PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/22, H04L 9/32	A1	(11) International Publication Number: **WO 99/39524** (43) International Publication Date: 5 August 1999 (05.08.99)

(21) International Application Number: PCT/FI99/00019

(22) International Filing Date: 13 January 1999 (13.01.99)

(30) Priority Data:
980085 16 January 1998 (16.01.98) FI

(71) Applicant *(for all designated States except US)*: SONERA OY [FI/FI]; Teollisuuskatu 15, FIN-00510 Helsinki (FI).

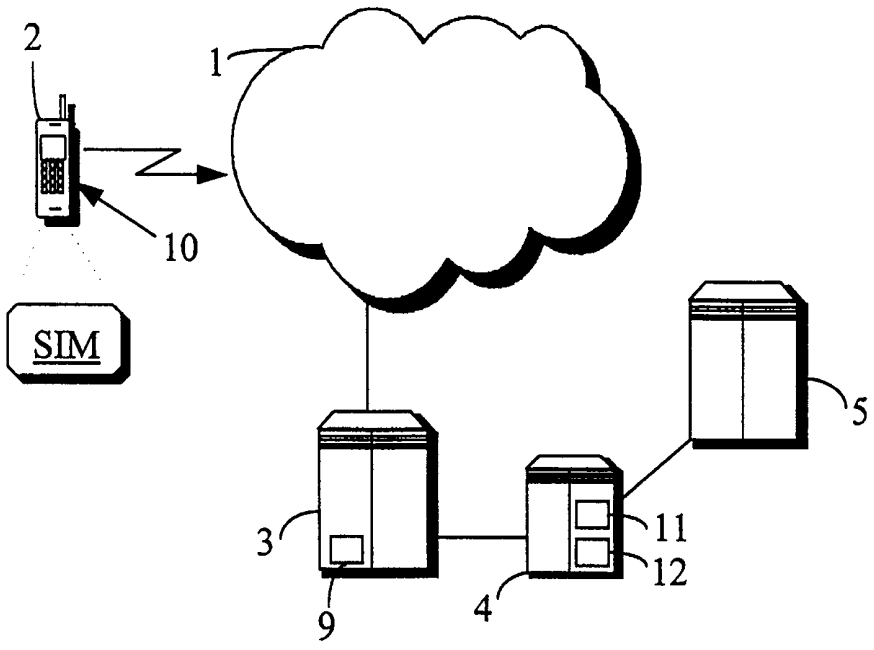
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: HEINONEN, Petteri [FI/FI]; Postipuuntie 12 D 52, FIN-02600 Espoo (FI).

(74) Agent: PAPULA REIN LAHTELA OY; Fredrikinkatu 61 A, P.O. Box 981, FIN-00101 Helsinki (FI).

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

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
In English translation (filed in Finnish).

(54) Title: PROCEDURE AND SYSTEM FOR THE PROCESSING OF MESSAGES IN A TELECOMMUNICATION SYSTEM



(57) Abstract

The present invention relates to telecommunication systems. The object of the present invention is to disclose a new type of procedure and system for encrypting the outgoing message traffic between mobile stations consistent with current mobile communication standards and/or between a mobile station and a service provider and for decrypting the incoming message traffic. In addition, the procedure and system of the invention allow encrypted messages to be sent to and received from a closed receiver group in a given area.

FOR THE PURPOSES OF INFORMATION ONLY

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

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

PROCEDURE AND SYSTEM FOR THE PROCESSING OF MESSAGES IN A TELECOMMUNICATION SYSTEM

FIELD OF THE INVENTION

The present invention relates to telecommunication technology. In particular, the invention relates to a procedure and a system for the encryption and decryption of short messages and for sender authentication in a telecommunication system.

BACKGROUND OF THE INVENTION

In telecommunication networks, e.g. GSM networks (GSM, Global System for Mobile communications), heavy encryption of speech transmission is used in the radio link between a mobile station and a base station. Besides voice communication, the use of text messages for communication via mobile stations has increased. With a rise in the service standard, services based on text communication have become common. Text communication can be utilised in various service functions, in paying for services etc. At present, an obstacle to easy encryption of messages is the fact that mobile stations consistent with current mobile communication standards do not permit changes facilitating encryption. The only component that is sufficiently standardised and allows encryption is the subscriber identity module (SIM).

Mobile telephones consistent with a current mobile communication standard, such as the GSM standard, do not directly provide a possibility to use encryption in text communication by mobile stations. Text communication can be used to implement services requiring a high level of data security. However, services requiring a high level of data security cannot become common before sufficient encryption of messages is possible.

Currently known closed user group solutions in mobile communication networks are implemented e.g. on the basis of mobile telephone numbers. In these applications, the message is delivered separately to each person included in a distribution list irrespective of location. A drawback is that there are considerable differences in the message delivery time between the first and last persons on the distribution list.

At present, a problem with message communication in accordance with a mobile communication standard is that it is possible for a third party to read the content of a text message. A further problem is how to encrypt the messages relating to different services so that the receiver can ascertain the identity of the sender. Another problem is encountered in the sending of encrypted messages to a closed receiver group in a given area.

The object of the present invention is to eliminate the above-mentioned drawbacks or at least to significantly alleviate them.

A specific object of the present invention is to disclose a new type of procedure and system for encrypting the outgoing message traffic between mobile stations consistent with a current mobile communication standard and/or between a mobile station and a service provider and for decrypting the incoming message traffic. In addition, the procedure and system of the invention allow encrypted messages to be sent to and received from a closed receiver group in a given area.

As for the features characteristic of the present invention, reference is made to the claims.

BRIEF DESCRIPTION OF THE INVENTION

In the procedure of the invention for encrypting a message and/or authenticating the sender of a message in a telecommunication network in a telecommunication system, the transmission software comprises

the applications and parameters of the encryption algorithm used. The message is e.g. an SMS message (SMS, Short Message Service) consistent with a mobile communication standard.

In the procedure, using a mobile station, messages are generated and sent and received via the message switching centre of the telecommunication system, the applications and parameters needed by the encryption and/or decryption algorithm used are stored on the subscriber identity module. In addition, the message encrypted and/or to be encrypted and/or the message decrypted and/or to be decrypted is/are stored on the subscriber identity module. As an encryption algorithm, it is possible to use e.g. an RSA algorithm or a corresponding algorithm providing a high level of data security, the function of which is obvious to the skilled person. The telecommunication system preferably comprises a telecommunication network, a mobile station connected to it and a subscriber identity module connected to the mobile station, a message switching centre, transmission software connected to the message switching centre and a service provider connected to the transmission software. A preferred example of the mobile communication system is the GSM system.

According to the invention, a given memory location in the subscriber identity module is monitored and encryption of a message and/or decryption of an encrypted message are/is started on the basis of a predetermined string stored in the given memory location. The memory location may be e.g. an ADN memory location (ADN, Abbreviated Dialling Number). Encryption of messages stored in the subscriber identity module is started if e.g. "Name: bank" and "No.: 1235" is stored in the ADN memory location. An encryption algorithm stored on the subscriber identity module performs the encrypting of the message or messages and returns decrypted messages to the SMS memory locations after the mobile station has been restarted. The string used to

activate encryption/decryption can be removed from the subscriber identity module automatically.

In this way, a kind of security feature is achieved. The string activating encryption/decryption will not be accidentally left in the ADN memory location. Messages stored and received on the subscriber identity module can also be automatically encrypted or decrypted.

An encrypted message can also be transmitted only to a closed user group in a predetermined area. Decryption is only possible if the receiver has the encryption key required for the decryption of the message. As a transmission means, it is possible to use e.g. the cell broadcast (CB) feature comprised in the mobile communication standard. When a message is to be sent, an area to which the message is to be delivered is defined. Since the message is transmitted to the receivers using areal mobile communication technology, all users will receive the message simultaneously. If a member of the closed receiver group is absent from the specified area, the information will not be transmitted to that user. The invention is applicable e.g. to the development of a regular customer concept in applications where given information is only to be made available to a desired group.

According to the invention, the user of a mobile station can send a service request in the form of a message. The transmission software gets the required information from the service provider and calls an encryption and/or decryption routine, which encrypts and/or decrypts the message received from the service provider and sends the encrypted and/or decrypted message to the message switching centre and further to the mobile station.

The system of the invention comprises means for monitoring a given memory location in the subscriber identity module and means for starting encryption of a message and/or decryption of an encrypted

message on the basis of a predetermined string stored in the given memory location in the subscriber identity module.

The system preferably comprises means for automatically removing the string activating encryption and/or decryption from the subscriber identity module. Moreover, the system comprises means for transmitting the message only to a closed user group in a given area. The user group preferably has means for decrypting the encrypted message.

According to the invention, the transmission software comprises means for calling an encrypting and/or decrypting routine for the encryption and/or decryption of a message received from a service provider and means for sending an encrypted and/or decrypted message further to the message switching centre and from there further to a mobile station.

The subscriber identity module preferably comprises means for automatically encrypting and decrypting messages stored on the subscriber identity module and received messages.

The invention also relates to a subscriber identity module. It comprises a data processing device, a storage device connected to the data processing device and a data transfer device connected to the data processing device. Moreover, the subscriber identity module is provided with an interface for data transfer between the mobile station and the subscriber identity module. The subscriber identity module comprises means for monitoring a given memory location and means for activating the encryption of a message or decryption of an encrypted message on the basis of a predetermined string stored in the given memory location in the subscriber identity module.

As compared with prior art, the invention has the advantage that it allows digital signature of messages as well as encryption and decryption. Thus it makes it possible to reliably identify the sender of a

message. In addition, the invention makes it possible to reach a plurality of users in a predetermined area simultaneously and without loading the network. Thus, the members of the closed user group only receive relevant information relating to the time and area in question. A further advantage of the invention is that the messages sent between a service provider and a mobile station can be encrypted while at the same time ascertaining the authenticity of the information.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, the invention will be described by way of example with reference to embodiments illustrated in the drawings, wherein

Fig. 1 presents a preferred telecommunication system according to the invention,

Fig. 2 presents a preferred subscriber identity module according to the invention,

Fig. 3 presents a preferred example of the subscriber identity module,

Fig. 4 presents a preferred example of a flow chart representing areal message transmission,

Fig. 5 presents a preferred example of message encryption, and

Fig. 6 presents a block diagram illustrating a preferred example of message encryption between a customer and a content provider.

DETAILED DESCRIPTION OF THE INVENTION

The telecommunication system presented in Fig. 1 comprises a telecommunication network 1 featuring a short message service (SMS) consistent with a mobile communication standard. Other types of message, such as USSD (USSD, Unstructured Service Data), can be used. Furthermore, instead of SMS messages, it is possible to utilise the WAP (WAP, Wireless Application Protocol). The telecommunication network is preferably a GSM net-

work, but other mobile communication networks, such as UMTS (UMTS, Universal Mobile Telecommunication Standard) networks, can also be used. Connected to the mobile communication network 1 is a mobile station 2 with a subscriber identity module SIM connected to it. Also connected to the mobile communication network 1 is a message switching centre 3, which may be e.g. a SM-SC (SM-SC, Short Message Service Centre) in a GSM system. The message switching centre 3 comprises means 9 for transmitting a message exclusively to a closed user group in a predetermined area.

Connected to the message switching centre 3 is transmission software 4, which comprises means 11 for calling an encrypting and/or decrypting routine for the processing of a message received from a service provider 5. Moreover, it comprises means 12 for sending an encrypted and/or decrypted message further to the switching centre 3 and from there to the mobile station 2. Furthermore, the system comprises a service provider 5. The service provider 5 may be e.g. a bank.

A preferred subscriber identity module SIM as presented in Fig. 2 comprises a data processing device 14, a storage device 15 connected to the data processing device 14 and a data transfer device 16, also connected to the data processing device 14. In addition, the subscriber identity module SIM is provided with an interface RP for data transfer between the mobile station 2 and the subscriber identity module SIM.

The subscriber identity module SIM preferably comprises means 6 for monitoring a given memory location in the subscriber identity module SIM and means 7 for activating the encryption of a message and/or decryption of an encrypted message on the basis of a predetermined string stored in the given memory location. In addition, the subscriber identity module comprises means 8 for automatically removing the string used to activate encryption/decryption from the subscriber identity module SIM. Moreover, it comprises means 13

for automatically encrypting and decrypting messages stored and received on the subscriber identity module SIM.

The means 6 -16 presented in Fig. 1 and 2 are implemented in a manner known per se and they will therefore not be described in detail.

Fig. 3 presents a preferred example of the subscriber identity module SIM according to the present invention. The subscriber identity module SIM is connected to a terminal, which in this example is a mobile station ME consistent with the GSM standard. An application in the DFx directory expects that a predetermined string code is stored in a given location in the EFadn file. When this occurs, the EF application program loads the short messages contained in the EFsms file in the DF directory and processes them in the desired manner. Finally, the program returns the processed short messages into the EFsms file. The communication between the mobile station ME and the subscriber identity module SIM is consistent with the GSM standard.

The system presented in Fig. 4 comprises a sender, a sending end application and a network application. In addition, the system comprises a receiving end application and a closed user group. 'Sender' here means a person and/or the apparatus and/or application which sends the messages according to the invention. The message may be e.g. an SMS or USSD message. The sending and receiving end application is a functional entity which contains both the physical apparatus and the associated application software. In this example, the physical apparatus comprises a mobile telephone, a subscriber identity module connected to it and a possible parallel subscriber identity module, e.g. an intelligent card external to the GSM system. The application software is located either in the mobile telephone and/or in the subscriber identity module and/or in the parallel subscriber identity module or in a system com-

municating with these. The application software can be distributed between the various parts of the physical apparatus.

'Areal receiver' means a person and/or apparatus and/or application which receives areal messages according to the invention. To receive the messages, mobile users in the area need a sufficient hardware and software assembly. This assembly consists of a physical apparatus and the associated application software. The principle corresponds to that of the sending end application, but there may be differences in concrete assemblies and functional properties.

The network application is a functional entity which communicates with the sending end application. 'Network application' may refer to service bases containing the physical apparatus and the software. The network application may consist of e.g. a short message service centre or a Cell Broadcast service centre and/or systems and interfaces etc. connected with these. The main functions of the network application include receiving the messages from the sending end application, routing them to the switching centres which manage areal message transmission and sending the messages to the receivers in a given area. In an alternative solution, the transmission of the messages can be implemented using other than wireless technology. The messages can be transferred to the network application using e.g. data networks, such as TCP/IP (TCP, Transmission Control Protocol; IP, Internet Protocol) of X.25.

In the following, the numbering used in Fig. 4 is referred to.

41. The sender enters a message, selects a closed user group as the receiver and indicates that he wants to send the message.

42. The sending end application encrypts the message using its encryption key and sends the message to the network application.

43. The network application transmits the message to the closed user group. The network transmits the message transparently without regard to its content or the encryption used with it.

44. The receiving end applications of the closed user group in the area decrypt the message. The receivers read the message in plain-language form.

Fig. 5 illustrates the procedure used to encrypt a message, e.g. an SMS message. In block 51, the user stores a short message or short messages on the subscriber identity module. In block 52, the user enters in the Name field of a memory location a predetermined string referring to encryption or decryption. In this example, the string is "bank". In the Number field, the user enters "12345". These strings function as the factor which starts encryption or decryption.

In the next block 53, the system checks whether the strings stored in the memory location require encryption or decryption of messages. If not, action is resumed from block 52. If the stored string functions as an activator of encryption or decryption, then the procedure goes on to block 54. In block 54, a check is made to determine whether there are any messages to be encrypted or decrypted on the subscriber identity module. If not, then action is resumed from block 52. If there are messages to be processed on the subscriber identity module, then these are loaded according to block 55. In block 56, the stored message is processed in the desired manner and using the required algorithm. For encryption, e.g. an RSA algorithm or some other corresponding algorithm creating a high level of data security can be used. Finally, according to block 57, the encrypted or decrypted message is returned into an EFsms file as shown in Fig. 1.

Fig. 6 illustrates the progress of a message when a service request in the form of a message is sent from a mobile station to a service provider. A customer sends (61) a request for the transmission of informa-

tion to the mobile station user. The SM-SC transmits (62) the request further to the transmission software. The transmission software converts the request into a form understandable to the service provider and transmits (63) it to the service provider. The service provider sends (64) information it has produced back to the transmission software. The transmission software calls (65) the encryption routine, which encrypts the information by using an agreed private key associated with the service provider and transmits the encrypted message to the SM-SC switching centre using a number associated with the private key as the sending telephone number. The encryption algorithm may be part of the transmission software or it may be located in a separate functional unit, e.g. a server. The SM-SC transmits (68) the message to the mobile user. The message is identified as proceeding from a telephone number recognised as being reliable, messages received from this number being decrypted by using a public key associated with the telephone number in question. The mobile station displays the message in a way that permits the user to ascertain its authenticity, e.g. "Message received from N. Read?". The above example can be applied to two-way communication instead of an one-way implementation as described.

The invention is not restricted to the embodiments illustrated above by means of examples, but instead many variations are possible within the scope of the inventive idea defined in the claims.

CLAIMS

1. Procedure for the encryption of a message and/or authentication of the sender of a message in telecommunication network (1) in a telecommunication system which comprises the telecommunication network (1), a mobile station (2) connected to it and a subscriber identity module (SIM) connected to the mobile station (2), a message switching centre (3) connected to the telecommunication network (1), transmission software (4) connected to the message switching centre and a service provider (5) connected to the transmission software, the transmission software (4) comprising the applications and parameters of the encryption algorithm to be used; and in the procedure messages are generated and sent and received by means of the mobile station (2) via the message switching centre (3) of the telecommunication network (1), the applications and parameters needed by the encryption and/or decryption algorithm to be used are stored on the subscriber identity module (SIM); and in the procedure the message to be processed is stored on the subscriber identity module (SIM), characterised in that

a given memory location in the subscriber identity module is monitored and encryption of a message and/or decryption of an encrypted message are/is started on the basis of a predetermined string stored in the given memory location in the subscriber identity module (SIM).

2. Procedure as defined in claim 1, characterised in that the string activating encryption and/or decryption is removed from the subscriber identity module (SIM) automatically.

3. Procedure as defined in claim 1 and 2, characterised in that a closed user group with a user group-specific decryption key is formed.

4. Procedure as defined in claims 1 - 3, characterised in that the message is only transmitted to a closed user group in a given area.

5. Procedure as defined in claims 1 - 4, characterised in that the transmission software (4) calls an encryption and/or decryption routine, which encrypts and/or decrypts a message received from the service producer (5) and sends the encrypted and/or decrypted message to the message switching centre (3) and further to the mobile station (2).

6. Procedure as defined in claims 1 - 5, characterised in that the message is a short message (SMS, Short Message Service) consistent with a mobile communication standard.

7. Procedure as defined in claims 1 - 6, characterised in that the memory location on the subscriber identity module (SIM) is an ADN memory location.

8. Procedure as defined in claims 1 - 7, characterised in that messages stored and received on the subscriber identity module (SIM) are encrypted and decrypted automatically.

9. Procedure as defined in claims 1 - 8, characterised in that the message is sent to a closed user group using CB (CB, Cell Broadcast).

10. System for the encryption of a message and/or authentication of the sender of a message in a telecommunication network (1) in a telecommunication system which comprises the telecommunication network (1), a mobile station (2) connected to it and a subscriber identity module (SIM) connected to the mobile station (2), a message switching centre (3) connected to the telecommunication network (1), transmission software (4) connected to the message switching centre and a service provider (5) connected to the transmission software, the transmission software (4) comprising the applications and parameters of the encryption algorithm to be used; and in the procedure messages are

generated and sent and received by means of the mobile station (2) via the message switching centre (3) of the telecommunication network (1), the applications and parameters needed for the encryption and/or decryption algorithm to be used are stored on the subscriber identity module (SIM); and in the procedure the message to be processed is stored on the subscriber identity module (SIM), characterised in that the system comprises

means for monitoring a given memory location in the subscriber identity module (SIM); and

means (7) for starting the encryption of a message and/or decryption of an encrypted message on the basis of a predetermined string stored in the given memory location in the subscriber identity module (SIM).

11. System as defined in claim 10, characterised in that the system comprises means (8) for automatically removing the string activating encryption and/or decryption of a message from the subscriber identity module (SIM).

12. System as defined in claim 10 and 11, characterised in that the system comprises means (9) for transmitting a message exclusively to a closed user group in a predetermined area.

13. System as defined in claims 10-12, characterised in that the system comprises user group-specific means (10) for decrypting an encrypted message.

14. System as defined in claims 10 - 13, characterised in that the transmission software (4) comprises means (11) for calling an encrypting and/or decrypting routine for the encryption and/or decryption of a message received from a service provider (5) and means (12) for sending an encrypted and/or decrypted message further to the message switching centre (3) and from there to the mobile station (2).

15. System as defined in claims 10 - 14, characterised in that the system comprises means

(13) for automatic encryption and decryption of messages stored on the subscriber identity module (SIM) and messages received.

16. System as defined in claims 10 - 15, characterised in that the encryption algorithm is an RSA algorithm or some other acceptable encryption algorithm providing a high level of data security.

17. Subscriber identity module (SIM), comprising a data processing device (14), a storage device (15) connected to the data processing device (14) and a data transfer device (16) which is connected to the data processing device (14) and provided with an interface (RP) for the transfer of information between the mobile station (2) and the subscriber identity module (SIM), characterised in that the subscriber identity module (SIM) comprises

means (6) for monitoring a given memory location in the subscriber identity module (SIM); and

means (7) for starting the encryption of a message and/or decryption of an encrypted message on the basis of a predetermined string stored in the given memory location in the subscriber identity module (SIM).

18. Subscriber identity module (SIM) as defined in claim 17, characterised in that the subscriber identity module (SIM) comprises means (8) for automatically removing the string activating message encryption and/or decryption from the subscriber identity module (SIM).

19. Subscriber identity module (SIM) as defined in claims 17 and 18, characterised in that the subscriber identity module (SIM) comprises means (13) for automatic encryption and decryption of messages stored on the subscriber identity module (SIM) and messages received.

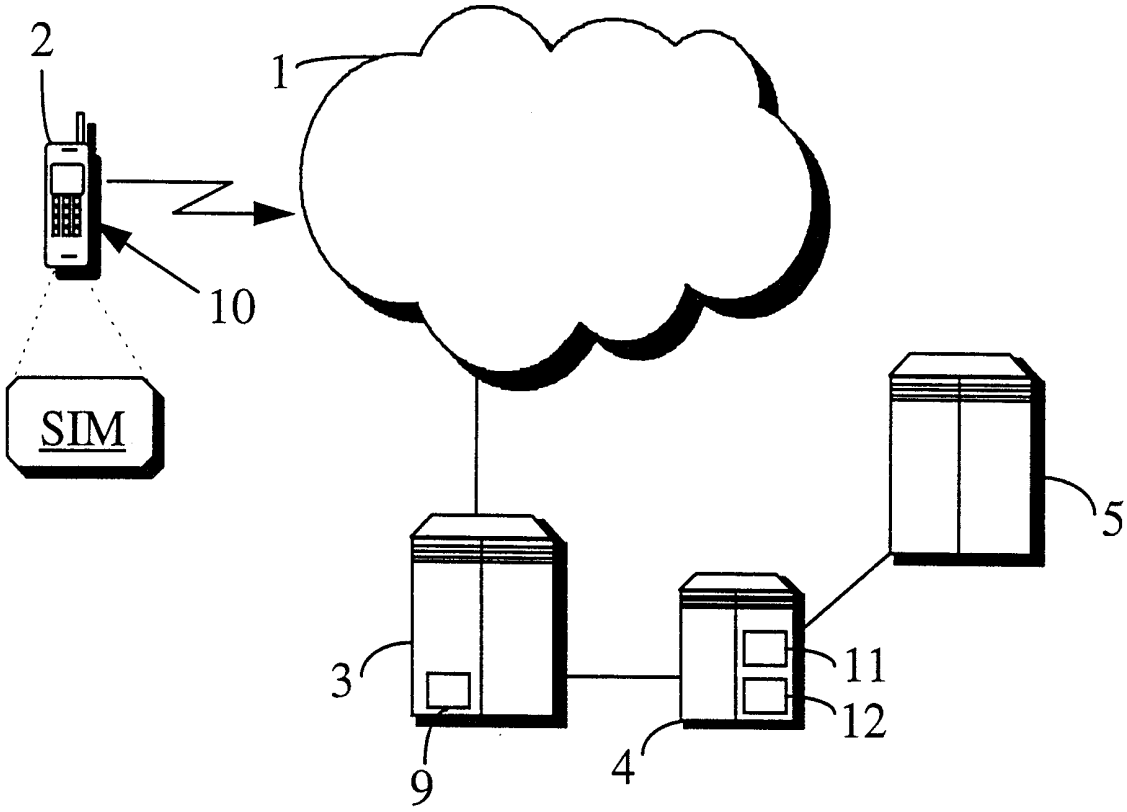


Fig. 1

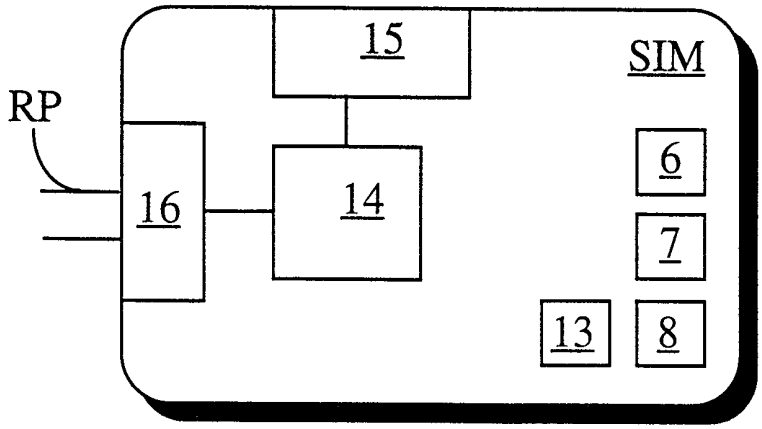


Fig. 2

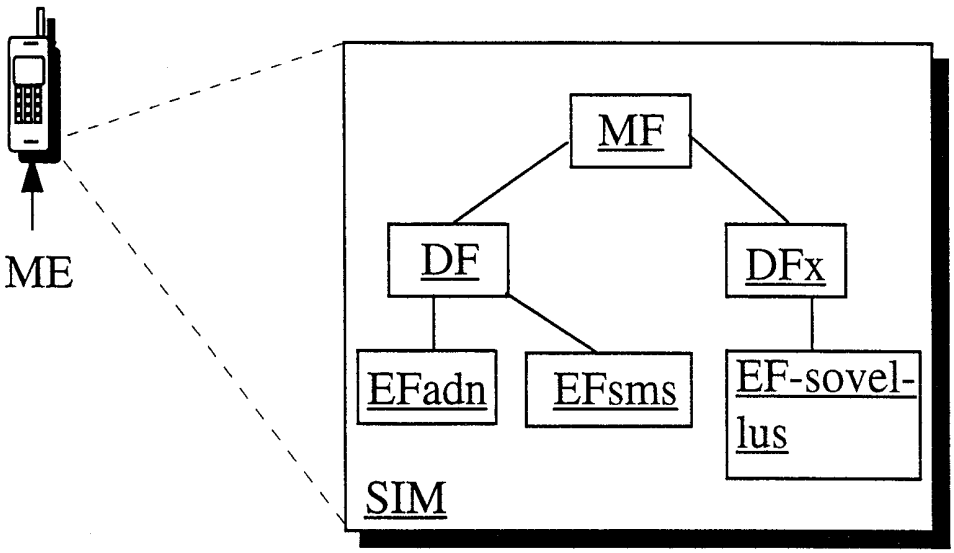

ME
MF
DF
DFx
EFadn
EFsms
EF-sovel-
lus
SIM

Fig. 3

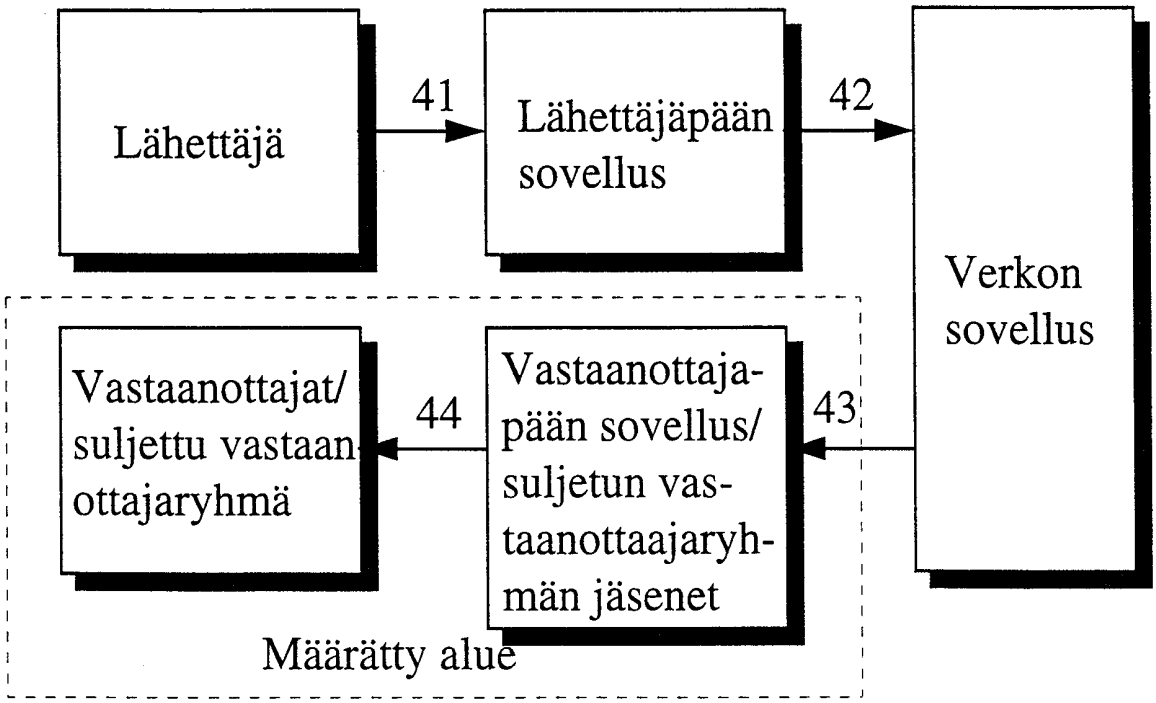

Lähettäjä
41
Lähettäjäpään
sovellus
42
Verkon
sovellus
Vastaanottajat/
suljettu vastaan
ottajaryhmä
44
Vastaanottaja-
pään sovellus/
suljetun vas-
taanottaajaryh-
män jäsenet
43
Määrätty alue

Fig. 4

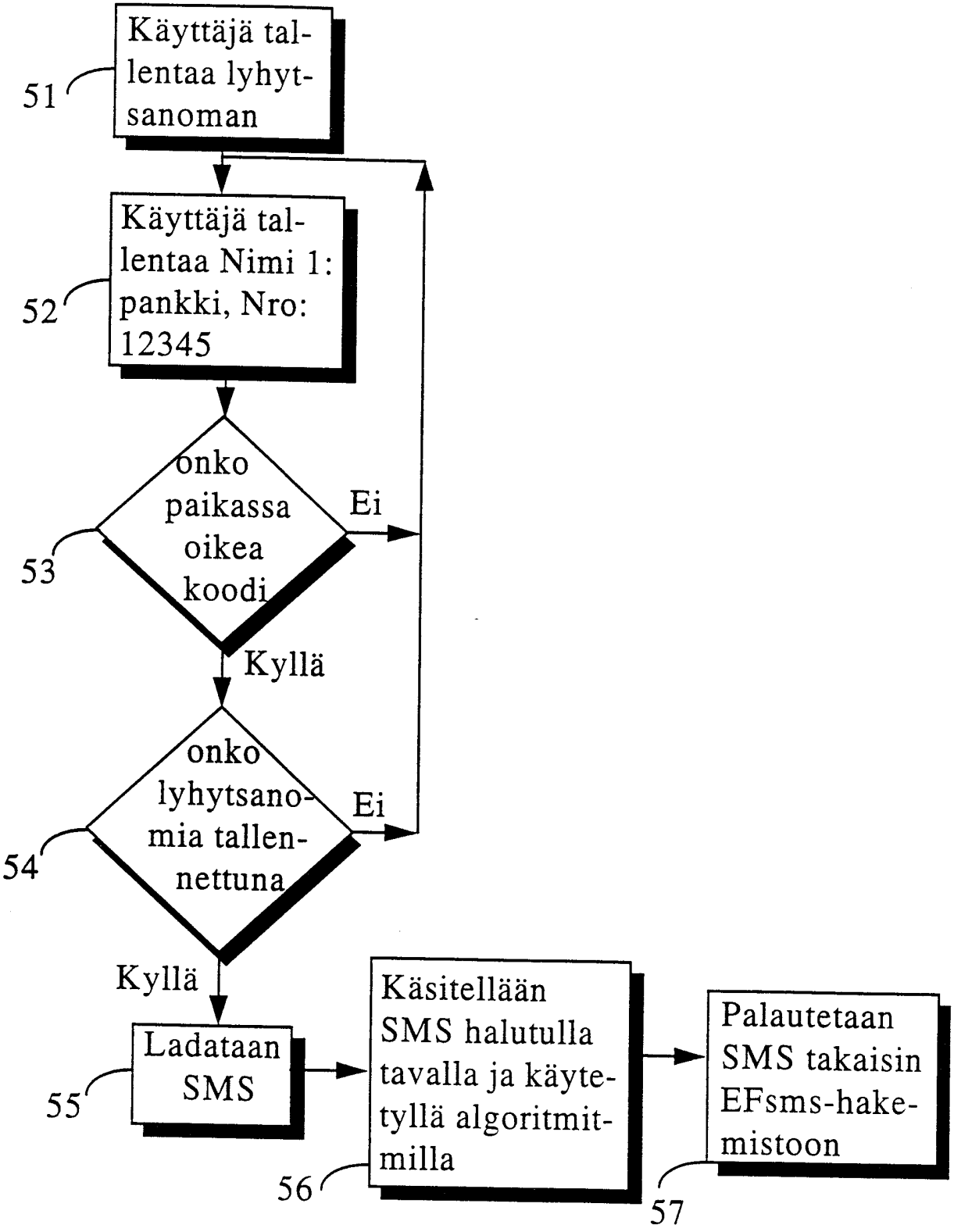

Käyttäjä tallentaa lyhytsanoman
51
Käyttäjä tallentaa Nimi 1: pankki, Nro: 12345
52
onko paikassa oikea koodi
53
Ei
Kyllä
onko lyhytsanomia tallennettuna
54
Ei
Kyllä
Ladataan SMS
55
Käsitellään SMS halutulla tavalla ja käytetyllä algoritmimilla
56
Palautetaan SMS takaisin EFsms-hakemistoon
57

Fig. 5

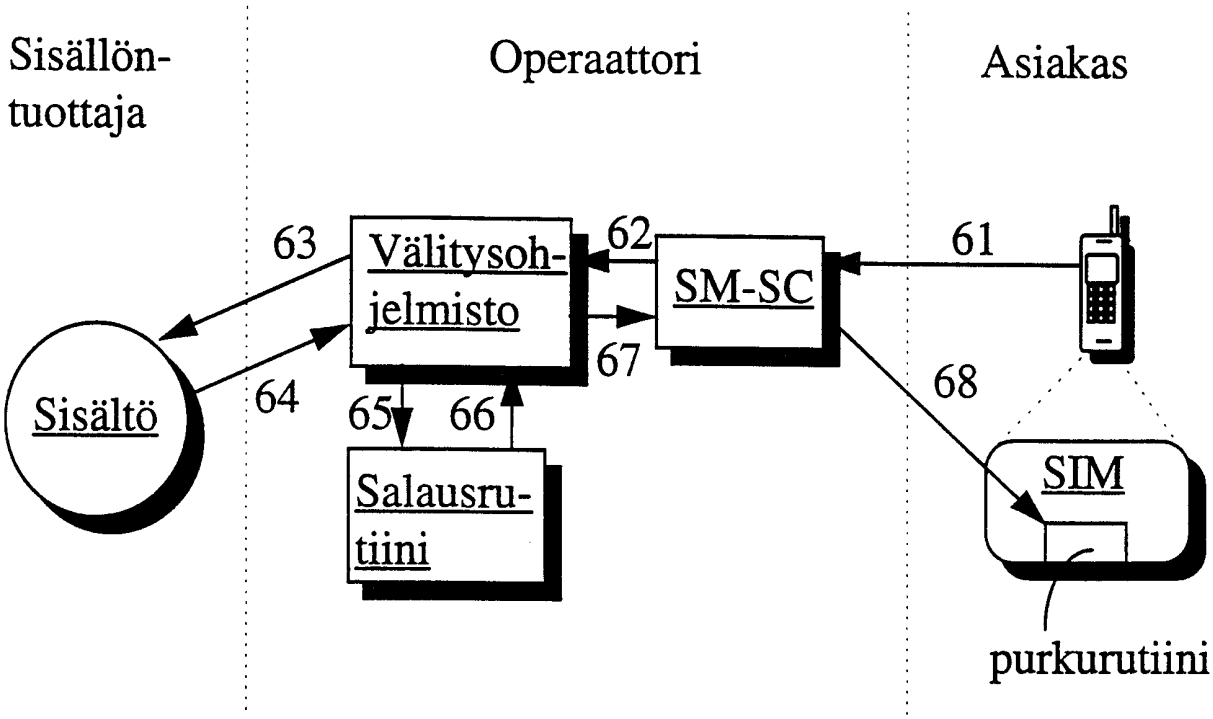

Sisällön-
tuottaja
Operaattori
Asiakas
63
Välitysoh-
jelmisto
62
SM-SC
61
64
67
68
Sisältö
65
66
Salausru-
tiini
SIM
purkurutiini

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 99/00019

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04Q 7/22, H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L, H04B

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

SE,DK,FI,NO classes as above

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

WPI, EPODOC, JAPIO

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5544246 A (RICHARD MANDELBAUM ET AL), 6 August 1996 (06.08.96), column 6, line 21 - column 7, line 34	1-19
A	WO 9501684 A1 (MOTOROLA INC.), 12 January 1995 (12.01.95), page 12, line 14 - line 29	1-19
A	US 5557679 A (TOMAS JULIN ET AL), 17 Sept 1996 (17.09.96), column 2, line 50 - column 3, line 7	1-19
A	US 5301234 A (GERALD MAZZIOTTO), 5 April 1994 (05.04.94), column 2, line 58 - column 3, line 27	1-19

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

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

Date of the actual completion of the international search	Date of mailing of the international search report
28 June 1999	- 01 -07- 1999
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Peter Hedman/MN Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 99/00019

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5590133 A (LARS BILLSTRÖM ET AL), 31 December 1996 (31.12.96), abstract -- --------	9

INTERNATIONAL SEARCH REPORT

Information on patent family members

01/06/99

International application No.
PCT/FI 99/00019

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5544246 A	06/08/96	CA 2131510 A	18/03/95
		EP 0644513 A	22/03/95
		JP 7152837 A	16/06/95
		NO 943457 A	20/03/95
WO 9501684 A1	12/01/95	CA 2141318 A	12/01/95
		EP 0663124 A	19/07/95
		FI 950714 A	17/02/95
		JP 8500950 T	30/01/96
		MX 9404953 A	31/01/95
		US 5455863 A	03/10/95
		US 5689563 A	18/11/97
US 5557679 A	17/09/96	AU 661048 B	13/07/95
		AU 2699092 A	03/05/93
		CA 2115435 A,C	15/04/93
		DE 606408 T	16/03/95
		EP 0606408 A	20/07/94
		FI 940804 A	21/02/94
		JP 6511125 T	08/12/94
		NO 940473 A	16/02/94
		NZ 244523 A	27/02/96
		SE 468068 B,C	26/10/92
		SE 9102835 A,O	26/10/92
		SG 44338 A	19/12/97
		WO 9307697 A	15/04/93
		SE 9200656 D	00/00/00
US 5301234 A	05/04/94	DE 69111553 D,T	18/01/96
		EP 0480833 A,B	15/04/92
		FR 2668002 A,B	17/04/92
		JP 2659637 B	30/09/97
		JP 6021886 A	28/01/94
US 5590133 A	31/12/96	AU 675898 B	20/02/97
		AU 1251595 A	27/06/95
		CA 2153871 A	15/06/95
		CN 1117335 A	21/02/96
		EP 0683963 A	29/11/95
		FI 953775 A	09/08/95
		JP 8506713 T	16/07/96
		SE 9304119 D	00/00/00
		SG 43755 A	14/11/97
		WO 9516330 A	15/06/95