(19) SUOMI - FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN
FINNISH PATENT AND REGISTRATION OFFICE

(10) **FI 20022014 A7**

(12) **JULKISEKSI TULLUT PATENTTIHAKEMUS**
PATENTANSÖKAN SOM BLIVIT OFFENTLIG
PATENT APPLICATION MADE AVAILABLE TO THE PUBLIC

(21) Patenttihakemus - Patentansökan - Patent application 20022014

(51) Kansainvälinen patenttiluokitus - Internationell patentklassifikation - International patent classification
H04L 9/32
H04Q 7/38
H04L 29/06
H04Q 7/32
H04W 12/06 (2009.01)

(22) Tekemispäivä - Ingivningsdag - Filing date **11.11.2002**

(23) Saapumispäivä - Ankomstdag - Reception date **11.11.2002**

(41) Tullut julkiseksi - Blivit offentlig - Available to the public **20.10.2003**

(43) Julkaisupäivä - Publiceringsdag - Publication date **14.06.2019**

(71) Hakija - Sökande - Applicant

1 •**Nokia Corporation,** Helsinki, Keilalahdentie 4, 02150 ESPOO, SUOMI - FINLAND, (FI)

(72) Keksijä - Uppfinnare - Inventor

1 •**Laurila, Pasi,** Tupos, SUOMI - FINLAND, (FI)
2 •**Haukka, Tao,** Oulu, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud - Agent

Kolster Oy Ab, Iso Roobertinkatu 23, 00120 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning - Title of the invention

Menetelmä tilaajapäätelaitteen autentikointiin pakettikytkentäisessä multimediaradiojärjestelmässä ja autentikointijärjestely

Förfarande för autenticering av abonnentterminaler i ett paketkopplat multimediaradiosystem och ett autenticeringssystem

(57) Tiivistelmä - Sammandrag - Abstract

Keksinnössä on kuvattu menetelmä tilaajapäätelaitteen autentikointiin pakettikytkentäisessä multimediaradiojärjestelmässä. Menetelmässä vastaanotetaan (406) tilaajapäätelaitteessa pakettikytkentäisestä multimediaradiojärjestelmästä lähetetty autentikointipyyntö, joka käsittää pakettikytkentäisen multimediaradiojärjestelmän autentikointiparametrejä ja lähetetään (416) tilaajapäätelaitteesta autentikointivastaus pakettikytkentäiseen multimediaradiojärjestelmään. Lisäksi menetelmä käsittää autentikointipyynnön vastaanottamisen ja autentikointivastauksen lähettämisen välissä myös: muodostetaan (407) tilaajapäätelaitteessa SMS (short message service)-viesti, johon vastaanotetut autentikointiparametrit sijoitetaan; lähetetään (408) muodostettu SMS-viesti GSM:n (Global System for Mobile Communications) SIM (subscriber identity module)-kortille; generoidaan (410) GSM:n SIM-kortilla vastaanotetun SMS-viestin sekä GSM:n SIM-kortille tallennetun autentikointiavaimen ja pakettikytkentäisen multimediaradiojärjestelmän autentikointialgoritmin perusteella pakettikytkentäisen multimediaradiojärjestelmän vastausparametrit; muodostetaan (414) tilaajapäätelaitteessa autentikointivastaus GSM:n SIM-kortilta vastaanotettujen pakettikytkentäisen multimediaradiojärjestelmän vastausparametrien perusteella.(Kuvio 4)

Uppfinningen beskriver ett förfarande för autenticering av en abonnentterminal i ett paketkopplat multimediaradiosystem. I förfarandet mottas (406) i abonnentterminalen en från ett paketkopplat multimediaradiosystem sänd au-tenticeringsbegäran, som omfattar autenticeringsparametrar för det paketkopplade multimediaradiosystemet och ett autenticeringssvar sänds (416) från abonnentterminalen till det paketkopplade multimediaradiosystemet. Dessutom omfattar förfarandet mellan mottagningen av en autenticeringsbegäran och sändningen av ett autenticeringssvar även: bildande (407) av ett SMS (short message service) -meddelande i abonnentterminalen, i vilket de mottagna autenticeringsparametrarna placeras; sändning (408) av det bildade SMS-meddelandet till ett GSM (Global System for Mobile communications)-SIM (subscriber identity module) -kort; generering (410) av svarsparametrar för det paketkopplade multimediaradiosystemet på basis av det med GSM-SIM-kortet mottagna SMS-meddelandet samt en på GSM-SIM-kortet lagrad autenticeringsnyckel och en autenticeringsalgoritm för det paketkopplade multimediaradiosystemet; bildande (414) av ett autenticeringssvar i abonnentterminalen på basis av de från GSM-SIM-kortet mottagna svarsparametrarna för det paketkopplade multimediaradiosystemet.

Menetelmä tilaajapäätelaitteen autentikointiin pakettikytkentäisessä multimediaradiojärjestelmässä ja autentikointijärjestely

Ala

Keksinnön kohteina ovat menetelmä tilaajapäätelaitteen autentikointiin pakettikytkentäisessä multimediaradiojärjestelmässä sekä autentikointijärjestely.

Tausta

Autentikointia käytetään radiojärjestelmissä tilaajapäätelaitteiden identiteettien todentamiseen. Autentikoinnissa tarkistetaan SIM (Subscriber Identity Module)-kortin validiteetti ja se, onko kyseisellä SIM-kortilla lupa tietyn verkon palveluihin. Autentikoinnilla myös varmistetaan tilaajapäätelaitteiden ja radiojärjestelmän välisen tiedonsiirron eheys (integrity) ja luottamuksellisuus. Autentikointi perustuu autentikointialgoritmiin, kuten A3, joka on tallennettu SIM-kortille ja tilaajan verkkoon. Autentikointialgoritmi käyttää yhtenä parametrinään tilaajan autentikointiavainta (Subscriber Authentication Key), Ki, joka on tallennettu vain SIM-kortille sekä verkkoon. Toinen parametri, satunnaisluku RAND, lähetetään verkosta tilaajapäätelaitteelle. Tilaajapäätelaite välittää RAND:in SIM-kortille, jossa sitä käytetään autentikointialgoritmin yhtenä parametrinä. Autentikointialgoritmin tulos palautetaan verkkoon, jossa sen validiteetti tarkistetaan vertaamalla sen arvoa verkossa laskettuun vertailuarvoon.

SIM on tunnetun tekniikan mukaisissa GSM (Global System for Mobile Communications) –radiojärjestelmissä fyysinen älykortti, jolle on tallennettu pysyvästi tilaajaa koskevia tunnistetietoja sekä autentikointialgoritmit. UMTS (Universal Mobile Telecommunications System) –järjestelmissä käytetään SIM-kortin sijasta UICC (Universal Integrated Circuit Card) –korttia, joka käsittää USIM (UMTS Subscriber Identity Module) –sovelluksen. UMTS-järjestelmissä SIM on esimerkiksi UICC-kortin eräs sovellus. Kolmannen sukupolven pakettikytkentäisissä multimediaradiojärjestelmissä, kuten IMS (IP Multimedia Subsystem) –järjestelmissä, käytetään UICC-kortissa ISIM (IMS Subscriber Identity Module) –sovellusta.

GSM-järjestelmän SIM-kortin avulla ei tunnetun tekniikan mukaisissa ratkaisuissa saavuteta yhtä luotettavaa autentikointia kuin UICC-kortin ja sen käsittämän USIM-sovelluksen avulla. SIM- ja USIM-spesifikaatioissa käytetyt algoritmit eroavat toisistaan esimerkiksi eheyden tarkistamisen ja keskinäisen autentikoinnin osalta. On kuitenkin syntynyt tarve luotettavasti käyttää

IMS-järjestelmän tarjoamia palveluita myös GSM-järjestelmän SIM-korttipohjaista tilaajapäätelaitetta käyttämällä. Myös IMS-spesifisiä parametrejä, joita ISIM-sovellus mahdollistaa, kaivataan GSM-järjestelmän SIM:lle.

Lyhyt selostus

Keksinnön tavoitteena on tarjota parannettu menetelmä tilaajapäätelaitteen autentikointiin pakettikytkentäisessä multimediaradiojärjestelmässä ja parannettu autentikointijärjestely. Keksinnön eräänä puolena esitetään menetelmä tilaajapäätelaitteen autentikointiin pakettikytkentäisessä multimediaradiojärjestelmässä, joka menetelmä käsittää: vastaanotetaan tilaajapäätelaitteessa pakettikytkentäisestä multimediaradiojärjestelmästä lähetetty autentikointipyyntö, joka käsittää pakettikytkentäisen multimediaradiojärjestelmän autentikointiparametrejä; ja lähetetään tilaajapäätelaitteesta autentikointivastaus pakettikytkentäiseen multimediaradiojärjestelmään. Keksinnön mukaisessa menetelmässä autentikointipyynnön vastaanottamisen ja autentikointivastauksen lähettämisen välissä menetelmä käsittää lisäksi: muodostetaan tilaajapäätelaitteessa SMS (short message service)-viesti, johon vastaanotetut autentikointiparametrit sijoitetaan; lähetetään muodostettu SMS-viesti GSM:n (Global System for Mobile Communications) SIM (subscriber identity module)-kortille; generoidaan GSM:n SIM-kortilla vastaanotetun SMS-viestin sekä GSM:n SIM-kortille tallennetun autentikointiavaimen ja pakettikytkentäisen multimediaradiojärjestelmän autentikointialgoritmin perusteella pakettikytkentäisen multimediaradiojärjestelmän vastausparametrit; muodostetaan tilaajapäätelaitteessa autentikointivastaus GSM:n SIM-kortilta vastaanotettujen pakettikytkentäisen multimediaradiojärjestelmän vastausparametrien perusteella.

Keksinnön eräänä puolena esitetään autentikointijärjestely, käsittäen: tilaajapäätelaitteen, joka käsittää lähetinvastaanottimen, joka lähetinvastaanotin on konfiguroitu vastaanottamaan pakettikytkentäisestä multimediaradiojärjestelmästä lähetetty autentikointipyyntö, joka autentikointipyyntö käsittää pakettikytkentäisen multimediaradiojärjestelmän autentikointiparametrejä, ja ohjausyksikön tilaajapäätelaitteen toimintojen ohjaamiseksi, joka ohjausyksikkö tilaajapäätelaitteen toimintojen ohjaamiseksi on konfiguroitu lähettämään autentikointivastaus pakettikytkentäiseen multimediaradiojärjestelmään; ja tilaajapäätelaitteeseen liitetyn GSM:n (Global System for Mobile Communications) SIM (subscriber identity module)-kortin, joka käsittää ohjausyksikön GSM:n SIM-kortin toimintojen ohjaamiseksi, ja muistin autentikointiavaimen ja autentikointialgoritmin tallentamiseksi. Keksinnön mukaisessa järjestelyssä tilaajapää-

telaitteen ohjausyksikkö on lisäksi konfiguroitu muodostamaan SMS (short message service)-viesti, joka käsittää vastaanotetun autentikointipyynnön käsittämät pakettikytkentäisen multimediaradiojärjestelmän autentikointiparametrit, lähettämään GSM:n SIM-kortille muodostettu SMS-viesti, ja muodostamaan autentikointivastaus GSM:n SIM-kortilta vastaanotettujen pakettikytkentäisen multimediajärjestelmän vastausparametrien perusteella; ja GSM:n SIM-kortin ohjausyksikkö on lisäksi konfiguroitu generoimaan pakettikytkentäisen multimediaradiojärjestelmän vastausparametrit vastaanotetun SMS-viestin sekä GSM:n SIM-kortille tallennetun autentikointiavaimen ja pakettikytkentäisen multimediaradiojärjestelmän autentikointialgoritmin perusteella.

Keksinnön edullisia suoritusmuotoja kuvataan epäitsenäisissä patenttivaatimuksissa.

Keksinnön mukaisella menettelyllä saavutetaan useita etuja. GSM:n SIM-korttia käyttävän tilaajapäätelaitteen autentikoinnin luotettavuus kasvaa. Menettely on myös helposti toteutettavissa. Menettelyn avulla GSM-järjestelmän SIM-korttia käyttävällä tilaajapäätelaitteella voidaan turvallisesti käyttää pakettikytkentäisen multimediaradiojärjestelmän palveluita.

Kuvioluettelo

Keksintöä selostetaan nyt lähemmin edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirroksiin, joissa

kuvio 1 kuvaa esimerkkiä tietoliikennejärjestelmän rakenteesta,

kuvio 2 esittää tilaajapäätelaitteen ja SIM-kortin yhdistelmää,

kuvio 3 esittää esimerkkiä SIM-kortin rakenteesta ja

kuvio 4 on signaalinsekvenssikaavio havainnollistaen menetelmää tilaajapäätelaitteen autentikointiin pakettikytkentäisessä multimediaradiojärjestelmässä.

Suoritusmuotojen kuvaus

Tarkastellaan kuvion 1 esimerkkiä eräästä radiojärjestelmästä, jossa keksinnön edullisia suoritusmuotoja voidaan soveltaa. Kuvio 1 havainnollistaa UMTS (Universal Mobile Telecommunications System) –järjestelmän rakennetta. Suoritusmuodot eivät kuitenkaan rajaudu vain näissä esimerkeissä kuvattaviin järjestelmiin, vaan alan ammattilainen voi soveltaa keksinnön mukaista ratkaisua myös muissa järjestelmissä.

Yleisellä tasolla radiojärjestelmän voidaan määritellä muodostuvan päätelaitteista ja verkko-osasta, joka sisältää radiojärjestelmän kiinteän infra-

struktuurin eli runkoverkon, radioliityntäverkon ja tukiasemajärjestelmän. Tilaajapäätelaitteet 100 voivat olla esimerkiksi käyttäjälaitteita tai matkapuhelimia.

Tilaajapäätelaite 100 on radioyhteydessä 102 radioliityntäverkkoon 104 (RAN, Radio Access Network), jonka kautta se on yhteydessä runkoverkon eri alijärjestelmiin 110, 120, 140, joita kuviossa 1 havainnollistetaan katkoviivoilla rajatuilla alueilla. Radioliityntäverkko 104 tukee alijärjestelmien 110, 120, 140 kautta tulevia palveluja.

Kuviossa 1 pakettikytkentäisestä tiedonsiirrosta vastaa PS_CN (Packet Switched Core Network) –järjestelmä 110, joka toteutetaan tyypillisesti GPRS (General Radio Packet System) –pohjaisena järjestelmänä. GPRS (General Radio Packet System) –verkko puolestaan toteutetaan Internet protokolla (IP, Internet Protocol) -pohjaisena verkkona, missä datapaketteja siirretään eri GPRS–verkkoelementtien välillä. PS_CN –järjestelmän 110 elementit operointisolmu (Serving GPRS Support Node, SGSN) 112 ja yhdyskäytäväsolmu (Gateway GPRS Support Node, GGSN) 114 vastaavat pakettikytkentäisten yhteyksien toteuttamisesta. Operointisolmu 112 on GPRS-runkoverkon pakettikytkentäpuolen keskipiste, ja sen päätehtävänä on lähettää ja vastaanottaa paketteja pakettikytkentäistä siirtoa tukevan tilaajapäätelaitteen 100 kanssa radioliityntäverkkoa 104 käyttäen. Operointisolmu 112 sisältää tilaajapäätelaitetta 100 koskevaa tilaajatietoa sekä sijaintitietoa. Se varastoi jokaisesta sen kanssa yhteydessä olevasta tilaajapäätelaitteesta erilaisia parametreja, joita käytetään pakettien reitittämiseen, esimerkiksi tietoja tilaajapäätelaitteen sijainnista. Yhdyskäytäväsolmu 114 reitittää GPRS-runkoverkosta 110 ulkopuolisiin verkkoihin, kuten Internettiin, ulosmenevän liikenteen.

CS_CN (Circuit Swiched Core Network) –järjestelmä 120 vastaa piirikytkentäisestä tiedonsiirrosta. CS_CN –järjestelmän 120 elementit MSC-palvelin (mobile services switching centre server) 122 ja yhdyskeskus (GMSC, gateway MSC) 126 vastaavat puhelunohjauksesta sekä liikkuvuuden ohjauksesta. Mediayhdyskäytävä (MGW, Media Gateway) 128 toteuttaa matkapuhelinkeskuksen (MSC, Mobile Switching Centre) 124 käyttäjätason toiminnot. Mediayhdyskäytävä 128 on yleisen matkapuhelinverkon (PLMN, Public Land Mobile Network) ja yleisen kiinteän puhelinverkon (PSTN, Public Switched Telephone Network) päätepiste tietylle verkolle.

IMS (IP Multimedia Subsystem) –järjestelmä 140 käsittää runkoverkkoelementit IP-multimediapalveluiden mahdollistamiseksi. Sellaiset palvelut vaativat IP-pohjaisen puhelunohjausprotokollan, kuten SIP-protokollan, tu-

kea. SIP (Session Initiation Protocol) on ohjausprotokolla istuntojen muodostamiseen, muokkaamiseen ja päättämiseen yhden tai useamman osapuolen välillä. IMS–järjestelmä 140 käyttää kotitilaajapalvelimen (HSS, Home Subscriber Server) 130 palveluita, ja se käsittää CSCF:n (Call State Control Function) 142. Lisäksi IMS-järjestelmä 140 voi käsittää muita elementtejä, joita ei ole kuvattu kuviossa 1, esimerkiksi puhelunohjauspalvelin (CPS, Call Prosessing Server) ja IP telephony gateway. IMS-järjestelmää 140 on kuvattu tarkemmin esimerkiksi julkaisussa: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2; Release 5 (3GPP, TS 23.228, V5.5.0).

Kotitilaajapalvelin 130 on tietyn tilaajan isäntätietokanta, jota käytetään mm. ylläpitämään listaa tilaajaan liittyvistä ominaisuuksista ja palveluista ja seuraamaan tilaajan sijaintia. Kotitilaajapalvelin vastaa samoista toiminnoista kuin kotirekisteri (HLR, Home Location Register), mutta se myös kommunikoi IP–pohjaisten rajapintojen kautta. Lisäksi kotitilaajapalvelin vastaa UMS (User Mobility Server) –toiminnoista. UMS osallistuu liikkuvuuden hallintaan, sijainnin selvittämiseen ja autentikointiin. UMS toteuttaa myös DNS (Domain Name Server)-palveluita.

CSCF (Call State Control Function) 142 vastaa istuntojen (session) reitittämisestä. CSCF käynnistää istunnoille tulevat palvelut, kuten istuntojen seulonnan, ja suorittaa käynnissä olevien istuntojen ohjausta. CSCF 142 voi kuulua puhelunohjauspalvelimeen (CPS, Call Prosessing Server), joka huolehtii puheluiden signaloinnista verkkoelementtien välillä. CSCF 142 käsittää elementit S-CSCF (Serving Call State Control Function) ja I-CSCF (Interrogating Call State Control Function). S-CSCF huolehtii tilaajapäätelähtöisistä yhteyksistä ja tukee tilaajapäätelaitteisiin päättyviä yhteyksiä. I-CSCF puolestaan vastaa tilaajapäätelaitteisiin päättyvistä yhteyksistä ja määrittelee kuinka tilaajapäätelaitteisiin päättyvät istunnot reititetään. I-CSCF kyselee kotitilaajapalvelimelta (HSS, home subscribe server) tietoja, jotka mahdollistavat istunnon ohjaamisen palvelevalle CSCF:lle.

UMTS-järjestelmissä, kuten IMS (Internet Protocol Multimedia Subsystem)-järjestelmässä, tilaajapäätelaitteen 100 autentikoinnissa tarkistetaan tilaajan identiteetti, mutta sen lisäksi myös tilaajapäätelaite 100 tarkistaa, että tilaajan kotiverkko on oikeuttanut verkon tekemään sen. Autentikoinnin kulmakivi on autentikointiavain (Ki, Shared Secret Key), jonka SIM-kortti sekä UMTS-järjestelmän tiedostot jakavat. Autentikointiavainta ei koskaan siirretä paikasta

toiseen eikä esimerkiksi tilaajapäätelaitteen 100 käyttäjällä ole tietoa omasta autentikointiavaimestaan. Autentikaatioavain ei ole luettavissa ulkoapäin eikä sitä voida muuttaa. Samanaikaisesti autentikoinnin kanssa muodostetaan myös salaus- ja eheysavaimet. Uudet salaus- ja eheysavaimet muodostetaan autentikointiavaimen perusteella jokaisen autentikointitapahtuman aikana.

Autentikointi alkaa, kun käyttäjän identiteetti, IMSI (International Mobile Subscriber Identity) tai TMSI (Temporary Mobile Subscriber Identity), on lähetetty esimerkiksi IMS-järjestelmän operointisolmulle 112. Operointisolmu 112 lähettää silloin autentikointidatapyynnön kotitilaajapalvelimelle 130. Kotitilaajapalvelimessa 130 on käyttäjän autentikointiavain ja IMSI:n perusteella saadun tiedon perusteella IMS-järjestelmässä muodostetaan käyttäjälle autentikointivektoreita, jotka lähetetään takaisin operointisolmulle 112 autentikointidatavasteen muodossa. Operointisolmu 112 lähettää seuraavaksi autentikointipyynnön tilaajapäätelaitteelle 100. Autentikointipyyntö käsittää esimerkiksi autentikointivektorin autentikointiparametrit: satunnaisluku RAND ja AUTN (Authentication Token).

Eräässä suoritusmuodossa vastaanotetaan päätelaitteessa 100 pakettikytkentäisestä multimediaradiojärjestelmästä lähetetty autentikointipyyntö, joka käsittää pakettikytkentäisen multimediaradiojärjestelmän autentikointiparametrejä. Pakettikytkentäinen multimediaradiojärjestelmä on esimerkiksi IMS-järjestelmä. Seuraavaksi päätelaitteessa 100 muodostetaan SMS (Short Message Service)-viesti, johon on sijoitettu vastaanotetut autentikointiparametrit. Muodostettu SMS-viesti lähetetään GSM (Global System for Mobile Communications) –järjestelmän, esimerkiksi toisen sukupolven mukainen GSM-järjestelmä, mukaiselle SIM (Subscriber Identity Module) –kortille.

GSM:n SIM-kortilla generoidaan vastaanotetun SMS-viestin sekä GSM:n SIM-kortille tallennetun autentikointiavaimen ja pakettikytkentäisen multimediaradiojärjestelmän autentikointialgoritmin perusteella pakettikytkentäisen multimediaradiojärjestelmän vastausparametrit.

Pakettikytkentäisen multimediajärjestelmän autentikointialgoritmi on etukäteen tallennettu GSM:n SIM-kortille. Erään suoritusmuodon mukaan autentikointialgoritmi on ladattu GSM:n SIM-kortille SIM-kortin varmentajan kirjoituslaitteen avulla. Vaihtoehtoisesti autentikointialgoritmi ladataan radiorajapinnan yli suoritettavalla viestinnällä. Autentikointialgoritmin lataaminen voidaan suorittaa esimerkiksi sinänsä tunnetulla OTA (Over-The-Air)-menetelmällä. OTA-menetelmässä radiojärjestelmä lähettää tilaajapäätelaitteelle 100 yhden

tai useamman SIM-spesifisen SMS-viestin käsittäen autentikointialgritmin. Sen jälkeen tilaajapäätelaite 100 lähettää SIM-kortille SMS-viestin esimerkiksi SAT (SIM Application Toolkit) –ohjauskomennon, kuten ENVELOPE-komennon, parametrinä. SAT (SIM Application Toolkit) käsittää SIM-kortin sovelluksia, ja sitä on tarkemmin kuvattu GSM:n teknisissä spesifikaatioissa, esimerkiksi julkaisussa: 3rd Generation Partnership Project; Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface, Release 1999 (3GPP TS 11.14 V8.11.0). SAT on tarkoitettu SIM-kortilla olevien sovellusten ja tilaajapäätelaitteen väliseen kommunikointiin.

Vastaanottamiensa autentikointiparametrien, pakettikytkentäisen multimediaradiojärjestelmän autentikointialgoritmin sekä autentikointiavaimen avulla SIM-kortti suorittaa laskennan, joka vastaa pakettikytkentäisessä multimediaradiojärjestelmässä suoritettavaa autentikointivektorien laskentaa. Vastausparametrien muodostamisen jälkeen päätelaitteessa 100 muodostetaan autentikointivastaus GSM:n SIM-kortilta vastaanotettujen pakettikytkentäisen multimediaradiojärjestelmän vastausparametrien perusteella ja lähetetään autentikointivastaus pakettikytkentäiseen multimediaradiojärjestelmään.

Pakettikytkentäisessä multimediaradiojärjestelmässä autentikointivastausta verrataan odotettuun vastaukseen XRES, joka on osa autentikointivektoria. Jos yhteensopivuus todetaan, autentikointi päättyy positiivisesti.

Radiojärjestelmän salaus- ja eheysavaimet, CK (Cipherkey) ja IK (Integrity Key), muodostetaan autentikointimenetelmän sivutuotteena. SIM-kortti voi laskea salaus- ja eheysavaimet esimerkiksi sen jälkeen kun se on saanut autentikointiparametrit ja varmentanut ne. Näitä väliaikaisia avaimia siirretään SIM-kortilta tilaajapäätelaitteeseen, missä salaus- ja eheyssuojausalgoritmeja sovelletaan.

Tarkastellaan seuraavaksi kuvion 2 esittämää autentikointijärjestelyä 200. Autentikointijärjestely 200 käsittää tilaajapäätelaitteen 100 sekä tilaajapäätelaitteeseen liitetyn GSM:n SIM-kortin 210.

Tilaajapäätelaite 100 käsittää lähetinvastaanottimen 204, joka on konfiguroitu vastaanottamaan pakettikytkentäisestä multimediaradiojärjestelmästä lähetetty autentikointipyyntö, joka autentikointipyyntö käsittää pakettikytkentäisen multimediaradiojärjestelmän autentikointiparametrejä. Tilaajapäätelaite 100 käsittää myös ohjausyksikön 202 tilaajapäätelaitteen 100 toimintojen ohjaamiseksi, joka ohjausyksikkö 202 on konfiguroitu lähettämään autentikointivastaus pakettikytkentäiseen multimediaradiojärjestelmään. Kuviossa 2

esitettävä tilaajapäätelaite 100 käsittää myös käyttöliittymäosan 208, jonka avulla laitteen käyttäjä voi käyttää laitetta sekä antennin 206, jonka välityksellä lähetinvastaanotin 204 vastaanottaa ja lähettää signaaleja radiotielle.

Tilaajapäätelaitteen 100 yhteydessä oleva SIM-kortti 210 on älykortti, jota kutsutaan myös tilaajan tunnistusyksiköksi. Siihen on talletettu pysyvästi tilaajaa koskevia tunnistetietoja sekä autentikointialgoritmeja ja siihen voidaan tallentaa muuttuvina tietoina puhelinnumeroita ja lyhytsanomia. SIM-kortti 210 identifioi tilaajapäätelaitteen 100 verkolle. Autentikoinnissa tarkistetaan SIM-kortin 210 validiteetti ja se, onko kyseisellä SIM-kortilla lupa tietyn verkon palveluihin. Kuvion 2 esittämä GSM:n SIM-kortti 210 käsittää ohjausyksikön 300, joka ohjaa SIM-kortin toimintoja. GSM:n SIM-kortissa 210 on myös muisti 306, jolle autentikointiavain sekä autentikointialgoritmit tallennetaan. Eräässä keksinnön suoritusmuodossa GSM:n SIM-kortti 210 käsittää SAT:n (SIM Application Toolkit) 308 ja autentikointialgoritmit tallennetaan muistissa 306 sijaitsevaan SAT:iin 308.

Tilaajapäätelaitteen 100 ja SIM-kortin 210 ohjausyksiköillä 202, 300 tarkoitetaan laitteiden toimintaa ohjaavia lohkoja, jotka nykyisin toteutetaan yleensä prosessorina ohjelmistoineen, mutta myös erilaiset laitteistototeutukset ovat mahdollisia, esimerkiksi erillisistä logiikkakomponenteista rakennettu piiri tai yksi tai useampi asiakaskohtainen integroitu piiri (Application-Specific Integrated Circuit, ASIC). Myös näiden eri toteutustapojen sekamuoto on mahdollinen. Toimenpiteiden kuvaama toiminnallisuus on siis toteutettavissa ohjausyksiköillä 210, 300.

Tilaajapäätelaitteen 100 ohjausyksikkö 202 on lisäksi konfiguroitu muodostamaan SMS-viesti, joka käsittää vastaanotetun autentikointipyynnön käsittämät pakettikytkentäisen multimediaradiojärjestelmän, kuten IMS–järjestelmän, autentikointiparametrit. Sen jälkeen tilaajapäätelaitteen 100 ohjausyksikkö 202 on konfiguroitu lähettämään GSM:n SIM-kortille 210 muodostettu SMS-viesti ja muodostamaan autentikointivastaus GSM:n SIM-kortilta 210 vastaanotettujen pakettikytkentäisen multimediajärjestelmän vastausparametrien perusteella.

GSM:n SIM-kortin 210 ohjausyksikkö 300 on lisäksi konfiguroitu generoimaan pakettikytkentäisen multimediaradiojärjestelmän vastausparametrit vastaanotetun SMS-viestin sekä GSM:n SIM-kortille tallennetun autentikointiavaimen ja pakettikytkentäisen multimediajärjestelmän autentikointialgoritmin perusteella.

Erään suoritusmuodon mukaan tilaajapäätelaitteen 100 GSM:n SIM-kortille 210 lähettämä SMS-viesti on SIM-kortin 210 SAT:lle 308 lähetettävä ohjauskomentoparametri. Erään suoritusmuodon mukaan GSM:n SIM-kortti 210 voi käsittää myös jonkun toisen ohjausprotokollan kuin SAT. Silloin GSM:n SIM-kortille 210 tilaajapäätelaitteelta 100 lähetettävä SMS-viesti on kyseiselle SIM-kortin ohjausprotokollalle lähetettävä ohjauskomentoparametri.

Kuviossa 3 on esitetty GSM:n SIM-kortti 210. Eräässä suoritusmuodoissa GSM:n SIM-kortti on esimerkiksi 2G GSM-järjestelmän mukainen SIM-kortti. GSM:n SIM-kortti 210 käsittää SIM-kortin 210 ohjausyksikön 300 SIM-kortin toimintojen ohjaamiseksi sekä muistin 302, 304, 306. SIM-kortin muisti jakaantuu työmuistiin (RAM, random access memory) 302, operointimuistiin (ROM, read only memory) sekä sovellusmuistiin (EEPROM, electronically erasable ROM) 306. Sovellusmuistia käytetään esimerkiksi puhelinnumeroiden muistipaikkoihin ja SMS-viestien vastaanottamiseen.

Myös SAT 308 tai vaihtoehtoisesti jokin muu ohjausprotokolla sijaitsee muistissa, esimerkiksi sovellusmuistissa 306. Keksinnön erään edullisen toteutusmuodon mukaan GSM:n SIM-kortti 210 on konfiguroitu tallentamaan etukäteen pakettikytkentäisen multimediaradiojärjestelmän autentikointialgoritmi ohjausyksikön 300 ohjaamana esimerkiksi SIM-kortin sovellusmuistiin 306. Pakettikytkentäisen multimediaradiojärjestelmän autentikointialgoritmi ladataan SIM-kortille 210 esimerkiksi SIM-kortin verkko-operaattorin toimesta kirjoituslaitteen avulla tai esimerkiksi radiorajapinnan yli suoritettavalla viestinnällä, kuten OTA-menetelmällä.

Tarkastellaan seuraavaksi kuvion 4 esimerkkiä tilaajapäätelaitteen autentikointimenetelmästä. Kuviossa 4 kuvaa ensimmäinen pystyviiva IMS 400 pakettikytkentäisestä multimediaradiojärjestelmästä, kuten IMS-järjestelmästä 400, lähtevää ja siihen päättyvää viestintää. Toinen pystyviiva UE 402 kuvaa puolestaan tilaajapäätelaitteen 402 viestintää ja laitteessa suoritettavia toimenpiteitä. Kolmas pystyviiva SIM 404 kuvaa GSM:n SIM-kortin viestintää ja SIM-kortissa suoritettavia toimenpiteitä.

Keksinnön eräässä suoritusmuodossa lähetetään 406:ssa IMS-järjestelmästä 400 tilaajapäätelaitteelle 402 autentikointipyyntö, joka käsittää IMS-järjestelmän 400 autentikointiparametrejä. Autentikointiparametrit ovat esimerkiksi AUTN (authentication token) ja satunnaisluku RAND. IMS-järjestelmän 400 ja tilaajapäätelaitteen 402 välisessä viestinnässä käytetään SIP (Session Initiation Protocol) -signalointia. 407:ssä tilaajapäätelaite 402 muo-

dostaa SMS-viestin, johon vastaanotetut autentikointiparametrit sijoitetaan. 408:ssa lähetetään 407:ssa muodostettu SMS-viesti GSM:n SIM-kortille 404. SMS-viesti lähetetään 408:ssa vaihtoehtoisesti GSM:n SIM-kortin 404 ohjausprotokollalle lähetettävänä ohjauskomentoparametrinä. SMS-viesti on esimerkiksi GSM:n SAT:lle lähetettävä ohjauskomentoparametri. SAT:lle lähetettävä ohjauskomento on esimerkiksi ENVELOPE-komento ja SMS-viesti autentikointiparametreineen on ohjauskomennon eräs parametri. Vaihtoehtoisesti jotain muuta kuin ENVELOPE-komentoa käytetään ohjauskomentona SAT:lle.

410:ssä generoidaan GSM:n SIM-kortilla 404 vastaanotetun SMS-viestin sekä GSM:n SIM-kortille tallennetun autentikointiavaimen ja IMS-järjestelmän autentikointialgoritmin perusteella IMS-järjestelmän vastausparametrit, kuten salausavain Kc (ciphering key) ja eheysavain IK (integrity key). Autentikointialgoritmin suorittaa GSM:n SIM-kortilla 404 esimerkiksi SAT tai vaihtoehtoisesti jokin muu ohjausprotokolla SMS-viestissä vastaanotettujen autentikointiparametrien avulla. 412:ssa lähetetään vastausparametrit GSM:n SIM-kortilta 404 tilaajapäätelaitteelle 402 esimerkiksi SAT:n ja tilaajapäätelaitteen 402 välisellä viestinnällä. 414:ssa muodostetaan tilaajapäätelaitteessa 402 autentikointivastaus GSM:n SIM-kortilta 404 vastaanotettujen IMS-järjestelmän 400 vastausparametrien perusteella. Autentikointivastauksen muodostamisessa 414:ssa käytetään esimerkiksi SAT:n Get Response –komentoa. Muodostettu autentikointivastaus lähetetään 416:ssa IMS-järjestelmälle 400.

Vaikka keksintöä on edellä selostettu viitaten oheisten piirustusten mukaiseen esimerkkiin, on selvää, ettei keksintö ole rajoittunut siihen, vaan sitä voidaan muunnella monin tavoin oheisten patenttivaatimusten esittämän keksinnöllisen ajatuksen puitteissa.

Patenttivaatimukset

1. Menetelmä tilaajapäätelaitteen autentikointiin pakettikytkentäisessä multimediaradiojärjestelmässä, joka menetelmä käsittää:

vastaanotetaan (406) tilaajapäätelaitteessa pakettikytkentäisestä multimediaradiojärjestelmästä lähetetty autentikointipyyntö, joka käsittää pakettikytkentäisen multimediaradiojärjestelmän autentikointiparametrejä; ja

lähetetään (416) tilaajapäätelaitteesta autentikointivastaus pakettikytkentäiseen multimediaradiojärjestelmään,

t u n n e t t u siitä, että autentikointipyynnön vastaanottamisen ja autentikointivastauksen lähettämisen välissä menetelmä käsittää lisäksi:

muodostetaan (407) tilaajapäätelaitteessa SMS (short message service)-viesti, johon vastaanotetut autentikointiparametrit sijoitetaan;

lähetetään (408) muodostettu SMS-viesti GSM:n (Global System for Mobile Communications) SIM (subscriber identity module)-kortille;

generoidaan (410) GSM:n SIM-kortilla vastaanotetun SMS-viestin sekä GSM:n SIM-kortille tallennetun autentikointiavaimen ja pakettikytkentäisen multimediaradiojärjestelmän autentikointialgoritmin perusteella pakettikytkentäisen multimediaradiojärjestelmän vastausparametrit;

muodostetaan (414) tilaajapäätelaitteessa autentikointivastaus GSM:n SIM-kortilta vastaanotettujen pakettikytkentäisen multimediaradiojärjestelmän vastausparametrien perusteella.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että pakettikytkentäinen multimediaradiojärjestelmä on IMS (Internet Protocol Multimedia Subsystem) –järjestelmä.

3. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että GSM:n SIM-kortille lähetettävä SMS-viesti on GSM:n SIM-kortin Application Toolkit:ille lähetettävä ohjauskomentoparametri.

4. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että GSM:n SIM-kortille lähetettävä SMS-viesti on SIM-kortin ohjausprotokollalle lähetettävä ohjauskomentoparametri.

5. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että pakettikytkentäisen multimediaradiojärjestelmän autentikointialgoritmi on etukäteen tallennettu GSM:n SIM-kortille jollakin seuraavista menetelmistä:

ladataan autentikointialgoritmi SIM-kortille SIM-kortin varmentajan kirjoituslaitteen avulla;

ladataan autentikointialgoritmi radiorajapinnan yli suoritettavalla viestinnällä.

6. Autentikointijärjestely (200), käsittäen:

tilaajapäätelaitteen (100), joka käsittää

lähetinvastaanottimen (204), joka lähetinvastaanotin on konfiguroitu vastaanottamaan pakettikytkentäisestä multimediaradiojärjestelmästä lähetetty autentikointipyyntö, joka autentikointipyyntö käsittää pakettikytkentäisen multimediaradiojärjestelmän autentikointiparametrejä, ja

ohjausyksikön (202) tilaajapäätelaitteen toimintojen ohjaamiseksi, joka ohjausyksikkö tilaajapäätelaitteen toimintojen ohjaamiseksi on konfiguroitu lähettämään autentikointivastaus pakettikytkentäiseen multimediaradiojärjestelmään; ja

tilaajapäätelaitteeseen liitetyn GSM:n (Global System for Mobile Communications) SIM (subscriber identity module)-kortin (210), joka käsittää

ohjausyksikön (300) GSM:n SIM-kortin toimintojen ohjaamiseksi, ja

muistin (302, 304, 306) autentikointiavaimen ja autentikointialgoritmin tallentamiseksi;

t u n n e t t u siitä, että:

tilaajapäätelaitteen (100) ohjausyksikkö (202) on lisäksi konfiguroitu muodostamaan SMS (short message service)-viesti, joka käsittää vastaanotetun autentikointipyynnön käsittämät pakettikytkentäisen multimediaradiojärjestelmän autentikointiparametrit, lähettämään GSM:n SIM-kortille (210) muodostettu SMS-viesti, ja muodostamaan autentikointivastaus GSM:n SIM-kortilta (210) vastaanotettujen pakettikytkentäisen multimediajärjestelmän vastausparametrien perusteella; ja

GSM:n SIM-kortin (210) ohjausyksikkö (300) on lisäksi konfiguroitu generoimaan pakettikytkentäisen multimediaradiojärjestelmän vastausparametrit vastaanotetun SMS-viestin sekä GSM:n SIM-kortille tallennetun autentikointiavaimen ja pakettikytkentäisen multimediaradiojärjestelmän autentikointialgoritmin perusteella.

7. Patenttivaatimuksen 6 mukainen järjestely, t u n n e t t u siitä, että pakettikytkentäinen multimediaradiojärjestelmä on IMS (Internet Protocol Multimedia Subsystem) –järjestelmä.

8. Patenttivaatimuksen 6 mukainen järjestely, t u n n e t t u siitä, että GSM:n SIM-kortti (210) käsittää SIM-kortin Application Toolkit:in (308) ja

GSM:n SIM-kortille lähetettävä SMS-viesti on SIM-kortin Application Toolkit:lle lähetettävä ohjauskomentoparametri.

9. Patenttivaatimuksen 6 mukainen järjestely, t u n n e t t u siitä, että GSM:n SIM-kortti (210) käsittää SIM-kortin ohjausprotokollan ja GSM:n SIM-kortille lähetettävä SMS-viesti on SIM-kortin ohjausprotokollalle lähetettävä ohjauskomentoparametri.

10. Patenttivaatimuksen 6 mukainen järjestely, t u n n e t t u siitä, että GSM:n SIM-kortti (210) on konfiguroitu tallentamaan etukäteen pakettikytkentäisen multimediaradiojärjestelmän autentikointialgoritmi SIM-kortin varmentajan kirjoituslaitteen avulla tai radiorajapinnan yli suoritettavalla viestinnällä.

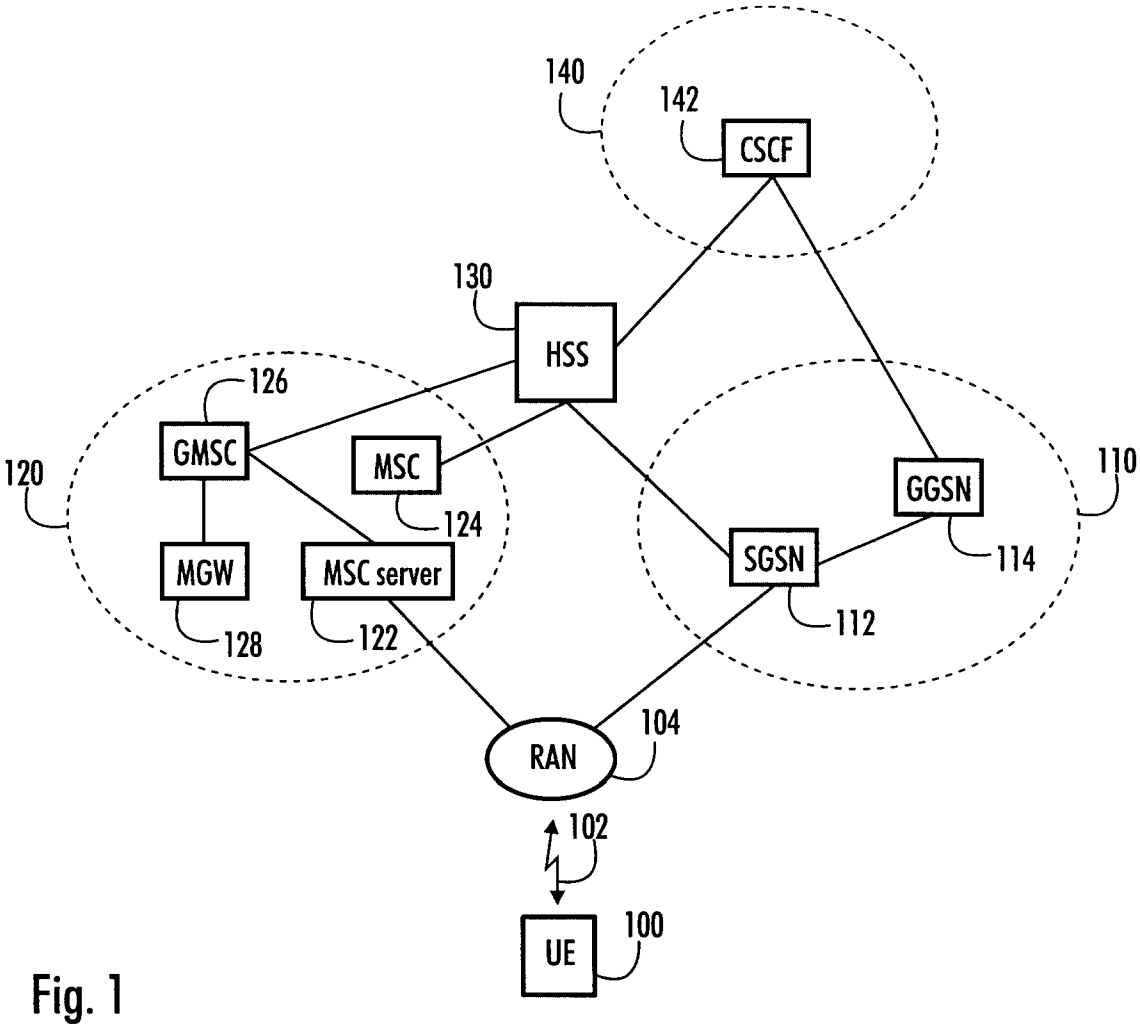
140
142
CSCF
130
HSS
126
GMSC
MSC
124
120
110
GGSN
114
MGW
MSC server
SGSN
128
122
112
104
RAN
102
100
UE

Fig. 1

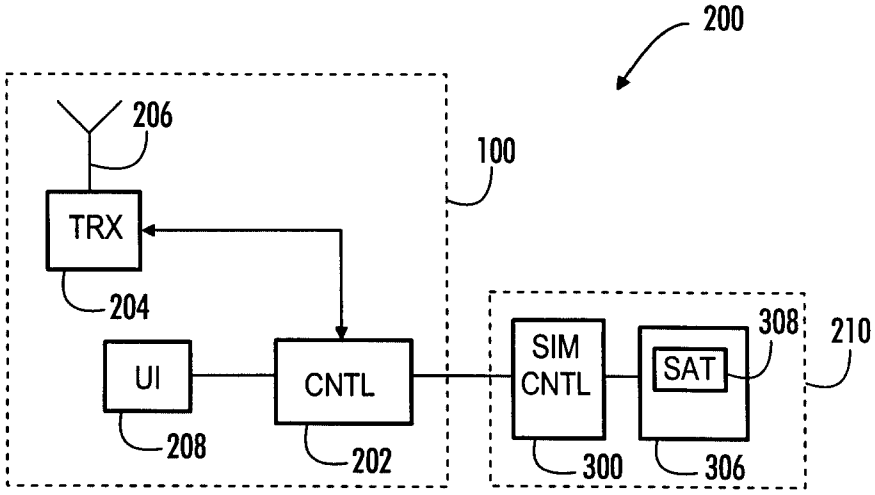
200
206
100
TRX
204
UI
CNTL
208
202
SIM
CNTL
SAT
308
210
300
306

Fig. 2

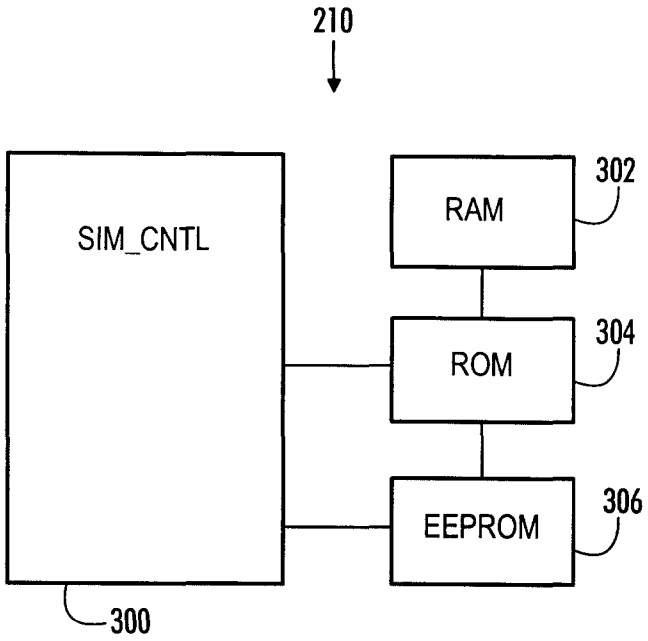
210
SIM_CNTL
RAM
302
ROM
304
EEPROM
306
300

Fig. 3

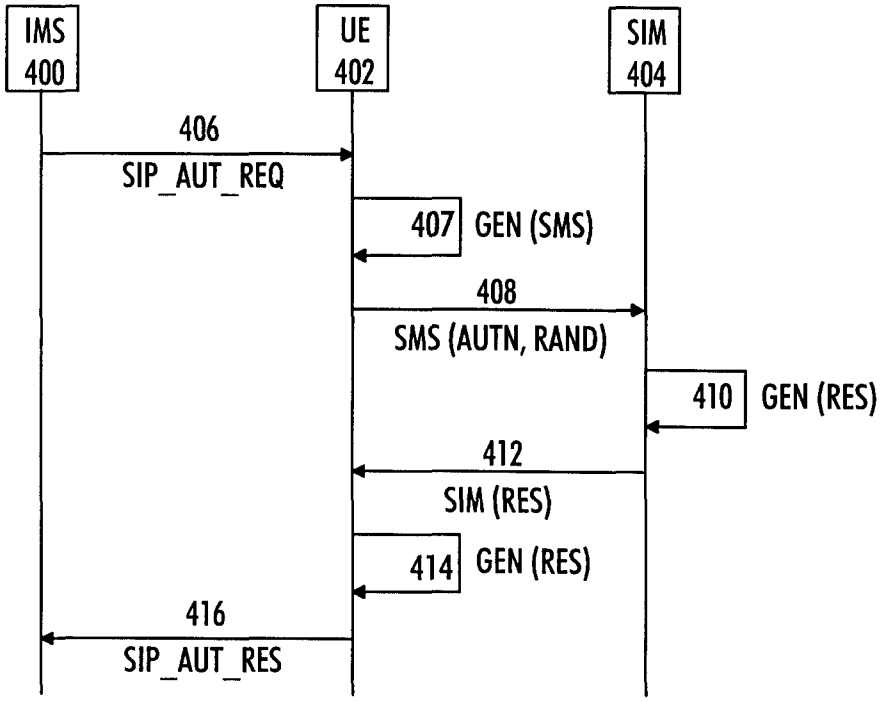
IMS
400
UE
402
SIM
404
406
SIP_AUT_REQ
407
GEN (SMS)
408
SMS (AUTN, RAND)
410
GEN (RES)
412
SIM (RES)
414
GEN (RES)
416
SIP_AUT_RES

Fig. 4