

(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
15 avril 2004 (15.04.2004)

PCT

(10) Numéro de publication internationale
WO 2004/032430 A2

(51) Classification internationale des brevets⁷ : **H04L 12/56**

(21) Numéro de la demande internationale :
PCT/FR2003/002808

(22) Date de dépôt international :
24 septembre 2003 (24.09.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/12132 1 octobre 2002 (01.10.2002) FR

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

(72) Inventeurs; et

(75) Inventeurs/Déposants (*pour US seulement*) : **AL-LAIN, Mickael** [FR/FR]; 18A, rue des Cordiers, Appt. F6, F-22300 Lannion (FR). **ZOUGHAMI, Yacine** [FR/FR]; 6 bis, rue Croas Oges, F-22300 Ploumillau (FR). **L'HOSTIS, Michel** [FR/FR]; 18, rue Neuve, F-22310 Plestin les Grèves (FR).

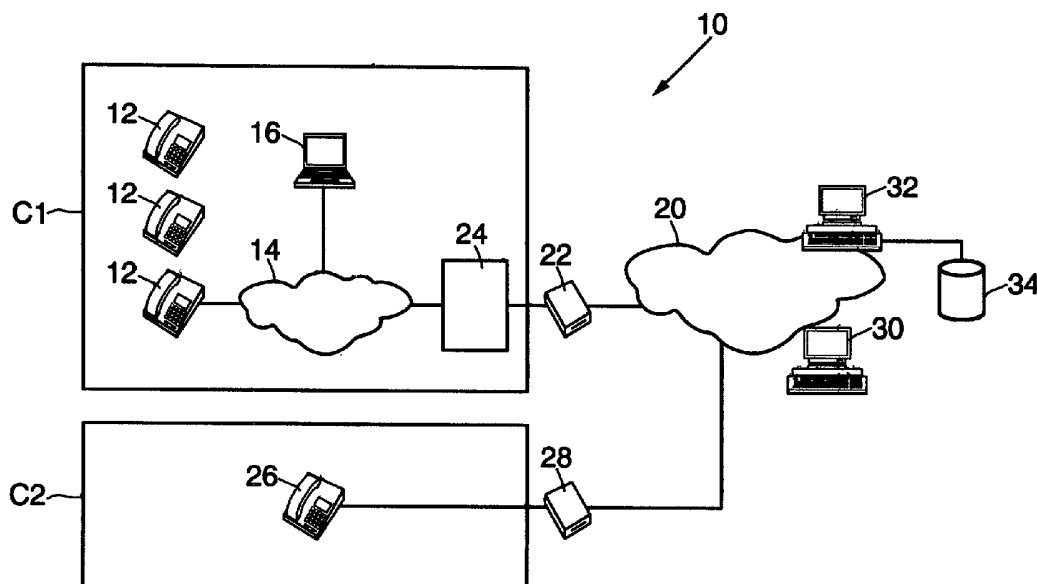
(74) Mandataire : **BUREAU D.A. CASALONGA-JOSSE**; 8, avenue Percier, F-75008 Paris (FR).

(81) États désignés (*national*) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[Suite sur la page suivante]

(54) Title: METHOD AND INSTALLATION FOR CONTROLLING A TELEPHONE CALL TRANSMITTER ON AN INTERNET NETWORK AND TELEPHONE TERMINAL THEREFOR

(54) Titre : PROCÉDE ET INSTALLATION DE CONTROLE DE L'IDENTITE DE L'EMETTEUR D'UN APPEL TELEPHONIQUE SUR UN RESEAU INTERNET ET TERMINAL DE TELEPHONIE POUR UNE TELLE INSTALLATION



(57) Abstract: The invention concerns a method for controlling the transmitter of a telephone call on an Internet network, which consists in : inserting an encrypted control code in the field of a frame requesting communication setup, the code containing parameters concerning the identity of a telecommunication terminal (12, 26) from which the telephone call is transmitted, decrypting by means of a remote call management server (32) the decrypted control code with corresponding data stored in a database (34) hosted in the server, and setting up the call based on the result of the comparison.

[Suite sur la page suivante]

WO 2004/032430 A2



SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés (régional)** : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— sans rapport de recherche internationale, sera republiée dès réception de ce rapport

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) **Abrégé :** Pour contrôler l'identité de l'émetteur d'un appel téléphonique sur une réseau Internet, on insère un code de contrôle crypté dans un champ d'une trame de demande d'établissement de communication, le code contenant des paramètres portant sur l'identité d'un terminal de télécommunication (12 ; 26) à partir duquel l'appel téléphonique est émis, on décrypte au moyen d'un serveur de gestion d'appels (32) distant le code de contrôle décrypté avec des informations correspondantes stockées dans une base de données (34) hébergée dans le serveur, et l'on établit l'appel en fonction du résultat de la comparaison.

Procédé et installation de contrôle de l'identité de l'émetteur d'un appel téléphonique sur un réseau Internet et terminal de téléphonie pour une telle installation.

5 L'invention concerne le domaine de la téléphonie sur Internet. Elle s'applique à tous les protocoles VoIP de voix sur Internet ("Voice over IP, en anglais"), tel que le protocole issu de l'Union des Télécommunications Internationales (ITU), connu sous l'appellation H.323, le protocole SIP (Session Initiation Protocol) issu de
10 l'IETF, ..., ainsi qu'à tous les types d'architectures de réseau de téléphonie résidentiel ou d'entreprise.

De manière conventionnelle, les services de téléphonie sur Internet mettent en œuvre un certain nombre de mécanismes d'authentification de l'abonné appelant afin d'éviter, notamment, que
15 des appels passés par des tiers non autorisés lui soient facturés.

Ces techniques d'authentification peuvent consister en des mécanismes de chiffrement par cryptographie asymétrique, qui utilisent un échange de certificat par clés publiques et clés privées. Cette technique repose sur des fonctions mathématiques à sens unique, c'est-à-dire des fonctions faciles à calculer mais extrêmement
20 difficiles à inverser. L'abonné détient une clé privée. Il divulgue une clé publique à son interlocuteur. Bien que la clé privée et la clé publique de l'abonné soient étroitement liées, la divulgation de la clé publique ne fournit aucun renseignement concernant la clé privée. La
25 connaissance de la clé publique de l'abonné permet notamment à un interlocuteur distant de chiffrer un message destiné à l'abonné.

Un autre mécanisme d'authentification de l'abonné est basé sur l'utilisation d'un identifiant et d'un mot de passe. Ainsi, pour établir une communication, il est nécessaire de fournir un identifiant et un
30 mot de passe. Si ceux-ci sont reconnus par un serveur d'appels de l'opérateur, alors l'établissement d'une communication devient possible.

Ces mécanismes d'authentification sont relativement faciles à mettre en œuvre avec des téléphones logiciels. Cependant, il n'en va pas de même pour des terminaux téléphoniques utilisés dans des réseaux internet. En effet, ces terminaux ne présentent pas tous la possibilité de saisir un mot de passe ou de mettre en œuvre le chiffrement par cryptographie asymétrique.

En outre, la cryptographie asymétrique nécessite, pour être réellement efficace, d'obtenir un certificat auprès d'un organisme certifié, ce qui est difficilement compatible avec un déploiement d'un service de voix sur Internet à grande échelle, c'est-à-dire pour plusieurs millions d'abonnés.

Le but de l'invention est donc de pallier ces inconvénients et de fournir un procédé et une installation de contrôle de l'identité d'un émetteur d'un appel téléphonique sur un réseau Internet, permettant de contrôler l'identité d'un émetteur utilisant un terminal téléphonique de type VoIP, c'est-à-dire un terminal de téléphonie sur internet, et qui soit compatible avec un développement de la téléphonie Internet à très grande échelle.

Ainsi, selon l'invention, il est proposé un procédé de contrôle de l'identité d'un émetteur d'un appel téléphonique sur un réseau Internet comprenant les étapes suivantes :

- insertion d'un code de contrôle crypté dans un champ d'une trame de demande d'un établissement de communication, le code contenant des paramètres portant sur l'identité d'un terminal de télécommunication à partir duquel l'appel téléphonique est émis ;
- décryptage, par un serveur de gestion d'appels distant, du code de contrôle ;
- comparaison d'au moins un paramètre extrait du code de contrôle décrypté avec des informations correspondantes stockées dans une base de données hébergée dans le serveur ; et
- établissement de l'appel en fonction du résultat de ladite comparaison.

Selon une autre caractéristique de ce procédé, celui-ci comporte en outre une étape de comparaison de paramètres extraits du code de contrôle décrypté avec des informations correspondantes extraites de la trame de demande d'établissement d'appels.

5 Ces informations, qui sont stockées dans la base de données, comportent, selon encore une autre caractéristique de ce procédé, une adresse d'identification du terminal.

Par exemple, les informations sont transférées du terminal vers la base de données lors d'un premier appel émis par le terminal. Ce
10 premier appel peut être constitué par un appel émis immédiatement après l'installation du terminal de téléphonie de l'abonné.

Selon un mode de mise en œuvre particulier, les paramètres extraits de la trame de demande d'établissement d'appel comportent l'adresse IP du terminal et le numéro d'appel du terminal. Ainsi, le
15 code de contrôle peut être élaboré à partir d'une fonction cryptée de l'adresse d'identification du terminal et de l'adresse IP de ce dernier.

En ce qui concerne l'adresse IP du terminal, celle-ci est transmise par un fournisseur d'accès à un réseau Internet, à un module de contrôle associé au terminal.

20 Selon une autre configuration du réseau de télécommunications mettant en œuvre un procédé selon l'invention, les paramètres extraits de la trame de demande d'établissement d'appel comportent l'adresse IP d'une passerelle de raccordement d'un réseau privé à un réseau de télécommunication et le numéro d'appel du terminal.

25 Le code de contrôle est alors élaboré à partir d'une fonction cryptée de l'adresse d'identification du terminal et de l'adresse IP de la passerelle.

L'adresse IP du terminal est transmise, selon cette variante de configuration, par un fournisseur d'accès à un réseau Internet, à
30 module de contrôle associé à la passerelle.

Selon l'invention, il est également proposé une installation de contrôle de l'identité de l'émetteur d'un appel téléphonique sur un réseau Internet, comprenant un serveur de gestion d'appels adapté pour provoquer l'établissement d'une communication entre des terminaux de

télécommunication respectivement appelant et appelé, en fonction de paramètres contenus dans une trame de demande d'établissement de communication émise par le terminal appelant.

5 Le serveur de gestion comporte des moyens de décryptage d'un code de contrôle crypté inséré dans la trame de demande d'établissement de communication, le code contenant des paramètres portant sur l'identité du terminal de télécommunication appelant, et des moyens de comparaison d'au moins un paramètre extrait du code de contrôle décrypté par les moyens de décryptage avec un code
10 correspondant stocké dans une base de données hébergée dans le serveur pour autoriser l'établissement de la communication en fonction du résultat de la comparaison.

Selon une autre caractéristique de l'invention, l'installation comporte en outre des moyens de comparaison de paramètres extraits
15 du code de contrôle décrypté avec des informations correspondantes extraites de la trame de demande d'établissement d'appel.

Enfin, selon l'invention, il est proposé un terminal de télécommunication pour installation de contrôle tel que défini ci-dessus, caractérisé en ce qu'il comporte un module de contrôle adapté
20 pour l'insertion d'un code de contrôle crypté dans une trame de demande d'établissement de communication.

Ce module de contrôle comporte des moyens pour l'élaboration d'une fonction cryptée de l'adresse d'identification du terminal et de l'adresse IP du terminal.

25 En variante, le module de contrôle comporte des moyens pour l'élaboration d'une fonction cryptée de l'adresse d'identification du terminal et de l'adresse IP d'une passerelle de raccordement d'un réseau local à un réseau de télécommunication public.

30 D'autres buts, caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante, donnée uniquement à titre d'exemple non limitatif, et faite en référence aux dessins annexés sur lesquels :

- la figure 1 illustre schématiquement la structure d'un réseau de télécommunication permettant d'accéder à un service de téléphonie

Internet, pourvu d'une installation de contrôle d'un émetteur d'un appel téléphonique et permettant de mettre en œuvre un procédé de contrôle conforme à l'invention ;

5 - la figure 2 est une vue de détail d'une portion du réseau de la figure 1, illustrant une séquence de demande d'établissement d'appel ; et

- la figure 3 est un organigramme illustrant les principales phases du procédé de contrôle conforme à l'invention.

10 Sur la figure 1, on a représenté l'architecture générale d'un réseau 10 de télécommunication permettant l'accès à un service de téléphonie sur Internet.

15 Comme on le voit sur cette figure, le réseau comporte, côté abonné, un ensemble d'équipements utilisables par des abonnés pour l'établissement de communications téléphoniques avec des abonnés distants.

Sur la figure 1, deux configurations distinctes ont été représentées, à savoir une configuration C1 et une configuration C2.

20 La première configuration C1 est agencée autour d'un réseau local privé, ou réseau LAN. Elle comporte un ensemble de terminaux de télécommunication 12, par exemple constitués par des téléphones VoIP, raccordés au réseau LAN 14. Des terminaux informatiques, tels que 16, constitués part exemple par des micro-ordinateurs, peuvent également être raccordés au réseau 14, comme cela est conventionnel dans un réseau informatique privé.

25 Une passerelle 24 assure l'interconnexion du réseau privé, et en particulier du réseau LAN 14 à un réseau public 20 d'un opérateur de télécommunication fournissant un service de téléphonie VoIP, par l'intermédiaire d'un modem 22.

30 La passerelle comporte un module de contrôle assurant, comme cela sera décrit en détail par la suite, un contrôle de l'identité de l'émetteur d'un appel téléphonique, c'est-à-dire un module capable de contrôler qu'aucune tentative d'usurpation du numéro d'appel du réseau local LAN n'a été faite par des tiers.

En ce qui concerne la deuxième configuration C2, qui correspond à une installation privée d'un abonné particulièrement adaptée pour être prévue dans des locaux d'habitation, les équipements de téléphonie sont constitués par des terminaux de télécommunication, tels que 26, auxquels est intégré le module de contrôle. Chaque terminal 26 communique avec le réseau public de l'opérateur 20 par l'intermédiaire d'un modem 28.

Du côté fournisseur de service, le réseau comporte, d'une part, un serveur 30 fournisseur d'accès au réseau Internet et, d'autre part, un serveur d'appels 32 qui exerce, conjointement avec les modules de contrôle, un contrôle de l'identité de l'émetteur d'un appel et qui établit des communications téléphoniques pour un abonné appelant en fonction du résultat du contrôle de l'émetteur et en fonction d'une configuration de services proposés par l'opérateur.

Le serveur d'appels 32 ainsi que le module de contrôle de la passerelle (configuration C1) ou des terminaux (configuration C2) comportent tous les moyens matériels et logiciels permettant de contrôler l'identité de l'émetteur d'un appel afin de vérifier qu'un numéro d'abonné n'a pas été usurpé par un tiers, comme cela sera décrit en détail par la suite.

On voit en particulier sur la figure 1 que le serveur d'appel 32 est associé à une base de données 34 dans laquelle sont chargées des informations relatives aux abonnés, telles que l'adresse d'identification du terminal, également connue sous l'appellation "adresse MAC".

Comme cela est connu en soi, de telles informations sont chargées en mémoire dans chaque terminal 12, lors de leur fabrication. Elles sont transférées dans la base de données 34, sous le contrôle du serveur d'appels 32, lors du premier appel effectué à partir de chaque terminal, c'est-à-dire juste après l'installation du terminal d'un abonné.

Par ailleurs, le serveur fournisseur d'accès Internet 30 transmet au module de contrôle de la passerelle 24 ou au terminal 26, dans le cas où le module est intégré dans ce dernier, une adresse IP publique, et ce, à chaque fois que cette adresse est modifiée.

Comme cela est connu en soi, pour l'établissement d'une communication VoIP sur le réseau Internet 20 à partir d'un terminal tel que 12, ce terminal élabore puis transmet au serveur d'appel 32 une trame de demande d'établissement d'appel. Cette trame comporte un ensemble de champs véhiculant chacun des informations nécessaires à l'établissement de la communication, telles que l'adresse IP du terminal appelant ou l'adresse IP de la passerelle, et le numéro de l'appelant et de l'appelé.

Afin de contrôler l'absence d'usurpation du numéro de l'abonné appelant, le module de contrôle 24 insère dans la trame de demande d'établissement d'appel un message crypté élaboré à partir de l'adresse MAC d'identification du terminal et de l'adresse IP de la passerelle, en ce qui concerne la première configuration C1, ou du terminal, en ce qui concerne la configuration C2.

Comme indiqué précédemment, la trame de demande d'établissement d'appel véhicule en clair, c'est-à-dire de manière non cryptée, l'adresse IP du terminal ou de la passerelle. En ce qui concerne l'adresse MAC d'identification du terminal, celle-ci est également stockée dans la base de données 34 associée au serveur d'appels 32.

Ainsi, pour procéder au contrôle de l'identité de l'émetteur de l'appel, le serveur d'appels 32 procède à un décryptage du code de contrôle inséré dans la trame, à une récupération du code MAC d'identification et de l'adresse IP de la passerelle ou du terminal appelant, puis, à une comparaison, d'une part, de l'adresse MAC récupérée à partir de la trame émise par le terminal appelant avec l'adresse MAC correspondante stockée dans la base de données 34 et, d'autre part, de l'adresse IP issue du décryptage du code de contrôle avec l'adresse IP véhiculée en clair par la trame. En cas de correspondance entre ces données, l'appel est autorisé.

On va maintenant décrire de manière détaillée, en référence à la figure 2 sur laquelle les principaux éléments du réseau ont été repris et sur laquelle on a représenté les flux de données par des flèches, les principales phases d'une séquence de demande d'établissement d'appel.

Comme indiqué précédemment, la demande d'appel débute par une première phase 36 au cours de laquelle le terminal 12 transmet au module de contrôle la trame de demande d'établissement d'appel. Celui-ci procède à un paramétrage d'un champ spécifique de la trame du code de contrôle. Par exemple, en utilisant la norme H.323, le module de contrôle 24 insère dans le champ "h323id" une fonction cryptée de l'adresse MAC du téléphone IP et de l'adresse IP du module de contrôle. La trame est alors transmise vers le serveur d'appels 32 (étape 38). Celui-ci comporte un portier 40, lequel partage avec le module de contrôle une bibliothèque de liens dynamiques ou DLL de manière à procéder à un décryptage du code de contrôle.

On notera que le cryptage réalisé par le module de contrôle peut être réalisé par tout type de cryptage de type classique. Les techniques de cryptage pouvant être utilisées dans le cadre de la présente description sont à la portée d'un homme du métier et ne seront donc pas décrites en détail par la suite.

Après décryptage, le serveur de gestion d'appels 32 met en œuvre un logiciel de service 44 (étape 41), lequel procède au contrôle proprement dit de l'émetteur de l'appel de manière à autoriser l'établissement de la communication en cas de correspondance entre les données véhiculées par le code de contrôle et les données stockées dans la base de données 34, d'une part, et les données véhiculées en clair par la trame de demande d'établissement de communication, d'autre part. Le logiciel de service transmet alors le résultat du traitement au portier (étape 42). Des instructions aptes à autoriser un appel peuvent alors être transmises au module de contrôle (étape 43) et au terminal (étape 45) en cas d'absence de tentative de fraude.

Plus particulièrement, en se référant à la figure 3, pour procéder au contrôle de l'identité de l'émetteur de l'appel, lors d'une première étape 46, il est procédé à une vérification de la fonction de contrôle. Dans le cas où cette fonction est inactivée, la communication est autorisée (étape 47).

Dans le cas contraire, c'est-à-dire si la fonction de contrôle est activée, lors de l'étape 48 suivante, le serveur d'appels procède à un

décryptage du code de contrôle, c'est-à-dire, lorsque la norme H.323 est utilisée, à un décryptage du champ h323id de manière à extraire l'adresse d'identification du terminal et l'adresse IP de ce terminal ou de l'adresse IP de la passerelle. Lors de l'étape 49 suivante, le serveur d'appels et en particulier le logiciel de services procède à une comparaison de l'adresse IP extraite du code de contrôle avec l'adresse IP véhiculée en clair par la trame de demande d'établissement d'appel. Dans le cas où ces adresses ne correspondent pas, la demande d'appel est rejetée (étape 50).

En cas de correspondance entre ces adresses IP, lors de l'étape 52 suivante, le serveur d'appels 32 vérifie si une adresse MAC est présente dans la base de données.

Si l'adresse MAC n'est pas présente, ce qui traduit le fait que la ligne vient d'être établie, l'adresse MAC obtenue à l'issue du décryptage est stockée dans la base de données (étape 54) et l'appel est autorisé.

Au contraire, dans le cas où il existe une adresse MAC dans la base 34, le serveur d'appels 32 procède à une comparaison de cette adresse MAC avec l'adresse MAC issue du décryptage. En cas de correspondance entre ces adresses, l'appel est autorisé (étape 47). Dans le cas contraire, l'appel est rejeté.

Ainsi, au niveau du serveur d'appels, après décryptage, le logiciel de services vérifie que l'adresse IP du module de contrôle est correcte. Un utilisateur, abonné ou non, récupérant une adresse IP d'un abonné pour passer des communications, ne pourra établir une communication. En effet, après décryptage du code de contrôle, l'adresse IP ne correspondra pas à celle de la ligne à partir de laquelle l'appel est émis.

Par ailleurs, le logiciel de services vérifie que l'adresse MAC du terminal à partir duquel l'appel est émis correspond à l'adresse MAC du terminal enregistrée dans la base de données 34. On vérifie ainsi que le terminal à partir duquel la tentative d'appel est faite correspond bien au terminal associé à la ligne

Ainsi, comme on le conçoit, selon l'invention, on procède, d'une part, à un contrôle de la ligne et, d'autre part, à un contrôle du terminal à partir duquel un appel est émis.

REVENDEICATIONS

1. Procédé de contrôle de l'identité d'un émetteur d'un appel téléphonique sur un réseau Internet, caractérisé en ce qu'il comprend les étapes suivantes :

- 5 - insertion d'un code de contrôle crypté dans un champ d'une trame de demande d'établissement de communication, le code contenant des paramètres portant sur l'identité d'un terminal de télécommunication à partir duquel l'appel téléphonique est émis ;
- décryptage, par un serveur (32) de gestion d'appels distant, du code de contrôle ;
- 10 - comparaison d'au moins un paramètre extrait du code de contrôle décrypté avec des informations correspondantes stockées dans une base de données (34) hébergée dans le serveur ; et
- établissement de l'appel en fonction du résultat de ladite comparaison.

15 2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte en outre une étape de comparaison de paramètres extraits du code de contrôle décrypté avec des informations correspondantes extraites de la trame de demande d'établissement d'appel.

20 3. Procédé selon l'une des revendications 1 et 2, caractérisé en ce que les informations stockées dans la base de données comportent une adresse d'identification du terminal (12 ; 26).

 4. Procédé selon la revendication 3, caractérisé en ce que lesdites informations sont transférées du terminal vers la base de données (34) lors d'un premier appel émis par le terminal (12 ; 26).

25 5. Procédé selon l'une quelconque des revendications 2 à 4, caractérisé en ce que les paramètres extraits de la trame de demande d'établissement d'appel comportent l'adresse IP du terminal et le numéro d'appel du terminal.

30 6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que le code de contrôle est élaboré à partir d'une fonction cryptée de l'adresse d'identification du terminal (MAC) et de l'adresse IP du terminal.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que l'adresse IP du terminal est transmise, par un fournisseur d'accès (30) à un réseau Internet, à module de contrôle (24) associé au terminal.

5 8. Procédé selon l'une quelconque des revendications 2 à 4, caractérisé en ce que les paramètres extraits de la trame de demande d'établissement d'appel comportent l'adresse IP d'une passerelle (24) de raccordement d'un réseau privé (14) à un réseau (20) de télécommunication et le numéro d'appel du terminal.

10 9. Procédé selon la revendication 8, caractérisé en ce que le code de contrôle est élaboré à partir d'une fonction cryptée de l'adresse d'identification du terminal (MAC) et de l'adresse IP de la passerelle.

15 10. Procédé selon l'une des revendications 8 et 9, caractérisé en ce que l'adresse IP du terminal est transmise, par un fournisseur d'accès (30) à un réseau Internet, à module de contrôle (24) associé à la passerelle.

20 11. Installation de contrôle de l'identité d'un émetteur d'un appel téléphonique sur un réseau Internet, comprenant un serveur (32) de gestion d'appels adapté pour provoquer l'établissement d'une communication entre des terminaux de télécommunication respectivement appelant et appelé en fonction de paramètres contenus dans une trame de demande d'établissement de communication émise par le terminal appelant (12 ; 26), caractérisée en ce que le serveur de
25 gestion (32) comporte des moyens de décryptage d'un code de contrôle crypté inséré dans la trame de demande d'établissement de communication, le code contenant des paramètres portant sur l'identité du terminal de télécommunication appelant, et des moyens de comparaison d'au moins un paramètre extrait du code de contrôle
30 décrypté par les moyens de décryptage avec un code correspondant stocké dans une base de données (34) hébergée dans le serveur pour autoriser l'établissement de la communication en fonction du résultat de la comparaison.

5 12. Installation selon la revendication 11, caractérisée en ce qu'elle comporte en outre des moyens (32) de comparaison de paramètres extraits du code de contrôle décrypté avec des informations correspondantes extraites de la trame de demande d'établissement d'appel.

10 13. Terminal de télécommunication pour installation de contrôle selon l'une des revendications 11 et 12, caractérisé en ce qu'il comporte un module de contrôle adapté pour l'insertion d'un code de contrôle crypté dans une trame de demande d'établissement de communication.

14. Terminal selon la revendication 13, caractérisé en ce que le module de contrôle comporte des moyens pour l'élaboration d'une fonction cryptée de l'adresse d'identification du terminal et de l'adresse IP du terminal.

15 15. Terminal selon la revendication 13, caractérisé en ce que le module de contrôle comporte des moyens pour l'élaboration d'une fonction cryptée de l'adresse d'identification du terminal et de l'adresse IP d'une passerelle (24) de raccordement d'un réseau local (14) à un réseau de télécommunication public (20).

FIG.1

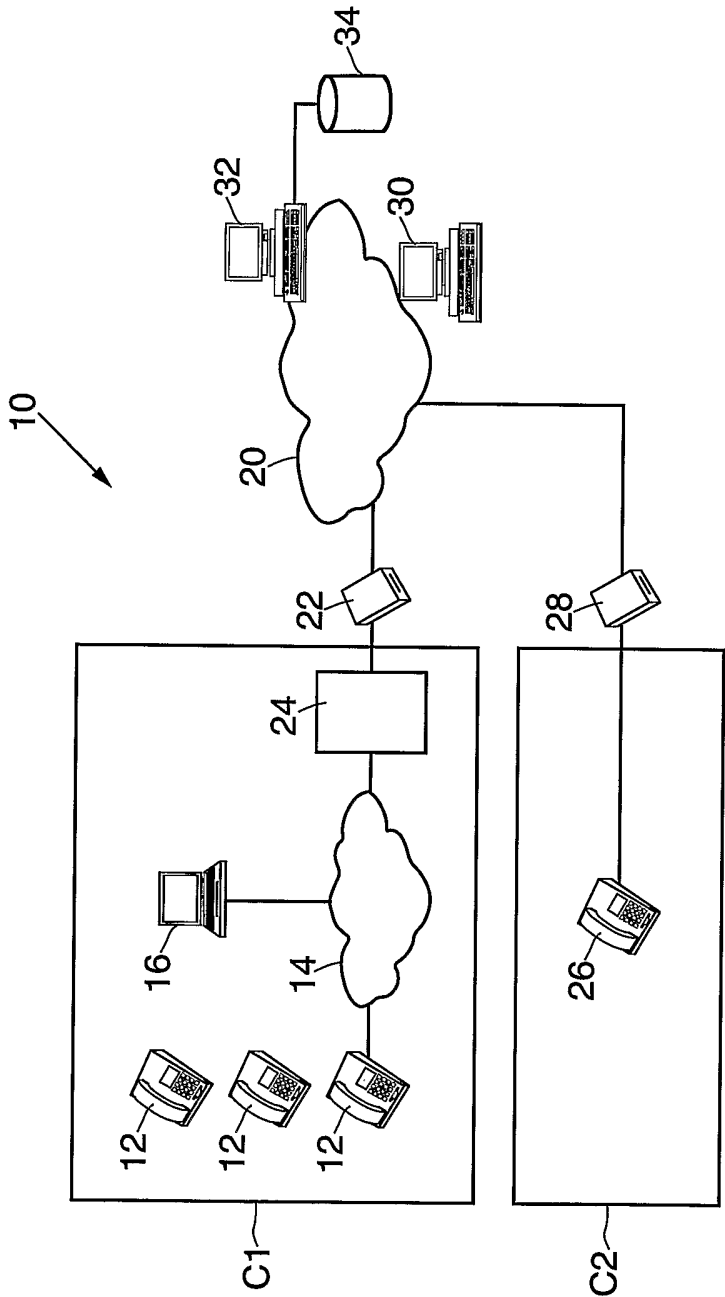
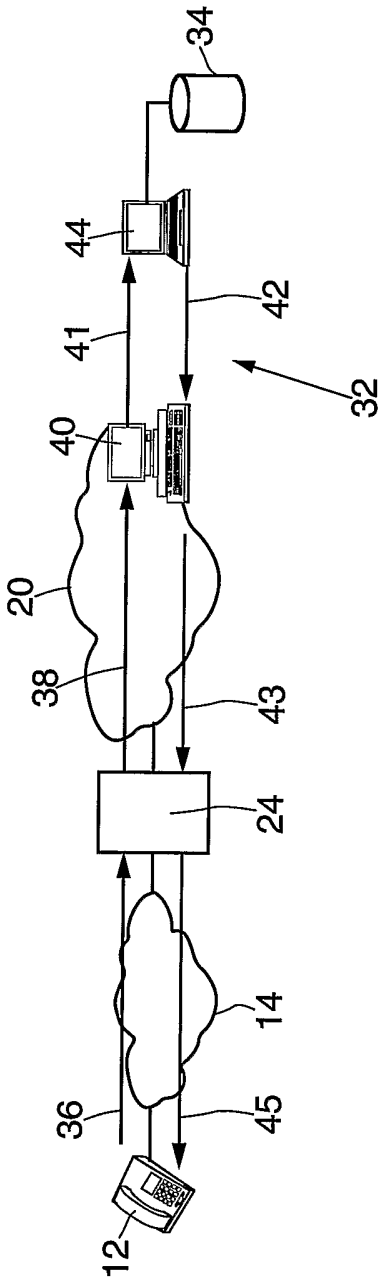


FIG.2



3/3

FIG.3