(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 104 760***

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

(21) **N° d'enregistrement national :** **19 14346**

(51) Int Cl[8] : ***G 06 F 21/34*** *(2019.12), G 06 Q 20/40, H 04 L 9/32, 9/08*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 13.12.19.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 18.06.21 Bulletin 21/24.

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

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

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

(71) **Demandeur(s) :** *INGENICO GROUP Société anonyme* — FR.

(72) **Inventeur(s) :** BEUNARDEAU Marc, CONNOLLY Aisling, GERAUD Rémi, KOUDOUSSI Hiba et NACCACHE David.

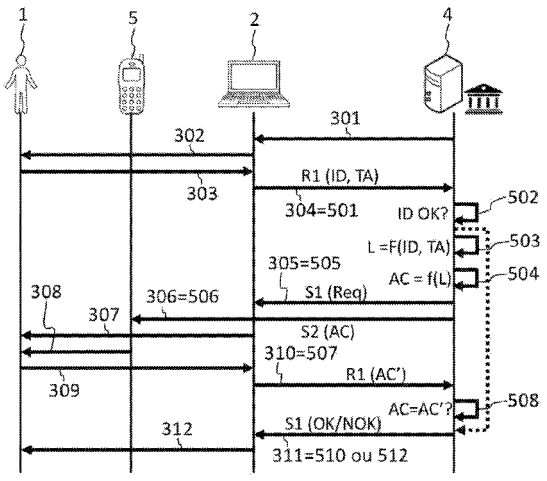
(73) **Titulaire(s) :** INGENICO GROUP Société anonyme.

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

(54) PROCEDE, SERVEUR ET SYSTEME D'AUTHENTIFICATION DE TRANSACTION UTILISANT DEUX CANAUX DE COMMUNICATION.

(57) L'invention concerne un procédé de transaction pour un utilisateur 1 utilisant un premier et un deuxième terminal 2 et relié à un serveur 4 via respectivement un premier et un deuxième canal de communication. Le premier terminal 2 envoie 304 au serveur 4 un montant de transaction TA. Le serveur 4 établit 502 à 504 un code de vérification AC dont une longueur L est fonction du montant de la transaction TA puis envoie 505 et 506 une requête Req au premier terminal 2 et le code de vérification AC au deuxième terminal 5. L'utilisateur renvoie 310 ladite requête remplie avec un code recopié AC' au serveur 4 à l'aide du premier terminal 2. Le serveur 4 compare 508 le code de vérification AC avec le code recopié AC' et envoie 510, 512 au premier terminal 2 un message de validation ou d'invalidation de transaction en fonction de la comparaison.

Figure pour l'abrégé : Fig.3



FR 3 104 760 - A1

Description

Titre de l'invention : PROCEDE, SERVEUR ET SYSTEME D'AUTHENTIFICATION DE TRANSACTION UTILISANT DEUX CANAUX DE COMMUNICATION

Domaine technique

[0001] La présente invention se rapporte à un procédé d'authentification de transaction utilisant deux canaux de communication ainsi qu'à un serveur et un système de transaction bancaire mettant en œuvre le procédé. Plus particulièrement, l'invention se rapporte à l'utilisation d'un deuxième canal de communication pour sécuriser une transaction réalisée à partir d'un premier canal de communication.

Technique antérieure

[0002] Les transactions de paiement électronique faisant l'objet de ce document concernent les opérations de paiement réalisées en ligne. Un paiement en ligne est réalisé lors de la vente ou l'achat de biens ou de services, aussi bien par des entreprises, des ménages, des particuliers, des gouvernements ou d'autres organisations, publiques ou privées, sur des réseaux interconnectés d'ordinateurs, tel que par exemple internet. Les biens et services sont commandés sur ces réseaux, mais le paiement et la livraison finale du bien ou du service peuvent être effectués en ligne ou hors ligne. De plus, les clients des banques effectuent régulièrement des opérations de paiement par virement en utilisant les services bancaires par Internet. De plus en plus de consommateurs utilisent le commerce électronique, pour rechercher et acheter des biens et des services sur des réseaux électroniques tels que, par exemple, Internet. Le paiement s'effectue généralement par la saisie d'un numéro de carte de débit et/ou de crédit, ou carte bancaire, ou à l'aide d'autres informations financières dans les champs respectifs d'un formulaire du site du commerçant en ligne. Les transactions peuvent également être effectuées à l'aide de fournisseurs de services de paiement en ligne ou mobiles, tels que ceux proposés par exemple par la société PayPal, Inc., de San Jose, en Californie. Pour assurer une meilleure sécurité, les systèmes de paiement électronique utilisent souvent des solutions de sécurité agglomérées telles que celle identifiées par les marques « 3Dsecure », « Verified by Visa », ou autre. De tels services de paiement et solutions de sécurité de paiement peuvent rendre les transactions plus faciles et/ou plus sûres pour les parties impliquées. Acheter avec l'aide d'un fournisseur de services de paiement depuis un terminal mobile portable est l'une des principales raisons pour lesquelles les achats en ligne et sur mobile se développent très rapidement.

[0003] Les systèmes de paiement en ligne traditionnels exposent les utilisateurs à des risques de sécurité. Par exemple, taper des numéros d'un identifiant de carte de crédit dans un

champ d'un formulaire de paiement en ligne expose un utilisateur au vol de ce numéro par une tierce personne qui regarde son écran, par un virus informatique de journalisation de frappe, etc. Bien que le stockage des numéros de carte de crédit par un détaillant en ligne puisse éviter d'obliger l'utilisateur à saisir manuellement à chaque achat les informations au cours de la transaction de paiement, il expose le détaillant en ligne à ses propres risques et responsabilités en matière de sécurité. Les informations sur les cartes de crédit peuvent également être capturées par des moyens simples, par exemple, en prenant une photo d'une carte exposée par inadvertance, sans oublier que des cartes de crédit peuvent être perdues ou volées, ce qui permet à une personne malintentionnée d'en faire un mauvais usage.

[0004] Par conséquent, les systèmes de paiement électroniques modernes, tels que les opérations bancaires en ligne et le commerce électronique, utilisent souvent une procédure dite d'authentification à deux facteurs de sécurité, ci-après désigné 2FA, pour authentifier en toute sécurité un client titulaire de carte bancaire lors de la transaction de paiement. Les procédures d'authentification à deux facteurs sont bien connues de l'homme du métier. L'une des formes les plus anciennes d'authentification à deux facteurs de sécurité, généralement utilisée par des banques pour les transactions bancaires par Internet, consiste à émettre aux clients titulaires de carte, avec la carte bancaire, une liste numérotée de nombres d'authentification de transaction, communément nommée TAN (de l'anglais Transaction Authentication Numbers), afin que, après la saisie des informations de carte dans un formulaire de demande de paiement sur un site Web d'une banque, dans une deuxième étape de la transaction, la banque demande à l'utilisateur de saisir manuellement la valeur TAN correspondant à un numéro choisi aléatoirement par la banque parmi la liste TAN.

[0005] Les inconvénients et la sécurité limitée de la solution 2FA susmentionnée conduisent à des formes plus avancées de procédures d'authentification à deux facteurs qui peuvent exiger, de nos jours, qu'un client dispose, outre la carte de paiement et/ou d'autres informations d'identité du client et d'un code PIN (de l'anglais Personnal Identification Number), d'un deuxième appareil personnel, enregistré par le système de paiement ou par la banque auprès de ce client, ledit appareil personnel étant utilisé comme second facteur d'authentification du client lors des transactions de paiement. Généralement, un tel appareil est un téléphone mobile ou un jeton sécurisé connecté à Internet ou à un autre réseau et qui est émis par la banque ou tout autre fournisseur de solution de paiement. Dans le cas d'une procédure 2FA, lors d'une transaction de paiement, un client utilise un appareil, généralement compatible avec Internet, pour sélectionner des biens, des services ou d'autres formes de transaction de paiement sur le site Web du marchand ou de la banque en ligne, et réalise une première étape de la transaction de paiement en remplissant les formulaires fournis par lesdits sites Internet

avec des informations de paiement requises, telles que le numéro de carte et/ou de compte bancaire, le nom et l'adresse du titulaire de la carte, etc. Une fois le formulaire envoyé, une banque, un fournisseur de solution de paiement ou un émetteur de carte de crédit envoie à un deuxième appareil du titulaire un code d'authentification de transaction à usage unique. Dans une deuxième étape, le code d'authentification est saisi manuellement par le titulaire puis envoyé via le réseau à la banque, au fournisseur de solution de paiement ou à l'émetteur de carte de crédit, afin que le code soit comparé au code d'authentification émis. Si la comparaison est correcte, l'opération de paiement sera réalisée avec succès, sinon, la transaction de paiement sera refusée, éventuellement avec notification au titulaire de la carte.

[0006] Bien que cette procédure d'authentification à deux facteurs augmente la sécurité globale des transactions de paiement électronique, elle augmente également le temps de transaction et d'abandon de panier d'achat. En effet, la saisie manuelle du code d'authentification prend non seulement un temps supplémentaire, mais plus important encore, elle est source d'erreur, ce qui crée une mauvaise expérience utilisateur qui peut entrainer l'abandon de la transaction à ce stade.

[0007] Un code d'authentification est généralement une chaîne alphanumérique d'une certaine longueur. La longueur de la chaine est définie a priori par un schéma de paiement et elle est la même pour toutes les transactions. Aujourd'hui, les implémentations de schémas à deux facteurs sont confrontées au dilemme suivant : soit le code d'authentification est court, ce qui est mieux pour l'expérience utilisateur, mais sa sécurité est médiocre car les codes courts peuvent être facilement devinés ; soit le code est long, ce qui est préférable pour la sécurité du système de paiement, mais augmente le risque d'erreur pour l'utilisateur.

[0008] La présente invention vise à remédier aux désagréments évoqués précédemment lors de l'utilisation de code d'authentification dans une procédure à deux facteurs de sécurité.

Résumé de l'invention

[0009] L'invention propose d'améliorer le système d'authentification à deux facteurs susmentionné en adaptant la complexité du code d'authentification, en particulier sa longueur, au montant payé lors de la transaction.

[0010] Selon un mode de réalisation, l'invention propose un procédé d'authentification de transaction utilisant deux canaux de communication de données pour un utilisateur utilisant un premier terminal relié à au moins un serveur de transaction bancaire via un premier canal de communication et un deuxième terminal relié à l'au moins un serveur de transaction bancaire via un deuxième canal de communication au moins logiquement distinct du premier canal de communication. Le procédé comporte :

- une première étape au cours de laquelle le premier terminal envoie à l'au moins un serveur de transaction bancaire des informations de transaction comprenant au moins un montant de la transaction, et une identification d'un compte et/ou d'une carte bancaire à débiter,
- une deuxième étape au cours de laquelle le serveur de transaction bancaire établit un code de vérification dont une longueur est fonction du montant de la transaction, détermine le deuxième terminal en fonction de l'identification du compte et/ou de la carte bancaire à débiter, puis envoie, d'une part, une requête de confirmation demandant le code de vérification au premier terminal via le premier canal de communication et, d'autre part, le code de vérification au deuxième terminal via le deuxième canal de communication,
- une troisième étape au cours de laquelle l'utilisateur copie le code de vérification reçu sur le deuxième terminal dans la requête de confirmation reçue par le premier terminal et renvoie ladite requête ainsi remplie avec le code recopié au serveur de transaction bancaire à l'aide du premier terminal via le premier canal de communication,
- une quatrième étape au cours de laquelle le serveur de transaction bancaire reçoit du premier terminal le code recopié, et compare le code de vérification avec le code recopié et envoie au premier terminal un message de validation de transaction si les codes sont identiques ou un message d'invalidation de transaction si les codes sont différents.

[0011] Ainsi, la longueur du code de vérification peut croître lorsque le montant de la transaction croît. Des codes d'authentification courts peuvent être attribués aux transactions impliquant de faibles montants de paiement, tandis que des codes plus longs et plus complexes, c'est-à-dire plus difficiles à deviner par des personnes malveillantes, peuvent être attribués aux montants de paiements plus importants. De manière préférée, la longueur du code de vérification peut être comprise entre une valeur minimale et une valeur maximale.

[0012] L'expérience utilisateur lors des transactions de paiement électronique est améliorée de deux manières. Tout d'abord, et surtout pour les transactions de faible montant, le travail de copie manuelle du code d'authentification d'un périphérique à un autre est allégé, ce qui est plus rapide et diminue le risque d'erreur pour l'utilisateur. Pour les transactions impliquant des sommes plus importantes, des codes d'authentification plus longs et plus complexes permettent à l'utilisateur d'apprécier que l'authentification par le second facteur, même si elle alourdit et ralentit la transaction, accroît la sécurité de la transaction, jouant ainsi un rôle rassurant.

[0013] En variante, les informations de transaction peuvent comprendre des informations d'identification du titulaire du compte et au moins une information redondante liée à l'identification du compte bancaire à débiter. La deuxième étape peut comporter une

étape préliminaire qui vérifie une concordance entre l'identification du compte bancaire à débiter, les informations d'identification du titulaire et la au moins une information redondante. La deuxième étape peut n'être réalisée que si la concordance est établie.

[0014] Considérant qu'un facteur de risque lors de la transaction peut dépendre d'autres paramètres que le montant de la transaction, la longueur du code de vérification peut dépendre en outre d'un facteur de risque déterminé à l'aide d'un ou plusieurs paramètres compris parmi : l'heure de la transaction, la date de la transaction, des informations relatives au titulaire de la carte, le nombre de transactions effectuées dans une période prédéterminée précédant la transaction.

[0015] Selon un deuxième mode de réalisation, l'invention propose un serveur de transaction bancaire comprenant une unité de traitement, une mémoire de programmes, au moins une interface de communication apte à communiquer via un premier canal de communication et via un deuxième canal de communication au moins logiquement distinct du premier canal de communication. La mémoire de programme comporte des instructions coopérant avec l'unité de traitement de sorte que le serveur soit configurer pour :

- à réception depuis le premier canal de communication d'une demande de transaction comprenant au moins un montant de la transaction et une identification d'un compte bancaire à débiter, calculer une longueur d'un code de vérification en fonction du montant de la transaction, déterminer le code de vérification à partir de la longueur de code calculée, déterminer un deuxième canal de communication en fonction de l'identification du compte bancaire à débiter, envoyer une requête de confirmation demandant le code de vérification via le premier canal de communication, et envoyer le code de vérification via le deuxième canal de communication,
- à réception d'un code reçu via le premier canal de communication en réponse à la requête de confirmation, comparer ledit code reçu avec le code de vérification et envoyer via le premier canal de communication un message de validation de transaction si lesdits codes sont identiques ou un message d'invalidation de transaction si lesdits codes sont différents.

[0016] Selon un autre mode de réalisation, l'invention propose un système de transaction bancaire comprenant au moins un serveur de transaction bancaire, un premier terminal d'un utilisateur relié à l'au moins un serveur de transaction bancaire via un premier canal de communication, et un deuxième terminal d'un titulaire d'un compte et/ou d'une carte bancaire relié à l'au moins un serveur de transaction bancaire via un deuxième canal de communication au moins logiquement distinct du premier canal de communication. Le premier terminal est configuré pour envoyer, sur demande de l'utilisateur, à l'au moins un serveur de transaction bancaire, une demande de

transaction comprenant au moins un montant de la transaction, et une identification du compte et/ou de la carte bancaire. Le serveur de transaction bancaire est configuré pour, à réception de la demande de transaction, établir un code de vérification dont la longueur est fonction du montant de la transaction, déterminer le deuxième terminal en fonction de l'identification du compte bancaire à débiter, puis envoyer, d'une part, une requête de confirmation demandant le code de vérification au premier terminal via le premier canal de communication et, d'autre part, le code de vérification au deuxième terminal via le deuxième canal de communication. Le deuxième terminal est configuré pour afficher, au titulaire du compte bancaire, le code de vérification envoyé par le serveur de transaction bancaire. Le premier terminal est configuré pour renvoyer au serveur de transaction bancaire un code recopié par l'utilisateur à partir du code de vérification affiché sur le deuxième terminal. Le serveur de transaction bancaire est configuré pour, à réception du code recopié, comparer avec le code de vérification avec le code recopié et envoyer au premier terminal un message de validation de transaction si les codes sont identiques ou un message d'invalidation de transaction si les codes sont différents.

Brève description des dessins

[0017] L'invention sera mieux comprise et d'autres caractéristiques et avantages de celle-ci apparaîtront à la lecture de la description suivante de modes de réalisation particuliers de l'invention, donnés à titre d'exemples illustratifs et non limitatifs, et faisant référence aux dessins annexés, parmi lesquels :

[0018] [fig.1] montre un système de transaction bancaire à deux facteurs d'authentification,

[0019] [fig.2] montre un système de transaction commerciale sur un réseau ouvert à deux facteurs d'authentification,

[0020] [fig.3] illustre une transaction sur le système de la figure 1 selon l'invention,

[0021] [fig.4] illustre une transaction sur le système de la figure 2 selon l'invention,

[0022] [fig.5] montre un organigramme de fonctionnement d'un serveur d'authentification selon l'invention,

Description détaillée

[0023] Les figures 1 et 2 montrent deux systèmes de transaction réalisée au travers d'un réseau ouvert, tel que par exemple internet, en utilisant une authentification à deux facteurs d'authentification. Sur ces deux figures, les mêmes références correspondent aux mêmes éléments ou à des éléments similaires. Ces deux figures correspondent à des schémas de transaction à deux facteurs de sécurité tel qu'utilisés dans l'état de la technique et selon l'invention.

[0024] Par « réseau ouvert », il faut comprendre un réseau de communication permettant des interconnexions entre une ou plusieurs machines informatiques accessible à tout

personne souhaitant le faire. Ce type de réseau peut être internet mais pourrait correspondre à d'autre types de réseaux dès lors que la connexion reste ouverte à tout le monde. Les réseaux ouverts ont l'avantage de faciliter une mise en relation des personnes permettant ainsi d'augmenter les possibilités de transactions commerciales entre personnes connectées audit réseau. Un inconvénient des réseaux ouverts est le risque d'interaction avec des machines appartenant à des personnes malveillantes.

[0025] La figure 1 correspond à un système de transaction bancaire permettant à un utilisateur de réaliser des opérations de transaction auprès de sa banque, tel que par exemple pour réaliser un virement bancaire ou pour réaliser un achat de titres en ligne ou tout autre type d'opération pour laquelle l'utilisateur réalise un transfert d'argent depuis son compte bancaire. Sur cette figure 1, l'utilisateur 1 interagit avec un premier terminal 2 connecté à un réseau ouvert 3, tel que par exemple internet, afin de communiquer avec un serveur de services bancaires 4 pour réaliser une opération correspondant à une transaction bancaire c'est-à-dire un transfert d'argent depuis un compte bancaire.

[0026] Le premier terminal 2 est par exemple un ordinateur personnel fixe ou portable, une tablette ou un smartphone disposant d'une unité de traitement, d'au moins une mémoire volatile et/ou non volatile, d'une interface de communication lui permettant de se connecter au réseau ouvert 3, d'une interface homme-machine permettant de visualiser et de rentrer des informations, tel que par exemple un écran de visualisation, un écran tactile, un clavier, une souris ou autre. Parmi les programmes stockés dans sa mémoire, le premier terminal dispose d'un programme de navigation sur le réseau ouvert 3, lui permettant de se connecter sur et d'interagir avec des sites web, notamment pour consulter des pages web ou pour remplir et envoyer des formulaires correspondant à des requêtes de transaction. De manière alternative, le premier terminal 2 peut disposer d'un programme spécifique lui permettant de se connecter au travers du réseau ouvert 3 au serveur de services bancaires 4.

[0027] Le serveur de services bancaires 4 est par exemple un ordinateur disposant d'une ou plusieurs unités de traitement, d'au moins une mémoire volatile et de masse, et d'au moins une interface de communication lui permettant de se connecter au réseau ouvert 3. La mémoire de masse mémorise entre autres une base de données contenant toutes les informations relatives aux comptes bancaires des clients de la banque à laquelle il appartient. Le serveur de services bancaires 4 comporte des programmes stockés en mémoire lui permettant de mettre à disposition de terminaux connectés, au travers du réseau ouvert 3, des pages web consultables qui permettent d'interagir avec des utilisateurs via des formulaires contenus dans lesdites pages web. Les formulaires, une fois remplis et renvoyés par l'utilisateur, sont ensuite traités par l'unité de traitement pour validation.

[0028] Lorsqu'une transaction est souhaitée par un utilisateur 1, celui-ci utilise le premier terminal 2 pour se connecter au serveur de services bancaires 4. Une page web est alors transmise au premier terminal 2 par le serveur de services bancaires 4. La page web peut comporter des informations à visualiser sur le premier terminal 2, ainsi que des commandes à exécuter en fonction de choix fait par l'utilisateur par l'intermédiaire de l'interface homme-machine. Parmi les choix offerts à l'utilisateur 1, une transaction, par exemple un virement bancaire, peut être réalisée. En choisissant de réaliser un virement, un formulaire de transaction est présenté à l'utilisateur 1, le formulaire pouvant être inclus dans la page web ou transmis par le serveur de services bancaires 4 après réception d'un message indiquant le choix de l'utilisateur 1 provenant du premier terminal 2. L'utilisateur 1 remplit alors le formulaire avec les informations nécessaires à la transaction qui peuvent comprendre l'identification du compte bancaire à créditer, l'identification du compte bancaire à débiter, le montant de la transaction. De nombreuses autres informations peuvent également être requises, telles que des identifiants redondants de l'utilisateur et/ou du compte bancaire ou de son titulaire, un secret connu uniquement de la banque et du titulaire, un identifiant de transaction ou toute autre information qui soit en relation avec la transaction. Une fois le formulaire rempli, l'utilisateur 1 envoie le formulaire rempli au serveur de services bancaires 4 via le premier terminal 2. Le formulaire peut être accompagné de l'heure et de la date d'envoi et également d'identifiants propres au premier terminal 2.

[0029] Ayant reçu le formulaire de transaction rempli, le serveur de services bancaires 4 vérifie les informations contenues dans le formulaire et notamment si la transaction demandée peut être autorisée ou non. A cet effet, le serveur de services bancaires 4 interroge sa base de données pour vérifier si le compte à débiter est toujours en service et si le crédit du compte à débiter peut permettre d'autoriser la transaction. Eventuellement, le serveur peut vérifier la justesse d'identifiants redondants ou d'informations sur le titulaire du compte bancaire. Cette première vérification correspond à un premier facteur de sécurité. Cependant, la transaction a été transmise par le réseau ouvert 3 et, malgré cette première vérification, il est possible que cette transaction provienne d'un détournement du formulaire et/ou des informations relatives au compte bancaire par un tiers malveillant.

[0030] En effet, les communications sur le réseau ouvert 3 peuvent être interceptées et rejouées éventuellement de manière modifiée. Afin de garantir un minimum de sécurité, il est connu d'encrypter les messages sensibles entre deux machines, tel que par exemple le terminal 2 et le serveur de services bancaires 4, à l'aide de clefs de sessions ou de clefs spécifiques. Cependant, tout message encrypté peut être décrypté au bout d'un certain temps, ce qui permet de récupérer un formulaire échangé et de réutiliser les informations qu'il contient. De plus, le fait que le réseau soit ouvert

permet à des personnes malintentionnées de diffuser des virus sur les machines qui y sont connectées et notamment le premier terminal 2. Parmi les virus, certains peuvent intercepter les informations échangées sur l'interfaces homme-machine et les renvoyer vers une autre machine rendant également inopérante la confidentialité de messages encryptés.

[0031] Afin de rajouter un niveau de sécurité, un deuxième facteur de sécurité peut être rajouté en utilisant un deuxième canal de communication pour envoyer un code à usage unique. A cet effet, le serveur de services bancaires 4 dispose d'une deuxième interface de communication apte à communiquer via le deuxième canal de communication avec un deuxième terminal 5 qui appartient à un titulaire de compte bancaire. Le deuxième terminal 5 est identifié dans la base de données du serveur de services bancaires 4 en relation avec le compte bancaire à débiter. Le deuxième terminal 5 peut être, classiquement, un téléphone mobile du titulaire du compte bancaire, mais peut également être tout autre type de dispositif connecté à un réseau de communication, tel que, par exemple, un boitier connecté à un réseau de téléphonie mobile fourni par la banque ou encore une tablette ou un ordinateur relié à internet. L'important est que le deuxième canal de communication soit au moins logiquement distinct du premier canal de communication utilisé pour l'envoi du formulaire de transaction.

[0032] Après avoir fait la première vérification, le serveur de services bancaires 4 récupère, dans sa base de données, l'identifiant du deuxième terminal 5 pour lui envoyer un code de vérification à usage unique. L'identifiant du deuxième terminal 5 est, par exemple, un numéro de téléphone mobile et le message est, par exemple, envoyé par un message court de type SMS (de l'anglais Short Message Service). Le message peut également indiquer le montant de la transaction et/ou le bénéficiaire de la transaction, de sorte que le titulaire du compte puisse vérifier que la transaction en cours est conforme à une transaction désirée.

[0033] En parallèle, le serveur de services bancaires 4 envoie au premier terminal 2 une requête de confirmation demandant le code à usage unique. L'utilisateur 1, s'il correspond au titulaire du compte bancaire, peut alors lire le code à usage unique sur le deuxième terminal 5 et le recopier dans un formulaire de réponse joint à la requête de confirmation afin de le renvoyer au serveur de services bancaires 4.

[0034] A réception du formulaire de réponse, le serveur de services bancaires 4 compare le code présent dans le formulaire avec le code à usage unique envoyé au deuxième terminal 5. Si les deux codes sont identiques, alors le serveur de services bancaires 4 valide la transaction et envoie un message au premier terminal 2 pour l'informer de l'acceptation de la transaction. Si les deux codes sont différents, alors la transaction est refusée et le serveur de services bancaires 4 envoie un message au premier terminal indiquant que la transaction est refusée. De manière optionnelle, le serveur de services

bancaires 4 peut réitérer l'envoi d'un nouveau code de vérification à usage unique au deuxième terminal 5 et d'une requête au premier terminal 2.

[0035] La figure 2 correspond à système de transaction commerciale permettant à un utilisateur 1 de réaliser un achat sur un site marchand 6. Le site marchand 6 est un ordinateur de type serveur qui est connecté au réseau ouvert 3 afin de fournir des pages web qui proposent des produits et/ou services à des utilisateurs s'y connectant à l'aide d'un terminal approprié. L'utilisateur 1 se connecte au site marchand 6 à l'aide du premier terminal 2 via le réseau ouvert 3. Une fois un choix de produits ou services réalisé par l'utilisateur 1, le site marchand 6 envoie un formulaire de transaction au premier terminal 2. Le formulaire de transaction est pré-rempli par le site marchand 6 avec l'identification du vendeur, de son compte bancaire et du montant de la transaction. Le formulaire de transaction est présenté à l'utilisateur 1 par le premier terminal 2, demandant à celui-ci de le compléter avec une identification de compte ou de carte bancaire. D'autres informations peuvent également être requises, telles que, par exemple, le fournisseur de la carte bancaire, le code CVV (de l'anglais Cardholder Verification Value) qui constitue un identifiant redondant de la carte, l'identification du titulaire de la carte bancaire ou toute autre information redondante qui soit en relation avec la carte ou son titulaire. Une fois le formulaire rempli, l'utilisateur 1 envoie le formulaire au site marchand 6 via le premier terminal 2. Le formulaire peut être accompagné de l'heure et de la date d'envoi et également d'identifiants propres au premier terminal 2 tel que, par exemple, son adresse sur le réseau ouvert 3.

[0036] Le site marchand 6 reçoit le formulaire et le transmet à un serveur de services acquéreurs 7 qui correspond à sa banque. Le serveur de services acquéreurs 7 est un ordinateur disposant d'une ou plusieurs unités de traitement, d'au moins une mémoire volatile et de masse, d'au moins une interface de communication lui permettant de se connecter avec le site marchand 6 et d'au moins une interface de communication pour se connecter à un réseau sécurisé dédié aux services bancaires. L'interface de communication communicant avec le site marchand 6 peut correspondre à une liaison spécifique sécurisée ou à un réseau ouvert mettant en œuvre une communication encryptée.

[0037] Le serveur de services acquéreurs 7 transmet ensuite le formulaire de transaction, via le réseau sécurisé, à un serveur de services débiteurs 4' qui correspond à l'émetteur de la carte bancaire. Le serveur de services débiteurs 4' est similaire au serveur de services bancaires 4. Le serveur de services débiteurs 4' peut être le serveur de la banque du titulaire de carte ou le serveur d'un organisme émetteur de carte de crédit.

[0038] A réception du formulaire de transaction, le serveur de services débiteurs 4' vérifie les informations contenues dans le formulaire et, notamment, si la transaction demandée peut être autorisée ou non. A cet effet, le serveur de services débiteurs 4'

interroge sa base de données pour vérifier si le compte ou la carte bancaire est toujours en service, si les éventuelles informations redondantes sont conformes avec la carte ou le compte bancaire et si le montant de la transaction correspond à un montant autorisé. Ce premier niveau de vérification de sécurité étant effectué, le serveur de services débiteurs 4' réalise une vérification selon un deuxième niveau de sécurité similaire à celui décrit en relation avec la figure 1 avec quelques différences.

[0039] Le serveur de services débiteurs 4' identifie dans sa base de données le deuxième terminal 5 en relation avec la carte ou le compte bancaire à débiter et un deuxième canal de communication distinct, au moins logiquement, du canal de communication avec le premier terminal 2. Le serveur de services débiteurs 4' envoie un message comportant un code de vérification à usage unique au deuxième terminal 5. Le message peut également indiquer le montant de la transaction et/ou le bénéficiaire de la transaction, de sorte que le titulaire du compte puisse vérifier que la transaction en cours est conforme à une transaction désirée.

[0040] En parallèle, le serveur de services débiteurs 4' envoie au premier terminal 2 une requête de confirmation demandant le code à usage unique. Cette requête peut être envoyer au premier terminal 2 par l'intermédiaire du serveur de services acquéreurs 7 et du site marchand 6 via le réseau ouvert 3 ou directement par le serveur de services débiteurs 4' via le réseau ouvert 3. L'utilisateur 1, s'il correspond au titulaire de la carte ou du compte bancaire peut alors lire le code à usage unique sur le deuxième terminal 5 et le recopier dans un formulaire de réponse joint à la requête de confirmation, afin de le renvoyer au serveur de services débiteurs 4' en utilisant le même canal de communication.

[0041] A réception du formulaire de réponse, le serveur de services débiteurs 4' compare le code présent dans le formulaire avec le code à usage unique envoyé au deuxième terminal 5. Si les deux codes sont identiques, alors le serveur de services bancaires 4 valide la transaction et envoie un message au serveur de services acquéreurs 7 qui enregistre la transaction et transmet un message de paiement validé au site marchand 6. Le site marchand 6 informe ensuite le premier terminal 2 que le paiement est accepté et délivre le service ou lance une procédure de livraison de produit(s) qui ne sera pas détaillée dans le présent document. Si les deux codes sont différents, alors la transaction est refusée et le serveur de services débiteurs 4' envoie un message au serveur de services acquéreurs 7 qui est retransmise au site marchand 6, puis au premier terminal 2 indiquant que la transaction est refusée et donc non réalisée. De manière optionnelle, le serveur de services débiteurs 4' peut réitérer l'envoi d'un nouveau code de vérification à usage unique au deuxième terminal 5 et d'une nouvelle requête au premier terminal 2 via l'un des chemins indiqués précédemment.

[0042] L'invention vise à améliorer les vérifications de transaction utilisant deux facteurs de

sécurité telles qu'indiquées précédemment et utilisant notamment un deuxième canal de communication avec le titulaire du compte ou de la carte bancaire. A cet effet, les figures 3 et 4 illustrent des étapes de procédés de transaction réalisés selon l'invention respectivement sur les systèmes de transaction décrit en relation avec les figures 1 et 2. L'organigramme de la figure 5 détaille des étapes du procédé de vérification de transaction effectuée selon l'invention par le serveur de services bancaires 4 ou le serveur de services débiteurs 4' au cours des échanges effectués en conformité avec la figure 3 ou la figure 4. Les étapes communes entre les figures 3, 4 et 5 portent les mêmes références et la description de la figure 5 est faite conjointement avec les descriptions des figures 3 et 4. Afin de mettre l'accent sur l'invention, les étapes préalables à un choix de transaction par l'utilisateur 1 ne sont pas détaillées sur des figures 3 et 4 qui commencent après qu'une décision de transaction, correspondant par à la réalisation d'un paiement, ait été validé par l'utilisateur 1 du premier terminal 2.

[0043] Sur la figure 3, le choix de la transaction ayant été réalisé par l'utilisateur 1, le serveur de services bancaires 4 envoie au premier terminal 2 un formulaire de transaction correspondant au choix de l'utilisateur 1 dans une première étape 301 du procédé de transaction. Dans une deuxième étape 302 du procédé de transaction, l'utilisateur 1 prend connaissance du formulaire reçu par le premier terminal 2, par exemple à l'aide d'un écran de visualisation du premier terminal 2. L'utilisateur remplit le formulaire avec les informations demandées au cours d'une troisième étape 303 du procédé de transaction, par exemple à l'aide d'un clavier du premier terminal 2. Une fois le formulaire rempli, l'utilisateur valide le formulaire pour l'envoyer.

[0044] Une quatrième étape 304 du procédé de transaction correspond à l'envoi du formulaire par le premier terminal 2 au serveur de services bancaires 4 via le réseau ouvert 3. Cette quatrième étape 304 du procédé de transaction correspond à une première étape de vérification 501 du serveur de services bancaires 4. Le serveur de services bancaires 4 reçoit un message entrant R1 arrivant par le premier canal de communication. Le message entrant R1 contient des informations d'identification ID d'un compte bancaire et d'un montant de transaction TA. Les informations d'identification ID comprennent au minimum le numéro de compte bancaire, mais peuvent comprendre des informations redondantes telles que, par exemple, un ou plusieurs éléments parmi : un mot de passe, un code PIN, une ou plusieurs informations d'identité du titulaire du compte bancaire. Les informations d'identification ID peuvent aussi comprendre des paramètres propres à la transaction, tels que par exemple l'heure, la date ou le lieu où se situe le premier terminal 2 ainsi qu'un identifiant dudit premier terminal 2.

[0045] Dans une deuxième étape de vérification 502, le serveur de services bancaires 4 vérifie que le compte bancaire existe et que celui-ci n'est pas bloqué. De manière optionnelle, d'autres vérifications peuvent être réalisées pour vérifier que d'éventuelles

informations redondantes sont bien conformes avec celles correspondant au compte bancaire. En outre, le serveur de services bancaires 4 peut également vérifier que le montant à débiter est conforme avec un débit autorisé du compte bancaire.

[0046] Cette vérification préliminaire de compte bancaire effectuée, le serveur de services bancaires 4 calcule ensuite une longueur L de code de vérification dans une troisième étape de vérification 503 où la longueur L correspond à un nombre de digits dudit code. De manière préférée, la longueur L est déterminée en fonction du montant de la transaction TA, de sorte que le code de vérification prenne en compte le montant de la transaction comme facteur de risque. A titre d'exemple simple, la formule suivante peut être utilisée :

[0047] [Math.1]

$$L = A * TA + B$$

[0048] Les paramètres A et B peuvent être fixés arbitrairement par la banque en fonction d'une acceptation de risque. Si A= 0,1 et B = 2 avec le résultat L arrondi à l'entier le plus proche, un paiement d'un euro aura pour résultat un code L de deux digits très simples à recopier pour une somme représentant un risque minime. Avec, ces mêmes paramètres un paiement de dix euros correspond à un code à trois digits et un paiement de cent euros correspond un code de douze digits.

[0049] De manière préférée, des informations d'identification ID peuvent être prises en compte dans la détermination du nombre de digit. A titre d'exemple, les paramètres A et B peuvent être mémorisés dans la base de données du serveur de services bancaires 4 et accessibles à l'aide de l'identification du numéro de compte. Ainsi, il est possible de définir les paramètres A et B en fonction d'un risque accepté par l'utilisateur ou par son gestionnaire de compte, B correspondant à un nombre de digits minimal et A étant déterminé en fonction d'un montant pour lequel un risque financier paraît acceptable. Afin d'éviter d'avoir des codes trop longs, il est également possible de fixer un nombre de digits maximal.

[0050] En variante, il est également possible d'avoir une croissance non linéaire du nombre de digits afin d'éviter d'avoir à limiter le nombre de digits. A titre d'exemple, la formule suivante peut également être utilisée :

[0051] [Math.2]

$$L = A * \log_{10}(TA) + B$$

[0052] L'utilisation d'une fonction logarithmique permet d'avoir une croissance de la longueur L du code de vérification proportionnelle au nombre de digits du montant de la transaction. A titre d'exemple, si A = 0,3 et B = 3, un montant de moins de dix euros produit une longueur de code de vérification de trois digits, un montant de cent euros correspond à une longueur de code de six digits et un montant de mille euros

correspond à une longueur de code de neuf digits.

[0053] La longueur L de code de vérification étant déterminée, le serveur de services bancaires 4 calcule ensuite un code de vérification AC lors d'une quatrième étape de vérification 504. Le code de vérification AC peut être généré de différentes manières, de préférence en utilisant un nombre aléatoire ou pseudo-aléatoire généré par l'unité de traitement du serveur de services bancaires 4. A titre d'exemple simple, la formule suivante peut être utilisée pour déterminer le code de vérification :

[0054] [Math.3]

$$AC = Seed \mod L$$

[0055] avec Seed correspondant à un nombre aléatoire ou pseudo aléatoire généré par l'unité de traitement du serveur de services bancaires 4, mod à la fonction modulo et L à la longueur de code calculée lors de la troisième étape de vérification 503. De très nombreuses variantes sont possibles en intégrant le montant de la transaction TA et une ou plusieurs informations d'identification de la transaction ID, tel que par exemple l'heure ou la date de la transaction. A titre d'exemple, la formule suivante peut également être utilisée :

[0056] [Math.4]

$$AC = H(Seed,\ TA,\ ID) \mod L$$

[0057] avec H correspondant à une fonction de hachage cryptographique, par exemple un SHA-3, réalisée sur la concaténation du nombre aléatoire Seed, du montant de la transaction TA et d'une ou plusieurs informations d'identification ID.

[0058] Le code de vérification AC étant calculé, une cinquième étape de vérification 505 est réalisée par le serveur de services bancaires 4. La cinquième étape de vérification 505 consiste à envoyer un message sortant S1, par le premier canal de communication, à destination du premier terminal 2, le message sortant contenant une requête Req demandant à l'utilisateur 1 du premier terminal 2 de renvoyer un code de vérification dans un formulaire de réponse.

[0059] En parallèle avec la cinquième étape de vérification 505, c'est-à-dire avant ou après cette cinquième étape 505, le serveur de services bancaires 4 effectue une sixième étape de vérification 506. La sixième étape de vérification 506 consiste à envoyer un message sortant S2 par le deuxième canal de communication à destination du deuxième terminal 5. Le deuxième terminal 5 est, préalablement à l'envoi, identifié dans la base de données du serveur de services bancaires 4 en association avec le compte bancaire à débiter. Le message sortant S2 contient le code de vérification AC calculé lors de la quatrième étape de vérification.

[0060] La cinquième étape de vérification 505 correspond à une cinquième étape 305 du procédé de transaction et la sixième étape de vérification 506 correspond à une sixième étape 306 du procédé de transaction.

[0061] Le premier terminal 2 ayant reçu la requête Req, celle-ci est présentée à l'utilisateur 1 au cours d'une septième étape 307 du procédé de transaction, le formulaire de réponse étant à remplir par l'utilisateur 1. Parallèlement à la septième étape 307, c'est-à-dire avant ou après cette septième étape 307, une huitième étape 308 du procédé de transaction consiste en la présentation du code de vérification AC par le deuxième terminal 5 à l'utilisateur 1.

[0062] L'utilisateur 1, disposant du code de vérification AC, remplit le formulaire de réponse en recopiant le code de vérification AC dans le formulaire au cours d'une neuvième étape 309 du procédé de transaction. Le code de vérification recopié AC' est envoyé au serveur de services bancaires 4 dans une dixième étape 310 du procédé de transaction. La dixième étape 310 du procédé de transaction correspond à une septième étape de vérification 507 réalisée par le serveur de services bancaires 4. Le serveur de services bancaires 4 reçoit un message entrant R1 arrivant du premier canal de communication ayant pour contenu le code recopié AC'. Une huitième étape de vérification 508 consiste ensuite à comparer le code recopié AC' avec le code de vérification AC calculé lors de la quatrième étape de vérification 504.

[0063] Si le code de vérification recopié AC' est identique au code de vérification AC, alors le serveur de services bancaires 4 effectue une neuvième étape de vérification 509 au cours de laquelle il valide et enregistre la réalisation de la transaction. Puis, une dixième étape de vérification 510 est réalisée pour envoyer un message sortant S1 par le premier canal de communication à destination du premier terminal 2 pour indiquer que la transaction est réalisée.

[0064] Si le code de vérification recopié AC' n'est pas identique au code de vérification AC, alors le serveur de services bancaires 4 effectue une onzième étape 511 au cours de laquelle il annule la transaction. Si, au cours de la deuxième étape de vérification 502, le serveur de services bancaires 4 n'a pas trouvé le compte bancaire ou a trouvé le compte bancaire mais que celui-ci est bloqué ou encore si d'autres vérifications ont montré que d'éventuelles informations redondantes ne sont pas conformes avec celles correspondant au compte bancaire, la deuxième étape de vérification 502 peut aboutir directement à la onzième étape de vérification 511 et également annuler la transaction. Après la onzième étape de vérification 511, une douzième étape de vérification 512 est réalisée pour envoyer en message sortant S1 par le premier canal de communication à destination du premier terminal 2 pour indiquer que la transaction est annulée.

[0065] La dixième étape de vérification 510 ou la douzième étape de vérification 512 correspond à une onzième étape 311 du procédé de transaction dans laquelle le premier terminal 2 reçoit le message sortant S1 pour l'afficher à l'utilisateur 1 au cours d'une douzième étape 312 du procédé de transaction. Ainsi, l'utilisateur 1 est informé de la réalisation ou de l'annulation de la transaction demandée.

[0066] La figure 4 divulgue un procédé de transaction réalisé à partir du site marchand 6. Après que l'utilisateur ait choisi de faire un achat, le site marchand 6 envoie au premier terminal 2 un formulaire de transaction dans une première étape 401 du procédé de transaction. Dans une deuxième étape 402 du procédé de transaction, l'utilisateur 1 prend connaissance du formulaire reçu par le premier terminal 2. L'utilisateur 1 remplit le formulaire avec les informations demandées au cours d'une troisième étape 403 du procédé de transaction. Le formulaire contient des informations d'identification ID d'une carte ou d'un compte bancaire et d'un montant de transaction TA. Les informations d'identification ID comprennent au minimum le numéro de carte ou de compte bancaire mais peuvent comprendre des informations redondantes telles que, par exemple, un ou plusieurs éléments parmi : un mot de passe, un code PIN, un code CVV, une ou plusieurs informations d'identité du titulaire du compte. Les informations d'identification ID peuvent aussi comprendre des paramètres propres à la transaction tels que, par exemple, l'heure, la date ou le lieu où se situe le premier terminal 2 ou encore un identifiant dudit premier terminal 2. Une fois le formulaire rempli, l'utilisateur 1 valide le formulaire pour l'envoyer.

[0067] Une quatrième étape 404 du procédé de transaction correspond à l'envoi du formulaire par le premier terminal 2 au site marchand 6 via le réseau ouvert 3. Le site marchand 6 retransmet le formulaire au serveur de services acquéreurs 7 au cours d'une cinquième étape 405 du procédé de transaction. A partir des informations d'identification ID de la carte ou du compte bancaire, le serveur de services acquéreurs 7 détermine un serveur de services débiteurs 4' correspondant, afin de lui retransmettre le formulaire au cours d'une sixième étape 406 du procédé de transaction.

[0068] Cette sixième étape 406 du procédé de transaction correspond à la première étape de vérification 501, réalisée par le serveur de services débiteurs 4', correspondant à la réception du message entrant R1 arrivant du premier canal de communication. Le serveur de services débiteurs 4' réalise ensuite la deuxième étape de vérification 502, afin de vérifier que le compte ou la carte bancaire existe et que celui-ci ou celle-ci n'est pas bloqué. De manière optionnelle, d'autres vérifications peuvent être réalisées pour vérifier que d'éventuelles informations redondantes sont bien conformes à celles correspondant au compte ou à la carte bancaire. En outre, le serveur de services débiteurs 4' peut également vérifier que le montant à débiter est conforme avec un débit autorisé du compte ou de la carte bancaire.

[0069] Le serveur de services débiteurs 4' réalise la troisième étape de vérification 503 et calcule une longueur L de code de vérification AC correspondant à un nombre de digits dudit code. La longueur L est déterminée en fonction du montant de la transaction TA de sorte que le code de vérification AC prenne en compte le montant de la transaction comme facteur de risque comme précédemment décrit.

[0070] De plus, la transaction étant réalisée sur un site marchand et non sur un serveur bancaire, le risque se trouve être plus important. La longueur L du code de vérification peut également intégrer d'autres facteurs de risque tels qu'une heure de transaction et/ou un nombre de transactions effectuées récemment. A titre d'exemple, une telle intégration peut se traduire par la formule suivante :

[0071] [Math.5]

$$L = A^* \ log_2(Nb)^*R(T)^*log_{10}(TA) + B$$

[0072] avec Nb représentant le nombre de transactions effectuées dans les dernières vingt-quatre heures avec le même numéro de compte ou la même carte bancaire, T représentant l'heure de la transaction et R(T) étant un coefficient de risque dépendant de l'heure T, le coefficient R(T) étant par exemple lu dans une table de correspondance réalisée à partir de statistiques sur l'heure de réalisation de transactions frauduleuses.

[0073] Le serveur de services débiteurs 4' calcule ensuite le code de vérification AC lors de la quatrième étape de vérification 504 comme précédemment décrit. Les cinquième et sixième étapes de vérification 505 et 506 sont ensuite réalisées en parallèle. La cinquième étape de vérification 505 consiste à envoyer un message sortant S1 par le premier canal de communication à destination du premier terminal 2 qui contient une requête de confirmation Req demandant à l'utilisateur 1 du premier terminal 2 de renvoyer un code de vérification dans un formulaire de réponse. La sixième étape de vérification 506 consiste à envoyer un message sortant S2 par le deuxième canal de communication, à destination du deuxième terminal 5, le deuxième terminal 5 ayant été préalablement identifié à partir de la base de données du serveur de services débiteurs 4' en association avec le compte ou la carte bancaire à débiter. Le message sortant S2 contient le code de vérification AC calculé lors de la quatrième étape de vérification 504.

[0074] La cinquième étape de vérification 505 correspond à une septième étape 407 du procédé de transaction. Au cours de la septième étape 407, le serveur de services débiteurs 4' transfère un message sortant contenant la requête S1(Req) au serveur de services acquéreurs 7. Le serveur de services acquéreurs 7 transfère ce message au site marchand 6 au cours d'une huitième étape 408 du procédé de transaction. Le site marchand 6 retransmet ensuite la requête au premier terminal 2 dans une neuvième étape 409 du procédé de transaction.

[0075] La sixième étape de vérification 506 correspond à une dixième étape 410 du procédé de transaction au cours de laquelle le deuxième terminal 5 reçoit le code de vérification AC.

[0076] Le premier terminal 2 ayant reçu la requête Req, celle-ci est présentée à l'utilisateur 1 au cours d'une onzième étape 411 du procédé de transaction, le formulaire de réponse

étant à remplir par l'utilisateur 1. Parallèlement à la onzième étape 411, une douzième étape 412 du procédé de transaction consiste en la présentation du code de vérification AC, par le deuxième terminal 5, à l'utilisateur 1.

[0077] L'utilisateur 1, disposant du code de vérification AC, remplit le formulaire de réponse en recopiant le code de vérification AC dans le formulaire de réponse au cours d'une treizième étape 413 du procédé de transaction. Le code de vérification recopié AC' est envoyé au site marchand 6 dans une quatorzième étape 414 du procédé de transaction. Au cours d'une quinzième étape 415 du procédé de transaction, le site marchand 6 retransmet le formulaire de réponse au serveur de services acquéreurs 7. Dans une seizième étape 416 du procédé de transaction, le serveur de services acquéreurs 7 transmet le formulaire rempli au serveur de services débiteurs 4'.

[0078] La seizième étape 416 du procédé de transaction correspond à la septième étape de vérification 507 réalisée par le serveur de services débiteurs 4'. Le serveur de services débiteurs 4' reçoit un message entrant R1 arrivant par le premier canal, ayant pour contenu le code recopié AC'. Au cours de la huitième étape de vérification 508, le serveur de services débiteurs 4' compare le code recopié AC' avec le code de vérification AC calculé lors de la quatrième étape de vérification 504.

[0079] Si le code de vérification recopié AC' est identique au code de vérification AC, alors le serveur de services débiteurs 4' effectue la neuvième étape 509 au cours de laquelle il valide et enregistre la réalisation de la transaction. Puis, la dixième étape de vérification 510 est réalisée pour envoyer un message sortant S1 par le premier canal de communication, à destination du premier terminal 2, pour indiquer que la transaction est réalisée.

[0080] Si le code de vérification recopié AC' n'est pas identique au code de vérification AC, alors le serveur de services débiteurs 4' effectue la onzième étape 511 au cours de laquelle il annule la transaction. Si, au cours de la deuxième étape de vérification 502, le serveur de services débiteurs 4' a constaté que le compte ou la carte bancaire est bloqué ou encore si d'autres vérifications ont montré que d'éventuelles informations redondantes ne sont pas conformes avec celles correspondant au compte ou à la carte bancaire, la deuxième étape de vérification 502 peut aboutir directement à la onzième étape de vérification 511 et également annuler la transaction. Après la onzième étape de vérification 511, une douzième étape de vérification 512 est réalisée pour envoyer un message sortant S1, par le premier canal de communication, à destination du premier terminal 2 pour indiquer que la transaction est annulée.

[0081] La dixième étape de vérification 510 ou la douzième étape de vérification 512 correspondent à une dix-septième étape 417 du procédé de transaction dans laquelle le serveur de services acquéreurs 7 reçoit le message sortant S1. Le serveur de services acquéreurs 7 enregistre la réalisation ou l'annulation de la transaction et transmet le

message sortant au site marchand 6 au cours d'une dix-huitième étape 418 du procédé de transaction. Le site marchand 6 constate la validation ou l'annulation de la transaction. Si la transaction est validée, le site marchand 6 délivre le service ou déclenche la livraison du produit acheté. Au cours d'une dix-neuvième étape 419, le site marchand 6 envoie un message de confirmation ou d'annulation de transaction au premier terminal 2. Le premier terminal 2 affiche le message de confirmation à l'utilisateur 1 au cours d'une vingtième étape 420 du procédé de transaction. Ainsi, l'utilisateur 1 est informé de la réalisation ou de l'annulation de l'achat effectué.

[0082] De nombreuses variantes de réalisation sont possibles tout en restant en conformité avec le procédé de vérification faisant l'objet de l'invention. A titre d'exemple, les septième à neuvième étapes 407 à 409 du procédé de transaction décrit en relation avec la figure 4 peuvent être remplacées par une première étape alternative 421 qui transmet directement la requête de code de confirmation du serveur de services débiteurs 4' au premier terminal 2 via le réseau ouvert 3. Egalement, une deuxième étape alternative 422 peut remplacer les quatorzième à seizième étapes 414 à 416 du procédé de transaction pour transmettre directement le code de vérification recopié AC' du premier terminal 2 au serveur de services débiteurs 4'.

[0083] Dans le présent document, le premier terminal 2 est un ordinateur connecté à internet et le deuxième terminal 5 est un téléphone mobile. Comme indiqué précédemment dans la description, les premier et deuxième terminaux 2 et 5 peuvent être n'importe quel type d'appareil connecté qui puisse échanger des données avec un serveur distant. Selon une variante, les premier et deuxième terminaux 2 et 5 peuvent être un seul et même terminal physique. L'important est que les premier et deuxième canaux de communication soient séparés au moins logiquement l'un de l'autre de sorte qu'une interception malveillante du premier canal n'entraine pas automatiquement une interception malveillante du deuxième canal.

[0084] A titre d'exemple, les premier et deuxième terminaux peuvent être un seul et même ordinateur personnel avec un premier canal de communication comprenant un logiciel de navigation sur internet et un deuxième canal de communication comprenant un logiciel de messagerie, l'identification du deuxième canal de communication se faisant à l'aide d'une adresse de courriel. Dans cet exemple, les premier et deuxième canaux de communication sont logiquement distincts l'un de l'autre, bien que la connexion physique des terminaux utilise une même interface de communication à savoir une même carte de connexion au réseau. Cependant, le code de vérification envoyé par le deuxième canal n'est pas directement accessible par le logiciel de navigation et il est nécessaire que l'utilisateur agisse sur une interface homme-machine de l'ordinateur personnel pour visualiser et recopier ledit code. Ainsi, seul un logiciel interceptant les actions réalisées sur l'interface homme-machine peut intercepter le code de véri-

fication. Or, ce type d'interception peut également être réalisé lorsque les deux canaux de communication sont physiquement distincts et par conséquent la différentiation logique constitue un même niveau de sécurité qu'une différentiation physique des canaux de communication.

[0085] En référence aux figures 2 et 4, il est décrit un serveur de services débiteurs 4' et un serveur de services acquéreurs 7. Typiquement, une transaction électronique est réalisée entre deux comptes bancaires appartenant à deux titulaires différents qui disposent de deux banques différentes ayant chacune leur serveur. Cependant, il est possible que le vendeur et l'acheteur dispose d'un compte bancaire dans une même banque. Dans ce cas, les serveurs de services débiteurs 4' et acquéreurs 7 ne forment qu'un seul et même serveur, ce qui permet de réduire le nombre d'échanges.

[0086] A l'inverse, un ou plusieurs prestataires de services intermédiaires peuvent également être interposés entre les serveurs de services débiteurs 4' et acquéreurs 7. C'est notamment le cas lorsque des cartes de crédit sont utilisées. La liaison n'est pas faite directement de banque à banque, mais passe par un fournisseur de cartes qui peut se substituer à la banque du titulaire de carte ou simplement servir de relais intermédiaire lors d'une transaction en ligne.

[0087] De même, les serveurs de services bancaires 4, débiteurs 4' et acquéreurs 7 peuvent être des serveurs distribués. Vu le volume de données bancaire et le nombre de requêtes de transaction, plusieurs ordinateurs indépendants et reliés en réseau peuvent assurer le rôle de chacun des serveurs de services bancaires 4, débiteurs 4' et acquéreurs 7. Chaque ordinateur constituant l'un des serveurs peut effectuer la totalité des opérations d'une transaction ou seulement une partie, les différentes opérations de transaction étant réalisée sur différents ordinateurs.

Revendications

[Revendication 1] Procédé d'authentification de transaction utilisant deux canaux de communication de données pour un utilisateur (1) utilisant un premier terminal (2) relié à au moins un serveur de transaction bancaire (4, 4') via un premier canal de communication et un deuxième terminal (5) relié à l'au moins un serveur de transaction bancaire (4, 4') via un deuxième canal de communication au moins logiquement distinct du premier canal de communication, caractérisé en ce que le procédé comporte :

- une première étape (304, 404, 405, 406, 501) au cours de laquelle le premier terminal (2) envoie à l'au moins un serveur de transaction bancaire (4, 4') des informations de transaction comprenant au moins un montant de la transaction (TA), et une identification (ID) d'un compte et/ou d'une carte bancaire à débiter,
- une deuxième étape (502 à 506) au cours de laquelle le serveur de transaction bancaire (4, 4') établit un code de vérification (AC) dont une longueur (L) est fonction du montant de la transaction (TA), détermine le deuxième terminal en fonction de l'identification (ID) du compte et/ou de la carte bancaire à débiter, puis envoie, d'une part, une requête de confirmation (505) demandant le code de vérification au premier terminal (2) via le premier canal de communication et, d'autre part, le code de vérification (506) au deuxième terminal (5) via le deuxième canal de communication,
- une troisième étape (307, 308, 309, 411, 412, 413) au cours de laquelle l'utilisateur (1) copie le code de vérification (AC) reçu sur le deuxième terminal (5) dans la requête de confirmation reçue par le premier terminal (2) et renvoie (309, 413) ladite requête ainsi remplie avec le code recopié (AC') au serveur de transaction bancaire (4, 4') à l'aide du premier terminal (2) via le premier canal de communication,
- une quatrième étape (507 à 512) au cours de laquelle le serveur de transaction bancaire (4, 4') reçoit (507) du premier terminal (2) le code recopié (AC'), et compare (508) le code de vérification (AC) avec le code recopié (AC') et envoie (510, 512) au premier terminal (2) un message de validation de transaction si les codes sont identiques ou un message d'invalidation de transaction si les codes sont différents.

[Revendication 2] Procédé selon la revendication précédente, dans lequel les informations de transaction comprennent en outre des informations d'identification

du titulaire du compte et au moins une information redondante liée à l'identification du compte bancaire à débiter, dans laquelle, la deuxième étape (502 à 506) comporte une étape préliminaire (502) qui vérifie une concordance entre l'identification du compte bancaire à débiter, les informations d'identification du titulaire et la au moins une information redondante et dans laquelle la deuxième étape n'est réalisée que si la concordance est établie.

[Revendication 3] Procédé selon l'une des revendications précédentes dans lequel la longueur (L) du code de vérification (AC) dépend en outre d'un facteur de risque déterminé à l'aide d'un ou plusieurs paramètres compris parmi : l'heure de la transaction, la date de la transaction, des informations relatives au titulaire de la carte, le nombre de transactions effectuées dans une période prédéterminée précédant la transaction.

[Revendication 4] Procédé selon l'une des revendications précédentes dans lequel la longueur (L) du code de vérification (AC) croît lorsque le montant (TA) de la transaction croît.

[Revendication 5] Procédé selon l'une des revendications précédentes dans lequel la longueur (L) du code de vérification (AC) est comprise entre une valeur minimale et une valeur maximale.

[Revendication 6] Serveur de transaction bancaire (4, 4') comprenant une unité de traitement, une mémoire de programmes, au moins une interface de communication apte à communiquer via un premier canal de communication et via un deuxième canal de communication au moins logiquement distinct du premier canal de communication caractérisé en que la mémoire de programme comporte des instructions coopérant avec l'unité de traitement de sorte que le serveur soit configurer pour :
- à réception (501) depuis le premier canal de communication d'une demande de transaction comprenant au moins un montant de la transaction (TA) et une identification (ID) d'un compte bancaire à débiter, calculer (503) une longueur (L) d'un code de vérification (AC) en fonction du montant de la transaction (TA), déterminer le code de vérification (AC) à partir de la longueur (L) de code calculée, déterminer un deuxième canal de communication en fonction de l'identification (ID) du compte bancaire à débiter, envoyer (505) une requête (Req) de confirmation demandant le code de vérification via le premier canal de communication, et envoyer (506) le code de vérification (AC) via le deuxième canal de communication,
- à réception (507) d'un code reçu (AC') via le premier canal de com-

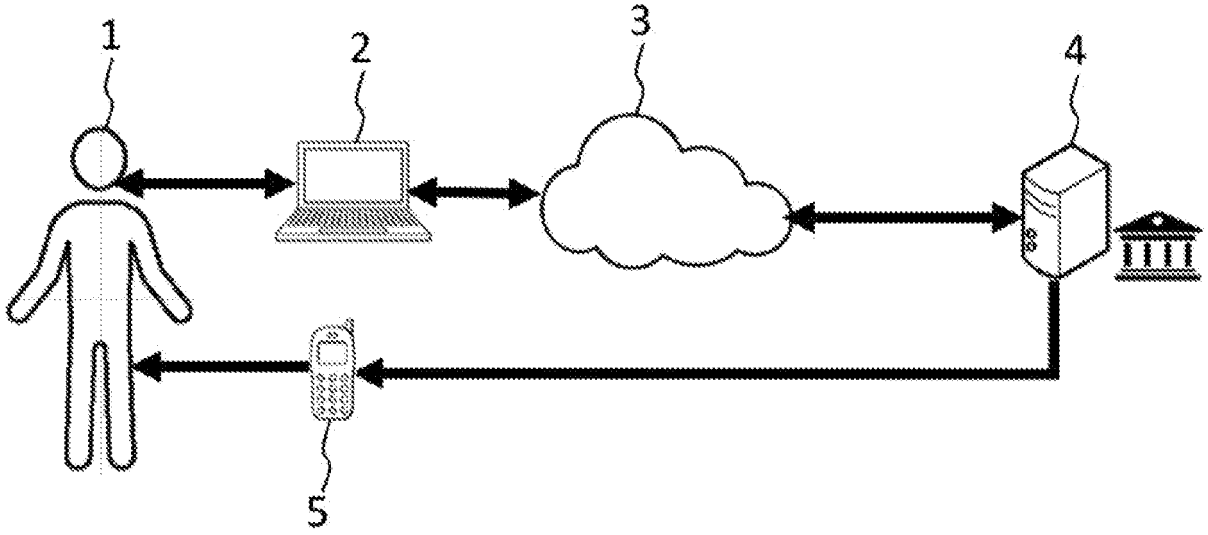
munication en réponse à la requête de confirmation, comparer ledit code reçu (AC') avec le code de vérification (AC) et envoyer via le premier canal de communication un message de validation (510) de transaction si lesdits codes sont identiques ou un message d'invalidation (512) de transaction si lesdits codes sont différents.

[Revendication 7] Système de transaction bancaire comprenant au moins un serveur de transaction bancaire (4, 4'), un premier terminal (2) d'un utilisateur (1) relié à l'au moins un serveur de transaction bancaire (4,4') via un premier canal de communication, et un deuxième terminal (5) d'un titulaire d'un compte et/ou d'une carte bancaire relié à l'au moins un serveur de transaction bancaire (4, 4') via un deuxième canal de communication au moins logiquement distinct du premier canal de communication caractérisé en ce que :

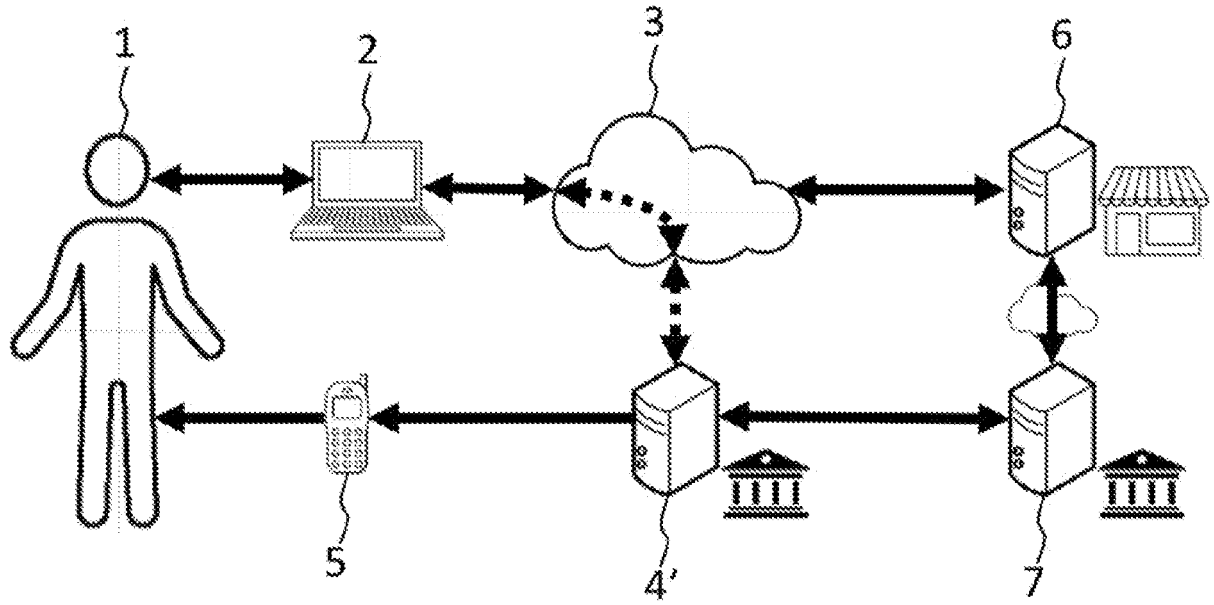
- le premier terminal (2) est configuré pour envoyer (304, 404, 405, 406), sur demande de l'utilisateur (1), à l'au moins un serveur de transaction bancaire (4, 4'), une demande de transaction comprenant au moins un montant de la transaction (TA), et une identification (ID) du compte et/ou de la carte bancaire,
- le serveur de transaction bancaire (4, 4') est configuré pour, à réception (501) de la demande de transaction, établir (503, 504) un code de vérification (AC) dont la longueur (L) est fonction du montant de la transaction (TA), déterminer le deuxième terminal (5) en fonction de l'identification du compte bancaire à débiter, puis envoyer, d'une part, une requête (505) de confirmation demandant le code de vérification au premier terminal (2) via le premier canal de communication et, d'autre part, le code de vérification (506) au deuxième terminal (5) via le deuxième canal de communication
- le deuxième terminal (5) est configuré pour afficher, au titulaire (1) du compte bancaire, le code de vérification envoyé par le serveur de transaction bancaire (4, 4'),
- le premier terminal (2) est configuré pour renvoyer (309, 413) au serveur de transaction bancaire (4, 4') un code recopié (AC') par l'utilisateur (1) à partir du code de vérification (AC) affiché sur le deuxième terminal (5),
- le serveur de transaction bancaire (4, 4') est configuré pour, à réception (507) du code recopié (AC'), comparer (508) avec le code de vérification (AC) avec le code recopié (AC') et envoyer au premier terminal un message de validation (510) de transaction si les codes sont

identiques ou un message d'invalidation (512) de transaction si les codes sont différents.

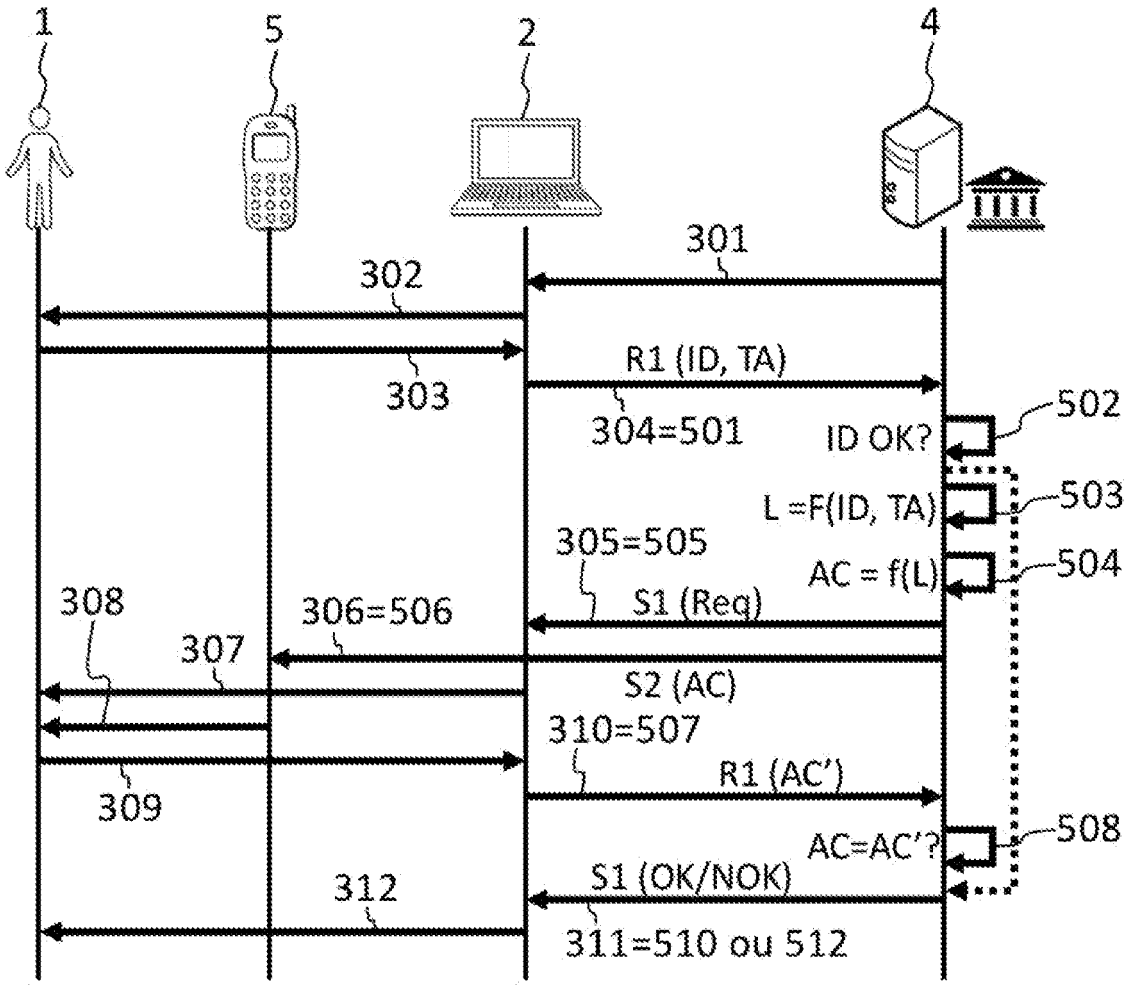
[Fig. 1]



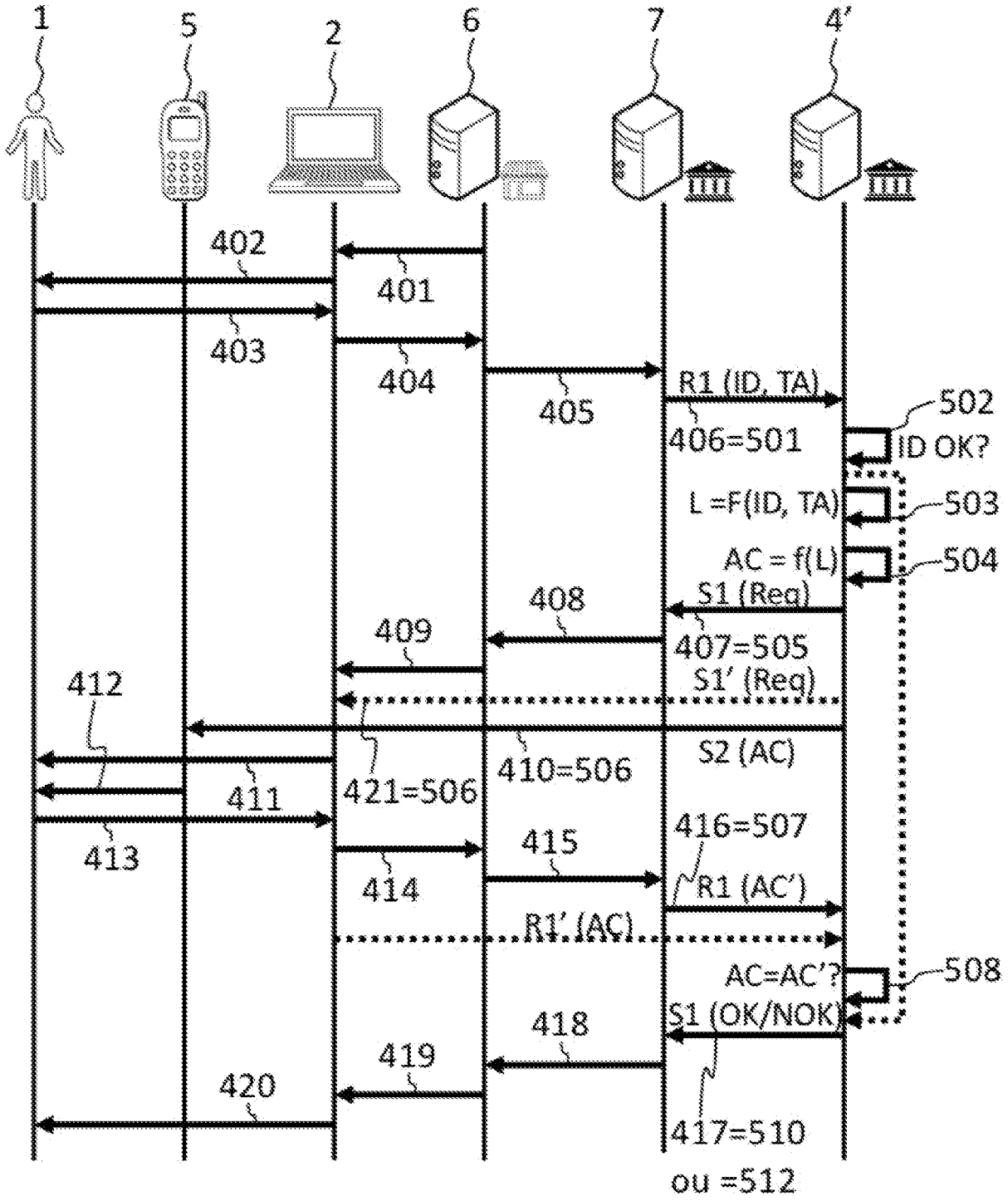
[Fig. 2]



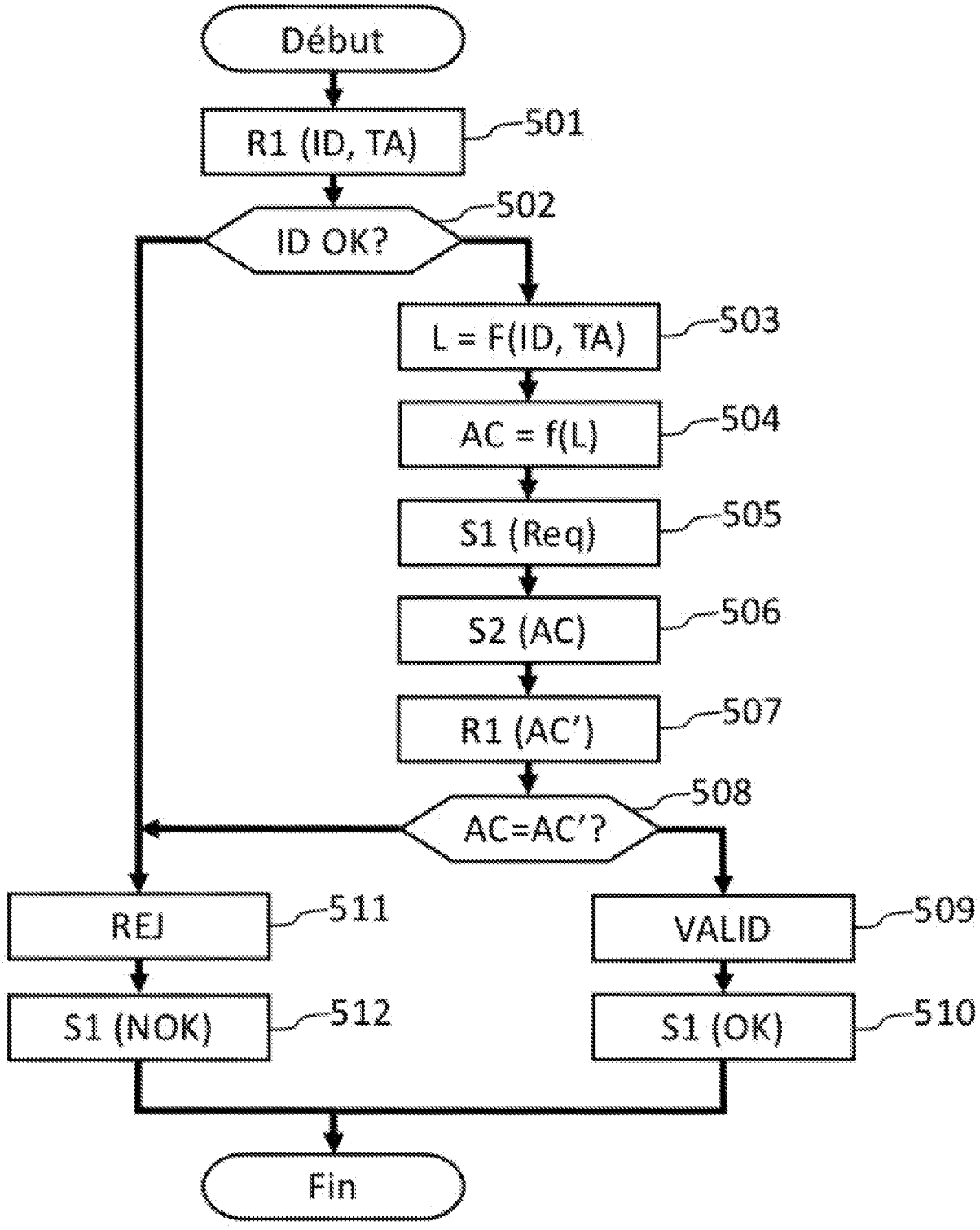
[Fig. 3]


1
5
2
4
301
302
303
R1 (ID, TA)
304=501
ID OK?
502
L =F(ID, TA)
503
305=505
AC = f(L)
504
S1 (Req)
306=506
308
307
S2 (AC)
310=507
309
R1 (AC')
AC=AC'?
508
312
S1 (OK/NOK)
311=510 ou 512

[Fig. 4]


1
5
2
6
7
4'
402
401
403
404
405
R1 (ID, TA)
406=501
502
ID OK?
L =F(ID, TA)
503
AC = f(L)
504
S1 (Req)
408
409
407=505
S1' (Req)
412
S2 (AC)
410=506
411
421=506
413
416=507
415
414
R1 (AC')
R1' (AC)
AC=AC'?
508
S1 (OK/NOK)
418
419
420
417=510
ou =512

[Fig. 5]


Début
R1 (ID, TA)
501
ID OK?
502
L = F(ID, TA)
503
AC = f(L)
504
S1 (Req)
505
S2 (AC)
506
R1 (AC')
507
AC=AC'?
508
REJ
511
VALID
509
S1 (NOK)
512
S1 (OK)
510
Fin

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 877379
FR 1914346

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	WO 02/091144 A1 (DZAMKO ROMAN [SK]; VACLAVIK MAREK [SK]) 14 novembre 2002 (2002-11-14) * Exemple 1 de la page 11 à la page 13 * * 2ème et 3ème alinéas à la page 10 *	1-7	G06F21/34 G06Q20/40 H04L9/32 H04L9/08
A	US 2011/099377 A1 (HOORNAERT FRANK [BE] ET AL) 28 avril 2011 (2011-04-28) * alinéas [0002], [0005], [0017] * * alinéa [0037] *	1-7	
A	US 2007/175978 A1 (STAMBAUGH ROD [US]) 2 août 2007 (2007-08-02) * alinéas [0018], [0051], [0052], [0058] *	1-7	
A	US 2015/188913 A1 (TEIXERON GUILLAUME [FR] ET AL) 2 juillet 2015 (2015-07-02) * alinéa [0041] *	1-7	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04L H04W G06F G06Q

Date d'achèvement de la recherche	Examinateur
26 août 2020	Kufer, Léna

CATÉGORIE DES DOCUMENTS CITÉS

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

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

.....

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1914346 FA 877379

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 26-08-2020
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 02091144 A1	14-11-2002	SK 5232001 A3	05-03-2002
		WO 02091144 A1	14-11-2002
US 2011099377 A1	28-04-2011	BR PI1003217 A2	23-10-2012
		CN 102696212 A	26-09-2012
		EP 2491696 A1	29-08-2012
		US 2011099377 A1	28-04-2011
		US 2014237242 A1	21-08-2014
		WO 2011050321 A1	28-04-2011
US 2007175978 A1	02-08-2007	EP 2122557 A2	25-11-2009
		US 2007175978 A1	02-08-2007
		WO 2008089383 A2	24-07-2008
US 2015188913 A1	02-07-2015	CN 106462706 A	22-02-2017
		EP 3090377 A1	09-11-2016
		JP 6702874 B2	03-06-2020
		JP 2017507552 A	16-03-2017
		US 2015188913 A1	02-07-2015
		US 2018316661 A1	01-11-2018
		WO 2015103302 A1	09-07-2015

EPO FORM P0465