US 20030101345A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2003/0101345 A1

Nyberg (43) Pub. Date: May 29, 2003

(54) SUBSCRIBER AUTHENTICATION

(76) Inventor: Kaisa Nyberg, Helsinki (FI)

Correspondence Address:
PILLSBURY WINTHROP, LLP
P.O. BOX 10500
MCLEAN, VA 22102 (US)

(21) Appl. No.: 10/256,256

(22) Filed: Sep. 27, 2002

Related U.S. Application Data

(63) Continuation of application No. PCT/FI01/00293, filed on Mar. 26, 2001.

(30) Foreign Application Priority Data

Mar. 30, 2000 (FI) 20000732

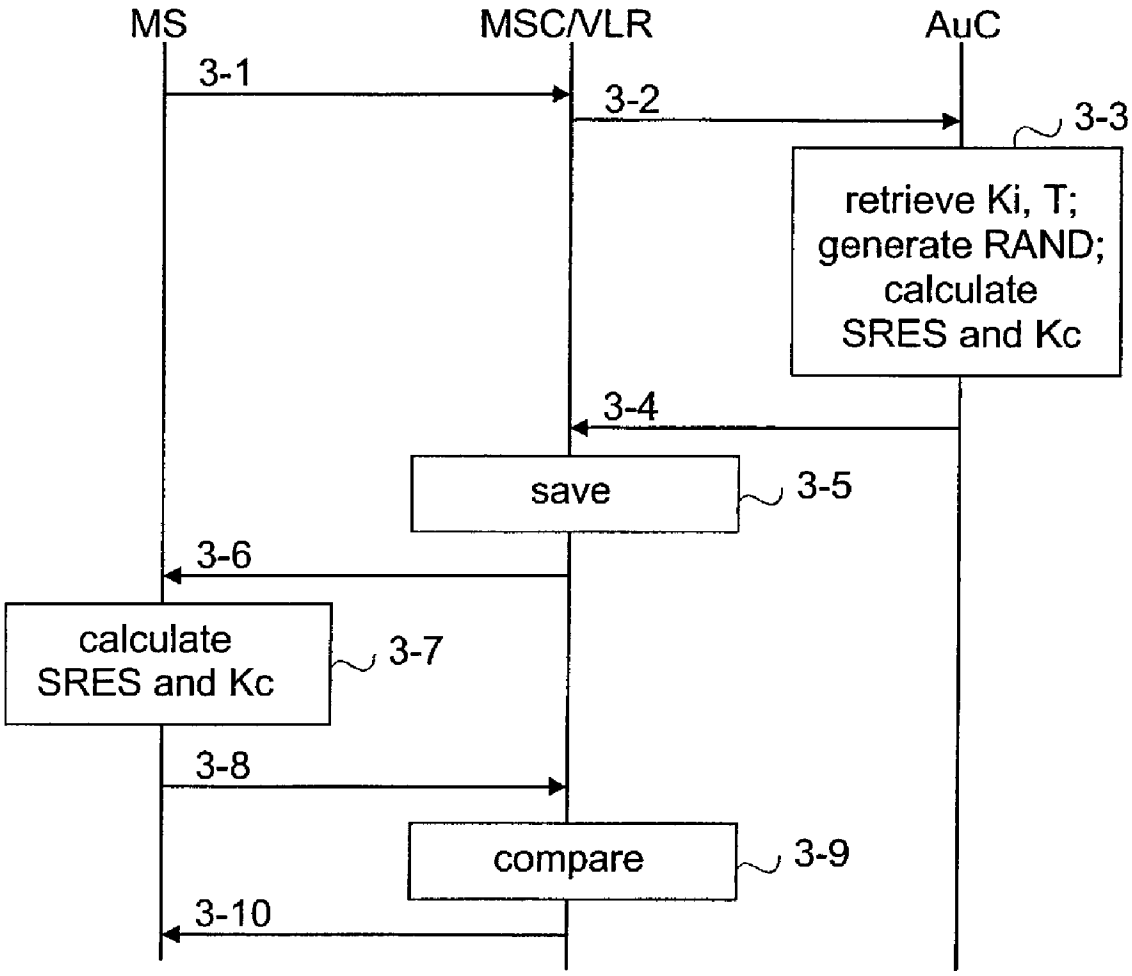
Publication Classification

(51) Int. Cl.[7] H04L 9/00

(52) U.S. Cl. 713/170

(57) ABSTRACT

To provide reliable and customized authentication, a parameter to be used in authentication is defined for the operator. A secret which may be stored e.g. in a subscriber identity module is calculated (404) from the operator parameter and a subscriber key. An authentication response is calculated (405) from the secret and the challenge to be used in authentication with a one-way function.



Salesforce EX1042
Salesforce, Inc. v. IQX Corp.
IPR2026-00475

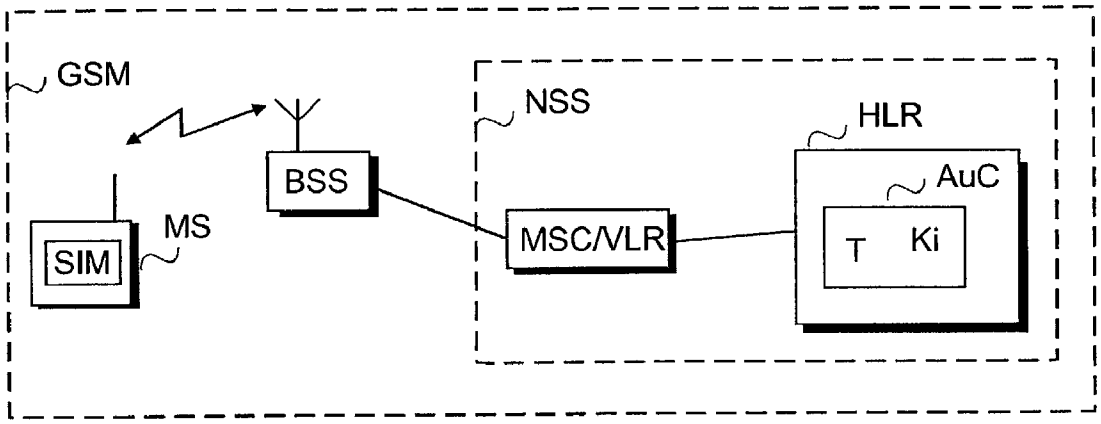

GSM
NSS
HLR
AuC
BSS
MS
SIM
MSC/VLR
T
Ki

FIG.1

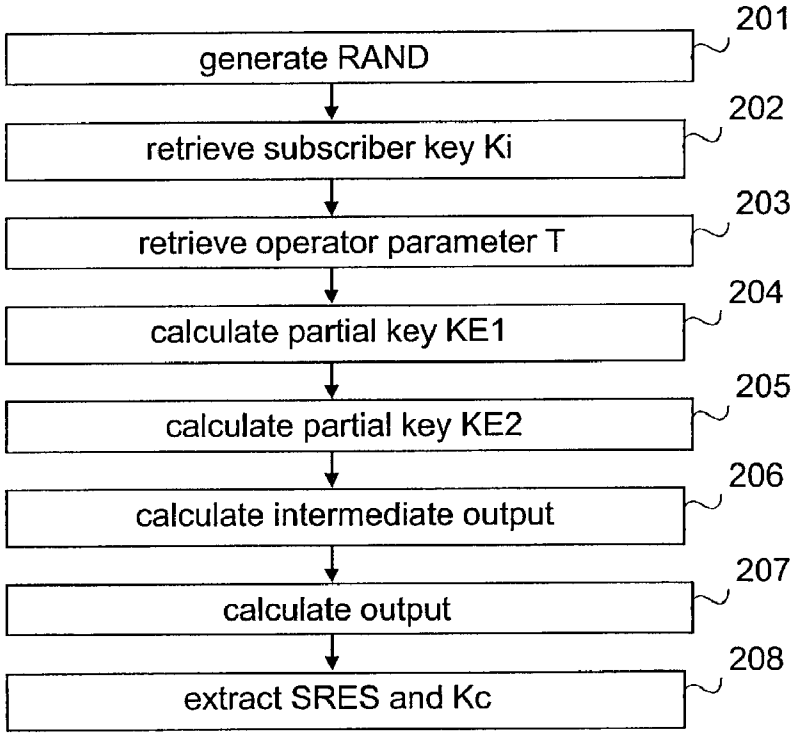

generate RAND
201
retrieve subscriber key Ki
202
retrieve operator parameter T
203
calculate partial key KE1
204
calculate partial key KE2
205
calculate intermediate output
206
calculate output
207
extract SRES and Kc
208

FIG.2

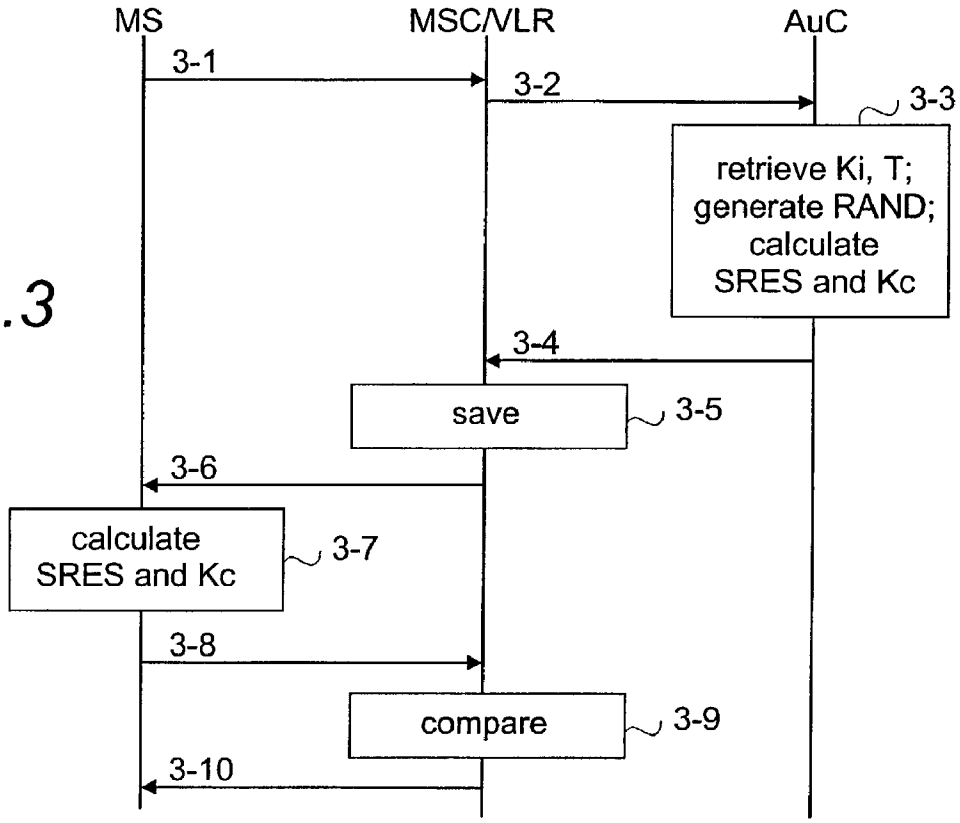

MS
MSC/VLR
AuC
3-1
3-2
3-3
retrieve Ki, T; generate RAND; calculate SRES and Kc
3-4
save
3-5
3-6
calculate SRES and Kc
3-7
3-8
compare
3-9
3-10

FIG.3

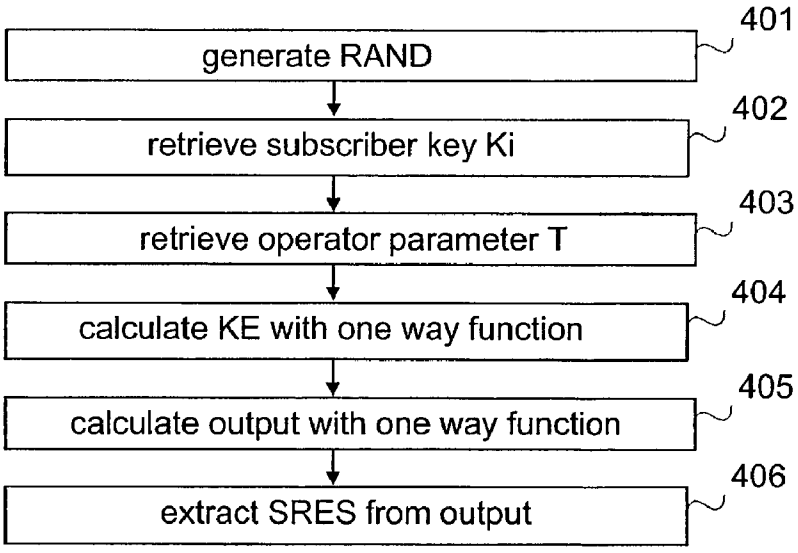

generate RAND
401
retrieve subscriber key Ki
402
retrieve operator parameter T
403
calculate KE with one way function
404
calculate output with one way function
405
extract SRES from output
406

FIG.4

SUBSCRIBER AUTHENTICATION

[0001] This application is a Continuation of International Application PCT/FI10/00293 filed Mar. 26, 2001 which designated the U.S. and was published under PCT Article 21(2) in English.

BACKGROUND OF THE INVENTION

[0002] The invention relates to an algorithm used in subscriber authentication in a mobile communication system, and particularly to an authentication response used in subscriber authentication.

[0003] The mobile communication system generally refers to any telecommunications system which enables wireless communication when users roam within the service area of the system. The public land mobile network PLMN is a typical example of a mobile communication system.

[0004] In mobile communication systems, mobile stations and the actual network usually communicate via radio paths. A radio path is physically open, which causes security risks and therefore both the users and the operator should be protected against intrusion by a third party, whether intrusion is unintentional or not. For example, illegal access to the network is prevented so that the network authenticates a mobile station when it registers with the network. The risk of eavesdropping is reduced by using encryption.

[0005] Authentication is a procedure in which one party authenticates the other party according to an agreed procedure. In the pan-European mobile communication system GSM (Global System for Mobile communications), for example, the algorithms to be used in authentication and the subscriber's key Ki are stored both in the subscriber identity module SIM and in the authentication center for authentication. In the GSM system the authentication response SRES to be used in authentication is calculated using algorithm **A3** and the key Ks to be used in encryption of the information to be transmitted over the radio path with algorithm **A8**. Typically these algorithms are combined so that both the authentication response SRES and the encryption key Kc are calculated during authentication. Algorithms **A3** and **A8** are operator-specific, proprietary and typically secret. The random number generator in the authentication center generates a challenge RAND which is transmitted to a mobile station over the radio path during authentication. The challenge RAND and the subscriber key Ki are used for calculating the authentication response SRES and the encryption key Kc both in the authentication center and in the mobile station. During authentication the mobile station sends the authentication response SRES calculated by it back to the network where it is compared with the authentication response calculated by the authentication center. If the responses are identical, the mobile station passes authentication, after which the information to be transmitted on the radio path is usually encrypted with an encryption key Kc.

[0006] The problem related to the authentication procedure described above is that operator-specific customization is not possible. Neither can the algorithms be revealed to different operators, for example, without at the same time giving the operator a chance of interfering with the authentication system of another operator. Thus the security of the system cannot be guaranteed, either.

BRIEF DESCRIPTION OF THE INVENTION

[0007] The object of the invention is to provide a method and an apparatus implementing the method to eliminate the above-mentioned problems. The objects of the invention are achieved with the methods, systems, authentication centers and subscriber identity modules which are characterized by what is disclosed in the independent claims. The preferred embodiments of the invention are disclosed in the dependent claims.

[0008] The invention is based on the idea that a parameter is defined for an operator and secret information is calculated from the subscriber key Ki and the operator parameter with a one-way function. The secret information and a challenge (public information) are used to calculate at least an authentication response with a one-way function, but the encryption key Kc can also be calculated at the same time, if desired. 'Key' is a general term for encrypted information, i.e. a secret. An advantage of the invention is that it enables operator-specific customization of authentication. A further advantage is that the security of the invention is not based on a secret algorithm but on a secret key, and thus the algorithm can be revealed to the operators.

[0009] In a preferred embodiment of the invention a secret (or secrets) calculated from the subscriber key and the operator parameter are stored in the subscriber identity module. An advantage of this embodiment is that calculation of the authentication response can be implemented easily in the subscriber identity module. Authentication will also become quicker when pre-calculated information is used. A further advantage of this embodiment is that the operator parameter cannot be derived even though the information included in the identity module could be decoded.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The invention will be described in greater detail by means of preferred embodiments with reference to the accompanying drawings, in which

[0011] **FIG. 1**, illustrates the network architecture of the GSM system;

[0012] **FIG. 2** is a flow chart of an authentication algorithm according to a first preferred embodiment of the invention;

[0013] **FIG. 3** illustrates signalling according to a first preferred embodiment of the invention; and

[0014] **FIG. 4** is a flow chart of an authentication algorithm according to a second preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0015] The present invention is applicable to any telecommunications system where the subscriber is authenticated. These include the GSM system, its next generation, known as GSM **2+**, and similar systems, such as the PCS (Personal Communication System) and DCS **1800** (Digital Cellular System for 1800 MHz). The invention is also applicable in the third generation mobile communication systems, such as the UMTS (Universal Mobile Telecommunications System) and IS-41 (Interim Standard). In the following the invention

will be described using the GSM system as an example without limiting the invention to this particular system.

[0016] **FIG. 1** illustrates the network architecture of the GSM system at a general level because a more detailed structure of the system is not relevant to the invention.

[0017] The structure of a network GSM according to the GSM system **1** consists of two parts: a base station subsystem BSS and a network subsystem NSS. The BSS and mobile stations MS communicate via radio connections. The base station subsystem is connected to a mobile switching center MSC of the network subsystem NSS. The function of the mobile switching center is to switch calls involving at least one mobile station MS. Some mobile switching centers are connected to other telecommunications networks, such as the PSTN (Public Switched Telephone Network) and they comprise switching functions for switching calls to and from these networks. These mobile switching centers are called gateway centers.

[0018] The network subsystem NSS comprises two types of databases. Subscriber information on all subscribers of the network is stored permanently or semipermanently in a home location register HLR, the subscriber information being connected to the subscriber's identifier IMSI. The other type of register is a visitor location register VLR. When a mobile station MS is active (is registered in the network and can make or receive calls), most of the subscriber information on the mobile station MS included in the home location register HLR is loaded (copied) into the visitor location register of the mobile switching center MSC in the area of which the mobile station MS is. In fact, the mobile switching center MSC and the visitor location register VLR are the central network elements in respect of mobility management, controlling and signalling.

[0019] The network subsystem also comprises an authentication center AuC. The authentication center AuC is typically part of the subscriber's home location register HLR. The authentication center AuC comprises a random number generator (not shown) for generating challenges, i.e. random number parameters RAND. The authentication center also has memory for storing authentication information on the subscriber and authentication algorithms. The subscriber's authentication information to be stored according to the first and second preferred embodiment of the invention includes a subscriber key Ki and an operator parameter T. If the operator has more than one parameter, the authentication center can combine the subscriber key Ki with the parameter of the correct operator e.g. by storing the operator parameter or an identifier identifying the operator parameter into the subscriber information. The authentication center preferably calculates an authentication response SRES and an encryption key from the subscriber key, operator parameter and random number using one of the authentication algorithms shown in **FIGS. 2, 3** and **4** and forms 'authentication triplets', i.e. entities consisting of the random number RAND, authentication response SRES and encryption key Kc. The operator parameter is preferably a binary parameter which consists of the operator's identifier and the operator's secret. The operator parameter does not need to be secret. The operator parameter T is described in greater detail in connection with **FIG. 2**.

[0020] In this application 'mobile station' MS generally refers to the entity formed by the mobile subscriber and the actual terminal. The terminal may be any device that can communicate in a mobile communication system or a combination of several devices, e.g. a multimedia computer equipped with a card phone produced by Nokia to provide mobile connection. The subscriber is identified from the subscriber identity module SIM detachably connected to the terminal. The SIM is a smart cart which is inserted into the mobile station and includes information related to identification of the subscriber, such as an international mobile subscriber identity IMSI, and means for authenticating the subscriber. In other words, the SIM includes the algorithms and secrets needed in authentication. Typically the SIM also comprises a temporary mobile subscriber identity of the location area TMSI by means of which transmission of the IMSI over the radio path can be avoided.

[0021] The telecommunications system, authentication center and mobile station implementing the functionality according to the present invention include, in addition to the prior art devices needed in authentication, means for taking the operator parameter into account in authentication. Existing network nodes comprise processors and memory that can be utilized in the functions according to the invention. All the changes needed to implement the invention can be carried out by means of added or updated software routines and/or application circuits (ASIC). The mobile station and/or the authentication center may also require additional memory.

[0022] **FIG. 2** shows algorithm **A3/A8** which is used in the first preferred embodiment of the invention and in which two different algorithms are combined, as is usual in the GSM system. For the algorithm of the invention it is necessary to define at least one operator parameter T and a separate key Ki for each subscriber. The subscriber-specific key Ki is defined according to the prior art and its length is 128 bits according to the GSM standard. In the first preferred embodiment of the invention the algorithm consists of two different encryption functions which are well known to the persons skilled in the art: the internationally standardized hash function RIPEMD-**128** and the encryption algorithm in accordance with the DES standard (Data Encryption Standard). This allows to combine the best properties of these functions. The algorithm used in the first preferred embodiment of the invention is thus one of the message authentication codes MAC. Hash algorithms are inherently non-reversible and numerically efficient. The encryption algorithms, on the other hand, are better suited for smart cards most of which support the DES algorithm. The encryption algorithm is a one-way function when secret input is used as the key of the encryption algorithm. By utilizing widely used and tested one-way functions we can ensure that the security requirements set for the network are fulfilled. Openness allows to ensure that the algorithm does not contain intentional trapdoors or other weaknesses. Breaking the algorithm completely, i.e. finding out the operator parameters and subscriber keys by analysing the algorithm is highly unlikely because this would require breaking of the corresponding international standards.

[0023] In the first preferred embodiment the operator parameter T is a 384-bit parameter consisting of the operator's code CC and the operator's secret CS. In other words, T is CC||CS. It should still be emphasized that the following

is only one example of defining the operator parameter. The invention does not in any way restrict the manner of defining the operator parameter.

[**0024**] The operator code CC is, in the first preferred embodiment of the invention, a 128-bit hash code which is obtained e.g. with the hash function RIPEMD-**128** from the following text when 27 X's are replaced e.g. with the operator's name and empty spaces, after which the text is coded with AS-CII: NOKIA NETWORKS GSM A3A8 FOR XXXXXXXXXXXXXXXXXXXXXXXXXXX. Thus different operators have different parameters. The same operator may also have several parameters if the operator adds different letters or numbers to the end of his name. The different value of even one X yields a different operator code CC.

[**0025**] The operator secret CS is, in the first preferred embodiment of the invention, a string consisting of 256 bits. The operator may select this string freely. It is, however, recommendable to generate a unique value for the operator secret so that it is unpredictable. This allows to ensure that the operators' values differ from one another considerably. The value of the operator parameter may also be a string of zeroes when the operator parameter is not intended to be secret. One operator may have several different secrets CS and thus different operator parameters.

[**0026**] In the authentication algorithm according to the first preferred embodiment of the invention a random number, the length of which is 128 bits according to the GSM standard, is generated into a challenge RAND in step **201**. The subscriber key Ki is retrieved in step **202** and the operator parameter T in step **203**. The sub-value is also called partial key. In steps **203** and **204** we calculate sub-values KE**1** and KE**2** for an extended key. Each sub-value consists of 128 bits. The sub-vales are calculated independently from the operator parameter T and the subscriber key Ki. To calculate the sub-value the operator parameter T and the subscriber key Ki are masked and after masking a sub-value is calculated from them using a hash function RIPEMD-**128** with one round. In the calculating a standard initial value is used but padding and length appending are not performed because the input has a standard length. The sub-value KE**1** is calculated using a mask IPAD which is a string consisting of 64 octets 00110110. The sub-value KE**2** is calculated using a mask OPAD which is a string consisting of 64 octets 01011100. After the sub-values KE**1** and KE**2** have been calculated, a 128-bit intermediate output is calculated from the sub-value KE**1** and the challenge RAND in step **206** using a three-round Feistel network F where the DES algorithm serves as the round function. The calculation will be described in greater detail below. In step **207** a 128-bit output is calculated from the sub-value KE**2** and the intermediate result using a three-round Feistel network F where the DES algorithm serves as the round function. 32 left-most bits are extracted from the output to form an authentication response SRES and the next 64 bits are used to form an encryption key Kc in step **208**.

[**0027**] The calculation described above can be expressed by the following formula according to the HMAC standard (keyed-hashing for message authentication):

$$H((\{Ki\|T\}\oplus OPAD)\|H((\{Ki\|T\}\oplus IPAD)\|RAND)),$$

[**0028**] where a novel proprietary hash function H of the invention is obtained by combining the standardized RIPEMD-**128** and the three-round Feistel network by means of a key-scheduling operation to be described below. Key-scheduling refers to the manner in which the algorithm utilizes the key parameter. In most cases more than one partial key is derived which are used in different phases of the algorithm calculation.

[**0029**] The three-round Feistel network F receives two inputs which in the first preferred embodiment of the invention are a 128-bit key KEj and a 128-bit data input DIj. A 128-bit output DOj (DOj=F(KEj; DIj)) is calculated in two phases.

[**0030**] In the first phase we perform key scheduling. In the first preferred embodiment of the invention three 64-bit DES keys are derived from the key KEj in a new manner. First the key KEj is divided into 16 octets KEJ[0] . . . KEj[15]. These octets are converted into 32 octets Mj[0] . . . Mj[31] as follows:

Mj[k] = KEj[k],	k = 0, . . ., 15;
Mj[k] = KEj[(k − 10) mod 8],	k = 16, . . ., 23;
Mj[k] = KEj[((k − 20) mod 8) + 8],	k = 24, . . ., 31.

[**0031**] Thus each octet of the key KEj occurs twice in array Mj in the following order:

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
6	7	0	1	2	3	4	5
12	13	14	15	8	9	10	11

[**0032**] The first 64-bit DES key Kj**1** is obtained by changing the halves of each octet in the first row and by performing an XOR operation on the octets obtained in the change and on the octets of the second row. The key of the second round is obtained by repeating the same procedure on the octets of the second and the third row. Correspondingly, the third key is obtained by repeating the procedure on the octets of the third and the fourth row. Derivation of the DES keys Kj**1**, Kj**2** and Kj**3** from the array Mj[0,1, . . . 31] can be expressed as follows:

$$Kjr[n]=(\text{swap } Mj[n+8(r-1)])\oplus Mj[n+8r],\ n=0, \ldots ,7;\ r=1,2,3;$$

[**0033**] where 'swap' changes the halves of the octet B=B [0, . . . ,7] as follows:

$$\text{swap } B=B[4,5,6,7,0,1,2,3].$$

[**0034**] In the second phase the data input DIj [0 . . . 127] is divided into two parts, i.e. a left part DIjL=DIj[0 . . . 63] and a right part DIjR=DIj[64 . . . 127]. The 128-bit output is generated in two parts, a left output part DOjL=[0 . . . 63] and a right output part DOjR=DOj[64 . . . 127], as follows:

$$DOjR=DIjL\oplus DES(Kj2;\ DIjR\oplus DES(Kj1;\ DIjL))$$

$$DOjL=DIjR\oplus DES(Kj1;\ DIjL)\oplus DES(Kj3;\ DOjR).$$

[**0035**] In step **206** of **FIG. 2** the challenge formed by the random number is used as the data input and in step **207** of

FIG. 2 the intermediate output DO**1**. Steps **206** and **207** can be expressed by the following formulae:

$$DI2=DO1=F(KE1;\ \mathrm{RAND}),\ (\text{step } 206)$$

$$DO2=F(KE2;\ DI2)=F(KE2;\ F(KE1;\ \mathrm{RAND}))\ (\text{step } 207).$$

[**0036**] The algorithm according to the first preferred embodiment of the invention can be utilized in two ways: in a pre-calculated mode and in a direct mode. In the pre-calculated mode the partial keys KE**1** and KE**2** are calculated in advance (i.e. steps **202** to **205** have been carried out) and stored. In the pre-calculated mode steps **206** to **208** are carried out during authentication in addition challenge generation. When the above-mentioned Feistel network F with DES rounds is used in steps **206** to **208**, the algorithm to be carried out during the actual authentication in the pre-calculated mode is the same as the 128-bit DES algorithm DEAL.

[**0037**] **FIG. 3** illustrates authentication according to the first preferred embodiment of the invention as the mobile station registers in the network. The first preferred embodiment of the invention utilizes the algorithm described in connection with **FIG. 2** as such in the authentication center AuC and in the pre-calculated mode in the subscriber identity module SIM. This means that in addition to the whole algorithm, the subscriber key Ki and the operator parameter T are stored in the authentication center, whereas only part of the algorithm and partial keys KE**1** and KE**2** of the extended key are stored in the subscriber identity module SIM. The partial keys are treated and secured in the same way as the subscriber key Ki. In the example of **FIG. 3** it is assumed, for the sake of clarity, that the mobile switching center and the visitor location register are integrated into the same unit MSC/VLR.

[**0038**] At the beginning of authentication the mobile station MS transmits the identification data on the basis of which the SIM and the subscriber are identified to the mobile switching center MSC/VLR in message **3-1**. Usually identification information is the IMSI or the TMSI. The mobile switching center MSC/VLR sends an authentication request to the authentication center AuC in message **3-2**. The message **3-2** includes the subscriber identity IMSI. The visitor location register can change the TMSI into an IMSI. In step **3-3** the authentication center AuC selects a subscriber-specific authentication key Ki and the operator parameter T on the basis of the subscriber identity IMSI included in the authentication request. The authentication center AuC calculates the partial keys KE**1** and KE**2** from the operator parameter T and the subscriber key Ki as described in connection with **FIG. 2**. Furthermore, the random number generator generates e.g. five random number parameters RAND into challenges. A check parameter SRES and an encryption key Kc is formed of each challenge with the partial keys KE**1** and KE**2** as was described in connection with **FIG. 2**. In other words, when more than one authentication triplet is calculated at a time, it is sufficient to calculate only the partial keys KE**1** and KE**2** with the first triplet and then store the partial keys transiently into the memory for the calculation of the following triplets. The authentication center AuC transmits the five authentication triplets RAND, SRES, Kc so calculated in message **3-4** to the visitor location register MSC/VLR where they are stored in step **3-5**.

[**0039**] The visitor location register MSC/VLR selects an RAND value for the parameter from the subscriber's RAND/SRES/Kc table and sends it to the mobile station MS in message **3-6** and further to the subscriber identity module SIM. In the first preferred embodiment of the invention the SIM comprises partial keys KE**1** and KE**2** which have been calculated from the subscriber key Ki and the operator parameter T. The SIM also comprises steps **206** to **208** of the authentication algorithm A**3** shown in **FIG. 2**. In step **3-7** the SIM calculates the SRES parameter and the encryption key Kc by means of the received RAND parameter and keys KE**1** and KE**2** utilizing the Feistel network F with DES rounds as was described above. The mobile station sends the SRES parameter back to the visitor location register MSC/VLR. In step **3-9** the visitor location register MSC/VLR compares the SRES value sent by the mobile station with the stored SRES value and informs the mobile station MS whether or not the authentication was successful in message **3-10**. If the SRES value sent by the mobile station is the same as the stored SRES value, authentication has succeeded and encryption with the encryption key Kc can be started on the radio path.

[**0040**] When the visitor location register VLR is to authenticate the subscriber for the next time, it selects the next value for the parameter RAND from the subscriber's RAND/SRES/Kc table and transmits it to the mobile station and further to the subscriber identity module SIM.

[**0041**] The fact that the first preferred embodiment of the invention utilizes the pre-calculated mode of the algorithm of the invention in the subscriber identity module SIM and the direct form of the algorithm in the authentication center provides the advantage that the best features of both one-way functions can be combined and optimal performance and security guaranteed in a customized manner. The RIPEMD-**128** is a considerably efficient one-way function but the 8-bit processor used by the subscriber identity module SIM does not do justice to it. The DES is not as efficient as the RIPEMD-**128**, but it is known best and it can also be implemented safely and efficiently in the subscriber identity module SIM.

[**0042**] Every time the authentication center AuC uses the operator parameter T in the network, it also checks that the partial keys KE**1** and KE**2** included in the subscriber identity module SIM have really been derived using the operator parameter in question. Usually one operator uses several subscriber identity module SIM producers, who also form the subscriber keys Ki themselves. The operator probably also gives them the operator parameter for forming partial keys KE**1** and KE**2**. The operator can give a different operator parameter to each producer e.g. by using a producer-specific secret part CS and/or changing the operator's name in the operator code CC. The operator can also form the subscriber keys Ki and the related partial keys KE**1** and KE**2** himself and give them to the producer of the subscriber identity module SIM so that they can be stored in the identity module.

[**0043**] The one-way functions, masks and key scheduling described above are only intended to describe how the invention can be implemented and do not in any way limit the invention. The masks and key scheduling described above are only examples and not even necessary. It is also possible to use other one-way functions which need not be

public functions. Furthermore, the same one-way function can be used in each phase. On the other hand, different functions can be used in every phase so that the same function is never used twice for calculations. In addition, the first function can be used once and the second function three times, for example.

[**0044**] In other preferred embodiments of the invention the precalculated mode can be employed in the authentication center AuC, too. In that case partial keys KE**1** and KE**2** have to be stored in the authentication center AuC for the subscriber. On the other hand, the direct form can be used in the subscriber identity module SIM, in which case the whole algorithm, subscriber key Ki and operator parameter T are stored in the subscriber identity module, but not the partial keys KE**1** and KE**2**.

[**0045**] **FIG. 4** illustrates a second preferred embodiment of the invention. Here the algorithm according to the invention is described at its simplest without any detailed descriptions of functions and comments on the length of the outputs and inputs. The subscriber key Ki and the operator parameter T are defined in the second preferred embodiment of the invention, too.

[**0046**] The algorithm according to the second preferred embodiment of the invention begins with generation of a challenge RAND in step **401**. The subscriber key Ki is retrieved in step **402** and the operator parameter T in step **403**. Thereafter a key KE is calculated from the subscriber key Ki and the operator parameter T in step **404** with a one-way function. In step **405** an output is calculated from the key KE and the challenge RAND with a one-way function and an authentication response SRES is extracted from the output in step **406**.

[**0047**] Calculation according to the second preferred embodiment of the invention can be expressed by the following formula:

$$H2(H1(Ki||T)||RAND)$$

[**0048**] In the second preferred embodiment of the invention it is possible to use the same one-way functions, e.g. RIPEMD-**128** functions. Two different one-way functions can also be used, e.g. the RIPEMD-**128** function in step **404** and a six-round Feistel network where the DES serves as a round function in step **405** as was explained in connection with **FIG. 2**.

[**0049**] The second preferred embodiment can also be applied in the pre-calculated mode and the direct mode. In the pre-calculated mode the key KE is calculated in advance and stored e.g. in the subscriber identity module SIM.

[**0050**] The steps illustrated in **FIGS. 2, 3** and **4** are not in an absolute chronological order and some of the steps can be performed simultaneously or in a different order from what has been shown. Furthermore, some other functions may take place between the steps. On the other hand, some steps may be omitted. What is important is that the operator parameter is also used as the input in the authentication. The signalling messages described above in connection with **FIG. 3** are only referential and may contain several separate messages for transmitting the same information. The messages may also contain other kind of information. Depending on the operator and the system, other network elements between which different functionalities have been divided can also take part in the data transmission and signalling. Furthermore, it is possible that the subscriber identity module is arranged to generate a challenge and send it to the authentication center in connection with authentication.

[**0051**] Even though the invention has been described above in connection with mobile communication systems, the authentication algorithm of the invention can be applied in fixed networks, too, where the subscriber is authenticated by means of the identity module.

[**0052**] It should be understood that the preceding specification and the related drawings are only intended to illustrate the present invention. It will be obvious to a person skilled in the art that the invention may be varied and modified without deviating from the scope and spirit of the invention defined in the appended claims.

1. A method of arranging subscriber authentication in a telecommunications system, the method comprising:

defining a key for the subscriber;

generating a challenge to be used in authentication;

defining a parameter for the subscriber's operator;

calculating a first secret from the key and the parameter with a first one-way function;

calculating an output from the challenge and the first secret with a second one-way function;

extracting an authentication response from the output; and

authenticating the subscriber with the authentication response.

2. The method of claim 1, further comprising:

storing the first secret in a subscriber identity module; and

calculating, during authentication, the output from the first secret and the challenge in the subscriber identity module with the second one-way function.

3. The method of claim 1 wherein

the first one-way function is a hash function; and

the second one-way function is an encryption algorithm.

4. A method of arranging subscriber authentication in a telecommunications system, the method comprising:

defining a key for the subscriber;

generating a challenge to be used in authentication;

defining a parameter for the subscriber's operator;

calculating a first secret from the key and the parameter with a first one-way function;

calculating a second secret from the key and the parameter with a second one-way function;

calculating an intermediate output from the challenge and the first secret with a third one-way function;

calculating an output from the intermediate output and the second secret with a fourth one-way function;

extracting an authentication response from the output; and

authenticating the subscriber with the authentication response.

5. The method of claim 4, further comprising:

masking the key and parameter with a first mask before the first secret is calculated;

calculating the first secret from the masked key and parameter;

masking the key and parameter with a second mask before calculating the second secret; and

calculating the second secret from the masked key and parameter.

6. The method of claim 4 further comprising:

storing the first and the second secret in the subscriber identity module; and

calculating, during authentication, the intermediate output from the first secret and the challenge in the subscriber identity module with the third one-way function and the output from the intermediate output and the second secret with the fourth one-way function.

7. The method of claim 4 wherein

the first and the second one-way functions are hash functions; and

the third and the fourth one-way functions are encryption algorithms.

8. The method of claim 3 wherein the encryption algorithm utilizes a DES encryption algorithm.

9. The method of claim 1 wherein the parameter of the subscriber's operator includes an operator code and an operator secret.

10. The method of claim 1, further comprising extracting an encryption key from the output.

11. A telecommunications system comprising a subscriber identity module and an authentication center

the system being arranged to use a challenge as a parameter in authentication and authenticate a subscriber by comparing an authentication response calculated by the subscriber identity module with an authentication response calculated by the authentication center; wherein

at least one operator parameter is defined for the subscriber's operator;

the authentication center is arranged to store authentication information on the subscriber which includes at least a subscriber key and the operator parameter, calculate a first secret from the subscriber key and the operator parameter with a first one-way function; calculate an output from the first secret and the challenge with a second one-way function; and extract an authentication response from the output;

the subscriber identity module includes the first secret and is arranged to calculate an output from the first secret and the challenge with the second one-way function, and extract an authentication response from the output.

12. A telecommunications system comprising a subscriber identity module and an authentication center

the system being arranged to use a challenge as a parameter in authentication and authenticate a subscriber by comparing an authentication response calculated by the subscriber identity module with an authentication response calculated by the authentication center;

wherein at least one operator parameter is defined for the subscriber's operator;

the authentication center is arranged to store authentication information on the subscriber which includes at least a subscriber key; and the operator parameter, calculate a first secret from the subscriber key and the operator parameter with a first one-way function; calculate a second secret from the subscriber key and the operator parameter with a second one-way function, calculate an intermediate output from the first secret and the challenge with a third one-way function, calculate an output from the second secret and the intermediate output with a fourth one-way function, and extract an authentication response from the output;

the subscriber identity module comprises a first and a second secret and is arranged to calculate an intermediate output with a third one-way function, calculate an output from the second secret and the intermediate output with a fourth one-way function and to extract an authentication response from the output.

13. An authentication center in a telecommunications system which comprises at least one subscriber and in which a challenge is used as a parameter in authentication, the authentication center being arranged to store authentication information on the subscriber which includes at least a subscriber key,

store the operator parameter defined for the subscriber's operator, calculate a first secret from the subscriber key and the operator parameter with a first one-way function, calculate an output from the first secret and the challenge with a second one-way function and extract an authentication response to be used in authentication from the output.

14. An authentication center in a telecommunications system which comprises at least one subscriber to whom a subscriber key is defined as authentication information and in which system a challenge is used as a parameter in authentication, the authentication center being arranged to store a first secret calculated from the subscriber key and the operator parameter defined for the subscriber's operator with a first one-way function, calculate an output from the first secret and the challenge with a second one-way function, and extract an authentication response to be used in authentication from the output.

15. An authentication center in a telecommunications system which comprises at least one subscriber and in which a challenge is used as a parameter in authentication, the authentication center being arranged

to store authentication information on the subscriber which includes at least a subscriber key, store an operator parameter defined for the subscriber's operator, calculate a first secret from the subscriber key and the operator parameter with a first one-way function, calculate a second secret from the subscriber key and the operator parameter with a second one-way function, calculate an intermediate output from the first secret and the challenge with a third one-way function, calculate the output from the second secret and the intermediate output with a fourth one-way function, and extract an authentication response from the output.

16. An authentication center in a telecommunications system which comprises at least one subscriber to whom a subscriber key is defined as authentication information and in which system a challenge is used as a parameter in authentication, the authentication center being arranged to store a first secret calculated from the subscriber key and the operator parameter defined for the subscriber's operator with a first one-way function and a second secret calculated from the subscriber key and the operator parameter with a second one-way function, calculate an intermediate output from the first secret and the challenge with a third one-way function, calculate an output from the second secret and the intermediate output with a fourth one-way function, and extract an authentication response from the output.

17. A subscriber identity module which can be connected to the terminal used by a subscriber in a telecommunications system where a challenge is used as a parameter in authentication, the identity module comprising a subscriber keyand an operator parameter defined for the subscriber's operator; and being arranged to calculate a first secret from the subscriber key and the operator parameter with a first one-way function, calculate an output from the first secret and the challenge with a second one-way function, and extract an authentication response to be used in authentication from the output.

18. A subscriber identity module which can be connected to the terminal used by a subscriber in a telecommunications system which utilizes a subscriber key in authentication and a challenge as the parameter, the subscriber identity module including a first secret calculated from the subscriber key and the operator parameter defined for the subscriber's operator with a first one-way function; and being arranged to calculate an output from the first secret and the challenge with a second one-way function, and extract an authentication response to be used in authentication from the output.

19. A subscriber identity module which can be connected to the terminal used by a subscriber in a telecommunications system where a challenge is used as the parameter in authentication, the identity module comprising a subscriber key and an operator parameter defined for the subscriber's operator; and being arranged to calculate a first secret from the subscriber's key and the operator parameter with a first one-way function, calculate a second secret from the subscriber key and the operator parameter with a second one-way function, calculate an intermediate output from the first secret and the challenge with a third one-way function, calculate an output from the second secret and the intermediate output with a fourth one-way function, and extract an authentication response to be used in authentication from the output.

20. A subscriber identity module which can be connected to the terminal used by a subscriber in a telecommunications system which utilizes a subscriber key in authentication and a challenge as the parameter, the subscriber identity module including a first secret calculated from the subscriber key and the operator parameter defined for the subscriber's operator with a first one-way function and a second secret calculated from the subscriber key and the operator parameter with a second one-way function; and

being arranged to calculate an intermediate output from the subscriber's challenge and the first secret with a third one-way function, calculate an output from the intermediate output and the second secret with a fourth one-way function, and extract an authentication response from the output.

21. A method of arranging subscriber authentication in a telecommunications system, the method comprising:

defining a key for the subscriber;

generating a challenge to be used in authentication;

defining a parameter for the subscriber's operator;

calculating a first secret from the key and the parameter with a hash function;

storing the first secret in a subscriber identity module; and

calculating, during authentication, an output from the challenge and the first secret in the subscriber identity module with an encryption algorithm;

extracting an authentication response from the output; and

authenticating the subscriber with the authentication response.

22. A method of arranging subscriber authentication in a telecommunications system, the method comprising:

defining a key for the subscriber;

generating a challenge to be used in authentication;

defining a parameter for the subscriber's operator;

masking the key and parameter with a first mask;

calculating a first secret from the masked key and the parameter with a first one-way function;

masking the key and parameter with a second mask;

calculating a second secret from the masked key and the parameter with a second one-way function;

storing the first and the second secret in the subscriber identity module;

calculating, during authentication, an intermediate output from the challenge and the first secret in the subscriber identity module with a third one-way function;

calculating, during authentication, an output from the intermediate output and the second secret in the subscriber identity module with a fourth one-way function;

extracting an authentication response from the output; and

authenticating the subscriber with the authentication response.

23. The method of claim 22 wherein

the first and the second one-way functions are hash functions; and

the third and the fourth one-way functions are encryption algorithms.

24. The method of claim 23 wherein

the hash function is an RIPEMD-128 function; and

the encryption algorithm utilizes a DES encryption algorithm.

* * * * *