



HU000032255T2

(19) **HU**(11) Lajstromszám: **E 032 255**(13) **T2****MAGYARORSZÁG**
Szellemi Tulajdon Nemzeti Hivatala**EURÓPAI SZABADALOM**
SZÖVEGÉNEK FORDÍTÁSA(21) Magyar ügyszám: **E 11 767373**(22) A bejelentés napja: **2011. 09. 13.**

(96) Az európai bejelentés bejelentési száma:

EP 20110767373

(97) Az európai bejelentés közzétételi adatai:

EP 2756703 A1 **2013. 03. 21.**

(97) Az európai szabadalom megadásának meghirdetési adatai:

EP 2756703 B1 **2016. 11. 09.**(51) Int. Cl.: **H04W 12/12** (2006.01)**H04W 4/12** (2006.01)**H04W 88/02** (2006.01)

(86) A nemzetközi (PCT) bejelentési szám:

PCT/EP 11/004583

(87) A nemzetközi közzétételi szám:

WO 13037383(72) Feltaláló(k):
HABERKORN, Günter, 92262 Birgland/Schwend (DE)(73) Jogosult(ak):
Deutsche Telekom AG, 53113 Bonn (DE)(74) Képviselő:
**Advopatent Szabadalmi és Védjegy Iroda,
Budapest**(54) **Eljárás csalás és visszaélés megakadályozására nyilvános földi mobilhálózat meghatározott szolgáltatásának használatakor felhasználói készülékkel, előfizetői azonosító modul és alkalmazási program**

Az európai szabadalom ellen, megadásának az Európai Szabadalmi Közlönyben való meghirdetésétől számított kilenc hónapon belül, felszólalást lehet benyújtani az Európai Szabadalmi Hivatalnál. (Európai Szabadalmi Egyezmény 99. cikk(1))

A fordítást a szabadalmat az 1995. évi XXXIII. törvény 84/H. §-a szerint nyújtotta be. A fordítás tartalmi helyességét a Szellemi Tulajdon Nemzeti Hivatala nem vizsgálta.

(19)



(11)

EP 2 756 703 B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
09.11.2016 Bulletin 2016/45

(51) Int Cl.:
H04W 12/12^(2009.01) H04W 4/12^(2009.01)
H04W 88/02^(2009.01)

(21) Application number: **11767373.1**

(86) International application number:
PCT/EP2011/004583

(22) Date of filing: **13.09.2011**

(87) International publication number:
WO 2013/037383 (21.03.2013 Gazette 2013/12)

(54) **METHOD FOR PREVENTING FRAUD OR MISUSE WHEN USING A SPECIFIC SERVICE OF A PUBLIC LAND MOBILE NETWORK BY A USER EQUIPMENT, SUBSCRIBER IDENTITY MODULE AND APPLICATION PROGRAM**

VERFAHREN ZUM SCHUTZ VOR BETRUG ODER VOR MISSBRAUCH BEI VERWENDUNG EINES BESTIMMTEN DIENSTES EINES ÖFFENTLICHEN LANDFUNKNETZES DURCH EIN BENUTZERGERÄT, TEILNEHMERIDENTITÄTSMODUL UND ANWENDUNGSPROGRAMM

PROCÉDÉ DE PRÉVENTION DE FRAUDE OU D'EMPLOI ABUSIF EN CAS D'UTILISATION D'UN SERVICE SPÉCIFIQUE D'UN RÉSEAU MOBILE TERRESTRE PUBLIC PAR UN ÉQUIPEMENT D'UTILISATEUR, MODULE D'IDENTITÉ D'ABONNÉ ET PROGRAMME D'APPLICATION

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(72) Inventor: **HABERKORN, Günter**
92262 Birgland/Schwend (DE)

(43) Date of publication of application:
23.07.2014 Bulletin 2014/30

(74) Representative: **Schwöbel, Thilo K. et al**
Kutzenberger Wolff & Partner
Theodor-Heuss-Ring 23
50668 Köln (DE)

(73) Proprietor: **Deutsche Telekom AG**
53113 Bonn (DE)

(56) References cited:
EP-A1- 1 225 747 WO-A2-03/005738

EP 2 756 703 B1

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Description

BACKGROUND

[0001] The present invention relates a method for preventing fraud or misuse when using a specific service of a public land mobile network by a User Equipment. The present invention further relates to Subscriber Identity Module for preventing fraud or misuse when a User Equipment equipped with the Subscriber Identity Module uses a specific service of a public land mobile network.

[0002] Operators of telecommunications network, especially public land mobile networks, typically protect network nodes that are used to provide specific services for User Equipments, such as the Short Message Service Center for providing the short message service, wherein the protection is provided such that customers that should not use such a network node are excluded from using such a network node.

[0003] In case this protection of such a network node is permanently or temporarily not available or efficient, fraud or misuse scenarios can occur. For example, with respect to the short message service, such a fraud or misuse scenario might occur in case when a User Equipment (of a home public land mobile network) roams in a visited public land mobile network (different to the home public land mobile network) and an unprotected Short Message Service Center in a further public land mobile network instead of the (home) Short Message Service Center in the home public land mobile network. In such a case, mobile originated short message service traffic is routed from the visited public land mobile network (where the User Equipment roams) to the further public land mobile network, and therefore bypasses the home public land mobile network. Nevertheless, the inter operator tariffs still apply in the relation between the visited public land mobile network and the home public land mobile network, which can cause huge damages to the operator of the home public land mobile network. Another example of primarily a misuse case and not a fraud situation would be to use a wrong Short Message Service Center address setting within a home public land mobile network due to the fact that the User Equipment has been bought second hand and has been used in another public land mobile network and hence with another setting of the Short Message Service Center address.

[0004] WO03/005738 A2 discloses a method to verify the Short Message Service Center address setting.

SUMMARY

[0005] An object of the present invention is to provide cost effective solution for preventing such fraud or misuse scenarios when using a specific service of a public land mobile network by a User Equipment.

[0006] The object of the present invention is achieved by a method for preventing fraud or misuse when using a specific service of a public land mobile network by a

User Equipment, wherein the User Equipment comprises a Subscriber Identity Module, wherein the Subscriber Identity Module comprises an address information used for the specific service of the public land mobile network, wherein the Subscriber Identity Module comprises an application program, wherein the application program comprises a reference address information, wherein the application program is provided such that the following steps are executed:

-- in a first step, it is verified whether the address information corresponds to the reference address information,

-- in a second step, and in case that the verification of the first step holds a negative result,

-- either the specific service is invoked using the reference address information, wherein a wrong address information is replaced by the reference address information in case the reference address information is either a complete address information being able to specify a network entity in a telecommunications network and/or the public land mobile network,

-- or the specific service is blocked, at least temporarily, for the User Equipment, in case the reference address information is an incomplete address information being unable to specify a network entity in a telecommunications network and/or the public land mobile network, wherein the reference address information comprises a country code of the address information to use.

[0007] According to the present invention, it is thereby advantageously possible that fraud or misuse can be effectively reduced by means of enforcing the use of the correct address information, especially for specifying a network node by means of the address information.

[0008] According to another preferred embodiment of the present invention, in case that, during the second step, the specific service is blocked for the User Equipment, an error message is sent to the public land mobile network.

[0009] According to the present invention, it is thereby advantageously that the public land mobile network, especially the home public land mobile network is informed about the incorrect setting of the address information such that a self-healing process can be triggered, e.g. by means of providing a configuration message to the corresponding User Equipment in order to change the incorrect address information.

[0010] According to a preferred embodiment of the present invention, the address information is provided at a specific memory location within the Subscriber Identity Module, wherein the application program is configured such that, during the first step, the specific memory location within the Subscriber Identity Module is verified repeatedly, at least once in a predetermined time interval.

[0011] Thereby, it is advantageously possible accord-

ing to the present invention that a wrong setting of the address information can be detected easily and quickly. Especially, it is advantageously possible to transmit the application program to the User Equipment and without an interruption of the functionality of the User Equipment / Subscriber Identity Module (especially without rebooting the User Equipment), verification of the address information is performed.

[0012] According to a further preferred embodiment of the present invention, a request of the User Equipment to use the specific service comprises the address information, wherein the User Equipment is configured such that each request of the User Equipment to use the specific service is directed to the Subscriber Identity Module, wherein the application program is configured such that, during the first step, the address information of the redirected request of the User Equipment to use the specific service is verified.

[0013] Thereby, it is advantageously possible according to the present invention that no request of the specific service can be transmitted to the public land mobile network without the verification by the Subscriber Identity Module (during the first step of the inventive method).

[0014] Of course, it is also possible that both a repeated verification of the correct address information is performed and a forced redirection of any requests of the User Equipment to the specific service towards the Subscriber Identity Module.

[0015] According to another preferred embodiment of the present invention, the specific service is the short message service.

[0016] Thereby, it is advantageously possible to avoid fraud and misuse damages for an operator of a public land mobile network in a comparably easy manner.

[0017] It is furthermore preferred that the address information and the reference address information relates to the address of a Short Message Service Center used by the User Equipment.

[0018] Thereby, it is easily possible according to the present invention that no short message service functionality can be used by the User Equipment without using the correct Short Message Service Center.

[0019] According to the present invention, it is furthermore preferred that the reference address information relates to the address of a Short Message Service Center used by the User Equipment but that the reference address information is not a complete address information, (being able to specify a network entity in the telecommunications network) such as, e.g., a global title, but that the reference address information corresponds to the country code of the correct address information 22 to be used or that the reference address information corresponds to the country code and additionally a certain number (such as one or two or three or four) of digits, specifying, e.g., the public land mobile network of the operator or the like. If in this case a comparison (during the first step of the method according to the present invention) of the reference address information with the

address information (or with the corresponding part or with the corresponding part of the address information) holds that the address information is not correct, the appropriate actions are taken as specified in the second step of the present invention.

[0020] Furthermore, the present invention relates to a Subscriber Identity Module for preventing fraud or misuse when a User Equipment equipped with the Subscriber Identity Module uses a specific service of a public land mobile network, wherein the Subscriber Identity Module comprises an address information used for the specific service of the public land mobile network, wherein the Subscriber Identity Module comprises an application program, wherein the application program comprises a reference address information, wherein the application program is provided such that:

-- a verification is executed whether the address information corresponds to the reference address information, and

-- in case that the verification holds a negative result, -- either the specific service is invoked using the reference address information, wherein a wrong address information is replaced by the reference address information in case the reference address information is either a complete address information being able to specify a network entity in a telecommunications network and/or the public land mobile network,

-- or the specific service is blocked, at least temporarily, for the User Equipment, in case the reference address information is an incomplete address information being unable to specify a network entity in a telecommunications network and/or the public land mobile network, wherein the reference address information comprises a country code of the address information to use.

[0021] Additionally, the present invention relates to a program comprising a computer readable program code which, when executed on a computer or on a Subscriber Identity Module, causes the computer or the Subscriber Identity Module to perform an inventive method.

[0022] Still additionally, the present invention relates to computer program product for preventing fraud or misuse when using a specific service of a public land mobile network by a User Equipment, the computer program product comprising a computer program stored on a storage medium, the computer program comprising program code which, when executed on a computer or on a Subscriber Identity Module, causes the computer or the Subscriber Identity Module to perform an inventive method.

[0023] These and other characteristics, features and advantages of the present invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, which illustrate, by way of example, the principles of the invention. The description is given for the sake of example only,

without limiting the scope of the invention. The reference figures quoted below refer to the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024]

Figure 1 schematically illustrates the handling of a mobile originating short message sent from a User Equipment roaming in a visited public land mobile network which is different from the home public land mobile network of that User Equipment.

Figure 2 schematically illustrates a fraud scenario of the handling of a mobile originating short message sent from a User Equipment roaming in a visited public land mobile network, wherein the home public land mobile network is bypassed by using a Short Message Service Center of a further public land mobile network instead of the Short Message Service Center of the home public land mobile network.

Figure 3 schematically illustrates a method for providing a Subscriber Identity Module with an application program for performing the inventive method.

Figure 4 schematically illustrates an implementation of the inventive method.

DETAILED DESCRIPTION

[0025] The present invention will be described with respect to particular embodiments and with reference to certain drawings but the invention is not limited thereto but only by the claims. The drawings described are only schematic and are non-limiting. In the drawings, the size of some of the elements may be exaggerated and not drawn on scale for illustrative purposes.

[0026] Where an indefinite or definite article is used when referring to a singular noun, e.g. "a", "an", "the", this includes a plural of that noun unless something else is specifically stated.

[0027] Furthermore, the terms first, second, third and the like in the description and in the claims are used for distinguishing between similar elements and not necessarily for describing a sequential or chronological order. It is to be understood that the terms so used are interchangeable under appropriate circumstances and that the embodiments of the invention described herein are capable of operation in other sequences than described or illustrated herein.

[0028] In Figure 1, the handling of a mobile originating short message (SMS) in a telecommunications network is schematically shown. The short message (SMS) is sent from a User Equipment 20 roaming in a visited public land mobile network B which is different from a home public land mobile network A of that User Equipment 20. The User Equipment 20 sends a request for using the

short message service of the visited public land mobile network B to a specific network node 30 (typically a Mobile Switching Center 30) of the visited public land mobile network B. The request of the User Equipment 20 specifies, by means of an address information, the Short Message Service Center 240 of the home public land mobile network A and the short message (SMS) is sent triggering an IOT (inter operator tariff) charging event 41 from the visited public land mobile network B to the home public land mobile network A and a client charging event 42 from the home public land mobile network A to the User Equipment / the subscriber.

[0029] In Figure 2, a fraud or misuse scenario of a mobile originating short message (SMS) in a telecommunications network is schematically shown. The short message (SMS) is sent from a User Equipment 20 roaming in a visited public land mobile network B which is different from a home public land mobile network A of that User Equipment 20. The User Equipment 20 sends a request for using the short message service of the visited public land mobile network B to a specific network node 30 (typically a Mobile Switching Center 30) of the visited public land mobile network B. The request of the User Equipment 20 specifies, by means of an address information (and instead of the Short Message Service Center 240 of the home public land mobile network A) the Short Message Service Center 220 of a further public land mobile network C. This results in the short message (SMS) being sent via the further public land mobile network C and bypassing the home public land mobile network A. Involving the visited public land mobile network nevertheless triggers an IOT (inter operator tariff) charging event 41 from the visited public land mobile network B to the home public land mobile network A. However, due to the fact that the home public land mobile network A is bypassed regarding the handling of the short message, a corresponding client charging event 42' from the home public land mobile network A to the User Equipment / the subscriber is not possible. That is why huge amounts of short messages can be sent using this fraud or misuse scenario causing at the home public land mobile network massive losses. Currently, it is not mandatorily required that the visited public land mobile network B informs the home public land mobile network A about such irregularities. Therefore, such frauds or misuses cannot be quickly detected by the home public land mobile network A.

[0030] According to the present invention, it is proposed to use a method that is able to avoid that a User Equipment uses a wrong address information 22 and hence a wrong network node (such as a Short Message Service Center 220). This is schematically illustrated in Figure 5.

[0031] According to the present invention, this is achieved by means of providing the Subscriber Identity Module 21, which is used with the User Equipment 20, such that the Subscriber Identity Module 21 comprises an address information 22 used for the specific service of the public land mobile network, wherein the Subscriber

Identity Module 21 comprises an application program 23, wherein the application program 23 comprises a reference address information 24, wherein the application program 23 is provided such that the following steps are executed:

- in a first step, it is verified whether the address information 22 corresponds to the reference address information 24,
- in a second step, and in case that the verification of the first step holds a negative result,
- either the specific service is blocked, at least temporarily, for the User Equipment 20,
- or the specific service is invoked using the reference address information 24.

[0032] Thereby, it is possible to provide a detection and/or correction mechanism of wrong address information 22 on the Subscriber Identity Modules 21 of users or subscribers of the home public land mobile network A. Thereby, it is advantageously possible to detect wrong settings in the address information 22. In case that a wrong setting of the address information 22 is detected, different options exist: In one alternative embodiment of the present invention, the specific service - e.g. the short message service - is blocked, i.e. no further service request of this kind (i.e. a user initiated short message) can be sent. In another alternative embodiment of the present invention, a correction is applied to the false address information 22 and a this wrong address information 22 is replaced by a reference address information 24 which part of the application program 23, i.e. the specific service is invoked using the reference address information 24.

[0033] In Figure 3, a method for providing a Subscriber Identity Module 21 with an application program 24 for performing the inventive method is schematically shown: a server (especially an OTA server (OTA meaning "Over The Air")) 50 checks with a database 51 whether a Subscriber Identity Module 21 of a specific User Equipment 20 is enabled to receive and store the program information of the application program 23. The information of the application program 23 is then transmitted to the User Equipment 20, especially using an short message service transmission method, involving an Short Message Service Center 52. The Short Message Service Center 52 sends binary short messages 53 comprising the application program 23 to the User Equipment 20. The application program 23 is then saved (and installed) to a memory of the Subscriber Identity Module 21.

[0034] According to the present invention, it is possible and preferred that once the application program 23 is saved and installed to the Subscriber Identity Module 21, certain parameters of the application program 23 such as values of the reference address information 24 or parameters defining the appropriate action to be taken in the second step of the inventive method (in case that it is verified in the first step that the verification of the first step holds a negative result) are modified. This is pref-

erably be realized by an OTA mechanism comparable to the transmission of the application program itself to the Subscriber Identity Module 21.

[0035] The application program 23 according to the present invention is preferably a so-called "SIM Application Toolkit application" or SAT application. The application program 23 or SAT application 23 can be provided to any new Subscriber Identity Modules to be distributed to new customers but also to all (or at least the vast majority) of Subscriber Identity Modules 21 already circulating. This is because the vast majority of circulating Subscriber Identity Modules 21 are OTA enabled such that the application program 23 can be simply stored on such Subscriber Identity Modules 21. This means that the method according to the present invention can be implemented in a very quick manner. During roll-out of the application program 23, it is possible to transfer (or not to transfer) the application program 23 to different Subscriber Identity Modules depending on an information in a database about the Subscriber Identity Modules.

[0036] Furthermore, especially for the case that some models of User Equipments are not compatible with running the application program 23, it is possible to control the use of the application program 23 by means of the following steps:

- in a first step, the application program 23 is stored in the Subscriber Identity Module 21 of a User Equipment 20,

- in a second step, the application program 23 sends an information to the public land mobile network about the value of the IMEI (International Mobile Equipment Identity),

- Based on this IMEI information, it is possible to look up in a database whether the Subscriber Identity Module (and the corresponding User Equipment 20) are compatible with running the application program 23. If this is the case the application program 23 is (remotely) switched on or off, dependant on the result of the database lookup.

[0037] Figure 4 schematically illustrates an implementation of the inventive method, where in a first step, a detection of the address information 22 is provided and compared with a reference address information 24.

The reference address information 24 is either a complete address information (e.g. in the form of a global title) being able to specify a network entity in the telecommunications network / public land mobile network.

In this case, it is possible according to the present invention to simply replace the use of the address information 22 by the use of the reference address information 24.

However, according to an alternative embodiment of the present invention, it is also possible that the reference address information 24 is not a complete address information (being able to specify a network entity in the telecommunications network). For example, the reference address information could simply comprise the country

code of the correct address information 22 to use. If in this case a comparison of the reference address information 24 with the address information 22 (or with the corresponding part of the address information 22) holds that the address information 22 is not correct, it is not possible to simply replace the use of the address information 22 by the use of the reference address information 24. In this case, it will be preferred to block the specific serve for the User Equipment at least temporarily.

Claims

1. Method for preventing fraud or misuse when using a specific service of a public land mobile network by a User Equipment (20), wherein the User Equipment (20) comprises a Subscriber Identity Module (21), wherein the Subscriber Identity Module (21) comprises an address information (22) used for the specific service of the public land mobile network, wherein the Subscriber Identity Module (21) comprises an application program (23), wherein the application program (23) comprises a reference address information (24), wherein the application program (23) is provided such that the following steps are executed:

-- in a first step, it is verified whether the address information (22) corresponds to the reference address information (24),
 -- in a second step, and in case that the verification of the first step holds a negative result,
 -- either the specific service is invoked using the reference address information (24), wherein a wrong address information is replaced by the reference address information (24) in case the reference address information (24) is either a complete address information being able to specify a network entity in a telecommunications network and/or the public land mobile network,
 -- or the specific service is blocked, at least temporarily, for the User Equipment (20), in case the reference address information (24) is an incomplete address information being unable to specify a network entity in a telecommunications network and/or the public land mobile network, wherein the reference address information comprises a country code of the address information (22) to use.

2. Method according to claim 1, wherein in case that, during the second step, the specific service is blocked for the User Equipment (20), an error message is sent to the public land mobile network.
3. Method according to any one of the preceding claims, wherein the address information (22) is provided at a specific memory location within the Subscriber Identity Module (21), wherein the application

program (23) is configured such that, during the first step, the specific memory location within the Subscriber Identity Module (21) is verified repeatedly, at least once in a predetermined time interval.

4. Method according to any one of the preceding claims, wherein a request of the User Equipment (20) to use the specific service comprises the address information (22), wherein the User Equipment (20) is configured such that each request of the User Equipment (20) to use the specific service is directed to the Subscriber Identity Module (21), wherein the application program (23) is configured such that, during the first step, the address information (22) of the redirected request of the User Equipment (20) to use the specific service is verified.
5. Method according to any one of the preceding claims, wherein the specific service is the short message service.
6. Method according to any one of the preceding claims, wherein the address information (22) and the reference address information (24) relates to the address of a Short Message Service Center (220, 240) used by the User Equipment (20).
7. Subscriber Identity Module (21) for preventing fraud or misuse when a User Equipment (20) equipped with the Subscriber Identity Module (21) uses a specific service of a public land mobile network, wherein the Subscriber Identity Module (21) comprises an address information (22) used for the specific service of the public land mobile network, wherein the Subscriber Identity Module (21) comprises an application program (23), wherein the application program (23) comprises a reference address information (24), wherein the application program (23) is provided such that:
 - a verification is executed whether the address information (22) corresponds to the reference address information (24), and
 - in case that the verification holds a negative result,
 - either the specific service is invoked using the reference address information (24), wherein a wrong address information is replaced by the reference address information (24) in case the reference address information (24) is either a complete address information being able to specify a network entity in a telecommunications network and/or the public land mobile network,
 - or the specific service is blocked, at least temporarily, for the User Equipment (20), in case the reference address information (24) is an incomplete address information being unable to specify a network entity in a telecommunications

network and/or the public land mobile network, wherein the reference address information comprises a country code of the address information (22) to use

8. Subscriber Identity Module (21) according to claim 7, wherein in case that the specific service is blocked for the User Equipment (20), an error message is sent to the public land mobile network.
9. Subscriber Identity Module (21) according to claim 7 or 8, wherein the address information (22) is provided at a specific memory location within the Subscriber Identity Module (21), wherein the application program (23) is configured such that the specific memory location within the Subscriber Identity Module (21) is verified repeatedly, at least once in a predetermined time interval.
10. Subscriber Identity Module (21) according to one claims 7 to 9, wherein a request of the User Equipment (20) to use the specific service comprises the address information (22), wherein the User Equipment (20) is configured such that each request of the User Equipment (20) to use the specific service is directed to the Subscriber Identity Module (21), wherein the application program (23) is configured such that the address information (22) of the redirected request of the User Equipment (20) to use the specific service is verified.
11. Subscriber Identity Module (21) according to one of claims 7 to 10, wherein the specific service is the short message service.
12. Subscriber Identity Module (21) according to one of claims 7 to 11, wherein the address information (22) and the reference address information (24) relates to the address of a Short Message Service Center (220, 240) used by the User Equipment (20).
13. Application program (23) comprising a computer readable program code which, when executed on a computer or on a Subscriber Identity Module (21), causes the computer or the Subscriber Identity Module (21) to perform a method according one of claims 1 to 6.
14. Computer program product for preventing fraud or misuse when using a specific service of a public land mobile network by a User Equipment (20), the computer program product comprising a computer program stored on a storage medium, the computer program comprising program code which, when executed on a computer or on a Subscriber Identity Module (21), causes the computer or the Subscriber Identity Module (21) to perform a method according one of claims 1 to 6.

Patentansprüche

1. Verfahren zum Verhindern von Betrug oder Missbrauch bei Nutzung eines bestimmten Dienstes eines öffentlichen landgestützten Mobilfunknetzes durch eine Nutzereinrichtung (20), wobei die Nutzereinrichtung (20) ein Teilnehmeridentitätsmodul (Subscriber Identity Modul) (21) umfasst, wobei das Teilnehmeridentitätsmodul (21) eine Adressinformation (22) umfasst, die für den bestimmten Dienst des öffentlichen landgestützten Mobilfunknetzes verwendet wird, wobei das Teilnehmeridentitätsmodul (21) ein Anwendungsprogramm (23) umfasst, wobei das Anwendungsprogramm (23) eine Referenzadressinformation (24) umfasst, wobei das Anwendungsprogramm (23) so ausgebildet ist, dass die folgenden Schritte ausgeführt werden:
 - in einem ersten Schritt wird verifiziert, ob die Adressinformation (22) der Referenzadressinformation (24) entspricht,
 - in einem zweiten Schritt, und für den Fall, dass die Verifizierung des ersten Schrittes ein negatives Resultat ergibt,
 - wird entweder der bestimmte Dienst unter Verwendung der Referenzadressinformation (24) aufgerufen, wobei eine falsche Adressinformation durch die Referenzadressinformation (24) ersetzt wird, falls die Referenzadressinformation (24) entweder eine vollständige Adressinformation ist, die in der Lage ist, eine Netzwerkentität in einem Telekommunikationsnetz und/oder dem öffentlichen landgestützten Mobilfunknetz zu spezifizieren,
 - oder der bestimmte Dienst wird, wenigstens vorübergehend, für die Nutzereinrichtung (20) gesperrt, falls die Referenzadressinformation (24) eine unvollständige Adressinformation ist, die nicht in der Lage ist, eine Netzwerkentität in einem Telekommunikationsnetz und/oder dem öffentlichen landgestützten Mobilfunknetz zu spezifizieren, wobei die Referenzadressinformation einen Ländercode der zu verwendenden Adressinformation (22) umfasst.
2. Verfahren nach Anspruch 1, wobei für den Fall, dass während des zweiten Schrittes der bestimmte Dienst für die Nutzereinrichtung (20) gesperrt wird, eine Fehlermeldung an das öffentliche landgestützte Mobilfunknetz gesendet wird.
3. Verfahren nach einem der vorangehenden Ansprüche, wobei die Adressinformation (22) an einem bestimmten Speicherort innerhalb des Teilnehmeridentitätsmoduls (21) bereitgestellt wird, wobei das Anwendungsprogramm (23) so ausgebildet ist, dass während des ersten Schrittes der bestimmte Speicherort innerhalb des Teilnehmeridentitätsmoduls

- (21) wiederholt, mindestens einmal in einem vorgegebenen Zeitintervall, verifiziert wird.
4. Verfahren nach einem der vorangehenden Ansprüche, wobei eine Anforderung der Nutzereinrichtung (20), den bestimmten Dienst zu nutzen, die Adressinformation (22) umfasst, wobei die Nutzereinrichtung (20) so ausgebildet ist, dass jede Anforderung der Nutzereinrichtung (20), den bestimmten Dienst zu nutzen, an das Teilnehmeridentitätsmodul (21) geleitet wird, wobei das Anwendungsprogramm (23) so ausgebildet ist, dass während des ersten Schrittes die Adressinformation (22) der umgeleiteten Anforderung der Nutzereinrichtung (20), den bestimmten Dienst zu nutzen, verifiziert wird.
 5. Verfahren nach einem der vorangehenden Ansprüche, wobei der bestimmte Dienst der Kurzmitteilungsdienst ist.
 6. Verfahren nach einem der vorangehenden Ansprüche, wobei die Adressinformation (22) und die Referenzadressinformation (24) sich auf die Adresse einer durch die Nutzereinrichtung (20) verwendeten Kurzmitteilungsdienstzentrale (220, 240) beziehen.
 7. Teilnehmeridentitätsmodul (21) zum Verhindern von Betrug oder Missbrauch, wenn eine mit dem Teilnehmeridentitätsmodul (21) ausgestattete Nutzereinrichtung (20) einen bestimmten Dienst eines öffentlichen landgestützten Mobilfunknetzes nutzt, wobei das Teilnehmeridentitätsmodul (21) eine Adressinformation (22) umfasst, die für den bestimmten Dienst des öffentlichen landgestützten Mobilfunknetzes verwendet wird, wobei das Teilnehmeridentitätsmodul (21) ein Anwendungsprogramm (23) umfasst, wobei das Anwendungsprogramm (23) eine Referenzadressinformation (24) umfasst, wobei das Anwendungsprogramm (23) so ausgebildet ist, dass:
 - eine Verifizierung ausgeführt wird, ob die Adressinformation (22) der Referenzadressinformation (24) entspricht, und
 - für den Fall, dass die Verifizierung ein negatives Resultat ergibt,
 - entweder der bestimmte Dienst unter Verwendung der Referenzadressinformation (24) aufgerufen wird, wobei eine falsche Adressinformation durch die Referenzadressinformation (24) ersetzt wird, falls die Referenzadressinformation (24) entweder eine vollständige Adressinformation ist, die in der Lage ist, eine Netzwerkentität in einem Telekommunikationsnetz und/oder dem öffentlichen landgestützten Mobilfunknetz zu spezifizieren,
 - oder der bestimmte Dienst, wenigstens vorübergehend, für die Nutzereinrichtung (20) gesperrt wird, falls die Referenzadressinformation (24) eine unvollständige Adressinformation ist, die nicht in der Lage ist, eine Netzwerkentität in einem Telekommunikationsnetz und/oder dem öffentlichen landgestützten Mobilfunknetz zu spezifizieren, wobei die Referenzadressinformation einen Ländercode der zu verwendenden Adressinformation (22) umfasst.
 8. Teilnehmeridentitätsmodul (21) nach Anspruch 7, wobei für den Fall, dass der bestimmte Dienst für die Nutzereinrichtung (20) gesperrt wird, eine Fehlermeldung an das öffentliche landgestützte Mobilfunknetz gesendet wird.
 9. Teilnehmeridentitätsmodul (21) nach Anspruch 7 oder 8, wobei die Adressinformation (22) an einem bestimmten Speicherort innerhalb des Teilnehmeridentitätsmoduls (21) bereitgestellt wird, wobei das Anwendungsprogramm (23) so ausgebildet ist, dass der bestimmte Speicherort innerhalb des Teilnehmeridentitätsmoduls (21) wiederholt, mindestens einmal in einem vorgegebenen Zeitintervall, verifiziert wird.
 10. Teilnehmeridentitätsmodul (21) nach einem der Ansprüche 7 bis 9, wobei eine Anforderung der Nutzereinrichtung (20), den bestimmten Dienst zu nutzen, die Adressinformation (22) umfasst, wobei die Nutzereinrichtung (20) so ausgebildet ist, dass jede Anforderung der Nutzereinrichtung (20), den bestimmten Dienst zu nutzen, an das Teilnehmeridentitätsmodul (21) geleitet wird, wobei das Anwendungsprogramm (23) so ausgebildet ist, dass die Adressinformation (22) der umgeleiteten Anforderung der Nutzereinrichtung (20), den bestimmten Dienst zu nutzen, verifiziert wird.
 11. Teilnehmeridentitätsmodul (21) nach einem der Ansprüche 7 bis 10, wobei der bestimmte Dienst der Kurzmitteilungsdienst ist.
 12. Teilnehmeridentitätsmodul (21) nach einem der Ansprüche 7 bis 11, wobei die Adressinformation (22) und die Referenzadressinformation (24) sich auf die Adresse einer durch die Nutzereinrichtung (20) verwendeten Kurzmitteilungsdienstzentrale (220, 240) beziehen.
 13. Anwendungsprogramm (23), das einen Computerlesbaren Programmcode umfasst, der, wenn er auf einem Computer oder in einem Teilnehmeridentitätsmodul (21) ausgeführt wird, bewirkt, dass der Computer oder das Teilnehmeridentitätsmodul (21) ein Verfahren nach einem der Ansprüche 1 bis 6 ausführt.
 14. Computerprogrammprodukt zum Verhindern von

Betrug oder Missbrauch bei Nutzung eines bestimmten Dienstes eines öffentlichen landgestützten Mobilfunknetzes durch eine Nutzereinrichtung (20), wobei das Computerprogrammprodukt ein Computerprogramm umfasst, das auf einem Speichermedium gespeichert wird, wobei das Computerprogramm Programmcode umfasst, der, wenn er auf einem Computer oder in einem Teilnehmeridentitätsmodul (21) ausgeführt wird, bewirkt, dass der Computer oder das Teilnehmeridentitätsmodul (21) ein Verfahren nach einem der Ansprüche 1 bis 6 ausführt.

Revendications

1. Procédé de prévention de fraude ou d'utilisation abusive lors de l'utilisation d'un service spécifique de réseau mobile terrestre public par un équipement d'utilisateur (20), dans lequel l'équipement d'utilisateur (20) comprend un module d'identification d'abonné (21), dans lequel le module d'identification d'abonné (21) comprend une information d'adresse (22) utilisée pour le service spécifique du réseau mobile terrestre public, dans lequel le module d'identification d'abonné (21) comprend un programme d'application (23), dans lequel le programme d'application (23) comprend une information d'adresse de référence (24), dans lequel le programme d'application (23) est conçu de manière à exécuter les étapes suivantes :

- à une première étape, il est vérifié si l'information d'adresse (22) correspond à l'information d'adresse de référence (24),
- à une seconde étape, et dans le cas où la vérification de la première étape donne un résultat négatif,
- soit le service spécifique est appelé à l'aide de l'information d'adresse de référence (24), une information d'adresse erronée étant remplacée par l'information d'adresse de référence (24), dans le cas où l'information d'adresse de référence (24) est une information d'adresse complète pouvant spécifier une entité de réseau dans un réseau de télécommunication et/ou le réseau mobile terrestre public,
- soit le service spécifique est bloqué, au moins temporairement, pour l'équipement d'utilisateur (20), dans le cas où l'information d'adresse de référence (24) est une information d'adresse incomplète ne pouvant pas spécifier une entité de réseau dans un réseau de télécommunication et/ou le réseau mobile terrestre public, l'information d'adresse de référence comprenant un code de pays de l'information d'adresse (22) à utiliser.

2. Procédé selon la revendication 1, dans lequel, dans

le cas où, au cours de la seconde étape, le service spécifique est bloqué pour l'équipement d'utilisateur (20), un message d'erreur est envoyé au réseau mobile terrestre public.

3. Procédé selon l'une quelconque des revendications précédentes, dans lequel l'information d'adresse (22) est fournie à un emplacement spécifique de mémoire à l'intérieur du module d'identification d'abonné (21), dans lequel programme d'application (23) est conçu de telle sorte qu'au cours de la première étape, l'emplacement spécifique de mémoire à l'intérieur du module d'identification d'abonné (21) est vérifié à plusieurs reprises, au moins une fois dans un intervalle de temps prédéterminé.
4. Procédé selon l'une quelconque des revendications précédentes, dans lequel une demande d'utilisation du service spécifique issue de l'équipement d'utilisateur (20) comprend l'information d'adresse (22), dans lequel l'équipement d'utilisateur (20) est conçu de manière que chaque demande d'utilisation du service spécifique issue de l'équipement d'utilisateur (20) soit transmise au module d'identification d'abonné (21), dans lequel le programme d'application (23) est conçu de telle sorte qu'au cours de la première étape, l'information d'adresse (22) de la demande retransmise d'utilisation du service spécifique issue de l'équipement d'utilisateur (20) est vérifiée.
5. Procédé selon l'une quelconque des revendications précédentes, dans lequel le service spécifique est le service de minimessages.
6. Procédé selon l'une quelconque des revendications précédentes, dans lequel l'information d'adresse (22) et l'information d'adresse de référence (24) se rapportent à l'adresse d'un centre de service de minimessages (220, 240) utilisé par l'équipement d'utilisateur (20).
7. Module d'identification d'abonné (21) destiné à prévenir la fraude ou l'utilisation abusive, lorsqu'un équipement d'utilisateur (20) équipé du module d'identification d'abonné (21) utilise un service spécifique de réseau mobile terrestre public, dans lequel le module d'identification d'abonné (21) comprend une information d'adresse (22) utilisée pour le service spécifique du réseau mobile terrestre public, dans lequel le module d'identification d'abonné (21) comprend un programme d'application (23), dans lequel le programme d'application (23) comprend une information d'adresse de référence (24), dans lequel le programme d'application (23) est conçu de telle sorte que :

- il est vérifié si l'information d'adresse (22) cor-

- répond à l'information d'adresse de référence (24), et
 - dans le cas où la vérification donne un résultat négatif,
 - soit le service spécifique est appelé à l'aide de l'information d'adresse de référence (24), une information d'adresse erronée étant remplacée par l'information d'adresse de référence (24), dans le cas où l'information d'adresse de référence (24) est une information d'adresse complète pouvant spécifier une entité de réseau dans un réseau de télécommunication et/ou le réseau mobile terrestre public,
 - soit le service spécifique est bloqué, au moins temporairement, pour l'équipement d'utilisateur (20), dans le cas où l'information d'adresse de référence (24) est une information d'adresse incomplète ne pouvant pas spécifier une entité de réseau dans un réseau de télécommunication et/ou le réseau mobile terrestre public, l'information d'adresse de référence comprenant un code de pays de l'information d'adresse (22) à utiliser.
- 8.** Module d'identification d'abonné 21 selon la revendication 7, dans lequel, dans le cas où le service spécifique est bloqué pour l'équipement d'utilisateur (20), un message d'erreur est envoyé au réseau mobile terrestre public.
- 9.** Module d'identification d'abonné (21) selon la revendication 7 ou 8, dans lequel l'information d'adresse (22) est fournie à un emplacement spécifique de mémoire à l'intérieur du module d'identification d'abonné (21), dans lequel programme d'application (23) est conçu de telle sorte que l'emplacement spécifique de mémoire à l'intérieur du module d'identification d'abonné (21) est vérifié à plusieurs reprises, au moins une fois dans un intervalle de temps prédéterminé.
- 10.** Module d'identification d'abonné (21) selon l'une des revendications 7 à 9, dans lequel une demande d'utilisation du service spécifique issue de l'équipement d'utilisateur (20) comprend l'information d'adresse (22), dans lequel l'équipement d'utilisateur (20) est conçu de manière que chaque demande d'utilisation du service spécifique issue de l'équipement d'utilisateur (20) soit transmise au module d'identification d'abonné (21), dans lequel le programme d'application (23) est conçu de telle sorte que l'information d'adresse (22) de la demande retransmise d'utilisation du service spécifique issue de l'équipement d'utilisateur (20) est vérifiée.
- 11.** Module d'identification d'abonné (21) selon l'une quelconque des revendications 7 à 10, dans lequel le service spécifique est le service de minimessages.
- 12.** Module d'identification d'abonné (21) selon l'une des revendications 7 à 11, dans lequel l'information d'adresse (22) et l'information d'adresse de référence (24) se rapportent à l'adresse d'un centre de service de minimessages (220, 240) utilisé par l'équipement d'utilisateur (20).
- 13.** Programme d'application (23) comprenant un code de programme lisible par ordinateur qui, lorsqu'il est exécuté sur un ordinateur ou sur un module d'identification d'abonné (21) fait que l'ordinateur ou le module d'identification d'abonné (21) mette en oeuvre un procédé selon l'une des revendications 1 à 6.
- 14.** Produit-programme informatique destiné à prévenir la fraude ou l'utilisation abusive lors de l'utilisation d'un service spécifique de réseau mobile terrestre public par un équipement d'utilisateur (20), le produit-programme informatique comprenant un programme informatique stocké sur un support de stockage, le programme informatique comprenant un code de programme qui, lorsqu'il est exécuté sur un ordinateur ou sur un module d'identification d'abonné (21), fait que l'ordinateur ou le module d'identification d'abonné (21) mette en oeuvre un procédé selon l'une des revendications 1 à 6.

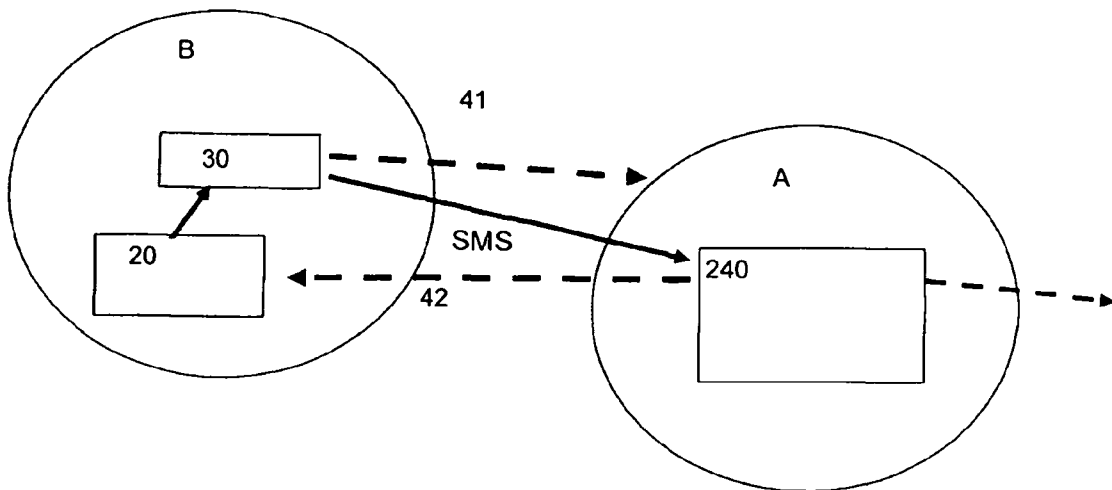


Fig. 1

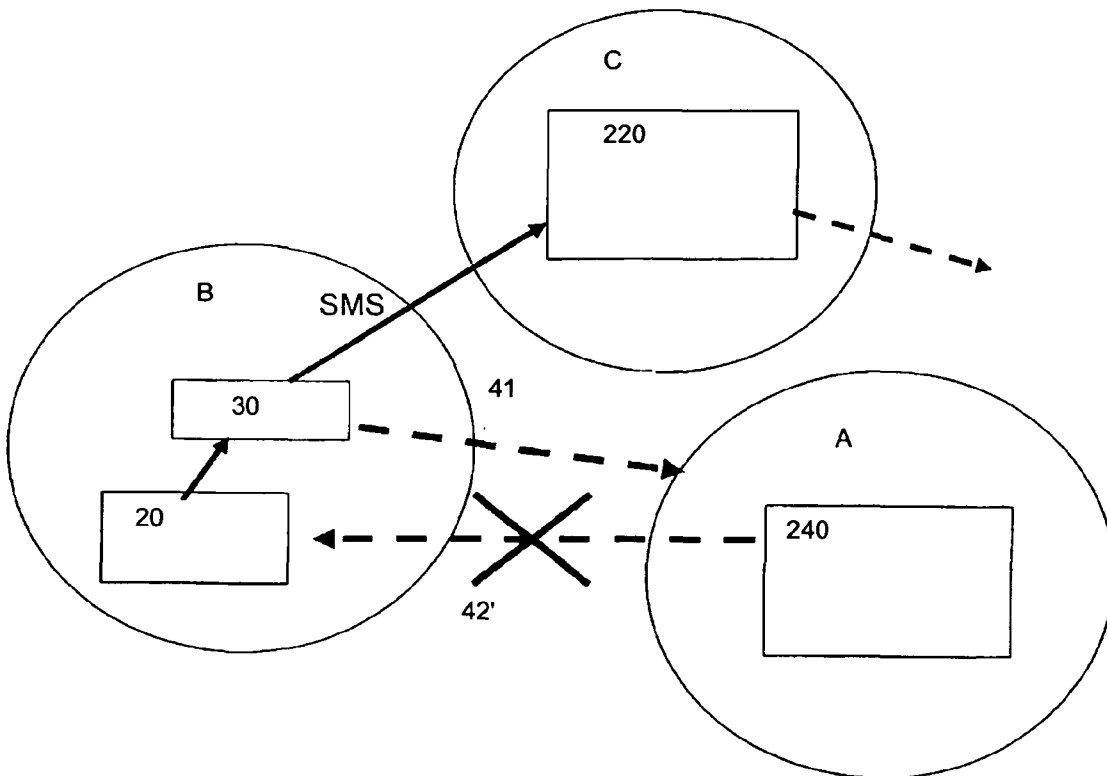


Fig. 2

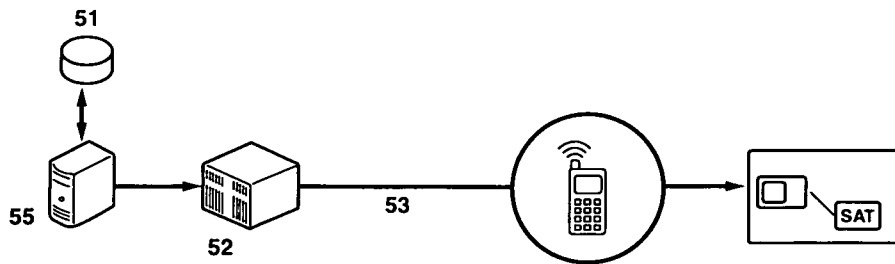


Fig. 3

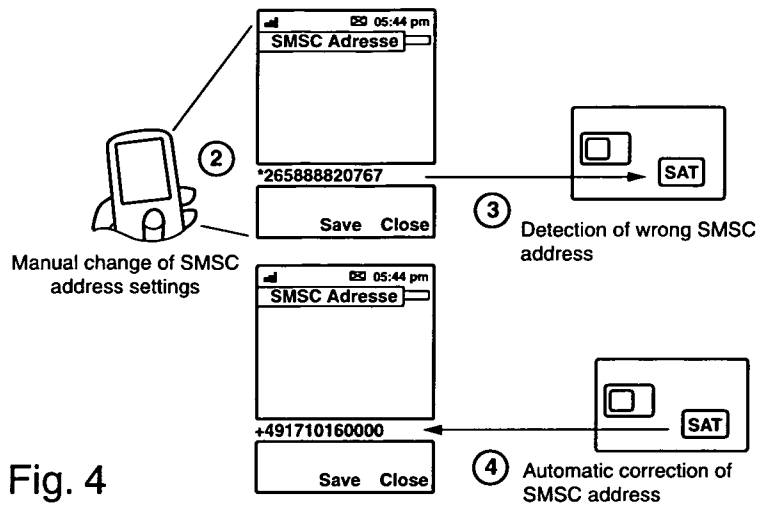


Fig. 4

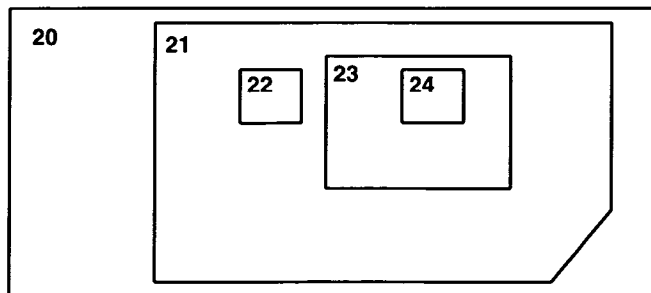


Fig. 5

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 03005738 A2 [0004]

EP 2 756 703

ELJÁRÁS CSALÁS ÉS VISSZAÉLÉS MEGAKADÁLYOZÁSÁRA NYILVÁNOS
FÖLDI MOBILHÁLÓZAT MEGHATÁROZOTT SZOLGÁLTATÁSÁNAK
HASZNÁLATAKOR FELHASZNÁLÓI KÉSZÜLÉKKEL, ELŐFIZETŐI AZONOSÍTÓ
MODUL ÉS ALKALMAZÁSI PROGRAM

Szabadalmi igénypontok



1. Eljárás csalás és visszaélés megakadályozására nyilvános földi mobilhálózat meghatározott szolgáltatásának használatakor felhasználói készülékekkel (20), a felhasználói készülék (20) előfizetői azonosító modult (Subscriber Identity Modul) (21) tartalmaz, az előfizetői azonosító modul (21) a nyilvános földi mobilhálózat meghatározott szolgáltatásához használt címinformációt (22) tartalmaz, továbbá az előfizetői azonosító modul (21) alkalmazási programot (23) tartalmaz, az alkalmazási program (23) referencia-címinformációt (24) tartalmaz, és az alkalmazási program (23) úgy van kialakítva, hogy a következő lépéseket hajtjuk végre:

- egy első lépésben ellenőrizzük, hogy a címinformáció (22) megfelel-e a referencia-címinformációnak (24),

- egy második lépésben, és abban az esetben, amikor az első lépés ellenőrzése negatív eredményt ad,

- vagy felhívjuk a meghatározott szolgáltatást a referencia-címinformáció (24) felhasználásával úgy, hogy egy hamis címinformációt a referencia-címinformációval (24) helyettesítünk, ha a referencia-címinformáció (24) teljes címinformáció, amely alkalmas egy hálózati entitás meghatározására egy telekommunikációs hálózatban és/vagy a nyilvános földi

mobilhálózatban,

- vagy legalább átmenetileg blokkoljuk a meghatározott szolgáltatást a felhasználói készülék (20) számára, ha a referencia-címinformáció (24) egy nem teljes címinformáció, amely nem alkalmas egy hálózati entitás meghatározására egy telekommunikációs hálózatban és/vagy a nyilvános földi mobilhálózatban, és a referencia-címinformáció tartalmazza az alkalmazandó címinformáció (22) országkódját.

2. Az 1. igénypont szerinti eljárás, amelynél abban az esetben, amikor a második lépés folyamán a meghatározott szolgáltatást blokkoljuk a felhasználói készülék (20) számára, hibaüzenetet küldünk a nyilvános földi mobilhálózatnak.

3. Az előző igénypontok egyike szerinti eljárás, amelynél a címinformációt (22) az előfizetői azonosító modulban (21) egy meghatározott tárolóhelyen bocsátjuk rendelkezésre, továbbá az alkalmazási program (23) úgy van kialakítva, hogy az első lépés folyamán a meghatározott tárolóhelyet az előfizetői azonosító modulban (21) ismételten, egy előre megadott időközben legalább egyszer ellenőrizzük.

4. Az előző igénypontok egyike szerinti eljárás, amelynél a felhasználói készüléknek (20) a meghatározott szolgáltatás használatára irányuló kérése tartalmazza a címinformációt (22), továbbá a felhasználói készülék (20) úgy van kialakítva, hogy a felhasználói készüléknek (20) a meghatározott szolgáltatás használatára vonatkozó minden kérését az előfizetői azonosító modulra (21) küldjük, továbbá az alkalmazási

program (23) úgy van kialakítva, hogy az első lépés folyamán a felhasználói készülék (20) meghatározott szolgáltatás használatára vonatkozó átirányított kérésének címinformációját (22) ellenőrizzük.

5. Az előző igénypontok egyike szerinti eljárás, amelynél a meghatározott szolgáltatás az sms-szolgáltatás (short message service).

6. Az előző igénypontok egyike szerinti eljárás, amelynél a címinformáció (22) és a referencia-címinformáció (24) a felhasználói készülék (20) által használt sms-szolgáltató központ (220, 240) címére vonatkozik.

7. Előfizetői azonosító modul (21) csalás és visszaélés megakadályozására, amikor az előfizetői azonosító modullal (21) felszerelt felhasználói készülék (20) nyilvános földi mobilhálózat meghatározott szolgáltatását használja, ahol az előfizetői azonosító modul (21) a nyilvános földi mobilhálózat meghatározott szolgáltatásához használt címinformációt (22) tartalmaz, továbbá az előfizetői azonosító modul (21) alkalmazási programot (23) tartalmaz, az alkalmazási program (23) referencia-címinformációt (24) tartalmaz, és az alkalmazási program (23) úgy van kialakítva, hogy:

- ellenőrzi, hogy a címinformáció (22) megfelel-e a referencia-címinformációnak (24),

- abban az esetben, amikor az ellenőrzés negatív eredményt ad,

- vagy felhívja a meghatározott szolgáltatást a referen-

cia-címinformáció (24) felhasználásával úgy, hogy egy hamis címinformációt a referencia-címinformációval (24) helyettesít, ha a referencia-címinformáció (24) teljes címinformáció, amely alkalmas egy hálózati entitás meghatározására egy telekommunikációs hálózatban és/vagy a nyilvános földi mobilhálózatban,

- vagy legalább átmenetileg blokkolja a meghatározott szolgáltatást a felhasználói készülék (20) számára, ha a referencia-címinformáció (24) egy nem teljes címinformáció, amely nem alkalmas egy hálózati entitás meghatározására egy telekommunikációs hálózatban és/vagy a nyilvános földi mobilhálózatban, és a referencia-címinformáció tartalmazza az alkalmazandó címinformáció (22) országkódját.

8. A 7. igénypont szerinti előfizetői azonosító modul (21), amely abban az esetben, amikor blokkolja a meghatározott szolgáltatást a felhasználói készülék (20) számára, hibaüzenetet küld a nyilvános földi mobilhálózatnak.

9. A 7. vagy 8. igénypont szerinti előfizetői azonosító modul (21), amelynél a címinformáció (22) az előfizetői azonosító modulban (21) egy meghatározott tárolóhelyen áll rendelkezésre, továbbá az alkalmazási program (23) úgy van kialakítva, hogy a meghatározott tárolóhelyet az előfizetői azonosító modulban (21) ismételten, egy előre megadott időközben legalább egyszer ellenőrzi.

10. A 7.-9. igénypontok egyike szerinti előfizetői azonosító modul (21), amelynél a felhasználói készüléknek (20) a megha-

tározott szolgáltatás használatára irányuló kérése tartalmazza a címinformációt (22), továbbá a felhasználói készülék (20) úgy van kialakítva, hogy a felhasználói készüléknek (20) a meghatározott szolgáltatás használatára vonatkozó minden kérését az előfizetői azonosító modulra (21) küldi, továbbá az alkalmazási program (23) úgy van kialakítva, hogy ellenőrzi a felhasználói készülék (20) meghatározott szolgáltatás használatára vonatkozó átirányított kérésének címinformációját (22).

11. A 7.-10. igénypontok egyike szerinti előfizetői azonosító modul (21), amelynél a meghatározott szolgáltatás az sms-szolgáltatás (short message service).

12. A 7.-11. igénypontok egyike szerinti előfizetői azonosító modul (21), amelynél a címinformáció (22) és a referencia-címinformáció (24) a felhasználói készülék (20) által használt sms-szolgáltató központ (220, 240) címére vonatkozik.

13. Alkalmazási program (23), amely számítógéppel olvasható programkódot tartalmaz, amely, amikor egy számítógépen vagy egy előfizetői azonosító modulban (21) végrehajtják, az 1.-6. igénypontok egyike szerinti eljárás végrehajtására készíti a számítógépet vagy az előfizetői azonosító modult (21).

14. Számítógépes programtermék csalás és visszaélés megakadályozására nyilvános földi mobilhálózat meghatározott szolgáltatásának használatakor felhasználói készülékkel (20), ahol a számítógépes programtermék tárolóközegen tárolt számítógépes

programot tartalmaz, továbbá a számítógépes program programkódot tartalmaz, amely, amikor egy számítógépen vagy egy előfizetői azonosító modulban (21) végrehajtják, az 1.-6. igénypontok egyike szerinti eljárás végrehajtására készíti a számítógépet vagy az előfizetői azonosító modult (21).

A meghatalmazott:

ADVOPATENT
SZABADALMI ÉS VÉDJEGY IRODA
1255 Budapest, Pf.: 80.

3.

