

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
6 July 2006 (06.07.2006)

PCT

(10) International Publication Number
WO 2006/069599 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/EP2004/053717

(22) International Filing Date:
28 December 2004 (28.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **TELECOM ITALIA S.p.A.** [IT/IT]; Piazza degli Affari, 2, I-20123 Milano (IT).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **BELLIFEMINE, Fabio** [IT/IT]; c/o Telecom Italia S.p.A., Via G. Reiss Romoli, 274, I-10148 Torino (IT). **BOCHICCHIO, Rosalba** [IT/IT]; c/o Telecom Italia S.p.A., Centro Direzionale Isola F6, I-80143 Napoli (IT). **CAIRE, Giovanni** [IT/IT]; c/o Telecom Italia S.p.A., Via G. Reiss Romoli, 274, I-10148 Torino (IT). **DI TRIA, Paolo** [IT/IT]; c/o Telecom Italia S.p.A., Via G. Reiss Romoli, 274, I-10148 Torino (IT). **TRUCCO, Tiziana** [IT/IT]; c/o Telecom Italia S.p.A., Via G. Reiss Romoli, 274, I-10148 Torino (IT). **VITAGLIONE, Giosuè** [IT/IT]; c/o Telecom Italia S.p.A., Centro Direzionale Isola F6, I-80143 Napoli (IT).

(74) Agents: **JORIO, Paolo** et al.; Studio Torta S.r.l., Via Viotti, 9, I-10121 Torino (IT).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, 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, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

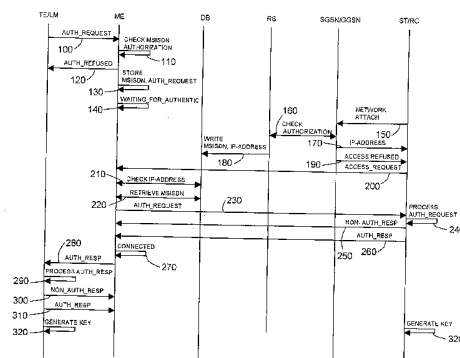
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: REMOTE ACCESS SYSTEM AND METHOD FOR ENABLING A USER TO REMOTELY ACCESS A TERMINAL EQUIPMENT FROM A SUBSCRIBER TERMINAL



(57) Abstract: Disclosed herein is a method for enabling a Subscriber Terminal to remotely access a Terminal Equipment, the Terminal Equipment storing identification data of the Subscriber Terminal, and the Subscriber Terminal being subscribed to a communication network and to a remote access service, wherein the method includes: receiving a request for authentication from the Terminal Equipment, the request for authentication including identification data of the Subscriber Terminal; receiving a request for access to the Terminal Equipment from the Subscriber Terminal; authenticating the Subscriber Terminal based on information from the communications network; forwarding the request for authentication from the Terminal Equipment to the Subscriber Terminal upon authenticating the Subscriber Terminal, the Subscriber Terminal processing the request for authentication to authenticate the Terminal Equipment; receiving an authentication notification from the Subscriber Terminal; forwarding the authentication notification to authenticate said Subscriber Terminal; receiving an authentication notification from the Terminal Equipment; and enabling the Subscriber Terminal to remotely access the Terminal Equipment upon receiving the authentication notification from the Terminal Equipment.

WO 2006/069599 A1

- 1 -

REMOTE ACCESS SYSTEM AND METHOD FOR ENABLING A USER TO REMOTELY ACCESS A TERMINAL EQUIPMENT FROM A SUBSCRIBER TERMINAL

5 TECHNICAL FIELD OF THE INVENTION

The present invention relates in general to remotely managing data stored in a networked device via another networked device, and in particular to a remote access system and a method for enabling a user to remotely access a terminal equipment, such as for example a personal computer, from a subscriber terminal,
10 such as for example a mobile phone.

BACKGROUND ART

Remote access systems allow users to access a computer or a computer network from a remote location using a remote computer. For example, employees
15 of businesses can use remote access systems to gain access to their business computers or their business computer network from various remote locations such as their homes, a branch office, or while traveling.

There are several remote access systems that are commercially available today such as pcAnyWhere produced by Symantec Corporation, Carbon Copy
20 produced by Compaq Corporation, and Timbuktu produced by Netopia. These remote access systems include software that must be installed on a target computer, such as a user's office computer or office computer system, and software that must be installed on a remote computer, such as a user's home computer.

One disadvantage of the conventional remote access systems described
25 above is that it is difficult to install and configure the software on the remote computers. The user must install software on the remote computer and then perform a configuration process, which typically requires entering information, such as the target computer's Internet Protocol (IP) address and a telephone number associated with the target computer's modem. Many users have difficulty performing these
30 configuration steps and in some cases fail to perform these configuration steps successfully. As a result, the user will not be able to access the target computer. Even if the user is able to perform these configuration steps, it may take an unacceptable amount of time to complete these steps. Another disadvantage of conventional remote access systems is that they do not support dynamic IP
35 addressing systems that are widely used in various network environments. Yet

- 2 -

another disadvantage of conventional remote access systems is that it is often difficult or impossible to access computers that are located behind firewalls using such conventional remote access systems. Yet another disadvantage of conventional remote access systems is that they do not allow applications to be remotely accessed during data conferences.

US2003/0084169A1 discloses a system and a method for accessing a target computer from a remote location using a remote computer. To access the target computer a user first accesses a central computer system (typically the computer of an Internet service provider) which performs also the function of user authentication. Once it is determined that the user has permission to access the target computer, the user can access the target computer via the central computer system and may control the applications present on the target computer and carry out file transfer from the remote computer.

However, the Applicant has observed that this system does not envisage any mechanism for remotely accessing the target computer from a mobile terminal, in particular a subscriber terminal such as a mobile phone, and in addition the setup thereof requires that an authentication procedure be made at a central or server computer (entering certain information such as username and password, possibly a credit-card number for the billing, an e-mail address, etc.) in order to obtain a new user account.

Further, WO01/74023 discloses a method and an apparatus for remotely managing data in a network system comprising at least one mobile device (e.g. a personal digital assistant, a cellular phone, a two-way pager, or a mobile computer) and at least one server computer connected via an interconnection fabric, wherein the mobile device is registered with the server and configured to issue commands to a service using electronic mail messages or some other viable data transmission mechanism. The service responds to the commands by interfacing with the server computer to perform the requested action on behalf of the mobile device. The command may for example regard management of the e-mail (sending, forwarding, erasing) or else querying of a database or any other action that can be performed on the server and generate a result that may be displayed on the mobile device.

The Applicant has observed that in this system, both the mobile device and the server computer are identified by their e-mail addresses, and therefore a drawback of this system is security. In fact, in the (SMTP) protocol used by the e-mail, it is extremely easy to change the "from" field, i.e., the sender of the e-mail,

- 3 -

and therefore the service could receive and execute malicious commands. Furthermore, the Applicant has noted that also this system requires that a registration procedure be made at a server computer in order to obtain a user account. The Applicant has also noted that, being based on the SMTP protocol, this system is slow to execute users' requests and therefore it is not able to be used with services requiring a quick reaction (for example a user requesting access to a remote directory).

Additionally, WO03/88577 describes a method for authenticating a user of a data transfer device (such as a terminal in a wireless local area network, i.e. WLAN). The method comprises: setting up a data transfer connection from the data transfer device to a service access point. Next, identification data of the mobile subscriber (for example an MSISDN) are inputted to the service access point. This is followed by checking from the mobile communication system whether the mobile subscriber identification data contains an access right to the service access point. If a valid access right exists, a password is generated, then transmitted, for example via SMS, to a subscriber terminal (for example a GSM mobile phone) corresponding to the mobile subscriber identification data, and login from the data transfer device to the service access point takes place with the password transmitted to the subscriber terminal.

The Applicant has noted that a disadvantage of this system is that access to the service requires two distinct interactions of the user, i.e., a first connection to the service to enter his MSISDN and a second connection to the service after receipt of the password for using the service, that can even be distant in time on account of the latencies inherent in SMS communication. Furthermore, the Applicant has observed that there are no means to make sure that the user will have available his own mobile phone, on which he will receive the password, at the moment when he wishes to access the service. The Applicant has also noted that this system requires that a registration procedure be made in order to obtain a user password.

OBJECT AND SUMMARY OF THE INVENTION

The object of the present invention is therefore to provide a remote access system and method for enabling a user to remotely access a terminal equipment, via a subscriber terminal, which are easy to implement, install and configure, which guarantee privacy and security of the communication between the terminal equipment and the subscriber terminal, and which allow billing to be made without

- 4 -

the need for the user to have a new dedicated account.

This object is achieved by the present invention in that it relates to a Remote Access Method and System for enabling a user to remotely access a Terminal Equipment from a Subscriber Terminal, as defined in claims 1 and 21, respectively, to Software Modules, as defined in claim 22, and to a Mobile Office Service, as defined in claim 23.

For the purposes of the present description, the term "Terminal Equipment" refers to any personal device that is accessible via an IP network, such as for example a personal computer, laptop or notebook linked to the IP network via a fixed or wireless link or a PDA or a smart phone linked to the IP network via a wireless link, and the term "Subscriber Terminal" refers to any mobile device, such as for example a mobile phone, able to be connected to a Mobile Communication Network.

For the purposes of the present description, the term "Mobile Communication Network" refers to any Communication Network able to use an authentication mechanism for authenticating Subscriber Terminals wireless connected to it (for example GPRS, EDGE, UMTS, WLAN Networks).

In a preferred embodiment, the present invention makes the mutual authentication between the Subscriber Terminal and the Terminal Equipment easy and immediate because the owner of the Subscriber Terminal is authenticated and hence authorized to access the Terminal Equipment reusing the account that the Mobile Communications Operator has assigned to the Subscriber Terminal. To be enabled to access the Terminal Equipment, it is therefore sufficient for the user to provide the Subscriber Terminal with a connection to a Mobile Communication Network (for example GPRS, EDGE, UMTS).

Advantageously, access credentials (i.e. the passwords) used to encrypt the communications between the Subscriber Terminal and the Terminal Equipment are not registered on any central server and therefore they are modifiable at any moment by the user acting only on the Subscriber Terminal and Terminal Equipment, thus guaranteeing confidentiality of the information exchanged.

BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding of the present invention, a preferred embodiment, which is intended purely by way of example and is not to be construed as limiting, will now be described with reference to the attached drawings, wherein:

- 5 -

- Figure 1 shows a block diagram of a remote access system for enabling a user to remotely access a terminal equipment via a subscriber terminal, according to an embodiment the present invention;

- Figure 2 shows a flowchart of the actions performed by the remote access system, the subscriber terminal and the terminal equipment to enable the user to remotely access the terminal equipment via the subscriber terminal; and

- Figure 3 shows a block diagram of a remote access system according to a different embodiment of the present invention.

10 DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

The following discussion is presented to enable a person skilled in the art to make and use the invention. Various modifications to the embodiments will be readily apparent to those skilled in the art, and the generic principles herein may be applied to other embodiments and applications without departing from the spirit and scope of the present invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features disclosed herein and defined in the attached claims.

Figure 1 shows a block diagram of a Remote Access System (RAS) which provides a so-called Mobile Office Service, i.e., a service which enables a user to remotely access his/her own Terminal Equipment (TE) via his/her own Subscriber Terminal (ST).

The Subscriber Terminal can include a GPRS-enabled or EDGE-enabled mobile equipment provided with a Subscriber Identity Module (SIM) card or a UMTS-enabled mobile equipment provided with a Universal Subscriber Identity Module (USIM) card. SIM/USIM cards store identification data of the subscriber of the mobile communications system, namely the IMSI (International Mobile Subscriber Identity) / IMUI (International Mobile User Identity), which are mapped by the operator to the Mobile Subscriber International Integrated Services Digital Network Number (MSISDN) that identifies the subscriber globally and unambiguously. The MSISDN consists of three parts: country code, national network identifier and subscriber number.

In order to remotely access the Terminal Equipment, the Subscriber Terminal has to be subscribed to a Mobile Communications Network (CN), such as GPRS (General Packet Radio System) or EDGE (Enhanced Data for GSM

- 6 -

Evolution) or UMTS (Universal Mobile Telecommunications System), and be authorized to use the Mobile Office Service provided by the Remote Access System.

5 The Mobile Communication Network can include a Radius (Remote Authentication Dial-In User Service) Server (RS), which is a security distributed system that secures remote access to networks and network services against unauthorized access, and to which user authentication is delegated.

10 According to a preferred embodiment of the present invention, the Remote Access System includes a Mediator software application, hereinafter referred to as Mediator (ME), running on a server at the Service Centre and communicating with the Radius Server; and an Authentication Database (DB) accessible by both the Radius Server and the Mediator, and containing information on the Subscriber Terminals connected to the Mobile Communications Network and authenticated by the Radius Server.

15 In addition, the Subscriber Terminal is provided with a Remote Control software application, hereinafter referred to as Remote Controller (RC), running on the Subscriber Terminal and enabling the user to remotely access the Mediator for controlling the Terminal Equipment via the Mediator itself, and the Terminal Equipment is provided with a Local Manager software application, hereinafter
20 referred to as Local Manager (LM), running on the Terminal Equipment and enabling the Mediator to remotely access the Terminal Equipment for executing the commands received from the Subscriber Terminal.

Preferably, the Mediator is a software application developed using a open source platform for peer-to-peer agent-based applications implemented in Java
25 language and known as JADE (Java Agent Development Framework; the related documentation being accessible on the Internet, as of the filing date of the present application, at the address <http://jade.tilab.com>). Jade simplifies the implementation of multi-agent systems through a middleware that complies with the FIPA (Foundation for Intelligent Physical Agents) specifications and through a set of
30 graphical tools that supports the debugging and deployment phases. The agent platform can be distributed across machines (which not even need to share the same operating system) and the configuration can be controlled via a remote graphical user interface (GUI). The configuration can be even changed at run-time by moving agents from one machine to another one, as and when required. The minimal system
35 requirement to implement Jade is the version 1.4 of JAVA™ (the run time

environment or the Java Development Kit).

The Mediator can communicate with the Remote Controller and the Local Manager using, for example, a Security Session Layer (SSL) protocol for authentication and confidentiality constraints between the Mediator and the Remote Controller and between the Mediator and the Local Manager.

An appropriate user interface on the Subscriber Terminal enables the user to access the functions of the Remote Controller for sending commands to the Terminal Equipment, for example in order to download user own files from the Terminal Equipment onto the Subscriber Terminal, to enable/disable sharing of remote files with other users, and to download files that other users have shared with him/her.

The Local Manager is able to execute commands received from the Subscriber Terminal via the Mediator, to manage requests from other users, to discriminate received commands on the basis of the sender, and to manage an access control list for the access to the resources of the Terminal Equipment.

After the Remote Controller and the Local Manager have been installed on the Subscriber Terminal and the Terminal Equipment, respectively, the two software modules may be configured by entering user access credentials, such as for example a password in the Subscriber Terminal, and the same user access credentials, i.e. the same password, and the MSISDN of the Subscriber Terminal in the Terminal Equipment. The Remote Controller and the Local Manager may be configured either to store the user passwords and the MSISDN of the Subscriber Terminal, which therefore will never be requested any more to the user, or to request input of the user passwords and the MSISDN of the Subscriber Terminal at each execution. In any case, the password is not communicated/transferred outside the two software applications, and consequently, it cannot be discovered even by the Service Provider of the Mobile Office Service. This password is used as a master key enabling Remote Controller and Local Manager to generate a common session key that they will use as a shared secret in order to protect the communication between them.

Figure 2 shows commands and responses exchanged by the Remote Access System, the Subscriber Terminal and the Terminal Equipment to enable the user to remotely access the Terminal Equipment via the Subscriber Terminal.

In particular, the user who later wants to remotely access his/her own Terminal Equipment via his/her own Subscriber Terminal has firstly to run the

Local Manager on the Terminal Equipment.

When executed, the Local Manager requests a connection of the Terminal Equipment to the Mediator by sending a request for authentication AUTH_REQUEST containing the MSISDN of the Subscriber Terminal which may
5 remotely control the Terminal Equipment, and data encrypted using the password entered by the user in the Terminal Equipment (100). For example, the request for authentication AUTH_REQUEST can have the following format:

AUTH_REQUEST=(MSISDN, E_{key=PairingSecret}(RandomString1, Nonce1,
10 HMAC_{key=PairingSecret}(RandomString1, Nonce1)))

where:

- E is an encryption function and HMAC (Keyed-Hashing for Message Authentication) is a signature function;
- 15 • PairingSecret is the password entered by the user in the Terminal Equipment and the corresponding Subscriber Terminal; this password is never transmitted, not even in an encrypted form and it is used both for generating the HMAC (i.e. the signature of the message) and for encrypting the entire message;
- RandomString1 is a random string generated by the Local Manager; and
- 20 • Nonce1 is a time-stamp of the message used to prevent reply-attack; whenever the addressee receives a message with a Nonce already received, the message is considered malicious and, potentially, an attack attempt; it is hence up to the sender to use always different Nonce values.

It may be appreciated that only the addressee of the request for authentication AUTH_REQUEST is in clear, i.e., not encrypted. It simply contains
25 the MSISDN of the Subscriber Terminal and it is the only part of the message that the Mediator can read and interpret.

Upon receiving the request for authentication AUTH_REQUEST from the Local Manager, the Mediator extracts the MSISDN, and verifies whether the user is
30 subscribed to the Mobile Office Service by checking if the MSISDN is in a *subscriber list* (110).

If the user is not subscribed to the Mobile Office Service, the Mediator executes a procedure to reject the request for authentication AUTH_REQUEST
(120). This procedure involves sending authentication refusal AUTH_REFUSED to
35 the Local Manager and blocking any connection to the latter. Furthermore, for a

- 9 -

given time interval, which can be defined by the Service Provider, the Mediator will not accept any other request for authentication from the IP address associated to the Terminal Equipment on which that Local Manager is installed, in so far as it could be potentially malicious. Once this time interval has elapsed, the procedure can be re-executed by the Local Manager by sending the request for authentication AUTH_REQUEST again, this time hopefully, with proper authorized data.

On the contrary, if the user is subscribed to the Mobile Office Service, the Mediator stores the request for authentication AUTH_REQUEST along with the MSISDN (130) until it receives a request for access ACCESS_REQUEST to the Terminal Equipment from a Subscriber Terminal having the same MSISDN as the one included in the stored request for authentication AUTH_REQUEST. The Mediator also sets the Local Manager to a state WAITING_FOR_AUTHENTICATION, in which the Mediator does not authorize the Local Manager to perform any operation (140).

At this point, when the user wants to remotely access his/her own Terminal Equipment, he/she has firstly to authenticate the Subscriber Terminal with the Mobile Communications Network (150). For example, if the Mobile Communications Network is a GPRS network, the standard "GPRS attach" procedure may be executed requiring the Subscriber Terminal to register itself with a Serving GPRS Support Node (SGSN) via a Gateway GPRS Support Node (GGSN) (both not shown). The Radius Server is the network component that authenticates the Subscriber Terminal by verifying whether it is enabled to access the GPRS network and that notifies the GGSN accordingly (160): if authentication is successful, the GGSN assigns and provides an IP address to the Subscriber Terminal (170) and the Radius Server writes into the Authentication Database information about the authenticated Subscriber Terminal, such as for example the username, the IP address, the MSISDN, etc. (180), whereas if authentication is not successful, the GGSN, which rejects the request for access of the Subscriber Terminal the GPRS network (190). EDGE and UMTS make use of an authentication procedure very similar to that described above.

Then, the Mobile Communications Network assigns the IP address to the Subscriber Terminal, and at this point, the Subscriber Terminal is connected to the Mobile Communications Network and the user's Remote Controller, installed on the Subscriber Terminal, may use the Mobile Communication Network for communicating with the Mediator.

- 10 -

Upon execution, the Remote Controller sends a request for access ACCESS_REQUEST of the Subscriber Terminal to the Mediator (200), which request for access ACCESS_REQUEST includes the IP address provided to the Subscriber Terminal by the Mobile Communications Network.

5 When the Mediator receives the request for access ACCESS_REQUEST, it authenticates the Subscriber Terminal by verifying whether the Subscriber Terminal is connected to the Mobile Communications Network, i.e., whether the Subscriber Terminal has already been authenticated by the Mobile Communications Network (210). In particular, the authentication is made by verifying whether the IP address
10 of the Subscriber Terminal, which is extracted from the request for access ACCESS_REQUEST, is in the Authentication Database. If authentication is successful, the Mediator grants access to the Subscriber Terminal and retrieves all the other information stored in the Authentication Database and relating to the Subscriber Terminal, including the MSISDN (220).

15 At this point, the Mediator has acquired mapping between the IP address and the MSISDN of the Subscriber Terminal that has requested access to a Terminal Equipment.

 Should the Subscriber Terminal disconnect from the Mobile Communications Network, for example due to a connection block, the Radius
20 Server writes this information into the Authentication Database. The Mediator, being connected to the Authentication Database, is thus informed of this disconnection, and may provide for a better use of the resources by re-allocating the ones no longer used by the Subscriber Terminal, now disconnected.

 Once the Subscriber Terminal has been authenticated by the Mediator, the
25 latter forwards the request for authentication AUTH_REQUEST received from the Terminal Equipment to the Subscriber Terminal (230), which processes the request for authentication AUTH_REQUEST in order to authenticate the Terminal Equipment (240). In particular, the Remote Controller on the Subscriber Terminal decrypts the request for authentication AUTH_REQUEST by using the password
30 entered by the user in the Subscriber Terminal, and then re-computes the request for authentication by using the same password. If the password has not been stored, the Remote Controller asks the user to enter it.

 If the re-computed request for authentication is different from the one forwarded by the Mediator, or if it contains a value of Nonce that was already
35 received, the Remote Controller does not authenticate the Local Manager and sends

- 11 -

to the Mediator a non-authentication notification NON_AUTH_RESP (250), which Mediator executes a procedure similar to the above-described procedure (120) to reject the request for authentication AUTH_REQUEST.

5 If, instead, the re-computed for authentication is equal to the one forwarded by the Mediator and it contains a never used value of Nonce, the Remote Controller authenticates the Local Manager and sends to the Mediator an authentication notification AUTH_RESP (260) with the following format:

10 AUTH_RESP=(MSISDN, $E_{\text{key=PairingSecret}}(\text{RandomString2, Nonce2, HMAC}_{\text{key=PairingSecret}}(\text{RandomString2, Nonce2}))$)

where the various fields have the meaning described above.

15 Once the Mediator has received the authentication notification AUTH_RESP, it promotes the Local Manager from the state WAITING_FOR_AUTHENTICATION to a state CONNECTED (270), and forwards the authentication notification AUTH_RESP to the latter (280), which processes the authentication notification AUTH_RESP in order to authenticate the Subscriber Terminal (290). From this moment on, the Local Manager is authorized to use the Mobile Office Service.

20 In particular, the Local Manager on the Terminal Equipment decrypts the notification authentication AUTH_RESP in order to extract "RandomString2" by using the password entered by the user in the Terminal Equipment, and then re-computes the notification authentication AUTH_RESP by using the same password.

25 If the re-computed authentication notification AUTH_RESP is different from the one forwarded by the Mediator, or if it contains a value of Nonce that was already received, the Local Manager does not authenticate the Remote Controller and detects a fraud attempt, logs it and sends to the Mediator a non-authentication notification NON_AUTH_RESP (300). At this point, the Mediator executes a procedure similar to the above-described procedure (120) to reject the request for access AUTH_ACCESS.

30 If, instead, the re-computed authentication notification is equal to the one forwarded by the Mediator and it contains a never used value of Nonce, the Local Manager authenticates the Subscriber Terminal and sends to the Mediator an authentication notification AUTH_RESP (310).

35 At this point, the Remote Controller and the Local Manager, being trusted

- 12 -

on each other, generate a common session key by using the two exchanged RandomStrings (320). This common session key will be used, from this moment on, in order to encrypt the entire communication between the Remote Controller and the Local Manager. In a preferred embodiment of the present invention the common session key can be generated by using the following algorithm:

$$K_{\text{sess}} = E_{\text{key}=\text{PairingSecret}}(\text{RandomString1 concatenated RandomString2}).$$

From this moment on, the Remote Controller and the Local Manager may exchange commands and messages via the Mediator at the Mobile Office Centre. These commands and messages are encrypted via the common session key K_{sess} .

In conclusion, the Remote Controller connects to the Mediator only if the Subscriber Terminal is authenticated by the Radius Server, whereas the Local Manager connects to the Mediator only if pairing with the Remote Controller, via the Pairing Secret, is successful.

It should be noted that basically the Mediator "trusts" the Remote Controller, whilst it does not "trust" the Local Manager. This is possible thanks to the connection of the Mediator at the Service Centre with the RADIUS Server, connection which guarantees that the Remote Controller is authenticated by the Mobile Network Operator. Therefore, the Mediator delegates authentication of Local Manager to the Remote Controller, and once the authentication is successful, the Remote Controller becomes responsible for the actions of the Local Manager, and the connection of the Subscriber Terminal to the Terminal Equipment may be billed directly on the account associated to the MSISDN of the Subscriber Terminal.

The advantages of the present invention are evident from the foregoing description.

The main advantage is the easily of installation and configuration of the software applications on the Subscriber Terminals and the Terminal Equipments. In fact, the user only installs a first software application on the Subscriber Terminal and a second software application on the Terminal Equipment, and then enters simple credentials upon the first execution of the two software applications, in particular a password on the Subscriber Terminal and the same password and the MSISDN of the Subscriber Terminal on the Terminal Equipment. Then, the connection of the Subscriber Terminal to the Terminal Equipment is automatic and

- 13 -

transparent to the user that has not to deal with difficult concepts, such as IP numbers, firewalls configurations, NAT, etc.

Another advantage of the present invention is that the user may remotely access the Terminal Equipment by reusing his/her own Network account and does not have to register at some Service Provider to obtain a new account. This aspect is important because frequently the introduction of new services is delayed owing to the psychological effect that the need to register and open a new account has on the users. The reuse of the Network account of the user further enables billing of the Mobile Office Service on an MSISDN basis.

A further advantage of the present invention is that the mutual authentication of the Subscriber Terminals and the controlled Terminal Equipments is very easy and immediate. In fact, the Subscriber Terminal is authenticated and hence authorized to access the Terminal Equipment via the Network account that the Mobile Communications operator has assigned to the Subscriber Terminal. To access the Terminal Equipment, it will thus be sufficient for the user to provide the Subscriber Terminal with a connection to the Mobile Communication Network (for example GPRS, EDGE, UMTS).

A yet further advantage of the present invention is privacy and security of transferred information. In fact, once the mutual authentication has been carried out, the Subscriber Terminal and the controlled Terminal Equipment can communicate in a confidential and safe way because the exchanged information is not in clear even during transit through the Mediator thanks to the end-to-end encryption of the information using the common session key K_{sess} .

Communication during the authentication procedure also occurs in an incorruptible way, because signatures are associated to the exchanged messages and commands and verified by the addressees using the shared passwords, thus verifying the authenticity of the origin of the exchanged messages and commands. Communication during the authentication procedure is also protected against the so-called replay attacks because each exchanged message and command contains a different number (Nonce), and is deemed valid by the addressee only if that number has never been used, thus preventing an hacker from "sniffing" the message and sending it a number of times.

Moreover, the identification of the users based on the MSISDNs enables management of an Access Control List (ACL) containing the authorizations of access to the various directories of the file

- 14 -

system of the Terminal Equipment based upon MSISDNs. In other words, a user will be able to grant read access to the file system of his Terminal Equipment for example to all the telephone numbers that are in the "VIP" category of his/her phone book, whilst he/she will be able to grant read/write access to all those in the "family" category.

In addition, the present invention enables remote access to the user Terminal Equipment even when this is located behind a Network Address Translation system and/or dynamic IP address assignment, and is protected by a firewall. In fact, as the Mediator mediates all the communication between the Terminal Equipment and the Subscriber Terminal, these latter two do not need to be directly connected: it is just the Mediator that needs to be reachable, not the Terminal Equipment and Subscriber Terminal.

Furthermore, the Terminal Equipment and the Subscriber Terminal do not need to process incoming connections (that would require proper configuration of the firewall and the NAT) but they only need to initiate a connection with the Mediator.

Moreover, the present invention enables automatic management of modifications of the IP address of the Subscriber Terminal even during the application session. In fact, in the case of modification of the IP address of one of the Subscriber Terminal and the Terminal Equipment (typically the Subscriber Terminal, as a consequence, for example, of a dead spot), the Mediator can simply update the mapping between logical name and IP address in a way that is transparent to the communication between the Terminal Equipment and the Subscriber Terminal, communication that continue to use the same logical names.

Finally, it is clear that numerous modifications and variants can be made to the present invention, all falling within the scope of the invention, as defined in the appended claims.

In particular, Figure 3 shows a possible corporate application of the present invention, wherein the Mediator is split into two logical modules:

- a Server module which is hosted at the Service Centre of the Mobile Communications Operator and which interfaces with the Radius Server and handles all the connections to the Subscriber Terminals; and
- a Muxer module which is hosted at the corporate Service Centre and which handles all the connections to the Terminal Equipments. The corporate manager can hence set the most appropriate access rules towards the Terminal

- 15 -

Equipments of the corporate network, and the Muxer module will interface with the Server module for communication to the Subscriber Terminals.

- 5 In this corporate scenario, the mapping between the Terminal Equipment and the Subscriber Terminal may be carried out automatically by the Local Manager. In fact, it can retrieve the MSISDN of the Subscriber Terminal by querying the corporate database, thus further simplifying the application of the invention in question in so far as the software applications will only ask the user for a password.

- 16 -

CLAIMS

1. A Remote Access Method for enabling a user to remotely access a Terminal Equipment (TE) from a Subscriber Terminal (ST) via a Remote Access System (RAS), said Terminal Equipment (TE) storing identification data (MSISDN) of said Subscriber Terminal (ST), said method being characterized by:
- receiving a request for authentication (AUTH_REQUEST) from said Terminal Equipment (TE), said request for authentication (AUTH_REQUEST) including said identification data (MSISDN) of said Subscriber Terminal (ST);
 - receiving a request for access (ACCESS_REQUEST) to said Terminal Equipment (TE) from said Subscriber Terminal (ST);
 - verifying that said Subscriber Terminal (ST) is subscribed to said Remote Access System (RAS);
 - authenticating said Subscriber Terminal (ST) based on information from a communications network (CN);
 - forwarding said request for authentication (AUTH_REQUEST) from said Terminal Equipment (TE) to said Subscriber Terminal (ST), said Subscriber Terminal (ST) processing said request for authentication (AUTH_REQUEST) to authenticate said Terminal Equipment (TE);
 - receiving an authentication notification (AUTH_RESP) from said Subscriber Terminal (ST);
 - forwarding said authentication notification (AUTH_RESP) from said Subscriber Terminal (ST) to said Terminal Equipment (TE), said Terminal Equipment (TE) processing said authentication notification (AUTH_RESP) to authenticate said Subscriber Terminal (ST); and
 - receiving an authentication notification (AUTH_RESP) from said Terminal Equipment (TE); and
 - enabling said Subscriber Terminal (ST) to remotely access said Terminal Equipment (TE).
2. A Remote Access Method as claimed in claim 1, wherein authenticating said Subscriber Terminal (ST) based on information from said communications network (CN) includes:
- verifying that said Subscriber Terminal (ST) has been previously authenticated by said communications network (CN).
3. A Remote Access Method as claimed in claim 1 or 2, wherein verifying that said Subscriber Terminal (ST) has been previously authenticated by said

communications network (CN) includes:

- verifying that said identification data (MSISDN) of said Subscriber Terminal (ST) has been stored by said communications network (CN) in a database (DB).

5 4. A Remote Access Method as claimed in any preceding claim, wherein said identification data include at least MSISDN of said Subscriber Terminal (ST).

5. A Remote Access Method as claimed in any of the preceding claims, further including:

- storing said request for authentication (AUTH_REQUEST) until said

10 Subscriber Terminal (ST) has been authenticated by said Communications Network (CN).

6. A Remote Access Method as claimed in any of the preceding claims, wherein verifying that said Subscriber Terminal (ST) is subscribed to said Remote Access System (RAS) includes:

- extracting said identification data of said Subscriber Terminal (ST) from said request for authentication (AUTH_REQUEST); and

15

- verifying that said extracted identification data are associated to a subscriber of said Remote Access System (RAS).

7. A Remote Access Method as claimed in claim 6, further including:

- rejecting said request for authentication (AUTH_REQUEST) if said

20 identification data are not associated to a subscriber of said Remote Access System (RAS).

8. A Remote Access Method as claimed in claim 7, further including:

- sending an authentication refusal (AUTH_REFUSED) to said Terminal

25 Equipment (TE) if said identification data are not associated to a subscriber of said Remote Access System (RAS).

9. A Remote Access Method as claimed in claim 7 or 8, further including:

- rejecting any subsequent request for authentication (AUTH_REQUEST)

30 from said Terminal Equipment (TE) for a time span if said identification data are not associated to a subscriber of said Remote Access System (RAS).

10. A Remote Access Method as claimed in any of the preceding claims, wherein said request for authentication (AUTH_REQUEST) from said Terminal Equipment (TE) includes data encrypted using user access credentials entered in said Terminal Equipment (TE), and wherein said Subscriber Terminal (ST)

35 authenticates said Terminal Equipment (TE) based on said encrypted data in said

- 18 -

request for authentication (AUTH_REQUEST).

11. A Remote Access Method as claimed in claim 7, wherein authenticating said Terminal Equipment (TE) based on said encrypted data includes:

- decrypting said encrypted data in said request for authentication (AUTH_REQUEST) by using user access credentials entered in said Subscriber Terminal (ST);
- encrypting said decrypted data using said user access credentials entered in said Subscriber Terminal (ST);
- comparing said encrypted data in said request for authentication (AUTH_REQUEST) with said data encrypted using said user access credentials entered in said Subscriber Terminal (ST); and
- authenticating said Terminal Equipment (TE) if said comparison has a positive outcome.

12. A Remote Access Method as claimed in claim 10 or 11, further including:

- rejecting said request for authentication (AUTH_REQUEST) upon receiving a non-authentication notification (NON_AUTH_RESP) from said Subscriber Terminal (ST).

13. A Remote Access Method as claimed in claim 12, further including:

- sending an authentication refusal (AUTH_REFUSED) to said Terminal Equipment (TE) upon receiving a non-authentication notification (NON_AUTH_RESP) from said Subscriber Terminal (ST).

14. A Remote Access Method as claimed in claim 12 or 13, further including:

- rejecting any subsequent request for authentication (AUTH_REQUEST) from said Terminal Equipment (TE) for a time span upon receiving said non-authentication notification (NON_AUTH_RESP) from said Subscriber Terminal (ST).

15. A Remote Access Method as claimed in any of the preceding claims, wherein said authentication notification (AUTH_RESP) from said Subscriber Terminal (ST) includes data encrypted using said access credentials entered in said Subscriber Terminal (ST), and wherein said Terminal Equipment (TE) authenticates said Subscriber Terminal (ST) based on said encrypted data in said authentication notification (AUTH_RESP).

16. A Remote Access Method as claimed in claim 15, wherein

- 19 -

authenticating said Subscriber Terminal (ST) based on said encrypted data in said authentication notification (AUTH_RESP) includes:

- decrypting said encrypted data in said authentication notification (AUTH_RESP) by using said access credentials entered in said Terminal Equipment (TE);
- encrypting said decrypted data using said access credentials entered in said Terminal Equipment (TE);
- comparing said encrypted data in said authentication notification (AUTH_RESP) with said data encrypted using said access credentials entered in said Terminal Equipment (TE); and
- authenticating said Subscriber Terminal (TE) if said comparison has a positive outcome.

17. A Remote Access Method as claimed in claim 15 or 16, further including:

- rejecting said request for access (AUTH_ACCESS) upon receiving a non-authentication notification (NON_AUTH_RESP) from said Terminal Equipment (TE).

18. A Remote Access Method as claimed in claim 17, further including:

- sending an authentication refusal (AUTH_REFUSED) to said Subscriber Terminal (ST) upon receiving said non-authentication notification (NON_AUTH_RESP) from said Terminal Equipment (TE).

19. A Remote Access Method as claimed in any of claims 17 or 18, further including:

- rejecting any subsequent request for access (AUTH_ACCESS) from said Subscriber Terminal (ST) for a time span upon receiving said non-authentication notification (NON_AUTH_RESP) from said Terminal Equipment (TE).

20. A Remote Access Method as claimed in any of the preceding claims, wherein said Remote Access System (RAS) stores an Access Control List (ACL) containing access authorizations for different Subscriber Terminals (ST), each access authorization specifying resources of said Terminal Equipment (TE) to which a corresponding Subscriber Terminal (ST) may access;

and wherein enabling said Subscriber Terminal (ST) to remotely access said Terminal Equipment (TE) includes:

- determining the access authorization associated to said Subscriber

- 20 -

Terminal (ST) in said Access Control List (ACL); and

- enabling said Subscriber Terminal (ST) to access the resources of said Terminal Equipment (TE) specified in said access authorization.

21. A Remote Access System (RAS) for enabling a user to remotely access
5 a Terminal Equipment (TE) from a Subscriber Terminal (ST), said Subscriber Terminal (ST), said Terminal Equipment (TE) and said Remote Access System (RAS) being configured to implement the Remote Access Method according to any preceding claims.

22. Software Modules able, when loaded in a Terminal Equipment (TE), a
10 Subscriber Terminal (ST), and a Remote Access System (RAS) for enabling a user to remotely access said Terminal Equipment (TE) from said Subscriber Terminal (ST), to cooperate in implementing the Remote Access Method according to any preceding claim 1 to 18.

23. A Mobile Office Service for enabling a user to remotely control a
15 Terminal Equipment (TE) from a Subscriber Terminal (ST) via a Remote Access System (RAS), said Terminal Equipment (TE) storing identification data (MSISDN) of said Subscriber Terminal (ST), said Mobile Office Service being characterized by:

- generating a request for authentication (AUTH_REQUEST) at said
20 Terminal Equipment (TE), said request for authentication (AUTH_REQUEST) including said identification data (MSISDN) of said Subscriber Terminal (ST);

- sending said request for authentication (AUTH_REQUEST) from said Terminal Equipment (TE) to said Remote Access System (RAS);

- generating at said Subscriber Terminal (ST) a request for access
25 (ACCESS_REQUEST) to said Terminal Equipment (TE);

- sending said request for access (ACCESS_REQUEST) from said Subscriber Terminal (ST) to said Remote Access System (RAS);

- verifying at said Remote Access System (RAS) that said Subscriber Terminal (ST) is subscribed to said Remote Access System (RAS);

- authenticating at said Remote Access System (RAS) said Subscriber
30 Terminal (ST) based on information from a communications network (CN);

- sending said request for authentication (AUTH_REQUEST) to said Subscriber Terminal (ST),

- processing at said Subscriber Terminal (ST) said request for
35 authentication (AUTH_REQUEST) to authenticate said Terminal Equipment (TE);

- 21 -

- generating an authentication notification (AUTH_RESP) at said Subscriber Terminal (ST);
- sending said authentication notification (AUTH_RESP) from said Subscriber Terminal (ST) to said Terminal Equipment (TE) via said Remote Access System (RAS);
- processing at said Terminal Equipment (TE) said authentication notification (AUTH_RESP) to authenticate said Subscriber Terminal (ST); and
- establishing a secure communication between said Subscriber Terminal (ST) and said Terminal Equipment (TE).

24. A Mobile Office Service as claimed in claim 23, wherein establishing a secure communication includes:

- generating a common session key (K_{sess}) at said Subscriber Terminal (ST) and said Terminal Equipment (TE); and
- encrypting communication between said Subscriber Terminal (ST) and said Terminal Equipment (TE) by using said common session key (K_{sess}).

25. A Mobile Office Service as claimed in claim 23 or 24, wherein said Remote Access System (RAS) stores an Access Control List (ACL) containing access authorizations for different Subscriber Terminals (ST), each access authorization specifying resources of said Terminal Equipment (TE) to which a Subscriber Terminal (ST) may access;

and wherein establishing a secure communication includes:

- determining the access authorization associated to said Subscriber Terminal (ST) in said Access Control List (ACL); and
- enabling said Subscriber Terminal (ST) to access the resources of said Terminal Equipment (TE) specified in said access authorization.

1 / 2

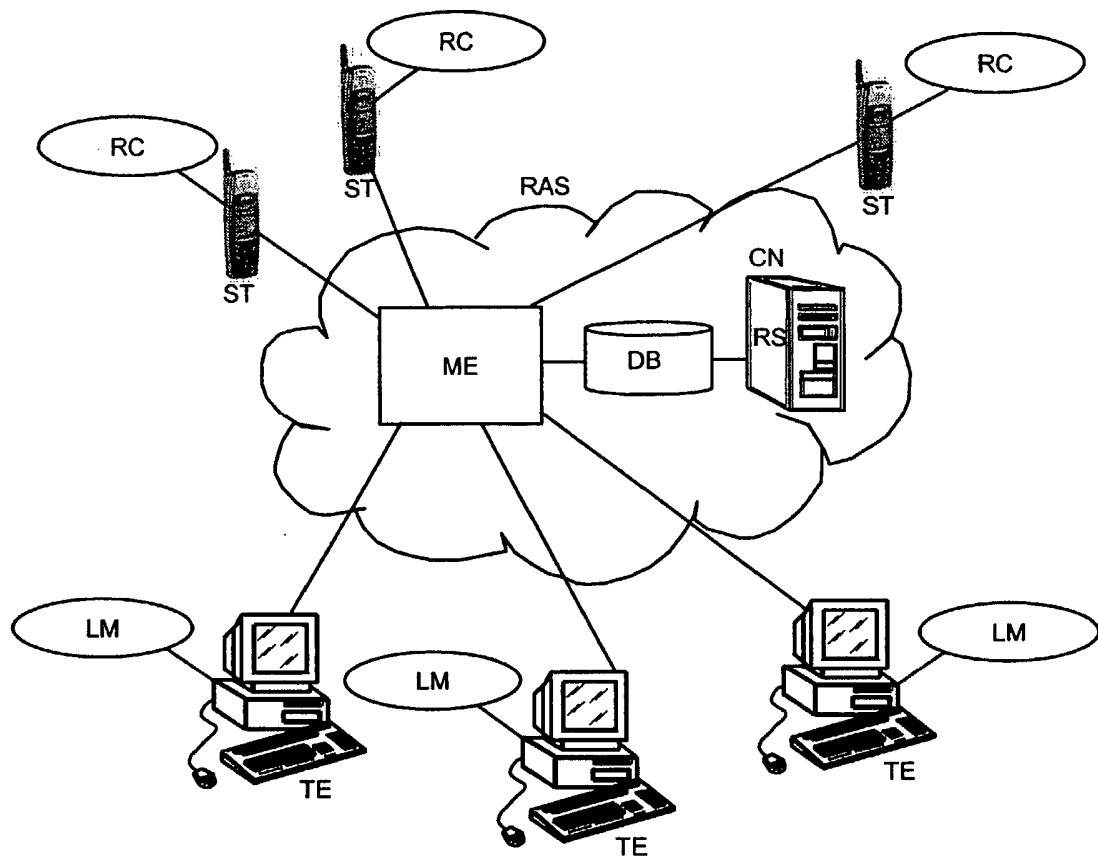


Fig.1

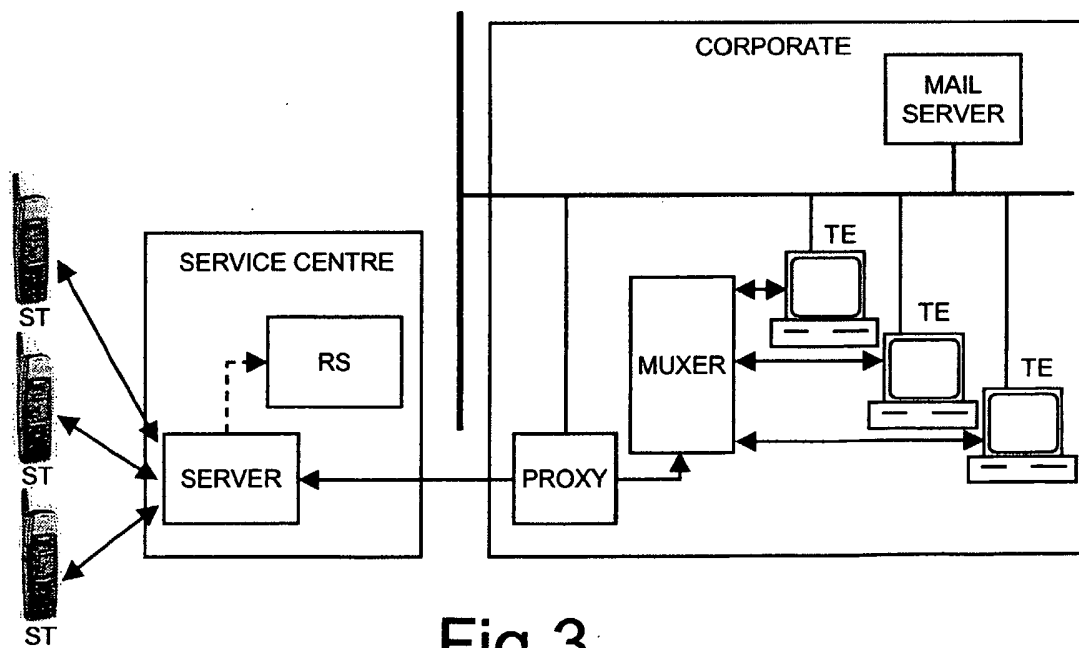
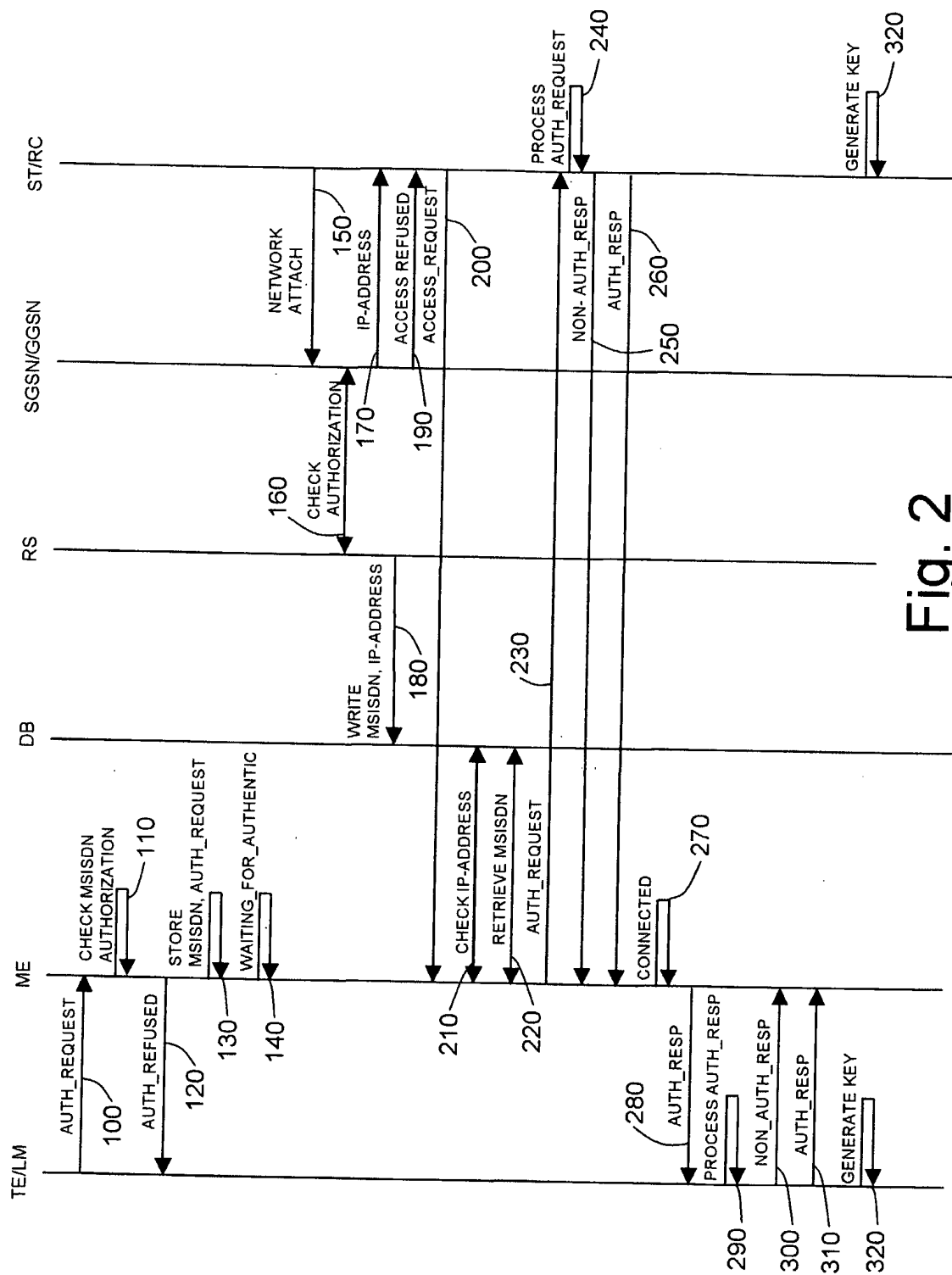


Fig.3

2 / 2



INTERNATIONAL SEARCH REPORT

International Application No.

PCT/EP2004/053717

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L29/06

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)

IPC 7 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, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 126 675 A (MISSION CRITICAL LINUX, INC) 22 August 2001 (2001-08-22) abstract paragraph '0035! - paragraph '0047! figures 2-4c	1-25
A	US 6 061 650 A (MALKIN ET AL) 9 May 2000 (2000-05-09) abstract column 3, line 21 - column 5, line 50 figures 2A-2C ----- -/--	1-25

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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

24 August 2005

Date of mailing of the international search report

31/08/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Bertolissi, E

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP2004/053717

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SRISURESH P: "RFC 2888 Secure Remote Access with L2TP" IETF STANDARD, INTERNET ENGINEERING TASK FORCE, IETF, CH, August 2000 (2000-08), pages 1-19, XP015008671 ISSN: 0000-0003 Abstract 5 Secure remote access -----	1-25
A	MALKIN G S: "Dial-in virtual private networks using layer 3 tunneling" LOCAL COMPUTER NETWORKS, 1997. PROCEEDINGS., 22ND ANNUAL CONFERENCE ON MINNEAPOLIS, MN, USA 2-5 NOV. 1997, LOS ALAMITOS, CA, USA, IEEE COMPUT. SOC, US, 2 November 1997 (1997-11-02), pages 555-561, XP010252462 ISBN: 0-8186-8141-1 Abstract 3 Operational algorithm Figure 2 -----	1-25
A	EP 1 150 474 A (NEC CORPORATION) 31 October 2001 (2001-10-31) abstract paragraph '0043! - paragraph '0048! figure 6 -----	1-25

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP2004/053717

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 1126675	A	22-08-2001	US 6874088 B1	29-03-2005
			EP 1126675 A2	22-08-2001
US 6061650	A	09-05-2000	NONE	
EP 1150474	A	31-10-2001	JP 2001309053 A	02-11-2001
			EP 1150474 A2	31-10-2001
			US 2001037394 A1	01-11-2001