



(12) BREVET D'INVENTION

- (11) N° de publication : **MA 27314 A1** (51) Cl. internationale : **H04M 3/24; H04L 29/12**
- (43) Date de publication : **02.05.2005**

-
- (21) N° Dépôt : **28029**
- (22) Date de Dépôt : **30.12.2004**
- (30) Données de Priorité : **28.06.2002 FR 02/08170**
- (86) Données relatives à la demande internationale selon le PCT: **PCT/FR2003/001975 26.06.2003**
- (71) Demandeur(s) : **SCHLUMBERGER PAYPHONES SAS, 50, AVENUE JEAN JAURES BP 369, F-92120 MONTROUGE CEDEX (FR)**
- (72) Inventeur(s) : **GRUNENWALD, Rodolphe ; VU VAN, Yolaine**
- (74) Mandataire : **TMP AGENTS**

-
- (54) Titre : **PROCEDE D'INDIVIDUALISATION D'UN TERMINAL RELIE A AU MOINS UN SERVEUR A TRAVERS UN RESEAU**
- (57) Abrégé : Le procédé d'individualisation d'un terminal (10) relié à au moins un serveur (5) à travers un réseau (2) comprend les étapes suivantes: a) au niveau du terminal (10), établir une session de connexion (20) avec le serveur (5), et b) au niveau du serveur (5), traiter la session de connexion selon un mode opératoire choisi. Le mode opératoire comprend les étapes suivantes: c) au niveau du serveur (5), en cas de demande de service du terminal incluse dans la session de connexion, générer un certificat (ESN) unique associé audit terminal (10), et communiquer ledit certificat audit terminal; d) au niveau du terminal (10), recevoir et stocker ledit certificat (ESN); et e) au niveau du serveur (5), valider la demande de service avec le terminal ainsi individualisé de manière unique.

Abrégé

Le procédé d'individualisation d'un terminal (10) relié à au moins un serveur (5) à travers un réseau (2) comprend les étapes suivantes: a) au niveau du terminal (10), établir une session de connexion (20) avec le serveur (5), et b) au niveau du serveur (5), traiter la session de connexion selon un mode opératoire choisi. Le mode opératoire comprend les étapes suivantes: c) au niveau du serveur (5), en cas de demande de service du terminal incluse dans la session de connexion, générer un certificat (ESN) unique associé audit terminal (10), et communiquer ledit certificat audit terminal; d) au niveau du terminal (10), recevoir et stocker ledit certificat (ESN); et e) au niveau du serveur (5), valider la demande de service avec le terminal ainsi individualisé de manière unique.

**PROCEDE D'INDIVIDUALISATION D'UN TERMINAL RELIE A AU
MOINS UN SERVEUR A TRAVERS UN RESEAU**

La présente invention concerne un procédé d'individualisation d'un
5 terminal relié à au moins un serveur à travers un réseau, un terminal et
un serveur adaptés à la mise en œuvre dudit procédé.

Elle trouve une application générale dans la gestion de terminaux de
service, et plus particulièrement de terminaux de communication tels
10 que des téléphones publics.

D'une manière générale, un réseau de téléphonie publique se compose
de téléphones publics répartis sur un territoire donné. Les téléphones
publics sont connectés à un réseau de communication, constitué par
15 exemple par le réseau téléphonique commuté PSTN (acronyme anglo-
saxon pour Public Switching Telephone Network), avec lequel il
communique au moyen d'un modem.

Un réseau de téléphonie publique comporte généralement un ou
20 plusieurs ordinateurs centraux ou serveurs de gestion, souvent appelés
serveurs PMS (acronyme du terme anglo-saxon Payphone Management
System), permettant à l'opérateur du réseau d'opérer la supervision des
différents téléphones de son réseau.

25 Ce serveur PMS, raccordé au réseau téléphonique commuté via un
routeur, a pour fonction d'échanger avec le parc de téléphones des
informations relatives au fonctionnement du système de téléphonie.

En pratique, le serveur PMS a pour fonction d'opérer le téléchargement
30 des mises à jour des programmes faisant fonctionner les circuits des
téléphones publics, mises à jour corrigeant d'éventuelles erreurs

détectées dans les programmes déjà en place ou bien encore introduisant de nouvelles prestations pour les usagers.

De plus, le serveur PMS a pour fonction de recevoir des rapports
5 émanant de chaque téléphone, notamment des rapports d'alarme ou bien des statistiques de facturation.

Deux téléphones, installés physiquement à deux endroits différents, peuvent être initialisés sur site (par un agent de surveillance et/ou de
10 service) avec le même numéro de téléphone, rendu possible par la saisie dudit numéro par l'agent de maintenance via un programme de maintenance disponibles dans le téléphone public.

Dans ce cas, le serveur PMS ne peut correctement traiter les rapports
15 émanant des deux téléphones distincts puisqu'ils sont considérés par erreur selon le numéro de téléphone associé comme provenant d'un seul et même téléphone. Dès lors apparaissent des doublons d'informations voire des cumuls erronés de données tels le nombre de taxe grillées, le nombre d'appels réalisés etc. gênant l'optimisation et le
20 calcul de rentabilité d'un ensemble de téléphones.

De même, le serveur PMS est dans l'incapacité de localiser à distance un téléphone dont l'initialisation est incorrectement mise en place sur
site par un agent de surveillance et/ou de service.

25

La présente invention remédie à ces inconvénients.

Elle porte sur un procédé d'individualisation d'un terminal relié à au moins un serveur de type PMS à travers un réseau, du type réseau
30 commuté comprenant les étapes suivantes :

- a) au niveau du terminal, établir une session de connexion avec le serveur, et
- b) au niveau du serveur, recevoir et traiter la session de connexion
5 selon un mode opératoire choisi.

Selon une définition générale de l'invention, le mode opératoire comprend les étapes suivantes :

- 10 c) au niveau du serveur, en cas de demande de service du terminal incluse dans la session de connexion, générer un certificat, baptisé ESN (pour Electronic Serial Number), unique associé audit terminal, et communiquer ledit certificat audit terminal. Cette demande de service ne pourra être qu'une demande d'initialisation ;
- 15 d) au niveau du terminal, recevoir et stocker ledit certificat dans ses mémoires internes; et
- e) au niveau du serveur, valider la demande de service du terminal
20 ainsi individualisé de manière unique.

Ainsi, un certificat unique est envoyé au terminal lors de certaines sessions de connexion correspondant à une demande de service prédéterminée.

25

En pratique la demande de service est du type initialisation.

Ce certificat permet de garantir l'absence de doublon ou duplicata dans les tables du serveur, ce qui permet un traitement correct des rapports
30 émanant de chaque terminal.

Avantageusement, le certificat est stocké au niveau du dès sa génération pour être soit transmis au terminal lors d'une session d'initialisation, soit contrôlé pour tout autre type de session (téléchargement, appel journalier, appel pour alarme...).

5

A ce stade deux points fondamentaux de l'invention sont à préciser :

- Au moment du démarrage initial d'un serveur de type PMS un certificat (ESN) source est généré codé sur 8 octets. Ce nombre aléatoire est propre et unique à chaque PMS. Cela garantit l'unicité des nombres générés sur chaque serveur spécialement en cas d'un système cascasant plusieurs serveurs PMS.
- Partant de ce nombre « racine », les certificats suivants générés se feront par incrément de 1 puis distribués terminal par terminal et enfin stockés dans les tables du serveur.
- Si dans toutes les sessions d'appels (téléchargement, appel journalier, appel pour alarme...) le certificat (ESN) est contrôlé, il sera généré lors des sessions d'initialisation uniquement dans les cas suivants :
 1. Si l'opérateur a autorisé de manière globale (tous les terminaux) l'initialisation desdits terminaux par choix d'une option via son interface homme machine,
 2. Si l'opérateur a autorisé de manière unique (un ou plusieurs terminaux) l'initialisation desdits terminaux par choix d'une option via son interface homme machine,
 3. Ce principe, évitera avantageusement les réinitialisations accidentelles (non autorisées) de terminaux existants.

10

15

20

25

Le tableau ci-dessous résumera les points ci-dessus :

PMS réinitialisation globale autorisée ?	PMS réinitialisation partielle autorisée ?	ESN généré ou contrôlé ?	Résultat
Non	Non	Contrôlé	Réinitialisation

			lancé si ESN présenté correct. Pas de génération d'un nouvel ESN
Non	Oui	Généré	Réinitialisation et renvoi d'un nouvel ESN
Oui	Oui ou Non	Généré	Réinitialisation et renvoi d'un nouvel ESN

Le PMS est équipé pour ce faire, d'une fonction autorisant :

- La génération d'un certificat (ESN) source au moment du démarrage du serveur PMS et son stockage dans ses tables,
- L'incrément de 1, puis le stockage de chaque ESN généré, transmis aux terminaux à la suite d'une demande d'initialisation,
- Le contrôle de tout certificat (ESN) dans toutes les sessions possibles émanant de terminaux,
- La possibilité de débrayer au besoin, de manière globale, le contrôle du certificat (ESN),
- La régénération d'un certificat (ESN) sur demande lors d'une nouvelle demande d'initialisation.

Selon un mode de réalisation préféré, le certificat source est un nombre aléatoire. Il servira de nombre de base à la génération des certificats suivants (ESN) par incrément successif de 1.

La présente invention a également pour objet une installation, un terminal et un serveur pour la mise en œuvre du procédé selon l'invention.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lumière de la description détaillée ci-après et des dessins dans lesquels :

- 5 - La figure 1 est une vue schématique d'un réseau de téléphonie publique utilisé pour la mise en œuvre du procédé selon l'invention ;
 - La figure 2 est un organigramme illustrant les étapes du procédé
10 selon l'invention ; et
 - La figure 3 est un schéma illustrant le mode opératoire selon l'invention.
- 15 Sur la figure 1, la référence 1 désigne un réseau 1 de téléphonie publique, comprenant un parc de téléphones publics 10.

Les téléphones 10 sont destinés à être utilisés par les usagers en libre service et sont donc installés à cette fin dans des lieux publics, tels que
20 les rues ou semi-publics, tels que les centres commerciaux, les aéroports, halls d'hôtels, restaurants, magasins, etc.

Ces téléphones 10 permettent aux usagers d'effectuer des communications téléphoniques, en utilisant un réseau téléphonique
25 approprié référencé 2.

Ce réseau téléphonique 2 est du type commuté analogique PSTN (Public Switching Telephone Network) ou du type numérique ISDN (Integrated Services Digital Network).

30

Ce réseau 2 peut également être constitué par un réseau de radiotéléphonie mobile et ce quelle que soit sa nature : GSM, CDMA,

TDMA, AMPS, D-AMPS, GPRS, ou encore par le réseau Internet ou plus généralement par tous réseaux de communication aptes à transmettre des données ainsi que par toutes combinaisons de tels réseaux.

- 5 Ces téléphones publics 10 peuvent également être adaptés pour accéder à des serveurs d'informations ou de fournitures de services du Web et de l'Internet, ainsi qu'à des serveurs d'informations ou de fournitures de services résidant sur des réseaux privés.
- 10 De tels accès permettent à l'opérateur exploitant le réseau 1, de proposer aux usagers une large palette de services, allant par exemple, et à titre non limitatif, de la lecture de leur courrier électronique à la consultation d'informations locales.
- 15 Ces téléphones publics 10 sont adaptés pour communiquer avec un serveur 5, encore appelé PMS dédié au fonctionnement et à la gestion du réseau de téléphonie publique 1.

Le serveur PMS 5 a pour fonction d'échanger avec le parc de téléphones
20 publics 10 des informations concernant leur fonctionnement et plus généralement le fonctionnement du système de téléphonie publique.

En particulier, le serveur PMS 5 gère les sessions d'initialisation des
25 téléphones publics et établit des données statistiques à partir des informations reçues des téléphones publics 10 (alarmes, compteurs d'exploitation).

Les téléphones publics 10 et les PMS 5 sont munis de moyens
appropriés de supervision et de réception / émission d'informations.

30

Ces moyens d'organisation et de réception / émission sont chargés d'organiser les échanges d'informations entre les téléphones publics 10

et le PMS 5 ou un serveur FTP 4 (Pour File Transfert Protocol), aptes à contrôler des transferts de données ou logiciels entre les téléphones publics 10 et le serveur FTP 4.

5 En autres fonctions, le serveur PMS 5 transfère vers les téléphones publics 10, les fichiers nécessaires à leur fonctionnement, tels que des tables tarifs, des paramètres de configuration comme le type de numérotation, les caractéristiques de la ligne, des listes d'opposition ou de surveillance des moyens de paiement utilisés.

10

Les téléphones publics 10 transmettent de leur côté des informations relatives à leur utilisation, à savoir un rapport journalier comportant des données relatives aux transactions effectuées, au trafic, un rapport d'alarme qui permet de signaler au PMS 5 la survenue d'incidents ou
15 des atteintes à leur intégrité, comme une panne sur le lecteur de cartes ou un combiné arraché, de manière à prévoir l'intervention d'un agent de surveillance et un fichier de statut caractérisant le contenu du téléphone (tel que des indications des différentes versions de programmes utilisés par le microprocesseur).

20

Pour faciliter les échanges de données, on peut utiliser un serveur 4 spécifiquement conçu et adapté au transfert de fichier 4, appelé FTP (File Transfert Protocol).

25 A partir de commandes reçues par le serveur PMS 5, chaque téléphone public 10 qui intègre une entité serveur FTP client, va se connecter au serveur FTP 4 et télécharger ou télécharger les fichiers appropriés.

Par ailleurs, les téléphones publics 10 peuvent se connecter à un
30 serveur PROXY 6 servant d'interface de communication entre les téléphones publics 10 et le serveur PMS 5.

Par ailleurs, pour permettre la connexion aux différents serveurs et notamment au serveur PROXY 6, au serveur PMS 5 ou au serveur FTP 4, les téléphones 10 sont équipés de protocoles de communication TCP/IP conformes aux recommandations techniques de l'IETF (Internet Engineering task Force).

En référence aux figures 2 et 3, le Demandeur propose un procédé d'individualisation permettant selon l'invention d'éviter la création de doublons pouvant intervenir dans certaines situations.

10

L'une de ces situations correspond à celle d'un agent de surveillance et/ou de service souhaitant installer un téléphone dans la localisation de son choix et souhaitant initialiser pour la première fois le terminal auprès du serveur PMS 5.

15

Selon l'invention, le procédé d'individualisation comprend les étapes suivantes.

Tout d'abord, le terminal 10 appelle le serveur PMS 5 selon une session de connexion 20 de type Connect, selon un format choisi, par exemple selon le protocole de transfert de données PDU (Protocol Data Unit).

La session de connexion 20 comprend une demande de service correspondant ici à une demande d'initialisation.

25

Cette demande de service est accompagnée de données de type identification, par exemple numéro du terminal NAP.

De son côté, le serveur PMS 5 vérifie l'identité NAP du terminal appelant.

30

La vérification (étapes 30 et 34, figure 3) porte ensuite sur le fait de savoir si le terminal en connexion est un nouveau terminal, déclaré au préalable ou non, avec possibilité d'initialisation générale ou partielle.

- 5 S'il s'agit d'un nouveau terminal, c'est-à-dire inconnu des tables du serveur 5, ou déclaré comme tel, alors un certificat ESN pour « Electronic Serial Number, c'est-à-dire numéro de série électronique » est généré par le serveur 5 (étape 32, figure 3).
- 10 Ce certificat ESN est unique pour le terminal en connexion. Il est associé au numéro d'identité du terminal NAP.

De préférence, le certificat ESN est un numéro aléatoire (à la première génération), par exemple codé sur 8 octets.

15

Le serveur 5 stocke le certificat ESN ainsi engendré dans une table en correspondance avec l'identité NAP associée.

- 20 Ensuite, le serveur 5 communique (étape 24, figure 2) le certificat ESN ainsi généré vers le terminal, via le cas échéant le serveur FTP 4 et/ou le serveur PROXY 6.

De son côté, le terminal reçoit le certificat ESN et le stocke dans une mémoire appropriée, par exemple une mémoire de type Flash.

25

Ce certificat ESN permet ainsi d'individualiser de manière unique le nouveau terminal, ce qui empêche les doublons mentionnés ci-avant

- 30 Dans le cas d'un terminal déjà inscrit dans les tables du serveur PMS, et pour lequel l'initialisation générale ou partielle est autorisée, le serveur 5 génère également un certificat ESN, de façon dynamique. Ce

certificat est ensuite écrit dans une table du serveur avant d'être envoyé au terminal, comme décrit précédemment.

En pratique, le certificat ESN-2 du terminal 10-2 d'identité NAP-2
5 comprend un incrément de 1 par rapport au certificat ESN-1 du terminal 10-1 d'identité NAP-1.

Dans le cas d'un terminal déjà connu et en l'absence d'une initialisation générale ou partielle (étape 36, figure 3), la demande de service est
10 validée après la vérification du certificat ESN du terminal en connexion. (Il n'y a pas ici de génération d'un nouveau certificat)

En cas de vérification négative du certificat ESN, la demande de service est refusée par le serveur.

15

En cas de vérification positive, la demande de service est autorisée par le serveur.

Le protocole de communication entre le serveur et le terminal peut le
20 cas échéant comprendre des étapes d'acceptation d'échange de données ACCEPT, (étape 22, figure 2) et DISCONNECT (étape 26, figure 2) conformément au protocole PDU.

Ces échanges permettent notamment de valider la réception du
25 certificat ESN côté terminal.

Ainsi, en cas de problème dans l'émission/réception du certificat ESN et en l'absence d'accusé de réception émis par le terminal, le serveur conserve dans ses tables l'ancienne valeur du certificat.

30

Le procédé d'individualisation répond également au problème rencontré lorsqu'un agent de service souhaitant installer un nouveau un terminal, fait une erreur dans la saisie du numéro d'identité du terminal NAP.

5 En effet dans ce cas, le serveur vérifie l'identité du numéro NAP.

Si celui-ci est inconnu, le serveur considère ce téléphone comme étant un nouveau téléphone et il est géré comme s'il s'agit d'une première initialisation telle que décrite ci-avant (pour peu que cette création
10 automatique soit autorisée par le serveur PMS).

Si le numéro NAP est connu, le serveur vérifie alors la paire NAP et ESN.

En cas de comparaison négative dans les tables du serveur, le téléphone
15 est refusé systématiquement. En cas de comparaison positive, l'initialisation est validée avec un terminal individualisé selon l'invention.

Le procédé d'individualisation selon l'invention répond également aux
20 opérations de maintenance, par exemple lorsqu'un agent souhaite changer une carte du terminal après une panne.

Si après le remplacement de la carte, le numéro NAP est inconnu du serveur, le terminal est considéré comme étant un nouveau terminal et
25 il est géré en tant que tel, c'est à dire calcul d'un certificat ESN et envoi par le serveur au terminal (pour peu que cette création automatique soit autorisée par le serveur PMS).

Dans le cas où le terminal est déjà connu par le serveur, une nouvelle
30 initialisation doit être mise en place en vue d'attribuer des nouveaux fichiers d'initialisation ainsi que le certificat ESN (la réinitialisation dudit terminal est autorisé par l'opérateur par mise à jour de l'interface

homme machine). Dans ce cas, le certificat ESN est contrôlé conformément à l'étape 36.

Le procédé selon l'invention trouve également une application lorsque
5 aucune initialisation n'est prévue ou planifiée et qu'un agent souhaite réaliser une initialisation en raison d'un problème technique.

Dans ce cas, le serveur vérifie la paire formée par le numéro NAP et le
certificat ESN pour garantir l'absence de duplication. En cas de
10 vérification positive, l'initialisation est autorisée et le serveur communique les fichiers correspondants tandis qu'en cas de vérification négative, la communication est refusée.

De préférence, le certificat ESN est systématiquement contrôlé,
15 notamment lors des demandes de service du type alarme, rapport quotidien, téléchargement d'objets, télé-diagnostic.

REVENDEICATIONS

1. Procédé d'individualisation d'un terminal (10) relié à au moins un serveur (5) à travers un réseau (2), du type comprenant les étapes suivantes :
- 5 a) au niveau du terminal (10), établir une session de connexion (20) avec le serveur (5) , et
- b) au niveau du serveur (5), traiter la session de connexion selon un mode opératoire choisi,
- 10 caractérisé en ce que ledit mode opératoire comprend les étapes suivantes :
- c) au niveau du serveur (5), en cas de demande de service du terminal incluse dans la session de connexion, générer un certificat (ESN) unique associé audit terminal (10), et communiquer ledit certificat
- 15 audit terminal ;
- d) au niveau du terminal (10), recevoir et stocker ledit certificat (ESN) ; et
- e) au niveau du serveur (5), valider la demande de service avec le terminal ainsi individualisé de manière unique.
- 20
2. Procédé selon la revendication 1, caractérisé en ce que le certificat (ESN) est stocké au niveau du serveur après réception d'un accusé de réception émis par le terminal à l'issue de l'étape d).
- 25
3. Procédé selon la revendication 1, caractérisé en ce qu'en cas de session de connexion dépourvue de demande de service, la session de connexion est traitée selon les étapes suivantes :,
- i) en l'absence de certificat (ESN) parmi la session de connexion, considérer ladite session de connexion comme étant pourvue
- 30 d'une demande de service et la traiter selon l'étape c),
- ii) en présence de certificat parmi la session de connexion, vérifier ledit certificat, et en cas de vérification positive, autoriser la demande

de connexion tandis qu'en cas de vérification négative, refuser la demande de connexion.

4. Procédé selon la revendication 1 ou la revendication 2, caractérisé en ce que le certificat source (ESN) est un nombre aléatoire.
5. Procédé selon l'une des revendications précédentes, caractérisé en ce que la demande de service est du type initialisation, alarme, téléchargement d'objets ou autre événement analogue.
- 10 6. Installation du type comprenant un terminal relié à au moins un serveur à travers un réseau pour la mise en œuvre du procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que le terminal (10) comporte des moyens de communication, des moyens de traitement et des moyens de mémorisation et en ce que le serveur (5) comprend des moyens de communication, des moyens de traitement, des moyens de mémorisation et des moyens de génération aptes à générer et/ou contrôler un certificat (ESN) unique pour chaque terminal.
- 20 7. Terminal pour la mise en œuvre du procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que le terminal comporte des moyens de communication, des moyens de traitement et des moyens de mémorisation.
- 25 8. Terminal selon la revendication 6, caractérisé en ce qu'il appartient au groupe formé par les téléphones public, les appareils de service et analogues.
- 30 9. Serveur pour la mise en œuvre du procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que le serveur (5) comprend des moyens de communication, des moyens de traitement,

des moyens de mémorisation et des moyens de génération aptes à générer et/ou contrôler un certificat unique (ESN) pour chaque terminal (10).

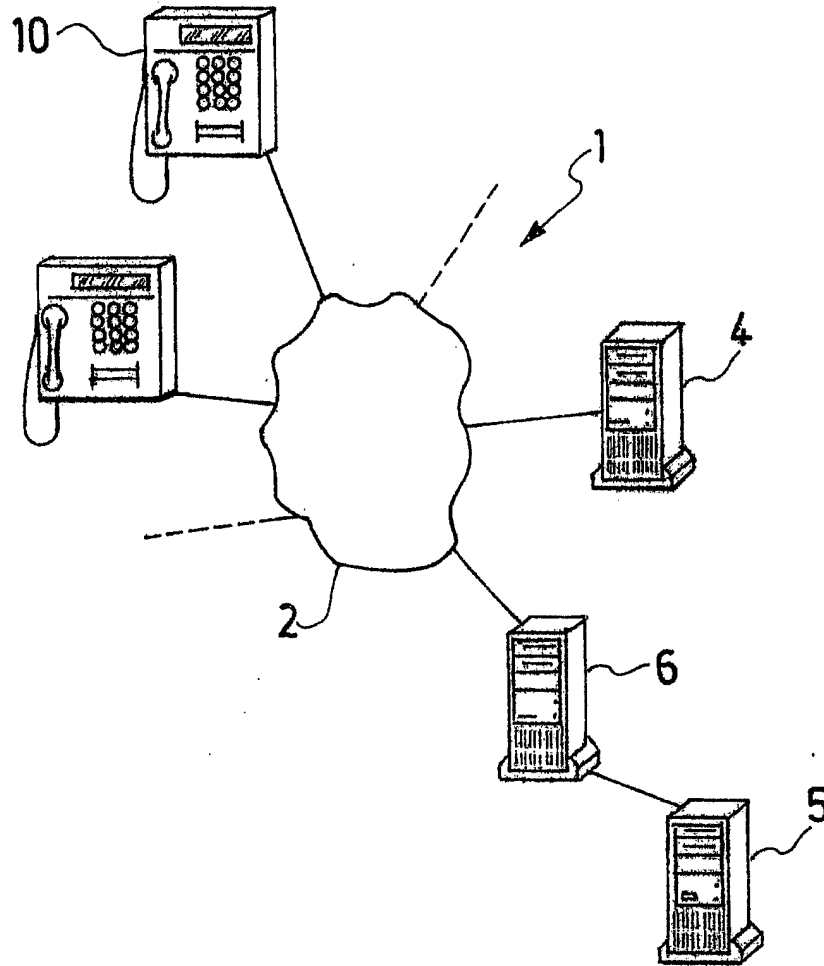


FIG.1

