PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/38, 7/32 — **A1**

(11) International Publication Number: **WO 96/36194**

(43) International Publication Date: 14 November 1996 (14.11.96)

(21) International Application Number: PCT/FI96/00266

(22) International Filing Date: 10 May 1996 (10.05.96)

(30) Priority Data:
952339 12 May 1995 (12.05.95) FI

(71) Applicant *(for all designated States except US)*: NOKIA TELECOMMUNICATIONS OY [FI/FI]; Upseerinkatu 1, FIN-02600 Espoo (FI).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: AHVENAINEN, Jouko [FI/FI]; Ristolantie 20 A 7, FIN-00320 Helsinki (FI).

(74) Agent: OY KOLSTER AB; Iso Roobertinkatu 23, P.O. Box 148, FIN-00121 Helsinki (FI).

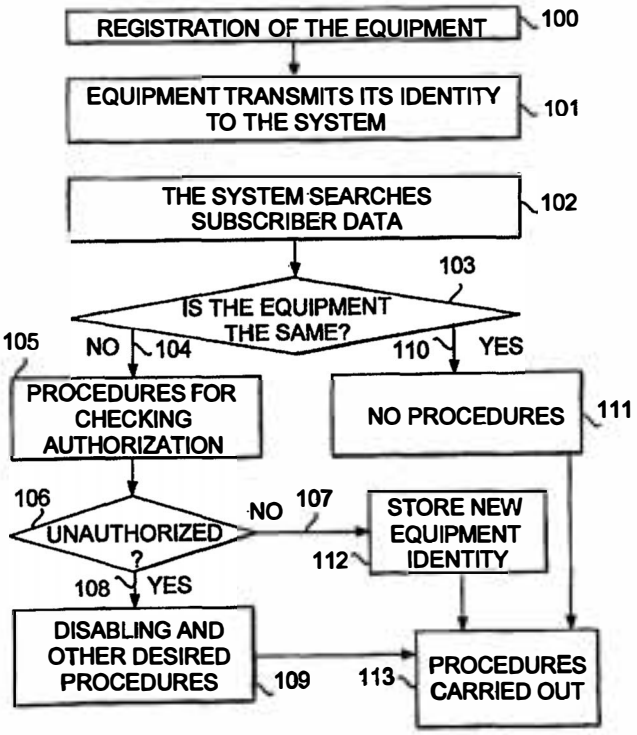
(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CHECKING THE ACCESS RIGHT OF A SUBSCRIBER EQUIPMENT

(57) Abstract

The invention relates to a method for checking the access right of a subscriber equipment in a mobile communication system. In the method, a mobile equipment is registered in a network infrastructure by transmitting the identity of the subscriber from the mobile equipment to the network infrastructure. In the method, the subscriber equipment identity of the mobile equipment is transmitted (101) to the network infrastructure, the subscriber data of the subscriber is checked (102) in the database of the mobile communication system, and the equipment identity of the subscriber, the equipment identity being stored in the database, is compared (103) to the equipment identity transmitted by the mobile equipment, and if the equipment identities are the same (110) the mobile equipment is allowed to continue operation normally, and if the equipment identities differ (104), the access right of the mobile equipment will be checked in the equipment identity register of the network infrastructure.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Annenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

Checking the access right of a subscriber equipment

Field of the Invention

The present invention relates to a method for checking the access right of a subscriber equipment in a mobile communication system comprising a network infrastructure containing a subscriber database, and mobile equipments each of which is a combination of a subscriber equipment provided with an equipment identity and a unique subscriber identity module which contains a subscriber identity and which is detachably coupled to the subscriber equipment, whereby the mobile equipment can be realized by connecting the subscriber identity module to any subscriber equipment, the method comprising the steps of transmitting, from the mobile equipment to the network infrastructure, the subscriber identity contained in the subscriber identity module of said mobile equipment, and transmitting, from the mobile equipment to the network infrastructure, the subscriber equipment identity of said mobile equipment.

The invention relates to a radio system in which subscribers and terminal equipments are not permanently connected together, and particularly terminal equipments and subscriber identity modules, for example SIM cards (SIM - Subscriber Identity Modules), within these networks. Such systems include, for example, cellular networks comprising phones wherein a subscriber is identified by a subscriber-specific subscriber identity module provided in the phones. The GSM (Global System for Mobile Communications) system represents one example of such a cellular communication system. Another example is the TETRA (Trans-European Trunked Radio) mobile communication system. The TETRA mobile communication system, in turn, represents an example of the PMR (Private Mobile Radio) mobile communication system.

Background of the Invention

The subscriber identity module, such as a SIM card, is subscriber specific, which means that subscriber equipments, i.e. the actual radio devices, are not confined to a specific subscriber. The subscriber identity module, such as a SIM card or a GSM card, is a functional card or a smart card which is placed in the mobile equipment and which contains information required for identifying a subscriber and for encrypting radio traffic. In this application, a subscriber identity module, such as a SIM card, refers to a functional card that can be removed from a mobile equipment and by means of which a subscriber is able to use a card controlled mobile equipment.

Consequently, the user need not have a mobile equipment of his own, but a subscriber identity module issued to him by the operator of the mobile communication system is all he needs. Such a subscriber identity module can be, for example, a SIM card (Subscriber Identity Module) which is, in a way, a phone card by means of which the subscriber can make (and receive) calls from any mobile equipment of the system.

As the subscriber identity module, a smart card can be used which has approximately the same dimensions as most credit cards. As an alternative way of implementing a SIM card in hand-held phones, a so-called plug-in-SIM has been introduced. A plug-in-SIM is a coin-sized part containing the electronics of a credit card sized SIM card, and it is placed in a phone so that the user is not able to replace it with ease. The phone may also have an incorporated plug-in-SIM and, in addition, a card reader. If the card reader contains a card, the phone is identified on the basis of the external card, otherwise on the basis of the incorporated plug-in-SIM. In this application, the term subscriber identity module, such as

a SIM card, refers to both the plug-in-SIM and the smart card SIM.

On a general level, the function of a SIM card is specified in the GSM recommendation 02.17, Subscriber Identity Modules, ETSI, of the GSM mobile communication system. It defines the terms associated with a SIM card and sets the requirements for the security of a SIM card, functions of the highest level, defines the tasks for the network operator and the information to be stored in a SIM card. It also specifies the minimum requirements for a SIM card of a user interface of a phone, such as a mobile equipment, concerning for example the input and change of a user's Personal Identification Number (PIN).

In addition, the GSM recommendation 11.11, SIM Application Protocol, ETSI, defines more closely the issues specified by the aforementioned GSM recommendation 02.17 by defining the protocols between a SIM card and a mobile equipment (ME = Mobile Equipment), the exact contents and length of the data fields of the SIM card, as well as the matters related to mechanical and electrical connections. The GSM recommendation 11.11 is a documentation on the basis of which engineers are expected to be able to provide the software and hardware implementation of a SIM interface.

As far as mobile communication systems are concerned, it is known that the mobile subscriber has an identity by means of which the subscriber equipment can be identified, and which indicates, for example, the manufacturer of the subscriber equipment. Mobile communication networks have a facility by which the equipment identity of the subscriber, (in the GSM system, the subscriber IMEI, i.e. International Mobile Equipment Identity) is checked by requesting the equipment identity from the user. The equipment identity of the subscriber is checked for example when it is to be ensured that the

subscriber equipment may be used in the network without it causing interference therein, i.e. that the particular equipment is not stolen or indicated as faulty. The detailed structure of a subscriber equipment identity in connection with the GSM system is described in the GSM standard 03.03, Numbering, Addressing and Identification, version 3.5.0, January 1991, ETSI. The subscriber equipment identity can typically be requested from the subscriber for example whenever the subscriber equipment has established a connection with the mobile telephone exchange. One manner of requesting for the subscriber equipment identity of the subscriber is described in the GSM standard 09.02, Mobile Application Part Specification version 3.8.0, January 1991, ETSI, item 5.9.1, Figure 5.9.1. The same item of the same reference also describes how the subscriber equipment identity is then transmitted to the equipment identity register (EIR) that checks whether the subscriber equipment concerned has the right to use the services of the mobile communication system, i.e. the register checks the access right of the subscriber equipment. The connection from the EIR to the mobile telephone exchange via an F interface is described in item 5.1 of the same standard, especially in Figure 5.1.1.

The EIR or some other part of the mobile telephone network comprises lists according to for example the GSM standard 02.16 (International MS Equipment Identities version 3.0.1, 1992, ETSI), the lists containing subscriber equipment identities or series of subscriber equipment identities and having list identifiers. The standard uses as list identifiers colours that naturally signify for example numerical identifiers. A white colour or identifier is the list identifier of the list consisting of all numerical series containing the equipment identities that have been allocated by the

operators using the same mobile telephone system, i.e. in this case the GSM system, to the subscriber equipments that can be used in the networks concerned. These numerical series are set forth by only indicating the first and last numbers of the series, i.e. not by listing the identities of individual subscriber equipments. A list marked with a black colour or list identifier contains the identities of all the subscriber equipments that must be denied access to the mobile network or to the mobile equipment, for example because the subscriber equipment concerned is faulty and might cause interference in the mobile system itself or because the equipment has been stolen.

When the use of a subscriber equipment is to be prevented in the mobile network or when for example a disabling signal is to be transmitted to a subscriber equipment, the access right of the subscriber equipment must be checked for example in the above-described manner. A typical situation requiring prevention of use of a subscriber equipment or disabling of the equipment occurs when the subscriber or terminal equipment has been stolen and its use is to be prevented. In such a case, a disabling message must be transmitted to the unauthorized subscriber equipment or the equipment must be rendered inoperative in some other manner.

As described above, it is known in the GSM mobile system that the mobile network checks the access right of a subscriber equipment by randomly requesting the identity data of the subscriber equipment from the equipment and by examining from its own equipment identity register (EIR) by means of the data whether the use of the subscriber equipment concerned is allowed in the network. However, the equipment identity of a subscriber equipment is not necessarily requested for, nor is the aforementioned checking performed in connection with each registration.

Therefore, there may be long periods during which the access right of the subscriber equipment is not checked. On the other hand, it is possible in the GSM system to request the identity of the subscriber equipment and thus to check the access right of the equipment randomly, at random intervals.

If the checkings are random, they load the radio path, the equipments on the path, and the data links between the exchange concerned and the equipment database, even though there were no reason to suspect that the equipment of the subscriber is on the black list of the EIR.

Random checkings do not prevent the use of a stolen equipment, either, if there happens to be no checking. This problem can be amended by performing checkings more often, but this in turn loads the connections and equipments even more.

Yet another alternative for checking the access right of a subscriber equipment is to perform the checking by means of the subscriber equipment identity in the EIR in connection with each registration.

Such transmission of the equipment data and the checking of the data in the EIR performed in connection with each registration load the equipments and the system considerably, as this takes up a lot of system internal data transmission capacity, and a lot of processing capacity in the equipment identity register itself.

Brief Description of the Invention

The purpose of the present invention is to solve the problems related to the prior art solutions. The object of the invention is to implement a method and a mobile communication system by means of which the checking of the access right of a subscriber equipment can be started at a necessary instant so that it can be ensured that the subscriber equipments using the mobile network

have the right to use the network, in such a way that the telecommunication equipments and the subscriber equipment register of the mobile network are not overloaded.

It is an object of the present invention to implement this new method and mobile communication system to be as efficient and reliable as possible.

This new type of method for checking the access right of the subscriber equipment will be achieved by the method of the invention, which is characterized by comprising the steps of:

maintaining, at the home database of the network infrastructure, subscriber-specific information on subscriber equipment identities allowed to the subscriber identity,

comparing the subscriber equipment identity, transmitted by the mobile equipment to the network infrastructure, to the equipment identities allowed to the subscriber identity, these being stored in the home database, and

if the equipment identity transmitted by said mobile equipment can be found among those equipment identities allowed to the subscriber identity, the operation of the mobile equipment continues in the normal manner, and

if the equipment identity transmitted by said mobile equipment cannot be found among those equipment identities allowed to the subscriber identity, the access right of the subscriber equipment will be checked in the equipment identity register of the network infrastructure.

The invention further relates to a mobile communication system comprising a network infrastructure containing a home database and an equipment identity register, and mobile equipments each of which is a combination of a subscriber equipment provided with an equipment identity and a unique subscriber identity module

which is detachably coupled to the subscriber equipment, whereby the mobile equipment can be realized by connecting the subscriber identity module to any subscriber equipment.

The mobile communication system of the invention is characterized in that the home database of the mobile communication network is arranged to maintain subscriber-specific information on subscriber equipment identities allowed to said subscriber identity.

The invention is based on the idea that the method includes maintaining, at the home database of the network infrastructure, subscriber-specific information on subscriber equipment identities allowed to the subscriber identity, and comparing the subscriber equipment identity, transmitted by the mobile equipment to the network infrastructure, to the equipment identities allowed to the subscriber identity, these being stored in the home database. For this purpose, there is stored in the subscriber data of the subscriber database the identity, i.e. subscriber equipment identity (IMEI), of the terminal equipment last used by the subscriber in question. When the mobile equipment is next registered in the network infrastructure, the subscriber is, in conjunction with the registration, requested the identity of the subscriber equipment he is using. As soon as the network infrastructure has obtained the subscriber equipment identity associated with the new registration, it is compared to the subscriber equipment identity stored earlier in the network infrastructure. On the basis of this comparison, if the subscriber equipment identities compared match, the network infrastructure finds out that the mobile equipment involves the same subscriber equipment and subscriber identity module as the last time. As a result, normal registration of the mobile equipment to the network infrastructure is initiated. If, on the

other hand, it is found out on the basis of the comparison that the subscriber equipment identities compared differ, the network infrastructure finds out that the mobile equipment involves a different subscriber equipment and subscriber identity module than the last time. As a result, the access right of the mobile equipment will be checked in the network infrastructure, for example by carrying out an enquiry to the equipment identity register (EIR). Therefore, the system is able to carry out procedures necessary for preventing the use of unauthorized equipments within the system. After completion of the checking, and after finding out that the subscriber data of the "new" subscriber does not contain an indication ordering said subscriber equipment to be disabled from the system or otherwise restricting the operation of the subscriber equipment, the identity data of the new subscriber is stored in the subscriber data and, consequently, the registration of the subscriber and the subscriber equipment to the system continues normally.

To sum up, the method and mobile communication system according to the invention operate so that the system compares, as the subscriber is registering into the system, the identity data i.e. the mobile equipment identity IMEI being transmitted by the subscriber equipment, to the identity data in the subscriber data of the system memory. If, on the basis of the identity data, the system finds out that a different equipment is being used from the subscriber connection than the last time, the system carries out necessary procedures to check the access right of the equipment, and on the basis of these procedures takes necessary measures, for example disables the mobile equipment from the mobile communication system.

Thus, the idea of the invention is that in a mobile communication system which does not restrict the subscriber to a specific terminal equipment, the identity

of the terminal equipment last used by the subscriber (i.e. the subscriber equipment identity) is stored in the subscriber data within the subscriber data register of the system. When the subscriber next registrates in the network, or the checking is carried out for example randomly, and if it is found out that the equipment of the subscriber connection is not the same, measures are taken by which the use of unauthorised equipments will be prevented. It should be noted that in the subscriber data it is possible to store several subscriber equipment identities as "allowed" previous equipment identities. This makes it unnecessary to check the identity of the subscriber equipment in the equipment identity register (EIR) even if the situation concerns some other subscriber equipment than the one that the subscriber last used, if the identity of the subscriber equipment can be found among the allowed equipment identities that have on purpose been programmed as allowed ones without checking the subscriber equipment identity.

The advantage of such an arrangement according to the invention is that the subscriber equipment identity is not transmitted and checked randomly, nor is the checking performed too often thus avoiding to overload the system resources. The system checks the data only when there is a real reason to suspect that the equipment is not used by an authorized user, for example. The load on the exchange, terminal equipment, radio link, equipment database and data links is decreased and the operation becomes faster, but a high level of security is maintained.

The solution according to the invention increases security also because in the system according to the invention a subscriber will not be able to avoid checkings with good luck when using an illegal equipment since the access rights of subscriber equipments are checked particularly in situations where it is likely that the

subscriber equipment is not used by an authorized user.

Further, the arrangement according to the invention provides faster detection of unauthorized equipments in the system compared to random checkings. For example in different networks used by the authorities this is very important, since they set very high requirements for information security. The use of a stolen equipment must be detected immediately after the theft has occurred, and an unauthorized user must not be able to use the radio for a long time. Unauthorized use can be minimized with the present invention.

The invention provides the advantage that in the solution thereof the use of an equipment and a subscriber connection can be prevented after a theft or a disappearance, but nevertheless it is not necessary to check the equipment data in the equipment identity register (EIR) in the majority of equipment registration.

If an unauthorized holder of an equipment uses the preceding subscriber identification module, for example a SIM card, in the equipment, the use of the equipment and the subscriber connection can be prevented if it is known that this subscriber equipment or interface should be disabled, whereupon the identity thereof can be set on the black list of the system. In such a case, when the data of this subscriber is checked, the equipment identity and possibly the location in the network can be seen from the subscriber data, whereupon the network can force the subscriber equipment to close. The subscriber data may also be supplemented with information causing the closing of the equipment during the next registration. The checking and identification of subscriber data from the mobile system registers and the possible prevention of the use of the equipment, based merely on equipment data, are thus necessary only in cases where an equipment that is in unauthorized use is not used with the same subscriber

identification module, for example a SIM card, as previously.

The advantages of the invention become evident for example in a situation where a subscriber equipment has been stolen and the new user uses the equipment with another SIM card. If the thief uses the equipment with a new SIM card, the use of the equipment and the subscriber connection can be prevented on the basis of checking the SIM card, since the checking is activated because in the home database there is stored a different equipment identity than the identity of the equipment used.

Brief Description of the Drawings

In the following, the invention will be described with reference to the attached drawings, in which

Figure 1 is a flow chart illustrating the operation of the method and mobile communication system of the invention, and

Figure 2 is a block diagram illustration of the mobile communication system according to the invention.

Detailed Description of the Invention

According to the method of the invention, checking the access right of the subscriber equipment in the equipment identity register (EIR) can be restricted to concern situations in which the subscriber equipment identity has not been stored in the home database in advance.

Figure 1 is a flow chart illustrating the operation of an embodiment of the method and mobile communication system according to the invention.

In the solution of the invention, in the subscriber data of the cellular network there is stored the identity data of the terminal equipment that was last used by the subscriber in question. In case the subscriber uses a different terminal equipment than the last time, the system can carry out desired procedures. For example,

procedures 105 can be activated in order to check the identity of the equipment, or the equipment can be included on a separate list of equipments under supervision.

The equipments must have a specific identity data which can be stored in the subscriber data. This equipment identity data must in some form be sent from the equipment to the system in connection with the subscriber registration. In the GSM system, the equipment identity data in question is IMEI.

In the following, the operation of the invention is described by means of the flow chart of Figure 1. As a subscriber registrates 100 in the mobile communication system, the system acquires the subscriber data and checks whether the subscriber in question is entitled to the services of the system. At the same time the mobile equipment, and particularly its subscriber equipment, also transmits 101 its equipment identity to the mobile communication system. Transmitting the equipment identity can take place automatically every time the mobile equipment registrates in the system, or the mobile communication system can request the mobile equipment identity (IMEI) from the mobile equipment by a specific message. Consequently, the mobile equipment responds to the request by transmitting 101 its subscriber equipment identity to the mobile communication system. Thereafter the system searches 102 the subscriber data from the database. Following this, the method of the invention proceeds to an analysis or comparison stage 103, at which the equipment identity of the mobile equipment stored at an earlier stage in the database is compared to the equipment identity transmitted by the mobile equipment in association with this registration. If, according to the invention, it is detected that the subscriber equipment has changed 104 compared to the one in the subscriber

data, measures 105 are taken in order to check the access right of the subscriber equipment. A multitude of methods are available for checking the access right of the equipment after finding out that the equipment is not the same 104 as the one previously used by the subscriber. The method to be applied may depend on which type of a system is in question and how the subscribers in it usually act. The procedures to be taken may include transmitting a checking request to the equipment identity register (EIR) or a similar database, such as a list of stolen equipments. Alternatively, the checking request can be repeated at predetermined intervals for a specific time, or the subscriber and the equipment can be included on a list of devices under supervision, whereupon their entitlement to use the network is checked at predetermined intervals or randomly during the predetermined time. In connection with the change, also time data can be included therein, whereby the aforementioned request can be repeated at predetermined intervals for a predetermined period of time. This makes it possible to ensure that information on the displacement or stealing of the equipment has reached the list of unauthorized equipments.

As a result, if a subscriber equipment in the mobile equipment is found to be unauthorized 108 on the basis of the comparison 106, it is possible to activate procedures of the network itself in order to disable 109 the subscriber equipment and the subscriber in question from the network. An effort can be made to disable the subscriber and the subscriber equipment, or their data can be stored in a register of susceptible subscribers or subscriber equipments, whereby their rights, for example speech rights in the network, can be restricted.

Information on a new equipment - subscriber combination can also be transmitted 109 to a separate list which stores the information for a specific time. The

contents of this list may be checked every time a new equipment is added on the list of unauthorized equipments.

The system may also contain a list of equipments that are known to pass to a new subscriber legally. The change data can be compared to the list, and further procedures will be unnecessary if the new equipment of the subscriber is found on the list. The list can be maintained by the operator, or by means of transmitting a message from the former owner of the equipment. If such messages are to be transmitted, it must be carried out by using a secret personal identification number in order for an unauthorized holder to be unable to send it.

If, on the basis of the various comparisons 106, it is found out that the subscriber equipment in question is not unauthorized 107, the identity (IMEI) of that equipment which has been attached to the subscriber and which together with the subscriber (i.e. the subscriber identity module, such as a SIM card) forms a mobile equipment is stored 112 in the subscriber database of the mobile communication system. The stored identity of the new subscriber equipment will then be employed in a similar comparison when the mobile equipment next registers in the mobile communication system in question.

If, on the other hand, it is found out on the basis of the aforementioned comparison 103 that the equipment used in connection with said subscriber is the same 110 as previously, no procedures are carried out, and the operation of the mobile equipment and the mobile communication system continues normally.

In all the preceding cases after steps 109, 111 and 112, upon completion of all the procedures of the invention, the process continues in accordance with normal operation of a mobile communication system.

Figure 2 is a block diagram illustration of the mobile communication system according to the invention.

Figure 2 shows a mobile communication system comprising a network infrastructure 600 containing a subscriber database 601, and mobile equipments 500 each of which is a combination of a subscriber equipment 200 provided with an equipment identity and a unique subscriber identity module 509, such as a SIM card. The subscriber identity module 509 is detachably coupled to the subscriber equipment 200, whereby the mobile equipment 500 can be realized by connecting the subscriber identity module 509 to any subscriber equipment 200.

The mobile communication system of the invention comprises a comparing means 602 for comparing 103 (Figure 1) the subscriber's mobile equipment identity (IMEI), stored in the subscriber database 601, to the equipment identity transmitted 101 (Figure 1) by said mobile equipment 500. On the basis of this comparison 103, if said equipment identities are identical 110 (Figure 1), the mobile equipment is allowed to continue normal operation 111. If said equipment identities are different 104, the access right of the mobile equipment will be checked 105 in the equipment identity register EIR of the network infrastructure.

The subscriber database 601 referred to in the above may be, for example, a home location register (HLR) of the GSM mobile communication system.

The mobile communication system of the invention further comprises a database 603, to which, according to said second checking alternative 105, the identity of the subscriber equipment 200 and the subscriber identity, which is obtained from the subscriber identity module 509, are stored 112 for a predetermined period of time.

Furthermore, the mobile communication system of the invention comprises a checking means 604 for checking 107 the access right of the subscriber equipment at predetermined intervals in the network infrastructure 600

in response to said database entry.

In addition, the mobile communication system according to the invention comprises a database 605 which stores the identities of those subscriber equipments 200 that have legally passed to a new owner.

The figures and the description related thereto are only intended to illustrate the idea of the invention. The method according to the invention for checking the access right of a subscriber equipment in a mobile communication system may vary in details within the scope of the claims. Although the invention is in the above described mainly in connection with the GSM and TETRA mobile communication systems, the invention is applicable to further developments thereof and in other types of mobile communication systems.

The solutions according to the invention do not deal with on how the equipment data is checked from the subscriber equipment register of the network. According to the solutions in accordance with the invention, the mobile communication system of the invention, for example the exchange to which the subscriber in question is registered, initiates checkings regarding the access right of the subscriber equipment in suspicious cases, i.e. when the subscriber tries to employ the mobile communication system from such a subscriber equipment whose equipment identity cannot be found among those equipment identities stored in the home database that are allowed to the subscriber identity.

Claims

1. A method for checking the access right of a subscriber equipment (200) in a mobile communication system comprising a network infrastructure containing a home database (601) and an equipment identity register, and mobile equipments (500) each of which is a combination of a subscriber equipment (200) provided with an equipment identity and a unique subscriber identity module (509) which contains a subscriber identity and which is detachably coupled to the subscriber equipment (200), whereby the mobile equipment (500) can be realized by connecting the subscriber identity module to any subscriber equipment (200), the method comprising the steps of

transmitting, from the mobile equipment (500) to the network infrastructure (600), the subscriber identity contained in the subscriber identity module (509) of said mobile equipment (500), and

transmitting, from the mobile equipment (500) to the network infrastructure (600), the subscriber equipment identity of said mobile equipment (500),

c h a r a c t e r i z e d by the method comprising the steps of:

maintaining, at the home database (601) of the network infrastructure (600), subscriber-specific information on subscriber equipment identities allowed to the subscriber identity,

comparing the subscriber equipment identity, transmitted by the mobile equipment (500) to the network infrastructure (600), to the equipment identities allowed to the subscriber identity, these being stored in the home database (601), and

if the equipment identity transmitted by said mobile equipment (500) can be found among those equipment

identities allowed to the subscriber identity, the operation of the mobile equipment (500) continues in the normal manner, and

if the equipment identity transmitted by said mobile equipment (500) cannot be found among those equipment identities allowed to the subscriber identity, the access right of the subscriber equipment (200) will be checked in the equipment identity register of the network infrastructure (600).

2. A method as claimed in claim 1, c h a r a c t e r i z e d in that if the checking into the equipment identity register results in that said subscriber equipment has an access right to said network infrastructure (600), the identity of said subscriber equipment is stored in the home database (601) of the network infrastructure (600) among the equipment identities allowed to said subscriber identity, and the operation of said mobile equipment (500) will be allowed to continue normally.

3. A method as claimed in claim 1, c h a r a c t e r i z e d in that if said checking into the equipment identity register results in that said subscriber equipment has no access right to the network infrastructure (600), said mobile equipment (500) will be disabled.

4. A method as claimed in claim 1, c h a r a c t e r i z e d in that said access right of the subscriber equipment (200) is checked at desired intervals.

5. A method as claimed in claim 1, c h a r a c t e r i z e d in that if the equipment identity transmitted by said mobile equipment (500) cannot be found among those equipment identities allowed to said subscriber identity, the subscriber equipment identity and the subscriber identity will be stored for a predetermined

time in a database within the network infrastructure (600), and the access right of the subscriber equipment (200) will be checked in the equipment identity register of the network infrastructure (600) at predetermined intervals in response to said database entry.

6. A method as claimed in claim 1, c h a r a c t e r i z e d in that if the equipment identity transmitted by said mobile equipment (500) cannot be found among equipment identities allowed to said subscriber identity, the access right of the subscriber equipment (200) will, on the basis of the subscriber equipment identity, be checked in the database which includes the identities of those subscriber equipments (200) that have legally passed to a new owner.

7. A mobile communication system comprising a network infrastructure (600) containing a home database (601) and an equipment identity register, and mobile equipments (500) each of which is a combination of a subscriber equipment (200) provided with an equipment identity and a unique subscriber identity module (509) which is detachably coupled to the subscriber equipment (200), whereby the mobile equipment (500) can be realized by connecting the subscriber identity module (509) to any subscriber equipment (200), c h a r a c t e r i z e d in that the home database (601) of the mobile communication network is arranged to maintain subscriber-specific information on subscriber equipment identities allowed to said subscriber identity.

8. A mobile communication system as claimed in claim 7, c h a r a c t e r i z e d in that the mobile communication system comprises a comparing means for comparing the subscriber equipment identity, transmitted by the mobile equipment (500) to the network infrastructure (600), to the subscriber equipment identities maintained in said home database that are

allowed to said subscriber identity.

9. A mobile communication system as claimed in claim 8, c h a r a c t e r i z e d in that said comparing means is, on the basis of the comparison carried out, arranged to allow the operation of the mobile equipment to continue normally if the equipment identity transmitted by said mobile equipment (500) can be found among those equipment identities allowed to said subscriber identity.

10. A mobile communication system as claimed in claim 8, c h a r a c t e r i z e d in that said comparing means is, on the basis of the comparison, arranged to check the access right of the subscriber equipment (200) in the equipment identity register of the network infrastructure (600), if the equipment identity transmitted by said mobile equipment (500) cannot be found among those equipment identities allowed to said subscriber identity.

11. A mobile communication system as claimed in claim 7, c h a r a c t e r i z e d in that the mobile communication system further comprises a checking means (604) for checking (105, 106) the access right of the subscriber equipment (200) in the network infrastructure (600) at predetermined intervals.

12. A mobile communication system as claimed in claim 7, c h a r a c t e r i z e d in that the mobile communication system further comprises a database (605) which includes the identities of those subscriber equipments (200) that have legally passed to new owners.

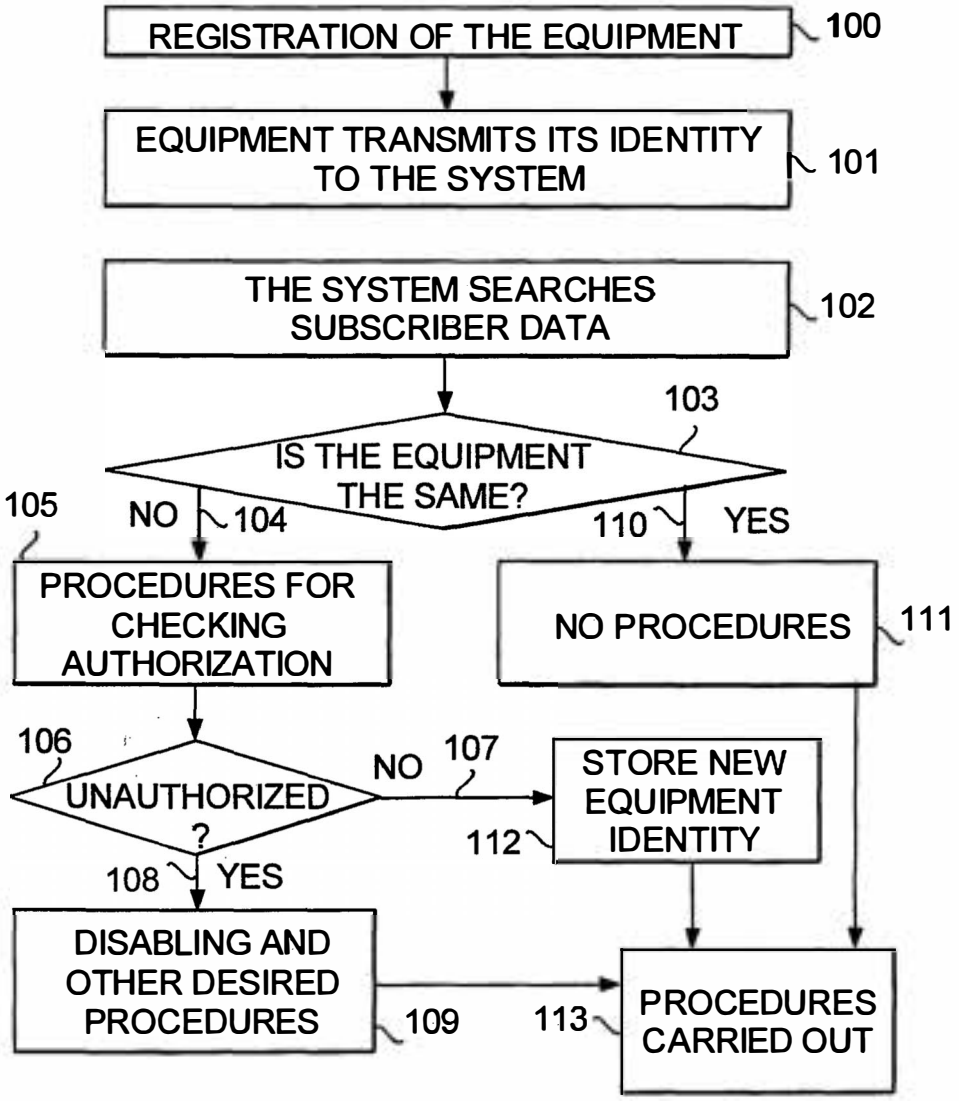

REGISTRATION OF THE EQUIPMENT
100
EQUIPMENT TRANSMITS ITS IDENTITY TO THE SYSTEM
101
THE SYSTEM SEARCHES SUBSCRIBER DATA
102
103
IS THE EQUIPMENT THE SAME?
105
NO
104
110
YES
PROCEDURES FOR CHECKING AUTHORIZATION
NO PROCEDURES
111
106
UNAUTHORIZED ?
NO
107
STORE NEW EQUIPMENT IDENTITY
112
108
YES
DISABLING AND OTHER DESIRED PROCEDURES
109
113
PROCEDURES CARRIED OUT

FIG. 1

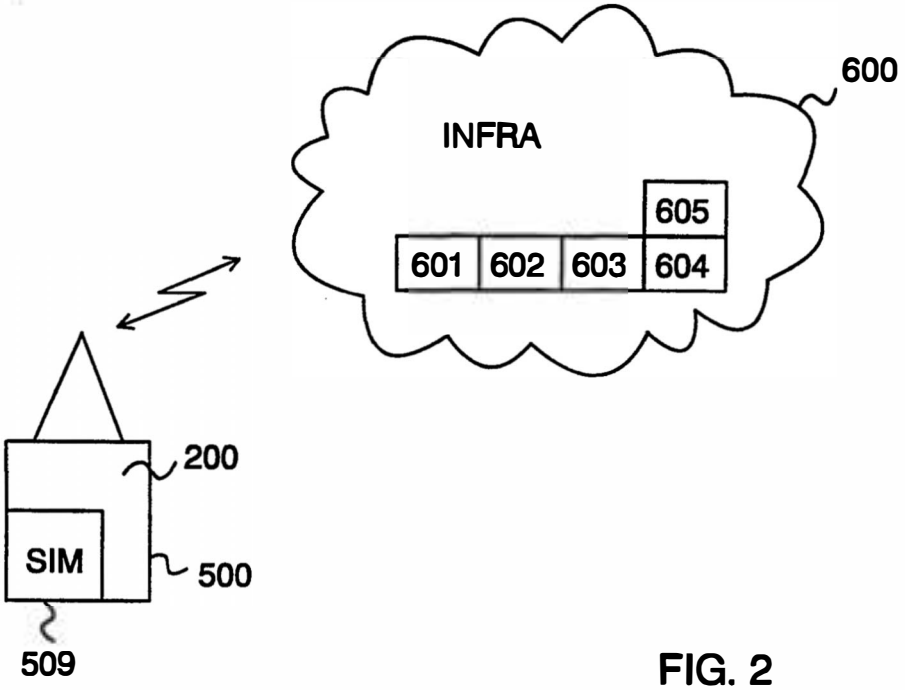


FIG. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 96/00266

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04Q 7/38, H04Q 7/32
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)

IPC6: H04Q, H04M

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

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0607767 A1 (ERICSSON - GE MOBILE COMMUNICATIONS INC.), 27 July 1994 (27.07.94), see whole document --	1-12
Y	GB 2248999 A (VODAFONE LIMITED), 22 April 1992 (22.04.92), page 2 - page 4 --	1-12
A	WO 9501695 A1 (MOTOROLA, INC.), 12 January 1995 (12.01.95), see whole document --	1-12
A	EP 0448369 A2 (NOKIA MOBILE PHONES LTD.), 25 Sept 1991 (25.09.91), page 4, line 6 - line 32 -- --------	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 Sept 1996	13 -09- 1996
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Marcus Wik Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT
Information on patent family members

31/07/96

International application No.
PCT/FI 96/00266

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A1- 0607767	27/07/94	AU-A- 5049893	19/05/94
		BR-A- 9304655	14/06/94
		BR-A- 9394655	14/06/94
		CA-A- 2102391	10/05/94
		CN-A- 1091877	07/09/94
		DE-U- 9217379	29/04/93
		FI-A- 934924	10/05/94
		JP-A- 6216842	05/08/94
		NZ-A- 248995	28/05/96
		SE-B,C- 470519	27/06/94
		SE-A- 9203351	10/05/94
GB-A- 2248999	22/04/92	EP-A- 0481714	22/04/92
		PT-A- 99263	31/01/94
WO-A1- 9501695	12/01/95	AU-A- 7245794	24/01/95
		CN-A- 1110892	25/10/95
		FR-A,B- 2708402	03/02/95
		GB-A- 2285559	12/07/95
		GB-D- 9504240	00/00/00
		IT-D- RM940425	00/00/00
		SE-A- 9500723	18/04/95
		US-A- 5444764	22/08/95
		ZA-A- 9404791	20/02/95
EP-A2- 0448369	25/09/91	JP-A- 7074856	17/03/95
		US-A- 5266782	30/11/93