FI0001079848

(12) **PATENTTIJULKAISU**
PATENTSKRIFT

(10) **FI 107984 B**

(45) Patentti myönnetty - Patent beviljats **31.10.2001**

(51) Kv.lk.7 - Int.kl.7
H04Q 7/38

(21) Patenttihakemus - Patentansökning **981132**

(22) Hakemispäivä - Ansökningsdag **20.05.1998**

(24) Alkupäivä - Löpdag **20.05.1998**

(41) Tullut julkiseksi - Blivit offentlig **21.11.1999**

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 •**Uskela, Sami**, Puistokaari 8 B 12, 00200 Helsinki, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud: Kolster Oy Ab
Iso Roobertinkatu 23, 00120 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning

Palvelun luvattoman käytön estäminen
Förhindrande av olovligt användande av tjänst

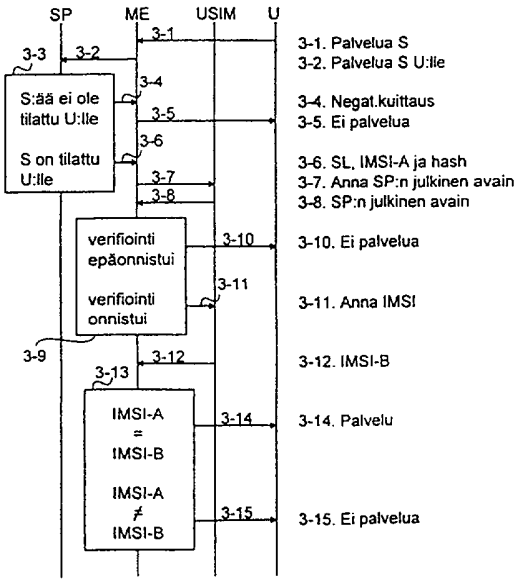
(56) Viitejulkaisut - Anförda publikationer

DE A 19647109 (H04M 3/42), WO A 95/21509 (H04Q 7/24), WO A 99/18746 (H04Q 7/38)

(57) Tiivistelmä - Sammandrag

Menetelmä, järjestelmä, tietoliikennejärjestelmän verkkoelementti ja laitteisto palvelun luvattoman käytön estämiseksi. Menetelmälle, jossa vastaanotetaan palvelun käyttäjältä palvelupyyntö, ja aikaansaadaan palvelu palvelulogiikan avulla, on tunnusomaista luvattoman käytön estämiseksi se, että palvelulogiikkaan liitetään autentikointitieto (3-6), autentikoidaan palvelua pyytävä käyttäjä autentikointitiedon avulla (3-9), ja suoritetaan palvelulogiikka (3-14) vain, mikäli autentikointi läpäistään.

Ett förfarande, ett system, ett nätelement i ett datatrafiksystem och en apparatur för att förhindra olovlig användning. Kännetecknande för förfarandet, i vilket en olovlig användning förhindras, är att från en användare av en tjänst mottages en tjänstebegäran och med hjälp av en tjänstelogik åstadkommes en tjänst, varvid till tjänstelogiken bifogas en autenticeringsinformation (3 - 6), den användare som begär tjänsten autenticeras med hjälp av autenticeringsinformationen (3 - 9), och varefter tjänstelogiken (3 - 14) utföres endast, om autenticeringen gsenomförts framgångsrikt.



Palvelun luvattoman käytön estäminen

Keksinnön tausta

Keksintö liittyy palveluiden luvattoman käytön estämiseen, ja erityisesti matkaviestinjärjestelmän palveluiden luvattoman käytön estämiseen.

Matkaviestinjärjestelmät on kehitetty, koska on ollut tarve vapauttaa ihmiset siirtymään pois kiinteiden puhelinpäätteiden luota ilman, että se vaikeuttaa heidän tavoitettavuuttaan. Matkaviestinjärjestelmien kanssa ovat kehittyneet myös matkaviestinten välityksellä tarjottavat palvelut. Tällä hetkellä ollaan suunnittelemassa erilaisia uusia palvelumuotoja nykyisiin ja erityisesti tuleviin ns. kolmannen sukupolven matkaviestinjärjestelmiin kuten Universal Mobile Telecommunication System (UMTS) sekä IMT-2000 (International Mobile Telecommunication 2000). UMTS on standardointityön alla ETSI:ssä (European Telecommunications Standards Institute), kun taas ITU (International Telecommunications Union) standardoi IMT-2000 -järjestelmää. Nämä tulevaisuuden järjestelmät ovat peruspiirteiltään hyvin samankaltaisia. Seuraavassa tullaan tarkemmin käsittelemään IMT-2000-järjestelmää, jonka arkkitehtuuria on havainnollistettu kuviossa 1.

Kuten kaikki matkaviestinjärjestelmät, IMT-2000 tuottaa langattomia tiedonsiirtopalveluita liikkeessä oleville käyttäjille. Järjestelmä tukee vaellusta, ts. IMT-2000-käyttäjät voidaan saavuttaa ja he voivat tehdä puheluita missä tahansa, kun he ovat sijoittuneet IMT-2000-järjestelmän peittoalueen sisälle. IMT-2000:n odotetaan tyydyttävän laajan valikoiman erilaisia tulevaisuuden palvelu-tarpeita, kuten virtuaalinen kotiympäristö VHE (Virtual Home Environment). Virtuaalisen kotiympäristön avulla IMT-2000-käyttäjällä on käytössään kaikkialla järjestelmän peittoalueen sisällä samat palvelut. Erilaisten palvelujen joustava toteuttaminen ja erityisesti vaelluksen (roaming) tukeminen edellyttää nykytietämyksen mukaan joidenkin palvelulogiikkojen lataamista käyttäjän päätelaitteeseen ja/tai palvelevaan verkkoon. Palveleva verkko on se verkko, jonka välityksellä palveluoperaattori (service provider) tarjoaa palveluaan loppukäyttäjälle. Palvelulogiikka on palveluun liittyvä ohjelma, osaohjelma, komentosarja (script) tai sovelma (applet). Palvelu aikaansaadaan palvelulogiikan avulla suorittamalla ainakin palvelulogiikka ja siinä määritellyt toiminnot. Palvelu voi käsittää myös useita palvelulogiikkoja.

Ongelmana yllä kuvatussa järjestelyssä on, että siinä ei mitenkään varmisteta sitä, että käyttäjällä on todella oikeus käyttää palvelua. Erityisesti

palveluja, joissa palvelulogiikka ladataan päätelaitteeseen ja/tai palvelevaan verkkoon, on helppo kopioida ja käyttää luvattomasti.

Keksinnön lyhyt selostus

Keksinnön tavoitteena on siten kehittää menetelmä ja menetelmän toteuttava laitteisto siten, että yllä mainittu ongelma saadaan ratkaistua. Keksinnön tavoitteet saavutetaan menetelmällä, järjestelmällä, verkkoelementillä ja laitteistolla, joille on tunnusomaista se, mitä sanotaan itsenäisissä patenttivaatimuksissa. Käsitteellä laitteisto tarkoitetaan tässä palvelevan verkon verkkoelementtiä, päätelaitetta tai muuta vastaavaa palvelualustaa, jonne palvelulogiikka voidaan ladata. Keksinnön edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Keksintö perustuu ajatukseen muodostaa palvelulogiikka kahdesta osasta: käyttäjän autentikoinnista ja varsinaisesta palvelulogiikasta. Käyttäjän autentikoimisessa tarvittava tieto liitetään palvelulogiikkaan ja käyttäjä autentikoidaan aina ennen varsinaisen palvelulogiikan suorittamista. Tällä saavutetaan se etu, että palvelulogiikan luvaton käyttö ja kopiointi estetään. Vain ne käyttäjät, joille palvelu on tilattu ja joilla siten on oikeus käyttää palvelua, voivat käyttää sitä.

Keksinnön eräässä edullisessa suoritusmuodossa palveluoperaattori verifioidaan aina ennen palvelun suorittamista. Tämä parantaa huomattavasti käyttäjän ja mahdollisen palvelualustan, jolle palvelulogiikka ladataan, turvallisuutta. Näin varmistetaan, että palvelulogiikka on todella peräisin palveluoperaattorilta.

Keksinnön eräässä edullisessa suoritusmuodossa käyttäjän autentikointiin käytetään käyttäjän yksilöinnissä käytettävää tilaajan tunnistetta. Tästä on se etu, että tilaajan autentikointi on yksinkertaista, mutta luotettavaa.

Keksinnön eräässä edullisessa suoritusmuodossa palvelulogiikka tallennetaan muistiin käyttäjä- ja autentikointitietoineen palvelualustalle, jonne se ladataan ja uutta käyttäjää varten ladataan vain uuden käyttäjän autentikointitieto. Tästä on se etu, että palvelulogiikkaa ei tarvitse ladata monta kertaa peräkkäin, jolloin verkon kuormitus vähenee.

Kuvioluettelo

Keksintöä selostetaan nyt lähemmin edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirustuksiin, joista

kuvio 1 havainnollistaa IMT-2000 arkkitehtuuria,

kuvio 2 esittää vuokaaviota palvelualustan toiminnoista keksinnön ensimmäisessä edullisessa suoritusmuodossa,

kuvio 3 on signalointikaavio keksinnön toisessa edullisessa suoritusmuodossa, ja

kuvio 4 esittää palveluoperaattorin palvelua ohjaavan verkkoelementin toimintaa kolmannessa edullisessa suoritusmuodossa.

Keksinnön yksityiskohtainen selostus

Esillä olevaa keksintöä voidaan soveltaa minkä tahansa tiedonsiirtojärjestelmän yhteydessä, jossa käyttäjä voi saada hänelle tilatut palvelut mihin tahansa palvelujen välitystä tukevaan päätelaitteeseen. Jäljempänä keksintöä on selostettu käyttäen esimerkkijärjestelmänä IMT-2000-järjestelmää keksintöä kuitenkaan tällaiseen tiettyyn järjestelmään rajaamatta. Matkaviestinjärjestelmien yleensä ja erityisesti IMT-2000- ja UMTS-järjestelmien määritykset kehittyvät nopeasti. Tällainen kehitys voi vaatia keksintöön ylimääräisiä muutoksia. Sen vuoksi kaikki sanat ja ilmaisut tulisi tulkita laajasti ja ne on tarkoitettu kuvaamaan eikä rajoittamaan keksintöä. Oleellista keksinnön kannalta on toiminto, eikä se, missä verkkoelementissä tai laitteessa toiminto suoritetaan.

Kuviossa 1 on esitetty IMT-2000-järjestelmän verkkoarkkitehtuuri karkealla tasolla, koska järjestelmämääritykset ovat parhaillaan työn alla. Verkon yksityiskohtaisemmalla rakenteella ei ole keksinnön kannalta olennaista merkitystä. Kolmannen sukupolven matkaviestinverkoissa erotellaan palveluoperaattori SP (service provider) ja verkko-operaattori (network operator) toisistaan. Palveluoperaattori tarjoaa palveluja loppukäyttäjälle yhden tai useamman verkko-operaattorin verkon SN välityksellä. Tällaisesta verkosta SN käytetään nimitystä palveleva verkko. Palveluoperaattori voi tarjota palvelua yhden tai useamman verkko-operaattorin palvelevan verkon SN välityksellä. Sen lisäksi palveluoperaattori voi vaihtaa palvelevaa verkkoa kesken palvelun niin, että käyttäjä ei huomaa vaihdosta. Palveluoperaattori voi olla myös verkko-operaattori. Palveleva verkko SN käsittää varsinaisen tilaajaverkon AN (access network) ja yhden tai useamman ydinverkon CN (core networks) sekä verkkojen välisen yhteistoimintayksikön IWU (Interworking Unit adapting interfaces) kutakin eri tyyppistä ydinverkkoa varten. Nykytietämyksen mukaan tilaajaverkko käsittää tukiasemia BS (Base Station) ja niitä ohjaavia radioverkko-ohjaimia (ei ole

esitetty kuvassa). Ydinverkkona voi toimia esimerkiksi yleiseurooppalainen matkaviestinjärjestelmän GSM (Global System for Mobile Communication) mukainen verkko. Ydinverkon CN välityksellä saadaan yhteys muihin verkkoihin ON.

Kuvion 1 esimerkissä laajennettu kotirekisteri HLRi (Home Location Register with IMT-2000 enhancement) ja palvelujen ohjaussolmu SCN (Service Control Node) on sijoitettu palvelevaan verkkoon SN. Laajennettu kotirekisteri HLRi sisältää ydinverkon kotirekisteritietojen lisäksi IMT-2000-järjestelmässä tarvittavat tilaaja- ja palvelutiedot. Näitä IMT-2000-tietoja ylläpitää palvelujen osalta palveluoperaattori SP. Tilaaja tekee tilaussopimuksen palveluoperaattorin kanssa, joka laskuttaa tilaajaa palvelujen käytöstä. Palvelujen ohjaussolmu SCN on eräs palvelualusta, jolle voidaan ladata ja jossa voidaan suorittaa palveluun liittyvä palvelulogiikka. Palvelun ohjaussolmu SCN voi myös huolehtia palvelun lataamisesta muualle verkkoon ja välittää palvelupyyntöjä käyttäjältä palveluoperaattorille. Sen lisäksi palvelun ohjaussolmu SCN huolehtii siitä, että kotiverkon palvelut ovat käytettävissä myös vierailtavissa verkoissa (visited networks).

Kolmannen sukupolven matkaviestinverkoissa myös tilaaja (subscriber) ja käyttäjä (user) erotellaan. Tilaaja antaa käyttäjälle käyttöoikeuden tilattuihin palveluihin luovuttamalla käyttäjälle identifiointikortin (IC Card), esimerkiksi USIM-kortin (User and Services and Identity Module). Käyttäjä saa palvelut käyttöönsä päätelaitteella MT (Mobile Terminal), joka on tukiasemien BS välityksellä radioteitse yhteydessä palvelevaan verkkoon SN. Liikuteltava päätelaite MT koostuu varsinaisesta matkaviestinlaitteesta ME (Mobile Equipment) ja siihen irrotettavasti kytketystä identifiointikortista USIM, josta käytetään myös nimitystä tilaajan tunnistusyksikkö. Se on päätelaitteesta irrotettavissa oleva älykortti, jonka avulla tilaaja voi käyttää korttiohjattua päätelaitetta. Käyttäjä tunnistetaan päätelaitteeseen syötetyn kortin eikä itse laitteen perusteella. Nykytietämyksen mukaan USIM on monitoimikortti ja se tukee matkaviestinjärjestelmän sovelluksia sekä muita sovelluksia, kuten Java-sovellukset, terveydenhuollon tarvitsemat sovellukset jne. Tilaaja voi tilata palveluja usealta eri palveluoperaattorilta samalle tilaajan tunnistusyksikölle USIM. Tilaaja ja käyttäjä voivat olla sama henkilö. Tilaajan tunnistusyksikköön USIM on tallennettu kansainvälinen matkaviestintilaajan tunnus IMSI, jonka avulla tilaaja voidaan tunnistaa yksikäsitteisesti ja jota voidaan käyttää myös

käyttäjän tunnistamiseen. Matkaviestintilaajan tunnuksesta käytetään nimitystä tilaajan tunnus.

Kolmannen sukupolvien järjestelmien päätelaitevalikoima muodostunee erittäin monipuoliseksi. Päätelaite voi olla pelkistetty, ainoastaan puhetta välittävä päätelaite tai se voi olla monipuolisia palveluja välittävä päätelaite, joka toimii palvelualustana ja tukee erilaisten palvelulogiikkojen lataamista ja suorittamista.

Esillä olevan keksinnön mukaisen toiminnallisuuden toteuttava matkaviestinjärjestelmä käsittää tekniikan tason mukaiseen palvelujen aikaansaamisessa ja lataamisessa tarvittavien välineiden lisäksi välineitä autentikointitiedon liittämiseksi palvelulogiikkaan ja välineitä käyttäjän autentikoimiseksi ennen palvelulogiikan suorittamista. Liittämisellä tarkoitetaan tässä myös tiedon upottamista palvelulogiikkaan. Sen lisäksi järjestelmä voi käsittää välineitä palveluoperaattorin verifioimiseksi ja välineitä palvelulogiikan tallentamiseksi muistiin oheistietoineen ja välineitä pelkän autentikointitiedon vastaanottamiseksi. Autentikointitiedon liittämisvälineet ja mahdolliset verifiointitiedon liittämisvälineet sijaitsevat edullisesti palveluoperaattorin palvelulogiikan lataamisessa tarvittavien välineiden yhteydessä. Muut välineet sijaitsevat edullisesti palvelualustan yhteydessä, esimerkiksi päätelaitteessa tai verkko-operaattorin palvelujen ohjauspisteessä. Välineet tai osa niistä voivat sijaita myös muualla, esimerkiksi tilaajaverkon verkkosolmussa tai ydinverkon palvelevassa tukisolmussa.

Kuvio 2 esittää vuokaaviota keksinnön ensimmäisen edullisen suoritusmuodon mukaisesta toiminnasta palvelualustalla, joka voi olla esimerkiksi varsinainen päätelaite ME tai palvelunohjaussolmu SCN. Keksinnön ensimmäisessä edullisessa suoritusmuodossa hyödynnetään sinänsä tunnettua julkiseen avaimeen perustuvaa salaustekniikkaa uudella ja keksinnöllisellä tavalla. Eräs tällainen salaustekniikka on RSA (Rivest Shamir Adleman public-key cryptographic algorithm), jota voidaan käyttää sekä salaukseen että digitaaliseen allekirjoitukseen. Ensimmäisessä edullisessa suoritusmuodossa tilaajan tunnistusyksikköön USIM tallennetaan ainakin tilaajan salainen avain ja palveluoperaattorin julkinen avain. Jos tilaajalla on useita avainpareja, tallennetaan sen parin salainen avain, jonka julkinen avain on merkitty käyttäjän tilaajatietoihin. Vastaavasti palveluoperaattorilla voi olla useita avainpareja, joista esimerkiksi yksi tallennetaan tilaajan tunnistusyksikköön ja tilaajatietoihin merkitään, minkä parin avain on

tallennettu tunnistusyksikköön. Näin varmistetaan se, että käytetään saman parin salaista ja julkista avainta. Ensimmäisessä edullisessa suoritusmuodossa palveluoperaattori verifioidaan digitaalisella allekirjoituksella. Se aikaansaadaan ensimmäisessä edullisessa suoritusmuodossa laskemalla palvelulogiikasta yksisuuntainen sekasumma (one way hash funktion), joka salataan. Tämän suoritusmuodon yllättävä etu on, että palveluoperaattorin verifioinnin yhteydessä tarkistetaan samalla myös se, onko palvelulogiikkaa muutettu. Jos palvelulogiikkaa on muutettu, muuttuu siitä laskettu sekasumma, eikä palveluoperaattori enää verifioidu.

Viitaten kuvioon 2 kohdassa 200 vastaanotetaan palvelua S1 koskeva palvelupyyntö käyttäjältä U1. Kohdassa 201 tarkistetaan, onko palveluun S1 liittyvä palvelulogiikka SL1 muistissa. Jos se ei ole muistissa, välitetään palvelupyyntö palveluoperaattorille kohdassa 202. Palveluoperaattori etsii palveluun S1 liittyvän varsinaisen palvelulogiikan SL1 sekä liittää palvelulogiikkaan käyttäjän autentikoinnissa tarvittavan autentikointitiedon A1, joka ensimmäisessä edullisessa suoritusmuodossa on tilaajan julkinen avain. Sen jälkeen palveluoperaattori laskee varsinaisesta palvelulogiikasta ja autentikointitiedosta sekasumman hash ja liittää sen verifiointitiedoksi V1 palvelulogiikkaan ja salaa näin syntyneen tiedoston omalla salaisella avaimellaan. Tiedosto sisältää verifiointitiedon V1, autentikointitiedoston A1 ja varsinaisen palvelulogiikan SL1. Vaihtoehtoisesti palveluoperaattori voisi salata sekasumman hash salaisella avaimellaan, liittää salatun sekasumman verifiointitiedoksi V1 tiedostoon ja salata sitten tiedoston käyttäjän julkisella avaimella. Sen jälkeen kohdassa 203 ladataan palvelualustalle tiedosto eli palveluun S1 liittyvä varsinainen palvelulogiikka SL1 sekä siihen käyttäjää U1 varten liitetty autentikointitieto A1 ja niistä laskettu verifiointitieto V1. Kohdassa 204 tallennetaan palvelulogiikka SL1 ja siihen käyttäjälle U1 liittyvä autentikointitieto A1 ja verifiointitieto V1 sekä tietysti tieto käyttäjästä U1, johon autentikointitieto A1 ja verifiointitieto V1 liittyy. Tiedot säilytetään muistissa salattuna. Sen jälkeen ensimmäisessä edullisessa suoritusmuodossa pyydetään käyttäjän päätelaitteessa olevalta tilaajan tunnistusyksiköltä USIM palveluoperaattorin julkista avainta kohdassa 205 ja vastaanotetaan se kohdassa 206, jonka jälkeen puretaan palvelulogiikan SL1, autentikointitiedon A1 ja verifiointitiedon V1 salaus kohdassa 207 vastaanotettua avainta käyttäen. Sellaisissa suoritusmuodoissa, joissa palveluoperaattorilla on vain yksi avainpari, tieto operaattorin julkisesta avaimesta voi olla jo

palvelualustalla, jolloin sitä ei tarvitse erikseen kysyä. Kun salaukset on purettu verifioidaan palveluoperaattori laskemalla kohdassa 208 sekasumma hash palvelulogiikasta ja autentikointitiedosta ja vertaamalla näin laskettua sekasummaa hash verifiointitietoon V1 kohdassa 209. Jos ne ovat samat, onnistui palveluoperaattorin verifiointi ja sen jälkeen valitaan haaste eli joku merkkijono kohdassa 210. Sillä, miten haaste valitaan, ei ole keksinnön kannalta merkitystä. Yksinkertainen ja turvallinen ratkaisu on käyttää satunnaislukugeneraattoria, jolloin haaste on satunnainen luku. Valittu haaste salataan kohdassa 211 tilaajan julkisella avaimella eli autentikointitiedolla A1. Sen jälkeen salattu haaste lähetetään kohdassa 212 palvelua pyytäneen käyttäjän U1 päätelaitteessa olevalle tilaajan tunnistusyksikölle USIM, joka purkaa salatun haasteen selväkieliseksi tekstiksi (plain text) tilaajan salaisella avaimella ja lähettää selväkielisen tekstin takaisin palvelualustalle. Palvelualusta vastaanottaa selväkielisen tekstin kohdassa 213 ja vertaa kohdassa 214 alkuperäistä haastetta selväkieliseen tekstiin. Jos merkkijonot ovat samat, läpäistään käyttäjän autentikointi ja varsinainen palvelulogiikka SL1 voidaan suorittaa kohdassa 215.

Jos kohdassa 209 havaitaan, että laskettu sekasumma hash ei ole sama kuin verifiointieto, ei palveluoperaattori verifioidu tai palvelulogiikkaa on muutettu. Molemmissa tapauksissa palvelulogiikan suorittaminen olisi turvallisuusriski, ja siksi palvelulogiikkaa ei suoriteta, vaan kohdassa 217 poistetaan muistista palvelua S1 varten tallennetut tiedot eli palvelulogiikka SL1 sekä kaikki siihen liitetyt autentikointi- ja verifiointitiedot käyttäjätietoineen.

Jos kohdassa 214 havaitaan, että haaste ei ole sama kuin selväkielinen teksti, autentikointia ei läpäistä eikä palvelulogiikkaa suoriteta, vaan poistetaan kohdassa 216 muistista palvelun S1 palvelulogiikkaan SL1 liitetty autentikointitieto A1, verifiointitieto V1 ja tieto käyttäjästä U1. Näin varsinaista palvelulogiikkaa SL1 ei tarvitse seuraavalla kerralla ladata, autentikointitiedon ja verifiointitiedon lataus riittää.

Jos kohdassa 201 havaitaan, että palveluun S1 liittyvä palvelulogiikka SL1 on muistissa, tarkistetaan kohdassa 218, liittyykö siihen käyttäjälle U1 autentikointi- ja verifiointitietoa. Jos myös ne ovat muistissa, siirrytään kohtaan 205 pyytämään palveluoperaattorin julkista avainta tilaajan tunnistusyksiköltä USIM. Kohdasta 205 jatketaan edellä esitetyllä tavalla. Näin verkon resursseja säästetään, kun kertaalleen ladattuja tietoja ei tarvitse enää ladata.

Jos kohdassa 218 havaitaan, että muistissa olevaan palvelulogiikkaan SL1 ei liity käyttäjälle U1 autentikointi- ja verifiointitietoa, pyydetään kohdassa 219 palveluoperaattorilta käyttäjälle U1 autentikointitieto ja verifiointitieto palvelulle S1. Autentikointitieto A1 ja verifiointitieto V1 vastaanotetaan kohdassa 220, jonka jälkeen ne ja tieto käyttäjästä U1 liitetään palvelulogiikan SL1 yhteyteen kohdassa 221. Sen jälkeen siirrytään kohtaan 205 pyytämään palveluoperaattorin julkista avainta tilaajan tunnistusyksiköltä USIM. Kohdasta 205 jatketaan edellä esitetyllä tavalla.

Palvelualustana voi toimia varsinainen päätelaite ME tai jokin palvelevan verkon verkkoelementti, kuten esimerkiksi palvelunohjaussolmu SCN. Muisti, jonne tiedot ja palvelulogiikat tallennetaan, voi olla myös välimuisti (cache). Suoritusmuodoissa, joissa palvelulogiikka tallennetaan muistiin, palvelualusta voi käsittää välineitä palvelulogiikan poistamiseksi muistista ennalta määritellyistä syistä, esimerkiksi tietyn ajan kuluttua.

Niissä suoritusmuodoissa, joissa palvelulogiikkaa ei tallenneta muistiin, suoritetaan kohdat 200, 202, 203 ja 205-215. Kohdissa 216 ja 217 esitettyjä tietojen poistamista muistista ei tehdä, vaan jätetään varsinainen palvelulogiikka suorittamatta.

Edellä kuviossa 2 esitetyt kohdat eivät ole absoluuttisessa aikajärjestyksessä ja osa kohdista voidaan suorittaa samanaikaisesti tai esitetystä järjestyksestä poiketen. Kohtien välissä voidaan myös suorittaa muita toimintoja. Osa kohdista, kuten esimerkiksi palveluoperaattorin verifiointi, voidaan myös jättää pois. Olennaista on käyttäjän autentikointi ennen varsinaisen ladatun palvelulogiikan suorittamista.

Kuviossa 3 esitetään keksinnön toisen edullisen suoritusmuodon mukaista signalointia. Toisessa edullisessa suoritusmuodossa autentikointitietona käytetään tilaajan tunnusta IMSI. Lisäksi oletetaan, että palvelulogiikka ladataan varsinaiseen päätelaitteeseen ME eikä sitä tallenneta sinne muistiin.

Viitaten kuvioon 3 käyttäjä U antaa käyttöliittymän välityksellä päätelaitteelle ME sanomassa 3-1 tiedon, että hän haluaa palvelua S. Päätelaite ME lähettää palvelevan verkon välityksellä palvelupyynnön palveluoperaattorille SP sanomassa 3-2. Palvelupyyntö sisältää tiedon halutusta palvelusta S sekä palvelua haluavasta käyttäjästä U. Kohdassa 3-3 palveluoperaattori tarkistaa, onko käyttäjälle U tilattu palvelu S. Jos käyttäjälle ei ole tilattu palvelua S, lähettää palveluoperaattori palvelevan verkon

välityksellä sanomassa 3-4 negatiivisen kuittauksen palvelupyyntöön päätelaitteelle ME, joka välittää tiedon sanomassa 3-5 käyttöliittymän välityksellä käyttäjälle U.

Jos käyttäjälle on tilattu palvelu S, hakee palveluoperaattori käyttäjän U tilaajan tunnuksen IMSI-A ja palveluun S liittyvän ladattavan palvelulogiikan SL ja laskee niistä sekasumman hash. Sen jälkeen palveluoperaattori salaa palvelulogiikan siihen liittyvine tietoineen (IMSI-A, hash) palveluoperaattorin salaisella avaimella. Palveluoperaattori lähettää sanomassa 3-6 palvelulogiikan SL, tunnuksen IMSI-A ja sekasumman hash päätelaitteelle ME. Vastaanotettuaan sanoman 3-6 pyytää päätelaite ME toisessa edullisessa suoritusmuodossa tilaajan tunnistusyksiköltä USIM palveluoperaattorin julkista avainta sanomassa 3-7. Tilaajan tunnistusyksikkö USIM lähettää sen päätelaitteelle sanomassa 3-8, jonka jälkeen päätelaite ME verifioi palveluoperaattorin kohdassa 3-9. Päätelaite purkaa palvelulogiikan SL, tilaajan tunnuksen A1 ja sekasumman hash salauksen vastaanottamallaan julkisella avaimella ja laskee palvelulogiikan ja tilaajan tunnuksen IMSI-A yhdistelmästä sekasumman hash. Jos laskettu sekasumma ei ole sama kuin sanomassa 3-6 vastaanotettu sekasumma, verifiointi ei onnistunut. Tällöin palvelulogiikkaa ei suoriteta, vaan päätelaite ME lähettää käyttöliittymän välityksellä sanomassa 3-10 tiedon verifioinnin epäonnistumisesta käyttäjälle U esimerkiksi ilmoittamalla, että palvelua ei saada.

Jos kohdassa 3-9 laskettu sekasumma ja vastaanotettu sekasumma ovat samat, verifiointi onnistui ja päätelaite ME pyytää tilaajan tunnistusyksiköltä USIM käyttäjän U tilaajan tunnusta IMSI sanomassa 3-11. Tilaajan tunnistusyksikkö USIM hakee muististaan tilaajan tunnuksen IMSI-B ja lähettää sen päätelaitteelle ME sanomassa 3-12. Päätelaite autentikoi käyttäjän kohdassa 3-13 tarkistamalla, onko palveluoperaattorilta vastaanotettu IMSI-A sama kuin tunnistusyksiköltä vastaanotettu IMSI-B. Jos käyttäjä läpäisee autentikoinnin kohdassa 3-9 (eli IMSI-A on sama kuin IMSI-B), suorittaa päätelaite ME varsinaisen palvelulogiikan SL ja välittää sanomissa 3-14 käyttöliittymän välityksellä palvelun käyttäjälle U. Jos tilaajan tunnusten IMSI arvot eroavat toisistaan, autentikointia ei läpäistä. Tällöin päätelaite ei suorita varsinaista palvelulogiikkaa, vaan ilmoittaa käyttöliittymän välityksellä sanomassa 3-10 käyttäjälle U, että autentikointi epäonnistui esimerkiksi ilmoittamalla, että palvelua ei saada.

Edellä kuvion 3 yhteydessä esitetyt signalointisanomat ovat vain viitteellisiä ja voivat sisältää useitakin erillisiä sanomia saman tiedon välittämiseksi. Sen lisäksi sanomat voivat sisältää muutakin tietoa. Sanomia voidaan myös yhdistellä vapaasti. Niissä suoritusmuodoissa, joissa palveluoperaattoria ei verifioida, jätetään verifiointiin liittyvät sanomat 3-7, 3-8 ja 3-10 sekä kohta 3-9 pois. Operaattoreista ja ydinverkosta ja päätelaitteista riippuen tietojen välitykseen ja signalointiin voivat osallistua muutkin verkkoelementit, joihin eri toiminnallisuuksia on hajotettu.

Kuvio 4 esittää vuokaaviota keksinnön kolmannessa edullisessa suoritusmuodossa palveluoperaattorin palvelua ohjaavassa verkkoelementissä. Kolmannessa edullisessa suoritusmuodossa autentikointi ja verifiointi suoritetaan ainoastaan silloin, kun palvelulogiikka ladataan vierailuverkkoon (visiting network) tai päätelaitteeseen. Vierailuverkko on palveleva verkko, jonka verkkoelementti, johon palvelu ladataan, on jonkun muun operaattorin kuin palveluoperaattorin verkkoelementti. Kolmannessa edullisessa suoritusmuodossa hyödynnetään sekä julkisen avaimen salaustekniikkaa että symmetristä salaustekniikkaa, kuten esimerkiksi DES (Data Encryption Standard). Viimeksi mainittua salaustekniikkaa käytetään silloin, kun palvelulogiikka ladataan päätelaitteeseen. Sitä varten on sekä tilaajan tunnistusyksikköön että käyttäjän tilaajatietoihin tallennettu yhteinen avain. Sen lisäksi vierailtaviin verkkoihin ladattavia palvelulogiikkoja varten tilaajan tunnistusyksikköön on tallennettu palveluoperaattorin julkinen avain. Allekirjoituksena käytetään ainoastaan palvelulogiikan salaamista palveluoperaattorin salaisella avaimella ennen palvelulogiikan lähettämistä palvelevaan verkkoon tai salaamista yhteisellä avaimella ennen lataamista päätelaitteeseen.

Viitaten kuvioon 4 kohdassa 400 vastaanotetaan palvelua S2 koskeva palvelupyyntö käyttäjältä U2. Kohdassa 401 tarkistetaan, onko käyttäjälle U2 tilattu palvelu S2. Jos käyttäjälle on tilattu palvelu S2 tarkistetaan kohdassa 402, onko palveluun S2 liittyvä palvelulogiikka SL2 sellainen, että se pitää ladata käyttäjän päätelaitteeseen ME. Jos palvelulogiikka SL2 ladataan käyttäjän päätelaitteeseen, haetaan kohdassa 403 käyttäjän U2 tilaajatiedoista yhteinen avain, jolla palvelulogiikka SL2 salataan kohdassa 404. Tätä yhteistä avainta käytetään sekä käyttäjän autentikointitietona että palveluoperaattorin verifiointitietona. Kenelläkään muulla ei pitäisi olla tietoa siitä, mikä on yhteinen avain tässä tapauksessa. Autentikointi ja

verifiointi tapahtuvat palvelulogiikan salauksen purkamisen yhteydessä. Salattu palvelulogiikka SL2 ladataan päätelaitteeseen ME kohdassa 405. Käyttäjä autentikoidaan ja palveluoperaattori verifioidaan päätelaitteessa esimerkiksi lähettämällä salattu palvelulogiikka päätelaitteessa olevaan tilaajan tunnistusyksikköön USIM, joka purkaa palvelulogiikan salauksen käyttäen muistissaan olevaa yhteistä avainta ja lähettää selväkielisen palvelulogiikan päätelaitteelle. Kun palvelulogiikka on saatu suoritettua, vastaanotetaan tieto siitä kohdassa 406, jonka jälkeen tilaajaa laskutetaan palvelun käytöstä kohdassa 407.

Jos kohdassa 402 havaitaan, että palvelulogiikkaa SL2 ei ladata päätelaitteeseen, tarkistetaan kohdassa 408, onko käyttäjä U2 kotiverkon alueella. Jos on, niin suoritetaan palvelulogiikka SL2 kohdassa 409, jonka jälkeen siirrytään kohtaan 407, jossa tilaajaa laskutetaan palvelun käytössä.

Jos kohdassa 408 havaitaan, että käyttäjä ei ole kotiverkon alueella, täytyy palvelulogiikka SL2 ladata vierailuverkkoon kolmannessa edullisessa suoritusmuodossa. Sen vuoksi tilaajatiedoista haetaan palvelulogiikkaan liitettäväksi autentikointitiedoksi käyttäjän U2 julkinen avain kohdassa 410. Kohdassa 411 liitetään käyttäjän julkinen avain palvelulogiikkaan SL2 ja salataan ne käyttäen palveluoperaattorin salaista avainta kohdassa 412. Salaus toimii samalla verifiointitietona. Jos palveluoperaattorilla on useita julkisen ja salaisen avaimen avainpareja, käytetään sitä salaista avainta, jonka parin julkinen avain on tallennettu käyttäjän tunnistusyksikköön. Salattu palvelulogiikka, johon autentikointitieto on liitetty, ladataan vierailuverkkoon kohdassa 413. Vierailuverkon verkkoelementti verifioi palveluntarjoajan purkamalla palvelulogiikan käyttäen palveluoperaattorin julkista avainta ja autentikoi käyttäjän esimerkiksi kuvion 2 yhteydessä esitetyllä tavalla, jonka jälkeen palvelulogiikka suoritetaan. Kun palvelulogiikka on saatu suoritettua, vastaanotetaan tieto siitä kohdassa 406, jonka jälkeen tilaajaa laskutetaan palvelun käytöstä kohdassa 407.

Jos kohdassa 411 havaittiin, että käyttäjälle ei ole tilattu pyydettyä palvelua, lähetetään tieto siitä, että käyttäjä ei saa palvelua kohdassa 414.

Edellä kuvion 4 yhteydessä oletettiin, että autentikointi läpäistään ja verifiointi onnistuu. Jos näin ei käy, ei palvelulogiikkaa suoriteta eikä tilaajaa laskuteta. Kuvion 4 yhteydessä esitetyt kohdat eivät ole absoluuttisessa aikajärjestyksessä ja osa kohdista voidaan suorittaa samanaikaisesti tai esitetystä järjestyksestä poiketen. Kohtien välissä voidaan suorittaa myös

muita toimintoja. Osa kohdista voidaan myös jättää pois. Oleellista on, että autentikointitieto liitetään jollain tavalla ladattavaan palvelulogiikkaan.

Edellä esitetyissä suoritusmuodoissa on muutettu varsinaista palvelulogiikkaa sen varmistamiseksi, että autentikointi ja verifiointi suoritetaan. Se on tehty lisäämällä palvelulogiikkaan autentikoinnista ja verifioinnista huolehtiva osa, joka suoritetaan aina ennen palvelulogiikkaa. Joissakin suoritusmuodoissa palvelulogiikkaa voidaan muuttaa ainoastaan autentikoinnin varmistamiseksi. Joissakin suoritusmuodoissa palvelulogiikkaa ei tarvitse muuttaa, vaan autentikointi- ja mahdolliset verifiointitiedot liitetään palvelulogiikan oheen erillisiksi tiedoiksi ja palvelualustalla huolehditaan siitä, että autentikointi ja mahdollinen verifiointi suoritetaan. Näissä suoritusmuodoissa voidaan käyttää jo valmiiksi salattuja palvelulogiikkoja, jolloin säästetään verkkoelementin kuormitusta, koska salaus tehdään vain kerran.

Edellä on kuvioiden 2, 3 ja 4 yhteydessä oletettu, että palveluoperaattori liittää autentikointitiedon palvelulogiikkaan ennen salausta. Autentikointitieto voidaan liittää myös ennalta salattuun palvelulogiikkaan. Tällöin myös palveleva verkko tai päätelaite voi olla sovitettu liittämään autentikointitiedon palvelulogiikkaan esimerkiksi palvelupyynnön ilmaiseman käyttäjätiedon avulla. Edellä on esitetty, että käyttäjä autentikoidaan vasta verifioinnin jälkeen. Järjestyksellä ei kuitenkaan ole keksinnön kannalta merkitystä. Käyttäjä voidaan autentikoida ennen palveluoperaattorin verifiointia niissä suoritusmuodoissa, joissa myös palveluoperaattori verifioidaan. Tietoja ja/tai palvelulogiikkaa ei ole myöskään välttämätön salata ellei salausta käytetä autentikointiin ja/tai verifiointiin. Autentikointiin, verifiointiin ja mahdolliseen salaukseen voidaan käyttää myös muita, kuin edellä edullisten suoritusmuotojen yhteydessä esitettyjä vaihtoehtoja. Edullisia suoritusmuotoja voidaan myös yhdistää. Oleellista on, että käyttäjä autentikoidaan ennen palvelulogiikan suorittamista ainakin silloin, kun palvelulogiikka ladataan päätelaitteeseen tai vierailuverkkoon. Niissä suoritusmuodoissa, joissa palvelulogiikka ladataan päätelaitteeseen, voidaan autentikointitietona käyttää myös palvelulogiikan salaamista tilaajan julkisella avaimella. Tilaaja autentikoidaan, kun tunnistusyksikkö USIM purkaa salauksen tilaajan salaisella avaimella. Turvallisuuden kannalta on edullista, että USIM ei koskaan lähetä edes päätelaitteelle sinne tallennettua salaista avainta, vaan salauksen purkaminen tällaisella salaisella avaimella suoritetaan aina

USIM:ssa. Autentikointiin ja mahdolliseen verifiointiin voidaan käyttää myös muita tietoja kuin edellä olevissa esimerkeissä on käytetty. Vaatimukset autentikointitiedolle ja mahdollisille verifiointitiedolle on niiden riittävä yksilöivyys, luotettavuus ja kiistämättömyys. Riittävällä yksilöivyydellä tarkoitetaan sitä, että ne yksilöivät käyttäjän ainakin tilaajakohtaisesti.

Palvelevan verkon rakenteeseen ei tarvita laitteistomuutoksia. Se käsittää prosessoreita ja muistia, jota voidaan hyödyntää keksinnön mukaisissa toiminnoissa. Sen sijaan kaikki keksinnön toteuttamiseen tarvittavat muutokset voidaan suorittaa lisättyinä tai päivitettyinä ohjelmistorutiineina niissä verkkoelementeissä, joihin palvelulogiikka ladataan. Esimerkki tällaisesta verkkoelementistä on palvelunohjaussolmu. Ladatun palvelulogiikan oheistietoineen tallentavassa verkkoelementissä tarvitaan myös lisämuistia.

Palveluoperaattorin rakenteeseenkaan ei tarvita laitteistomuutoksia. Palveluoperaattori käsittää prosessoreita ja muistia, joita voidaan hyödyntää keksinnön mukaisissa toiminnoissa. Kaikki keksinnön toteuttamiseen tarvittavat muutokset voidaan suorittaa lisättyinä tai päivitettyinä ohjelmistorutiineina keksinnön mukaisen toiminnallisuuden aikaansaamiseksi. Keksinnön suoritusmuodosta riippuen voidaan tarvita lisämuistia. Se rajoittuu kuitenkin pieneen määrään, joka riittää tallentamaan ylimääräiset autentikointi- ja mahdolliset verifiointitiedot.

Päätelaitteen rakenteeseen ei tarvita laitemuutoksia. Se käsittää prosessoreita ja muistia, jota voidaan hyödyntää keksinnön mukaisissa toiminnoissa. Sen sijaan kaikki keksinnön toteuttamiseen tarvittavat muutokset voidaan suorittaa lisättyinä tai päivitettyinä ohjelmistorutiineina päätelaitteessa, joka on sovitettu toimimaan palvelualustana. Jos palvelulogiikka tallennetaan päätelaitteeseen, tarvitaan myös lisämuistia.

Tilaajan tunnistusyksikössä USIM keksinnön toteuttamiseen mahdollisesti vaadittava lisämuisti rajoittuu pieneen määrään, joka riittää tallentamaan ylimääräiset autentikointi- ja mahdolliset verifiointitiedot sekä mahdollisesti tarvittavat salauksen purkualgoritmit.

On ymmärrettävä, että edellä oleva selitys ja siihen liittyvät kuviot on ainoastaan tarkoitettu havainnollistamaan esillä olevaa keksintöä. Alan ammattilaisille tulevat olemaan ilmeisiä erilaiset keksinnön variaatiot ja muunnelmat ilman, että poiketaan oheisissa patenttivaatimuksissa esitetyn keksinnön suojapiiristä ja hengestä.

Patenttivaatimukset

1. Menetelmä palvelun luvattoman käytön estämiseksi matkaviestinjärjestelmässä, jossa menetelmässä

vastaanotetaan palvelun käyttäjältä palvelupyyntö, ja

aikaansaadaan palvelu palvelulogiikan avulla,

t u n n e t t u siitä, että menetelmässä

liitetään palvelulogiikkaan autentikointitieto (3-6),

autentikoidaan palvelua pyytävä käyttäjä autentikointitiedon avulla (3-9), ja

suoritetaan palvelulogiikka (3-14) vain, mikäli autentikointi läpäistään.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että

liitetään palvelulogiikkaan lisäksi palveluoperaattorin verifiointitieto,

verifioidaan palveluoperaattori käyttäjän autentikoinnin yhteydessä (3-13), ja

suoritetaan palvelulogiikka vain, mikäli lisäksi verifiointi onnistuu.

3. Patenttivaatimuksen 2 mukainen menetelmä, t u n n e t t u siitä, että

käytetään palvelulogiikan verifiointitietona palvelulogiikasta laskettua ensimmäistä sekasummaa,

ladataan palvelulogiikka palvelualustalle, jossa se suoritetaan palvelun aikaansaamiseksi,

verifioidaan palveluoperaattori palvelualustalla laskemalla palvelulogiikasta toinen sekasumma, ja

mikäli ensimmäinen ja toinen sekasumma ovat samat, verifiointi onnistuu,

mikäli ensimmäinen ja toinen sekasumma eroavat toisistaan, verifiointi epäonnistuu.

4. Patenttivaatimuksen 2 mukainen menetelmä, t u n n e t t u siitä, että

käytetään verifiointitietona palveluoperaattorin allekirjoitusta,

allekirjoitetaan palvelulogiikka salaamalla se palveluoperaattorin salaisella avaimella, ja

verifioidaan palveluoperaattori purkamalla palvelulogiikan salaus palveluoperaattorin julkisella avaimella.

5. Jonkin edellä olevan patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

tallennetaan palvelun käyttäjällä olevaan tilaajan tunnistusyksikköön (USIM) tilaajan salainen avain,

käytetään autentikointitietona tilaajan julkista avainta,

lähetetään palvelua pyytäneen käyttäjän päätelaitteessa olevaan tilaajan tunnistusyksikköön tilaajan julkisella avaimella salattu haaste (207),

puretaan tunnistusyksikössä tilaajan salaisella avaimella haaste selväkieliseksi tekstiksi,

vastaanotetaan tunnistusyksiköltä selväkielinen teksti (208),

tarkistetaan, vastaavatko salaamaton haaste ja selväkielinen teksti toisiaan (209), ja

mikäli vastaavat, autentikointi läpäistään, ja

mikäli eivät vastaa, autentikointia ei läpäistä.

6. Patenttivaatimuksen 1, 2, 3 tai 4 mukainen menetelmä, t u n n e t t u siitä, että

käytetään autentikointitietona tilaajan yksilöivää tunnusta,

vastaanotetaan palvelupyyntö käyttäjältä (3-1),

kysytään käyttäjään liittyvää tilaajan yksilöivää tunnusta (3-7),

vastaanotetaan kysytty tunnus (3-8),

tarkistetaan, vastaavatko autentikointitieto ja kysytty tunnus toisiaan (3-9), ja

mikäli vastaavat, läpäistään autentikointi, ja

mikäli eivät vastaa, autentikointia ei läpäistä.

7. Jonkin edellä olevan patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

ladataan palvelulogiikka palvelualustalle, jossa se suoritetaan palvelun aikaansaamiseksi, ja

liitetään autentikointitieto palvelulogiikkaan sen lataamisen yhteydessä.

8. Patenttivaatimuksen 7 mukainen menetelmä, t u n n e t t u siitä, että

tallennetaan palvelulogiikka, siihen liitetty autentikointitieto ja käyttäjän ilmaiseva tieto palvelulogiikan lataamisen yhteydessä palvelualustalle (204),

vastaanotetaan käyttäjältä palvelupyyntö,

tarkistetaan, onko pyydettyyn palveluun liittyvä palvelulogiikka tallennettu palvelualustalle (201), ja

mikäli ei ole, ladataan palvelulogiikka (203),

mikäli on,

- tarkistetaan, onko palvelua pyytävälle käyttäjälle tallennettu autentikointitieto (217), ja

- mikäli on, autentikoidaan käyttäjä,

-mikäli ei ole,

-- pyydetään käyttäjälle autentikointitieto (218),

-- tallennetaan autentikointitieto ja käyttäjän ilmaiseva tieto palvelulogiikan yhteyteen (220), ja

-- autentikoidaan käyttäjä.

9. Tietoliikennejärjestelmä, joka käsittää

ensimmäisen osan (SP) palvelun tuottamiseksi käyttäjälle palvelulogiikan avulla, ja

toisen osan palvelun (SN, MT) välittämiseksi palvelun käyttäjälle,

jossa järjestelmässä ensimmäinen osa (SP) on sovitettu tunnistamaan palvelua pyytävä käyttäjä ja tarkistamaan, onko käyttäjälle tilattu palvelu ja mikäli käyttäjälle on tilattu palvelu, aikaansaamaan palvelu lataamalla palvelulogiikka toiseen osaan (SN, MT), joka on sovitettu välittämään palvelu suorittamalla ladatun palvelulogiikan,

t u n n e t t u siitä, että

ensimmäinen osa (SP) on sovitettu liittämään ladattavaan palvelulogiikkaan autentikointitieto käyttäjän autentikoimiseksi, ja

toinen osa (SN, MT) on sovitettu autentikoimaan käyttäjä ja suorittamaan palvelulogiikka vain vasteena autentikoinnin läpäisemiselle.

10. Patenttivaatimuksen 9 mukainen järjestelmä, t u n n e t t u siitä, että

ensimmäinen osa (SP) on sovitettu allekirjoittamaan palvelulogiikka salaamalla se toisen osan kanssa sovitulla salausavaimella, ja

toinen osa (SN, MT) on sovitettu verifioimaan ensimmäinen osa purkamalla palvelulogiikan salaus mainittua sovittua salausavainta vastaavalla avaimella ja suorittamaan palvelulogiikka, vain mikäli lisäksi verifiointi onnistuu.

11. Patenttivaatimuksen 9 tai 10 mukainen järjestelmä, t u n n e t t u siitä, että

tietoliikennejärjestelmä on matkaviestinjärjestelmä (IMT-2000), joka käsittää ainakin yhden palveluoperaattorin ja palvelevan verkon,

ensimmäinen osa on palveluoperaattori (SP), ja

toinen osa on palveleva verkko (SN), joka käsittää ainakin yhden verkkoelementin (SCN).

12. Patenttivaatimuksen 9 tai 10 mukainen järjestelmä, t u n n e t t u siitä, että

tietoliikennejärjestelmä on matkaviestinjärjestelmä (IMT-2000), joka käsittää ainakin yhden palveluoperaattorin (SP) ja päätelaitteen (MT), joka on palvelevan verkon (SN) välityksellä yhteydessä palveluoperaattoriin, ja joka päätelaite (MT) käsittää varsinaisen päätelaitteen (ME) lisäksi irrotettavasti päätelaitteeseen kytkettävän tilaajan tunnistusyksikön (USIM),

ensimmäinen osa on palveluoperaattori (SP), ja

toinen osa on varsinainen päätelaite (ME).

13. Tietoliikennejärjestelmän palvelua käyttäjälle tuottava verkkoelementti (SP), joka tuottaa palvelun palvelulogiikan avulla ja joka käsittää välineitä palvelua pyytävän käyttäjän tunnistamiseksi ja sen tarkistamiseksi, onko käyttäjälle tilattu palvelu ja palvelun aikaansaamiseksi lataamalla palvelulogiikka tietoliikennejärjestelmään, mikäli käyttäjälle on tilattu palvelu,

t u n n e t t u siitä, että verkkoelementti (SP) käsittää välineitä autentikointitiedon liittämiseksi ladattavaan palvelulogiikkaan siten, että palvelun käyttäjä autentikoidaan ennen palvelulogiikan suorittamista.

14. Patenttivaatimuksen 13 mukainen verkkoelementti (SP), t u n n e t t u siitä, että se käsittää välineitä palvelulogiikan allekirjoittamiseksi ennen sen lataamista verkkoon.

15. Patenttivaatimuksen 13 tai 14 mukainen verkkoelementti (SP), t u n n e t t u siitä, että se käsittää prosessorin, joka on järjestetty suorittamaan ohjelmistorutiineja, ja mainitut välineet on toteutettu ohjelmistorutiineina.

16. Tietoliikennejärjestelmän laitteisto, joka käsittää palvelulogiikan suorittamisvälineitä palvelun välittämiseksi tietoliikennejärjestelmän palveluoperaattorilta palvelun käyttäjälle,

t u n n e t t u siitä, että laitteisto (SCN, ME) käsittää

erotusvälineitä käyttäjän autentikointitiedon erottamiseksi ladatusta palvelulogiikasta,

erotusvälineille vasteellisia autentikoimisvälineitä käyttäjän autentikoimiseksi, ja

palvelulogiikan suorittamisvälineet on sovitettu olemaan vasteellisia autentikoimisvälineille.

17. Patenttivaatimuksen 16 mukainen laitteisto (SCN, ME), t u n n e t t u siitä, että

se käsittää verifiointivälineitä palveluoperaattorin verifioimiseksi ladatun palvelulogiikan sisältämän verifiointitiedon avulla, ja

palvelulogiikan verifiointivälineet on sovitettu olemaan vasteellisia autentikoimisvälineille.

18. Patenttivaatimuksen 16 tai 17 mukainen laitteisto (SCN, ME) t u n n e t t u siitä, että se käsittää prosessorin, joka on järjestetty suorittamaan ohjelmistorutiineja, ja mainitut välineet on toteutettu ohjelmistorutiineina.

19. Patenttivaatimuksen 16, 17 tai 18 mukainen laitteisto, t u n n e t t u siitä, että se on matkaviestinjärjestelmän verkkoelementti (SCN), joka on sovitettu toimimaan palvelualustana.

20. Patenttivaatimuksen 16, 17 tai 18 mukainen laitteisto, t u n n e t t u siitä, että se on matkaviestinjärjestelmän päätelaite (ME).

Patentkrav

1. Förfarande för att förhindra olovlig användning av en tjänst i ett mobilt kommunikationssystem, i vilket förfarande

en tjänstebegäran mottas från en användare av en tjänst, och

tjänsten åstadkoms med hjälp av en tjänstelogik,

k ä n n e t e c k n a t av att i förfarandet

bifogas autenticeringsinformation (3-6) till tjänstelogiken,

användaren som begär tjänsten autenticeras med hjälp av autenticeringsinformationen (3-9), och

tjänstelogiken (3-14) genomförs endast om autenticeringen godkänns.

2. Förfarande enligt patentkrav 1, k ä n n e t e c k n a t av att

till tjänstelogiken bifogas dessutom verifieringsinformation för en tjänsteoperatör,

tjänsteoperatören verifieras i samband med autenticeringen av användaren (3-13), och

tjänstelogiken genomförs endast om också verifieringen lyckas.

3. Förfarande enligt patentkrav 2, k ä n n e t e c k n a t av att

som tjänstelogikens verifieringsinformation används en första blandsumma som beräknats från tjänstelogiken,

tjänstelogiken laddas på ett tjänsteunderlag, där den genomförs för att åstadkomma tjänsten,

tjänsteoperatören verifieras på tjänsteunderlaget genom att en andra blandsumma beräknas från tjänstelogiken, och

om den första och andra blandsumman är lika, lyckas verifieringen,

om den första och andra blandsumman är olika, misslyckas verifieringen.

4. Förfarande enligt patentkrav 2, k ä n n e t e c k n a t av att

som verifieringsinformation används tjänsteoperatörens underskrift,

tjänstelogiken undertecknas genom chiffrering med tjänsteoperatörens hemliga nyckel, och

tjänsteoperatören verifieras genom dechiffrering av tjänstelogikens kryptering med tjänsteoperatörens offentliga nyckel.

5. Förfarande enligt något av de föregående patentkraven, k ä n n e t e c k n a t av att

abonnentens hemliga nyckel lagras i en abonnentidentifierings-

enhet (USIM) som finns hos användaren av tjänsten,

som autenticeringsinformation används abonnentens offentliga nyckel,

en utmaning, som är chiffrerad med abonnentens offentliga nyckel, sänds till abonnentidentifieringsenheten i en terminal hos den användare som bett om tjänsten (207),

utmatningen dechiffreras i identifieringsenheten med abonnentens hemliga nyckel till klartext,

klartexten mottas från identifieringsenheten (208),

kontrolleras om den icke-chiffrerade utmatningen och klartexten motsvarar varandra (209), och

ifall de motsvarar varandra, godkänns autenticeringen, och

ifall de inte motsvarar varandra, godkänns autenticeringen inte.

6. Förfarande enligt patentkrav 1, 2, 3 eller 4, k ä n n e t e c k n a t av att

som autenticeringsinformation används en identifierare som identifierar abonnenten,

en tjänstebegäran mottas från användaren (3-1),

frågas efter den till användaren hörande identifieraren som identifierar abonnenten (3-7),

den efterfrågade identifieraren mottas (3-8),

kontrolleras om autenticeringsinformationen och den efterfrågade identifieraren motsvarar varandra (3-9), och

om så är fallet, godkänns autenticeringen, och

om så inte är fallet, godkänns autenticeringen inte.

7. Förfarande enligt något av de föregående patentkraven, k ä n n e t e c k n a t av att

tjänstelogiken laddas på tjänsteunderlaget, där den genomförs för att åstadkomma tjänsten, och

autenticeringsinformationen bifogas till tjänstelogiken i samband med laddningen av denna.

8. Förfarande enligt patentkrav 7, k ä n n e t e c k n a t av att

tjänstelogiken, autenticeringsinformationen i anslutning därtill och information som anger användaren lagras i samband med laddningen av tjänstelogiken på tjänsteunderlaget (204),

en tjänstebegäran mottas från användaren,

kontrolleras om tjänstelogiken i anslutning till den begärda tjänsten är lagrad på tjänsteunderlaget (201), och

om så inte är fallet, laddas tjänstelogiken (203),

om så är fallet,

- kontrolleras om autenticeringsinformation lagrats för användaren som begär tjänsten (217), och

- om så är fallet, autenticeras användaren,

- om så inte är fallet,

-- begärs autenticeringsinformation för användaren (218),

-- lagras autenticeringsinformationen och information som anger användaren i anslutning till tjänstelogiken (220), och

-- autenticeras användaren.

9. Telekommunikationssystem, vilket omfattar

en första del (SP) för att producera en tjänst för en användare med hjälp av en tjänstelogik, och

en andra del för att förmedla tjänsten (SN, MT) till användaren av tjänsten,

i vilket system den första delen (SP) är anordnad att identifiera användaren som begär tjänsten och att kontrollera om tjänsten beställts åt användaren och, ifall tjänsten beställts åt användaren, att åstadkomma tjänsten genom att ladda tjänstelogiken i den andra delen (SN, MT), vilken är anordnad att förmedla tjänsten genom att genomföra den laddade tjänstelogiken,

k ä n n e t e c k n a t av att

den första delen (SP) är anordnad att till tjänstelogiken som skall laddas bifoga autenticeringsinformation för autenticering av användaren, och

den andra delen (SN, MT) är anordnad att autenticera användaren och att genomföra tjänstelogiken endast som svar på att autenticeringen godkänts.

10. System enligt patentkrav 9, k ä n n e t e c k n a t av att

den första delen (SP) är anordnad att underteckna tjänstelogiken genom att chiffrera den med en hemlig nyckel, som man kommit överens om med den andra delen, och

den andra delen (SN, MT) är anordnad att verifiera den första delen genom att dechiffrera tjänstelogikens kryptering med en nyckel, som motsvarar nämnda överenskomna hemliga nyckel, och att genomföra tjänstelogiken, endast om också verifieringen lyckas.

11. System enligt patentkrav 9 eller 10, k ä n n e t e c k n a t av att telekommunikationssystemet är ett mobilt kommunikationssystem (IMT-2000), vilket omfattar åtminstone en tjänsteoperatör och ett betjänande nät,

den första delen är en tjänsteoperatör (SP), och

den andra delen är ett betjänande nät (SN), som omfattar åtminstone ett nätelement (SCN).

12. System enligt patentkrav 9 eller 10, k ä n n e t e c k n a t av att telekommunikationssystemet är ett mobilt kommunikationssystem (IMT-2000), vilket omfattar åtminstone en tjänsteoperatör (SP) och en terminal (MT), som via det betjänande nätet (SN) står i förbindelse med tjänsteoperatören, och vilken terminal (MT) förutom den egentliga terminalen (ME) dessutom omfattar en abonnentidentifieringsenhet (USIM) som kan kopplas löstagbart till terminalen,

den första delen är en tjänsteoperatör (SP), och

den andra delen är den egentliga terminalen (ME).

13. Nätelement (SP) som producerar en tjänst för en användare i ett telekommunikationssystem, vilket nätelement producerar tjänsten med hjälp av en tjänstelogik och omfattar medel för att identifiera användaren som begär tjänsten och för att kontrollera, om tjänsten beställts åt användaren och för att åstadkomma tjänsten genom att ladda tjänstelogiken i telekommunikationssystemet, om tjänsten beställts åt användaren,

k ä n n e t e c k n a t av att nätelementet (SP) omfattar medel för att bifoga autenticeringsinformation till tjänstelogiken som skall laddas, så att användaren av tjänsten autenticeras innan tjänstelogiken genomförs.

14. Nätelement (SP) enligt patentkrav 13, k ä n n e t e c k n a t av att det omfattar medel för att underteckna tjänstelogiken innan den laddas i nätet.

15. Nätelement (SP) enligt patentkrav 13 eller 14, k ä n n e t e c k n a t av att det omfattar en processor, som är anordnad att utföra programrutiner, och nämnda medel har förverkligats som programrutiner.

16. Apparatur i ett telekommunikationssystem, vilken apparatur omfattar medel för att genomföra en tjänstelogik för förmedling av en tjänst från en tjänsteoperatör i telekommunikationssystemet till en användare av tjänsten,

k ä n n e t e c k n a d av att apparaturen (SCN, ME) omfattar

skiljemedel för att skilja användarens autenticeringsinformation från den laddade tjänstelogiken,

autenticeringsmedel som svarar på skiljemedlen för autenticering av användaren, och

medlen för att genomföra tjänstelogiken är anordnade att svara på autenticeringsmedlen.

17. Apparatur (SCN, ME) enligt patentkrav 16, k ä n n e t e c k n a d av att

den omfattar verifieringsmedel för verifiering av en tjänsteoperatör med hjälp av verifieringsinformation som ingår i den laddade tjänstelogiken, och

tjänstelogikens verifieringsmedel är anordnade att svara på autenticeringsmedlen.

18. Apparatur (SCN, ME) enligt patentkrav 16 eller 17, k ä n n e t e c k n a d av att den omfattar en processor, som är anordnad att utföra programrutiner, och nämnda medel har förverkligats som programrutiner.

19. Apparatur enligt patentkrav 16, 17 eller 18, k ä n n e t e c k n a d av att den är ett nätelement (SCN) i ett mobilt kommunikationssystem, vilket nätelement är anordnat att fungera som ett tjänsteunderlag.

20. Apparatur enligt patentkrav 16, 17 eller 18, k ä n n e t e c k n a d av att den är en terminal (ME) i ett mobilt kommunikationssystem.

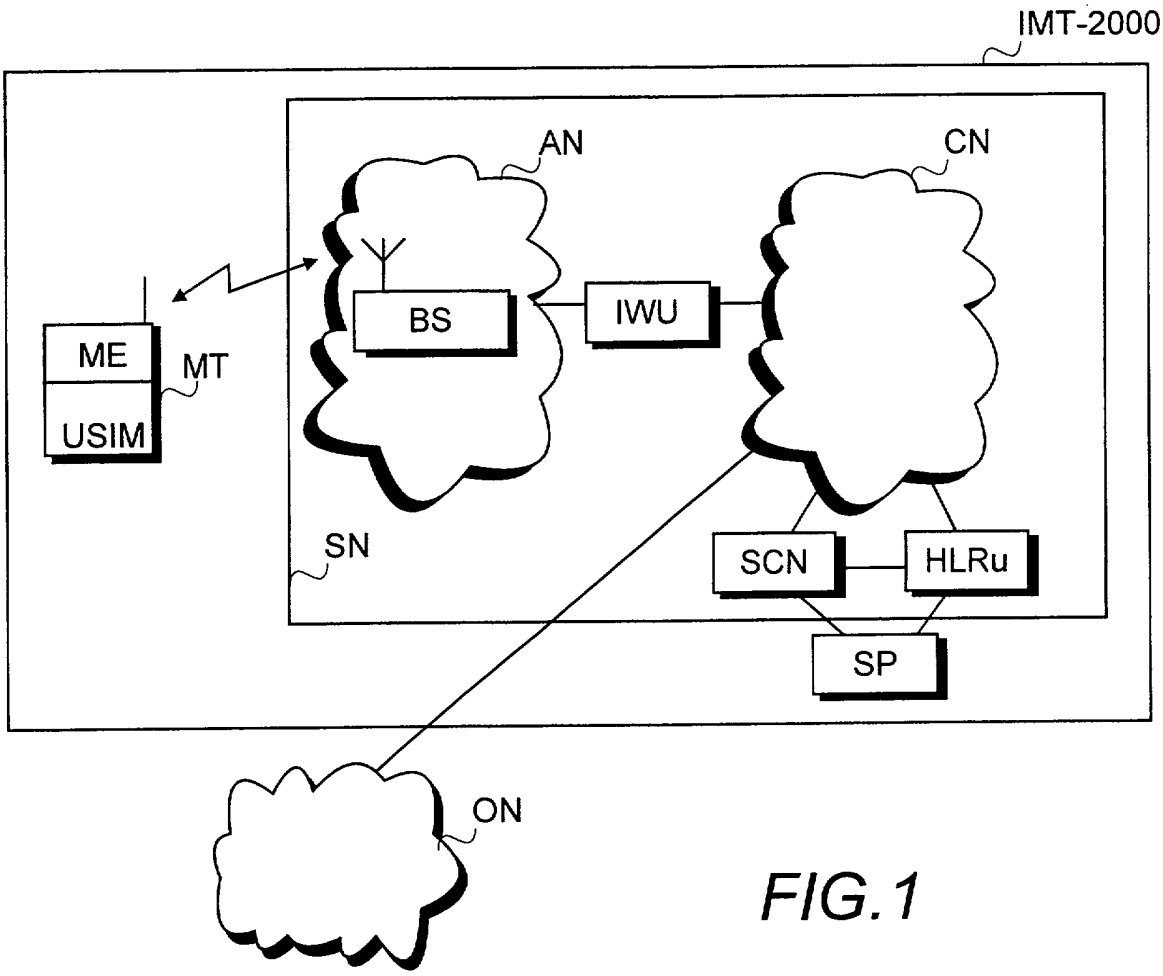


FIG.1

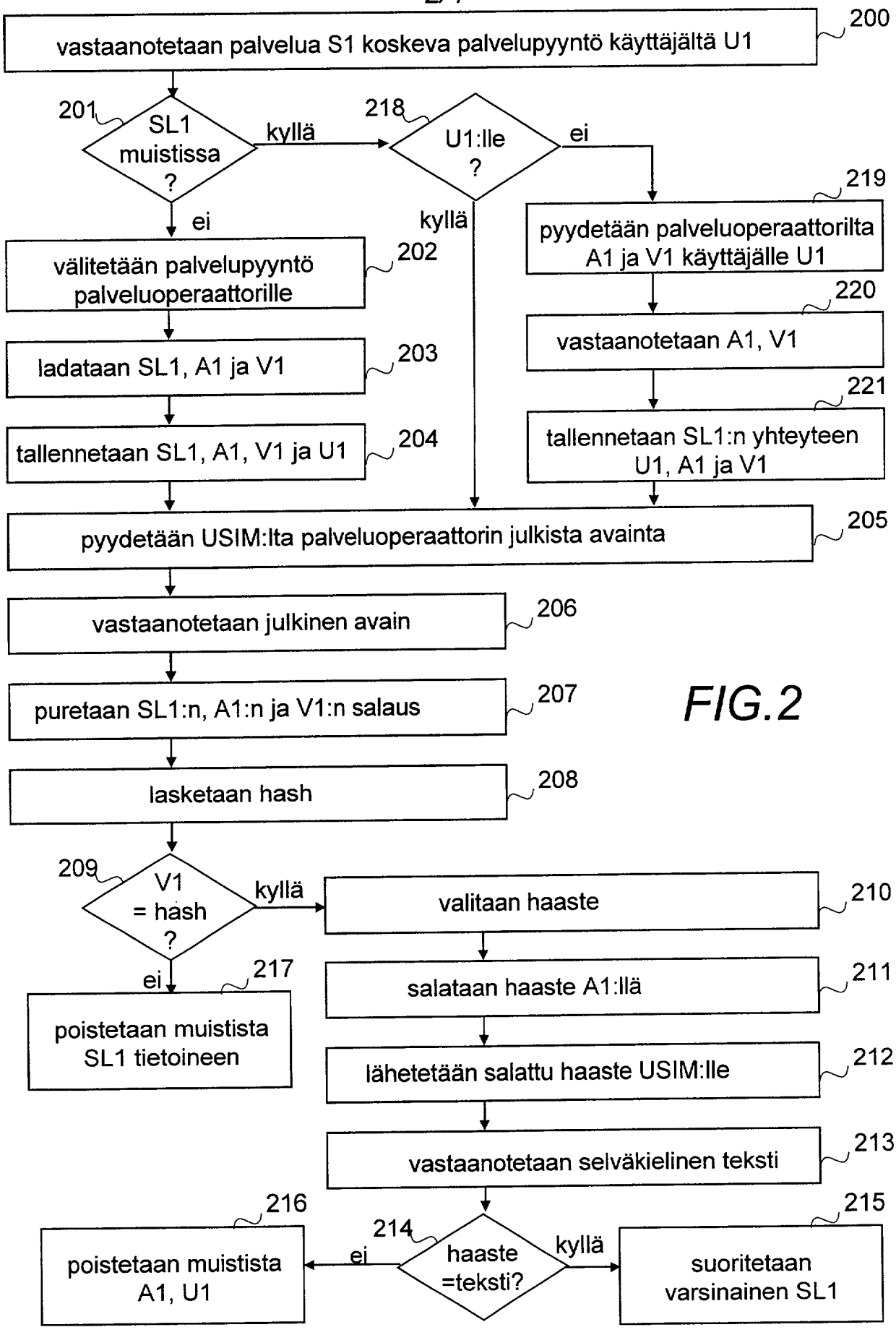
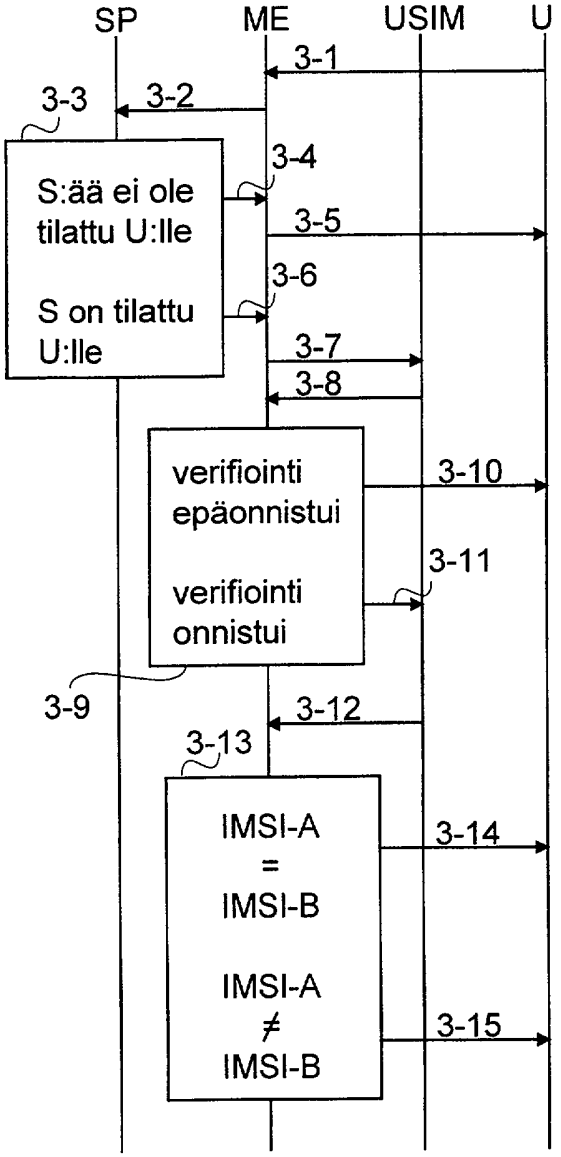

vastaanotetaan palvelua S1 koskeva palvelupyyntö käyttäjältä U1
200
201
SL1 muistissa ?
kyllä
218
U1:lle ?
ei
219
pyydetään palveluoperaattorilta A1 ja V1 käyttäjälle U1
ei
kyllä
välitetään palvelupyyntö palveluoperaattorille
202
220
vastaanotetaan A1, V1
ladataan SL1, A1 ja V1
203
221
tallennetaan SL1:n yhteyteen U1, A1 ja V1
tallennetaan SL1, A1, V1 ja U1
204
pyydetään USIM:lta palveluoperaattorin julkista avainta
205
vastaanotetaan julkinen avain
206
puretaan SL1:n, A1:n ja V1:n salaus
207
lasketaan hash
208
209
V1 = hash ?
kyllä
valitaan haaste
210
ei
217
salataan haaste A1:llä
211
poistetaan muistista SL1 tietoineen
lähetetään salattu haaste USIM:lle
212
vastaanotetaan selväkielinen teksti
213
216
214
haaste =teksti?
kyllä
215
ei
poistetaan muistista A1, U1
suoritetaan varsinainen SL1

FIG.2



3-1. Palvelua S
3-2. Palvelua S U:lle

3-4. Negat.kuittaus
3-5. Ei palvelua

3-6. SL, IMSI-A ja hash
3-7. Anna SP:n julkinen avain
3-8. SP:n julkinen avain

3-10. Ei palvelua

3-11. Anna IMSI

3-12. IMSI-B

3-14. Palvelu

3-15. Ei palvelua

FIG.3

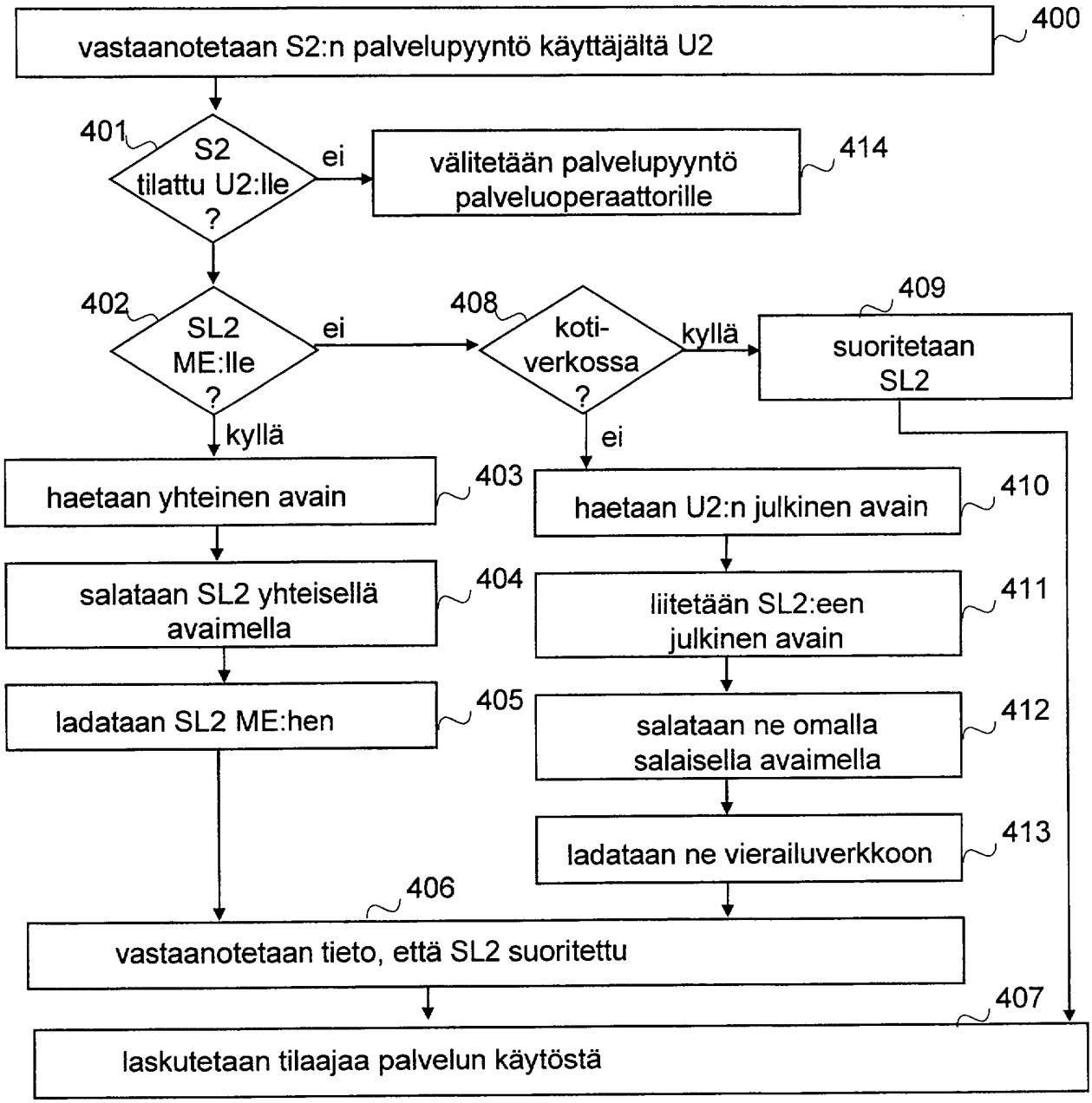

vastaanotetaan S2:n palvelupyyntö käyttäjältä U2
400
401
S2 tilattu U2:lle ?
ei
välitetään palvelupyyntö palveluoperaattorille
414
402
SL2 ME:lle ?
ei
408
koti-verkossa ?
kyllä
409
suoritetaan SL2
kyllä
ei
haetaan yhteinen avain
403
haetaan U2:n julkinen avain
410
salataan SL2 yhteisellä avaimella
404
liitetään SL2:een julkinen avain
411
ladataan SL2 ME:hen
405
salataan ne omalla salaisella avaimella
412
ladataan ne vierailuverkkoon
413
406
vastaanotetaan tieto, että SL2 suoritettu
407
laskutetaan tilaajaa palvelun käytöstä

FIG.4