(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 699 30 318 T2** 2006.12.07

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 123 603 B1**
(21) Deutsches Aktenzeichen: **699 30 318.4**
(86) PCT-Aktenzeichen: **PCT/US99/24522**
(96) Europäisches Aktenzeichen: **99 971 175.7**
(87) PCT-Veröffentlichungs-Nr.: **WO 2000/025475**
(86) PCT-Anmeldetag: **19.10.1999**
(87) Veröffentlichungstag der PCT-Anmeldung: **04.05.2000**
(97) Erstveröffentlichung durch das EPA: **16.08.2001**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **08.03.2006**
(47) Veröffentlichungstag im Patentblatt: **07.12.2006**

(51) Int Cl.[8]: ***H04L 9/08*** (2006.01)
H04Q 7/38 (2006.01)

(30) Unionspriorität:
178192 **23.10.1998** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Qualcomm, Inc., San Diego, Calif., US

(72) Erfinder:
QUICK, Franklin, Roy, San Diego, CA 92107, US

(74) Vertreter:
WAGNER & GEYER Partnerschaft Patent- und Rechtsanwälte, 80538 München

(54) Bezeichnung: **VERTRAGSPORTABILITÄT FÜR DRAHTLOSE SYSTEME**

Beschreibung

I. Technisches Gebiet

[0001] Die Erfindung betrifft drahtlose Sprach- und Datensysteme und bezieht sich insbesondere darauf es einem Teilnehmer zu ermöglichen sein Subskription von einem drahtlosen Terminal zu einem anderen zu bewegen. Die Erfindung sieht somit Subskriptionsportabilität vor, was manchmal auch als persönliche Mobilität bezeichnet wird.

II. Hintergrund

[0002] Ein drahtloses Terminal (portables Telefon, Laptopcomputer, etc.) kann nicht als solches verwendet werden bis der Benutzer an einem drahtlosen Kommunikationsdienst teilnimmt bzw. diesen abonniert hat, so dass das Terminal diesen Dienst verwenden kann, um mit anderen Terminals zu kommunizieren, sowohl drahtlos wie auch drahtgebunden. Dies erfordert wiederum, dass der Dienstprovider das Terminal registriert und versorgt, das bedeutet, das Terminal als berechtigt zur Teilnahme am Dienst zu registrieren und das Terminal mit Identifikations- und Sicherheitsinformation zu programmieren, welche ihm erlaubt, auf den drahtlosen Dienst zu zugreifen.

[0003] In der Branche drahtloser Dienste hat der Ausdruck „Registrierung" mehrere Bedeutungen. Hierin wird der Ausdruck „Registrierung" verwendet, um einen Austausch der Information, welche benötigt wird, um die Identität des Benutzers eines Terminals aufzubauen und um Zugriff zu drahtlosen Diensten zu erlauben, zu bedeuten.

[0004] Die Registration kann in zwei Situationen benötigt werden. Zunächst ist das Terminal wenn es ursprünglich gekauft wurde bei niemandem registriert. Diese Situation wird als ursprüngliche Bereitstellung bezeichnet. Zweitens kann ein Teilnehmer wählen, sich erneut zu registrieren, das bedeutet, seine Subskription von einem drahtlosen Terminal zu einem anderen zu transferieren.

[0005] Diese erneute Registration kann zum Beispiel von dem portablen Telefon zu seinem Laptopcomputer oder von seinem regulären portablen Telefon zu dem portablen Telefon, welches er soeben gemietet hat bei einer Reise zu einer entfernten Stadt sein. Diese erneute Registration wird als Subskriptionsportabilität bezeichnet.

[0006] In frühen drahtlosen Systemen wie dem analogen Advanced Mobile Phone Systems (AMPS) wird die Bereitstellung manuell durch geschultes Personal an der Vertriebsstelle des Terminals durchgeführt. Einer dieser Angestellten registriert manuell das Terminal bei dem Dienstprovider, typischerweise über das Landleitungstelefon. Dieser Angestellte gibt Information in das Terminal durch das Tastenpad ein, unter Verwendung von geheimer Information, welche der Dienstprovider zu ihm/ihr verfügbar gemacht hat, und speichert die Subskriptionsinformation in dem Terminal permanent. Diese Anordnung ist teuer, weil der Verkäufer intensiv geschulte Angestellte bei jeder Endkundenverkaufsstelle haben muss. Ferner ist der Vorgang nicht sicher, weil die geheime Information diesen Angestellten frei verfügbar ist.

[0007] Eine alternative Art und Weise der Verwendung von sowohl anfänglicher Bereitstellung wie auch Subskriptionsportabilität ist, dem Benutzer ein separates, entfernbares Gerät, welches als Benutzeridentifikationsmodul (UIM = user identification module) bekannt ist, zu liefern. Der Dienstprovider versorgt das UIM mit Identitäts- und Sicherheitsinformation, bevor es zu dem Benutzer ausgeliefert wird. Wenn der Benutzer das UIM in ein Terminal einsetzt liest das Terminal die notwendige Identitätsinformation von dem UIM aus und erhält dadurch die Identität der Subskription des Benutzers. Dieses Mittel ist populär in dem globalen System für Mobileinheiten (GSM = Global System for Mobiles) System. Die Registrierung des Terminals nach dem Einfügen des UIM ist ein über-die-Luft Vorgang, und beinhaltet einen Dreiwegetransfer von Information zwischen dem Modul, einer Basisstation, welche durch den Dienstprovider betrieben wird (welcher eine einzigartige Identifikationsnummer hat), und dem drahtlosen Terminal selbst (welches eine einzigartige elektronische Seriennummer, oder ESN = Electronic Serial Number hat).

[0008] Dieses erste alternative Mittel ist immer noch nicht vollständig zufrieden stellend. Es erfordert ein elektronisches Interface zwischen dem Modul und dem drahtlosen Terminal und dieses Interface addiert Kosten zu dem Terminal. Ferner ist das Interface offen zur Kontamination wenn das UIM entfernt wird und eingesetzt wird, und kann somit bei wiederholter Verwendung unzuverlässig werden.

[0009] Ein zweites alternatives Mittel, beschäftigt sich mit ursprünglicher Bereitstellung aber nicht mit Subskriptionsportabilität. Dieses zweite Mittel erfordert, dass, wenn der Teilnehmer anfänglich ein neues Telefon kauft, der Benutzer eine spezielle Nummer wählt, um einen Benutzerservice-Repräsentanten zu erreichen, welcher das Guthaben bzw. die Kreditwürdigkeit des Benutzers bestimmen kann und dann die notwendige Subskriptionsinformation in das Terminal unter Verwendung von über-die-Luft Nachrichten programmieren kann.

[0010] Dieses zweite alternative Mittel ist eine Verbesserung gegenüber dem UIM Mittel derart, dass es kein spezielles Interface in dem Terminal benötigt. Dieses zweite Mittel ist jedoch auch nicht vollständig zufrieden stellend, weil der Dienstprovider immer noch hochgradig geschicktes Personal in dem Benut-

zerservicecenter haben muss, um die über-die-Luft Programmierausrüstung zu bedienen. Die aufwändige Art des Benutzerservicevorgangs hindert den Teilnehmer daran, ein Telefon erneut zu registrieren, welches ihm ein Freund für einen Tag oder zwei ausgeliehen hat.

[0011] Der Zweck dieser Erfindung ist es, ein Verfahren für anfängliche Bereitstellung und Subskriptionsportabilität vorzusehen, welches weder ein befähigtes Personal benötigt, um den Versorgungs- und Registrationsvorgang zu vervollständigen, noch einen entfernbaren Gegenstand, welchen der Benutzer physikalisch in das Terminal einfügen muss.

[0012] Die hierin beschriebene Prozedur benötigt nur, dass der Teilnehmer seinen/ihren portablen drahtlosen Subskriptionsidentifizierer eingibt, oder Benutzeridentifizierer (konventionell seinen International Mobile User Identifier oder IMUI) und ein Passwort (konventionell seine persönliche Identifikationsnummer, oder PIN = Personal Identification Number) in ein drahtloses Terminal. Das Passwort kann in das Terminal in jeder angenehmen Art und Weise eingegeben werden, wie das Eingeben einer Nummer in ein Tastenpad, das Sprechen eines Satzes (mit geeigneter Spracherkennungstechnologie) in das Mikrofon, oder irgendeine andere angenehme Art und Weise. Das drahtlose Terminal ist dann dazu in der Lage, den Dienstprovider unter Verwendung von über-die-Luft Signalen zu kontaktieren, die notwendige Subskriptionsinformation zu erhalten, und automatisch sich selbst erneut zu programmieren – und den Dienstprovider erneut zu programmieren – derart, dass der Dienstprovider danach das drahtlose Terminal als registriert zu diesem Teilnehmer erkennt. Das Passwort muss ziemlich kurz sein – typischerweise vier bis sechs Stellen, wie in den PINs einer Bankkarte – weil sich der durchschnittliche Teilnehmer keinen Sicherheitscode merken kann, welcher ausreichend lang ist (zwanzig Zeichen oder mehr), um einen Brute-Force-Angriff abzuwehren.

[0013] Es ist offensichtlich, dass das Passwort davor geschützt werden muss, dass es während des Registrationsvorgangs beschädigt wird, anderenfalls würde die Subskriptionsinformation Klonen durch betrügerische Benutzer, welche den Benutzeridentifizierer und das Passwort erhalten, ausgesetzt sein. Jüngste Fortschritte in der Kryptographie wie die Arbeit von Bellovin und Merritt, welche untenstehend zitiert sind, liefern Techniken zum sicheren Verifizieren, dass das Terminal und das drahtlose Netzwerk beide das korrekte Passwort ohne Enthüllung des Passworts kennen. Diese Techniken sehen auch Mittel zum Etablieren von Verschlüsselungsschlüsseln vor, welche in der Verschlüsselung der Subskriptionsinformation verwendet werden können, welche nachfolgend zu der anfänglichen Passwortbestätigung ausgetauscht werden. Die Existenz dieser Techniken macht es möglich, die Registration für anfängliche Versorgung und Teilnehmerportabilität ohne die Erfordernis für entfernbare UIMs oder für Benutzerserviceintervention zu unterstützen. Das Dokument EP 0 535 863 beschreibt ein Verfahren und ein System zum Einigen auf einen Schlüssel zwischen zwei Geräten, wobei das erste Gerät seine Öffentlichkeit durch Verwendung eines ausgetauschten Passworts verschlüsselt. Das zweite Gerät erzeugt eine Zufallszahl und verschlüsselt sie unter Verwendung eines privaten Schlüssels, und sendet sie zu dem ersten Gerät. Beide erzeugen einen ausgetauschten Sitzungsschlüssel.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0014] Die Anmelderin hat eine Subskription entwickelt, welche tatsächlich von einem drahtlosen Terminal zu einem anderen portabel ist, und welches Passwörter benutzt, welche sowohl kurz wie auch sicher sind.

[0015] Wann immer ein Teilnehmer wünscht, ein Terminal zu seiner Subskription zu registrieren, gibt er eine Benutzeridentifikation (konventionell seinen internationalen mobilen Benutzeridentifizierer oder IMUI = International Mobile User Identifier) und sein Passwort (konventionell seine persönliche Identifikationsnummer, oder PIN = Personal Identification Number) in das Terminal ein. Dieses Terminal erzeugt ein Paar von öffentlichem/privatem Schlüssel und speichert es. Dieses Schlüsselpaar ist bevorzugterweise ein Diffie-Hellman (D-H) Schlüsselpaar. Es verkettet bevorzugterweise den öffentlichen Schlüssel mit einer Zufallszahl und verschlüsselt die (optional verkettete) Nummer mit dem Passwort. Jedes geeignetes sicheres Schlüsselaustausch- (SKE = Secure Key Exchange) Verfahren kann verwendet werden. Mehrere geeignete SKE Verfahren sind beschrieben in Thomas Wu, „The Secure Remote Password Protocol." Proc. 1998 Internet Society Network and Distributes System Security Symposium, San Diego, CA, März 1998, Seiten 97 bis 111 http://jafar.Stanford.edu/srp/ndss.html, und in David P. Jablon, „Strong Password-Only Authenticated Key Exchange," of Integrity Sciences, Inc., von Westbury Massachusetts, USA, 2. März 1997, http://world.std.com/~dpj/speke97.html, deren Offenbarungen hierin durch Referenz mit aufgenommen werden. Das Diffie-Hellman Encrypted Key Exchange (DH-EKE) – Verfahren von Bellovin und Merritt ist insbesondere geeignet, und die verbleibende Beschreibung der vorliegenden Erfindung wird mit Bezug auf DH-EKE gemacht. Man beachte Stefan M. Bellovin und Michael Merritt, „Encrypted Key Exchange: Password-based Protocols Secure Against Dictionary Attacks." in Proc. IEEE Computer Society Symposium on Research in Security and Privacy, Seiten 72 bis 84, Mai 1992. Entweder eine elliptische Kurve oder exponentielle Gruppen können mit diesen

Verfahren verwendet werden. Die resultierende verschlüsselte Nachricht wird als die DH-EKE Nachricht bezeichnet.

[0016] Das Terminal stellt dann einen drahtlosen Kontakt her mit einem lokalen Dienstsystem und fordert die Registrierung an. Dieses Dienstsystem kann das Heimsystem des Teilnehmers sein, aber es ist es oft nicht. In jedem Fall müssen das Terminal und das Heimsystem sich gegenseitig über ihre Identitäten sicher sein, ob es kein zwischen liegendes Dienstsystem, ein System, oder sogar mehrere sind. Das Verbleibende dieser Beschreibung nimmt ein dazwischen liegendes System an, aber wird einfach modifiziert, um keines oder mehrere zu handhaben. Dies bedeutet, dass das Terminal und das Heimsystem immer die Quelle und das Ziel (oder entgegengesetzt) von Nachrichten sein werden, unabhängig davon, wie viele dazwischen liegende Systeme (wenn vorhanden) sie durchqueren müssen.

[0017] Das Terminal teilt dem Dienstsystem mit, was das Heimsystem des Teilnehmers ist, entweder durch Angabe des vollen Benutzeridentifizierers oder genug von dem Benutzeridentifizierer wie notwendig ist, um das Heimsystem zu identifizieren. Es gibt auch die GH-EKE Nachricht an. Bevorzugterweise liefert das Dienstsystem zunächst seinen D-H öffentlichen Schlüssel zu dem Terminal, so dass die Details davon, wer Registration anfordert, nicht im Klartext übertragen werden. Auch öffnet bevorzugterweise das Dienstsystem einen Kanal mit dem Terminal um den Registrationsvorgang zu erleichtern.

[0018] Das Dienstsystem sendet die DH-EKE Nachricht zu dem Heimsystem, welches es mit dem Passwort entschlüsselt. Das Passwort ist nur dem Heimsystem und dem Teilnehmer bekannt. Das Heimsystem stellt somit den öffentlichen Schlüssel des Teilnehmers wieder her. Das Heimsystem erzeugt sein eigenes D-H öffentlich/privat Schlüsselpaar und speichert es. Dann verkettet es den neu generierten öffentlichen Schlüssel mit einer Zufallszahl, verschlüsselt die verkettete Zahl mit dem Passwort unter Verwendung von DH-EKE, und sendet die neu erzeugte DH-EKE Nachricht zurück zu dem Terminal. Das Terminal entschlüsselt es mit dem Passwort und stellt den öffentlichen Schlüssel des Heimsystems wieder her.

[0019] Das Terminal und das Heimsystem sind jetzt jeweils im Besitz ihres eigenen privaten Schlüssels und des öffentlichen Schlüssels des jeweils anderen, welche beide wesentlich länger sind als das Passwort. Jeder ist deshalb dazu in der Lage, einen gemeinsamen Sitzungsschlüssel unter Verwendung von konventionellen Verfahren zu erzeugen. Jeder ist ferner dazu in der Lage, den Sitzungsschlüssel sicher zu benutzen, um ein virtuelles Benutzeridentifikationsmodul (VUIM = Virtual User Identification Module) in das Terminal down zu loaden, das bedeutet, zu dem Terminal über die Luft einige oder alle der Informationen zu liefern, welche anderweitig von einem physikalischen UIM (PUIM = physical UIM) erhalten werden würden, welches in das Terminal eingesetzt wird.

[0020] Die Registrierung kann nun in der konventionellen Art und Weise fortfahren, wie wenn ein PUIM verwendet worden wäre. Alternativ kann die Registrierung innerhalb des Download Vorgangs beinhaltet sein. Dies ist möglich, weil das Terminal mit einem VUIM etwas hat, was ein Terminal mit einem PUIM nicht vor später erwirbt, nämlich eine Kommunikationsverbindung zu (und einen geteilten geheimen Sitzungsschlüssel mit) dem Heimsystem.

[0021] Eine Stärke dieses Verfahrens ist, dass die öffentlichen Schlüssel temporär sind, und bei jeder nachfolgenden Registrierung ersetzt werden können. Ferner ist jeder öffentliche Schlüssel im Wesentlichen eine Zufallszahl, wodurch kein Anhaltspunkt geliefert wird, ob eine versuchte Entschlüsselung erfolgreich war oder nicht. Ein offline Dictionary- bzw. Wörterbuch-Angriff schlägt deshalb fehl. Das Einzige, was ein Dictionary-Angreifer erlangt ist eine Sammlung von möglichen öffentlichen Schlüsseln, von denen keiner irgendetwas hat, was ihn von irgendeinem der anderen unterscheiden würde. Es gibt somit nichts, um eine korrekte Vermutung des Passworts von einer nicht korrekten Vermutung zu unterscheiden. Der nachfolgende online Angriff muss deshalb immer noch das gesamte Wörterbuch von Passwörtern verwenden, und wird deshalb fehlschlagen.

[0022] Diese Stärke kann auch derart gesehen werden, dass das Passwort als ein privater Schlüssel in einer Schlüsselaustauschprozedur verwendet wird, anstatt als ein Verschlüsselungsschlüssel per se. Aus diesem Grund wird der Vorgang sicherer Schlüsselaustausch anstatt verschlüsselter Schlüsselaustausch genannt. Es ist nicht notwendig, dass das Terminal und das Heimsystem Passwörter oder Sitzungsschlüssel in verschlüsselter Form austauschen. Was wichtig ist, ist, dass das Heimsystem versichert ist, dass das Terminal das Passwort weiß, und den gemeinsamen Sitzungsschlüssel hat. Es ist auch wichtig, dass das Passwort nicht durch Lauscher auffindbar ist, während das Terminal seine Identität zu dem Heimsystem demonstriert. Wenn das Passwort nicht in der Nachricht enthalten ist, sogar in verschlüsselter Form, dann ist es schwieriger, dass einem geschadet wird.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0023] Fig. 1 zeigt einen Austausch von DH-EKE Nachrichten.

[0024] Fig. 2 zeigt eine Authentifikationsprozedur.

DETAILLIERTE BESCHREIBUNG

[0025] Fig. 1 zeigt einen Austausch **100** von DH-EKE Nachrichten. Der Benutzer **102** gibt den Benutzeridentifizierer und das Passwort in das drahtlose Terminal **104** ein. Das Terminal **104** erzeugt ein Paar von Diffie-Hellman (D-H) privaten und öffentlichen Schlüsseln, und speichert diese. Optional führen das Terminal **104** und die Basisstation des Dienstsystems **106** eine separate Prozedur aus, um einen lokalen Sitzungsverschlüsselungsschlüssel SESS (Session Encryption Key) **108** aufzubauen, um den Benutzeridenifizierer vor dem Abfangen zu schützen. Das Terminal **104** verwendet das Passwort, um den D-H öffentlichen Schlüssel zu verschlüsseln, optional verkettet mit einer Zufallszahl vor der Verschlüsselung, sendet dann den Benutzeridenifizierer (optional verschlüsselt unter dem lokalen Sitzungsschlüssel) und den verschlüsselten öffentlichen Schlüssel, das bedeutet, eine erste DH-EKE Nachricht **110** zu der Basisstation des Dienstsystems **106** in einer Registrationsanforderung. Diese Anforderung sollte zu einer dedizierten Kanalzuweisung führen, um die Download Prozedur effizient zu vervollständigen.

[0026] Das Dienstsystem **106** kontaktiert das Heimsystem **112** unter Anforderung einer Subskriptionsregistrierung. Das Heimsystem **112** entschlüsselt den öffentlichen Schlüssel des drahtlosen Terminals unter Verwendung des Passworts in dem Subskriptionseintrag. Das Heimsystem erzeugt dann einen privaten und öffentlichen D-H Schlüssel, von welchem ein vorläufiger Sitzungsschlüssel erhalten wird unter Verwendung des öffentlichen Schlüssels des Terminals und des privaten Schlüssels des Heimsystems. Das Heimsystem verschlüsselt dann seinen eigenen öffentlichen Schlüssel, optional unter Verkettung einer Zufallszahl vor der Verschlüsselung, unter Verwendung des Passworts, welches in dem Subskriptionseintrag gespeichert ist und gibt es in der Form einer zweiten DH-EKE Nachricht **114** zu dem drahtlosen Terminal **104** über das Dienstsystem **106** zurück. Das drahtlose Terminal **104** entschlüsselt den öffentlichen Schlüssel des Heimsystems und erzeugt (hoffentlich) den gleichen vorläufigen Sitzungsschlüssel, unter Verwendung des öffentlichen Schlüssels des Heimsystems und seines eigenen privaten Schlüssels.

[0027] Fig. 2 zeigt eine Authentifikationsprozedur **200**, welche dem DH-EKE Austausch folgen muss. Das drahtlose Terminal **104** und das Heimsystem **112** führen diese Prozedur aus, um zu beweisen, dass jeder den gleichen Schlüssel hat. Diese Autentifikation kann entweder unilateral (zum Beispiel nur dem Heimsystem **112** erlaubend, das drahtlose Terminals **104** zu authentifizieren) oder bilateral sein. Die bilaterale Technik hat drei Schritte. Zunächst verschlüsselt das drahtlose Terminal **104** eine Zufallszahl C_W und sendet die verschlüsselte Zahl E (C_W) **202** zu dem Heimsystem **112**. Zweitens erzeugt das Heimsystem **112** seine eigene Zufallszahl C_H, verschlüsselt (C_W, C_H) und sendet die verschlüsselte Zahl E (C_W, C_H) **204** zu dem drahtlosen Terminal **104**. Drittens verschlüsselt das drahtlose Terminal **104** C_H und sendet die verschlüsselte Zahl E (C_H) **206** zu dem Heimsystem **112**. Eine unilaterale Prozedur kann zum Beispiel den ersten Schritt übergehen, und C_W in dem zweiten Schritt durch eine zweite Zufallszahl ersetzen.

[0028] Die öffentlichen Schlüssel wurden durch das Passwort verschlüsselt, und die Authentifikation besteht aus drei verschiedenen Dingen, welche in einer verknüpften Art und Weise gesendet werden. Deshalb kann ein „man-in-themiddle" Angreifer keine falsche Akzeptanz von Schlüsseln verursachen, und kann nicht die gegenseitigen Schlüssel wissen, ohne den diskreten Logarithmus oder die elliptische Kurvengruppe aufzubrechen. Ein solches Aufbrechen wird derzeit als nicht realisierbar angesehen, wenn die Gruppengröße ausreichend groß ist.

[0029] Wenn das Heimsystem **112** den Sitzungsschlüssel des drahtlosen Terminals **104** verifiziert wird es die Subskriptionsinformation – das bedeutet, alles oder einen Teil des virtuellen UIM (VUIM) zu dem Dienstsystem **106** übertragen, sowohl in verschlüsselter Form für über die Luft Übertragung wie auch in nicht verschlüsselter Form zur Verwendung durch das Dienstsystem. Der Sitzungsschlüssel – oder mindestens ein erster Teil davon – kann auch als ein Autentifikationsschlüssel AUTH **116** für nachfolgende Authentifikationen des Terminals **104** in dem Dienstsystem **106** dienen. Dies hat Vorteile gegenüber den derzeitigen zellularen Authentifikationsprozeduren darin, dass der Authentifikationsschlüssel bei jeder Registrierung erzeugt wird, und deshalb zufällig von Registration zu Registration sich verändern wird. Typischerweise erzeugt der D-H Austausch 512 bits von Ausgabe, was mehr ist als benötigt wird zur Authentifikation. Als ein Ergebnis kann das verbleibende des Sitzungsschlüssels, das bedeutet ein zweiter Teil davon, als ein konventioneller Verschlüsselungsschlüssel für nachfolgende Steuerungssignalübertragungen dienen.

[0030] Das Dienstsystem **106** downloaded die verschlüsselten Subskriptionsdaten – das VUIM – zu dem Terminal und macht den Registrationseintrag in dem Benutzerortsregister (VLR = Visitor Location Register). Der Benutzer ist nun dazu bereit, Anrufe auszuführen.

[0031] Für nachfolgende Systemzugriffe kann den Benutzer ein temporärer Mobilbenutzeridentifizierer (TMUI = Temporary Mobile User Identifier) zugeordnet werden, wie in existierenden zellularen Stan-

dards beschrieben ist. Die Erzeugung von Verschlüsselungsschlüsseln pro Anruf kann unter Verwendung des Authentifikationsschlüssels unter Verwendung von Prozeduren, welche in den existierenden zellularen Standards beschrieben sind, durchgeführt werden. Mit anderen Worten können die Sicherheitsprozeduren für Luftverbindungen in existierenden zellularen Standards ohne Modifikation nach der Erzeugung des Authentifikationsschlüssels unter Verwendung der hierin beschriebenen Verfahren verwendet werden.

Industrielle Anwendbarkeit

[0032] Meine Erfindung ist dazu in der Lage, in der Industrie verwendet zu werden, und kann ausgeführt und verwendet werden, wann immer es erwünscht ist, eine drahtlose Subskription in einem neuen drahtlosen Terminal zu registrieren. Die individuellen Komponenten der Vorrichtung und des Verfahrens, welche hierin gezeigt sind, separat und unabhängig von einander genommen, können vollständig konventionell sein, es ist ihre Kombination, welche ich als meine Erfindung beanspruche.

[0033] Während ich verschiedene Modi von Vorrichtungen und Verfahren beschrieben habe, ist der Umfang meiner Erfindung nicht hierauf eingeschränkt, sondern ist nur durch die folgenden Ansprüche eingeschränkt.

Patentansprüche

1. Ein Verfahren zur Registrierung einer drahtlosen Subskription bei einem drahtlosen Terminal, wobei das Verfahren folgende Schritte aufweist:
a) Eingeben eines Anwenderidentifikators und eines Passworts in das drahtlose Terminal;
b) beim drahtlosen Terminal:
i) Generieren eines öffentlichen/privaten Schlüsselpaars;
ii) Verwenden des Passworts, um den öffentlichen Schlüssel des drahtlosen Terminals gemäß einem sicheren Schlüsselaustauschprotokoll (SKE = Secure Key Exchange) zu verschlüsseln, dabei eine erste SKE-Nachricht bildend; und
iii) Senden des Anwenderidentifikators und der ersten SKE-Nachricht zu einem Heimsystem;
c) beim Heimsystem:
i) Generieren eines öffentlichen/privaten Schlüsselpaars;
ii) Verwenden des Anwenderidentifikators, um das Passwort zu bestimmen; **dadurch gekennzeichnet**, dass das Verfahren folgende Schritte aufweist:
beim Heimsystem:
i) Verwenden des Passworts, um den öffentlichen Schlüssel des Heimsystems gemäß einem SKE-Protokoll zu verschlüsseln, dabei eine zweite SKE-Nachricht bildend;
ii) Senden der zweiten SKE-Nachricht zum drahtlosen Terminal;
iii) Verwenden des Passworts, um den öffentlichen Schlüssel des drahtlosen Terminals zu entschlüsseln; und
iv) Verwenden des privaten Schlüssels des Heimsystems und des öffentlichen Schlüssels des drahtlosen Terminals, um einen Sitzungsschlüssel zu bilden;
d) beim drahtlosen Terminal:
i) Verwenden des Passworts, um den öffentlichen Schlüssel des Heimsystems zu entschlüsseln; und
ii) Verwenden des privaten Schlüssels des drahtlosen Terminals und des öffentlichen Schlüssels des Heimsystems, um den Sitzungsschlüssel zu bilden; und
e) bei beiden, dem drahtlosen Terminal und dem Heimsystem, verwenden des Sitzungsschlüssels, um das Ganze oder Teile von einem virtuellen Anwenderidentifikationsmodul (VUIM = virtual user identification module) von dem Heimsystem zum drahtlosen Terminal herunterzuladen.

2. Verfahren nach Anspruch 1, welches weiterhin den Schritt aufweist, den Anwenderidentifikator zu verschlüsseln, bevor er gesendet wird.

3. Verfahren nach Anspruch 1, welches weiterhin den Schritt aufweist, einen Kommunikationskanal zu öffnen, bevor die zweite SKE-Nachricht zum drahtlosen Terminal gesendet wird.

4. Verfahren nach Anspruch 1, wobei die Schritte, bei denen die SKE-Nachrichten von einer Quelle zu einem Ziel gesendet werden, weiterhin folgende Schritte aufweisen:
a) Senden der SKE-Nachrichten von einer Quelle zu einem dazwischen liegenden Dienstsystem; und
b) Senden der SKE-Nachrichten von dem dazwischen liegenden Dienstsystem zu einem Ziel.

5. Verfahren nach Anspruch 4, wobei das Verfahren weiter folgende Schritte aufweist:
a) Verwenden eines ersten Teils des Sitzungsschlüssels als einen Authentifizierungsschlüssel in einer nachfolgenden Authentifizierung des drahtlosen Terminals in dem dazwischen liegenden Dienstsystem; und
b) Verwenden eines zweiten Teils des Sitzungsschlüssels als einen Verschlüsselungsschlüssel in nachfolgenden Steuersignaltransmissionen.

6. Das Verfahren nach Anspruch 1, wobei:
a) die öffentlichen/privaten Schlüsselpaare weisen Diffie-Hellman-öffentliche/private Schlüsselpaare auf; und
b) die SKE-Nachrichten weisen Diffie-Hellman verschlüsselte Schlüsselaustauschnachrichten (DH-EKE = Diffie Hellman encrypted key exchange) auf.

7. Verfahren nach Anspruch 1, wobei:

a) der Schritt, bei dem das Passwort benutzt wird um den öffentlichen Schlüssel des drahtlosen Terminals zu verschlüsseln, folgende Schritte aufweist:
i) zuerst Verknüpfen des öffentlichen Schlüssels des drahtlosen Terminals mit einer ersten zufälligen Zahl, dabei eine erste verknüpfte Zahl bildend; und
ii) Verwenden des Passworts, um die erste verknüpfte Zahl zu verschlüsseln; und
b) der Schritt, bei dem das Passwort benutzt wird, um den öffentlichen Schlüssel des Heimsystems zu verschlüsseln, folgende Schritte aufweist:
i) zuerst Verknüpfen des öffentlichen Schlüssels des Heimsystems mit einer zweiten zufälligen Zahl, dabei eine zweite verknüpfte Zahl bildend; und
ii) Verwenden des Passworts, um die zweite verknüpfte Zahl zu verschlüsseln.

8. Ein System zur Registrierung von einer drahtlosen Subskription bei einem drahtlosen Terminal, wobei das System Folgendes aufweist:
a) Mittel zum Eingeben eines Anwenderidentifikators und eines Passworts in ein drahtloses Terminal;
b) bei dem drahtlosen Terminal:
i) Mittel zum Generieren eines öffentlichen/privaten Schlüsselpaars;
ii) Mittel für das Verwenden des Passworts, um den öffentlichen Schlüssel des drahtlosen Terminals gemäß einem sicheren Schlüsselaustauschprotokolls (SKE) zu verschlüsseln, dabei eine erste SKE-Nachricht bildend; und
iii) Mittel zum Senden des Anwenderidentifikators und der ersten SKE-Nachricht zu einem Heimsystem;
c) bei dem Heimsystem:
i) Mittel zum Generieren eines öffentlichen/privaten Schlüsselpaars;
ii) Mittel für das Verwenden des Anwenderidentifikators, um das Passwort zu bestimmen; wobei das System dadurch gekennzeichnet ist, dass es weiterhin aufweist:
beim Heimsystem:
i) Mittel zum Verwenden des Passworts, um den öffentlichen Schlüssel des Heimsystems gemäß einem SKE-Protokoll zu verschlüsseln, dabei eine zweite SKE-Nachricht bildend;
ii) Mittel zum Senden der zweiten SKE-Nachricht zum drahtlosen Terminal;
iii) Mittel zum Verwenden des Passworts, um den öffentlichen Schlüssel des drahtlosen Terminals zu entschlüsseln; und
iv) Mittel zum Verwenden des öffentlichen Schlüssels des Heimsystems und des öffentlichen Schlüssels des drahtlosen Terminals, um einen Sitzungsschlüssel zu bilden;
d) beim drahtlosen Terminal:
i) Mittel zum Verwenden des Passworts, um den öffentlichen Schlüssel des Heimsystems zu entschlüsseln; und
ii) Mittel für das Verwenden des privaten Schlüssels des drahtlosen Terminals und des öffentlichen Schlüssels des Heimsystems, um den Sitzungsschlüssel zu bilden; und
e) bei beiden, dem drahtlosen Terminal und dem Heimsystem, Mittel zum Verwenden des Sitzungsschlüssels, um das ganze oder einen Teil von einem virtuellen Anwenderidentifikationsmodul (VUIM) von dem Heimsystem zum drahtlosen Terminal herunterzuladen.

9. System nach Anspruch 8, wobei das System weiterhin Mittel aufweist, den Anwenderidentifikator vor dem Senden zu verschlüsseln.

10. System nach Anspruch 8, wobei das System weiterhin Mittel aufweist, den Kommunikationskanal vor dem Senden der zweiten SKE-Nachricht zum drahtlosen Terminal zu öffnen.

11. System nach Anspruch 8, wobei die Mittel zum Senden der SKE-Nachrichten von einer Quelle zu einem Ziel weiterhin aufweisen:
a) Mittel zum Senden der SKE-Nachrichten von einer Quelle zu einem dazwischen liegenden Dienstsystem; und
b) Mittel zum Senden der SKE-Nachrichten von dem dazwischen liegenden Dienstsystem zum Ziel.

12. System nach Anspruch 11, wobei das System weiterhin aufweist:
a) Mittel zum Verwenden eines ersten Teils des Sitzungsschlüssels als einen Authentifizierungsschlüssel in nachfolgenden Authentifizierungen des drahtlosen Terminals in dem dazwischen liegenden Dienstsystem; und
b) Mittel zur Verwendung eines zweiten Teils des Sitzungsschlüssels als einen Verschlüsselungsschlüssel in nachfolgenden Steuersignaltransmissionen.

13. System nach Anspruch 8, wobei:
a) die öffentlichen/privaten Schlüsselpaare Diffie-Hellman-öffentliche/private Schlüsselpaare aufweisen; und
b) die SKE-Nachrichten Diffie-Hellman verschlüsselte Schlüsselaustauschnachrichten (DH-EKE) aufweisen.

14. System nach Anspruch 8, wobei:
a) die Mittel für das Verwenden des Passworts, um den öffentlichen Schlüssel des drahtlosen Terminals zu verschlüsseln, aufweisen:
i) Mittel für die erste Verknüpfung des öffentlichen Schlüssels des drahtlosen Terminals mit einer ersten zufälligen Zahl, dabei eine erste verknüpfte Zahl bildend; und
ii) Mittel zum Verwenden des Passworts, um die erste verknüpfte Zahl zu verschlüsseln; und
b) die Mittel zum Verwenden des Passworts, um den öffentlichen Schlüssel des Heimsystems zu verschlüsseln, aufweisen:
i) Mittel für das erste Verknüpfen des öffentlichen

Schlüssels des Heimsystems mit einer zweiten zufälligen Zahl, dabei eine zweite verknüpfte Zahl bildend; und
ii) Mittel zum Verwenden des Passworts, um die zweite verknüpfte Zahl zu verschlüsseln.

15. Ein drahtloses Terminal, konstruiert zum:
a) Empfangen eines Anwenderidentifikators und eines Passworts in dem drahtlosen Terminal;
b) Generieren eines öffentlichen/privaten Schlüsselspaares;
c) Verwenden des Passworts, um den öffentlichen Schlüssel des drahtlosen Terminals gemäß einem sicheren Schlüsselaustauschprotokoll (SKE) zu verschlüsseln, dabei eine SKE-Nachricht bildend;
d) Senden des Anwenderidentifikators und der SKE-Nachricht zu einem Heimsystem;
e) Empfangen eines verschlüsselten öffentlichen Schlüssels von dem Heimsystem; dadurch gekennzeichnet, dass es konstruiert wurde, um zu:
f) Verwenden des Passworts, um den verschlüsselten öffentlichen Schlüssel vom Heimsystem zu entschlüsseln;
g) Verwenden des privaten Schlüssels des drahtlosen Terminals und des öffentlichen Schlüssels des Heimsystems, um den Sitzungsschlüssel zu bilden; und
h) Verwenden des Sitzungsschlüssels, um das Ganze oder einen Teil eines virtuellen Anwenderidentifikationsmoduls (VUIM) von dem Heimsystem zum drahtlosen Terminal herunterzuladen.

16. Terminal nach Anspruch 15, wobei das Terminal weiter Mittel aufweist, den Anwenderidentifikator vor dem Senden zu verschlüsseln.

17. Terminal nach Anspruch 15, wobei das Terminal weiterhin Mittel aufweist, einen Kommunikationskanal vor dem Senden des Anwenderidentifikators und der SKE-Nachricht zu öffnen.

18. Terminal nach Anspruch 15, wobei ein Teil des Terminals, der konstruiert ist, die SKE-Nachrichten von einer Quelle zu einem Ziel zu senden, weiterhin Folgendes aufweist:
a) Mittel zum Senden der SKE-Nachrichten von der Quelle zu einem dazwischen liegenden Dienstsystem; und
b) Mittel zum Senden der SKE-Nachrichten von dem dazwischen liegenden Dienstsystem zum Ziel.

19. Terminal nach Anspruch 18, wobei ein Teil des Terminals, der konstruiert ist, den öffentlichen Schlüssel des Terminals zu verschlüsseln, Folgendes aufweist:
a) Mittel zum Verwenden eines ersten Teils des Sitzungsschlüssels als einen Authentifizierungsschlüssel in nachfolgenden Authentifizierungen des drahtlosen Terminals im dazwischen liegenden Dienstsystem; und
b) Mittel zum Verwenden eines zweiten Teils des Sitzungsschlüssels als einen Verschlüsselungsschlüssel in nachfolgenden Steuersignaltransmissionen.

20. Terminal nach Anspruch 15, wobei:
a) die öffentlichen/privaten Schlüsselpaare Diffie-Hellman-öffentliche/private Schlüsselpaare aufweisen; und
b) die SKE-Nachrichten Diffie-Hellman verschlüsselte Schlüsselaustauschnachrichten (DH-EKE) aufweisen.

21. Terminal nach Anspruch 15, wobei:
a) ein Teil des Terminals, der konstruiert ist, das Passwort für die Verschlüsselung des öffentlichen Schlüssels des drahtlosen Terminals zu verwenden, Folgendes aufweist:
i) Mittel um zuerst den öffentlichen Schlüssel des drahtlosen Terminals mit einer ersten zufälligen Zahl zu verknüpfen, dabei eine erste verknüpfte Zahl bildend; und
ii) Mittel zum Verwenden des Passworts, um die erste verknüpfte Zahl zu verschlüsseln; und
b) ein Teil des Terminals, der konstruiert wurde, das Passwort zum Verschlüsseln des öffentlichen Schlüssels des Heimsystems zu verwenden, Folgendes aufweist:
i) Mittel zum zuerst Verknüpfen des öffentlichen Schlüssels des Heimsystems mit einer zweiten zufälligen Zahl, dabei eine zweite verknüpfte Zahl bildend; und
ii) Mittel zum Verwenden des Passworts, um die zweite verknüpfte Zahl zu verschlüsseln.

22. Ein Heimsystem, konstruiert zum:
a) Generieren eines öffentlichen/privaten Schlüsselpaars;
b) Empfangen eines Anwenderidentifikators und eines verschlüsselten öffentlichen Schlüssels von einem drahtlosen Terminal;
c) Verwenden des Anwenderidentifikators zum Bestimmen des Passworts; dadurch gekennzeichnet, dass es konstruiert wurde zum:
d) Verwenden des Passworts, um den öffentlichen Schlüssel des Heimsystems gemäß einem sicheren Schlüsselaustauschprotokoll (SKE) zu verschlüsseln, dabei eine SKE-Nachricht bildend;
e) Senden der SKE-Nachricht;
f) Verwenden des Passworts, um den öffentlichen Schlüssel des drahtlosen Terminals zu entschlüsseln;
g) Verwenden des privaten Schlüssels des Heimsystems und des öffentlichen Schlüssels des drahtlosen Terminals, um einen Sitzungsschlüssel zu bilden; und
h) Verwenden des Sitzungsschlüssels, um das Ganze oder einen Teil von einem virtuellen Anwenderidentifikationsmodul (VUIM) von dem Heimsystem zum drahtlosen Terminal herunterzuladen.

23. System nach Anspruch 22, wobei das System weiterhin Mittel aufweist, einen Kommunikationskanal vor dem Empfang des Anwenderidentifikators zu öffnen.

24. System nach Anspruch 22, wobei ein Teil des Systems konstruiert wurde, um die SKE-Nachrichten von einer Quelle zu einem Ziel zu senden, wobei dieser Teil des Systems weiterhin aufweist:
a) Mittel zum Senden der SKE-Nachrichten von der Quelle zu einem dazwischen liegenden Dienstsystem; und
b) Mittel zum Senden der SKE-Nachrichten von dem dazwischen liegenden Dienstsystem zum Ziel.

25. System nach Anspruch 24, wobei das System weiterhin aufweist:
a) Mittel zum Verwenden eines ersten Teils des Sitzungsschlüssels als einen Authentifizierungsschlüssel in nachfolgenden Authentifizierungen des drahtlosen Terminals in dem dazwischen liegenden Dienstsystem; und
b) Mittel zum Verwenden eines zweiten Teils des Sitzungsschlüssels als einen Verschlüsselungsschlüssel in nachfolgenden Steuersignaltransmissionen.

26. System nach Anspruch 22, wobei:
a) die öffentlichen/privaten Schlüsselpaare Diffie-Hellman öffentliche/private-Schlüsselpaare aufweisen; und
b) die SKE-Nachrichten Diffie-Hellman verschlüsselte Schlüsselaustauschnachrichten (DH-EKE) aufweisen.

27. System nach Anspruch 22, wobei:
a) ein Teil des Terminals, der konstruiert ist, das Passwort für die Verschlüsselung des öffentlichen Schlüssels des drahtlosen Terminals zu verwenden, Folgendes aufweist:
i) Mittel zum zuerst Verknüpfen des öffentlichen Schlüssels des drahtlosen Terminals mit einer erste zufälligen Zahl, dabei eine erste verknüpfte Zahl bildend; und
ii) Mittel zum Verwenden des Passworts, um die erste verknüpfte Zahl zu verschlüsseln; und
b) ein Teil des Terminals, der konstruiert ist, das Passwort für die Verschlüsselung des öffentlichen Schlüssels des Heimsystems zu verwenden, Folgendes aufweist:
i) Mittel zum zuerst Verknüpfen des öffentlichen Schlüssels des Heimsystems mit einer zweiten zufälligen Zahl, dabei eine zweite verknüpfte Zahl bildend; und
ii) Mittel zum Verwenden des Passworts, um die zweite verknüpfte Zahl zu verschlüsseln.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

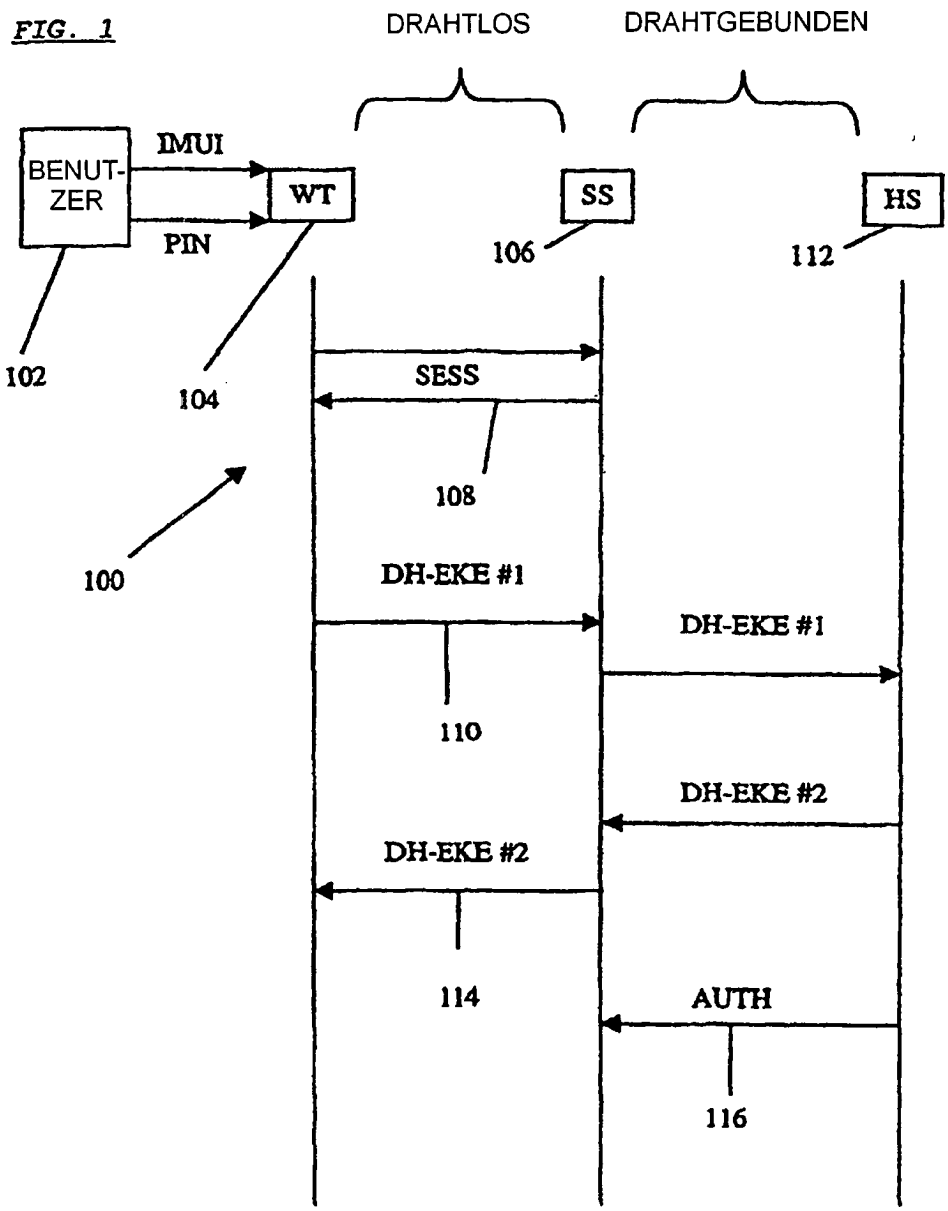

FIG. 2