du procédé de traitement des données transactionnelles, selon les instructions du programme d'ordinateur 43 pour effectuer une validation de transactions avec une carte à microcircuits, comme une carte de paiement sans contact.

Pour cela, le dispositif 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 apte à mettre en œuvre des algorithme de cryptographie tel que l'algorithme RSA.

Dans un mode de réalisation particulier de l'invention, le module de paiement de l'utilisateur, pouvant être intégré (c'est à dire physiquement soudé ou attaché) à un Smartphone, une tablette, un ordinateur portable, un PDA, intègre des moyens de gestion de transaction tels que décrit précédemment. Ces moyens peuvent se présenter sous la forme d'un processeur particulier implémenté au sein du module de paiement, ledit processeur étant un processeur sécurisé. Selon un mode de réalisation particulier, ce module de paiement met en œuvre une application particulière qui est en charge de la gestion 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 et de manière complémentaire, permettre une gestion du module de paiement à partir du serveur intermédiaire sécurisé. Dans un autre mode de réalisation, l'application de gestion installée sur le module de paiement comprend également d'identification uniques permettent soit d'assurer l'authenticité de l'application soit d'assurer l'identification du porteur du module de paiement, soit les deux.

REVENDICATIONS

1. Procédé de traitement de données transactionnelles, mis en œuvre au sein d'un serveur intermédiaire sécurisé, connecté à un réseau de communication, procédé caractérisé en ce qu'il comprend :

- une étape de réception, par le serveur intermédiaire sécurisé d'une requête de paiement comprenant une donnée représentative d'une identification d'un terminal de communication utilisé par un utilisateur pour effectuer une opération d'achat sur un serveur marchand connecté audit réseau de communication ;
- une étape de recherche, au sein d'une base de données, d'au moins une donnée représentative d'un identifiant d'un module de paiement attaché audit terminal de communication à l'aide de ladite donnée représentative d'une identification d'un terminal de communication ;
- une étape de vérification de la validité dudit module de paiement ;
- une étape d'obtention d'au moins une donnée permettant d'établir une liaison sécurisée avec ledit module de paiement lorsque ladite étape de vérification de la validité dudit module de paiement est positive ;
- une étape d'établissement d'une liaison sécurisée point à point avec ledit module de paiement du terminal de communication, à l'aide de ladite au moins une donnée permettant d'établir une liaison sécurisée, ledit module de paiement étant apte à communiquer sans contact avec une carte à microcircuit dudit utilisateur pour la réalisation de ladite opération d'achat ;
- une étape de transmission, audit module de paiement, d'une requête d'exécution de paiement ;
- une étape de réception de la part du module de paiement, d'une information de paiement ;
- une étape de transmission, d'un message d'information au serveur marchand.

2. Procédé de traitement de données transactionnelles, mis en œuvre au sein d'un module de paiement attaché à un terminal de communication et connecté à un réseau de communication, procédé caractérisé en ce qu'il comprend :

Date Reçue/Date Received 2021-09-20

- une étape de réception, par le module de paiement et par l'intermédiaire du terminal de communication, d'une requête d'établissement d'une liaison sécurisée point à point avec un serveur intermédiaire sécurisé, en fonction d'une donnée représentative d'une identification dudit terminal de communication ;
- une étape d'établissement de ladite liaison sécurisée à l'aide d'au moins une clé de chiffrement comprise dans ledit module de paiement ;
- une étape de réception, de la part du serveur intermédiaire sécurisé, d'une requête d'exécution de transaction de paiement ;
- une étape de calcul d'un certificat de transaction en utilisant des clés de chiffrement et au moins une donnée issue d'une carte à microcircuit présentée par un utilisateur pour effectuer la transaction ;
- une étape de transmission dudit certificat de transaction au serveur intermédiaire sécurisé ;
- une étape de réception d'un acquittement correspondant à la transaction en provenance dudit serveur intermédiaire sécurisé.

3. Procédé de traitement de données transactionnelles selon la revendication 2, caractérisé en ce que ladite étape de calcul d'un certificat de transaction comprend une étape d'authentification de ladite la carte à microcircuit.

4. Procédé de traitement de données transactionnelles selon la revendication 2, caractérisé en ce qu'il comprend une étape de saisie, par ledit utilisateur, d'un code d'identification personnel attaché à ladite carte à microcircuit.

5. Serveur de traitement de données transactionnelles, dit serveur intermédiaire sécurisé, connecté à un réseau de communication, caractérisé en ce qu'il comprend :

- des moyens de réception d'une requête de paiement comprenant une donnée représentative d'une identification d'un terminal de communication utilisé par un utilisateur pour effectuer une opération d'achat sur un serveur marchand connecté audit réseau de communication ;

Date Reçue/Date Received 2021-09-20

- des moyens de recherche, au sein d'une base de données, d'au moins une donnée représentative d'un identifiant d'un module de paiement attaché audit terminal de communication à l'aide de ladite donnée représentative d'une identification d'un terminal de communication ;
- des moyens de vérification de la validité dudit module de paiement ;
- des moyens d'obtention d'au moins une donnée permettant d'établir une liaison sécurisée avec ledit module de paiement lorsque la vérification de la validité dudit module de paiement est positive ;
- des moyens d'établissement d'une liaison sécurisée point à point avec ledit module de paiement du terminal de communication, à l'aide de ladite au moins une donnée permettant d'établir une liaison sécurisée, ledit module de paiement étant apte à communiquer sans contact avec une carte à microcircuit dudit utilisateur pour la réalisation de ladite opération d'achat ;
- des moyens de transmission, audit module de paiement, d'une requête d'exécution de paiement ;
- des moyens de réception de la part du module de paiement, d'une information de paiement ;
- des moyens de transmission, d'un message d'information au serveur marchand.

6. Module de paiement rattachable à un terminal de communication connecté à un réseau de communication, caractérisé en ce qu'il comprend :

- des moyens de réception, par l'intermédiaire du terminal de communication, d'une requête d'établissement d'une liaison sécurisée point à point avec un serveur intermédiaire sécurisé ;
- des moyens d'établissement de ladite liaison sécurisée à l'aide d'au moins une clé de chiffrement comprise dans ledit module de paiement ;
- des moyens de réception, de la part du serveur intermédiaire sécurisé, d'une requête d'exécution de transaction de paiement ;
- des moyens de calcul d'un certificat de transaction en utilisant des clés de chiffrement et au moins une donnée issue d'une carte à microcircuit présentée par un utilisateur pour effectuer la transaction ;

Date Reçue/Date Received 2021-09-20

- des moyens de transmission dudit certificat de transaction au serveur intermédiaire sécurisé ;
- des moyens de réception d'un acquittement correspondant à la transaction en provenance dudit serveur intermédiaire sécurisé.

7. Support non-transitoire d'informations lisible par ordinateur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution d'un procédé de traitement de données de transactionnelles selon la revendication 1, lorsque les instructions sont exécutées sur un ordinateur.

8. Support non- transitoire d'informations lisible par ordinateur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution d'un procédé de traitement de données de transactionnelles selon la revendication 2, lorsque les instructions sont exécutées sur un ordinateur.

Date Reçue/Date Received 2021-09-20

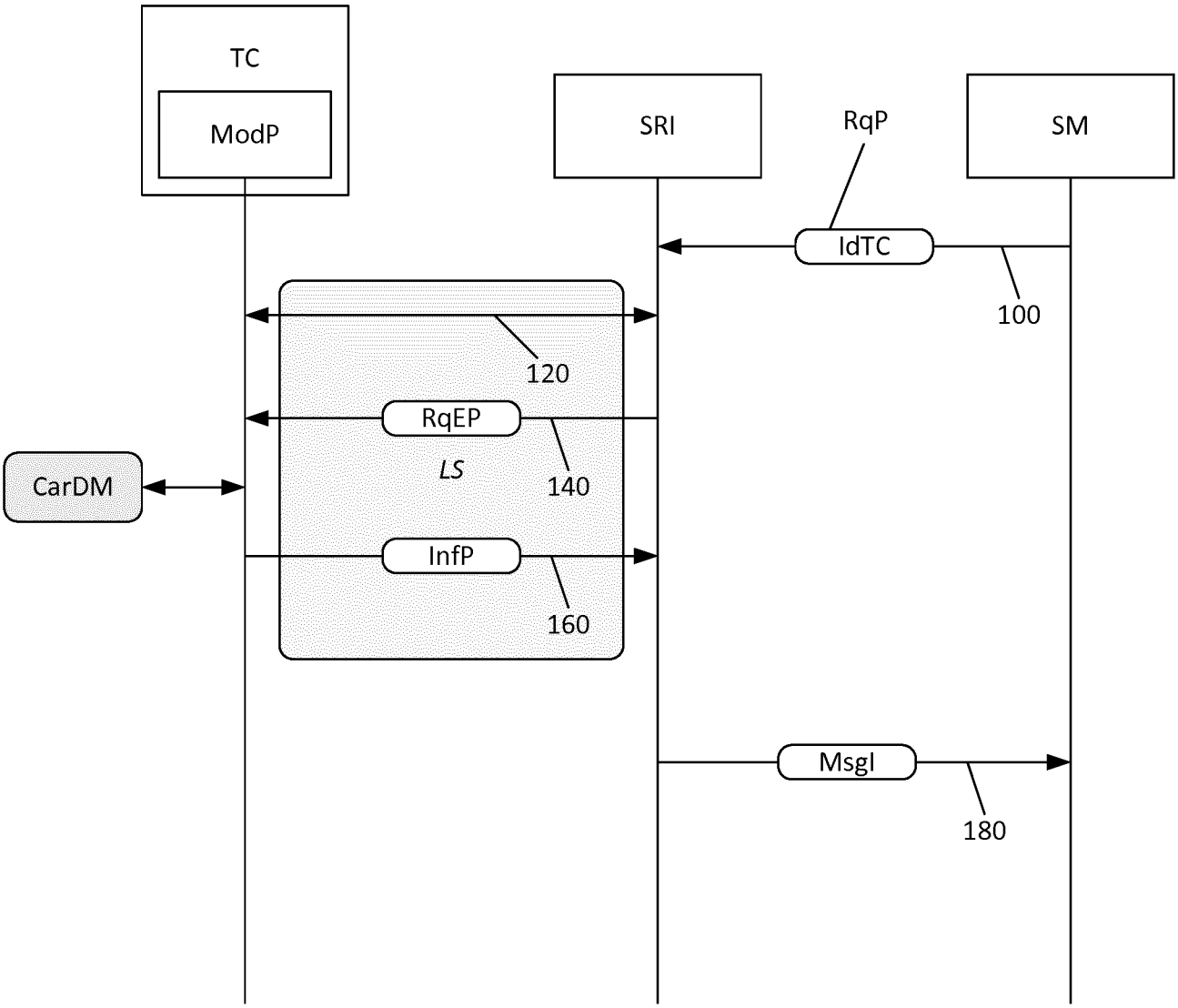

TC
ModP
SRI
RqP
SM
IdTC
100
120
RqEP
LS
140
CarDM
InfP
160
MsgI
180

Figure 1

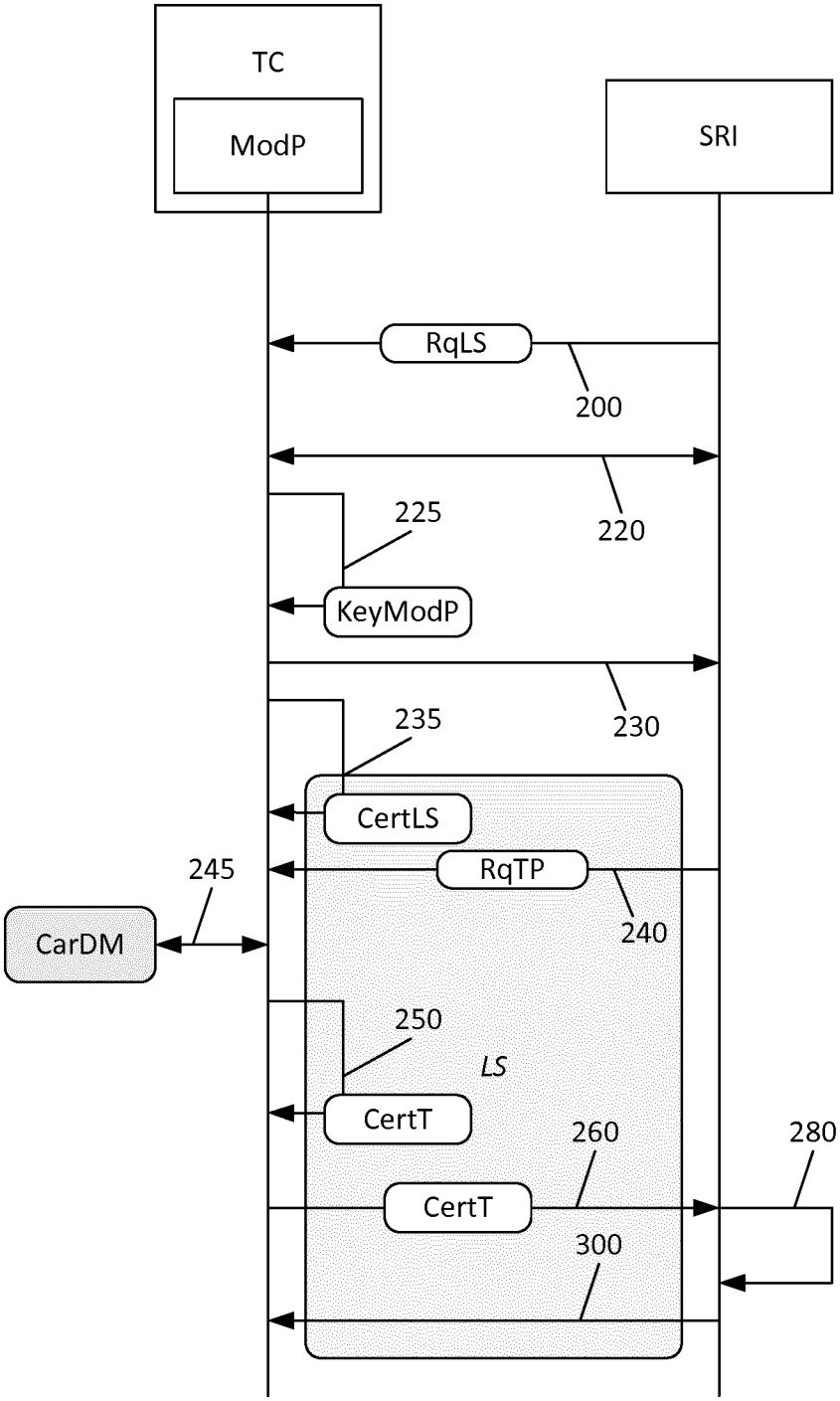

TC
ModP
SRI
RqLS
200
220
225
KeyModP
230
235
CertLS
RqTP
240
245
CarDM
250
LS
CertT
260
280
CertT
300

Figure 2

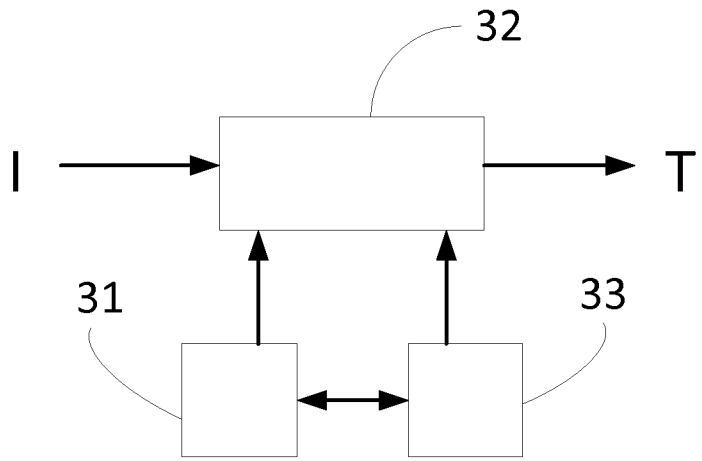


Figure 3

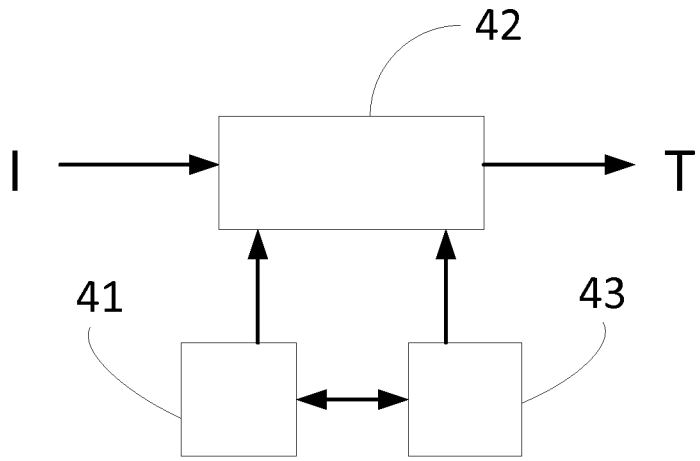
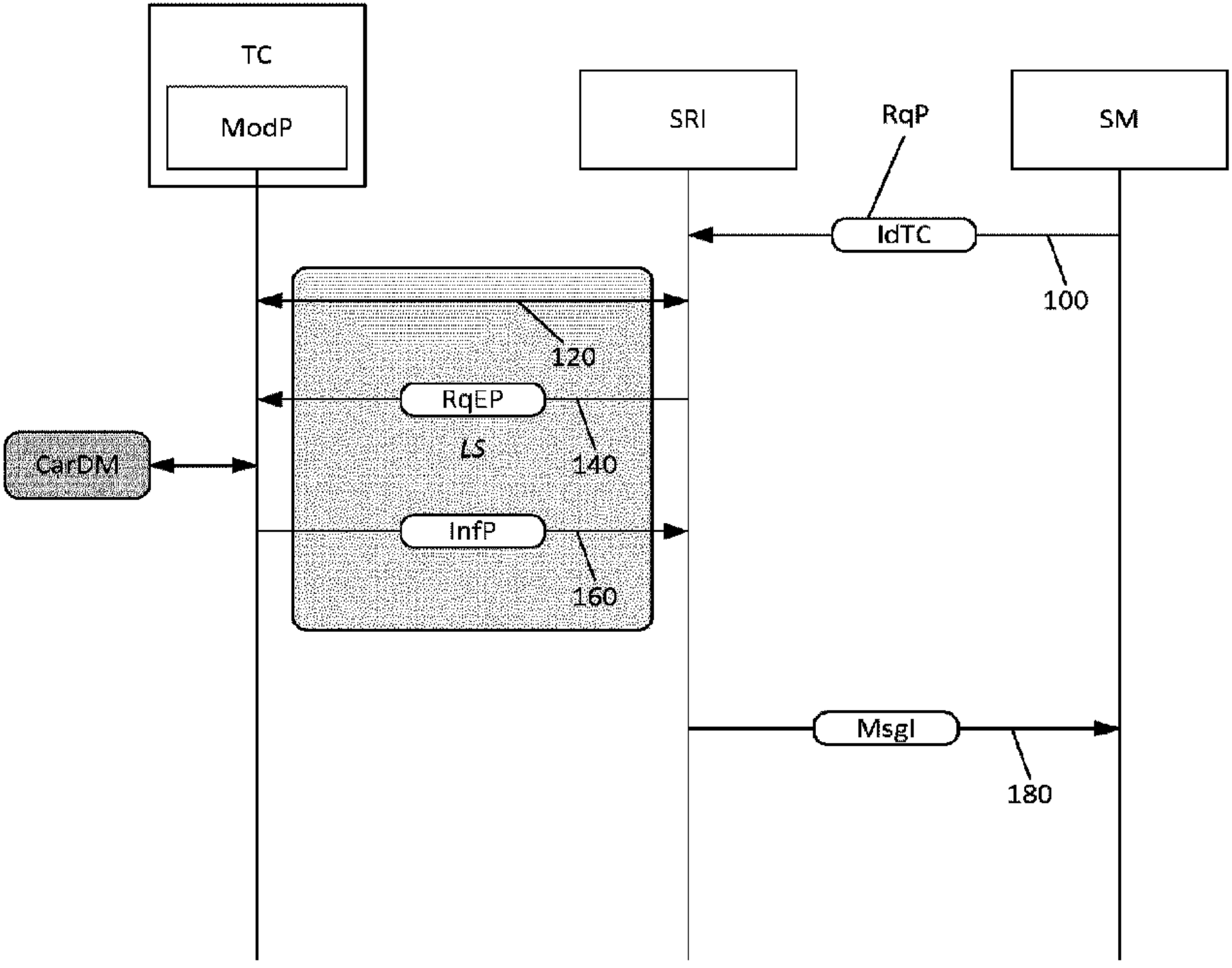


Figure 4


TC
ModP
SRI
RqP
SM
IdTC
100
120
RqEP
LS
140
CarDM
InfP
160
MsgI
180