(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
25 novembre 2010 (25.11.2010)

PCT

(10) Numéro de publication internationale
WO 2010/133783 A1

(51) Classification internationale des brevets :
H04L 29/06 (2006.01) *H04L 12/58* (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2010/050828

(22) Date de dépôt international :
30 avril 2010 (30.04.2010)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0953403 20 mai 2009 (20.05.2009) FR

(71) Déposant *(pour tous les États désignés sauf US)* :
FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* :
BATTISTELLO, Patrick [FR/FR]; 35, rue Toul Al Lann, F-22700 Perros Guirec (FR).

(74) Mandataire : **FRANCE TELECOM R&D/PIV/BREVETS**; MUSTAKI Daniel, 38-40, rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (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, SE, SI, SK, SM,

[Suite sur la page suivante]

(54) Title : METHOD FOR PROTECTING AGAINST UNWANTED MESSAGES IN A TELECOMMUNICATION NETWORK

(54) Titre : PROCÉDÉ DE PROTECTION CONTRE LES MESSAGES INDÉSIRABLES DANS UN RÉSEAU DE TÉLÉCOMMUNICATIONS

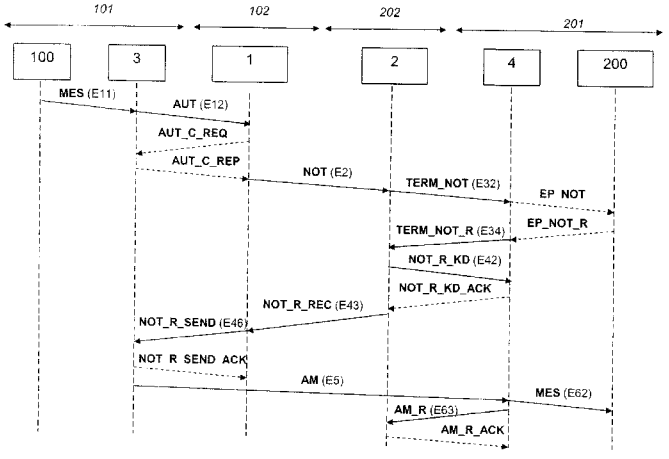


FIG. 2

(57) Abstract : When a sender client affiliated with a sender domain and connected to a transmitting server sends an original message (MES) to at least one destination client affiliated with a destination domain and connected to a receiving server: a) a sender server belonging to the sender domain acknowledges that a transaction associated with the sender client and the destination client has been initiated; b) if the sender server decides to authorize said transaction, it sends or makes the transmitter server send a notification request to a destination server belonging to the destination domain, the notification request including elements containing an identifier of the destination client; c) if the destination sever decides to authorize the transaction, it randomly generates a mark (K_REC) and sends a transaction decision containing said mark (K_REC) to the sender server; d) the sender server and the destination server separately calculate a same token (KD) resulting from the application of a predetermined encrypting algorithm to a data set contingent upon at least the mark (K_REC) using an encryption key shared by the sender server and the destination server; e) the sender server sends or makes the transmitting server send an authenticated message (AM) including the original message (MES) and the token (KD) or a value derived from

[Suite sur la page suivante]

WO 2010/133783 A1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

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

the token (KD) to the destination server (2) or to the receiving server (4); and f) if the destination server or the receiving server decides to authorize the transaction on the basis of at least the value of the token (KD) or a value derived from the token (KD) received in the authenticated message (AM), the destination client accepts the original message (MES).

(57) Abrégé : Lorsqu'un client expéditeur rattaché à un domaine expéditeur et connecté à un serveur émetteur envoie un "message original" (MES) à destination d'au moins un client destinataire rattaché à un domaine destinataire et connecté à un serveur récepteur : a) un serveur expéditeur appartenant au domaine expéditeur prend acte qu'une transaction associée à ce client expéditeur et à ce client destinataire a été initiée; b) si le serveur expéditeur décide d'autoriser ladite transaction, il envoie, ou fait envoyer par le serveur émetteur, une requête de notification à un serveur destinataire appartenant au domaine destinataire, ladite requête de notification comprenant des éléments incluant un identifiant du client destinataire; c) si le serveur destinataire décide d'autoriser la transaction, il engendre aléatoirement un témoin (K_REC), et envoie au serveur expéditeur une décision de transaction comprenant ce témoin (K_REC); d) le serveur expéditeur et le serveur destinataire calculent indépendamment un même jeton (KD), qui résulte de l'application d'un algorithme de chiffrement prédéterminé à un ensemble de données dépendant au moins du témoin (K_REC), en utilisant une clé de chiffrement partagée entre le serveur expéditeur et le serveur destinataire; e) le serveur expéditeur envoie, ou fait envoyer par ledit serveur émetteur, au serveur destinataire (2) ou au serveur récepteur (4) un "message authentifié" (AM) comprenant le message original (MES), et le jeton (KD) ou une valeur dérivée du jeton (KD); et f) si le serveur destinataire ou le serveur récepteur décide, au moins sur la base de la valeur du jeton (KD) ou de la valeur dérivée du jeton (KD) reçue dans ledit message authentifié (AM), d'autoriser la transaction, le client destinataire accepte le message original (MES).

PROCEDE DE PROTECTION CONTRE LES MESSAGES INDESIRABLES DANS UN RESEAU DE TELECOMMUNICATIONS

La présente invention concerne la protection contre la réception de messages indésirables dans un réseau de télécommunications.

Les réseaux de télécommunications, comme l'Internet, transmettent des données via une infrastructure commune entre différentes entités de service, telles qu'un serveur web ou un serveur de messagerie électronique. Ces réseaux subissent des attaques à destination de cibles professionnelles, administratives ou individuelles. Une attaque courante de nos jours consiste à envoyer vers le plus grand nombre de destinataires possible des messages indésirables qu'ils n'ont pas sollicités, tels que des "Spam" pour des courriers électroniques ou des "Spit" pour des appels téléphoniques sur Internet. Le qualificatif "indésirable" est pris au sens large et s'applique à la fois à l'identité de l'expéditeur du message, qui peut être authentique ou falsifiée, et au contenu du message.

Par exemple, la possibilité d'attaques du type Spam repose sur les facteurs suivants :

- la faiblesse des protocoles utilisés sur Internet, tels que le protocole SMTP ("*Simple Mail Transfer Protocol*" en anglais) le plus utilisé pour le transfert de courrier électronique et qui n'incorpore notamment pas de fonctions d'authentification de l'émetteur d'un courrier ;
- l'augmentation de la puissance des ordinateurs qui peuvent envoyer des messages indésirables en masse de façon automatique sur une période très courte ; et
- l'augmentation du nombre de réseaux ayant accès à Internet et de la connectivité entre ces réseaux, ce qui présente un très grand nombre de cibles à des attaquants qui peuvent s'abriter derrière des réseaux

relativement permissifs ou hors de portée légale ou administrative des réseaux cibles.

Par ailleurs, un domaine émetteur peut relayer vers un domaine destinataire un message émis par un client expéditeur qui est connecté au domaine émetteur mais qui n'est pas rattaché au domaine émetteur (dans le cadre de la présente invention, on dira qu'un client est "rattaché" à un domaine réseau lorsque ce client possède un lien de service et/ou logique et/ou administratif avec ce domaine ; dans le cas du courrier électronique, l'adresse logique correspond à l'adresse "email"). Par exemple, un client expéditeur itinérant connecté à un domaine émetteur "émetteur.fr" envoie un courrier électronique dont l'adresse d'origine est user@expéditeur.fr et dont l'adresse de destination est user2@destinataire.fr.

Or, il n'est pas aisé, pour le domaine émetteur, de déterminer si l'adresse du client expéditeur est valide, c'est-à-dire si l'adresse de ce client est effectivement attribuée dans le domaine "expéditeur.fr" et si le client expéditeur dispose des droits pour envoyer un message depuis cette adresse : en effet, le domaine émetteur ne gère pas les identités, c'est-à-dire les adresses logiques du type "expéditeur.fr". Cette difficulté de contrôle est souvent utilisée par des attaquants pour émettre des messages sous une fausse identité depuis un domaine auquel les attaquants ont accès ou bien via une machine corrompue dans un domaine légitime.

Une solution à cette difficulté de contrôle consiste à bloquer dans le domaine émetteur l'envoi de tout message dont l'adresse d'origine n'est pas rattachée au domaine émetteur, mais cette solution est trop limitative, notamment pour la mobilité des services de "voix sur IP" VoIP ("*Voice over Internet Protocol*" en anglais) qui permettent à un terminal itinérant d'utiliser un relais tiers tel qu'un domaine émetteur pour établir un appel téléphonique.

Cela pose le problème de trouver des moyens permettant à un domaine destinataire de s'assurer que des contrôles suffisants sont réalisés au niveau du domaine émetteur du message.

On peut évidemment, en principe, authentifier des messages au moyen d'une infrastructure à clé publique PKI ("*Public Key Infrastructure*" en anglais). Mais comme il est bien connu, les infrastructures PKI sont très lourdes à mettre en place et à utiliser.

La demande internationale FR2007/052057 divulgue un procédé pour protéger un domaine destinataire donné, et les clients qui lui sont rattachés, contre les messages indésirables. Ce procédé permet de contrôler l'envoi d'un "message original" vers ce domaine destinataire par un client expéditeur rattaché à un domaine expéditeur et connecté à un domaine émetteur (le domaine émetteur pouvant ou non être distinct du domaine expéditeur). Par "message original", on entend ici un ensemble quelconque d'informations, par exemple un courrier électronique ou une demande d'initiation d'appel VoIP ou encore un "message instantané".

On définit une "transaction" comme étant l'ensemble des échanges protocolaires permettant d'envoyer un message original de façon sécurisée. A chaque nouveau message original envoyé depuis un domaine expéditeur vers un domaine destinataire correspond une nouvelle transaction. A l'inverse, la répétition d'une étape protocolaire, par exemple du fait d'un problème réseau, n'est pas considérée comme une nouvelle transaction.

Selon la demande internationale FR2007/052057, chaque transaction comprend schématiquement les étapes suivantes : si le domaine expéditeur, après authentification du client expéditeur, accepte la transaction, le domaine émetteur envoie au domaine destinataire une requête contenant notamment l'adresse logique du client expéditeur ; si le client destinataire accepte de recevoir le message original, alors le domaine destinataire engendre un témoin, qu'il envoie au domaine

émetteur ; le domaine émetteur envoie au domaine destinataire un message authentifié contenant le message original et, pour vérification, ledit témoin ; si la vérification est positive, le message original est finalement transmis au client destinataire.

Ce procédé impose ainsi une responsabilisation, d'une part, du domaine expéditeur qui doit authentifier l'expéditeur du message, et d'autre part du domaine émetteur qui intervient dans le contrôle des messages qu'il émet, de façon à faire porter une partie de la charge des contrôles au domaine expéditeur et au domaine émetteur plutôt que de la laisser entièrement au domaine destinataire.

Ce procédé, qui ne requiert notamment aucune procédure cryptographique lourde, est avantageusement simple à mettre en œuvre. Par ailleurs, il est indépendant de l'architecture du réseau de communications concerné. Il est en particulier compatible avec les protocoles courants d'envoi de messages, tels que le protocole "SMTP" pour les applications de courrier électronique. De plus, la vérification de l'origine du message peut être avantageusement faite par le domaine destinataire quel que soit le nombre de serveurs relais qui ont retransmis le message vers le domaine destinataire.

Toutefois, le procédé selon la demande FR2007/052057 est vulnérable à l'attaque suivante. Un "pirate" pourrait écouter l'autorisation de transaction envoyée par le domaine destinataire au domaine émetteur, y lire la valeur dudit témoin, et, en usurpant une adresse réseau dans le domaine émetteur, envoyer au domaine destinataire un message original illicite accompagné du témoin ainsi frauduleusement acquis. Le domaine destinataire est trompé car la valeur du témoin est correcte ; il va alors transmettre ce message original illicite au client destinataire.

La présente invention concerne donc un procédé de protection contre les messages indésirables dans un réseau de télécommunications, comprenant, lorsqu'un client expéditeur rattaché à un domaine dit

domaine expéditeur et connecté à un dispositif, dit serveur émetteur, envoie un message, dit message original MES, à destination d'au moins un client destinataire rattaché à un domaine dit domaine destinataire et connecté à un dispositif, dit serveur récepteur, les étapes suivantes :

a) un dispositif, dit serveur expéditeur, appartenant audit domaine expéditeur prend acte qu'une transaction associée audit client expéditeur et audit client destinataire a été initiée,

b) si ledit serveur expéditeur décide d'autoriser ladite transaction, il envoie, ou fait envoyer par ledit serveur émetteur, une requête de notification à un dispositif, dit serveur destinataire, appartenant audit domaine destinataire, ladite requête de notification comprenant des éléments incluant un identifiant du client destinataire, et

c) si ledit serveur destinataire décide d'autoriser la transaction, il engendre aléatoirement un témoin K_REC, et envoie au serveur expéditeur une décision de transaction comprenant ledit témoin K_REC.

Ledit procédé est remarquable en ce qu'il comprend en outre les étapes suivantes :

d) le serveur expéditeur et le serveur destinataire calculent indépendamment un même jeton KD, qui résulte de l'application d'un algorithme de chiffrement prédéterminé à un ensemble de données dépendant au moins dudit témoin K_REC, en utilisant une clé de chiffrement TID_N partagée entre le serveur expéditeur et le serveur destinataire,

e) le serveur expéditeur envoie, ou fait envoyer par ledit serveur émetteur, au serveur destinataire ou audit serveur récepteur un message authentifié AM comprenant ledit message original MES, et le jeton KD ou une valeur dérivée du jeton KD, et

f) si le serveur destinataire ou le serveur récepteur décide, au moins sur la base de la valeur du jeton KD ou de la valeur dérivée du jeton

KD reçue dans ledit message authentifié AM, d'autoriser la transaction, le client destinataire accepte le message original MES.

On notera que, dans le cadre de la présente invention, le mot "serveur" dans les expressions "serveur expéditeur", "serveur destinataire", "serveur émetteur" et "serveur récepteur" est, pour simplifier l'exposé, utilisée pour désigner uniformément tout type de dispositif informatique, et non uniquement les dispositifs informatiques classiquement désignés sous le nom de "serveurs".

Grâce à l'invention, on peut bénéficier des avantages du procédé selon la demande FR2007/052057, tout en se protégeant contre le type d'attaques mentionné ci-dessus. En effet, lorsque l'on met en œuvre la présente invention, si un pirate "écoutait" la décision de transaction envoyée par le serveur destinataire au serveur expéditeur, il pourrait éventuellement, de manière similaire au cas du procédé selon la demande FR2007/052057, y lire la valeur du témoin K_REC. Mais le pirate ne peut alors calculer le jeton KD correspondant à ce témoin K_REC, car le pirate ne connaît pas la clé de chiffrement TID_N. Le pirate se trouve donc dans l'impossibilité de tromper le serveur récepteur en lui envoyant un message illicite MES' accompagné du jeton KD (ou d'une valeur dérivée du jeton KD).

De préférence, la décision de la part du serveur expéditeur, entre les étapes a) et b) mentionnées ci-dessus, d'autoriser ou non la transaction est au moins fondée sur une évaluation de l'authenticité du client expéditeur ; le domaine expéditeur pourra, pour ce faire, mettre en œuvre tout procédé d'authentification connu.

On impose ainsi une responsabilisation du domaine expéditeur afin de diminuer les risques de réception d'un message indésirable par le client destinataire.

De préférence également :

- lesdits éléments de la requête de notification incluent en outre un identifiant du client expéditeur, et

- ladite décision de la part dudit serveur destinataire, entre les étapes b) et c) ci-dessus, d'autoriser ou non la transaction est au moins fondée sur une évaluation du souhait de la part du client destinataire de recevoir ledit message original MES ; le client destinataire pourra, pour ce faire, signifier soit de façon explicite, soit de façon implicite (utilisation de listes "blanches" et/ou "noires"), s'il souhaite ou non recevoir un message en provenance de ce client expéditeur.

On diminue ainsi encore plus les risques de réception de messages indésirables par le client destinataire.

Selon des caractéristiques particulières, ladite requête de notification est protégée en intégrité.

On notera que cette protection peut être réalisée par tout moyen connu, par exemple au moyen d'un "code d'authentification de message". On rappelle à cet égard que, de manière classique, un code d'authentification de message (en anglais "*Message Authentication Code*", ou "MAC") est un chiffré des données contenues dans un message, le chiffrement s'effectuant au moyen d'une clé secrète partagée entre l'émetteur et le récepteur du message. En envoyant un message accompagné de son code d'authentification, l'émetteur permet au récepteur de vérifier que ces données n'ont pas été altérées entre leur émission et leur réception.

Grâce à ces dispositions, on peut, en premier lieu, authentifier le serveur expéditeur auprès du serveur destinataire afin de permettre au serveur destinataire de rejeter les communications provenant d'une source non autorisée ; en particulier, on protège ainsi le serveur destinataire contre une attaque par inondation. En second lieu, on protège ainsi les éléments de la requête de notification contre toute altération ; or une telle altération ferait échouer la transaction dans la plupart des cas.

Selon d'autres caractéristiques particulières, lesdits éléments de la requête de notification incluent en outre une valeur h(MES) obtenue en appliquant une fonction à sens unique "h" à tout ou partie dudit message original MES.

Grâce à ces dispositions, le serveur récepteur pourra, après avoir reçu communication de cette valeur h(MES), vérifier, entre les étapes e) et f) mentionnées ci-dessus, que cette valeur est bien égale à la valeur qu'il obtient en appliquant la fonction "h" au message original MES contenu dans le message authentifié AM. On peut ainsi faire obstacle à un pirate qui aurait non seulement les moyens d'écouter les communications selon l'invention, mais également les moyens d'intercepter certaines de ces communications pour y remplacer le contenu par un contenu illicite (attaques du type "MITM", initiales des mots anglais "*Man In the Middle*" signifiant "individu inséré"). En effet, un tel pirate pourrait, en l'absence de telles dispositions, tromper le serveur récepteur en interceptant un message authentifié licite, en y substituant le message original MES par un "message original" illicite MES' sans modifier le jeton KD (ou la valeur dérivée du jeton KD), et en envoyant au serveur récepteur le "message authentifié" illicite ainsi constitué.

Selon encore d'autres caractéristiques particulières, le serveur émetteur et le serveur expéditeur sont distincts, et

- le serveur émetteur envoie au serveur expéditeur, avant l'étape a) mentionnée ci-dessus, une requête d'authentification comprenant au moins un identifiant du ou des client(s) destinataire(s), et
- le serveur expéditeur envoie au serveur émetteur, entre les étapes d) et e) mentionnées ci-dessus, une notification d'éléments comprenant ledit jeton KD.

Grâce à ces dispositions, on peut avantageusement appliquer l'invention à un client expéditeur en situation de mobilité par rapport à son domaine de rattachement. De préférence, ladite requête d'authentification

comprend en outre un identifiant du client expéditeur, afin de permettre ultérieurement au client destinataire de signifier s'il souhaite ou non recevoir un message en provenance de ce client expéditeur.

Selon des caractéristiques encore plus particulières, ladite requête d'authentification comprend en outre ladite valeur h(MES).

Grâce à ces dispositions, on peut compléter, dans le cas visé, les dispositions, exposées succinctement ci-dessus, consistant à inclure la valeur h(MES) dans ladite requête de notification.

Selon d'autres caractéristiques encore plus particulières, les communications entre le serveur émetteur et le serveur expéditeur, supposés distincts, sont protégées en intégrité.

Grâce à ces dispositions, on peut se protéger contre une attaque par déni de service dans laquelle un pirate changerait la valeur du jeton KD dans ladite notification d'éléments, de sorte que le serveur récepteur, recevant de la part du serveur émetteur une valeur du jeton KD (ou de la valeur dérivée du jeton KD) qui ne concorde pas avec la valeur du jeton KD calculée par le serveur destinataire à l'étape d) mentionnée ci-dessus, refuserait la transaction.

De plus, dans le cas où, comme succinctement exposé ci-dessus, on inclut la valeur h(MES) dans la requête de notification, ces dispositions permettent de faire obstacle à une attaque du type MITM dans laquelle un pirate :

- intercepterait une requête d'authentification envoyée par le serveur émetteur au serveur expéditeur, y substituerait h(MES) par h(MES'), où MES' désigne un message illicite, puis enverrait une requête d'authentification illicite au serveur expéditeur, puis
- intercepterait le message authentifié AM comprenant le message original MES avant qu'il ne parvienne au serveur récepteur, y substituerait MES par MES' sans modifier le jeton KD (ou la valeur

dérivée du jeton KD), et enverrait au serveur récepteur le "message authentifié" illicite ainsi constitué.

Selon encore d'autres caractéristiques particulières, ladite décision de transaction est protégée en intégrité.

Grâce à ces dispositions, on peut, en premier lieu, authentifier le serveur destinataire auprès du serveur expéditeur. En second lieu, on protège ainsi les données contenues dans la décision de transaction contre toute altération ; il est clair, en particulier, que l'altération de la valeur du témoin K_REC entraînerait le calcul d'une fausse valeur pour le jeton KD par le serveur expéditeur, et donc l'échec de la transaction.

Selon encore d'autres caractéristiques particulières, le serveur destinataire et le serveur récepteur sont distincts, et :

- le serveur destinataire envoie au serveur récepteur, entre les étapes b) et c) mentionnées ci-dessus, une notification de transaction comprenant des éléments extraits de ladite requête de notification, et
- le serveur destinataire envoie au serveur récepteur, entre les étapes d) et e) mentionnées ci-dessus, une notification de paramètres comprenant ledit jeton KD.

Grâce à ces dispositions, on peut avantageusement appliquer l'invention à un client destinataire en situation de mobilité par rapport à son domaine de rattachement. Ladite notification de transaction permet en particulier, dans le cas envisagé ici, de vérifier que le client destinataire est d'accord pour recevoir le message.

Selon des dispositions encore plus particulières, ladite notification de paramètres comprend en outre ladite valeur h(MES).

Grâce à ces dispositions, on peut compléter, dans le cas visé, les dispositions, exposées succinctement ci-dessus, consistant à inclure la valeur h(MES) dans ladite requête de notification.

Selon encore d'autres caractéristiques particulières, le serveur destinataire et le serveur récepteur sont distincts, et les communications entre ces deux serveurs sont protégées en intégrité.

Grâce à ces dispositions, on peut faire obstacle à une attaque du type MITM dans laquelle un pirate enverrait au serveur récepteur une notification de paramètres contenant un jeton KD' illicite. En effet, le pirate pourrait alors tromper le serveur récepteur en lui envoyant ensuite un pseudo-message authentifié contenant un message MES' illicite accompagné de ce même jeton KD' illicite.

En résumé, on voit que l'invention permet, au moyen de précautions assez simples à mettre en œuvre, mais judicieusement choisies, non seulement de protéger les usagers d'un réseau contre la réception de messages indésirables, mais en outre de protéger les transmissions de messages *désirables* contre diverses attaques par des tiers mal intentionnés.

Corrélativement, l'invention concerne divers dispositifs.

Elle concerne ainsi, premièrement, un dispositif, dit serveur expéditeur, de protection contre les messages indésirables dans un réseau de télécommunications. Ledit dispositif est remarquable en ce qu'il comprend des moyens pour, lorsqu'un client expéditeur rattaché à un domaine dit domaine expéditeur auquel appartient ledit serveur expéditeur et connecté à un dispositif, dit serveur émetteur, envoie un message, dit message original MES, à destination d'au moins un client destinataire rattaché à un domaine dit domaine destinataire et connecté à un dispositif, dit serveur récepteur :

- prendre acte qu'une transaction associée audit client expéditeur et audit client destinataire a été initiée,

- au cas où il décide d'autoriser ladite transaction, envoyer, ou faire envoyer par ledit serveur émetteur, une requête de notification à un dispositif, dit serveur destinataire, appartenant audit domaine destinataire,

ladite requête de notification comprenant des éléments incluant un identifiant du client destinataire,

- recevoir de la part dudit serveur destinataire une décision de transaction comprenant un témoin K_REC,

- calculer un jeton KD, qui résulte de l'application d'un algorithme de chiffrement prédéterminé à un ensemble de données dépendant au moins dudit témoin K_REC, en utilisant une clé de chiffrement TID_N partagée avec le serveur destinataire, et

- envoyer, ou faire envoyer par ledit serveur émetteur, au serveur destinataire ou audit serveur récepteur un message authentifié AM comprenant ledit message original MES, et le jeton KD ou une valeur dérivée du jeton KD.

Elle concerne aussi, deuxièmement, un dispositif, dit serveur destinataire, de protection contre les messages indésirables dans un réseau de télécommunications. Ledit dispositif est remarquable en ce qu'il comprend des moyens pour, lorsqu'un client expéditeur rattaché à un domaine dit domaine expéditeur et connecté à un dispositif, dit serveur émetteur, envoie un message, dit message original MES, à destination d'au moins un client destinataire rattaché à un domaine dit domaine destinataire auquel appartient ledit serveur destinataire et connecté à un dispositif, dit serveur récepteur :

- recevoir de la part dudit serveur émetteur ou d'un dispositif, dit serveur expéditeur, appartenant audit domaine expéditeur une requête de notification comprenant des éléments incluant un identifiant dudit client destinataire,

- au cas où il décide d'autoriser la transaction, engendrer aléatoirement un témoin K_REC, et envoyer audit serveur expéditeur une décision de transaction comprenant ledit témoin K_REC, et

- calculer un jeton KD, qui résulte de l'application d'un algorithme de chiffrement prédéterminé à un ensemble de données dépendant au moins

dudit témoin K_REC, en utilisant une clé de chiffrement TID_N partagée entre le serveur expéditeur et le serveur destinataire.

Selon des dispositions particulières, ce dispositif de protection contre les messages indésirables comprend en outre des moyens pour :

- recevoir de la part dudit serveur expéditeur ou dudit serveur émetteur un message authentifié AM comprenant ledit message original MES, et le jeton KD ou une valeur dérivée du jeton KD, et
- décider d'autoriser la transaction, au moins sur la base de la valeur du jeton KD ou de la valeur dérivée du jeton KD reçue dans ledit message authentifié AM.

Selon d'autres dispositions particulières, ce dispositif de protection contre les messages indésirables comprend en outre des moyens pour envoyer audit serveur récepteur :

- une notification de transaction comprenant des éléments incluant un identifiant dudit client destinataire, et
- une notification de paramètres comprenant ledit jeton KD, et l'adresse du serveur émetteur destiné à envoyer au serveur récepteur un message authentifié AM comprenant ledit message original MES, et le jeton KD ou une valeur dérivée du jeton KD.

Les avantages offerts par ces dispositifs sont essentiellement les mêmes que ceux offerts par les procédés corrélatifs succinctement exposés ci-dessus.

On notera qu'il est possible de mettre en œuvre le procédé de protection contre les messages indésirables selon l'invention au moyen d'instructions logicielles et/ou au moyen de circuits électroniques.

L'invention vise donc également un programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur. Ce programme d'ordinateur est remarquable en ce qu'il comprend des instructions pour la mise en œuvre desdits moyens compris dans l'un

quelconque des dispositifs de protection contre les messages indésirables décrits succinctement ci-dessus.

Les avantages offerts par ce programme d'ordinateur sont essentiellement les mêmes que ceux offerts par lesdits dispositifs.

D'autres aspects et avantages de l'invention apparaîtront à la lecture de la description détaillée ci-dessous de modes de réalisation particuliers, donnés à titre d'exemples non limitatifs. La description se réfère aux figures qui l'accompagnent, dans lesquelles :

- la figure 1 représente schématiquement un réseau de télécommunications et les principales entités auxquelles s'applique l'invention, et
- la figure 2 représente schématiquement les étapes d'un mode de réalisation du procédé selon l'invention.

Le système illustré sur la **figure 1** comprend un réseau principal de télécommunications 300, par exemple l'Internet, auquel sont reliés les quatre domaines, ou réseaux, de télécommunications suivants :

- un domaine dit domaine émetteur 101,
- un domaine dit domaine expéditeur 102,
- un domaine dit domaine récepteur 201, et
- un domaine dit domaine destinataire 202.

Ces domaines sont aptes à transmettre, de manière classique, des messages de nature quelconque tels que, par exemple, des courriers électroniques ou des appels téléphoniques sur des canaux fixes ou mobiles.

Le présent mode de réalisation comprend une étape préalable à l'envoi de tout message, dite phase de mise en relation, dans laquelle le domaine expéditeur 102 a demandé à être mis en relation avec le domaine destinataire 202, et le domaine destinataire 202 a accepté en imposant ses conditions quant à la future association. Lorsque la phase de mise en relation aboutit, une association est créée entre le domaine

expéditeur et le domaine destinataire, et cette association est enregistrée et maintenue de façon synchrone par le domaine expéditeur et par le domaine destinataire. L'association comporte des paramètres constants, fixés lors de la phase de mise en relation, et des paramètres variables qui évoluent en fonction des transactions se déroulant entre les deux domaines. La phase de mise en relation comprend :

- la désignation d'au moins un dispositif, dit serveur expéditeur 1, dans ledit domaine expéditeur, et d'au moins un dispositif, dit serveur destinataire 2, dans ledit domaine destinataire, et
- le partage d'informations, dites informations de synchronisation (qui seront décrites ci-dessous) entre le serveur expéditeur 1 et le serveur destinataire 2, notamment en fonction, généralement, d'exigences de la part du domaine destinataire 202.

On notera qu'il est tout-à-fait possible, dans le cadre de l'invention, de prévoir, sous réserve de l'accord du domaine destinataire 202, une pluralité de serveurs expéditeurs. De même, lors de la mise en relation, le domaine destinataire 202 peut indiquer au domaine expéditeur 102 une pluralité de serveurs destinataires adressables pour les futures transactions.

La désignation de S_E serveurs dans le domaine expéditeur et de S_D serveurs dans le domaine destinataire, avec $S_E \geq 1$ et $S_D \geq 1$, fournit des propriétés de redondance ou de partage de charge. Chaque serveur, dans le domaine expéditeur et dans le domaine destinataire est caractérisé au minimum par un indice et par une adresse réseau ou de transport, à laquelle ce serveur est adressable.

De plus, une matrice dite "de connectivité", de taille $S_E \cdot S_D$, et notée ASIM, peut être fixée par le domaine destinataire, dans le cadre de la phase de mise en relation, et constituer l'un des paramètres de l'association. Par définition ASIM[i, j] est un élément booléen indiquant

si le serveur d'indice i dans le domaine expéditeur est autorisé à participer à des transactions impliquant le serveur d'indice j dans le domaine destinataire, et inversement si le serveur d'indice j dans le domaine destinataire est autorisé à participer à des transactions impliquant le serveur d'indice i dans le domaine expéditeur. Dans un mode d'application simplifié, la matrice ASIM est non spécifiée, ce qui signifie que tout serveur expéditeur peut participer à des transactions avec tout serveur destinataire.

Les serveurs sont supposés "stables" au niveau réseau, c'est-à-dire qu'ils échangent les messages protocolaires à des adresses préalablement enregistrées par le domaine expéditeur et le domaine destinataire. Toute modification de l'un de ces serveurs doit être exceptionnelle et avalisée par le domaine destinataire. Dans le cadre d'une association établie, des demandes fréquentes de la part du domaine expéditeur pour modifier les adresses de routage de ses serveurs dénotent probablement un domaine attaquant.

Certains paramètres enregistrés dans l'association, comme par exemple la matrice de connectivité ASIM, peuvent évoluer au fil du temps, sur décision du domaine destinataire ou sur demande du domaine expéditeur, avalisée par le domaine destinataire. Ce mode de décision unilatéral vise à protéger le domaine destinataire contre toute dérive ou tentative d'abus de la part du domaine expéditeur.

Une fois cette étape préalable de mise en relation accomplie, on peut appliquer le procédé selon l'invention à tout message, dit "message original" MES, envoyé par un client expéditeur 100 rattaché au domaine expéditeur 102 (c'est-à-dire enregistré auprès de ce domaine expéditeur), à destination d'au moins un client destinataire 200 rattaché au domaine destinataire 202.

Afin de prendre en compte une éventuelle mobilité du client expéditeur 100, on dira de manière générale que ce client est connecté à

un domaine dit domaine émetteur 101 ; on dira aussi de manière générale que ce domaine émetteur 101 comprend au moins un serveur-relais, dit serveur émetteur 3, qui participe à la gestion des transactions, en lien avec un serveur expéditeur 1, sans pour autant connaître les informations de synchronisation qui constituent le secret partagé établi entre le serveur expéditeur 1 et le serveur destinataire 2 lors de la phase de mise en relation. Mais il est clair que les domaines émetteur 101 et expéditeur 102 ne sont pas nécessairement distincts ; lorsque les domaines émetteur et expéditeur sont confondus, le serveur émetteur 3 peut éventuellement être physiquement confondu avec le serveur expéditeur 1, et/ou le client expéditeur peut éventuellement être physiquement confondu avec le serveur émetteur.

De même, afin de prendre en compte une éventuelle mobilité du client destinataire 200, on dira de manière générale que ce client est connecté à un domaine dit domaine récepteur 201 ; on dira aussi de manière générale que ce domaine récepteur 201 comprend au moins un serveur-relais, dit serveur récepteur 4, qui participe à la gestion des transactions, en lien avec un serveur destinataire 2, sans pour autant connaître les informations de synchronisation qui constituent le secret partagé établi entre le serveur destinataire 2 et le serveur expéditeur 1 lors de la phase de mise en relation. Mais il est clair que les domaines récepteur 201 et destinataire 202 ne sont pas nécessairement distincts ; lorsque les domaines récepteur et destinataire sont confondus, le serveur récepteur 4 peut éventuellement être physiquement confondu avec le serveur destinataire 2, et/ou le client destinataire peut éventuellement être physiquement confondu avec le serveur récepteur.

Les transactions se déroulant entre un même domaine expéditeur et un même domaine destinataire sont ordonnées selon un numéro d'ordre, également appelé "indice de transaction" N. A un instant donné, plusieurs transactions peuvent être simultanément actives entre un même

domaine expéditeur et un même domaine destinataire, dans la limite d'un nombre maximal MNSAT défini dans le cadre de l'association entre ces deux domaines. La valeur MNSAT est fixée par le domaine destinataire, lors de l'établissement de l'association entre les deux domaines, afin de protéger le domaine destinataire contre tout risque d'inondation en provenance du domaine expéditeur. Dans un mode d'application simplifié, la valeur MNSAT est non spécifiée, ce qui signifie que le domaine destinataire accepte un nombre quelconque de transactions actives à un instant donné.

De plus, dans le cadre d'une association donnée, les domaines expéditeur et destinataire peuvent calculer indépendamment, pour toute transaction d'indice N, une clé de chiffrement secrète TID_N associée à cette transaction.

De préférence, on veillera à ce que cette clé de chiffrement TID_N varie (de manière concertée) d'une transaction à une autre, afin d'éviter les attaques par rejeu et les attaques résultant de la découverte frauduleuse par un attaquant de certaines informations de synchronisation. Pour éviter de transmettre la clé TID_N via le réseau, cette clé est calculée simultanément par le domaine expéditeur et par le domaine destinataire à partir de l'indice de transaction N ; par exemple, la clé de chiffrement TID_N peut être dérivée à partir de l'indice de transaction N et d'une clé secrète choisie par les domaines expéditeur et destinataire lors de la phase de mise en relation. Dans un mode d'application simplifié, la clé de chiffrement TID_N peut être indépendante de l'indice de transaction, et être constante, c'est-à-dire fixée lors de l'établissement de l'association.

La **figure 2** représente schématiquement les étapes d'un mode de réalisation du procédé selon l'invention.

Pour fixer les idées, on se placera ici dans le cas où à la fois le client expéditeur 100 et le client destinataire 200 sont en situation de

mobilité. On supposera de plus (toujours pour fixer les idées), d'une part, que le client expéditeur 100 et le serveur émetteur 3 sont distincts, et d'autre part que le client destinataire 200 et le serveur récepteur 4 sont distincts. L'homme du métier adaptera aisément la description ci-dessous aux autres agencements possibles.

Comme expliqué ci-dessus, les échanges entre serveur émetteur 3 et serveur expéditeur 1 sont, de préférence, protégés en intégrité ; cette protection peut par exemple être mise en œuvre, de manière classique, en associant au contenu des échanges entre serveur émetteur et serveur expéditeur un code d'authentification de ce contenu, ledit code étant obtenu au moyen d'une clé secrète SK_A partagée par le serveur émetteur 3 et le serveur expéditeur 1. Optionnellement, une autre clé secrète SK_C partagée entre ces serveurs, ou pouvant être dérivée de SK_A, est utilisée pour chiffrer les échanges entre le serveur émetteur 3 et le serveur expéditeur 1.

On va décrire à présent les étapes principales de ce mode de réalisation de l'invention.

Lors d'une première étape E1, une nouvelle transaction est authentifiée, et autorisée, par le serveur expéditeur 1.

Plus précisément, lors d'une sous-étape E11, le client expéditeur 100 initie une transaction en envoyant un message original MES au serveur émetteur 3.

Lors d'une sous-étape E12, ledit serveur émetteur 3 envoie une requête d'authentification AUT au serveur expéditeur 1. Cette requête d'authentification AUT contient notamment l'identifiant du client expéditeur, l'identifiant du client destinataire et une valeur h(MES) obtenue en appliquant une fonction à sens unique "h" (par exemple une fonction de "hachage") à tout ou partie du message original MES.

Lors d'une sous-étape E13, le serveur expéditeur 1 décide, sur la base desdites informations de synchronisation et d'une évaluation de

l'authenticité du client expéditeur 100, d'autoriser ou d'interdire la poursuite de la transaction. En particulier, si un paramètre MNSAT tel que défini ci-dessus a été choisi pour l'association considérée entre le domaine expéditeur 102 et le domaine destinataire 202, le serveur expéditeur 1 vérifie que le nombre de transactions déjà initiées entre ces deux domaines est strictement inférieur à ce paramètre MNSAT, avant d'autoriser éventuellement une nouvelle transaction.

L'évaluation de l'authenticité du client expéditeur 100 implique, dans le cas, considéré ici, où le client expéditeur 100 est en situation de mobilité par rapport à son domaine de rattachement, un échange de messages AUT_C_REQ et AUT_C_REP entre le serveur expéditeur 1 et le serveur émetteur 3 ; par exemple, le message AUT_C_REQ contient un défi à l'intention du client expéditeur 100, et le message AUT_C_REP contient la réponse du client expéditeur 100 à ce défi. Dans le cas où le client expéditeur 100 n'est pas en situation de mobilité, un tel échange de messages d'authentification peut éventuellement s'avérer superflu.

S'il décide d'autoriser la transaction, le serveur expéditeur 1, à l'étape E2, notifie la transaction au serveur destinataire 2. Dans le cas où plusieurs serveurs ont été déclarés par le domaine destinataire :

- si, lors de la phase de mise en relation, une matrice de connectivité ASIM telle que définie ci-dessus a été choisie, alors le serveur destinataire est choisi parmi les serveurs autorisés par la matrice ASIM, et
- sinon, il est choisi parmi l'ensemble des serveurs du domaine destinataire.

Plus précisément, le serveur expéditeur 1 envoie, ou fait envoyer par le serveur émetteur 3, une requête de notification NOT au serveur destinataire 2. Cette requête de notification NOT contient, d'une part, des éléments comprenant au moins un identifiant du client expéditeur 100, un identifiant du ou des clients(s) destinataire(s) 200, et la valeur h(MES) ;

ces trois éléments reprennent les valeurs extraites de la requête d'authentification AUT reçue par le serveur expéditeur 1.

De plus, en cas de pluralité de serveurs expéditeurs et destinataires autorisés, la requête de notification NOT contient l'indice i du serveur expéditeur 1 particulier qui a autorisé la transaction considérée, et l'indice j du serveur destinataire 2 à qui est destinée la requête de notification NOT. Lorsque la requête de notification NOT doit être envoyée par le serveur émetteur 3, le serveur expéditeur 1 ajoute de plus l'adresse réseau du serveur destinataire 2 qui n'est, *a priori*, pas connue du serveur émetteur 3.

Avantageusement, le serveur expéditeur 1 insère un marqueur temporel dans la requête de notification NOT, afin d'éviter les attaques par rejeu.

De plus, la requête de notification NOT contient l'adresse réseau du serveur émetteur 3 qui a généré la requête d'authentification AUT et qui, dans ce mode de réalisation, enverra postérieurement le message authentifié AM.

D'autre part, la requête de notification NOT contient l'indice de transaction N, qui permet notamment au serveur expéditeur 1 et au serveur destinataire 2 de sélectionner ou engendrer la même clé de chiffrement TID_N pour la transaction considérée lorsque cette clé de chiffrement dépend de N.

Enfin, la requête de notification NOT est de préférence protégée par un code d'authentification obtenu au moyen d'une clé $SSK_{i,j,}$, partagée entre le serveur expéditeur 1 et le serveur destinataire 2. En effet, comme expliqué ci-dessus, ce code d'authentification permet de rejeter les communications provenant d'une source non autorisée, et de protéger en intégrité les éléments de la requête de notification NOT.

A l'étape E3, cette nouvelle transaction est vérifiée par le serveur destinataire 2.

Plus précisément, lors d'une sous-étape E31, après réception d'une requête de notification NOT, le serveur destinataire 2 évalue sa validité sur la base desdites informations de synchronisation. Le serveur destinataire 2 vérifie notamment que le serveur expéditeur 1 est authentique, et que la requête de notification NOT n'a pas été altérée. Avantageusement, le serveur destinataire 2 vérifie que le serveur expéditeur 1 d'indice i est effectivement autorisé, selon la matrice de connectivité ASIM, à lui envoyer une requête de notification NOT, que le marqueur temporel est inclus dans une fenêtre temporelle autorisée, et que la valeur de l'indice de transaction N est compris dans une fenêtre de transactions autorisées.

En effet, le maintien, pour une association donnée, d'une fenêtre de transactions autorisées permet de se protéger du cas où un attaquant, ayant eu frauduleusement accès à la clé $SSK_{i,j,}$, pourrait générer des transactions en grande quantité impliquant le serveur destinataire 2. La fenêtre de transactions autorisées est définie par l'indice de la première transaction active, et par la largeur de la fenêtre qui est égale au paramètre MNSAT.

Lors d'une sous-étape E32, si le résultat de ladite évaluation est positif, le serveur destinataire 2 envoie au serveur récepteur 4 une notification de transaction TERM_NOT contenant des éléments extraits de la requête de notification NOT, dont, notamment, un identifiant du client expéditeur 100, un identifiant du ou des clients(s) destinataire(s) 200 et la valeur h(MES).

Lors d'une sous-étape E33, après réception d'une notification de transaction TERM_NOT, le serveur récepteur 4 détermine si le client destinataire 200 souhaite recevoir le message original MES (ou, en cas de pluralité de clients destinataires, lequel d'entre eux souhaite recevoir le message original MES). Pour ce faire, diverses options sont possibles,

seules ou en combinaison, pour chacun des destinataires connectés à ce serveur récepteur 4.

Plus précisément, le serveur récepteur 4 consulte des listes d'adresses d'expéditeur pour essayer de déterminer si l'adresse du client expéditeur 100 est autorisée, pour au moins un client destinataire 200, afin d'accepter la réception du message original MES en provenance de cette adresse. A cet effet, le serveur récepteur 4 peut consulter une liste blanche LBDD d'adresses autorisées au sein de tout le domaine destinataire 202, et une liste blanche LBU d'adresses autorisées par un client destinataire 200 particulier. Le serveur récepteur 4 peut consulter également des listes noires d'adresses interdites respectives LNDD et LNU. A partir du ou des destinataire(s) indiqués dans la notification de transaction TERM_NOT, le serveur récepteur 4 engendre alors, en fonction des listes consultées, une liste de refus RDR, une liste d'accord définitif RDA et une liste d'accord provisoire RPA définies comme suit :

- la liste de refus RDR inclut les identificateurs des destinataires pour lesquels la réception du message MES est refusée, soit parce que ces destinataires n'existent pas dans le domaine de destinataire, soit parce que l'adresse de l'expéditeur apparaît au moins dans une des listes LNDD ou LNU relatives à ces destinataires ;

- la liste d'accord définitif RDA inclut les identificateurs des destinataires pour lesquels la réception du message MES est accordée définitivement ; la condition pour qu'un destinataire soit ajouté à cette liste est que l'adresse de l'expéditeur n'apparaisse dans aucune des listes LNDD ou LNU relative à ce destinataire, et qu'à l'inverse l'adresse de l'expéditeur apparaisse dans les listes LBDD ou LBU relative à ce destinataire ; et

- la liste d'accord provisoire RPA inclut les identificateurs des destinataires pour lesquels la réception du message MES est accordée provisoirement, c'est-à-dire n'est, *a priori*, ni refusée, ni acceptée.

En variante, le serveur récepteur 4 engendre la liste de refus RDR, respectivement d'accord définitif RDA, sans recourir aux listes noires LNDD ou LNU, respectivement listes blanches LBDD ou LBU, par exemple en recueillant des refus, respectivement des accords, explicites de la part des destinataires indiqués dans la notification de transaction TERM_NOT. Pour ce faire, le serveur récepteur 4 peut envoyer à chaque client destinataire 200 une requête d'accord explicite EP_NOT contenant les données pertinentes de la notification de transaction TERM_NOT, et chaque client destinataire 200 envoie en retour une réponse EP_NOT_R à la requête d'accord explicite EP_NOT, ladite réponse EP_NOT_R contenant son accord ou son refus.

Dans tous les cas, la liste RPA contient les identificateurs des destinataires n'entrant ni dans la liste RDR ni dans la liste RDA.

Au moins dans le cas où le résultat de ladite détermination est positif (c'est-à-dire si la liste RDA est non-vide), le serveur récepteur 4 envoie au serveur destinataire 2, lors d'une sous-étape E34, une réponse de notification TERM_NOT_R contenant ce résultat. Optionnellement, la réponse de notification TERM_NOT_R peut également comprendre une copie des listes LR, LAP et LAD, qui seront, *in fine*, retransmises, pour information, au client expéditeur 100.

Lors d'une sous-étape E35, s'il reçoit une réponse de notification TERM_NOT_R contenant un résultat positif, le serveur destinataire 2 engendre aléatoirement un témoin K_REC pour ladite transaction.

A l'étape E4, un jeton KD est calculé et communiqué à qui de droit.

Plus précisément, lors d'une sous-étape E41, le serveur destinataire 2 calcule un jeton KD en appliquant un algorithme de chiffrement prédéterminé à un ensemble de données dépendant (au moins) dudit témoin K_REC, à l'aide de la clé de chiffrement TID_N, présentée ci-dessus. Optionnellement, on pourra faire dépendre le jeton

KD de la valeur h(MES), afin d'augmenter la variabilité des valeurs prises par le jeton KD d'une transaction à une autre.

Lors d'une sous-étape E42, le serveur destinataire 2 envoie au serveur récepteur 4 une notification de paramètres NOT_R_KD comprenant ledit jeton KD, la valeur h(MES) et l'adresse du serveur émetteur 3 qui, dans ce mode de réalisation, enverra postérieurement le message authentifié AM.

Au moins s'il décide d'autoriser la transaction, le serveur destinataire 2 envoie au serveur expéditeur 1, lors d'une sous-étape E43, une décision de transaction NOT_R_REC exprimant son autorisation ou son refus. Optionnellement, l'autorisation de la part du serveur destinataire 2 peut être soumise à la réception, dans un délai prédéterminé après l'envoi de ladite notification de paramètres NOT_R_KD, d'un accusé de réception NOT_R_KD_ACK de la part du serveur récepteur 4. En cas d'autorisation, le serveur destinataire 2 inclut, dans ladite décision de transaction NOT_R_REC, le témoin K_REC ainsi que l'adresse réseau du serveur récepteur 4 à qui devra être envoyé le message authentifié AM.

Dans tous les cas, la décision de transaction NOT_R_REC comprend lesdites listes RPA, RDA et RDR, un marqueur temporel pour éviter les attaques par rejeu, et l'indice de la première transaction active pour l'association considérée, vu du domaine expéditeur.

De préférence, la décision de transaction NOT_R_REC est protégée par un code d'authentification obtenu au moyen d'une clé $RSK_{i,j}$, où i est l'identifiant du serveur expéditeur 1 et j est l'identifiant du serveur destinataire 2 qui engendre la décision de transaction NOT_R_REC. En effet, ce code d'authentification permet d'authentifier le serveur destinataire 2 auprès du serveur expéditeur 1, et de se protéger contre une attaque par déni de service comme expliqué ci-dessous en référence à la sous-étape E45.

Lors d'une sous-étape E44, après réception d'une décision de transaction NOT_R_REC, le serveur expéditeur 1 vérifie son authenticité, dont notamment l'authenticité du serveur destinataire 2 qui a envoyé cette décision de transaction NOT_R_REC. Avantageusement, le serveur expéditeur 1 vérifie que le marqueur temporel est inclus dans une fenêtre temporelle autorisée.

Lors d'une sous-étape E45, si le résultat de ladite vérification est positif, et que la liste RDA extraite de la décision de transaction NOT_R_REC est non-vide, le serveur expéditeur 1 calcule le jeton KD comme décrit ci-dessus en référence à la sous-étape E41. Par ailleurs, l'utilisation, à la sous-étape E43 ci-dessus, d'un code d'authentification protégeant notamment la valeur du témoin K_REC assure que le serveur expéditeur 1 calcule la bonne valeur du jeton KD.

Lors d'une sous-étape E46, le serveur expéditeur 1 envoie au serveur émetteur 3, dans une notification d'éléments NOT_R_SEND, des éléments comprenant au moins le jeton KD et la liste RDA des clients destinataires ayant accepté la transaction. Optionnellement, le serveur émetteur 3 peut, après réception de la notification d'éléments NOT_R_SEND, envoyer un accusé de réception NOT_R_SEND_ACK au serveur expéditeur 1.

A l'étape E5, après réception d'une notification d'éléments NOT_R_SEND, le serveur émetteur 3 envoie au serveur récepteur 4 un "message authentifié" AM comprenant au moins le message original MES, et le jeton KD ou, de préférence, une valeur obtenue à partir du jeton KD au moyen d'un procédé de dérivation prédéterminé (par exemple, en appliquant au jeton KD une fonction à sens unique), de manière à éviter d'émettre la valeur jeton KD en clair.

A l'étape E6, le serveur récepteur 4 dépouille le message authentifié AM.

Plus précisément, lors d'une sous-étape E61, après réception d'un message authentifié AM, le serveur récepteur 4 évalue son authenticité. Le serveur récepteur 4 vérifie notamment :

- que l'adresse du serveur émetteur 3 est bien l'adresse qu'il a reçue, à la sous-étape E42, dans la notification de paramètres NOT_R_KD,
- que les identités des clients expéditeur (100) et destinataire(s) (200) sont bien celles qui étaient indiquées dans la notification de transaction TERM_NOT et la notification de paramètres NOT_R_KD,
- qu'en appliquant la fonction "h" au message MES reçu, il obtient la même valeur h(MES) que celle qui était indiquée dans la notification de paramètres NOT_R_KD, et
- qu'en appliquant le procédé de dérivation au jeton KD qu'il a reçu dans la notification de paramètres NOT_R_KD, il obtient la même valeur que celle contenue dans le message authentifié AM.

Puis, lors d'une sous-étape E62, si le résultat de ladite évaluation est positif, le serveur récepteur 4 transmet le message original MES au(x) client(s) destinataire(s) 200 inclus dans la liste d'accord définitif RDA décrite ci-dessus.

Enfin, lors d'une sous-étape E63, le serveur récepteur 4 envoie au serveur destinataire 2 (plus précisément, en cas de pluralité de serveurs destinataires, celui qui lui avait envoyé la notification de paramètres NOT_R_KD) une notification de fin de transaction AM_R. Optionnellement, ce serveur destinataire peut envoyer au serveur récepteur 4 un accusé de réception AM_R_ACK.

Sur la base du mode de réalisation de l'invention décrit ci-dessus, on comprendra que lesdites "informations de synchronisation" doivent inclure au moins :

- la liste des serveurs expéditeurs et des serveurs destinataires autorisés dans le cadre de l'association entre les deux domaines, chaque

serveur étant caractérisé par son indice et par au moins une adresse réseau ou de transport à laquelle ce serveur est adressable,

- la matrice de connectivité ASIM fixant les autorisations de transaction entre les serveurs expéditeurs et les serveurs destinataires,

- des informations secrètes permettant au domaine expéditeur 102 d'authentifier le serveur destinataire 2, et au domaine destinataire 202 d'authentifier le serveur expéditeur 1, c'est-à-dire, respectivement, les clés $SSK_{i,j,}$ et $RSK_{i,j,}$,

- des informations permettant au domaine expéditeur 102 et au domaine destinataire 202 d'obtenir la valeur, pour toute transaction d'indice N, de la clé de chiffrement TID_N utilisée pour calculer le jeton KD,

- l'indice à utiliser pour la première transaction, et

- la largeur MNSAT de la fenêtre de transactions.

La mise en œuvre de l'invention au sein des nœuds du réseau de télécommunications (notamment, les serveurs expéditeur 1, destinataire 2, émetteur 3 et récepteur 4 dans le mode de réalisation décrit ci-dessus) peut être réalisée au moyen de composants logiciels et/ou matériels.

Les composants logiciels pourront être intégrés à un programme d'ordinateur classique de gestion de nœud de réseau. C'est pourquoi, comme indiqué ci-dessus, la présente invention concerne également un système informatique. Ce système informatique comporte de manière classique une unité centrale de traitement commandant par des signaux une mémoire, ainsi qu'une unité d'entrée et une unité de sortie. De plus, ce système informatique peut être utilisé pour exécuter un programme d'ordinateur comportant des instructions pour la mise en œuvre du procédé de protection contre les messages indésirables selon l'invention.

En effet, l'invention vise aussi un programme d'ordinateur téléchargeable depuis un réseau de communication comprenant des instructions pour l'exécution de certaines au moins des étapes d'un

procédé de protection contre les messages indésirables selon l'invention, lorsqu'il est exécuté sur un ordinateur. Ce programme d'ordinateur peut être stocké sur un support lisible par ordinateur et peut être exécutable par un microprocesseur.

Ce programme peut utiliser n'importe quel langage de programmation, et se présenter 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 ordinateur, et comportant des instructions d'un programme d'ordinateur 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*" en anglais) 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 d'ordinateur selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

En variante, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour être utilisé dans un dispositif de protection contre les messages indésirables selon l'invention.

REVENDICATIONS

1. Procédé de protection contre les messages indésirables dans un réseau de télécommunications, comprenant, lorsqu'un client expéditeur (100) rattaché à un domaine dit domaine expéditeur (102) et connecté à un dispositif, dit serveur émetteur (3), envoie un message, dit "message original" (MES), à destination d'au moins un client destinataire (200) rattaché à un domaine dit domaine destinataire (202) et connecté à un dispositif, dit serveur récepteur (4), les étapes suivantes :

a) un dispositif, dit serveur expéditeur (1), appartenant audit domaine expéditeur (102) prend acte qu'une transaction associée audit client expéditeur (100) et audit client destinataire (200) a été initiée,

b) si ledit serveur expéditeur (1) décide d'autoriser ladite transaction, il envoie, ou fait envoyer par ledit serveur émetteur (3), une requête de notification (NOT) à un dispositif, dit serveur destinataire (2), appartenant audit domaine destinataire (202), ladite requête de notification (NOT) comprenant des éléments incluant un identifiant du client destinataire (200),

c) si ledit serveur destinataire (2) décide d'autoriser la transaction, il engendre aléatoirement un témoin (K_REC), et envoie au serveur expéditeur (1) une décision de transaction (NOT_R_REC) comprenant ledit témoin (K_REC),

ledit procédé étant caractérisé en ce qu'il comprend en outre les étapes suivantes :

d) le serveur expéditeur (1) et le serveur destinataire (2) calculent indépendamment un même jeton (KD), qui résulte de l'application d'un algorithme de chiffrement prédéterminé à un ensemble de données dépendant au moins dudit témoin (K_REC), en utilisant une clé de chiffrement (TID_N) partagée entre le serveur expéditeur (1) et le serveur destinataire (2),

e) le serveur expéditeur (1) envoie, ou fait envoyer par ledit serveur émetteur (3), au serveur destinataire (2) ou audit serveur récepteur (4) un "message authentifié" (AM) comprenant ledit message original (MES), et le jeton (KD) ou une valeur dérivée du jeton (KD), et

f) si le serveur destinataire (2) ou le serveur récepteur (4) décide, au moins sur la base de la valeur du jeton (KD) ou de la valeur dérivée du jeton (KD) reçue dans ledit message authentifié (AM), d'autoriser la transaction, le client destinataire (200) accepte le message original (MES).

2. Procédé de protection contre les messages indésirables selon la revendication 1, caractérisé en ce que ladite requête de notification (NOT) est protégée en intégrité.

3. Procédé de protection contre les messages indésirables selon la revendication 1 ou la revendication 2, caractérisé en ce que lesdits éléments de la requête de notification (NOT) incluent en outre une valeur h(MES) obtenue en appliquant une fonction à sens unique "h" à tout ou partie dudit message original (MES).

4. Procédé de protection contre les messages indésirables selon l'une quelconque des revendications 1 à 3, caractérisé en ce que ledit serveur émetteur (3) et ledit serveur expéditeur (1) sont distincts, et en ce que :

- avant ladite étape a), le serveur émetteur (3) envoie au serveur expéditeur (1) une requête d'authentification (AUT) comprenant au moins un identifiant dudit client destinataire (200), et

- entre lesdites étapes d) et e), le serveur expéditeur (1) envoie au serveur émetteur (3) une notification d'éléments (NOT_R_SEND) comprenant ledit jeton (KD).

5. Procédé de protection contre les messages indésirables selon la revendication 3 et la revendication 4, caractérisé en ce que ladite requête d'authentification (AUT) comprend en outre ladite valeur h(MES).

6. Procédé de protection contre les messages indésirables selon la revendication 4 ou la revendication 5, caractérisé en ce que les communications entre ledit serveur émetteur (3) et ledit serveur expéditeur (1) sont protégées en intégrité.

7. Procédé de protection contre les messages indésirables selon l'une quelconque des revendications 1 à 6, caractérisé en ce que ladite décision de transaction (NOT_R_REC) est protégée en intégrité.

8. Procédé de protection contre les messages indésirables selon l'une quelconque des revendications 1 à 7, caractérisé en ce que ledit serveur destinataire (2) et ledit serveur récepteur (4) sont distincts, et en ce que :

- entre lesdites étapes b) et c), le serveur destinataire (2) envoie au serveur récepteur (4) une notification de transaction (TERM_NOT) comprenant des éléments extraits de ladite requête de notification (NOT), et

- entre lesdites étapes d) et e), le serveur destinataire (2) envoie au serveur récepteur (4) une notification de paramètres (NOT_R_KD) comprenant ledit jeton (KD).

9. Procédé de protection contre les messages indésirables selon la revendication 3 et la revendication 8, caractérisé en ce que ladite notification de paramètres (NOT_R_KD) comprend en outre ladite valeur h(MES).

10. Procédé de protection contre les messages indésirables selon l'une quelconque des revendications 1 à 9, caractérisé en ce que ledit serveur destinataire (2) et ledit serveur récepteur (4) sont distincts, et en

ce que les communications entre ces deux serveurs sont protégées en intégrité.

11. Dispositif, dit serveur expéditeur (1), de protection contre les messages indésirables dans un réseau de télécommunications, caractérisé en ce qu'il comprend des moyens pour, lorsqu'un client expéditeur (100) rattaché à un domaine dit domaine expéditeur (102) auquel appartient ledit serveur expéditeur (1) et connecté à un dispositif, dit serveur émetteur (3), envoie un message, dit "message original" (MES), à destination d'au moins un client destinataire (200) rattaché à un domaine dit domaine destinataire (202) et connecté à un dispositif, dit serveur récepteur (4) :

- prendre acte qu'une transaction associée audit client expéditeur (100) et audit client destinataire (200) a été initiée,

- au cas où il décide d'autoriser ladite transaction, envoyer, ou faire envoyer par ledit serveur émetteur (3), une requête de notification (NOT) à un dispositif, dit serveur destinataire (2), appartenant audit domaine destinataire (202), ladite requête de notification (NOT) comprenant des éléments incluant un identifiant du client destinataire (200),

- recevoir de la part dudit serveur destinataire (2) une décision de transaction (NOT_R_REC) comprenant un témoin (K_REC),

- calculer un jeton (KD), qui résulte de l'application d'un algorithme de chiffrement prédéterminé à un ensemble de données dépendant au moins dudit témoin (K_REC), en utilisant une clé de chiffrement (TID_N) partagée avec le serveur destinataire (2), et

- envoyer, ou faire envoyer par ledit serveur émetteur (3), au serveur destinataire (2) ou audit serveur récepteur (4) un "message authentifié" (AM) comprenant ledit message original (MES), et le jeton (KD) ou une valeur dérivée du jeton (KD).

12. Dispositif, dit serveur destinataire (2), de protection contre les messages indésirables dans un réseau de télécommunications, caractérisé en ce qu'il comprend des moyens pour, lorsqu'un client expéditeur (100) rattaché à un domaine dit domaine expéditeur (102) et connecté à un dispositif, dit serveur émetteur (3), envoie un message, dit "message original" (MES), à destination d'au moins un client destinataire (200) rattaché à un domaine dit domaine destinataire (202) auquel appartient ledit serveur destinataire (2) et connecté à un dispositif, dit serveur récepteur (4) :

- recevoir de la part dudit serveur émetteur (3) ou d'un dispositif, dit serveur expéditeur (1), appartenant audit domaine expéditeur (102) une requête de notification (NOT) comprenant des éléments incluant un identifiant dudit client destinataire (200),

- au cas où il décide d'autoriser la transaction, engendrer aléatoirement un témoin (K_REC), et envoyer audit serveur expéditeur (1) une décision de transaction (NOT_R_REC) comprenant ledit témoin (K_REC), et

- calculer un jeton (KD), qui résulte de l'application d'un algorithme de chiffrement prédéterminé à un ensemble de données dépendant au moins dudit témoin (K_REC), en utilisant une clé de chiffrement (TID_N) partagée entre le serveur expéditeur (1) et le serveur destinataire (2).

13. Dispositif (2) de protection contre les messages indésirables dans un réseau de télécommunications selon la revendication 12, caractérisé en ce qu'il comprend en outre des moyens pour :

- recevoir de la part dudit serveur expéditeur (1) ou dudit serveur émetteur (3) un "message authentifié" (AM) comprenant ledit message original (MES), et le jeton (KD) ou une valeur dérivée du jeton (KD), et

- décider d'autoriser la transaction, au moins sur la base de la valeur du jeton (KD) ou de la valeur dérivée du jeton (KD) reçue dans ledit message authentifié (AM).

14. Dispositif (2) de protection contre les messages indésirables dans un réseau de télécommunications selon la revendication 12, caractérisé en ce qu'il comprend en outre des moyens pour envoyer audit serveur récepteur (4) :

- une notification de transaction (TERM_NOT) comprenant des éléments incluant un identifiant dudit client destinataire (200), et
- une notification de paramètres (NOT_R_KD) comprenant ledit jeton (KD), et l'adresse du serveur émetteur (3) destiné à envoyer au serveur récepteur (4) un "message authentifié" (AM) comprenant ledit message original (MES), et le jeton (KD) ou une valeur dérivée du jeton (KD).

15. Moyen de stockage de données inamovible, ou partiellement ou totalement amovible, comportant des instructions de code de programme informatique pour la mise en œuvre desdits moyens compris dans un dispositif de protection contre les messages indésirables selon l'une quelconque des revendications 11 à 14.

16. Programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions pour la mise en œuvre desdits moyens compris dans un dispositif de protection contre les messages indésirables selon l'une quelconque des revendications 11 à 14.

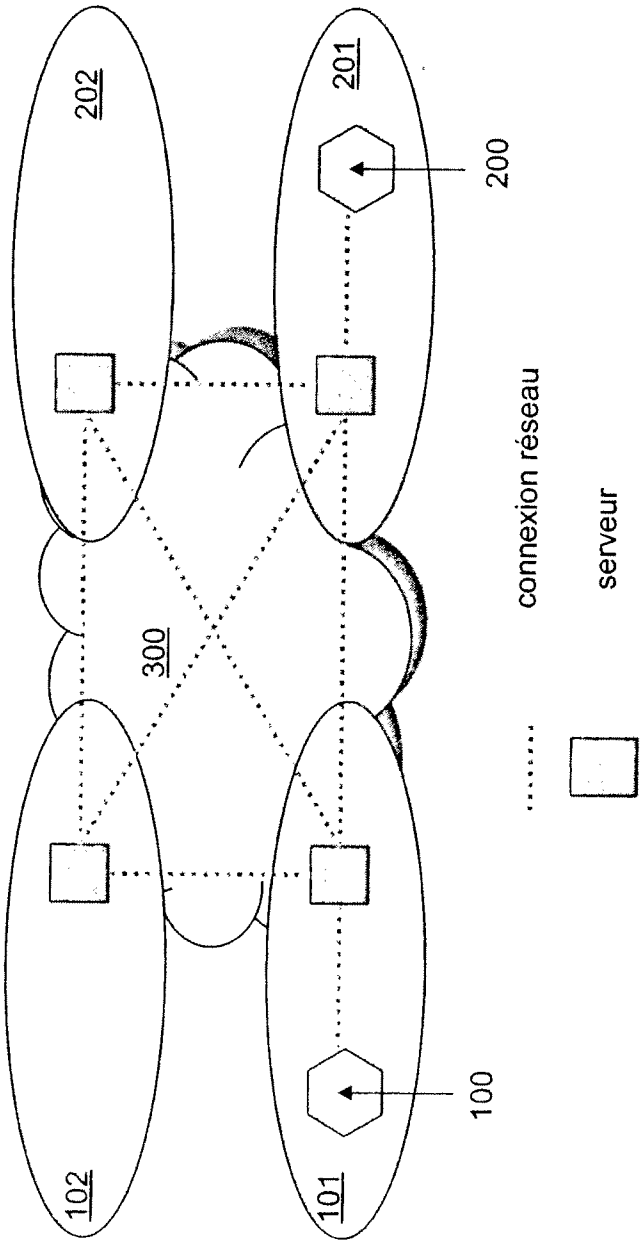


FIG. 1

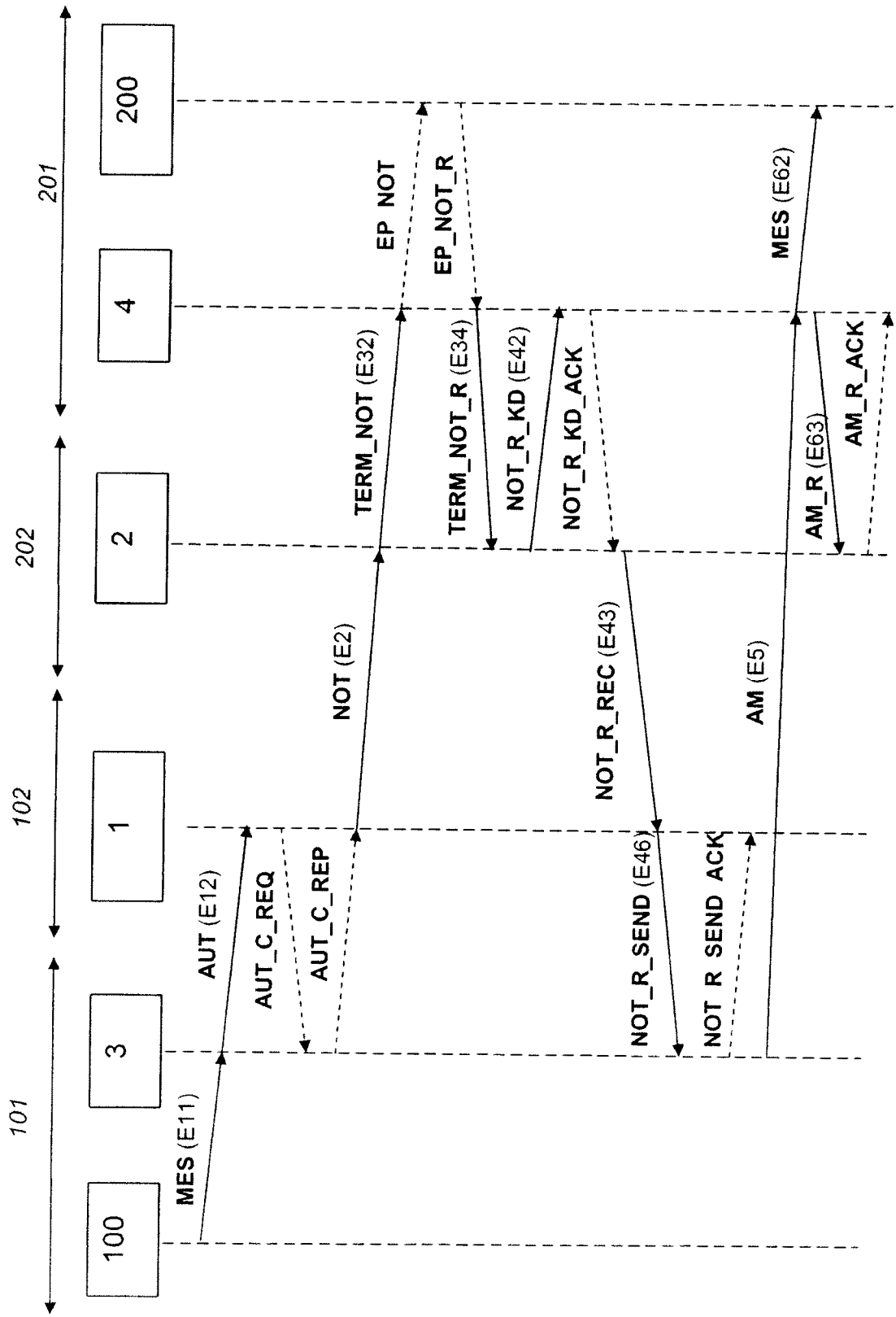

101
102
202
201
100
3
1
2
4
200
MES (E11)
AUT (E12)
AUT_C_REQ
AUT_C_REP
NOT (E2)
TERM_NOT (E32)
EP NOT
EP_NOT_R
TERM_NOT_R (E34)
NOT_R_KD (E42)
NOT_R_KD_ACK
NOT_R_REC (E43)
NOT_R_SEND (E46)
NOT R SEND ACK
AM (E5)
MES (E62)
AM_R (E63)
AM_R_ACK

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2010/050828

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L12/58
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FR 2 907 292 A (FRANCE TELECOM [FR]) 18 April 2008 (2008-04-18) cited in the application page 1, line 4 - page 7, line 10 page 13, line 19 - page 18, line 33 page 36, line 1 - line 14 page 38, line 18 - page 40, line 15 figure 2	1-16
Y	US 2007/073817 A1 (GORTY SURYANARAYANA M [US]) 29 March 2007 (2007-03-29) * abstract page 7, paragraph 74 - paragraph 78	1-16
A	US 2004/181585 A1 (ATKINSON ROBERT GEORGE [US] ET AL) 16 September 2004 (2004-09-16) * abstract page 1, paragraph 3 - page 3, paragraph 25	1-16

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 July 2010	04/08/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Avilés Martinez, M

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2010/050828

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2907292 A	18-04-2008	AT 467966 T	15-05-2010
		EP 2092703 A1	26-08-2009
		WO 2008047024 A1	24-04-2008
US 2007073817 A1	29-03-2007	NONE	
US 2004181585 A1	16-09-2004	US 2009193093 A1	30-07-2009

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2010/050828

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/06 H04L12/58
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	FR 2 907 292 A (FRANCE TELECOM [FR]) 18 avril 2008 (2008-04-18) cité dans la demande page 1, ligne 4 - page 7, ligne 10 page 13, ligne 19 - page 18, ligne 33 page 36, ligne 1 - ligne 14 page 38, ligne 18 - page 40, ligne 15 figure 2	1-16
Y	US 2007/073817 A1 (GORTY SURYANARAYANA M [US]) 29 mars 2007 (2007-03-29) * abrégé page 7, alinéa 74 - alinéa 78	1-16
A	US 2004/181585 A1 (ATKINSON ROBERT GEORGE [US] ET AL) 16 septembre 2004 (2004-09-16) * abrégé page 1, alinéa 3 - page 3, alinéa 25	1-16

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
28 juillet 2010	04/08/2010

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Avilés Martinez, M

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2010/050828

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2907292 A	18-04-2008	AT 467966 T	15-05-2010
		EP 2092703 A1	26-08-2009
		WO 2008047024 A1	24-04-2008
US 2007073817 A1	29-03-2007	AUCUN	
US 2004181585 A1	16-09-2004	US 2009193093 A1	30-07-2009