FI0001059658

(12) **PATENTTIJULKAISU**
PATENTSKRIFT

(10) **FI 105965 B**

(45) Patentti myönnetty - Patent beviljats **31.10.2000**

(51) Kv.lk.7 - Int.kl.7
H04L 9/32, 12/46, 29/06

(21) Patenttihakemus - Patentansökning **981564**

(22) Hakemispäivä - Ansökningsdag **07.07.1998**

(24) Alkupäiva - Löpdag **07.07.1998**

(41) Tullut julkiseksi - Blivit offentlig **08.01.2000**

SUOMI – FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN

(73) Haltija - Innehavare

1 •Nokia Networks Oy, Helsinki, Keilalahdentie 4, 02150 Espoo, SUOMI - FINLAND, (FI)

(72) Keksijä - Uppfinnare

1 •Verkama, Markku, Hakamäki 2 A 12, 02120 Espoo, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud: Patenttitoimisto Compatent Oy
Pitkänsillanranta 3 B, 00530 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning

Autentikointi tietoliikenneverkosssa
Autentisering i telekommunikationsnät

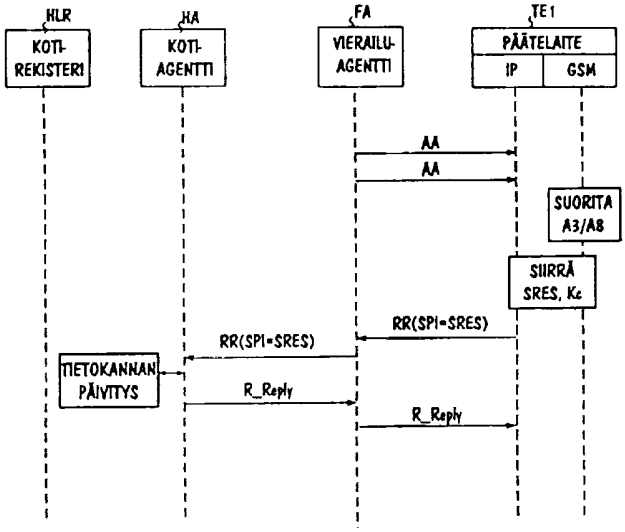
(56) Viitejulkaisut - Anförda publikationer

EP A 0912017 (H04L 12/56, Lucent Technologies Inc., sivu 8 rivi 36 - rivi 58, sivu 15 rivi 58 - sivu 17 rivi 23, sivu 20 rivi 16 - sivu 21 rivi 1, sivu 23 rivi10 - rivi 12)

(57) Tiivistelmä - Sammandrag

Keksintö koskee tietoliikenneverkkoa, erityisesti IP-verkkoa varten tarkoitettua autentikointimenetelmää. Verkon päätelaitteelta (TE1) lähetetään verkolle ensimmäinen sanoma (RR), joka sisältää autentikaattorin ja tietoyksikön, joka sisältää autentikaattorin muodostamistapaan liittyvää tietoa. Autentikoinnin suorittamiseksi verkossa määritetään ensimmäisen sanoman sisältämän tietoyksikön perusteella tarkastusarvo, jota verrataan mainittuun autentikaattoriin. Jotta päätelaitteen ei tarvitsisi suorittaa monimutkaista ja raskasta sanomanvaihtoa kytkeytyessään verkkoon ja silti saataisiin halutut turvaominaisuudet käyttöön, päätelaitteessa käytetään sellaista tunnistusyksikköä, jolle syötteenä annetusta haasteesta voidaan määrittää vaste ja avain oleellisesti samalla tavalla kuin tunnetun matkaviestinjärjestelmän tilaajan tunnistusyksikössä, verkkoon generoidaan joukko autentikointitietolohkoja, joista kukin sisältää haasteen, vasteen ja avaimen, jolloin generointi suoritetaan samalla tavalla kuin mainitussa matkaviestinjärjestelmässä, päätelaitteelle välitetään ainakin osa autentikointitietolohkojen sisältämistä haasteista, päätelaitteella valitaan yksi haasteista käyttöön ja sen perusteella määritetään päätelaitteen tunnistusyksikön avulla vaste ja käyttöön otettava avain, mainitussa ensimmäisessä sanomassa (RR) ilmoitetaan verkolle mainitun tietoyksikön avulla, mitä haastetta vastaava avain on valittu, ja ensimmäisen sanoman autentikaattori ja mainittu tarkastusarvo määritetään valitun avaimen avulla.

Uppfinningen avser ett autenticeringsförfarande som är avsett för telekommunikationsnät, särskilt för IP-nät. Från en terminal (TE1) i nätet sänds ett första meddelande (RR) som innehåller en autenticerare och en dataenhet, som innehåller data om det sätt på vilket autenticeraren har bildats, till nätet. I nätet bestäms ett kontrollvärde, som jämförs med nämnda autenticerare, på basis av den i det första meddelandet ingående dataenheten för utföring av autenticeringen. För att terminalen inte skall behöva utföra komplicerad och tung meddelandeväxling vid uppkoppling mot nätet och för att man ändå skall få önskade säkerhetsegenskaper i bruk, används i terminalen en identifieringsenhet i fråga om vilken i en utmaning som givits åt denna som input kan bestämmas svar och nyckel väsentligen på samma sätt som i den abonnentidentifieringsenhet som används i det kända mobilkommunikationssystemet, genereras ett antal autenticeringsinformationsblock, som vart och ett innehåller en utmaning, ett svar och en nyckel, i nätet, varvid genereringen utförs på samma sätt som i nämnda mobilkommunikationssystem, förmedlas åtminstone en del av utmaningarna i autenticeringsinformationsblocken till terminalen, väljs en av utmaningarna för att användas med terminalen och bestäms ett svar och vilken nyckel kommer att tas i bruk på basis av denna, med hjälp av terminalens identifieringsenhet, meddelas till nätet i nämnda första meddelande (RR), med hjälp av nämnda dataenhet, mot vilken utmaning svarande nyckel har valts och bestäms en autenticerare för det första meddelandet och nämnda kontrollvärde med hjälp av den valda nyckeln.



Autentikointi tietoliikenneverkossa

Keksinnön ala

Keksintö liittyy yleisesti autentikoinnin toteuttamiseen tietoliikenneverkossa, erityisesti IP-verkossa (IP=Internet Protocol). Autentikoinnilla tarkoitetaan tietoa generoineen osapuolen, kuten tilaajan, identiteetin todennusta. Autentikoinnin avulla voidaan myöskin taata kyseisen tiedon eheys (integrity) ja luottamuksellisuus (confidentiality). Autentikointi voidaan suorittaa erilaisia tarkoitusperiä, kuten verkkopalvelujen käyttöoikeuksien tarkistamista varten. Keksintö on tarkoitettu käytettäväksi erityisesti liikkuvien päätelaitteiden yhteydessä, mutta keksinnön mukaista ratkaisua voidaan käyttää myös kiinteiden päätelaitteiden yhteydessä.

Keksinnön tausta

Eräs televiestinnän nykyisistä suuntauksista on erilaisten liikkuvien päätelaitteiden, kuten kannettavien tietokoneiden (laptops), PDA-laitteiden (Personal Digital Assistant) tai älypuhelimien yleistyminen.

Perinteisissä IP-verkoissa eivät liikkuvat käyttäjät ole voineet vastaanottaa dataa oman IP-aliverkkonsa ulkopuolella, koska verkon reitittimet eivät ole pystyneet välittämään tietosähkeitä käyttäjän uuteen sijaintipaikkaan. Koska tämä rajoittaa oleellisesti kannettavien päätelaitteiden käytettävyyttä, on IP-protokollaan kehitetty liikkuvuutta tukevia ominaisuuksia. Mobile IP-protokolla (jatkossa MIP) on mekanismi, jolla hallitaan käyttäjän liikkuvuutta eri IP-aliverkkojen välillä. MIP on olemassa olevan IP:n versio, joka tukee päätelaitteen liikkuvuutta.

MIP perustuu siihen, että kullakin liikkuvalla tietokoneella tai solmulla (mobile host, mobile node) on sille osoitettu agentti ("kotiagentti", home agent), joka välittää paketit liikkuvan solmun sen hetkiseen sijaintipaikkaan. Kun liikkuva solmu liikkuu aliverkosta toiseen, se rekisteröityy kyseistä aliverkkoa palvelevalle agentille ("vierailuagentti", foreign agent). Viimemainittu suorittaa tarkistuksia liikkuvan solmun kotiagentin kanssa, rekisteröi liikkuvan solmun ja lähettää sille rekisteröinti-informaation. Liikkuvalle solmulle osoitetut paketit lähetetään liikkuvan solmun alkuperäiseen sijaintipaikkaan (kotiagentille omaan aliverkkoon), josta ne välitetään edelleen sen hetkiselle vierailuagentille, joka lähettää ne edelleen liikkuvalle solmulle. Koska esillä oleva keksintö ei liity MIPiin, ei protokollaa kuvata tässä yhteydessä tarkemmin. MIP-periaatetta

kuvataan esim. RFC 2002:ssa, October 1996 (Request For Comments) tai artikkelissa Upkar Varshney, *Supporting Mobility with Wireless ATM*, Internet Watch, January 1997, joista kiinnostunut lukija löytää halutessaan taustainformaatiota.

Kuten edellä mainittiin, rekisteröinti suoritetaan kotialiverkossa sijaitsevan kotiagentin kanssa aina silloin, kun käyttäjä vierailee jossakin muussa IP-aliverkossa. Rekisteröinnin yhteydessä kotiagentti autentikoi käyttäjän. Toisin sanoen, kotiagentti varmistaa rekisteröintipyynnön lähettäneen osapuolen identiteetin.

Autentikoinnissa tarvittavien avaimien hallinta on kuitenkin Internetissä vaikea ongelma. Verkon tietoturvaominaisuuksien parantamiseksi on kehitetty erilaisia järjestelmiä, joiden avulla käyttäjät voivat lähettää tiedon salattuna vastakkaiselle osapuolelle. Eräs tällainen järjestelmä on Kerberos, joka on palvelu, jonka avulla verkon käyttäjät ja palvelut voivat autentikoida toisensa ja jonka avulla käyttäjät ja palvelut voivat luoda väliinsä salattuja tiedonsiirtoyhteyksiä. Tällaiset järjestelmät on kuitenkin tarkoitettu lähinnä kiinteille päätelaitteille, ne ovat monimutkaisia ja raskaita ja vaativat joko etukäteen suoritettua rekisteröintiä ko. järjestelmien käyttäjiksi tai ainakin raskasta kommunikointia osapuolten välillä ennen kuin päätelaite pääsee lähettämään varsinaista hyötyinformaatiota.

Keksinnön yhteenveto

Keksinnön tarkoituksena on päästä eroon edellä kuvatusta epäkohdasta ja saada aikaan ratkaisu, jonka avulla päätelaite pystyy aloittamaan hyötyliikenteen nopeasti sen jälkeen, kun se on kytkeytynyt verkkoon.

Tämä päämäärä saavutetaan ratkaisulla, joka on määritelty itsenäisissä patenttivaatimuksissa.

Keksinnössä käytetään matkaviestinverkon yhteydestä tunnettua menettelyä verkon ja verkossa olevan päätelaitteen välisen yhteisen salaisuuden generoimiseen, jolloin päätelaitteen kytkeytyessä verkkoon se voi suorittaa normaalin (vain vähäistä sanomanvaihtoa vaativan) rekisteröinnin, jonka yhteydessä kulkee tieto, joka indikoi ko. salaisuuden. Keksintö perustuu siihen ajatukseen, että MIP:ssä määriteltyä indeksiä SPI (Security Parameter Index), joka on osoitin, joka osoittaa normaalisti tietoyksikköön, joka kertoo erilaista autentikoinnin suoritustapaan liittyvää tietoa, voidaan käyttää pelkästään kyseisen salaisuuden ilmoittamiseen, ja jättää muut SPI-parametrin avulla

osoitettavissa olevat asiat etukäteen määritellyiksi vakioiksi. Tällöin ko. salaisuuden synnyttämiseen voidaan käyttää matkaviestinverkosta tunnettuja keinoja.

Keksinnön mukaisen ratkaisun ansiosta päätelaite pystyy verkkoon kytkeytyessään aloittamaan hyötyliikenteen hyvin helposti ja ilman raskasta tai pitkällistä sanomanvaihtoa. Vaikka päätelaitteen ja verkon välistä salaisuutta ei olekaan määritelty tarkasti etukäteen, tarvitaan IP-verkkoon kytkeytymisen yhteydessä ainoastaan normaali MIP-rekisteröinti. Lisäksi turvataso paranee, koska osapuolien keskinäinen salaisuus ei ole enää kiinteä, vaan dynaamisesti muuttuva avain.

Keksinnön mukaisen ratkaisun ansiosta sellaisten ISP-operaattorien, jotka tarjoavat myös matkaviestinpalveluja ei tarvitse erikseen hankkia avaimienhallintajärjestelmää IP-verkkoon, vaan he voivat hyödyntää operoimansa matkaviestinverkon ominaisuuksia myös tähän tarkoitukseen.

Kuvioluettelo

Seuraavassa keksintöä ja sen edullisia toteutustapoja kuvataan tarkemmin viitaten kuvioihin 1...5 oheisten piirustusten mukaisissa esimerkeissä, joissa

kuvio 1 havainnollistaa erästä keksinnön mukaisen menetelmän toimintaympäristöä,

kuvio 2 havainnollistaa eri elementtien välillä käytävää sanomanvaihtoa,

kuvio 3 havainnollistaa liikkuvan solmun ja kotiagentin välillä lähetettävien rekisteröintisanomien rakennetta,

kuvio 4 havainnollistaa rekisteröintisanoman autentikointilaajennuskentän rakennetta, ja

kuvio 5 havainnollistaa päätelaitteen niitä toiminnallisia lohkoja, jotka ovat keksinnön kannalta oleellisia.

Keksinnön yksityiskohtainen kuvaus

Kuviossa 1 on esitetty keksinnön mukaisen menetelmän tyypillistä toimintaympäristöä. Järjestelmän alueella liikkuvilla käyttäjillä on käytössään kannettavia tietokoneita tai muita vastaavia päätelaitteita, esim. PDA-laitteita tai älypuhelimia. Kuviossa on havainnollistettu vain yhtä päätelaitetta TE1, jonka oletetaan tässä esimerkissä olevan kannettava tietokone. Kuvioon on merkitty kaksi IP-aliverkkoa: ensimmäinen lähiverkko LAN1, esim. Ethernet-

lähiverkko, joka on liitetty Internetiin reitittimen R1 kautta ja toinen lähiverkko LAN2, joka on kytketty Internetiin reitittimen R2 kautta. Lähiverkot voivat olla esim. yritysten sisäisiä verkkoja

Päätelaitteilla on pääsy aliverkkoihin liityntäpisteiden (access point) AP1 ja vastaavasti AP2 kautta sinänsä tunnetulla tavalla, esim. langattomasti, kuten kuviossa esitetään. Kuviossa oletetaan, että päätelaite TE1 on yhteydessä lähiverkkoon LAN1.

Päätelaitteessa on tyypillisesti liityntäelimet sekä lähiverkkoon (IP-verkkoon) että GSM-matkaviestinverkkoon (Global System for Mobile Communications). Lähiverkkoon liityntä tapahtuu esim. päätelaitteessa olevan LAN-kortin avulla ja GSM-verkkoon GSM-kortin avulla, joka on käytännössä riisuttu puhelin, joka on sijoitettu esim. tietokoneen PCMCIA-korttipaikkaan. GSM-korttiin liittyy lisäksi SIM-kortti (Subscriber Identity Module).

GSM-verkon osalta keksintö ei vaadi mitään erikoisratkaisuja, joten GSM-verkon toteutus on sinänsä tunnettu. Kuviossa GSM-verkosta on esitetty päätelaite TE1, kolme tukiasemaa BTS1...BTS3 (Base Transceiver Station), niiden yhteinen tukiasemaohjain BSC1 (Base Station Controller), matkaviestinkeskus MSC (Mobile Services Switching Centre), jonka järjestelmärajapinnan kautta matkaviestinverkko kytkeytyy muihin verkkoihin ja kotirekisteri HLR (Home Location Register), jonka yhteydessä on tunnistuskeskus AuC (Authentication Center). Lisäksi kuviossa on esitetty lyhytsanomakeskus SMSC (Short Message Switching Centre), jota käytetään hyväksi keksinnön eräässä toteutustavassa.

Lisäksi kuviossa on esitetty päätelaitteen TE1 kotiagentti HA, joka on Internetiin yhteydessä olevan reitittimen R3 yhteydessä. Käytännössä kotiagentin omistava organisaatio toimii usein paitsi ISP-operaattorina (Internet Service Provider), myös matkaviestinoperaattorina, minkä vuoksi kotiagentilta HA voidaan esteettä luoda yhteys matkaviestinverkkoon. Käytännössä reititin, jossa on kotiagenttitoiminto ja kotirekisteri voivat olla vaikkapa samassa laitehuoneessa.

Kuvion kaltaisessa ympäristössä käyttäjä voi (tunnettuja MIP-mekanismeja hyödyntäen) siirtyä vapaasti (liikenteen katkeamatta) IP-aliverkosta toiseen. Lisäksi datayhteys voidaan säilyttää GSM-verkon avulla, vaikka päätelaite poistuukin (langattoman) lähiverkon peittoalueelta. Lähiverkot muodostavat tällä tavoin paikallisia alueita (ns. hot spot), joiden sisällä päätelaitteella on suurinopeuksinen datayhteys ja käyttäjän liikkuessa ulos lähiver-

kon alueelta yhteys voidaan säilyttää GSM-verkon avulla. Koska nämä menettelyt ovat sinänsä tunnettuja, eivätkä ne liity varsinaiseen keksintöön, ei niitä kuvata tässä yhteydessä tarkemmin.

Keksinnön mukaisesti päätelaitteen rekisteröinnin yhteydessä suoritettavassa autentikoinnissa hyödynnetään GSM-verkon autentikointimekanismeja. Seuraavassa kuvataan ensin rekisteröitymistä ja sen yhteydessä suoritettavaa autentikointia.

Kuviossa 2 on esimerkki rekisteröitymisen yhteydessä suoritettavasta sanomanvaihdosta. MIP-protokollan mukaisesti vierailuagentti FA lähettää omaan aliverkkoonsa jatkuvasti broadcast-sanomia, joita kutsutaan nimellä "agent advertisement" ja joita on kuviossa merkitty viitemerkillä AA. Kun päätelaite kytkeytyy kyseiseen aliverkkoon, se vastaanottaa näitä sanomia ja päättelee niiden perusteella, onko se omassa kotiverkossaan vai jossakin muussa verkossa. Jos päätelaite huomaa, että se on kotiverkossaan, se toimii ilman liikkuvuuteen liittyviä palveluja (mobility services). Muussa tapauksessa päätelaite saa c/o-osoitteen (care-of address) ko. vieraaseen verkkoon. Tämä osoite on siis verkon sen pisteen osoite, johon päätelaite on väliaikaisesti kytkeytyneenä. Tämä osoite muodostaa samalla ko. päätelaitteelle johtavan tunnelin (tunnel) päätepisteen (termination point). Päätelaite saa osoitteen tyypillisesti em. broadcast-sanomista, joita vierailuagentti lähettää. Tämän jälkeen päätelaite lähettää omalle kotiagentilleen rekisteröintipyyntösanoman RR (Registration Request) vierailuagentin FA kautta. Sanoma sisältää mm. sen c/o-osoitteen, jonka päätelaite on juuri saanut. Vastaanottamansa pyyntösanoman perusteella kotiagentti päivittää kyseisen päätelaitteen sijaintitiedon tietokantaansa ja lähettää päätelaitteelle vierailuagentin kautta rekisteröintivastauksen (Registration Reply) R_Reply. Vastaussanomassa on kaikki tarpeelliset tiedot siitä, miten (millä ehdoilla) kotiagentti on hyväksynyt rekisteröintipyynnön.

Liikkuva solmu voi rekisteröityä myös suoraan kotiagentille. Em. RFC:ssä on kuvattu ne säännöt, jotka määräävät sen, rekisteröityykö liikkuva solmu kotiagentille suoraan vai vierailuagentin kautta. Jos liikkuva solmu saa c/o-osoitteen edellä kuvatulla tavalla, on rekisteröinti tehtävä aina vierailuagentin kautta.

Kaikki edellä mainitut, päätelaitteen, vierailuagentin ja kotiagentin väliset sanomat ovat MIP-protokollan mukaisia sanomia. Seuraavassa kuvataan tarkemmin, kuinka näitä sanomia käytetään esillä olevassa keksinnössä.

Rekisteröinnin yhteydessä suoritettava autentikointi perustuu rekisteröintisanomasta laskettuun tarkastusarvoon (hash-arvoon). Laskennassa käytetään hyväksi verkon ja käyttäjän yhteisesti tuntemaa salaisuutta. MIPissä on liikkuvia solmuja varten määritelty liikkuvuuden turvayhteys (Mobility Security Association), jonka avulla solmut voivat keskenään sopia käyttämistään turvaominaisuuksista. Liikkuvuuden turvayhteys käsittää joukon viitekehyksiä (contexts), joista kukin ilmoittaa autentikointialgoritmin, moodin, jossa ko. algoritmia käytetään, mainitun salaisuuden (esim. avain tai avainpari) ja tavan, jolla suojaudutaan ns. replay-hyökkäyksiä vastaan. Liikkuvat solmut valitsevat tietyn viitekehyksen käyttöön em. turvaparametri-indeksillä SPI, joka indikoi kulloinkin käytettävän viitekehyksen.

MIP:ssä on määritelty erityinen laajennusmekanismi, jonka avulla MIP-ohjaussanomiin tai ICMP-sanomiin (Internet Control Message Protocol) liitetään ns. laajennuskenttiä (extensions), joissa voidaan siirtää optionaalista informaatiota.

Rekisteröintipyyntö ja -vastaus (RR ja R_Reply, kuvio 2) käyttävät UDP-protokollaa (User Datagram Protocol). Kuviossa 3 on esitetty näiden rekisteröintisanomien otsikkojen yleistä rakennetta. IP- ja UDP-otsikkoja seuraavat MIP-kentät, joihin kuuluu tyyppikenttä 31, joka kertoo MIP-sanoman tyypin, koodikenttä 32, joka kertoo rekisteröintipyynnön tapauksessa erilaista liikkuvaan solmuun ja rekisteröintipyyntöön liittyvää tietoa ja rekisteröintivastauksen tapauksessa rekisteröintipyynnön tuloksen, elinaikakenttä 33, joka kertoo pyynnön tai hyväksytyn rekisteröinnin voimassaoloajan, kotiosoitekenttä 34, joka sisältää liikkuvan solmun IP-osoitteen, kotiagenttikenttä 35, joka sisältää liikkuvan solmun kotiagentin IP-osoitteen ja identifiointikenttä 37, joka sisältää numeron, joka liittää pyynnön ja siihen liittyvän vastauksen toisiinsa. Rekisteröintipyynnössä on lisäksi c/o-osoitekenttä 36, indikoi em. tunnelin pään IP-osoitteen (tätä kenttää ei ole rekisteröintivastauksessa).

Edellä kuvattua kiinteää otsikko-osaa seuraavat em. laajennuskentät. Autentikointia varten on omat laajennuskenttänsä (authentication extensions). Esim. liikkuvan solmun ja sen kotiagentin väliset rekisteröintisanomat autentikoidaan tähän nimenomaiseen tarkoitukseen varatun laajennuskentän (Mobile-Home Authentication Extension) avulla, joka on oltava kaikissa rekisteröintipyynnöissä ja kaikissa rekisteröintivastauksissa. (Sen sijaan liikkuvan solmun ja vierailuagentin välillä käytettävä laajennuskenttä (Mobile-Foreign

Authentication Extension) on rekisteröintipyynnöissä ja -vastauksissa vain, jos liikkuvan solmun ja vierailuagentin välillä on liikkuvuuden turvayhteys.)

Kuviossa 4 on havainnollistettu liikkuvan solmun ja sen kotiagentin välillä käytettävän laajennuskentän rakennetta. Laajennuskenttä sisältää tyyppitiedon, joka kertoo laajennuskentän tyypin, pituustiedon, joka osoittaa kentän kokonaispituuden, SPI-indeksin, jonka pituus on 4 tavua ja autentikaattorin, jonka pituus voi vaihdella ja jonka pituus on oletusarvoisesti 128 bittiä.

Autentikoinnissa käytetään oletusarvoisesti tunnettua MD5-algoritmia ns. prefix+suffix-moodissa. MD5 on algoritmi, joka laskee mielivaltaisen pituisesta sanomasta 128 bitin pituisen tiivistelmän (digest), joka on em. tarkastustai hash-arvo ja joka toimii tässä tapauksessa autentikaattorina, johon autentikointi perustuu. Prefix+suffix-moodilla tarkoitetaan sitä, että siinä bittijonossa, josta autentikaattori lasketaan on verkon ja liikkuvan solmun yhteinen salaisuus (esim. yhteinen avain) ensimmäisenä ja viimeisenä. Autentikointilaajennuskentässä ilmoitetaan indeksin SPI avulla, mitä viitekehystä käytetään. Viitekehys puolestaan indikoi, kuinka autentikaattori (hash-arvo) on muodostettava. Autentikaattori välitetään vastekerrokselle (peer) autentikointilaajennuskentässä (kuviot 3 ja 4), jolloin vastekerros pystyy muodostamaan SPI:n avulla itsenäisesti autentikaattorin ja vertaamaan sitä vastaanotettuun autentikaattoriin.

Keksinnössä hyödynnetään matkaviestinverkon, erityisesti GSM-verkon ominaisuuksia yhteisen salaisuuden muodostamiseen seuraavalla tavalla.

Kotiagentti HA hakee matkaviestinverkon kotirekisterin HLR yhteydessä olevasta tunnistuskeskuksesta AuC joukon tilaajakohtaisia tunnistuskolmikkoja (authentication triplets), joista kukin sisältää tunnettuun tapaan haasteen (RAND), vasteen SRES (Signed Response) ja avaimen Kc (yhteyskohtainen salausavain). Tilaajakohtainen tieto voidaan hakea esim. siten, että kotiagentille on talletettu päätelaitteiden IP-osoitteita vastaavat tilaajatunnukset IMSI (International Mobile Subscriber Identity) kyselyjä varten. Tunnistuskolmikkojen siirto voidaan tehdä millä tahansa tunnetulla tavalla, esim. varustamalla tunnistuskeskus TCP/IP-pinolla ja välittämällä kolmikot kotiagentille yhdessä tai useammassa IP-tietosähkeessä. Kuten edellä todettiin, kotiagentti ja kotirekisteri sekä tunnistuskeskus ovat tyypillisesti saman operaattorin omistuksessa ja voivat olla vaikkapa samassa huoneessa, joten

kyseinen siirtoyhteys on suojattu. Keksinnön kannalta oleellista on ainoastaan se, että kotiagentti saa tunnistuskolmikoista vasteen ja avaimen Kc. Haasteet voidaan siis jopa jättää välittämättä. Kotiagentti HA tallettaa tunnistuskolmikot itselleen.

Lisäksi tunnistuskolmikkojen sisältämät haasteet (RANDit) välitetään edelleen liikkuvalle solmulle (päätelaitteelle TE1) jollakin sopivalla, olemassa olevalla siirtotavalla. Lähetyksen voi suorittaa joko kotiagentti saatuaan tunnistuskolmikot tai HLR/AuC vasteena kotiagentin lähettämään tunnistuskolmikkopyyntöön. Eräs vaihtoehto on välittää haasteet HLR/AuC:lta lyhytsanomaa käyttäen lyhytsanomakeskuksen SMSC kautta päätelaitteelle. Toinen vaihtoehto on siirtää haasteet Internetin kautta IP-tietosähkeessä. Jos päätelaite ei ole vielä kertaakaan ollut yhteydessä IP-verkkoon, on lähetys kuitenkin suoritettava GSM-verkon avulla (lyhytsanomalla). Toinen vaihtoehto tällaisessa tapauksessa on tehdä sopimus, jonka mukaan ensimmäisellä rekisteröitymiskerralla käytetään jotakin tiettyä ennalta sovittua RAND-arvoa, jolloin haasteiden lähetys voidaan tämän jälkeen tehdä IP-verkon kautta.

Tunnistuskolmikkojen ja haasteiden siirtomekanismit eivät ole keksinnön kannalta oleellisia, vaan siirtoon voidaan käyttää mitä tahansa tunnettua tekniikkaa. Kerralla haettavien ja siirrettävien tunnistuskolmikkojen ja haasteiden lukumäärä riippuu siitä, mitä siirtomekanismia käytetään. Esim. lyhytsanoman maksimipituus (160 merkkiä) rajoittaa kerrallaan siirrettävien haasteiden lukumäärän kymmeneen, koska haasteen pituus on 16 tavua.

Kun liikkuva solmu TE1 haluaa suorittaa MIP-rekisteröinnin, yksi kyseisistä haasteista valitaan liikkuvassa solmussa käyttöön, minkä jälkeen suoritetaan tunnetut A3- ja A8-algoritmit SIM-kortilla kyseistä haastetta käyttäen (vrt. kuvio 2). Tuloksena saadaan vaste (SRES) ja avain Kc, joista edellinen on 32 bitin pituinen ja jälkimmäinen 64 bitin pituinen. Edellä mainitussa rekisteröintipyyntösanomassa RR lähetetään tämän jälkeen juuri laskettu SRES-arvo SPI-parametrinä (vrt. kuviot 2 ja 4) ja saatua avainta Kc käytetään em. salaisuutena, jonka perusteella lasketaan autentikaattori, joka sisällytetään rekisteröintipyyntösanomaan. Kuten edellä mainittiin, MIPissä SPIn pituudeksi on määritelty juuri 32 bittiä. Vastaanotettuaan SRES-arvon kotiagentti huomaa, minkä haasteen käyttäjä on valinnut, jolloin se voi valita vastaavan Kc:n ja suorittaa autentikaattorin tarkistuksen.

Rekisteröintisanomien vaihto tapahtuu siis muuten tunnetusti, mutta lasketun vasteen arvo siirretään rekisteröintipyyntösanoman SPI-kentässä ja

sen lisäksi autentikaattorin laskennassa käytettävänä salaisuutena käytetään matkaviestinjärjestelmän avulla generoitua avainta (GSM-järjestelmässä generoitava yhteyskohtainen salausavain Kc).

Tunnistuskolmikot voidaan myös tallettaa esim. HLR/AuC:n yhteyteen tai johonkin kolmanteen paikkaan siirtämättä niitä kotiagentille. Tällöin toimitaan siten, että saadessaan rekisteröintipyyntösanoman kotiagentti kysyy tunnistuskolmikkojen tallennuspaikasta, mikä avain oli kysymyksessä. Tämä edellyttää kuitenkin turvattua yhteyttä kotiagentin ja tallennuspaikan välillä.

MIP määrittelee SPI:n sallitut arvot; arvot 0...255 ovat varattuja, eikä niitä saa käyttää missään turvayhteydessä. Jos haaste tuottaa sellaisen SRES-arvon, joka ei ole sallittu SPI:n arvona, kyseinen haaste on hylättävä. HLR/AuC:n yhteyteen voidaan rakentaa logiikka, joka suodattaa pois sellaiset haasteet, jotka tuottaisivat ei-sallitun arvon. Vaihtoehtoisesti tällainen logiikka voidaan rakentaa liikkuvan solmun päähän. Tällöin liikkuva solmu ei lähetä sellaisia rekisteröintipyyntöjä, joissa SRES-arvo vastaa ei-sallittua SPI-arvoa.

On mahdollista, että päätelaitteelle tarkoitetuista tai sille jo välitetyistä haasteista kaksi tai useampi on sellaisia, että ne antavat saman SRES-arvon. Jos näin käy, käytetty salaisuus ei ole yksikäsitteisesti määritelty. Tällöin hylätään kyseisistä haasteita yhtä lukuunottamatta kaikki muut. Tämä logiikka voi olla HLR/AuC:n yhteydessä tai päätelaitteissa.

Kuviossa 5 on havainnollistettu päätelaitteen niitä toiminnallisia lohkoja, jotka ovat keksinnön kannalta oleellisia. Kuviossa on esitetty vain yksi liityntä verkkoon (IP-verkko). Verkosta tulevat haasteet tulevat sanomien lähetys- ja vastaanottolohkolle MEB, josta ne talletetaan muistilohkoon MB. Valintalohko SB valitsee talletetuista haasteista yhden ja syöttää sen SIM-kortille. Tuloksena saatava vaste syötetään lähetys- ja vastaanottolohkolle MEB, joka sijoittaa vasteen lähtevän rekisteröintipyyntösanoman SPI:lle varattuun kenttään. Autentikointilohko AB määrittää lähteviin sanomiin autentikaattorin SIM-kortilta saamaansa avainta Kc käyttäen ja suorittaa saapuvien sanomien autentikointia ko. avaimen avulla.

GSM-verkon autentikointi perustuu 32-bittisen SRES-arvon vertaamiseen. Koska keksinnössä käytetään autentikoinnissa 64-bittistä avainta Kc, autentikoinnin suojaustaso ylittää GSM:n tason. Salausavaimella Kc ei ole MIP:n kannalta sinänsä käyttöä, vaan se muodostaa ainoastaan liikkuvan solmun ja verkon välisen yhteisen salaisuuden. Jos saavutettua autentikoinnin

suojaustasoa pidetään kuitenkin liian heikkona, on mahdollista käyttää salaisuutena esim. kahden peräkkäisen RANDin tuottamaa avainta Kc.

Ns. replay-hyökkäyksen estämiseksi voidaan käyttää MIP:ssä määriteltyjä keinoja, aikaleimaa tai satunnaislukua (nonce), jotka molemmat käyttävät edellä kuvattua identifiointikenttää. Aikaleimaa käytettäessä on erikseen varmistuttava käyttäjän ja verkon kellojen riittävästä synkronoinnista. Käytetty menettely on kuitenkin valittava etukäteen, koska sitä ei voida ilmoittaa SPI:n avulla.

Vaihtoehtoisesti voidaan käyttää menettelyä, jolla varmistetaan, että käytetyt haasteet ovat ainutkertaisia, jolloin verkko ei saa lähettää tai hyväksyä jo kertaalleen käytettyjä haasteita. Tämä edellyttää lisätoiminnallisuutta HLR/AuC:ssä tai kotiagentissa (tai molemmissa) siten, että ne eivät hyväksy jo kertaalleen käytettyä haastetta.

Keksintöä voidaan käyttää myös ilman matkaviestinverkkoa, riittää kun järjestelmässä on verkkoelementti, joka osaa muodostaa tunnistuskolmikot samalla tavalla kuin HLR/AuC. Näin ollen myös päätelaite voi olla kiinteä. Jos matkaviestinverkkoa ei hyödynnetä, ensimmäisen haastejoukon välittämiseen ei voida käyttää lyhytsanomaa, vaan ensimmäinen rekisteröinti on suoritettava esim. etukäteen sovitulla haastearvolla.

Haasteen arvoa ei tarvitse välittää päätelaitteelta, vaan riittää, että kotiagentti saa tietää, mikä avain on valittu käyttöön. Tämä ilmoitus voidaan suorittaa esim. siten, että haasteet lajitellaan samanlaiseen järjestykseen molemmissa päissä ja päätelaite ilmoittaa vain järjestysnumeron, joka vastaa valittua haastetta. Käytetyt järjestysnumerot voivat alkaa mistä tahansa tahansa numerosta, joka on suurempi kuin SPI:n suurin ei-sallittu arvo (255), esim. arvosta 300.

Vaikka keksintöä on edellä selostettu viitaten oheisten piirustusten mukaisiin esimerkkeihin, on selvää, ettei keksintö ole rajoittunut siihen, vaan sitä voidaan muunnella oheisissa patenttivaatimuksissa esitetyn keksinnöllisen ajatuksen puitteissa. Keksinnön mukainen ratkaisu ei esim. välttämättä ole sidottu MIPiin, vaan sitä voidaan käyttää minkä tahansa samankaltaisen protokollan yhteydessä, jossa välitetään, yhden sanoman tai vaikkapa usean erillisen sanoman avulla, autentikaattori ja tieto siitä, kuinka autentikaattori on muodostettava. Näin ollen keksintö ei myöskään ole välttämättä sidottu IP-verkkoon. Autentikointia ei myöskään välttämättä tehdä rekisteröitymisen yhteydessä. Tunnistusyksikön (SIM) toteutus voi myös vaihdella, mutta sen on

muodostettava vaste samalla tavalla kuin matkaviestinverkossa tehdään, jotta vertailu voidaan tehdä.

Patenttivaatimukset

1. Autentikointimenetelmä tietoliikenneverkkoa, erityisesti IP-verkkoa varten, jonka menetelmän mukaisesti

- verkon päätelaitteelta (TE1) lähetetään verkolle autentikaattori ja tietoyksikkö (SPI), joka sisältää autentikaattorin muodostamistapaan liittyvää tietoa, ja

- tietoyksikön avulla määritetään verkossa tarkastusarvo, jota verrataan mainittuun autentikaattoriin,

t u n n e t t u siitä, että

- verkon päätelaitteessa käytetään sellaista tunnistusyksikköä, jolle syötteenä annetusta haasteesta voidaan määrittää vaste ja avain oleellisesti samalla tavalla kuin tunnetun matkaviestinjärjestelmän tilaajan tunnistusyksikössä,

- generoidaan verkkoon joukko tilaajakohtaisia autentikointitietolohkoja, joista kukin sisältää haasteen, vasteen ja avaimen, jolloin generointi suoritetaan samalla tavalla kuin mainitussa matkaviestinjärjestelmässä,

- päätelaitteelle välitetään ainakin osa autentikointitietolohkojen sisältämistä haasteista,

- päätelaitteella valitaan yksi haasteista käyttöön ja sen perusteella määritetään päätelaitteen tunnistusyksikön avulla vaste ja käyttöön otettava avain,

- verkolle ilmoitetaan mainitun tietoyksikön avulla, mitä haastetta vastaava avain on valittu, ja

- autentikaattori ja mainittu tarkastusarvo määritetään valitun avaimen avulla.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että tietoyksikkö on mobile IP -protokollan rekisteröintisanomassa oleva indeksi SPI (Security Parameter Index).

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, t u n n e t t u siitä, että tietoyksikölle sijoitetaan päätelaitteella määritetyn vasteen arvo.

4. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että haasteet lajitellaan päätelaitteella ennalta määrättyjen lajittelukriteerien avulla järjestykseen ja tietoyksikölle sijoitetaan valittua haastetta vastaava järjestysnumero.

5. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että päätelaitteessa käytetään tunnistusyksikkönä tunnetun GSM-järjestelmän

käyttämää tilaajan tunnistusyksikköä SIM (Subscriber Identity Module) ja mainitut autentikointitietolohkot ovat GSM-järjestelmän käyttämiä tunnistuskolmikkoja.

6. Patenttivaatimuksen 5 mukainen menetelmä, t u n n e t t u siitä, että tunnistuskolmikot haetaan GSM-järjestelmän tunnistuskeskuksesta AuC.

7. Patenttivaatimuksen 6 mukainen menetelmä, t u n n e t t u siitä, että päätelaitteelle välitettävät haasteet välitetään tunnettua lyhytsanomapalvelua käyttäen.

8. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että päätelaitteelle välitettävät haasteet välitetään IP-verkon kautta lähetettävässä IP-tietosähkeessä.

9. Patenttivaatimuksen 1 mukainen menetelmä IP-verkkoa varten, t u n n e t t u siitä, että autentikointitietolohkot välitetään päätelaitteen kotiagentille ja kotiagentille ilmoitetaan mainitun tietoyksikön avulla, mitä haastetta vastaava avain on valittu, jolloin mainittu tarkastusarvo määritetään kotiagentissa.

10. Autentikointijärjestelmä tietoliikenneverkkoa, erityisesti IP-verkkoa varten, joka järjestelmä sisältää

- verkon päätelaitteessa (TE1) ensimmäiset sanomanlähetyselimet (MEB) autentikaattorin ja tietoyksikön (SPI) lähettämiseksi verkolle, joka tietoyksikkö sisältää autentikaattorin muodostamistapaan liittyvää tietoa, ja
- tarkastuselimet (HA) tarkastusarvon määrittämiseksi tietoyksikön avulla,

t u n n e t t u siitä, että

- verkon päätelaite käsittää sellaisen tunnistusyksikön, jolle syötteenä annetusta haasteesta voidaan määrittää vaste ja avain oleellisesti samalla tavalla kuin tunnetun matkaviestinjärjestelmän tilaajan tunnistusyksikössä,
- järjestelmä sisältää generointielimet (HLR/AuC) autentikointitietolohkojen generoimiseksi samalla tavalla kuin mainitussa matkaviestinjärjestelmässä, jotka autentikointitietolohkot ovat sellaisia, että kukin niistä sisältää haasteen, vasteen ja avaimen,
- järjestelmä sisältää välityselimet autentikointitietolohkojen sisältämien haasteiden välittämiseksi päätelaitteelle,
- päätelaitteessa on valintaelimet (SB) yhden haasteen valitsemiseksi käyttöön,

- ensimmäiset sanomanlähetyselimet (MEB) sijoittavat mainitulle tietoyksiköllе arvon, joka osoittaa, mitä haastetta vastaava avain on valittu käyttöön päätelaitteessa, ja

- ensimmäiset sanomanlähetyselimet (MEB) määrittävät autentikaattorin ja tarkastuselimet mainitun tarkastusarvon valitun avaimen perusteella.

11. Patenttivaatimuksen 10 mukainen järjestelmä, t u n n e t t u siitä, että päätelaitteen yhteydessä oleva tunnistusyksikkö on GSM-matkaviestinjärjestelmässä käytettävä tilaajan tunnistusyksikkö SIM.

12. Patenttivaatimuksen 10 mukainen järjestelmä, t u n n e t t u siitä, että mainitut generointielimet käsittävät GSM-matkaviestinjärjestelmän tunnistuskeskuksen AuC.

13. Patenttivaatimuksen 10 mukainen järjestelmä, t u n n e t t u siitä, että mainitut välityselimet käsittävät tunnetun lyhytsanomapalvelun toteuttavat elimet (SMSC).

Patentkrav

1. Autenticeringsförfarande för telekommunikationsnät, särskilt för IP-nät, enligt vilket förfarande

sänds en autenticerare och en dataenhet (SPI), som innehåller data om det sätt på vilket autenticeraren har bildats, från en terminal (TE1) i nätet till nätet och

i nätet med hjälp av dataenheten bestäms ett kontrollvärde som jämförs med nämnda autenticerare,

k ä n n e t e c k n a t av att

i terminalen i nätet används en identifieringsenhet i fråga om vilken i en utmaning som givits åt denna som input kan bestämmas svar och nyckel väsentligen på samma sätt som i den abonnentidentifieringsenhet som används i det kända mobilkommunikationssystemet,

i nätet genereras ett antal abonnentspecifika autenticeringsinformationsblock som vart och ett innehåller en utmaning, ett svar och en nyckel, varvid genereringen utförs på samma sätt som i nämnda mobilkommunikationssystem,

till terminalen förmedlas åtminstone en del av utmaningarna i autenticeringsinformationsblocken,

med terminalen väljs en av utmaningarna för att användas och på basis av denna, med hjälp av terminalens identifieringsenhet, bestäms ett svar och vilken nyckel kommer att tas i bruk,

till nätet meddelas med hjälp av nämnda dataenhet mot vilken utmaning svarande nyckel har valts, och

autenticeraren och nämnda kontrollvärde bestäms med hjälp av den valda nyckeln.

2. Förfarande enligt patentkrav 1, k ä n n e t e c k n a t av att dataenheten utgörs av indexet SPI (Security Parameter Index) som ingår i inregistreringsmeddelandet enligt mobile IP –protokollet.

3. Förfarande enligt patentkrav 1 eller 2, k ä n n e t e c k n a t av att i dataenheten placeras värdet för det med terminalen bestämda svaret.

4. Förfarande enligt patentkrav 1, k ä n n e t e c k n a t av att utmaningarna ordnas i ordningsföljd med terminalen, med hjälp av på förhand ställda ordningskriterier, och i dataenheten placeras det ordningsnummer som motsvarar den valda utmaningen.

5. Förfarande enligt patentkrav 1, k ä n n e t e c k n a t av att i terminalen som identifieringsenhet används abonnentidentifieringsenheten SIM (Subscriber Identity Module) som är i bruk i det kända GSM-systemet, och nämnda autenticeringsinformationsblock är identifieringstriplett som används i GSM-systemet.

6. Förfarande enligt patentkrav 5, k ä n n e t e c k n a t av att identifieringstripletten söks i ett autenticeringscenter AuC enligt GSM-systemet.

7. Förfarande enligt patentkrav 6, k ä n n e t e c k n a t av att de utmaningar som skall förmedlas till terminalen förmedlas genom att använda den kända kortmeddelandetjänsten.

8. Förfarande enligt patentkrav 1, k ä n n e t e c k n a t av att de utmaningar som skall förmedlas till terminalen förmedlas i ett IP-datagram som sänds via IP-nätet.

9. Förfarande enligt patentkrav 1 för IP-nät, k ä n n e t e c k n a t av att autenticeringsinformationsblocken förmedlas till terminalens hemagent och till hemagenten meddelas med hjälp av nämnda dataenhet mot vilken utmaning svarande nyckel har valts, varvid nämnda kontrollvärde bestäms i hemagenten.

10. Autenticeringssystem för telekommunikationsnät, särskilt för IP-nät, vilket system innefattar

första meddelandesändningsorgan (MEB) i en terminal (TE1) i nätet för sändning av en autenticerare och en dataenhet (SPI) till nätet, vilken dataenhet innehåller data om det sätt på vilket autenticeraren har bildats, och

kontrollorgan (HA) för att bestämma ett kontrollvärde med hjälp av dataenheten,

k ä n n e t e c k n a t av att

terminalen i nätet innefattar en identifieringsenhet i fråga om vilken i en utmaning som givits åt denna som input kan bestämmas svar och nyckel väsentligen på samma sätt som i den abonnentidentifieringsenhet som används i det kända mobilkommunikationssystemet,

systemet innefattar genereringsorgan (HLR/AuC) för generering av autenticeringsinformationsblock på samma sätt som i nämnda mobilkommunikationssystem, vilka autenticeringsinformationsblock är sådana att vart och ett av dem innehåller en utmaning, ett svar och en nyckel,

systemet innefattar förmedlingsorgan för förmedling av utmaningarna i autenticeringsinformationsblocken till terminalen,

terminalen innefattar väljarorgan (SB) för att välja en utmaning för att användas,

de första meddelandesändningsorganen (MEB) placerar i nämnda dataenhet ett värde som anger mot vilken utmaning svarande nyckel har valts för att användas i terminalen, och

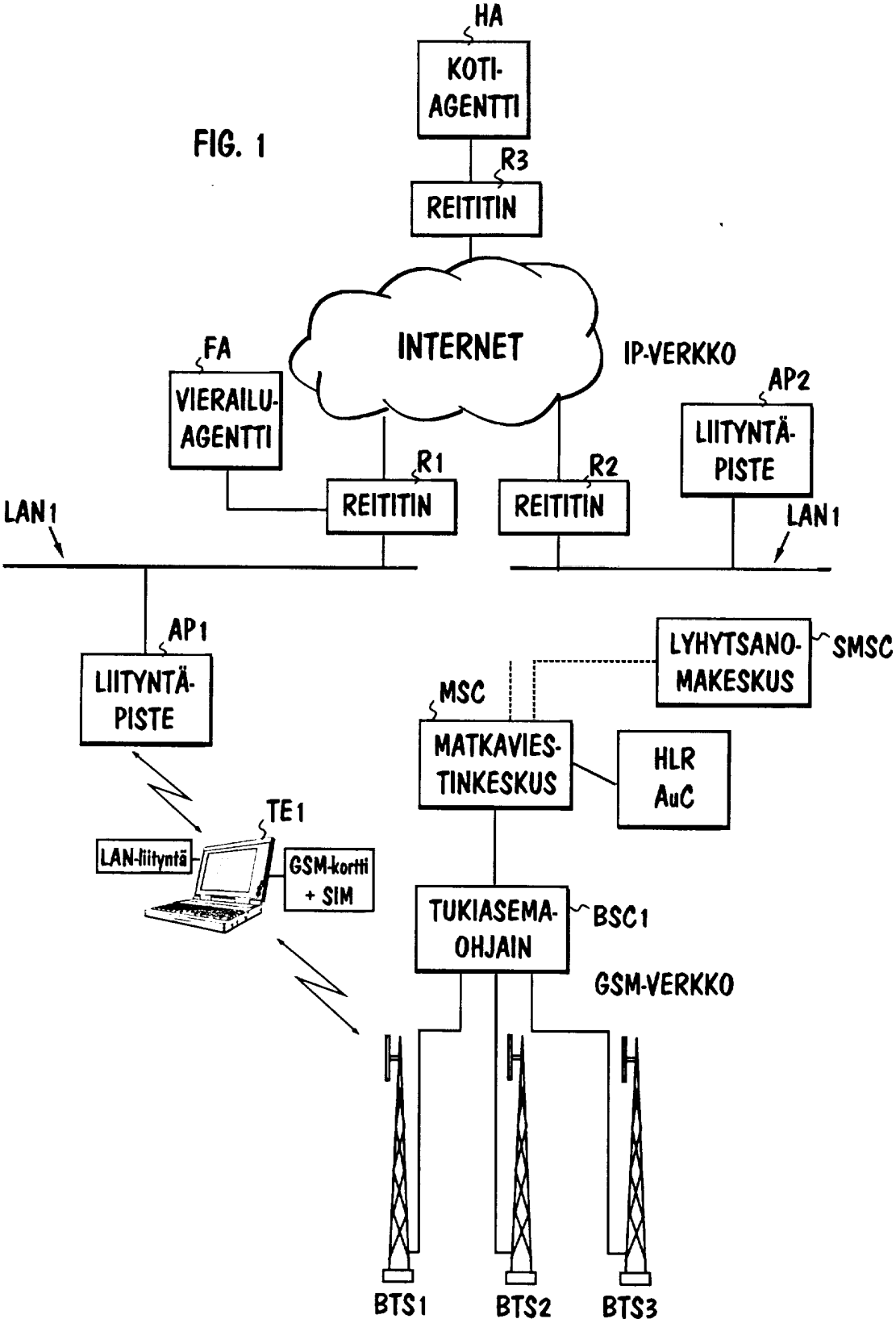
de första meddelandesändningsorganen (MEB) bestämmer autenticeraren och kontrollorganen bestämmer nämnda kontrollvärde på basis av den valda nyckeln.

11. System enligt patentkrav 10, k ä n n e t e c k n a t av att den i samband med terminalen belägna identifieringsenheten är en abonnentidentifieringsenhet SIM som används i GSM-mobilkommunikationssystemet.

12. System enligt patentkrav 10, k ä n n e t e c k n a t av att i nämnda genereringsorgan ingår ett autenticeringscenter AuC enligt GSM-systemet.

13. System enligt patentkrav 10, k ä n n e t e c k n a t av att i nämnda förmedlingsorgan ingår organ (SMSC) som utför den kända kortmeddelandetjänsten.

FIG. 1


HA
KOTI-
AGENTTI
R3
REITITIN
INTERNET
IP-VERKKO
FA
VIERAILU-
AGENTTI
AP2
LIITYNTÄ-
PISTE
R1
REITITIN
R2
REITITIN
LAN1
LAN1
AP1
LIITYNTÄ-
PISTE
LYHYTSANO-
MAKESKUS
SMSC
MSC
MATKAVIES-
TINKESKUS
HLR
AuC
TE1
LAN-liityntä
GSM-kortti
+ SIM
TUKIASEMA-
OHJAIN
BSC1
GSM-VERKKO
BTS1
BTS2
BTS3

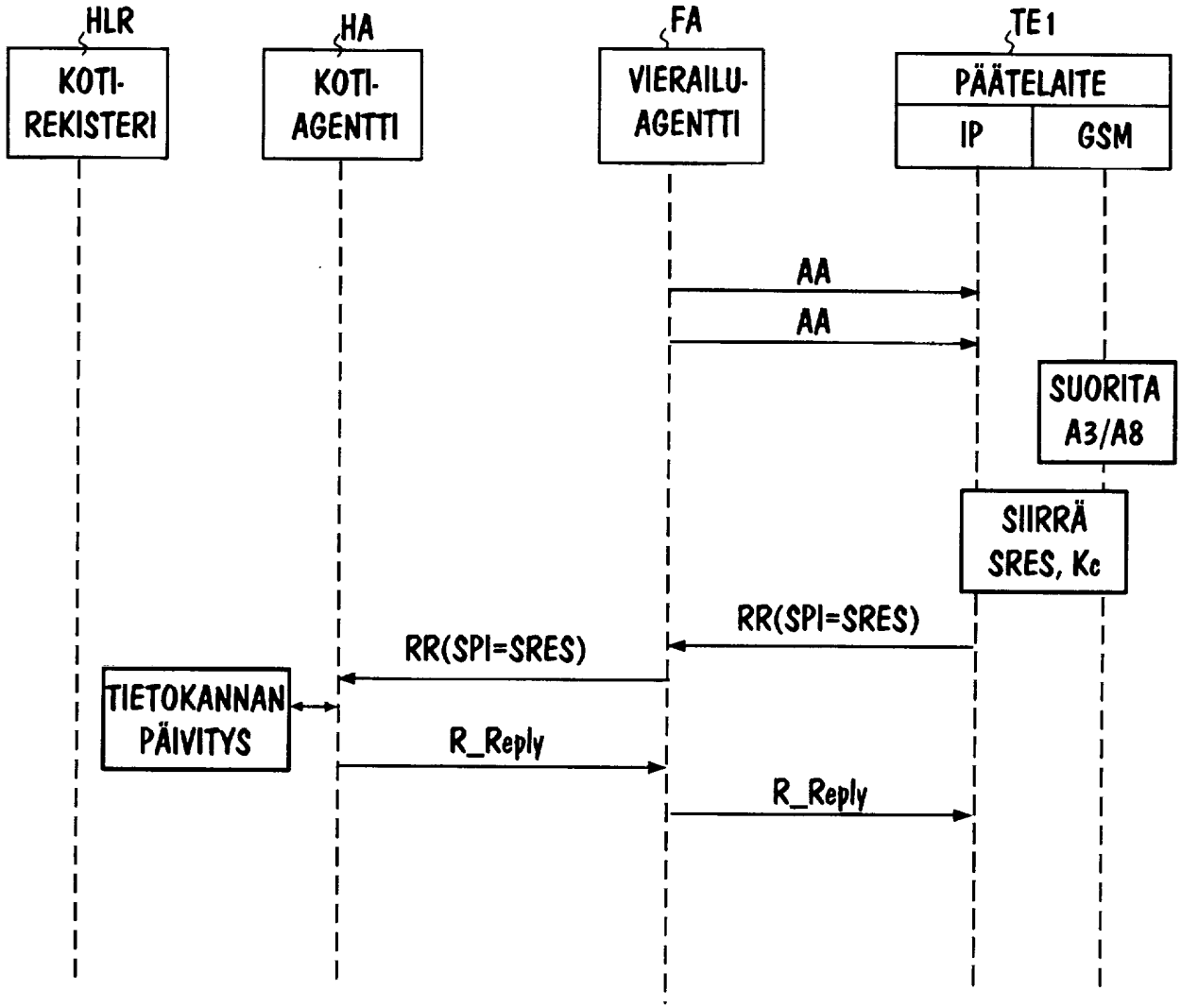

HLR
KOTI-
REKISTERI
HA
KOTI-
AGENTTI
FA
VIERAILU-
AGENTTI
TE1
PÄÄTELAITE
IP
GSM
AA
AA
SUORITA
A3/A8
SIIRRÄ
SRES, Kc
RR(SPI=SRES)
RR(SPI=SRES)
TIETOKANNAN
PÄIVITYS
R_Reply
R_Reply

FIG. 2

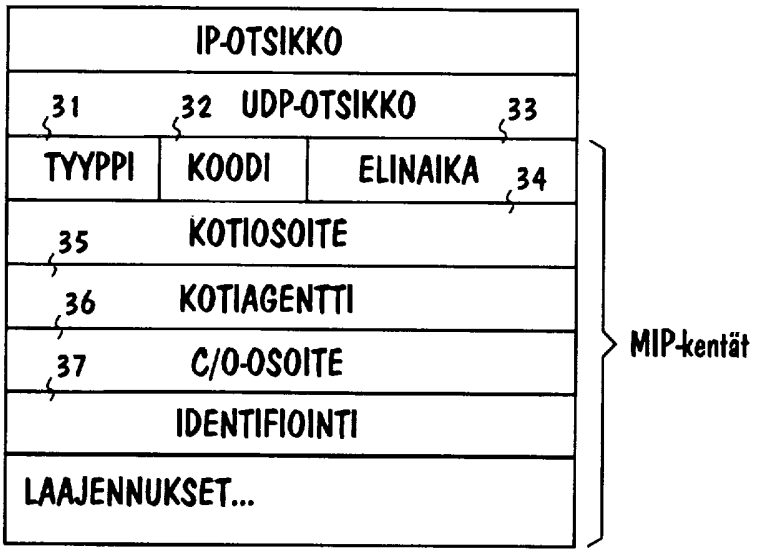


FIG. 3

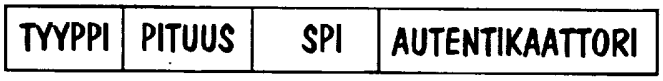


FIG. 4

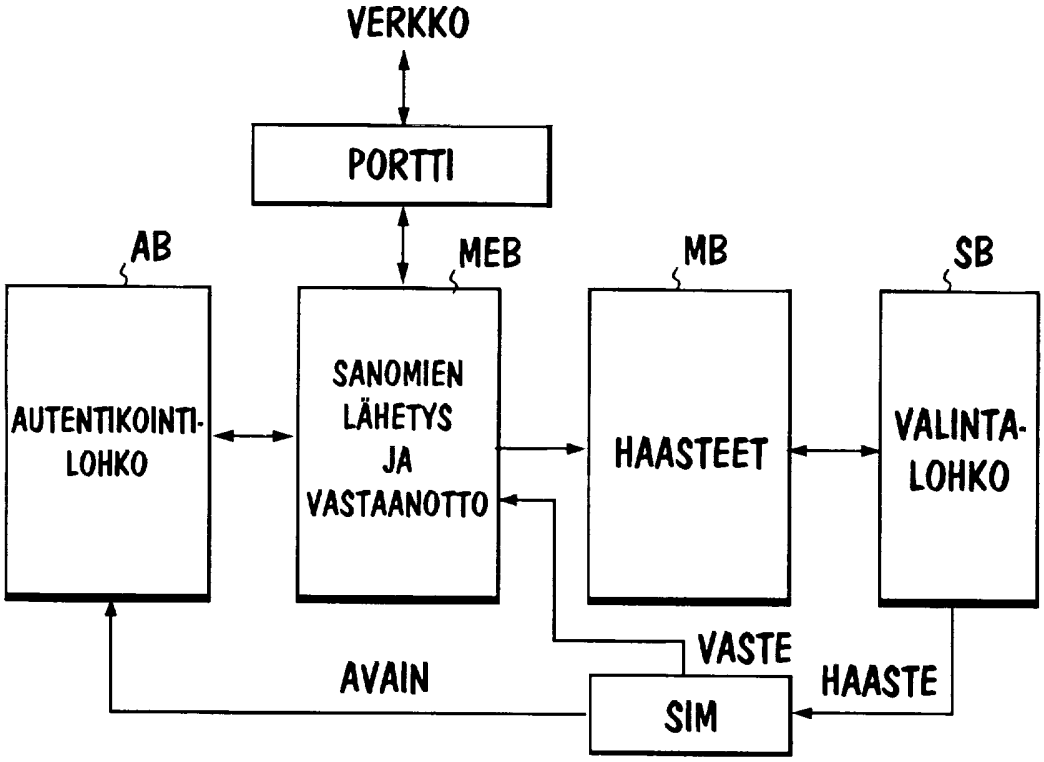


FIG. 5