PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04L 9/08, H04Q 7/38

A1

(11) International Publication Number: WO 00/25475

(43) International Publication Date: 4 May 2000 (04.05.00)

(21) International Application Number: PCT/US99/24522

(22) International Filing Date: 19 October 1999 (19.10.99)

(30) Priority Data:
09/178,192 23 October 1998 (23.10.98) US

(71) Applicant: QUALCOMM INCORPORATED [US/US]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(72) Inventor: QUICK, Roy, Franklin, Jr.; 4502 Del Monte Avenue, San Diego, CA 92107 (US).

(74) Agents: OGROD, Gregory, D. et al.; Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, 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, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, 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).

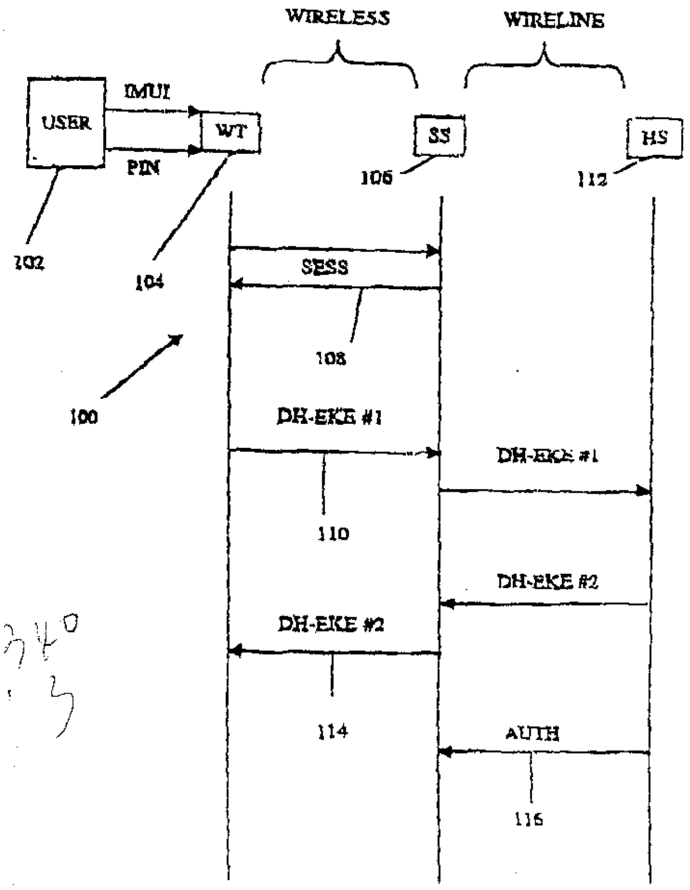
Published

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.

(54) Title: SUBSCRIPTION PORTABILITY FOR WIRELESS SYSTEMS

(57) Abstract

A short Personal Identification Number (PIN) is used to transfer a subscription for wireless service to a new wireless terminal (104), thereby providing enhanced personal mobility to the subscriber. The transfer is rendered secure by the exchange of Diffie-Hellman Encrypted Key Exchange (DH-EKE) messages (110, 114).



445 X 12 = 5340
3

SUBSCRIPTION PORTABILITY FOR WIRELESS SYSTEMS

I. Technical Field

This invention relates to wireless voice and data systems, and has particular relation to allowing a subscriber to move his subscription from one wireless terminal to another. The invention thus provides subscription portability, sometimes also called personal mobility.

II. Background Art

A wireless terminal (portable telephone, laptop computer, etc.) cannot be used as such unless its user has subscribed to a wireless communications service, so that the terminal may use that service to communicate with other terminals, both wireless and wireline. This in turn requires the service provider to register and provision that terminal, that is, to recognize that terminal as being entitled to service and to program the terminal with identification and security information that allows it to access the wireless service.

In the wireless service industry the term "registration" has several meanings. Herein the term "registration" will be used to mean an exchange of the information needed to establish the identity of the user of a terminal and to permit access to wireless services.

This registration may be required in two situations. First, when the terminal is originally purchased, it is not registered to anyone. This situation is referred to as initial provisioning. Second, a subscriber may choose to re-register, that is, to transfer his subscription from one wireless terminal to another. This re-registration might be, for example, from his portable telephone to his laptop computer, or from his regular portable telephone to the portable telephone which he has just rented on a trip to a distant city. This re-registration is referred to as subscription portability.

In early wireless systems such as the analog Advanced Mobile Phone Systems (AMPS), provisioning is performed manually by trained personnel at a terminal distribution site. One of these employees manually registers the terminal with the service provider, typically over the landline telephone. The employee enters information into the terminal through the keypad, using secret information which the service provider has made available to him/her, and storing the subscription information permanently in the terminal. This arrangement is expensive because the seller must have extensively trained employees at every retail outlet. Furthermore, the process is not secure, since the secret information is readily available to these employees.

One alternative means for dealing with both initial provisioning and subscription portability is to provide to the user a separate, removable device known as a user identification module (UIM). The service provider provisions identity and security information into the UIM before distributing it to the user. When the user inserts the UIM into a terminal, the terminal reads the necessary identity information from the UIM and thereby acquires the identity of the user's subscription. This means is popular in the Global System for Mobiles (GSM) system. Registering the terminal after insertion of the UIM is an over-the-air process, and involves a three-way transfer of information between the module, a base station operated by the service provider (which has a unique identification number), and the wireless terminal itself (which has a unique Electronic Serial Number, or ESN).

This first alternative means is still not entirely satisfactory. It requires an electronic interface between the module and the wireless terminal and this interface adds cost to the terminal. Further, the interface is open to contamination when the UIM is removed and inserted, and consequently may become unreliable with repeated use.

A second alternative means deals with the initial provisioning but not with subscription portability. This second means requires that, when the subscriber first buys a new telephone, the user dials a special number to reach a customer service representative who can determine the credit of the user and can then program the necessary subscription information into the terminal using over the air messages.

This second alternative means is an improvement over the UIM means in that it requires no special interface in the terminal. This second means, however, is also not entirely satisfactory, because the service provider must still have highly skilled personnel in the customer service center to operate the over-the-air programming equipment. The expensive nature of the customer service process prohibits the subscriber from re-registering a telephone which a friend has loaned to him for a day or two.

The purpose of this invention is to provide a method for initial provisioning and subscription portability that does not require skilled

2/6

personnel to complete the provisioning and registration process, nor a removable item that the user must physically insert into the terminal.

The procedure described herein requires only that the subscriber enter his/her portable wireless subscription identifier, or user identifier (conventionally, his International Mobile User Identifier, or IMUI) and a password (conventionally, his Personal Identification Number, or PIN) into a wireless terminal. The password may be entered into the terminal in any convenient manner, such as keying a number into a keypad, speaking a phrase (with suitable voice recognition technology) into the microphone, or any other convenient manner. The wireless terminal is then able to contact the service provider using over-the-air signals, obtain necessary subscription information, and automatically reprogram itself – and reprogram the service provider – so that the service provider thereafter recognizes this wireless terminal as being registered to this subscriber. The password must be fairly short – typically four to six digits, as in bank card PINs – because the average subscriber cannot memorize a security code that is sufficiently long (twenty digits or more) to impede a brute-force attack.

It is evident that the password must be protected from compromise during the registration process, otherwise the subscription information would be subject to cloning by fraudulent users who obtain the user identifier and password. Recent advances in cryptography, such as the work of Bellovin and Merritt, cited below, provide techniques for securely verifying that the terminal and wireless network both know the correct password without revealing the password. These techniques also provide means for establishing encryption keys that can be used in the encryption of subscription information exchanged subsequent to the initial password confirmation. The existence of these techniques makes it possible to support registration for initial provisioning and subscription portability without need for removable UIMs nor for customer service intervention.

BRIEF DISCLOSURE OF THE INVENTION

Applicant has developed a subscription which is truly portable from one wireless terminal to another, and which uses passwords which are both short and secure.

Whenever a subscriber wishes to register a terminal to his subscription, he enters his user identifier (conventionally, his International Mobile User Identifier, or IMUI) and his password (conventionally, his

Personal Identification Number, or PIN) into the terminal. The terminal generates a public/private key pair and stores it. This key pair is preferably a Diffie-Hellman (D-H) key pair. It optionally concatenates the public key with a random number, and encrypts the (optionally concatenated) number with the password. Any convenient Secure Key Exchange (SKE) method may be used. Several suitable SKE methods are described in Thomas Wu, "The Secure Remote Password Protocol," *Proc. 1998 Internet Society Network and Distributed System Security Symposium*, San Diego, CA, March 1998, pp. 97-111, http://jafar.stanford.edu/srp/ndss.html, and in David P. Jablon, "Strong Password-Only Authenticated Key Exchange," of Integrity Sciences, Inc., of Westboro, Massachusetts, USA, March 2, 1997, http://world.std.com/~dpj/speke97.html, the disclosures of which are incorporated herein by reference. The Diffie-Hellman Encrypted Key Exchange (DH-EKE) method of Bellovin and Merritt is particularly suitable, and the remaining description of the present invention is made with reference to DH-EKE. See Steven M. Bellovin and Michael Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks," in *Proc. IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 72-84, May 1992, the disclosure of which is incorporated herein by reference. Either elliptic curve or exponential groups can be used with this method. The resulting encrypted message is called the DH-EKE message.

The terminal then makes wireless contact with a local serving system and requests registration. This serving system may be the subscriber's home system, but often it is not. In any event, the terminal and the home system must be assured of each other's identities, whether there is no intermediate serving system, one system, or even several. The remainder of this description assumes one intermediate system, but is readily modified to handle none or several. That is, the terminal and the home system will always be the source and destination (or vice versa) of messages, regardless of how many intermediate systems (if any) they have to pass through.

The terminal tells the serving system what the subscriber's home system is, by stating either the full user identifier or enough of the user identifier as is necessary to identify the home system. It also states the DH-EKE message. Preferably, the serving system first provides its D-H public key to the terminal, so that the specifics of who is requesting registration are not sent in the clear. Also preferably, the serving system opens a channel with the terminal to facilitate the registration process.

The serving system sends the DH-EKE message to the home system, which decrypts it with the password. The password is known only to the home system and the subscriber. The home system thereby recovers the subscriber's public key. The home system generates its own D-H public/private key pair and stores it. It then concatenates the newly generated public key with a random number, encrypts the concatenated number with the password using DH-EKE, and transmits this newly generated DH-EKE message back to the terminal. The terminal decrypts it with the password and recovers the home-system public key.

The terminal and the home system are now each in possession of its own private key and the other's public key, both of which are far larger than the password. Each is thus able to generate a common session key using conventional methods. Each is further able to securely use the session key to download a virtual User Identification Module (VUIM) into the terminal, that is, to provide to the terminal, over the air, some or all of the information which otherwise would be obtained from a physical UIM (PUIM) being inserted into the terminal.

Registration may now continue in the conventional fashion, as though a PUIM had been used. Alternatively, registration may be included within the downloading process. This is possible since a terminal with a VUIM already has something which a terminal with a PUIM does not acquire until later, namely, a communications link to (and a shared secret session key with) the home system.

A strength of this method is that the public keys are temporary, and can be replaced on each subsequent registration. Further, each public key is essentially a random number, providing no indication whether an attempted decryption was or was not successful. An off-line dictionary attack therefore fails. The only thing that a dictionary attacker recovers is a collection of possible public keys, none of which has anything to distinguish it from any of the others. There is thus nothing to distinguish a correct guess of the password from an incorrect guess. The follow-on on-line attack must therefore still use the entire dictionary of passwords, and will therefore fail.

This strength may also be viewed as the password being used as a private key in a key exchange procedure, rather than as an encryption key *per se*. It is for this reason that the process is called *Secure* Key Exchange rather than *Encrypted* Key Exchange. It is not necessary that the terminal and home system exchange passwords nor session keys in encrypted form. What is important is that the home system be assured that the terminal knows the password and has the common session key. It is also important that the password not be discoverable by eavesdroppers while the terminal is demonstrating its identity to the home system. If the password is not included in the message, even in encrypted form, then it is more difficult to be compromised.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows an exchange of DH-EKE messages.

FIG. 2 shows an authentication procedure.

DETAILED DESCRIPTION

FIG. 1 shows an exchange 100 of DH-EKE messages. The user 102 enters the user identifier and password into the wireless terminal 104. The terminal 104 generates a pair of Diffie-Hellman (D-H) private and public keys, and stores them. Optionally, the terminal 104 and the base station of the serving system 106 carry out a separate procedure to establish a local session encryption key SESS 108 to protect the user identifier from interception. The terminal 104 uses the password to encrypt the D-H public key, optionally concatenated with a random number before encryption, then transmits the user identifier (optionally encrypted under the local session key) and the encrypted public key, that is, a first DH-EKE message 110, to the base station of the serving system 106 in a registration request. This request should result in a dedicated channel assignment in order to complete the download procedure efficiently.

The serving system 106 contacts the home system 112 requesting a subscription registration. The home system 112 decrypts the wireless terminal's public key using the password in the subscription record. The home system then creates a private and public D-H key, from which a tentative session key is obtained using the terminal's public key and the home system's private key. The home system then encrypts its own public key, optionally concatenating a random number before encryption, using the password stored in the subscription record and returns it in the form of a second DH-EKE message 114 to the wireless terminal 104 via the serving system 106. The wireless terminal 104 decrypts the home system's public key and creates (hopefully) the same tentative session key, using the home system's public key and its own private key.

FIG. 2 shows an authentication procedure 200 which must follow the DH-EKE exchange. The wireless terminal 104 and home system 112 carry out this procedure to prove that each have the same key. This authentication could be either unilateral (for example, only allowing the home system 112 to authenticate the wireless terminal 104) or bilateral. The bilateral technique has three steps. First, the wireless terminal 104 encrypts a random number C_W and sends the encrypted number $E(C_W)$ 202 to the home system 112. Second, the home system 112 generates its own random number C_H, encrypts (C_W, C_H) and sends the encrypted number $E(C_W, C_H)$ 204 to the wireless terminal 104. Third, the wireless terminal 104 encrypts C_H and sends the encrypted number $E(C_H)$ 206 to the home system 112. A unilateral procedure could, for example, omit the first step, and replace C_W in the second step by a second random number.

The public keys were encrypted by the password, and the authentication consists of three different things being sent in an interlocked manner. Therefore, a man-in-the-middle attacker cannot cause a false acceptance of keys, and cannot know the mutual key without breaking the discrete logarithm or elliptic-curve group. Such breakage is currently considered infeasible if the group size is sufficiently large.

If the home system 112 verifies the session key of the wireless terminal 104, it will transfer the subscription information – that is, all or part of a virtual UIM (VUIM) -- to the serving system 106, in both encrypted form for over-the-air transmission and in unencrypted form for use by the serving system. The session key – or, at least, a first portion of it – can also serve as an authentication key AUTH 116 for subsequent authentications of the terminal 104 in the serving system 106. This has advantages over the current cellular authentication procedures in that the authentication key is created at each registration, and therefore will change randomly from registration to registration. Typically the D-H exchange produces 512 bits of output, which is more than are needed for authentication. As a result, the remainder of the session key, that is, a second portion of it, can serve as a conventional encryption key for subsequent control signal transmissions.

The serving system 106 downloads the encrypted subscription data – the VUIM – to the terminal and makes a registration entry in the Visitor Location Register (VLR). The user is now ready to make calls.

For subsequent system accesses, the user can be assigned a Temporary Mobile User Identifier (TMUI) as described in existing cellular standards. The generation of per-call encryption keys can be carried out using the authentication key using procedures described in existing cellular standards.

In other words, the airlink security procedures in existing cellular standards can be used without modification after the generation of the authentication key using the methods described here.

Industrial Application

My invention is capable of exploitation in industry, and can be made and used, whenever is it desired to register a wireless subscription in a new wireless terminal. The individual components of the apparatus and method shown herein, taken separate and apart from one another, may be entirely conventional, it being their combination which I claim as my invention.

While I have described various modes of apparatus and method, the true spirit and scope of my invention are not limited thereto, but are limited only by the following claims and their equivalents, and I claim such as my invention.

CLAIMS

1) A method for registering a wireless subscription to a wireless terminal, the method comprising the steps of:

a) entering a user identifier) and a password) into the wireless terminal;

b) at the wireless terminal:

i) generating a public/private key pair;

ii) using the password to encrypt the wireless terminal's public key according to a secure key exchange (SKE) protocol, thereby forming a first SKE message; and

iii) transmitting the user identifier and the first SKE message to a home system;

c) at the home system:

i) generating a public/private key pair;

ii) using the user identifier to determine the password;

iii) using the password to encrypt the home system's public key according to an SKE protocol, thereby forming a second SKE message;

iv) transmitting the second SKE message to the wireless terminal;

v) using the password to decrypt the wireless terminal's public key; and

vi) using the home system's private key and the wireless terminal's public key to form a session key;

d) at the wireless terminal:

i) using the password to decrypt the home system's public key; and

ii) using the wireless terminal's private key and the home system's public key to form the session key; and

e) at both the wireless terminal and at the home system, using the session key todownload all or part of a Virtual User Identification Module (VUIM) from the home system to the wireless terminal.

2) The method of Claim 1, further comprising the step of encrypting the user identifier before transmitting it.

3) The method of Claim 1, further comprising the step of opening a communications channel before transmitting the second SKE message to the wireless terminal.

4) The method of Claim 1, wherein the steps of transmitting the SKE messages from a source to a destination further comprise the steps of:

a) transmitting the SKE messages from the source to an intermediate serving system; and

b) transmitting the SKE messages from the intermediate serving system to the destination.

5) The method of Claim 4, further comprising the steps of:

a) using a first portion of the session key as an authentication key in subsequent authentications of the wireless terminal in the intermediate serving system; and

b) using a second portion of the session key as an encryption key in subsequent control signal transmissions.

6) The method of Claim 1, wherein:

a) the public/private key pairs comprise Diffie-Hellman public/private key pairs; and

b) the SKE messages comprise Diffie-Hellman Encrypted Key Exchange (DH-EKE) messages.

7) The method of claim 1, wherein:

a) the step of using the password to encrypt the wireless terminal's public key comprises the steps of:

i) first concatenating the wireless terminal's public key with a first random number, thereby forming a first concatenated number; and

ii) using the password to encrypt the first concatenated number; and

b) the step of using the password to encrypt the home system's public key comprises the steps of:

i) first concatenating the home system's public key with a second random number, thereby forming a second concatenated number; and

ii) using the password to encrypt the second concatenated number.

8) Apparatus for registering a wireless subscription to a wireless terminal, the apparatus comprising:

a) means for entering a user identifier and a password into the wireless terminal;

b) at the wireless terminal:

i) means for generating a public/private key pair;

ii) means for using the password to encrypt the wireless terminal's public key according to a secure key exchange (SKE) protocol, thereby forming a first SKE message; and

iii) means for transmitting the user identifier and the first SKE message to a home system;

c) at the home system:

i) means for generating a public/private key pair;

ii) means for using the user identifier to determine the password;

iii) means for using the password to encrypt the home system's public key according to an SKE protocol, thereby forming a second SKE message;

iv) means for transmitting the second SKE message to the wireless terminal;

v) means for using the password to decrypt the wireless terminal's public key; and

vi) means for using the home system's private key and the wireless terminal's public key to form a session key;

d) at the wireless terminal:

i) means for using the password to decrypt the home system's public key; and

ii) means for using the wireless terminal's private key and the home system's public key to form the session key; and

e) at both the wireless terminal and at the home system, means for using the session key to download all or part of a Virtual User Identification Module (VUIM) from the home system to the wireless terminal.

9) The apparatus of Claim 8, further comprising means for encrypting the user identifier before transmitting it.

10) The apparatus of Claim 8, further comprising means for opening a communications channel before transmitting the second SKE message to the wireless terminal.

11) The apparatus of Claim 8, wherein the means for transmitting the SKE messages from a source to a destination further comprises:

a) means for transmitting the SKE messages from the source to an intermediate serving system; and

b) means for transmitting the SKE messages from the intermediate serving system to the destination.

12) The apparatus of Claim 11, further comprising:

a) means for using a first portion of the session key as an authentication key in subsequent authentications of the wireless terminal in the intermediate serving system; and

b) means for using a second portion of the session key as an encryption key in subsequent control signal transmissions.

13) The apparatus of Claim 8, wherein:

a) the public/private key pairs comprise Diffie-Hellman public/private key pairs; and

b) the SKE messages comprise Diffie-Hellman Encrypted Key Exchange (DH-EKE) messages.

14) The apparatus of claim 8, wherein:

a) the means for using the password to encrypt the wireless terminal's public key comprises:

i) means for first concatenating the wireless terminal's public key with a first random number, thereby forming a first concatenated number; and

ii) means for using the password to encrypt the first concatenated number; and

b) the means for using the password to encrypt the home system's public key comprises:

i) means for first concatenating the home system's public key with a second random number, thereby forming a second concatenated number; and

ii) means for using the password to encrypt the second concatenated number.

15) A wireless terminal constructed to:

a) receive a user identifier and a password into the wireless terminal;

b) generate a public/private key pair;

c) use the password to encrypt the wireless terminal's public key according to a secure key exchange (SKE) protocol, thereby forming an SKE message;

d) transmit the user identifier and the SKE message to a home system;

e) receive an encrypted public key from the home system;

f) use the password to decrypt the encrypted public key from the home system;

g) use the wireless terminal's private key and the home system's public key to form the session key; and

h) use the session key to download all or part of a Virtual User Identification Module (VUIM) from the home system to the wireless terminal.

16) The terminal of Claim 15, further comprising means for encrypting the user identifier before transmitting it.

17) The terminal of Claim 15, further comprising means for opening a communications channel before transmitting the user identifier and the SKE message.

18) The terminal of Claim 15, wherein a portion of the terminal constructed to transmit the SKE messages from a source to a destination further comprises:

a) means for transmitting the SKE messages from the source to an intermediate serving system; and

b) means for transmitting the SKE messages from the intermediate serving system to the destination.

19) The terminal of Claim 18, wherein a portion of the terminal constructed to encrypt the terminal's public key comprises:

a) means for using a first portion of the session key as an authentication key in subsequent authentications of the wireless terminal in the intermediate serving system; and

b) means for using a second portion of the session key as an encryption key in subsequent control signal transmissions.

20) The terminal of Claim 15, wherein:

a) the public/private key pairs comprise Diffie-Hellman public/private key pairs; and

b) the SKE messages comprise Diffie-Hellman Encrypted Key Exchange (DH-EKE) messages.

21) The terminal of claim 15, wherein:

a) a portion of the terminal constructed to use the password to encrypt the wireless terminal's public key comprises:

i) means for first concatenating the wireless terminal's public key with a first random number, thereby forming a first concatenated number; and

ii) means for using the password to encrypt the first concatenated number; and

b) a portion of the terminal constructed to use the password to encrypt the home system's public key comprises:

i) means for first concatenating the home system's public key with a second random number, thereby forming a second concatenated number; and

ii) means for using the password to encrypt the second concatenated number.

22) A home system constructed to:

a) generate a public/private key pair;

b) receive a user identifier and an encrypted public key from a wireless terminal;

c) use the user identifier to determine password;

d) use the password to encrypt the home system's public key according to a secure key exchange (SKE) protocol, thereby forming a SKE message;

e) transmit the SKE message;

f) use the password to decrypt the wireless terminal's public key;

g) use the home system's private key and the wireless terminal's public key to form a session key; and

h) use the session key to download all or part of a Virtual User Identification Module (VUIM) from the home system to the wireless terminal.

23) The system of Claim 22, further comprising means for opening a communications channel before receiving the user identifier.

24) The system of Claim 22, wherein a portion of the system constructed to transmit the SKE messages from a source to a destination further comprises:

a) means for transmitting the SKE messages from the source to an intermediate serving system; and

b) means for transmitting the SKE messages from the intermediate serving system to the destination.

25) The system of Claim 24, further comprising:

a) means for using a first portion of the session key as an authentication key in subsequent authentications of the wireless terminal in the intermediate serving system; and

b) means for using a second portion of the session key as an encryption key in subsequent control signal transmissions.

26) The system of Claim 22, wherein:

a) the public/private key pairs comprise Diffie-Hellman public/private key pairs; and

b) the SKE messages comprise Diffie-Hellman Encrypted Key Exchange (DH-EKE) messages.

27) The system of claim 22, wherein:

a) a portion of the terminal constructed to use the password to encrypt the wireless terminal's public key comprises:

i) means for first concatenating the wireless terminal's public key with a first random number, thereby forming a first concatenated number; and

ii) means for using the password to encrypt the first concatenated number; and

b) a portion of the terminal constructed to use the password to encrypt the home system's public key comprises:

i) means for first concatenating the home system's public key with a second random number, thereby forming a second concatenated number; and

ii) means for using the password to encrypt the second concatenated number.

6

FIG. 1

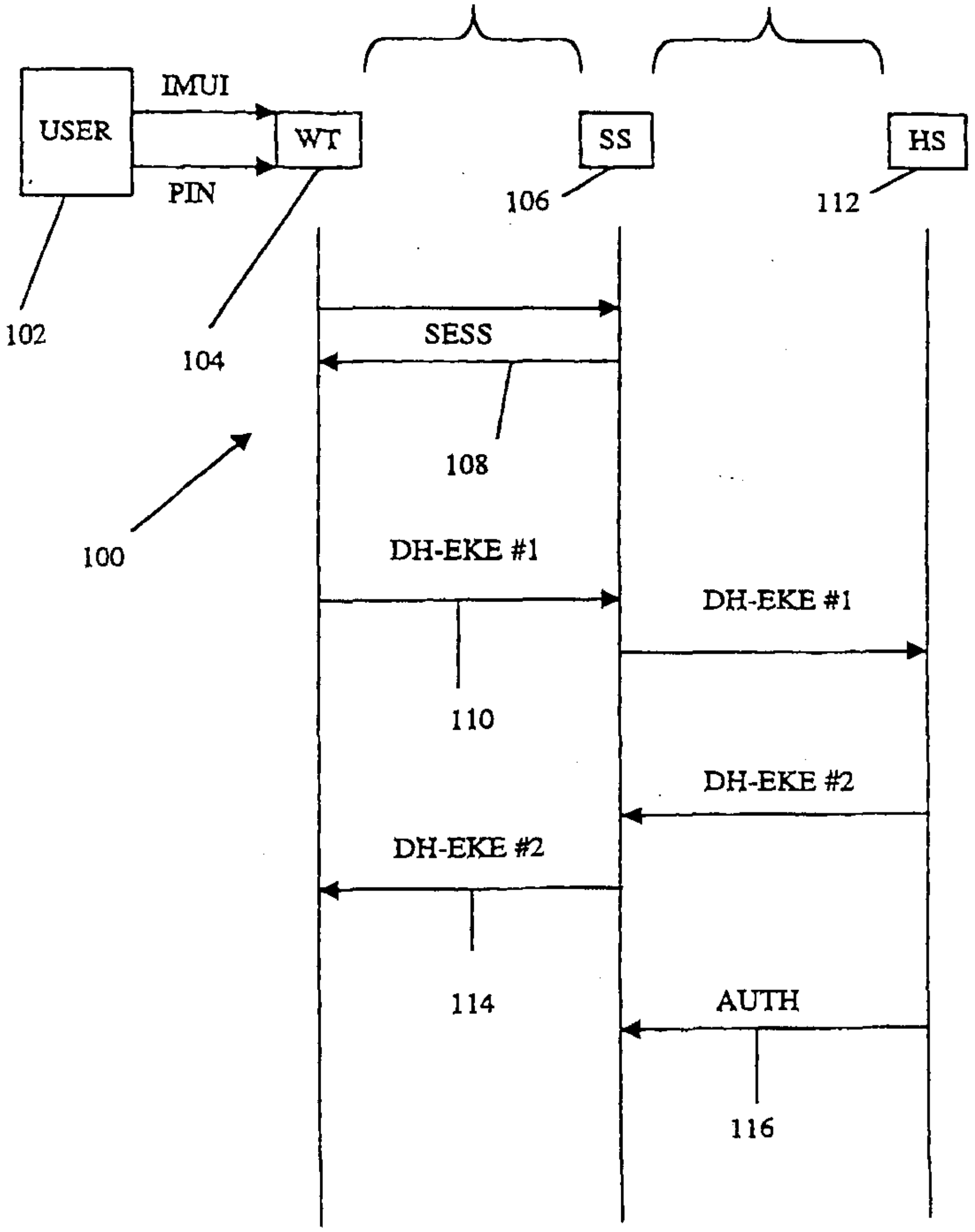
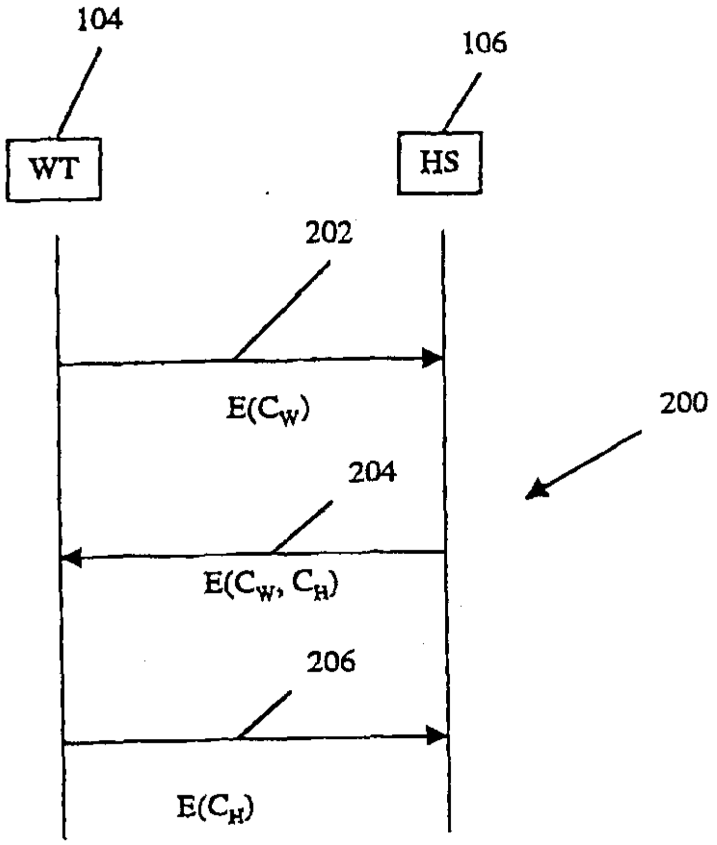

WIRELESS
WIRELINE
USER
IMUI
PIN
WT
SS
HS
102
104
106
112
SESS
108
100
DH-EKE #1
110
DH-EKE #1
DH-EKE #2
DH-EKE #2
114
AUTH
116

FIG. 2



INTERNATIONAL SEARCH REPORT

onal Application No
PCT/US 99/24522

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04Q7/38

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)
IPC 7 H04Q H04L

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 535 863 A (AMERICAN TELEPHONE & TELEGRAPH) 7 April 1993 (1993-04-07) page 3, line 44 - line 56 page 4, line 43 -page 5, line 6 page 9, line 11 - line 23 page 11, line 18 -page 12, line 10 figures 1,5,6 ---	1-3,6, 8-10,13, 15-17, 20,22, 23,26

-/--

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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" earlier 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 21 February 2000	Date of mailing of the international search report 01/03/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Barel, C

1

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/24522

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 562 890 A (HUTCHISON MICROTEL LIMITED) 29 September 1993 (1993-09-29) column 1, line 9 - line 56 column 3, line 22 -column 4, line 29 figure 1 ---	1-3,6, 8-10,13, 15-17, 20,22, 23,26
A	EP 0 651 533 A (SUN MICROSYSTEMS INC) 3 May 1995 (1995-05-03) page 5, line 22 - line 49 page 6, line 39 -page 7, line 28 claim 1 figures 4A,4B,4C ---	1-27
A	TAYLOR A: "OVER-THE-AIR SERVICE PROVISIONING" ANNUAL REVIEW OF COMMUNICATIONS, 1 January 1998 (1998-01-01), XP000793196 -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 99/24522

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0535863 A	07-04-1993	US 5241599 A	31-08-1993
		AU 648433 B	21-04-1994
		AU 2351392 A	08-04-1993
		CA 2076252 A,C	03-04-1993
		JP 2599871 B	16-04-1997
		JP 6169306 A	14-06-1994
		NO 923740 A	05-04-1993
EP 0562890 A	29-09-1993	NONE	
EP 0651533 A	03-05-1995	US 5371794 A	06-12-1994
		JP 7193569 A	28-07-1995

[19]中华人民共和国国家知识产权局

[51]Int. Cl⁷

H04L 9/08
H04Q 7/38

[12]发明专利申请公开说明书

[21]申请号 99815025.8

[43]公开日 2002年1月16日

[11]公开号 CN 1331874A

[22]申请日 1999.10.19 [21]申请号 99815025.8

[30]优先权

[32]1998.10.23 [33]US [31]09/178,192

[86]国际申请 PCT/US99/24522 1999.10.19

[87]国际公布 WO00/25475 英 2000.5.4

[85]进入国家阶段日期 2001.6.22

[71]申请人 高通股份有限公司

地址 美国加利福尼亚州

[72]发明人 小R·F·奎克

[74]专利代理机构 上海专利商标事务所

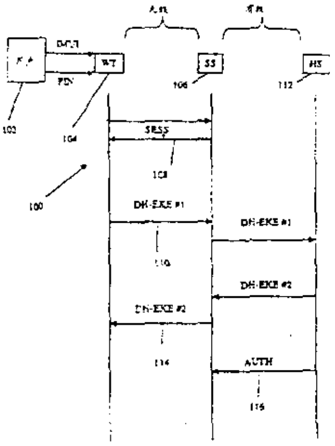
代理人 吴蓉军

权利要求书6页 说明书6页 附图页数2页

[54]发明名称 对于无线系统的预订可移植性

[57]摘要

用短个人标识号(PIN)将无线服务的预订转移到新的无线终端(104),从而 向用户提供增强的个人可移动性。通过交换 Diffie－Hellman 加密密钥交换(DH－EKE)消息(110,114)使得这种转移很安全。



ISSN 1008-4274

知识产权出版社出版

权 利 要 求 书

1 一种向无线终端登记无线预订的方法，其特征在于，所述方法包括下列步骤：

a) 将用户标识符)和密码)输入到无线终端；

b) 在无线终端处：

i) 产生公/私钥对；

ii) 运用密钥根据安全密码交换(SKE)协议加密无线终端的公钥，从而形成第一 SKE 消息；和

iii) 发送所述用户标识符和所述第一 SKE 消息到归属系统；

c) 在所述归属系统处：

i) 产生公/私钥对；

ii) 用用户标识符确定密码；

iii) 根据 SKE 协议，用密码加密归属系统的公钥，从而形成第二 SKE 消息；

iv) 把所述第二 SKE 消息发送到所述无线终端；

v) 用所述密码解密所述无线终端的公钥；和

vi) 用所述归属系统的私钥和所述无线终端的公钥形成对话密钥；

d) 在所述无线终端处：

i) 用所述密码解密所述归属系统的公钥；和

ii) 用所述无线终端的私钥和所述归属系统的公钥形成会话密钥；和

e) 在所述无线终端和所述归属系统中，用所述对话密钥将所有或部分虚拟用户标识模块(VUIM)从归属系统下载到无线终端。

2 如权利要求 1 所述的方法，其特征在于，还包括在发送之前加密所述用户标识符的步骤。

3. 如权利要求 1 所述的方法，其特征在于，还包括在发送所述第二 SKE 消息到所述无线终端之前开放通信信道的步骤。

4. 如权利要求 1 所述的方法，其特征在于，把 SKE 消息从源发送到目的地的步骤还包括下列步骤：

a) 把 SKE 消息从源发送到中间服务系统；和

b) 把 SKE 消息从中间服务系统发送到目的地。

5. 如权利要求4所述的方法，其特征在于，还包括下列步骤：

a) 在所述中间服务系统中随后鉴定无线终端的过程中，将第一部分对话密钥用作鉴定密钥；和

b) 在随后的控制信号传输过程中将第二部分对话密码用作加密密钥。

6. 如权利要求1所述的方法，其特征在于：

a) 所述公/私钥对包括Diffie-Hellman公/私钥对；和

b) SKE消息包括Diffie-Hellman加密密钥交换(DH-EKE)消息。

7. 如权利要求1所述的方法，其特征在于：

a) 用密码加密无线终端的公钥的步骤包括下列步骤：

i)将无线终端的公钥与第一随机号第一链接，从而形成第一链接号码；和

ii) 用密码加密所述第一链接号码；和

b) 用密码加密归属系统的公钥的步骤包括下列步骤：

i) 将归属系统的公钥与第二随机号第一链接，从而形成第二链接号码；和

ii) 用密码加密所述第二链接号码。

8. 一种向无线终端登记无线预订的装置，其特征在于，所述装置包括：

a) 将用户标识符和密码输入到无线终端的装置；

b) 在无线终端处：

i) 产生公/私钥对的装置；

ii) 运用密钥根据安全密码交换(SKE)协议加密无线终端的公钥，从而形成第一SKE消息的装置；和

iii) 发送所述用户标识符和所述第一SKE消息到归属系统的装置；

c) 在所述归属系统处：

i) 产生公/私钥对的装置；

ii) 用用户标识符确定密码的装置；

iii) 根据SKE协议，用密码加密归属系统的公钥，从而形成第二SKE消息的装置；

iv) 把所述第二SKE消息发送到所述无线终端的装置；

v) 用所述密码解密所述无线终端的公钥的装置；和

vi) 用所述归属系统的私钥和所述无线终端的公钥形成对话密钥的装

置；

d) 在所述无线终端处：

i) 用所述密码解密所述归属系统的公钥的装置；和

ii) 用所述无线终端的私钥和所述归属系统的公钥形成会话密钥的装置；和

e) 在所述无线终端和所述归属系统中，用所述对话密钥将所有或部分虚拟用户标识模块(VUIM)从归属系统下载到无线终端的装置。

9. 如权利要求8所述的装置，其特征在于，还包括在发送它之前加密用户标识符。

10. 如权利要求8所述的装置，其特征在于，还包括在将第二SKE消息发送到无线终端之前开放通信信道的装置。

11. 如权利要求8所述的装置，其特征在于，将SKE消息从源发送到目的地的装置还包括：

a) 将SKE消息从源发送到中间服务系统的装置；和

b) 将SKE消息从中间服务系统发送到目的地的装置。

12. 如权利要求11所述的装置，其特征在于，还包括：

a) 在所述中间服务系统中随后鉴定无线终端的过程中，将第一部分对话密钥用作鉴定密钥的装置；和

b) 在随后的控制信号传输过程中将第二部分对话密码用作加密密钥的装置。

13. 如权利要求8所述的装置，其特征在于：

a) 所述公/私钥对包括Diffie-Hellman公/私钥对；和

b) SKE消息包括Diffie-Hellman加密密钥交换(DH-EKE)消息。

14. 如权利要求8所述的装置，其特征在于：

a) 用密码加密无线终端的公钥的装置包括：

i) 将无线终端的公钥与第一随机号第一链接，从而形成第一链接号码的装置；和

ii) 用密码加密所述第一链接号码的装置；和

b) 用密码加密归属系统的公钥的装置包括：

i) 将归属系统的公钥与第二随机号第一链接，从而形成第二链接号码的装置；和

ii）用密码加密所述第二链接号码的装置。

15. 一种无线终端，构成以：

a）把用户标识符和密码接收到所述无线终端中；

b）产生公钥/私钥对；

c）根据安全密钥交换(SKE)协议，用密码加密无线终端的公钥，从而形成SKE消息；

d）把用户标识符和SKE消息发送到归属系统；

e）接收来自所述归属系统的经加密的公钥；

f）用密钥解密来自归属系统的经加密的公钥；

g）用无线终端的私钥和归属系统的公钥形成对话密钥；和

h）用对话密钥将所有或部分虚拟用户标识模块(VUIM)从归属系统下载到无线终端。

16. 如权利要求15所述的终端，其特征在于，还包括用于在发送之前加密用户标识符的装置。

17. 如权利要求15所述的终端，其特征在于，还包括在发送用户标识符和SKE消息之前开放通信信道的装置。

18. 如权利要求15所述的终端，其特征在于，构成将SKE消息从源发送到目的地的一部分终端还包括：

a）将SKE消息从源发送到中间服务系统的装置；和

b）将SKE消息从中间服务系统发送到目的地的装置。

19. 如权利要求18所述的终端，其特征在于，构成以加密终端的公钥的一部分终端包括：

a）在所述中间服务系统中随后鉴定无线终端的过程中，将第一部分对话密钥用作鉴定密钥的装置；和

b）在随后的控制信号传输过程中将第二部分对话密码用作加密密钥的装置。

20. 如权利要求15所述的终端，其特征在于；

a）所述公钥/私钥对包括Diffie-Hellman公/私钥对；和

b）SKE消息包括Diffie-Hellman加密密钥交换(DH-EKE)消息。

21. 如权利要求15所述的终端，其特征在于：

a）构成以用密码加密无线终端的公钥的一部分终端包括：

i）将无线终端的公钥与第一随机号第一链接，从而形成第一链接号码的装置；和

ii）用密码加密所述第一链接号码的装置；和

b）用密码加密归属系统的公钥的一部分终端包括：

i）将归属系统的公钥与第二随机号第一链接，从而形成第二链接号码的装置；和

ii）用密码加密所述第二链接号码的装置。

22. 一种归属系统，构成以：

a）产生公钥/私钥对；

b）接收来自无线终端的用户标识符和加密公钥；

c）用用户标识符确定密码；

d）根据安全密钥交换(SKE)协议，用密码加密归属系统的公钥，从而形成SKE消息；

e）发送SKE消息；

f）用密码解密无线终端的公钥；

g）用归属系统的私钥和无线终端的公钥形成对话密钥；和

h）用对话密钥将所有和部分虚拟用户标识模块(VUIM)从归属系统下载到无线终端。

23. 如权利要求22所述的系统，其特征在于，还包括在接收用户标识符之前开放通信信道的装置。

24. 如权利要求22所述的系统，其特征在于，构成以将SKE消息从源发送到目的地的一部分系统还包括：

a）将SKE消息从源发送到中间服务系统的装置；和

b）将SKE消息从中间服务系统发送到目的地的装置。

25. 如权利要求24所述的系统，其特征在于，还包括：

a）在所述中间服务系统中随后鉴定无线终端的过程中，将第一部分对话密钥用作鉴定密钥的装置；和

b）在随后的控制信号传输过程中将第二部分对话密码用作加密密钥的装置。

26. 如权利要求22所述的系统，其特征在于：

a）所述公钥/私钥对包括Diffie-Hellman公/私钥对；和

b）SKE 消息包括 Diffie-Hellman 加密密钥交换(DH-EKE)消息。

27. 如权利要求 22 所述的系统，其特征在于：

a）构成以用密码加密无线终端的公钥的一部分终端包括：

i）将无线终端的公钥与第一随机号第一链接，从而形成第一链接号码的装置；和

ii）用密码加密所述第一链接号码的装置；和

b）构成以用密码加密归属系统的公钥的一部分终端包括：

i）将归属系统的公钥与第二随机号第一链接，从而形成第二链接号码的装置；和

ii）用密码加密所述第二链接号码的装置。

说　明　书

对于无线系统的预订可移植性

发明领域

本发明涉及无线语音和数据系统，特别是，涉及允许用户将他的预订从一个无线终端移到另一个。本发明提供预订可移植性，有时也称为个人可移动性。

背景技术

无线终端(便携式电话、手提计算机，等)不能被用作这样，除非它的用户已预订无线通信服务，从而终端可用该服务来与其它终端进行无线和有线的通信。而这又要求服务提供者登记和提供该终端，即，识别有权服务的终端并用标识和安全信息对该终端编程以允许它接入无线服务。

在无线服务工业中，术语“登记”有几种意义。这里，术语“登记”用来表示交换建立终端用户的身份所需的信息并允许接入无线服务。

在两种情况下可能要求这种登记。首先，当最初购买终端时，它未登记给任何人。将这种情况称为初始预备(initial provisioning)。其次，用户可选择重新登记，即，将他的预订从一个无线终端转移给另一个。例如，该重新登记可以从他的便携式电话到他的便携式计算机，或者从他的常规便携式电话转移到他在去遥远城市的途中租用的便携式电话。将这种重新登记称为预订可移植性。

在早期的无线系统(诸如，模拟先进移动电话系统(AMPS))中，通过在终端分配位置处的受训人员人工执行预备。这些雇员之一向服务提供者人工登记终端，一般是通过陆线电话。雇员运用业务提供者使得他/她可用的保密信息并将预订信息永久存储在终端中，通过键盘将信息输入终端。这种布局是昂贵，因为卖方必须在每个零售渠道广泛地培训雇员。此外，处理是不安全的，因为保密信息很容易被这些雇佣者获得。

另一种处理初始预备和预订可移植性的装置是向用户提供分立的，可移动(removable)装置，所谓的用户标识模块(UIM)。该服务提供者在将模块分配给用户之前，把标识和安全信息把准备到 UIM 中了。当用户将 UIM 插入终端时，

终端从 UIM 读取所需的标识信息并获得用户的预订身份(identity)。这种手段在全球移动通信系统(GSM)中十分普遍。在插入 UIM 之后登记终端是空中(over-the-air)处理过程，而且包括在模块、由服务提供者操作的基站(它具有唯一的标识号)和无线终端本身(它具有唯一的电子序号,或 ESN)之间的信息三路交换。

这第一种变通装置并不完全令人满意。它要求在模块和无线终端之间有电子接口，而这种接口使得终端的成本上升。此外，当去除或插入 UIM 时，接口打开易受污染，并在重复使用中变得不可靠。

第二种变通装置处理初始预备，但是不处理预订可移植性。这第二种装置要求当用户首先购买新的电话时，用户拨打特定号码来与可确定用户的信用的客户服务代表联系，并随后运用空中消息把所需预订信息编程到终端中。

这第二种变通装置比 UIM 装置有进步，因为它不要求在终端中有特定接口。然而，这第二种装置也不是完全令人满意的，因为服务提供者必须在客户服务中心中有高技能的人以操作无线空中编程设备。客户服务处理的昂贵本性阻止用户重新登记朋友借给他一天或两天的电话。

本发明的目的在于提供一种初始预备和预订可移植性的方法，他不要求有技术的人员完成预备和登记处理，也不要求用户必须物理插入终端的可移动物。

这里所述的过程仅要求用户将他的/她的可移植无线预订标识符，或用户标识符(常规的是他的国际移动用户标识符，或 IMUI)和密码(传统上，他的个人标识号，或 PIN)输入到无线终端。用任何方便的方法，诸如，用键盘键入号码、在麦克风中说出一个词组(以适当的语音识别技术或任何其它传统方法)来将密码输入到终端。于是，无线终端能够运用空中信号与服务提供者进行联系、获得必须的预订信息和自动地自己重编程-和对服务提供者重编程-从而服务提供者随后认识到正向它的用户登记这个无线终端。密码必须非常短--一般 4 至 6 个数字，如在银行信用卡 PIN 中-因为一般用户不能记住安全代码，这种安全代码长得(20 个数字或更多)足以阻止野蛮攻击。

显然，必须在登记过程中保护秘密不泄露(compromise)，否则预订信息将受到获得用户标识符和秘密的欺骗性用户的克隆。最近密码术的进步(诸如，如下所述的 Bellovin 和 Merritt 的研究)提供了在不暴露密码的情况下安全地验证终端和无线网都知道正确密码的技术。这些技术还提供了建立可在加密预

订信息中使用的加密密钥的装置，该加密密钥随后与初始密码确认信息交换。这些技术的存在使得支持初始预备和预订可移植性登记而无需可移动UIM也无需客户服务介入成为可能。

发明概述

申请人已开发了一种预订，它可真正从一个无线终端移植到另一个并运用短而安全的密码。

无论何时用户希望向他的预订登记终端，他都可将他的用户标识符(一般，他的国际移动用户标识符或IMUI)和他的密码(一般，他的个人标识号，或PIN)输入到终端。终端产生公/私钥对并存储它。该密钥对最好是Diffie-Hellman(D-H)密钥对。它任选地将公钥和随机号链接起来并用密码对该(任选链接的)号码加密。可用任何方便的安全密钥交换(SKE)方法。在Thomas Wu所著的"安全远程密码协议"(Proc. 1998因特网社会网和分布式系统安全研讨会，加州圣地亚哥，1998年3月，页97-111，http://jafar.stanford.edu/srp/ndss/html)和David P. Jablon所著的"强仅密码(strong password-only)鉴定的密钥交换"(美国麻萨诸塞州Westboro市的完整科学股份有限公司，1997年3月2日，http://world.std.com/-dpj/speke97.html)中描述了几种适当的SKE方法，上述内容作为参考资料在此引入。Bellovin和Merritt的Diffie-Hellman加密密钥交换(DH-EKE)方法是特别适当的，而且本发明的以下描述也是参照DH-EKE的。参见Steven M.Bellovin和Michael Merritt所著的"加密密钥交换：抗词典攻击的基于密钥的协议安全"(Proc. IEEE计算机社会对安全性和保密性研究的研讨会，1992年5月，页72-84)，其在此作为参考资料引入其内容。椭园曲线簇和指数簇均可用于此方法。把所得加密消息称为DH-EKE消息。

于是，终端与本地服务系统联系并要求登记。该服务系统可以是用户的归属系统(home system)，但通常不是。在任何情况下，终端和归属系统必须确信相互的身份，无论是否有中间服务系统，一个系统或甚至几个系统。以下的描述假设一个中间系统，但是可容易地改变为不处理任何系统或处理几个系统。即，终端和归属系统通常是消息的源和目的地(或反之亦然)，无论它们必须通过多少个中间系统(如果有的话)。

终端通过陈述全用户标识符或标识归属系统所需的足够的用户标识符，告

诉服务系统用户的归属系统是什么。它还陈述 DH-KEK 消息。较佳的是，服务系统首先向终端提供它的 D-H 公钥，从而不以明文发送谁要求登记的细节。较佳的是，服务系统向终端开放一个信道以方便登记处理。

服务系统把 DH-EKE 消息发送到归属系统，它用密码对它解密。只有归属系统和用户才知道密码。从而，归属系统恢复用户的公钥。归属系统产生它自己的 D-H 公/私钥对并存储它。于是，它将新产生的公钥与随机号链接，运用 DH-EKE 通过密码加密该链接的号码并把这新产生的 DH-KEK 消息送回到终端。终端用密码对它解密并恢复归属系统公钥。

现在，终端和归属系统都具备它自己的私钥其它人的公钥，两者都比密码要大得多。每个都能运用传统方法产生公共对话密钥。每个还能安全地用对话密钥将虚拟(virtual)用户标识模块(VUIM)下载到终端，即，通过空中向终端提供一些或全部信息，否则的话要从被插入终端的物理 UIM 获得。

现在，登记以传统的方式继续，就像已使用了 PUIM。另一方面，登记可包括在下载处理中。这是可行的，原因在于带有 VUIM 的终端已具有带有 PUIM 的终端直至以后才能获得的一些东西，即，到归属系统的通信链路(和与它共享的对话密钥)。

本方法的有利之处在于公钥是临时而且可在每个后来的登记中被替换。此外，实际上每个公钥是随机号，不提供关于尝试的解密是否成功的指示。因此，脱机词典攻击失败。词典攻击恢复的唯一一样东西是收集可行公钥，但是这些可行公钥中没有一个能够将它与其它区分开来。于是，将对密钥的正确猜测与错误猜测区分开来毫无意义。因此，继续联机攻击必须用整个密码词典，并因而失败。

也可将这一优点看作在密钥交换过程中将密码用作私钥，而不是其加密密钥本身。由于这一原因，将该过程称为安全密钥交换，而不是加密密钥交换。终端和归属系统不必交换密码，也不必交换以加密形式的对话密钥。重要的是，归属系统保证终端知道密码而且具有公共对话密钥。还重要的是，当终端向归属系统展示它的身份时，该密码不会被窃听者发现。如果在消息没有包括密码（即使以加密形式），那么它很难被泄露。

附图简述

图 1 示出 DH-KEK 消息的交换。

图 2 示出鉴定程序。

详细描述

图 1 示出 DH-EKE 消息的交换 100。用户 102 将他的标识符和密码输入到无线终端 104。终端 104 尝试一对 Diffie-Hellman(D-H)私钥和公钥并存储它们。任选的是，终端 104 和服务系统 106 的基站执行分开的程序以建立本地对话加密密钥 SESS108 来保护用户标识符不被截取(interception)。终端 104 用密码加密 D-H 公钥，在加密之前任选地与随机号链接，然后在登记要求中把用户标识符(在本地对话密钥之下任选地加密)和加密的公钥，即，第一 DH-EKE 消息 110，发送到服务系统 106 的基站。这种要求应导致专用信道分配，从而有效地完成下载过程。

服务系统 106 联系要求预订登记的归属系统 112。归属系统 112 运用在预订记录中的密码解密无线终端的公钥。于是，归属系统产生私钥和公钥 D-K 密钥，运用终端的公钥和归属系统的私钥，从上述公/私钥中获得临时对话密钥。于是，归属系统加密它本身的公钥，运用存储在预订记录中的密码，任选地在加密之前链接随机号，并以第二 DH-EKE 消息 114 的形式通过服务系统 106 将它返回到无线终端 104。无线终端 104 解密归属系统的公钥，并运用归属系统的公钥和它自己的私钥，产生(有希望)相同的临时对话密钥。

图 2 示出鉴定过程 200，它必须跟随 DH-EKE 交换。无线终端 104 和归属系统 112 执行该处理以证明每个具有相同的密钥。该鉴定可以是单边(例如，只允许归属系统 112 鉴定无线终端 104)或双边的。双边技术有三个步骤。首先，无线终端 104 加密随机号 C_W，并把加密号 $E(C_W)$202 发送到归属系统 112。其次，归属系统 112 产生它自己的随机号 C_H，加密 (C_W, C_H) 并把加密的号码 $E(C_W, C_H)$204 发送到无线终端 104。第三，无线终端 104 加密 C_H 并把加密号码 $E(C_H)$206 发送到归属系统 112。单边过程可以例如，省略第一步骤，并在第二步骤中用第二随机号替换 C_W。

用密码加密公钥，而且鉴定包括以互锁方式发送的三种不同的东西。因此，中间人攻击者(man-in-the-middle attacker)在不破坏离散对数或椭圆曲线簇的情况下，不会引起错误接受密钥，而且不会知道相互密钥(mutual key)。如果簇的尺寸足够大，那么当前这种破坏被认为是不可行的。

如果归属系统 112 证实无线终端 104 的会话密钥，那么它将预订信息-即，

所有或部分虚拟UIM(VUIM)-转移到服务系统106，对于空中传输以加密的形式和对于供服务系统使用以不加密的形式。对话密钥-或者，至少其第一部分-还可以作为鉴定密钥AUTH116用于在服务系统106中的随后终端104鉴定。这优于当前蜂窝鉴定过程之处在于在每次登记使产生鉴定密钥，而且在不同登记间随机变化。一般，D-H交换产生512位输出，这多于鉴定所需的。结果，剩余的对话密钥，即，其第二部分，可以作为传统加密密钥用于后来的控制信号传输。

服务系统106将加密的预订数据-VUIM-下载到终端，并在访问者位置寄存器(VLR)中有一登记项目(registration entry)。用户现可准备打电话。

对于后来的系统接入，可将临时移动用户标识符(TMUI)分配给用户，如在现有的蜂窝标准中所述的那样。运用鉴定密钥，通过在现有蜂窝标准中所述的过程，可产生每次呼叫(per-call)加密密钥。换句话说，在运用这里所述的方法产生鉴定密钥之后可运用在现有蜂窝标准中的空中链路安全程序，无需进行修改。

工业引用

我的发明能够在工业中实施，而且可进行和使用，无论它何时希望在新的无线终端中登记无线预订。这里所示的装置和方法的各成分(分立并相互分开)完全可以是传统的，它是它们的组合，这是我在我的发明中所要求保护的。

虽然我已描述了装置和方法的各种模式，但是我的发明的真正构思和范围并不局限于此，而是只受下列权利要求书和它们的等同物限制。

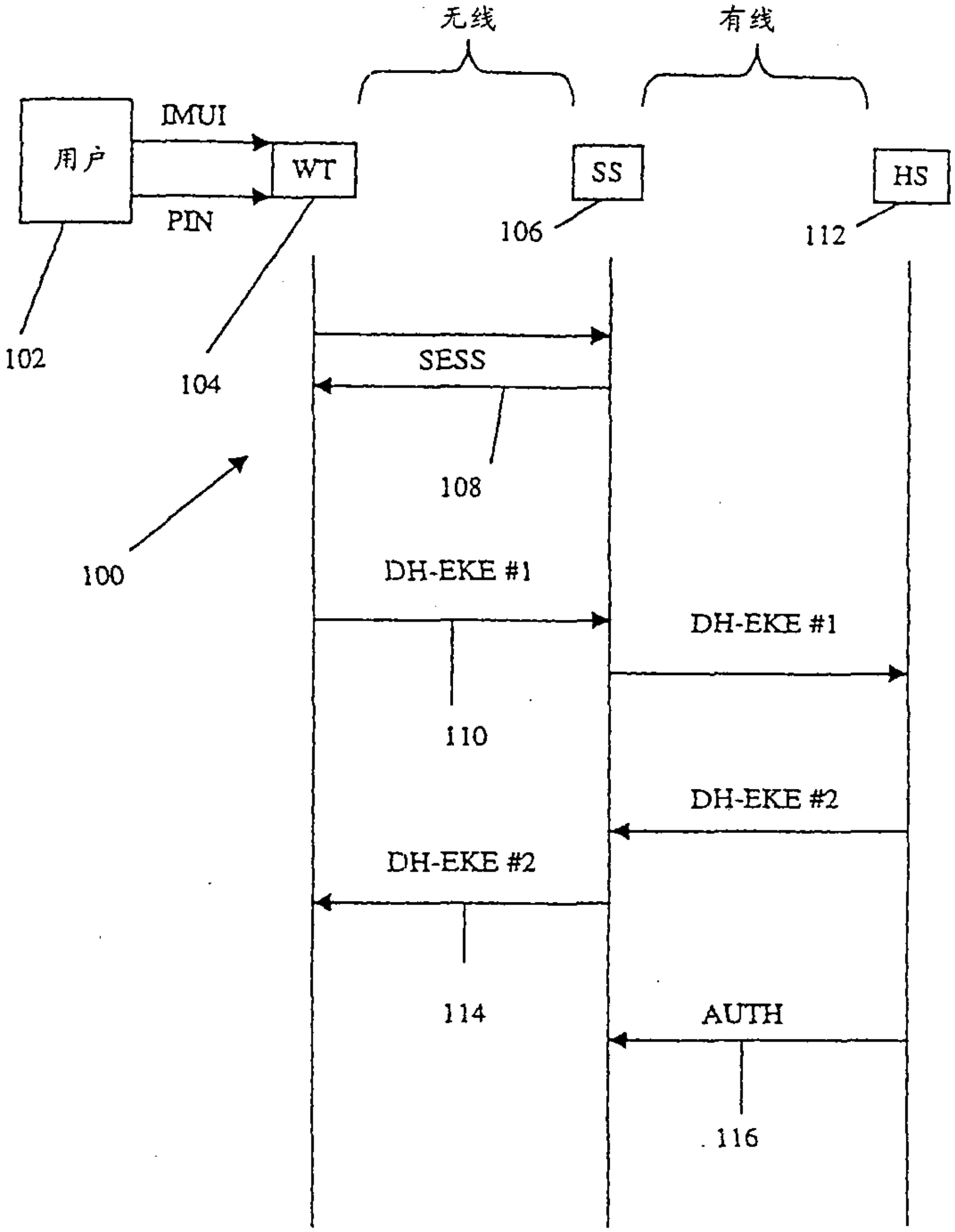

无线
有线
IMUI
用户
WT
PIN
SS
HS
106
112
102
104
SESS
108
100
DH-EKE #1
DH-EKE #1
110
DH-EKE #2
DH-EKE #2
114
AUTH
116

图 1

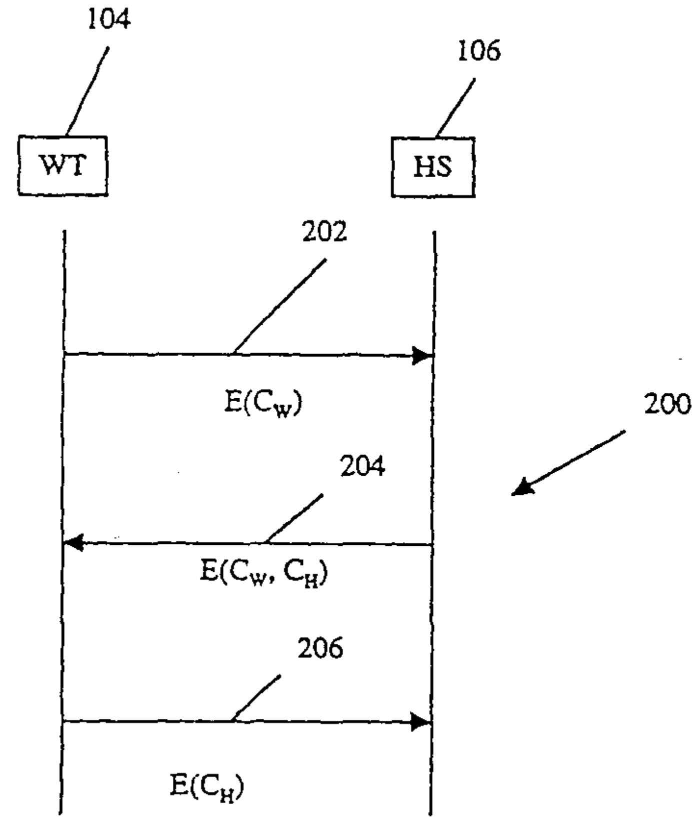


图　　2