(12) **PATENTTIJULKAISU**
PATENTSKRIFT

FI000116182B

(10) **FI 116182 B**

(45) Patentti myönnetty - Patent beviljats **30.09.2005**

(51) Kv.lk.7 - Int.kl.7

H04L 9/32

(21) Patenttihakemus - Patentansökning **20045094**

(22) Hakemispäivä - Ansökningsdag **23.03.2004**

(24) Alkupäivä - Löpdag **23.03.2004**

(41) Tullut julkiseksi - Blivit offentlig **24.09.2005**

SUOMI – FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN

(73) Haltija - Innehavare

1 •TeliaSonera Finland Oyj, Teollisuuskatu 15, 00510 Helsinki, SUOMI - FINLAND, (FI)

(72) Keksijä - Uppfinnare

1 •Keisala,Ilkka, Kavallinkuja 6a, 02710 Espoo, SUOMI - FINLAND, (FI)
2 •Vitikka,Ilpo, Dagmarinkatu 13 b 5, 00100 Helsinki, SUOMI - FINLAND, (FI)

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

(54) Keksinnön nimitys - Uppfinningens benämning

Tilaajan autentikointi
Autenticering av en abonnent

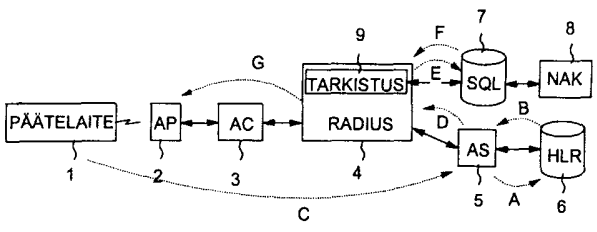
(56) Viitejulkaisut - Anförda publikationer

US 20030051041 A1, US 20030233580 A1,US 20020161927 A1, WO 03030445 A1, WO 2004036823 A1

(57) Tiivistelmä - Sammandrag

Tämän keksinnön kohteena on menetelmä tilaajan autentikoimiseksi, joka menetelmä käsittää: autentikointiviestin vastaanottamisen (C) tilaajalta, ja mainitun tilaajan autenttisuuden tarkistamisen. Jotta varmistettaisiin, että tilaaja, joka operaattorin mielestä on vailla oikeutta, ei pääse järjestelmään, käsittää menetelmä: mainittua tilaajaa koskevan statustietojen hakemisen (E, F) tilaajatietokannasta, viestin lähettämisen (G), joka osoittaa autentikoinnin epäonnistuneen, mikäli yksi tai useampi seuraavista ehdoista täyttyy: mainitun tilaajan autentikointi autentikointiviestin perusteella on epäonnistunut, statustiedot osoittavat, että tilaajalla on pääsy järjestelmään toisen autentikointimekanismin välityksellä, tai tilaajan tili on peruutettu.

Föreliggande uppfinning avser ett förvarande för att autentikera en abonnent, vilket förfarande omfattar: mottagande (C) av ett autentikeringsmeddelande från en abonnent, och kontroll av nämnda abonnents autenticitet. För att säkra att en abonnent som enligt en operatör anses vara oberättigad inte får access till systemet omfattar förfarandet: sökning (E, F) av statusinformation gällande nämnda abonnent från en abonnentdatabas, sändande (G) av ett meddelande som indikerar att autentikeringen har misslyckats, ifall ett eller flera av följande villkor uppfylls: nämnda abonnents autentikering på basen av autentikeringsmeddelandets innehåll har misslyckats, statusinformationen indikerar att abonnenten har access till systemet via en annan autentikeringsmekanism, eller abonnentens konto har annullerats.



Tilaajan autentikointi

KEKSINNÖN TAUSTA

1. Keksinnön ala

Tämä keksintö liittyy tilaajan autentikointiin. Keksintöä voidaan edullisesti hyödyntää WLAN (Wireless Local Area Network) järjestelmässä tilaajan autentikoimiseksi. Kuitenkin, on tärkeä havaita, että esillä olevaa keksintöä voidaan hyödyntää myös muun tyyppisissä järjestelmissä.

2. Tekniikan tason kuvaus

Ennestään tunnetaan ratkaisuja, joissa tilaaja autentikoidaan tai vastaavasti uudelleenautentikoidaan siten, että autentikointipalvelimelle annetaan tarvittavat autentikointitiedot tilaajan autentikoimiseksi. Täten autentikointipalvelin voi, käyttämällä autentikointitietoja ja tilaajalta vastaanotettua autentikointiviestiä, varmistaa onko autentikointiviesti lähetetty autenttiselta tilaajalta. Jos näin, on autentikointi onnistunut, muussa tapauksessa autentikointi on epäonnistunut. Mikäli autentikointi on onnistunut, tilaajalle tarjotaan pääsy viestintäjärjestelmän tarjoamiin palveluihin.

Yllä kuvatun tyyppisiin tunnettuihin autentikointimenetelmiin liittyy sellainen ongelma, että tunnetut autentikointimenetelmät saattavat tietyissä tilanteissa tarjota tilaajalle pääsyn viestintäjärjestelmään, vaikka operaattori kyseisellä hetkellä katsoo, että tämä tilaaja ei ole oikeutettu käyttämään viestintäjärjestelmää. Tämän tyyppinen tilanne saattaa ilmetä esimerkiksi kun operaattori on äskettäin peruuttanut tilaajan tilin, ja tilaaja vierailee toisessa verkossa. Tällaisessa tilanteessa tilaajan uudelleenautentikointi saattaa onnistua ja tilaajalle annetaan pääsy vierailtavaan verkkoon. Tämän tyyppinen tilanne saattaa myös ilmetä kun autentikointi perustuu tilaajatunnukseen ja salasanaan, jonka tilaaja syöttää tilaajalaitteen käyttöliittymän kautta. Tässä tapauksessa saattaa ilmetä tilanne, jossa kahta eri tilaajalaitetta käytetään viestintäjärjestelmään pääsemiseksi samanaikaisesti käyttäen samaa tilaajatunnusta ja salasanaa.

Keksinnön yhteenveto

Tämän keksinnön eräs tarkoitus on ratkaista edellä selostettu ongelma ja tarjota käyttöön ratkaisu, joka mahdollistaa sen estämisen, että tilaajat, jotka operaattorin mielestä eivät ole oikeutettuja käyttämään järjestelmää, eivät pääse käyttämään viestintäjärjestelmää. Nämä ja muut keksinnön päämäärät saavutetaan itsenäisen vaatimuksen 1 mukaisella menetelmällä, itsenäisen

vaatimuksen 5 mukaisella viestintäjärjestelmällä, ja itsenäisen vaatimuksen 9 mukaisella palvelimella.

Esillä oleva keksintö parantaa tekniikan tason mukaisia autentikointiratkaisuja tuomalla lisätarkistuksen tilaajan autentikointiin. Tämä lisätarkistus suoritetaan hakemalla tilaajaa koskevaa statustietoa tilaajatietokannasta autentikoinnin yhteydessä. Täten ei ole enää riittävää, että tilaaja kykenee tuottamaan oikean autentikointiviestin järjestelmälle pääsyn saamiseksi järjestelmään. Sitävastoin suoritetaan myös statustarkistus kyseessä olevalle tilaajalle. Tämä statustarkistus tuo lisäinformaatiota tilaajasta siten, että voidaan välttää tilanne, jossa tilaajalle tarjotaan pääsy, vaikka operaattori kyseisellä hetkellä katsoo, että tilaaja ei ole oikeutettu tilaaja.

Merkittävin etu joka saavutetaan keksinnöllä on se, että se parantaa operaattorin mahdollisuutta rajata ei-oikeutettujen tilaajien pääsyä verkkoon, koska operaattori voi muuttaa näiden tilaajien statustietoja tilaajatietokannassa sellaisella tavalla, että pääsy kielletään autentikoinnin yhteydessä. Eräs esillä olevan keksinnön toinen merkittävä etu on se, että tilanteet, joissa kaksi tilaajalaitetta samanaikaisesti käyttää järjestelmää hyödyntämällä samaa käyttäjätunnusta ja salasanaa autentikoinnissa, voidaan välttää.

Keksinnön mukaisen menetelmän, viestintäjärjestelmän ja palvelimen edulliset suoritusmuodot ilmenevät epäitsenäisistä vaatimuksista 2 - 4, 6 - 8 ja 10.

Kuvioiden lyhyt kuvaus

Keksintöä selostetaan seuraavassa esimerkinomaisesti lähemmin viittaamalla oheisiin kuvioihin, joista:

kuvio 1 esittää lohkokaaviota esillä olevan keksinnön ensimmäisestä edullisesta suoritusmuodosta, ja

kuvio 2 esittää lohkokaaviota esillä olevan keksinnön toisesta edullisesta suoritusmuodosta.

Joidenkin suoritusmuotojen kuvaus

Kuvio 1 esittää lohkokaaviota keksinnön ensimmäisestä edullisesta suoritusmuodosta. Kuviossa 1 oletetaan esimerkinomaisesti, että tilaaja 1 on WLAN-tilaaja, joka käyttää viestintäjärjestelmää liityntäpisteen 2 (tässä esimerkissä tukiasema) tarjoaman radiotien ja liityntäpalvelimen 3 välityksellä.

Tilaajan 1 käyttämän päätelaitteen oletetaan olevan päätelaite, jossa on EAP SIM (Extensible Authentication Protocol IEEE 802.1x, Subscriber Identity Module) sovellus (client). Päätelaitteeseen kuuluu täten SIM, joka mahdollistaa sen käyttäjälle WLAN-palveluiden käytön ja käytetyistä palveluista aiheutuvien kulujen lisäämisen tilaajan matkapuhelimen laskuun.

Kuvion 1 järjestelmään kuuluu lisäksi palvelin 4, jonka oletetaan olevan RADIUS-palvelin (Remote Authentication Dial In User Service). RADIUS-palvelimia käytetään usein eri operaattoreiden WLAN-verkkojen yhdistämiseen toisiinsa. Tämä yhdistäminen mahdollistaa esimerkiksi verkkovierailupalveluiden (roaming) tarjoamisen tilaajille. Kuvion 1 järjestelmä sisältää lisäksi autentikointivälineet 5, jotka on järjestetty autentikointipalvelimeen. Tämä palvelin toimii EAP SIM-palvelimena, joka mahdollistaa niiden tilaajien autentikoinnin, joilla on EAP SIM-sovelluksia. Tällaisen autentikoinnin toteuttamiseksi autentikointivälineet kommunikoivat matkaviestinjärjestelmän kanssa, kuten GSM-järjestelmän (Global System for Mobile communications) kotirekisterin 6 kanssa.

Tilaajatietokantaan 7 sisältyy tietoja WLAN-tilaajista. Kuvion 1 esimerkissä tilaajatietokanta 7 on yhdistetty operaattorin asiakashallinta- ja laskutusjärjestelmään 8, jota operaattori käyttää esimerkiksi tilaajarekisterin 7 ja kotirekisterin 6 tilaajatietojen päivittämiseen. Kun WLAN-järjestelmään lisätään uusi tilaaja, jolla on EAP SIM-sovellus operaattori lisää tätä uutta tilaajaa koskevat tilaajatiedot tilaajatietokantaan 7 ja kotirekisteriin 6. Jos, toisaalta, WLAN-tilaajan olemassa oleva tili peruutetaan, operaattori käyttää asiakashallinta- ja laskutusjärjestelmää 8 tämän tiedon syöttämiseen tilaajatietokantaan 7.

EAP SIM-sovelluksen tilaaja-autentikointi perustuu matkaviestinjärjestelmästä saataviin autentikointitietoihin. EAP SIM-autentikointi on ennestään tunnettua eikä sitä siksi selosteta yksityiskohtaisesti. Lyhyesti, kun tilaaja 1 on tunnistettu autentikointivälineet 5 vastaanottavat autentikointitietoja matkaviestinjärjestelmältä, joka tässä tapauksessa on GSM-järjestelmä. Autentikointi perustuu haaste-vaste mekanismiin. EAP SIM-sovellus vastaanottaa haasteen RAND ja käyttää ennalta määrättyä algoritmia vasteen SRES laskemiseen hyödyntämällä salaista avainta, joka on uniikki kyseessä olevalle SIM-kortille. Autentikointivälineet 5 vastaanottavat GSM-triplettejä sisältävät autentikointitiedot matkaviestinjärjestelmältä. Nämä autentikointitiedot sisältävät RAND ja SRES pareja. RAND lähetetään tilaajalle 1, joka käyttää SIM-kortin salaista

avainta vasteen laskemiseksi käyttämällä autentikointialgoritmia. Tämä vaste palautetaan autentikointiviestissä autentikointivälineille, jotka vertaavat vastetta SRES:ään. Mikäli vaste vastaa SRES:ää, on autentikointi onnistunut. EAP SIM-autentikoinnissa, kuitenkin, useita GSM-triplettejä yhdistetään yhden autentikoinnin suorittamiseksi. EAP SIM-autentikointi myös parantaa perus GSM-autentikointia toimittamalla RAND haasteiden ja muiden viestien mukana Message Authentication Cod:in molemminpuolisen autentikoinnin aikaansaamiseksi.

Seuraavassa selostetaan esillä olevan keksinnön mukaista autentikointia. Kuviot eivät esitä kaikkia viestejä, jotka liittyvät autentikointiin, vaan ainoastaan ne viestit, jotka ovat tärkeitä esillä olevan keksinnön ymmärtämiseksi. Jotta tilaajan 1 autentikointi olisi mahdollista, lähettävät autentikointivälineet pyynnön A autentikointitriplettien saamiseksi GSM-järjestelmän kotirekisterille 6. Kotirekisteri vastaa tähän pyyntöön lähettämällä B autentikointitietoja autentikointivälineille 5. Autentikointitiedot sisältävät useita triplettejä tilaajalle 1, mikä merkitsee, että autentikointivälineet voivat autentikoida tilaajan 1 useita kertoja, ennen kuin niiden tarvitsee pyytää lisää triplettejä kotirekisteriltä.

Kun tilaaja 1 autentikoinnin yhteydessä lähettää autentikointiviestin C radioteitse, vastaanottaa ja välittää liityntäpiste 2 tämän viestin verkon kautta autentikointivälineille 5. Käsite autentikointiviesti viittaa tässä viestiin, joka sisältää tarvittavat tiedot, jotka mahdollistavat tilaajan autentikoinnin. Mikäli tilaaja on jo aikaisemmin autentikoitu ja autentikointiviesti liittyy uudelleenautentikointiin, niin autentikointivälineille saattaa jo ennestään olla tarvittavat autentikointitiedot kyseessä olevalle tilaajalle, eikä viestejä jotka on merkitty A ja B lähetetä ennen autentikointiviestin vastaanottoa. Kun autentikointiviesti on vastaanotettu, autentikointivälineet vertaavat autentikointiviestin C sisältöä tilaajan 1 osalta aikaisemmin saatuihin autentikointitietoihin. Tästä vertailusta riippuen autentikointivälineet 5 ilmoittavat D palvelimelle 4, että autentikointi on onnistunut tai että se on epäonnistunut.

Mikäli palvelin vastaanottaa tietoja, jotka osoittavat autentikoinnin onnistuneen, niin palvelimen tarkistusvälineet 9 lähettävät viestin E tilaajatietokannalle 7 statustietojen saamiseksi koskien kyseessä olevaa tilaajaa. Tarkistusvälineet voidaan toteuttaa piirinä, tietokoneohjelmana tai näiden yhdistelmänä. Nämä statustiedot palvelin vastaanottaa viestissä F. Vastaanotettuja statustietoja palvelin 4 käyttää suorittamaan tarkastuksen, jossa selvitetään onko käyttäjätili peruutettu.

Mikäli tarkistusvälineet 9 detektoivat, että käyttäjätili on peruutettu, niin palvelin 4 lähettää verkon kautta liityntäpisteelle 2 viestin G, joka osoittaa, että autentikointi on epäonnistunut. Muussa tapauksessa tämä viesti G osoittaa, että autentikointi on onnistunut. Mikäli liityntäpiste vastaanottaa viestin G, joka osoittaa, että autentikointi on epäonnistunut, niin tilaajalle 1 ei enää tarjota pääsyä verkkoon.

Esillä olevaa keksintöä on yllä kuvattu "täyden autentikoinnin" yhteydessä, toisin sanoen kun autentikointitiedot on haettu matkaviestinjärjestelmästä. Kuitenkin esillä olevaa keksintöä voidaan edullisesti käyttää myös uudelleenautentikointiin, jossa aikaisemmin autentikoitu tilaaja autentikoidaan uudelleen. Tässä tapauksessa autentikointivälineet 5 eivät pyydä tai vastaanota mitään uusia "ajan tasalla" olevia autentikointitietoja matkaviestinjärjestelmältä. Sitävastoin aikaisemmin saatuja triplettejä, jotka on tallennettu autentikointivälineiden 5 muistiin, käytetään uudelleenautentikointiin. Muilta osin uudelleenautentikointi suoritetaan yllä selostetusti. Tässä yhteydessä ylimääräinen statustarkistus varmistaa, että "vanhoja" autentikointitietoja voidaan käyttää ilman riskiä, koska mikäli muutoksia on äskettäin ilmaantunut tilaajan osalta (kuten tilin peruuttaminen), niin tällöin nämä muutokset voidaan detektoida statustarkistuksessa, joka perustuu ajan tasalla oleviin statustietoihin.

Kuvio 2 on lohkokaavio joka havainnollistaa erästä toista esillä olevan keksinnön edullista suoritusmuotoa. Kuvion 2 suoritusmuoto on hyvin samantapainen kuin kuvion 1 yhteydessä selostettu. Siksi kuvion 2 suoritusmuotoa selostetaan seuraavassa pääasiassa selittämällä eroja verrattuna kuvion 1 suoritusmuotoon.

Kuviossa 2 tilaaja 1' ei ole tilaaja, jolla on EAP SIM-sovellus, vaan sen sijan tilaajan 1' autentikointi suoritetaan käyttäjätunnuksen ja salasanan perusteella, jotka WLAN-päätteen käyttäjä tuntee. Järjestelmän verkko-osa on lähes identtinen kuin se, jota on selostettu kuvion 1 yhteydessä, koska samat verkkoelementit voivat käsitellä sekä tilaajia, joilla on EAP SIM-sovelluksia, ja tilaajia, jotka autentikoidaan käyttäjätunnuksella ja salasanalla. Kuitenkin tässä tapauksessa autentikointivälineet 5' on järjestetty palvelimeen 4', joka siten kykenee autentikoimaan tilaajan 1'. Autentikointivälineet 5' voidaan toteuttaa piirinä, tietokoneohjelmana tai näiden yhdistelmänä. Kotirekisteriä ja kuvion 1 autentikointipalvelinta ei ole esitetty kuviossa 2, koska niitä ei tarvita sellaisen tilaajan autentikointiin, jonka autentikointi perustuu käyttäjätunnukseen ja salasanaan. Kuvion 2 järjestelmä voi kuitenkin edullisesti sisältää myös kuvion 1

kotirekisterin 6 ja autentikointipalvelimen 5, jotta se voisi autentikoida sekä EAP SIM-sovelluksia omaavia tilaajia että tilaajia, joiden autentikointi perustuu käyttäjätunnukseen ja salsanaan.

Kuvion 2 suoritusmuodossa ei ole tarpeen saada mitään autentikointitietoja matkaviestinjärjestelmältä. Sitävastoin tilaajien käyttäjätunnuksista ja salasanoista muodostuvat autentikointitiedot voidaan tallentaa etukäteen autentikointivälineisiin 5', kun tilaajien tilejä avataan järjestelmässä.

Autentikointiviesti C', jonka tilaaja lähettää kuviossa 2 sisältää siten salasanan tai käyttäjätunnuksen ja salasanan. Palvelimessa 4' olevat autentikointivälineet 5' vastaanottavat tämän viestin ja tarkistavat onko tilaajan salsana oikein. Jos näin, niin autentikointivälineet 5' osoittavat autentikoinnin onnistuneen. Palvelimen 4' tarkistusvälineet 9' on järjestetty pyytämään E statustietoja kyseessä olevalle tilaajalle tilaajatietokannasta 7. Vastaanotettuja F statustietoja käytetään tarkistamaan onko autentikoidulla tilaajalla 1 pääsy järjestelmään jonkin toisen autentikointimekanismin välityksellä. Jos näin, tällöin tilanne olisi sellainen, jossa samalla tilaajalla, jota ollaan autentikoimassa, jo olisi pääsy järjestelmään toisella päätelaitteella. Mikäli tällainen tilanne detektoidaan, niin lähetään viesti G liityntäpisteelle sen osoittamiseksi että autentikointi on epäonnistunut. Muussa tapauksessa tätä viestiä G käytetään osoittamaan liityntäpisteelle, että autentikointi on onnistunut. Mikäli autentikointi on onnistunut, niin palvelin 4' lähettää viestin H tilaajatietokannalle 7, jotta tilaajatietokantaan tallentuisi tietoja, jotka osoittavat, että tilaaja on onnistuneesti autentikoitu ja tilaajalle on tarjottu pääsy järjestelmään. Tämä tallennettu informaatio haetaan mahdollisessa myöhäisemmässä statustarkistuksessa sen osoittamiseksi, että tilaajalla on pääsy järjestelmään toisen autentikointimekanismin välityksellä. Täten voidaan välttää, että sama tilaaja saisi pääsyn järjestelmään toisella päätelaitteella.

Kun autentikoitu tilaaja jostain syystä katkaisee yhteyden verkossa tarjolla olevien palveluiden käytön lopettamiseksi, tällöin liityntäpiste ja/tai liityntäpalvelin 3 havaitsee tämän ja lähettää esimerkiksi "laskutus lopetus" viestin palvelimelle 4' sen osoittamiseksi, että tilaajalla ei enää ole pääsyä verkkoon. Palvelin 4' välittää tämän tiedon edelleen laskutuksen lopettamiseksi, ja lisäksi se lähettää tilaajatietokannalle 7 viestin sen osoittamiseksi, että tilaajalla ei enää ole pääsyä järjestelmään. Tämä tieto tallennetaan tilaajatietokantaan haettavaksi sen osoituksena, että tilaajalla ei ole pääsyä järjestelmään toisen au-

tentikointimekanismin välityksellä kun tilaajaa autentikoidaan seuraavan kerran.

On selostettu edellä olevassa suoritusmuotojen selityksessä, että kuvion 1 suoritusmuodossa statustarkistusta käytetään varmistamaan, että tilaajan tiliä ei ole peruutettu, ja kuvion 2 suoritusmuodossa sen tarkistamiseen, että tilaajalla ei ole pääsyä järjestelmään toisella autentikointimekanismilla. Kuitenkin on edullista, että samassa autentikointimenettelyssä käytetään molempia tarkistuksia. Täten statustarkistus tehdään sen varmistamiseksi, että tilaajan tiliä ei ole peruutettu, ja että tilaajalla ei ole pääsyä järjestelmään toisen autentikointimekanismin välityksellä. Tässä tapauksessa lähetetään viesti, joka osoittaa, että autentikointi on epäonnistunut, mikäli jommalla kummalla tai molemmilla tarkistuksilla on positiivinen lopputulos, toisin sanoen tili on peruutettu tai tilaajalla on pääsy toisen autentikointimekanismin välityksellä.

On ymmärrettävä, että edellä oleva selitys ja siihen liittyvät kuviot on ainoastaan tarkoitettu havainnollistamaan esillä olevaa keksintöä. Alan ammattimiehelle on ilmeistä, että keksintöä voidaan muunnella ja modifioida myös muilla tavoin ilman että poiketaan keksinnön suojapiiristä.

Patenttivaatimukset:

1. Menetelmä viestintäjärjestelmän tilaajan autentikoimiseksi, joka menetelmä käsittää:

autentikointiviestin vastaanottamisen (C, C') tilaajalta, ja

mainitun tilaajan autenttisuuden tarkistamisen hyödyntämällä mainitun autentikointiviestin sisältöä, t u n n e t t u siitä, että

haetaan (E, F) mainittua tilaajaa koskevaa statustietoa tilaajatietokannasta,

lähetetään (G) viesti, joka osoittaa mainitun tilaajan autentikoinnin epäonnistuneen, mikäli yksi tai useampi seuraavista ehdoista täyttyy:

- mainitun tilaajan autentikointi mainitun autentikointiviestin sisällön perusteella on epäonnistunut,
- statustiedot osoittavat, että tilaajalla on pääsy järjestelmään toisen autentikointimekanismin välityksellä, tai
- statustiedot osoittavat, että tilaajan tili on peruutettu.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että mainittu autentikointiviesti on uudelleenautentikointiviesti.

3. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että mainittu viestintäjärjestelmä on WLAN-järjestelmä ja mainittu menetelmä edelleen käsittää:

pyynnön lähettämisen (A) mainitusta WLAN-järjestelmästä matkaviestinjärjestelmälle autentikointitietojen saamiseksi,

autentikointitietojen vastaanottamisen (B) matkaviestinjärjestelmästä, ja

tilaajan autenttisuuden tarkistamisen hyödyntämällä mainitun autentikointiviestin sisältöä sekä matkaviestinjärjestelmästä saatuja autentikointitietoja.

4. Jonkin patenttivaatimuksen 1 - 3 mukainen menetelmä, t u n n e t t u siitä, että mainittu tilaaja on EAP SIM sovellus.

5. Viestintäjärjestelmä, joka käsittää:

liityntäpisteen (2), joka tarjoaa autentikoiduille tilaajille pääsyn järjestelmään,

tilaajatietokannan (7), joka sisältää tietoja koskien järjestelmän tilaajia, ja

autentikointivälineitä (5, 5') tilaajan (1, 1') autentikoimiseksi hyödyntämällä mainitulta tilaajalta (1, 1') vastaanotetun autentikointiviestin sisältöä, tunnettu siitä, että mainittu viestintäjärjestelmä lisäksi käsittää:

tarkistusvälineet (9, 9') mainittua tilaajaa (1, 1') koskevien statustietojen hakemiseksi tilaajatietokannasta (7) kun autentikointivälineet osoittavat, että mainittu tilaaja (1, 1') on onnistuneesti autentikoitu, tarkistuksen suorittamiseksi mainittujen haettujen statustietojen perusteella, ja viestin lähettämiseksi liityntäpisteelle (2):

- joka osoittaa, että mainitun tilaajan (1, 1') autentikointi on epäonnistunut, kun tarkistus osoittaa, että tilaajalla on pääsy järjestelmään toisen autentikointimekanismin välityksellä ja/tai että tilaajan tili on peruutettu, tai

- joka osoittaa, että tilaajan (1, 1') autentikointi on onnistunut, kun tarkistus osoittaa, että tilaajalla ei ole pääsyä järjestelmään toisen autentikointimekanismin välityksellä, ja että tilaajan tiliä ei ole peruutettu.

6. Patenttivaatimuksen 5 mukainen järejstelmä, tunnettu siitä, että

mainittu liityntäpiste (2) on tukiasema, joka tarjoaa autentikoiduille tilaajille pääsyn viestintäjärjestelmään radiorajapinnan välityksellä,

mainitut autentikointivälineet (5) on järjestetty lähettämään solukkoradiojärjestelmälle pyynnön autentikointitietojen saamiseksi, vastaanottamaan autentikointitietoja solukkoradiojärjestelmältä, ja autentikoimaan mainitun tilaajan (1) autentikointiviestin sisällön sekä autentikointitietojen perusteella.

7. Patenttivaatimuksen 5 tai 6 mukainen järjestelmä, tunnettu siitä, että mainittu autentikointiviesti on uudelleenautentikointiviesti.

8. Jonkin patenttivaatimuksen 5 - 7 mukainen viestintäjärjestelmä, tunnettu siitä, että mainittu viestintäjärjestelmä on WLAN-järjestelmä, mainittu tilaaja on EAP SIM sovellus, ja mainitut tarkistusvälineet (9, 9') on järjestetty Radius palvelimeen (4, 4').

9. Viestintäjärjestelmän palvelin (4, 4'), mainitun palvelimen ollessa vasteellinen viestintäjärjestelmän autentikointivälineelle, tunnettu siitä, että mainittu palvelin käsittää tarkistusvälineet (9, 9'), jotka mainittujen autentikointivälineiden (5, 5') osoittaessa, että tilaajan (1, 1') autentikointi on onnistunut, on järjestetty hakemaan statustietoja mainitulle tilaajalle tilaajatietokannasta (7) tarkistuksen suorittamiseksi mainittujen statustietojen perusteella, ja lähettämään:

- viestin, joka osoittaa, että tilaajan (1, 1') autentikointi on epäonnistunut, kun tarkistuksen tulos osoittaa, että tilaajalla on pääsy viestintäjärjestelmään toisen autentikointimekanismin välityksellä ja/tai että tilaajan tili on peruutettu, tai

- viestin, joka osoittaa, että tilaajan (1, 1') autentikointi on onnistunut, kun tarkistus osoittaa, että tilaajalla ei ole pääsyä viestintäjärjestelmään toisen autentikointimekanismin välityksellä, ja että tilaajan tiliä ei ole peruutettu.

10. Patenttivaatimuksen 9 mukainen palvelin, t u n n e t t u siitä, että mainittu palvelin (4, 4') on Radius palvelin.

Patentkrav:

1. Förvarande för att autentikera en abonnent i ett kommunikationssystem, vilket förfarande omfattar:

mottagande (C, C') av ett autentikeringsmeddelande från en abonnent, och

kontroll av nämnda abonnents autenticitet genom att utnyttja innehållet i nämnda autentikeringsmeddelande, k ä n n e t e c k n a t av att

statusinformation gällande nämnda abonnent söks (E, F) från en abonnentdatabas,

ett meddelande som indikerar att nämnda abonnents autentikering har misslyckats sänds (G), ifall ett eller flera av följande villkor uppfylls:

- nämnda abonnents autentikering på basen av autentikeringsmeddelandets innehåll har misslyckats,

- statusinformationen indikerar att abonnenten har access till systemet via en annan autentikeringsmekanism, eller

- statusinformationen indikerar att abonnentens konto har annullerats.

2. Förfarande enligt patentkrav 1, k ä n n e t e c k n a t av att nämnda autentikeringsmeddelande är ett reautentikeringsmeddelande.

3. Förfarande enligt patentkrav 1, k ä n n e t e c k n a t av att nämnda kommunikationssystem är ett WLAN-system och nämnda förfarande omfattar vidare:

sändning (A) av en begäran om att få autentikeringsinformation från nämnda WLAN-system till ett mobilkommunikationssystem,

mottagande (B) av autentikeringsinformation från mobilkommunikationssystemet, och

kontroll av abonnentens autenticitet genom att utnyttja nämnda autentikeringsmeddelandes innehåll samt autentikeringsinformationen som erhållits från mobilkommunikationssystemet.

4. Förfarande enligt något av patentkraven 1 - 3, k ä n n e t e c k n a t av att nämnda abonnent är en EAP SIM applikation.

5. Kommunikationssystem som omfattar:

en accesspunkt (2) som erbjuder autentikerade abonnenter access till systemet,

en abonnentdatabas (7) som innehåller information gällande systemets abonnenter, och

autentikeringsdon (5, 5') för autentikering av en abonnent (1, 1') genom att utnyttja innehållet i ett autentikeringsmeddelande som mottagits av nämnda abonnent (1, 1'), k ä n n e t e c k n a t av att nämnda kommunikationssystem dessutom omfattar:

kontrolldon (9, 9') för att söka statusinformation gällande nämnda abonnent (1, 1') från abonnentdatabasen (7) då autentikeringsdonen indikerar att autentikeringen av nämnda abonnent (1, 1') har lyckats, att genomföra en kontroll på basen av nämnda sökta statusinformation, och att sända ett meddelande till accesspunkten (2):

- vilket indikerar att autentikeringen av nämnda abonnent (1, 1') har misslyckats, då kontrollen visar att abonnenten har access till systemet via en annan autentikeringsmekanism och/eller abonnentens konto har annullerats, eller

- vilket indikerar att autentikeringen av abonnenten (1, 1') har lyckats, då kontrollen visar att abonnenten inte har access till systemet via en annan autentikeringsmekanism och att abonnentens konto inte har annullerats.

6. System enligt patentkrav 5, k ä n n e t e c k n a t av att

nämnda accesspunkt (2) är en basstation som erbjuder autentikerade abonnenter access till kommunikationssystemet via ett radiogränssnitt,

nämnda autentikeringsdon (5) har anordnats att sända till ett mobilkommunikationssystem en begäran om att erhålla autentikeringsinformation, mottaga autentikeringsinformation från mobilkommunikationssystemet, och autentikera nämnda abonnent (1) på basen av innehållet i autentikeringsmeddelandet och autentikeringsinformationen.

7. System enligt patentkrav 5 eller 6, k ä n n e t e c k n a t av att nämnda autentikeringsmeddelande är ett reautentikeringsmeddelande.

8. System enligt något av patentkraven 5 - 7, k ä n n e t e c k n a t av att nämnda kommunikationssystem är ett WLAN-system, nämnda abonnent är en EAP SIM applikation, och nämnda kontrolldon (9, 9') är anordnade i en Radius server (4, 4').

9. Server (4, 4') för ett kommunikationssystem, vilken server gensvarar på kommunikationssystemets autentikeringsdon, k ä n n e t e c k n a d av att nämnda server omfattar kontrolldon (9, 9') som, då nämnda autentikeringsdon (5, 5') indikerar att en abonnents (1, 1') autentikering har lyckats, är anordnade att söka statusinformation för nämnda abonnent från en abonnentda-

tabas (7) för att utföra en kontroll på basen av nämnda statusinformation, och sända:

- ett meddelande som indikerar att abonnentens (1, 1') autentikering har misslyckats, då kontrollens resultat visar att abonnenten har access till kommunikationssystemet via en annan autentikeringsmekanism och/eller att abonnentens konto har annullerats, eller

- ett meddelande som indikerar att abonnentens (1, 1') autentikering har lyckats, då kontrollen visar att abonnenten inte har access till kommunikationssystemet via en annan autentikeringsmekanism, och att abonnentens konto inte har annullerats.

10. Server enligt patentkrav 9, k ä n n e t e c k n a d av att nämnda server (4, 4') är en Radius server.

116182

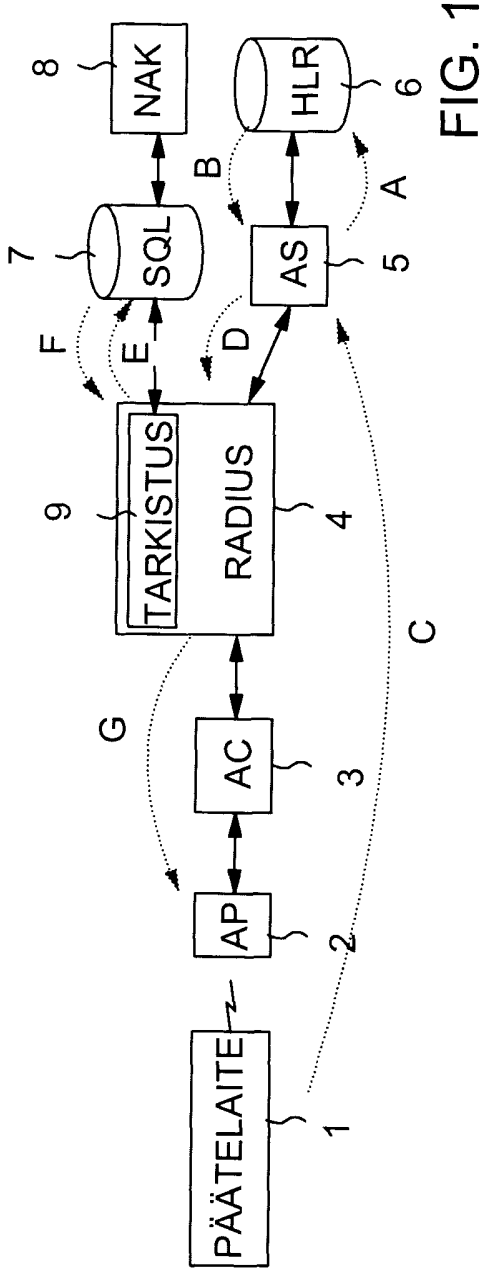


FIG. 1

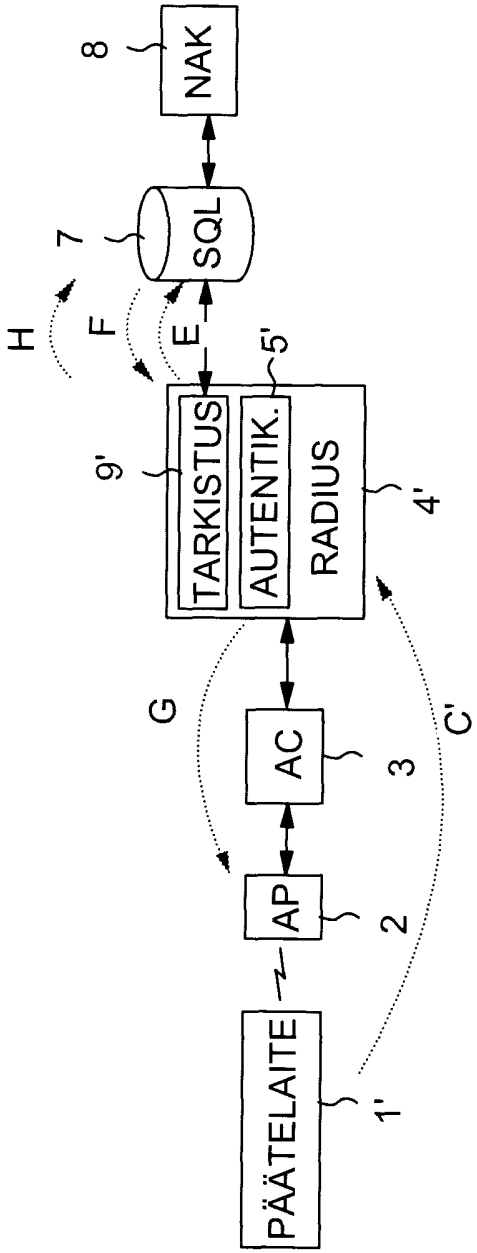


FIG. 2