US 20160021532A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2016/0021532 A1**

(43) **Pub. Date: Jan. 21, 2016**

Schenk et al.

(54) **METHOD FOR PREVENTING FRAUD OR MISUSE BASED ON A RISK SCORING APPROACH WHEN USING A SERVICE OF A SERVICE PROVIDER, SYSTEM FOR PREVENTING FRAUD OR MISUSE, AND MOBILE COMMUNICATION NETWORK FOR PREVENTING FRAUD OR MISUSE**

(71) Applicant: **Deutsche Telekom AG**, Bonn (DE)

(72) Inventors: **Volker Schenk**, Euskirchen (DE); **Wolfgang Wirths**, Bonn (DE); **Guenter Haberkorn**, Birgland/Schwend (DE); **Uwe-Georg Wilhelm**, Bonn (DE)

(21) Appl. No.: **14/793,754**

(22) Filed: **Jul. 8, 2015**

(30) **Foreign Application Priority Data**

Jul. 17, 2014 (EP) 14177483.6

Publication Classification

(51) **Int. Cl.**

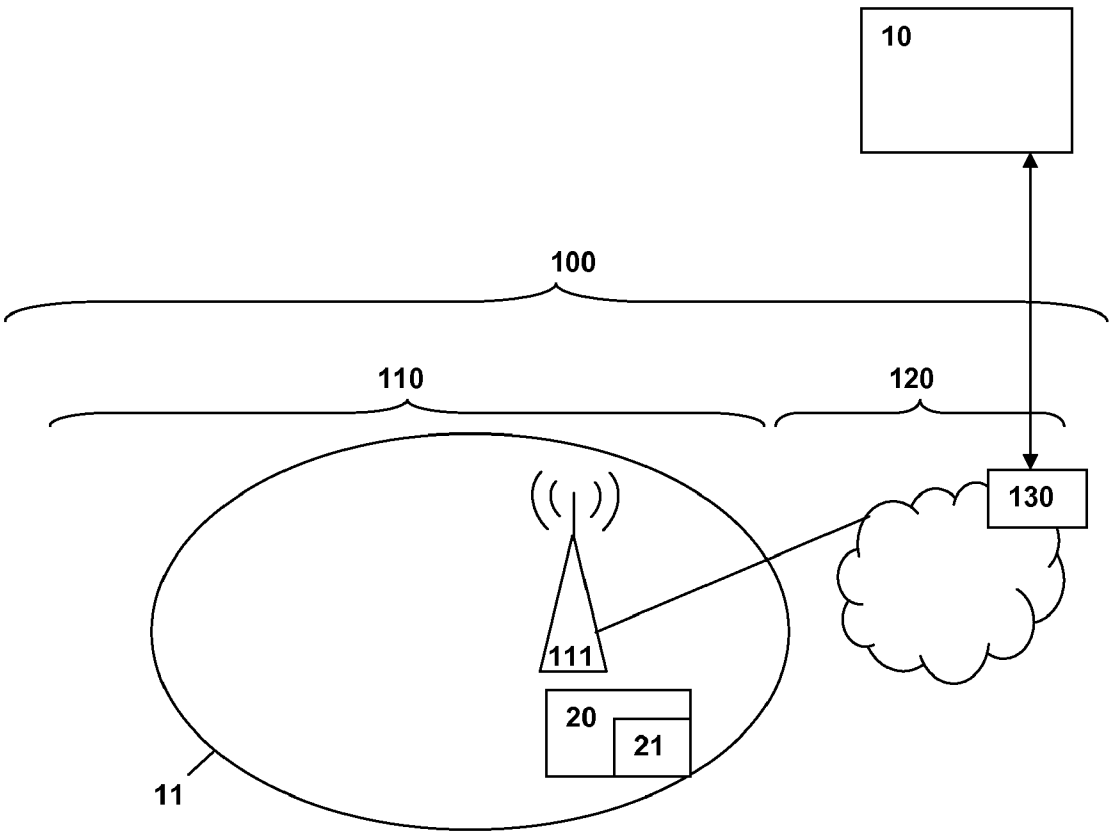
H04W 12/02 (2006.01)
H04W 12/06 (2006.01)
H04B 1/3816 (2006.01)

(52) **U.S. Cl.**

CPC ***H04W 12/02*** (2013.01); ***H04B 1/3816*** (2013.01); ***H04W 12/06*** (2013.01)

(57) **ABSTRACT**

A method for preventing fraud or misuse based on a risk scoring approach when using a service of a service provider requested by a user equipment includes: in connection with a first occurrence of providing the service, the service provider transmits a request message to a subscriber database, the request message being related to the MSISDN of the user equipment, and the request message requesting additional data related to the user equipment and/or the subscriber identity module; the service provider receives an answer message from the subscriber database, the answer message comprising the additional data; and in connection with a second occurrence of providing the service, an authentication information is transmitted between the service provider and the user equipment without transmitting a request message and a corresponding answer message.



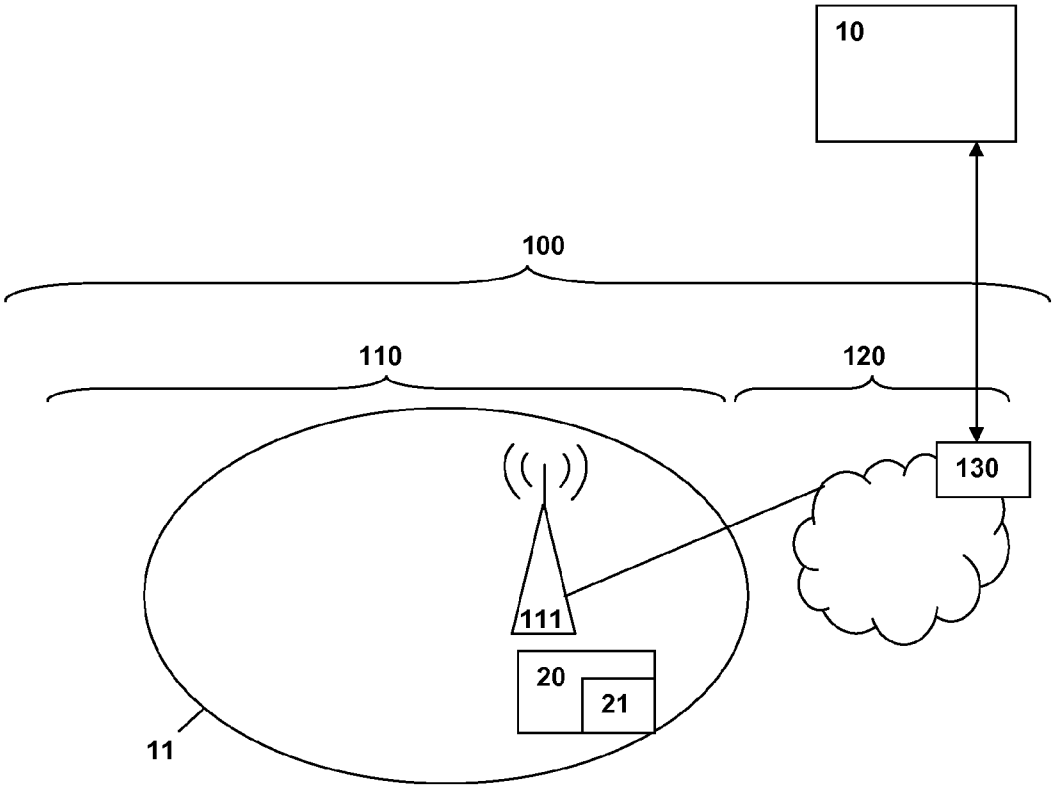


Fig. 1

METHOD FOR PREVENTING FRAUD OR MISUSE BASED ON A RISK SCORING APPROACH WHEN USING A SERVICE OF A SERVICE PROVIDER, SYSTEM FOR PREVENTING FRAUD OR MISUSE, AND MOBILE COMMUNICATION NETWORK FOR PREVENTING FRAUD OR MISUSE

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] Priority is claimed to European Patent Application No. EP14177483.6, filed on Jul. 17, 2014, the entire disclosure of which is hereby incorporated by reference herein.

FIELD

[0002] The present invention relates to a method for preventing fraud or misuse based on a risk scoring approach when using a service of a service provider.

[0003] The present invention further relates to a system for preventing fraud or misuse based on a risk scoring approach.

[0004] Additionally, the invention relates to a mobile communication network for preventing fraud or misuse based on a risk scoring approach.

[0005] Furthermore, the invention relates to a program comprising a computer readable program code and to a computer program product.

BACKGROUND

[0006] Operators of mobile communication networks, especially public land mobile networks, can help prevent fraud or misuse in cases where such fraud or misuse is carried out using a user equipment connected to the mobile communication network.

[0007] However, the mobile network operator needs to avoid—especially in order to conform to national data protection measures—that pieces of information related to customers are treated and communicated in an inappropriate manner.

SUMMARY

[0008] In an embodiment, the present invention provides a method for preventing fraud or misuse based on a risk scoring approach when using a service of a service provider requested by a user equipment, the user equipment being connected to a mobile communication network and the user equipment comprising a subscriber identity module. A subscriber database is assigned to the mobile communication network, the subscriber database comprising information related to the user equipment and/or related to the subscriber identity module. For different occurrences of providing the service of the service provider with respect to the user equipment, the user of the user equipment is authenticated by transmitting an authentication information between the service provider and the user equipment, wherein for the purpose of the transmission of authentication information between the service provider and the user equipment, the user equipment is identified using a Mobile Station Integrated Services Digital Network (MSISDN) number of the user equipment. The method includes: in connection with a first occurrence of providing the service, the service provider transmits, in a first step, a request message to the subscriber database of the mobile communication network, the request message being related to the MSISDN of the user equipment, and the request message requesting additional data related to the user equipment and/or related to the subscriber identity module; the service provider receives, in a second step, subsequent to the first step, an answer message from the subscriber database, the answer message comprising the additional data related to the user equipment and/or related to the subscriber identity module; and in connection with a second occurrence of providing the service, the second occurrence of providing the service being either prior or subsequent to the first occurrence of providing the service, an authentication information is transmitted between the service provider and the user equipment without transmitting a request message and a corresponding answer message.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The present invention will be described in even greater detail below based on the exemplary figures. The invention is not limited to the exemplary embodiments. All features described and/or illustrated herein can be used alone or combined in different combinations in embodiments of the invention. The features and advantages of various embodiments of the present invention will become apparent by reading the following detailed description with reference to the attached drawings which illustrate the following:

[0010] FIG. **1** schematically illustrates an exemplary situation according to the present invention where a mobile communication network—with a user equipment connected to the mobile communication network—is connected to a service provider, and the service provider is able to exchange pieces of information with a subscriber database of the mobile communication network.

DETAILED DESCRIPTION

[0011] In an embodiment, the present invention provides a cost effective solution for preventing fraud or misuse scenarios based on a risk scoring approach when using a service of a service provider, the service being requested by a user equipment connected to a mobile communication network.

[0012] In an embodiment, the present invention provides a method for preventing fraud or misuse based on a risk scoring approach when using a service of a service provider, wherein the service of the service provider is requested by a user equipment, the user equipment being connected to a mobile communication network and the user equipment comprising a subscriber identity module,

wherein a subscriber database is assigned to the mobile communication network, the subscriber database comprising information related to the user equipment and/or related to the subscriber identity module,

wherein for different occurrences of providing the service of the service provider with respect to the user equipment, the user of the user equipment is authenticated by means of transmitting an authentication information between the service provider and the user equipment, wherein for the purpose of the transmission of authentication information between the service provider and the user equipment, the user equipment is identified by means of the MSISDN (Mobile Station Integrated Services Digital Network number) of the user equipment,

wherein the method comprises the following steps:

[0013] in connection with a first occurrence of providing the service, the service provider transmits, in a first step, a request message to the subscriber database of the mobile

communication network, the request message being related to the MSISDN of the user equipment, and the request message requesting additional data related to the user equipment and/or related to the subscriber identity module,

[0014] the subscriber database transmits, in a second step, subsequent to the first step, an answer message to the service provider, the answer message comprising the additional data related to the user equipment and/or related to the subscriber identity module,

[0015] in connection with a second occurrence of providing the service, the second occurrence of providing the service being either prior or subsequent to the first occurrence of providing the service, an authentication information is transmitted between the service provider and the user equipment without transmitting a request message and a corresponding answer message.

[0016] According to the present invention, it is thereby advantageously possible that fraud or misuse can be effectively reduced by means of providing an answer message to the service provider, wherein the answer message comprises the additional data related to the user equipment and/or related to the subscriber identity module. From a point of view of the service provider, the mobile network operator of the mobile communication network can be considered a trusted entity that transmits—by means of the answer message comprising the additional data related to the user equipment and/or related to the subscriber identity module—auxiliary information that are related to the user equipment (i.e. to a subscriber of the service provider). The service provider (i.e. a third party or partner of the mobile communication network) is then able to use the additional data related to the user equipment and/or related to the subscriber identity module for providing value-added services. The service provider or third party may be a partner company of the mobile communication network or could also be another consumer (or subscriber) or a user group, e.g. a family member or a friend.

[0017] As an example, a bank (as a service provider) could use such additional information or data (related to the user equipment and/or related to the subscriber identity module) to enhance fraud detection mechanisms within the bank such that fraud schemes that have occurred (e.g. attacks against online banking systems by obtaining replacement subscriber identity modules (i.e. SIM cards or so-called multi-SIM cards, additional SIM cards for a post-paid contract) which enabled such fraudsters to eavesdrop on mobile transaction authentication numbers (TAN numbers)) can be either avoided or considerably reduced. Thus a request of the service provider for a transaction addressed to a SIM card that has been exchanged just recently can serve as an indicator of a higher fraud risk, and a requested transaction could be either refused or additional authentication required.

[0018] According to the present invention, any such data transmissions from the mobile network operator to service providers (or third parties) requires either an appropriate legal basis or some form of user consent of the user whose data is being transmitted. Therefore, according to the present invention, the additional data related to the user equipment and/or related to the subscriber identity module is preferably such that data reduction and data economy is applied.

[0019] According to a preferred embodiment of the present invention, the first occurrence of providing the service, including transmitting the request message and the answer message, is performed in case that—upon requesting the service by the user equipment—a risk scoring threshold of the service provider is exceeded.

[0020] It is thereby advantageously possible to limit requesting the additional data related to the user equipment and/or related to the subscriber identity module only to such cases where the risk scoring threshold of the service provider is exceeded. This allows to avoid the exchange of the request message and the answer message between the service provider and the subscriber database (i.e. the mobile network operator) in most of the normal cases and provides the possibility to nevertheless realize an enhanced level of fraud protection.

[0021] According to another preferred embodiment of the present invention, the information related to the user equipment and/or related to the subscriber identity module corresponds to at least one out of the following:

[0022] a time information related to a swap of the subscriber identity module,

[0023] a time information related to a change of the subscriber identity module,

[0024] a time information related to a generation of an analogous subscriber identity module (Multi-SIM card), related to the same MSISDN of the user equipment,

[0025] a time information related to a change of the user equipment,

[0026] a time information related to a change of the type of the user equipment,

[0027] a time information related to a change of the class of the user equipment,

[0028] a time information related to a change of the IMEI (International Mobile Equipment Identity).

[0029] According to the present invention, it is thereby advantageously possible for the service provider to be informed, on request, whether a swap of the subscriber identity module occurred recently, and/or whether a change of the subscriber identity module occurred recently, and/or whether the generation of an analogous subscriber identity module (Multi-SIM card) occurred recently, and/or whether a change of the user equipment (i.e. the hardware used in connection with the subscriber identity module) occurred recently, and/or whether a change of the type of the user equipment occurred recently, and/or whether a change of the class of the user equipment occurred recently, and/or whether a change of the IMEI occurred recently.

[0030] According to still another preferred embodiment of the present invention, a time information corresponds to the indication whether the respective event did occur or did not occur within one of a plurality of preceding time intervals, the time intervals being preferably predefined and referring to the time of either the request message or the answer message.

[0031] Thereby, it is advantageously possible according to the present invention that data reduction and data protection is applied as no piece of information regarding the subscriber identity module or regarding the type or class of the user equipment is transmitted but only the time information.

[0032] According to a further preferred embodiment of the present invention, the information related to the user equipment and/or related to the subscriber identity module corresponds to at least one out of the following:

[0033] an amount information related to the number of analogous subscriber identity modules (Multi-SIM cards) used, related to the same MSISDN of the user equipment,

[0034] an information relating to the type of the subscriber identity module,

[0035] an information relating to the subscription (or tariff) of the user equipment with the mobile communication network,

[0036] an information relating to a radio access technology used by the user equipment within the mobile communication network,

[0037] an information related to which type of an encryption algorithm is used by the user equipment within the mobile communication network,

[0038] an information related to a visited mobile communication network (VPLMN) of the user equipment,

[0039] an information related to unique identifiers of mobile data connections or their respective endpoints,

[0040] an information related to location information such as the distance of analogous subscriber identity modules, related to the same MSISDN of the user equipment.

[0041] Thereby, it is advantageously possible according to the present invention that the service provider is informed, on request, about an amount information related to the number of analogous subscriber identity modules (Multi-SIM cards) used, and/or about the type of the subscriber identity module, and/or about the subscription (or tariff) of the user equipment with the mobile communication network, and/or about a radio access technology used by the user equipment within the mobile communication network, and/or about which type of encryption algorithm is used by the user equipment within the mobile communication network, and/or about a visited mobile communication network (VPLMN) of the user equipment, and/or about unique identifiers of mobile data connections or their respective endpoints.

[0042] According to another preferred embodiment of the present invention, the user equipment is identified by means of:

[0043] the MSISDN (Mobile Station Integrated Services Digital Network number) of the user equipment connected with the mobile communication network or

[0044] an IP-address (Internet Protocol-address) according to IPv6 or

[0045] an IP-address and an information regarding a point in time of an IP-connection of the user equipment with the mobile communication network.

[0046] Thereby, it is advantageously possible still enhance the level of data protection as the MSISDN of the user equipment and/or the IP-address according to IPv6 and/or the IP-address (especially an IPv4 IP-address) and the information regarding a point in time of the IP-connection of the user equipment with the mobile communication network is known to the service provider.

[0047] Furthermore, the present invention relates to a system for preventing fraud or misuse based on a risk scoring approach when using a service of a service provider, the system comprising the service provider and a mobile communication network, wherein the service of the service provider is requested by a user equipment, the user equipment being connected to the mobile communication network and the user equipment comprising a subscriber identity module, wherein a subscriber database is assigned to the mobile communication network, the subscriber database comprising information related to the user equipment and/or related to the subscriber identity module,

wherein for different occurrences of providing the service of the service provider with respect to the user equipment, the user of the user equipment is authenticated by means of transmitting an authentication information between the service provider and the user equipment, wherein for the purpose of the transmission of authentication information between the service provider and the user equipment, the user equipment is identified by means of the MSISDN (Mobile Station Integrated Services Digital Network number) of the user equipment,

wherein the system is configured such that:

[0048] in connection with a first occurrence of providing the service, a request message is transmitted by the service provider to the subscriber database of the mobile communication network, the request message being related to the MSISDN of the user equipment, and the request message requesting additional data related to the user equipment and/or related to the subscriber identity module,

[0049] an answer message is transmitted by the subscriber database to the service provider, the answer message comprising the additional data related to the user equipment and/or related to the subscriber identity module,

[0050] in connection with a second occurrence of providing the service, an authentication information is transmitted between the service provider and the user equipment without transmitting a request message and a corresponding answer message.

[0051] By means of such a system, it is advantageously possible that fraud or misuse can be effectively reduced by means of providing an answer message to the service provider.

[0052] Especially with respect to the inventive system, it is preferred that the system is configured such that the first occurrence of providing the service, including transmitting the request message and the answer message, is performed in case that—upon requesting the service by the user equipment—a risk scoring threshold of the service provider is exceeded.

[0053] Especially with respect to the inventive system, it is preferred that the information related to the user equipment and/or related to the subscriber identity module corresponds to at least one out of the following:

[0054] a time information related to a swap of the subscriber identity module,

[0055] a time information related to a change of the subscriber identity module,

[0056] a time information related to a generation of an analogous subscriber identity module (Multi-SIM card), related to the same MSISDN of the user equipment,

[0057] a time information related to a change of the user equipment,

[0058] a time information related to a change of the type of the user equipment,

[0059] a time information related to a change of the class of the user equipment,

[0060] a time information related to a change of the IMEI (International Mobile Equipment Identity).

[0061] Especially with respect to the inventive system, it is preferred that a time information corresponds to the indication whether the respective event did occur or did not occur within one of a plurality of preceding time intervals, the time intervals being preferably predefined and referring to the time of either the request message or the answer message.

[0062] Additionally, the present invention relates to a mobile communication network for preventing fraud or misuse based on a risk scoring approach when using a service of

a service provider, wherein the service of the service provider is requested by a user equipment connected to the mobile communication network and the user equipment comprising a subscriber identity module,

wherein a subscriber database is assigned to the mobile communication network, the subscriber database comprising information related to the user equipment and/or related to the subscriber identity module,

wherein for different occurrences of providing the service of the service provider with respect to the user equipment, the user of the user equipment is authenticated by means of transmitting an authentication information between the service provider and the user equipment, wherein for the purpose of the transmission of authentication information between the service provider and the user equipment, the user equipment is identified by means of the MSISDN (Mobile Station Integrated Services Digital Network number) of the user equipment,

wherein the mobile communication network is configured such that:

[0063] in connection with a first occurrence of providing the service, a request message is transmitted by the service provider to the subscriber database of the mobile communication network, the request message being related to the MSISDN of the user equipment, and the request message requesting additional data related to the user equipment and/or related to the subscriber identity module,

[0064] an answer message is transmitted by the subscriber database to the service provider, the answer message comprising the additional data related to the user equipment and/or related to the subscriber identity module,

[0065] in connection with a second occurrence of providing the service, an authentication information is transmitted between the service provider and the user equipment without transmitting a request message and a corresponding answer message.

[0066] By means of such a mobile communication network, it is advantageously possible that fraud or misuse can be effectively reduced by means of providing an answer message to the service provider.

[0067] Especially with respect to the inventive mobile communication network, it is preferred that the mobile communication network is configured such that the first occurrence of providing the service, including transmitting the request message and the answer message, is performed in case that—upon requesting the service by the user equipment—a risk scoring threshold of the service provider is exceeded.

[0068] Especially with respect to the inventive mobile communication network, it is preferred that the information related to the user equipment and/or related to the subscriber identity module corresponds to at least one out of the following:

[0069] a time information related to a swap of the subscriber identity module,

[0070] a time information related to a change of the subscriber identity module,

[0071] a time information related to a generation of an analogous subscriber identity module (Multi-SIM card), related to the same MSISDN of the user equipment,

[0072] a time information related to a change of the user equipment,

[0073] a time information related to a change of the type of the user equipment,

[0074] a time information related to a change of the class of the user equipment,

[0075] a time information related to a change of the IMEI (International Mobile Equipment Identity).

[0076] Especially with respect to the inventive mobile communication network, it is preferred that a time information corresponds to the indication whether the respective event did occur or did not occur within one of a plurality of preceding time intervals, the time intervals being preferably predefined and referring to the time of either the request message or the answer message.

[0077] Furthermore, the present invention relates to a program comprising a computer readable program code which, when executed on a computer or on a network node of a mobile communication network or on a network node of a service provider, or in part on a network node of the mobile communication network and in part on a network node of a service provider, causes the computer or the network node of the mobile communication network and/or the network node of the service provider to perform an inventive method.

[0078] Still additionally, the present invention relates to computer program product for using a mobile communication network or a system comprising a service provider and a mobile communication network, 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 network node of a mobile communication network or on a network node of a service provider, or in part on a network node of the mobile communication network and in part on a network node of a service provider, causes the computer or the network node of the mobile communication network and/or the network node of the service provider to perform an inventive method.

[0079] 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.

[0080] 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.

[0081] 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.

[0082] 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.

[0083] In FIG. **1**, a mobile communication network **100**, e.g., a public land mobile network **100**, is schematically shown, the mobile communication network **100** comprising an access network **110** and a core network **120**. The mobile

communication network **100** is preferably a cellular telecommunications network comprising typically a plurality of network cells (or radio cells), one of which is represented in FIG. **1** by means of a drawn-through circular line and reference sign **11**. Typically, a base station entity **111** (or eNodeB or enhanced NodeB) is assigned to each network cell **11**, the base station entity **111** being part of the access network **110** of the mobile communication network **100**. In the mobile communication network **100**, typically a plurality of user equipments are camping on the mobile communication network **100**. Representative for the plurality of user equipments within the network cell (or radio cell) **11**, a user equipment **20** is schematically shown.

[0084] The mobile communication network **100** comprises a subscriber database **130** and the mobile communication network **100** (and especially the subscriber database **130** is in contact with (or connected to) a service provider **10**. By means of the connection between the service provider **10** and the mobile communication network **100**, e.g., the subscriber database **10** of the mobile communication network **100**, the additional data related to the user equipment **20** and/or related to the subscriber identity module can be transferred to the service provider in case that the service provider requests such additional data (which is only the case in connection with the first occurrence of providing the service, not in connection with the second occurrence of providing the service.

[0085] According to the present invention, the mobile network operator transmits auxiliary information (i.e. additional data) related to a subscriber, i.e. to the user equipment **20**, to the service provider, i.e. a partner, such as, e.g., a bank, a payment provider, a game provider or to another third party. This additional data may comprise:

[0086] data of the device (or user equipment used) such as

[0087] the unique identifier of the SIM card used (e.g. MSISDN (Mobile Subscriber ISDN (integrated services digital network) number), or the IMSI (International Mobile subscriber identity),

[0088] data related to the mobile (e.g. the IMEI (International Mobile Equipment identity),

[0089] information about SIM type (SIM card platform, form factor, embedded SIM, specific IMSI classes or categories),

[0090] subscription data such as

[0091] tariff information (e.g. pre-paid vs. post-paid)

[0092] configuration of embedded SIMs, e.g. what MNO is currently provided?

[0093] booking of tariff options

[0094] customer's credit-worthiness class

[0095] network-related data such as

[0096] network generation (2G/3G/4G, the term 2G referring to second generation mobile radio networks (e.g. GSM), the term 3G referring to third generation mobile radio networks (such as UMTS), the term 4G referring to fourth generation mobile radio networks (such as LTE)) and other parameters like the encryption algorithm (A5/1 vs. A5/3, corresponding to modes of GSM encryption algorithm A5 which provide different cryptographic strength) used of the current mobile connection of the user equipment,

[0097] visited network (VPMN identifier)

[0098] usage data such as

[0099] unique identifiers of mobile data connections or their endpoints (e.g. IP addresses, dynamic DNS (domain name system) information),

[0100] additional information like location information (e.g. cell tower data, or geographical distance between two Multi-SIM cards—if cards are usually close to each other, higher distance can be an indication of a stolen SIM card),

[0101] information about set-up of call forwarding (national or international), or forwarding of messaging services (such as SMS, or e-mail, or instant messaging), or calling line identity restriction (CLIR),

[0102] special interaction with customer care, such as: ordering of multi-SIMs, replacement SIMs

[0103] information about what mobile device is currently in use.

[0104] According to the present invention, all these data can be combined with timestamps. Taken together these data and these timestamps provide information such as:

[0105] the validity period of the subscriber identity module: When did the last SIM swap take place (when was the last time the IMSI has changed) or did the last SIM swap/the last time the IMSI has changed occur in the last 5 days? This additional information provides an indication of fraud scenarios (e.g. a fraudster has ordered a multi-SIM card, or requested an exchange SIM card, in order to intercept mobile TAN);

[0106] When was the last time the customer changed his/her mobile device?

[0107] Is call forwarding set up, and if, since when?

[0108] According to the present invention, potential use cases include but are not restricted to:

[0109] risk scoring/fraud detection,

[0110] location based services,

[0111] location tracking/location sharing, for service providers or partner companies (e. g. in the banking or transportation sector) or even law enforcement.

[0112] All this information can be used as input for value-added services and other services (e.g. like fraud risk scoring/fraud detection systems).

[0113] The transmission of any such customer-related data, which may constitute personally identifiable information, requires either an appropriate legal foundation or some form of user consent, either implicit or explicit.

[0114] According to the present invention, it is preferred that, the additional information which is transmitted to the service provider or a third party is consolidated prior to its transmission in such a way such that only the necessary information is passed on to the service provider or third party. This includes, e.g.,

[0115] the raw data can be pre-processed according to certain rule sets,

[0116] they can be combined by logical (Boolean expressions, like AND, OR, NOT)

[0117] arithmetical calculations (computing an average, minimum, maximum, difference, etc.) can be performed, or

[0118] the service provider or partner may define the pre-processing operations in the form of a program (code written in a programming language) or a so-called script.

[0119] Only the consolidated data, which are the result of the computation, are then transmitted to the service provider **10** or partner. This takes care of concepts like appropriation

(data is only used for a well-defined purpose), data reduction and data economy (only the data needed is collected and transmitted).

[0120] For example, in order to detect a SIM swap, the IMSI (which constitutes personally identifiable information) does not have to be passed on to the third party. Instead, only the timestamp of the last IMSI change (and thus SIM card change) has to be transmitted. Depending on the scenario, only coarse information like "SIM card did not change within the last 3 months" or to transmit finer-grained information like "last SIM card swap took place 234 days ago" is transmitted.

[0121] While the invention has been illustrated and described in detail in the drawings and foregoing description, such illustration and description are to be considered illustrative or exemplary and not restrictive. It will be understood that changes and modifications may be made by those of ordinary skill within the scope of the following claims. In particular, the present invention covers further embodiments with any combination of features from different embodiments described above and below. Additionally, statements made herein characterizing the invention refer to an embodiment of the invention and not necessarily all embodiments.

[0122] The terms used in the claims should be construed to have the broadest reasonable interpretation consistent with the foregoing description. For example, the use of the article "a" or "the" in introducing an element should not be interpreted as being exclusive of a plurality of elements. Likewise, the recitation of "or" should be interpreted as being inclusive, such that the recitation of "A or B" is not exclusive of "A and B," unless it is clear from the context or the foregoing description that only one of A and B is intended. Further, the recitation of "at least one of A, B and C" should be interpreted as one or more of a group of elements consisting of A, B and C, and should not be interpreted as requiring at least one of each of the listed elements A, B and C, regardless of whether A, B and C are related as categories or otherwise. Moreover, the recitation of "A, B and/or C" or "at least one of A, B or C" should be interpreted as including any singular entity from the listed elements, e.g., A, any subset from the listed elements, e.g., A and B, or the entire list of elements A, B and C.

1. A method for preventing fraud or misuse based on a risk scoring approach when using a service of a service provider requested by a user equipment, the user equipment being connected to a mobile communication network and the user equipment comprising a subscriber identity module,

wherein a subscriber database is assigned to the mobile communication network, the subscriber database comprising information related to the user equipment and/or related to the subscriber identity module,

wherein for different occurrences of providing the service of the service provider with respect to the user equipment, the user of the user equipment is authenticated by transmitting an authentication information between the service provider and the user equipment, wherein for the purpose of the transmission of authentication information between the service provider and the user equipment, the user equipment is identified using a Mobile Station Integrated Services Digital Network (MSISDN) number of the user equipment,

wherein the method comprises:

in connection with a first occurrence of providing the service, transmitting by the service provider, in a first step, a request message to the subscriber database of the mobile communication network, the request message being related to the MSISDN of the user equipment, and the request message requesting additional data related to the user equipment and/or related to the subscriber identity module,

receiving by the service provider, in a second step, subsequent to the first step, an answer message from the subscriber database, the answer message comprising the additional data related to the user equipment and/or related to the subscriber identity module, and

in connection with a second occurrence of providing the service, the second occurrence of providing the service being either prior or subsequent to the first occurrence of providing the service, transmitting an authentication information between the service provider and the user equipment without transmitting a request message and a corresponding answer message.

2. The method according to claim **1**, wherein the first occurrence of providing the service, including transmitting the request message and receiving the answer message, is performed based on a risk scoring threshold of the service provider being exceeded.

3. The method according to claim **1**, wherein the information related to the user equipment and/or related to the subscriber identity module corresponds to at least one of the following:

a time information related to a swap of the subscriber identity module,

a time information related to a change of the subscriber identity module,

a time information related to a generation of an analogous subscriber identity module, related to the same MSISDN of the user equipment,

a time information related to a change of the user equipment,

a time information related to a change of the type of the user equipment,

a time information related to a change of the class of the user equipment, and

a time information related to a change of the International Mobile Equipment Identity (IMEI).

4. The method according to claim **3**, wherein each respective time information corresponds to an indication of whether the respective event did occur or did not occur within one of a plurality of preceding time intervals.

5. The method according to claim **4**, wherein the time intervals are predefined and refer to the time of the request message or the answer message.

6. The method according claim **1**, wherein the information related to the user equipment and/or related to the subscriber identity module corresponds to at least one of the following:

an amount information related to the number of analogous subscriber identity modules used, related to the same MSISDN of the user equipment (**20**),

an information relating to the type of the subscriber identity module,

an information relating to the subscription or tariff of the user equipment with the mobile communication network,

an information relating to a radio access technology used by the user equipment within the mobile communication network,

an information related to which type of an encryption algorithm is used by the user equipment within the mobile communication network,

an information related to a visited mobile communication network (VPLMN) of the user equipment,

an information related to unique identifiers of mobile data connections or their respective endpoints, and

an information related to location information of analogous subscriber identity modules related to the same MSISDN of the user equipment.

7. The method according to claim **1**, wherein the user equipment is identified via:

the MSISDN of the user equipment connected with the mobile communication network, or

an Internet Protocol (IP)-address according to IPv6, or an IP-address and an information regarding a point in time of an IP-connection of the user equipment with the mobile communication network.

8. A system for preventing fraud or misuse based on a risk scoring approach when using a service of a service provider, the system comprising:

the service provider, and

a mobile communication network,

wherein the service provider is configured to allow requesting of the service of the service provider by a user equipment connected to the mobile communication network, the user equipment comprising a subscriber identity module,

wherein a subscriber database is assigned to the mobile communication network, the subscriber database comprising information related to the user equipment and/or related to the subscriber identity module,

wherein for different occurrences of providing the service of the service provider with respect to the user equipment, the service provider is configured to provide authentication of the user of the user equipment is authenticated via transmission of an authentication information between the service provider and the user equipment, wherein for the purpose of the transmission of authentication information between the service provider and the user equipment, the user equipment is identified using the Mobile Station Integrated Services Digital Network (MSISDN) number of the user equipment, and

wherein the service provider is configured to:

in connection with a first occurrence of providing the service, transmit a request message to the subscriber database of the mobile communication network, the request message being related to the MSISDN of the user equipment, and the request message requesting additional data related to the user equipment and/or related to the subscriber identity module,

receive an answer message from the subscriber database, the answer message comprising the additional data related to the user equipment and/or related to the subscriber identity module, and

in connection with a second occurrence of providing the service, facilitate transmission of an authentication information between the service provider and the user equipment without transmitting a request message and a corresponding answer message.

9. The system according to claim **8**, wherein the first occurrence of providing the service, including transmission of the request message and reception of the answer message, is based on a risk scoring threshold of the service provider being exceeded.

10. The system according to claim **8**, wherein the information related to the user equipment and/or related to the subscriber identity module corresponds to at least one of the following:

a time information related to a swap of the subscriber identity module,

a time information related to a change of the subscriber identity module,

a time information related to a generation of an analogous subscriber identity module, related to the same MSISDN of the user equipment,

a time information related to a change of the user equipment,

a time information related to a change of the type of the user equipment,

a time information related to a change of the class of the user equipment, and

a time information related to a change of the International Mobile Equipment Identity (IMEI).

11. The system according to claim **10**, wherein each respective time information corresponds to an indication of whether the respective event did occur or did not occur within one of a plurality of preceding time intervals.

12. The system according to claim **11**, wherein the time intervals are predefined and refer to the time of the request message or the answer message.

13. A mobile communication network for preventing fraud or misuse based on a risk scoring approach when using a service of a service provider requested by a user equipment connected to the mobile communication network, the user equipment comprising a subscriber identity module,

wherein a subscriber database is assigned to the mobile communication network, the subscriber database comprising information related to the user equipment and/or related to the subscriber identity module,

wherein for different occurrences of providing the service of the service provider with respect to the user equipment, the user of the user equipment is authenticated via transmitting an authentication information between the service provider and the user equipment, wherein for the purpose of the transmission of authentication information between the service provider and the user equipment, the user equipment is identified via a Mobile Station Integrated Services Digital Network (MSISDN) number of the user equipment,

wherein the mobile communication network is configured such that:

in connection with a first occurrence of providing the service, a request message is transmitted by the service provider to the subscriber database of the mobile communication network, the request message being related to the MSISDN of the user equipment, and the request message requesting additional data related to the user equipment and/or related to the subscriber identity module,

an answer message is transmitted by the subscriber database to the service provider, the answer message comprising the additional data related to the user equipment and/or related to the subscriber identity module, and

in connection with a second occurrence of providing the service, an authentication information is transmitted

between the service provider and the user equipment without transmitting a request message and a corresponding answer message.

14. A non-transitory, processor-readable medium having processor-executable instructions stored thereon for preventing fraud or misuse based on a risk scoring approach when using a service of a service provider requested by a user equipment, the user equipment being connected to a mobile communication network and the user equipment comprising a subscriber identity module,

wherein a subscriber database is assigned to the mobile communication network, the subscriber database comprising information related to the user equipment and/or related to the subscriber identity module,

wherein for different occurrences of providing the service of the service provider with respect to the user equipment, the user of the user equipment is authenticated by transmitting an authentication information between the service provider and the user equipment, wherein for the purpose of the transmission of authentication information between the service provider and the user equipment, the user equipment is identified using a Mobile Station Integrated Services Digital Network (MSISDN) number of the user equipment,

wherein the processor-executable instructions, when executed, facilitate performance of the following steps:

in connection with a first occurrence of providing the service, transmitting by the service provider, in a first step, a request message to the subscriber database of the mobile communication network, the request message being related to the MSISDN of the user equipment, and the request message requesting additional data related to the user equipment and/or related to the subscriber identity module,

receiving by the service provider, in a second step, subsequent to the first step, an answer message from the subscriber database, the answer message comprising the additional data related to the user equipment and/or related to the subscriber identity module, and

in connection with a second occurrence of providing the service, the second occurrence of providing the service being either prior or subsequent to the first occurrence of providing the service, transmitting an authentication information between the service provider and the user equipment without transmitting a request message and a corresponding answer message.

* * * * *