FI000111208B

(12) **PATENTTIJULKAISU**
PATENTSKRIFT

(10) **FI 111208 B**

(45) Patentti myönnetty - Patent beviljats **13.06.2003**

(51) Kv.lk.7 - Int.kl.7
H04L 9/32, 12/56

(21) Patenttihakemus - Patentansökning **20001567**

(22) Hakemispäivä - Ansökningsdag **30.06.2000**

(24) Alkupäivä - Löpdag **30.06.2000**

(41) Tullut julkiseksi - Blivit offentlig **31.12.2001**

SUOMI – FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN

(73) Haltija - Innehavare

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

(72) Keksijä - Uppfinnare

1 •Ala-Laurila, Juha, Mustanlahdenkatu 10 A 5, 33210 Tampere, SUOMI - FINLAND, (FI)
2 •Honkanen,Jukka Pekka, Opiskelijankatu 18 A 15, 33720 Tampere, SUOMI - FINLAND, (FI)
3 •Rinnemaa,Jyri, Kaiturinkatu 16 A 5, 33820 Tampere, SUOMI - FINLAND, (FI)

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

(54) Keksinnön nimitys - Uppfinningens benämning

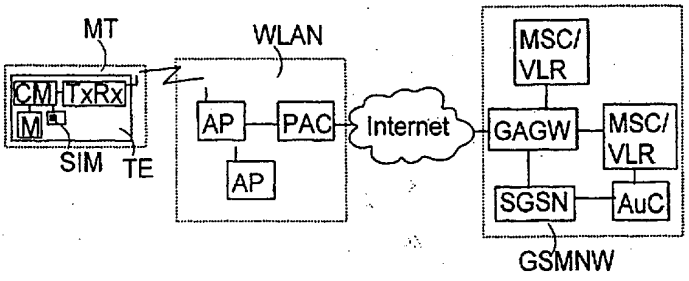
Datan salauksen järjestäminen langattomassa tietoliikennejärjestelmässä
Arrangemang av datakryptering i ett trådlöst telekommunikationssystem

(56) Viitejulkaisut - Anförda publikationer

EP A 0930795 (H04Q 7/38, H04Q 7/24), WO A 0113666 (H04Q 7/38), WO A 0001187 (H04Q 7/38), WO A 0076238 (H04Q 7/32)

(57) Tiivistelmä - Sammandrag

Datan salauksen (ciphering) järjestäminen tietoliikennejärjestelmässä, joka käsittää ainakin yhden langattoman päätelaitteen, langattoman lähiverkon ja yleisen matkaviestinverkon. Päätelaitteelle tarjotaan tunniste ja tunnisteelle spesifinen salainen avain, joka on myös tallennettu matkaviestinverkkoon. Päätelaitteelta lähetetään matkaviestinverkolle päätelaitteen tunniste. Matkaviestinverkossa lasketaan matkaviestinverkon mukainen ainakin yksi ensimmäinen salausavain tunnisteelle spesifisen salaisen avaimen ja ensimmäistä salaista avainta varten valitun haasteen avulla. Ainakin yksi haaste lähetetään päätelaitteelle salausavaimen muodostamista varten. Päätelaitteessa lasketaan matkaviestinverkon mukainen ainakin yksi ensimmäinen salausavain salaisen avaimen ja ainakin yhden haasteen avulla. Tiedonsiirto hoidetaan matkaviestinverkon ja päätelaitteen välillä langattoman lähiverkon kautta. Päätelaitteessa ja matkaviestinverkossa lasketaan toinen salausavain mainitun ainakin yhden ensimmäisen salausavaimen avulla. Toinen salausavain lähetetään matkaviestinverkosta langattomaan lähiverkkoon. Päätelaitteessa ja langattomassa lähiverkossa salataan päätelaitteen ja verkon välinen data toista salausavainta käyttäen.



Uppfinningen avser ett arrangemang för chiffrering (ciphering) av data i ett datatrafiksystem, vilket omfattar minst en trådlös terminal- apparat, ett trådlöst närnät och ett allmänt mobiltelefonnät. Åt sagda terminalapparat ges ett identifieringtecken och åt sagda identifieringtecken en specifik hemlig nyckel, vilken även är minneslagrad i sagda mobiltelefonnät. Terminalapparatens identifieringtecken sändes från terminalapparaten till sagda mobiltelefonnät. I sagda mobiltelefonnät beräknas minst en mobiltelefonnätsenlig chiffreringsnyckel för sagda identifieringtecken med hjälp av sagda specifika hemliga nyckel och en för sagda första hemliga nyckel val anfordran. Åtminstone en anfordran sändes till sagda terminalapparat för bildande av en chiffreringsnyckel. I sagda terminalapparat beräknas minst en första mobiltelefonnätsenlig chiffreringsnyckel med hjälp av sagda hemliga nyckel och minst ena anfordran. Dataöverföringen mellan sagda mobiltelefonnät och sagda terminalapparat sker via sagda trådlösa närnät. I sagda terminalapparat och mobiltelefonnät beräknas en andra chiffreringsnyckel med hjälp av sagda minst ena första chiffreringsnyckel. Den andra chiffreringsnyckeln sändes från sagda mobiltelefonnät till sagda trådlösa närnät. I sagda terminalapparat och trådlösa närnät chiffreras datan mellan terminalapparaten och nätet med användning av den andra chiffreringsnyckeln.

Datan salauksen järjestäminen langattomassa tietoliikennejärjestelmässä

Keksinnön tausta

Keksintö liittyy datan salauksen järjestämiseen langattomissa tietoliikennejärjestelmissä ja erityisesti langattomissa lähiverkoissa WLAN (Wireless Local Area Network).

Viime vuosina yleisten matkaviestinverkkojen PLMN (Public Land Mobile Network) lisäksi ovat yleistyneet erilaiset langattomat lähiverkot. Eräitä tällaisia langattomia lähiverkkoja ovat IEEE802.11-standardiin perustuvat verkot. IEEE802.11-verkkojen turvallisuusnäkökohtiin on kiinnitetty huomiota kehittämällä WEP-toiminnallisuus (Wired Equivalent Privacy). WEP kuvaa liikenteen salauksen 2-kerroksella (MAC) IEEE802.11-standardia tukevien päätelaitteen ja liityntäpisteen (Access Point) välillä. WEP on symmetrinen algoritmi, jossa käytetään samaa salausavainta sekä datan salaukseen (enciphering) että datan salauksen purkuun (deciphering).

Eräissä langattomissa tietoliikenneverkoissa, kuten IEEE802.11 WLAN-verkoissa, on kuitenkin ongelmana se, että liikenteen salaukseen käytettävät salausavaimet on oltava etukäteen tallennettuina sekä päätelaitteeseen että liityntäpisteeseen. Jos verkossa ei ole samaa avainta kuin päätelaitteessa, verkon ja päätelaitteen välistä dataa ei voida salata. Eri salausavaimien lisääminen on työlästä, eikä eri verkoissa liikkuville päätelaitteille aina voida tarjota turvallista tiedonsiirtoa.

Keksinnön lyhyt selostus

Keksinnön tavoitteena on siten kehittää uudenlainen tapa muodostaan salaukseen käytettävät avaimet langatonta lähiverkkoa varten ja käyttää niitä siten, että yllä mainitut ongelmat voidaan välttää. Keksinnön tavoitteet saavutetaan menetelmällä, järjestelmällä, päätelaitteella ja liityntäpisteellä, joille on tunnusomaista se, mitä sanotaan itsenäisissä patenttivaatimuksissa. Keksinnön edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Keksintö perustuu siihen, että päätelaitteessa ja yleisessä matkaviestinverkossa lasketaan ns. toinen salausavain yleisen matkaviestinverkon mukaisen ainakin yhden ns. ensimmäisen salausavaimen perusteella. Toinen salausavain lähetetään matkaviestinverkosta langattomaan lähiverkkoon. Pää-

telaitteessa ja langattomassa lähiverkossa sekä salataan päätelaitteen ja verkon välinen data että puretaan datan salaus toista salausavainta käyttäen.

Tästä saavutetaan se etu, että voidaan hyödyntää matkaviestinverkkoa ja sen tarjoamaa tunnistusyksikköä langattomassa lähiverkossa käytettävän salausavaimen laskemisessa. Liikkuvia päätelaitteita varten voidaan langattomaan lähiverkkoon tarjota salausavain dynaamisesti päätelaitteen muodostaessa yhteyttä. Tällöin salausavainta ei tarvitse tallentaa etukäteen langattomaan lähiverkkoon.

Keksinnön erään edullisen suoritusmuodon mukaisesti päätelaitteessa ja matkaviestinverkossa lasketaan matkaviestinverkon mukainen ainakin yksi autentikaatiovaste ainakin yhden haasteen ja salaisen avaimen perusteella. Päätelaitteessa lasketaan tarkistusvaste ainakin yhden autentikaatiovasteen ja ensimmäisen salausavaimen perusteella. Tarkistusvaste lähetetään matkaviestinverkkoon. Matkaviestinverkossa lasketaan tarkistusvaste ainakin yhden autentikaatiovasteen ja ainakin yhden ensimmäisen salausavaimen perusteella. Päätelaitteen lähettämää tarkistusvastetta verrataan matkaviestinverkon laskemaan tarkistusvasteeseen. Toinen salausavain lähetetään matkaviestinverkosta langattomaan lähiverkkoon, jos päätelaitteen lähettämä ja matkaviestinverkon laskema tarkistusvaste vastaavat toisiaan. Tästä suoritusmuodosta saavutetaan se etu, että matkaviestinverkossa voidaan suorittaa luotettava tilaajan (tunnistusyksikön) autentikointi. Näin ainoastaan autentikoiduille päätelaitteille voidaan sallia tiedonsiirtoyhteys ja datan salaus langattomassa lähiverkossa.

Keksinnön vielä erään edullisen suoritusmuodon mukaisesti päätelaitteesta lähetetään suojakoodi matkaviestinverkolle. Matkaviestinverkossa lasketaan tarkistussumma suojakoodin ja ainakin yhden ensimmäisen salausavaimen avulla. Tarkistussumma lähetetään päätelaitteelle, jossa tarkastetaan tarkistussumma. Toinen salausavain lasketaan päätelaitteessa, jos vastaanotettu tarkistussumma on oikea. Tästä saavutetaan se etu, että päätelaitteessa voidaan varmistua matkaviestinverkon luotettavuudesta, eli siitä, onko sillä tiedossaan tunnistusyksikköön liittyvä salainen avain.

Kuvioiden lyhyt selostus

Keksintöä selostetaan nyt lähemmin edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirroksiin, joista:

Kuvio 1 esittää lohkokaaviona erään edullisen suoritusmuodon mukaista langatonta tietoliikennejärjestelmää;

Kuvio 2 esittää signalointikaaviona erään edullisen suoritusmuodon mukaista autentikaatiota ja salausavaimen laskemista;

Kuvio 3 havainnollistaa erään edullisen suoritusmuodon mukaista salauksen järjestämistä päätelaitteen ja liityntäpisteen välillä;

Kuvio 4 havainnollistaa salausvälineitä datan salaamiseksi; ja

Kuvio 5 havainnollistaa salausvälineitä salauksen purkamiseksi.

Keksinnön yksityiskohtainen selostus

Keksintöä voidaan soveltaa missä tahansa langattomassa tietoliikennejärjestelmässä, joka käsittää langattoman lähiverkon ja yleisen matkaviestinverkon. Kuviossa 1 esitetään keksinnön erään edullisen suoritusmuodon mukaista tietoliikennejärjestelmää. Järjestelmä käsittää päätelaitteen MT, IEEE802.11 standardin mukaisen WLAN verkon WLAN ja yleisen matkaviestinverkon, tässä suoritusmuodossa GSM-verkon GSMNW. Keksintöä voidaan kuitenkin soveltaa myös muunlaisiin verkkoihin: Langaton lähiverkko voi olla erimerkiksi BRAN-standardien (Broadband Radio Access Network) mukainen verkko. BRAN-standardit käsittävät tyyppien 1 ja 2 HIPERLAN-standardit (High Performance Radio Local Area Network), HIPERACCESS- ja HIPERLINK-standardit. Matkaviestinverkko ei myöskään ole rajoittunut GSM-verkkoon, keksintöä voidaan soveltaa esimerkiksi myös UMTS-verkossa (Universal Mobile Telecommunications System).

Verkon WLAN operaattori, WISP (Wireless Internet Service Provider), tarjoaa langattomia erään suoritusmuodon mukaisesti IP-pohjaisia palveluita niin, että päätelaitteet MT voivat liikkua erilaisissa, tyypillisesti suuresti kuormitetuissa, tiloissa (hotspot), kuten hotelleissa, lentokentillä jne. WLAN-verkko WLAN käsittää WLAN-liityntäpisteitä AP, jotka tarjoavat langattoman yhteyden useille päätelaitteille MT. IEEE 802.11 -standardi määrittää sekä fyysisen tason että MAC-tason protokollat tiedonsiirrolle radiorajapinnan yli. Tiedonsiirrossa voidaan käyttää infrapunaa tai kahta hajaspektritekniikkaa (Direct Sequence Spread Spectrum DSSS, Frequency Hopped Spread Spectrum FHSS). Molemmissa hajaspektritekniikoissa käytetään 2,4 gigahertsin kaistaa. IEEE 802.11-standardin mukaisesti MAC-kerroksella käytetään ns. CSMA/CA-tekniikkaa (Carrier Sense Multiple Access with Collision Avoidance).

Päätelaitteen MT laiteosaan TE (Terminal Equipment) on kytketty GSM-verkolle spesifinen tilaajan tunnistusyksikkö SIM (Subscriber Identity Module), eli päätelaite MT käsittää sekä TE:n että SIM:n. Päätelaitteessa MT käytettävä tunnistusyksikkö voi olla erilainen matkaviestinverkosta riippuen,

esimerkiksi UMTS-verkoissa käytetään tunnistusyksikköä USIM (UMTS Subscriber Identity Module). SIM on tyypillisesti tallennettuna IC-kortille (Integrated Circuit), jota voidaan vaihtaa laitteesta TE toiseen. SIM on matkaviestinverkon GSMNW operaattorin luovuttama ja matkaviestinverkossa GSMNW on tallennettuna tiedot SIM:stä. SIM käsittää tilaajan tunnistetiedon IMSI (International Mobile Subscriber Identity), joka edustaa tilaajaa verkossa ja toimii näinollen päätelaitteen MT tunnisteena. Päätelaitteen MT laiteosalla TE voi olla myös oma laitetunnisteensa IMEI (International Mobile Equipment Identity), joka ei kuitenkaan ole relevantti keksinnön kannalta. SIM käsittää myös salaisen avaimen Ki, algoritmin A8 salausavaimen Kc muodostamista varten ja algoritmin A3 autentikaatiovasteen SRES (Signed Response) muodostamista varten.

MT käsittää kontrollivälineet CM, jotka ohjaavat MT:n toimintaa ja kommunikointia langattoman lähiverkon WLAN kanssa muistia M hyödyntäen. Kontrollivälineet CM mm. hoitavat toisen salausavaimen laskemisen MT:ssä myöhemmin kuvatun tavan mukaisesti. MT:n käsittämien kortinlukuvälineiden (ei esitetty) avulla CM voi hyödyntää tunnistusyksikköä SIM ja sen käsittämiä tietoja. MT käsittää myös lähetinvastaanottimen TxRx ainakin verkon WLAN liityntäpisteen AP kanssa kommunikoimista varten. MT voi olla esimerkiksi kannettava tietokone, jossa on älykortin käsittävä WLAN-adapterikortti. Päätelaite MT voi myös käsittää GSM-matkaviestinosan GSM-verkkojen kanssa kommunikoimista varten.

WLAN-päätelaitteet MT voivat muodostaa ns. adhoc -verkon yksinkertaisesti muodostamalla yhteyden toiseen liikkuvaan päätelaitteeseen. Ns. infrastruktuuriverkkoja (Infrastucture Networks) muodostetaan tekemällä yhteyksiä liityntäpisteiden AP ja päätelaitteiden MT välille. Liityntäpisteet AP tarjoavat verkkoyhteyksiä päätelaitteille MT ja näin muodostavat ns. laajennetun palvelusetin (ESS, Extended Service Set). Liityntäpisteet AP ainakin kontrolloivat lähetysaikojen allokaatioita, datan vastaanottoa, bufferointia ja lähetystä päätelaitteen MT ja verkon WLAN välillä. Liityntäpisteet AP voivat muodostaa aliverkkoja (Sub-Network). Looginen WLAN-verkko WLAN voi puolestaan käsittää yhden tai useampia aliverkkoja.

WLAN-verkko WLAN voi tarjota myös yhteyden yhdyskäytävän kautta muihin verkkoihin, kuten Internetiin. Yhteys muihin verkkoihin voidaan järjestää verkosta WLAN pääsykontrollerin PAC (Public Access Controller) kautta. PAC on verkon WLAN entiteetti, joka kontrolloi pääsyä esimerkiksi Internet-palveluihin. Edullisen suoritusmuodon mukaisesti se allokoi IP-osoitteen

päätelaitteelle MT ja sallii yhteyden muodostuksen Internetiin vain, jos päätelaite MT saadaan autentikoitua. Tyypillisesti WLAN-verkko NW käsittää myös muita palvelimia, kuten DHCP (Dynamic Host Configuration Protocol) palvelimen, joka allokoi IP-osoitteita verkossa WLAN.

Matkaviestinverkko GSMNW käsittää yhden tai useampia tyypillisesti vierailijarekisterin VLR (Visitor Location Register) käsittäviä matkaviestinkeskuksia MSC/VLR (Mobile Switching Center) ja tai GPRS-operointisolmuja SGSN (Serving (General Packet Radio Service) Support Node). Matkaviestinverkko GSMNW käsittää myös GSM/GPRS autentikaatio- ja laskutusyhdyskäytävän GAGW (GSM/GPRS Authentication and Billing Gateway), joka on kytketty Internetiin. GAGW on matkaviestinverkon GSMNW entiteetti, joka tarjoaa matkaviestintilaajien autentikaatiopalveluita WLAN-verkoille WLAN ja edullisesti myös kerää laskutusinformaatiota. Näin matkaviestinverkon GSMNW tilaajatietoja ja autentikaatiopalveluita voidaan käyttää WLAN-verkossa WLAN olevien tunnistusyksikön SIM käsittävien päätelaitteiden MT palvelemiseksi. Päätelaitteen MT käyttäjällä ei välttämättä tarvitse olla ennalta sovittua sopimusta WLAN-verkon WLAN operaattorin kanssa. Vieraileva päätelaite MT voi käyttää tunnistusyksikköä SIM ja matkaviestinverkkoa GSMNW autentikaation ja laskutuksen toteuttamiseksi vieraillessaan verkossa WLAN. Tällöin verkon WLAN tarjoamasta langattomasta yhteydestä voidaan laskuttaa matkaviestinverkon GSMNW yhdyskäytävän GAGW kautta. Matkaviestinoperaattori voi myöhemmin hyvittää WLAN-operaattoria verkon käytöstä.

Kuten GSM-järjestelmästä on tunnettua, tunnistusyksikön SIM omistava tilaajan kotiverkko käsittää tilaajatietoja, jotka on tallennettu GSM-kotirekisteriin HLR (Home Location Register). WLAN-verkon WLAN entiteetti PAC lähettää autentikaatio- ja laskutustietoja yhdyskäytävälle GAGW. GAGW voi käyttää tunnettua GSM-signalointia pyytääkseen autentikaatiotietoja tunnistusyksikölle SIM ja suorittaa autentikaation ja salausavaimen laskemisen myöhemmin kuvatulla tavalla. Jos SIM saadaan autentikoitua, PAC voi tarjota yhteyden Internetiin tai muihin verkon WLAN osiin. PAC voi käyttää myös muita tapoja kuin SIM-pohjaista autentikaatiota päätelaitteen MT tunnistamiseksi, esimerkiksi salasanan tunnistusta.

PAC voi välittää käyttäjän dataa Internetin ja päätelaitteen MT välillä. Rajapinnat päätelaitteen MT ja kontrollerin PAC ja PAC ja GAGW:n välillä ovat keksinnön esillä olevan erään edullisen suoritusmuodon mukaisesti IP-pohjaisia. On huomioitava, että myös muita tekniikoita kuin IP:tä voidaan käyt-

tää. Kuviosta 1 poiketen PAC:n ja GAGW:n välissä ei myöskään välttämättä ole Internetiä, vaikka käytettäisiinkin IP-protokollaa. Jatkossa oletetaan, että käytössä on IP, jolloin MT, PAC ja GAGW identifioidaan niiden IP-osoitteiden avulla. Yhdyskäytävän GAGW ja matkaviestinverkon GSMNW välinen rajapinta riippuu toteutuksesta, esim. matkaviestinverkon ollessa esimerkiksi UMTS-verkko, tämä rajapinta voi olla erilainen GSM-verkkoon verrattuna. Yhdyskäytävä GAGW peittääkin matkaviestinverkon GSMNW infrastruktuurin PAC:lta. Näinollen PAC:n ja GAGW:n välinen rajapinta pysyy samana riippumatta matkaviestinverkosta GSMNW.

Kuvio 2 esittää keksinnön erään edullisen suoritusmuodon mukaisia olennaisia toimintoja päätelaitteen MT autentikoimiseksi ja salausavaimen laskemiseksi. Päätelaitteelle MT tarjotaan tunniste IMSI ja salainen avain Ki sen käsittämällä tilaajan tunnistussovelluksella SIM. Päätelaitteen MT autentikaatioprosessi tyypillisesti käynnistetään (trigger), kun MT alkaa muodostaa yhteyttä 201 (Connection setup) WLAN-verkkoon WLAN. Tällöin MT hankkii IP-osoitteen DHCP-palvelimen (Dynamic Host Configuration Protocol) kautta. Ennenkuin päätelaitteelle MT sallitaan yhteyden muodostaminen muihin verkkoihin kuin verkkoon WLAN, autentikaatio täytyy suorittaa hyväksytysti.

MT pyytää 202 (IMSI request) tunnistusyksiköltä SIM IMSI-tunnistetta ja SIM palauttaa 203 IMSI-tunnisteen. MT lähettää 204 autentikaation aloittamispyynnön (MT_PAC_AUTHSTART_REQ), joka edullisesti käsittää verkkotunnisteen NAI (Network Access Identifier). NAI käsittää tunnistusyksiköltä SIM saadun IMSI-tunnisteen. NAI voi olla esimerkiksi muotoa 12345@GSM.org, missä 12345 on IMSI-tunniste ja GSM.org on tunnistusyksikön SIM luovuttaneen matkaviestinverkon domain-nimi. Pyyntö 204 lähetään edullisesti salattuna PAC:lle esimerkiksi käyttämällä Diffie-Hellman-algoritmia. MT edullisesti myös lähettää pyynnössä 204 oman suojakoodinsa MT_RAND, joka on tyypillisesti satunnaisluku. Suojakoodin MT_RAND avulla MT voi myöhemmin varmentua, että GSM-tripletit luovuttavalla osapuolella on todella pääsy tilaajan GSM-kotiverkossa säilytettävään salaiseen avaimeen Ki. Suojakoodin käyttäminen ei kuitenkaan ole mitenkään pakollista.

PAC tarpeen mukaan purkaa pyynnön 204 salauksen ja lähettää 205 GAGW:lle verkkotunnisteen NAI domain-osan perusteella pyynnön (PAC_GAGW_AUTHSTART_REQ) IMSI-tunnisteen mukaisen tunnistusyksikön SIM autentikoimiseksi. Tämä viesti käsittää verkkotunnisteen NAI ja päätelaitteen MT lähettämän suojakoodin MT_RAND.

GAGW pyytää 206 (Send_Parameters) ainakin yhtä triplettiä matkaviestinverkolta GSMNW. Tämä voidaan hoitaa niin, että GAGW välittää pyynnön lähimmälle matkaviestinkeskukselle MSC/VLR (tai operointisolmulle SGSN). MSC/VLR tarkastaa IMSI-tunnisteen ja lähettää pyynnön tunnistusyksikön SIM omistavan verkon kotirekisteriin HLR, joka tyypillisesti käsittää autentikaatiokeskuksen AuC (Authentication Center) (kuviossa jo verkon GSMNW AuC). Matkaviestinverkon GSMNW käsittämissä ensimmäisissä laskemisvälineissä eli GSM-verkon ollessa kyseessä autentikaatiokeskuksessa AuC muodostetaan 207 (Calculate Kc(s)) IMSI-tunnisteen mukaisen salaisen avaimen Ki avulla yksi tai useampia GSM-triplettejä (RAND, SRES, Kc) jo tunnetulla tavalla. GSM-tripletti käsittää haasteen RAND, RAND:n ja salaisen avaimen Ki perusteella algoritmia A3 käyttäen muodostetun autentikaatiovasteen SRES, ja RAND:n ja salaisen avaimen Ki perusteella algoritmia A8 käyttäen muodostetun ensimmäisen salausavaimen Kc. HLR lähettää tripletin MSC/VLR:lle, joka välittää tripletit edelleen GAGW:lle 208 (Send_Parameters_Result). Matkaviestinverkosta GSMNW voidaan myös lähettää useita triplettejä, jolloin GAGW edullisesti valitsee yhden ja se voi tallentaa muut tripletit myöhempää käyttöä varten.

GAGW edullisesti laskee 209 (Calculate SIGNrand) myös tarkistussumman tai MAC-viestintunnistuskoodin (Message Authentication Code) SIGNrand päätelaitteen MT lähettämän suojakoodin MT_RAND ja Kc:n avulla. SIGNrand on kryptografinen tarkistussumma, jonka avulla voidaan varmentaa, että lähetetyt tiedot todella ovat entiteetiltä, jolla on yhteys matkaviestinverkossa GSMNW olevaan salaiseen avaimeen Ki.

GAGW lähettää 210 PAC:lle autentikaation pyynnön kuittausviestin GAGW_PAC_AUTHSTART_RESP, joka käsittää yhden tai useampia haasteita RAND päätelaitetta MT varten ja edullisesti myös tarkistussumman SIGNrand. Tässä viestissä voi olla myös laskutukseen liittyviä tietoja. Viesti voidaan myös salata käyttämällä suojakoodia MT_RAND. PAC lähettää 211 päätelaitteelle MT autentikaation pyynnön kuittausviestin PAC_MT_AUTHSTART_RESP, joka käsittää ainakin yhden haasteen RAND ja edullisesti tarkistussumman SIGNrand.

Päätelaitteessa MT syötetään 212 haaste(et) RAND tunnistusyksikköön SIM. SIM laskee 213 (Calculate Kc(s)) matkaviestinverkon GSMNW mukaisen ainakin yhden ensimmäisen salausavaimen Kc ja autentikaatiovasteen (-vasteita) SRES vastaavalla tavalla kuin autentikaatiokeskuksessa AuC ja vä-

littää 214 ne päätelaitteen MT muulle osalle (edullisesti autentikaatiota ja salausavaimen K laskentaa hoitavalle kontrollivälineille CM). MT voi SIM:ltä saatujen tietojen (Kc:t) ja suojakoodin MT_RAND perusteella tarkastaa 215 (Check SIGNrand) PAC:n lähettämän tarkistussumman SIGNrand. Jos vastaanotettu SIGNrand vastaa tunnistusyksikön SIM laskemien Kc-arvojen perusteella saatua arvoa, MT, tarkemmin ottaen CM, laskee 216 (Calculate SIGNsres) tarkistusvasteen SIGNsres välitettäväksi GAGW:lle. SIGNsres on edullisesti yhden tai useamman ensimmäisen salausavaimen Kc ja autentikaatiovasteen SRES laskettu tiivistefunktio eli hash-funktio, jonka avulla GAGW voi autentikoida MT:n. MT voi myös pyytää käyttäjän hyväksyntää PAC:n mahdollisesti lähettämille hintatiedoille.

MT käsittämissä toisissa laskemisvälineissä, edullisesti kontrollivälineissä CM lasketaan 217 (Calculate K) toinen salausavain K käyttämällä SIM:n laskemaa yhtä tai useampaa matkaviestinverkon GSMNW mukaista ensimmäistä salausavainta Kc. K lasketaan erään edullisen suoritusmuodon mukaisesti:

K = HMAC(n*Kc, n*RAND | IMSI | MT_RAND), missä
HMAC: mekanismi autentikoinnille hash-funktiota käyttämällä,
n*Kc: n kappaletta Kc:tä,
n*RAND: n RAND:a
IMSI: tilaajatunniste SIM:ltä ja
MT_RAND on MT:n generoima satunnaisluku.

Näin laskettu toinen salausavain K on vaikeammin selvitettävissä kuin ensimmäinen salausvain Kc ja salauksesta saadaan vahvempi kuin GSM-salauksesta. MT tallentaa K:n muistiinsa M tai älykortin muistiin myöhempää käyttöä varten. Esimerkiksi MD5- ja SHA-1 algoritmeja voidaan käyttää K:n laskemiseen.

MT lähettää 218 PAC:lle autentikaatiovastausviestin (MT_PAC_AUTHANSWER_REQ). Viesti käsittää ainakin tarkistusvasteen SIGNsres ja MT:n suojakoodin MT_RAND (kuten edullisesti kaikki autentikaatioon liittyvät viestit). PAC lähettää 219 GAGW:lle autentikaatiovastausviestin (PAC_GAGW_AUTHANSWER_REQ), joka käsittää päätelaitteen MT lähettämän viestin (218) käsittämien tietojen lisäksi verkkotunnisteen NAI ja PAC:n osoitetiedot. GAGW tarkastaa 220 (Check SIGNsres) MT:n lähettämän tarkistusvasteen SIGNsres. On myös mahdollista, että GAGW on generoinut tarkistusvasteen SIGNsres jo tarkistussumman SIGNrand laskemisen (209) yhtey-

dessä. Jos GAGW:n laskema SIGNsres vastaa päätelaitteen MT lähettämää SIGNsres-arvoa, tarkistus on onnistunut ja päätelaite MT on autentikoitu hyväksyttävästi.

Jos autentikaatio on hyväksyttävä, matkaviestinverkon toiset laskemisvälineet eli GAGW laskevat 221 (Calculate K) toisen salausavaimen K käyttämällä matkaviestinverkon GSMNW mukaista ainakin yhtä ensimmäistä salausavainta Kc. K lasketaan samalla tavalla ja samoilla parametreillä kuin päätelaitekin MT on sen laskenut (217):

K = HMAC(n*Kc, n*RAND | IMSI | MT_RAND).

On myös mahdollista kuviosta 2 poiketen, että GAGW laskee ja tallentaa muistiinsa toisen salausavaimen K jo saadessaan tripletin verkosta GSMNW (208) ja lähettää muistiin tallennetun K:n WLAN-verkkoon WLAN, jos autentikaatio on hyväksyttävä.

GAGW lähettää 222 PAC:lle tiedon autentikaation hyväksymisestä (GAGW_PAC_AUTHANSWER_RESP_OK). Tämä viesti käsittää ainakin toisen salausavaimen K. Viestissä 222 voidaan myös lähettää tietoja (esimerkiksi palvelun laatutietoja QoS) palveluista, joita MT on oikeutettu käyttämään. PAC välittää 223 päätelaitteelle MT tiedon autentikaation hyväksymisestä (PAC_MT_AUTHANSWER_RESP_OK). Tällöin autentikaatio on suoritettu ja sekä päätelaite MT että PAC käsittävät samanlaisen toisen salausavaimen K, joka voidaan välittää salauksen suorittaville salausvälineille liikenteen salaamiseksi.

Jos autentikaatio ei onnistunut, viesti 222 (ja 223) käsittävät tiedon autentikaation epäonnistumisesta ja päätelaitteelle MT edullisesti ei tarjota palveluita verkossa WLAN.

Päätelaitteen MT ja pääsykontrollerin PAC:n välisessä tiedonsiirrossa voidaan hyödyntää esimerkiksi IKE-protokollaan (Internet Key Exchange) perustuvia viestejä. RADIUS-protokollaan (Remote Authentication Dial In User Service) perustuvia viestejä voidaan käyttää puolestaan PAC:n ja GAGW:n välillä.

Kuviossa 3 on havainnollistettu erään edullisen suoritusmuodon mukaista salauksen järjestämistä päätelaitteen MT ja liityntäpisteen AP välillä. MT:n löytäessä tavoitettavissa olevan liityntäpisteen AP, se lähettää edullisesti IEEE802.11-standardin mukaisesti pyynnön 301 (Open_system_authentication_request) avoimen järjestelmän autentikaatiosta liityntäpisteelle AP. Avoimen järjestelmän autentikaatiossa ei käytännössä

suoriteta todellista autentikaatiota, jolloin mikä tahansa IEEE802.11-standardin mukainen MT voidaan autentikoida. MT ainoastaan lähettää tiedon identiteetistään pyynnössä 301. AP lähettää 302 (Open_system_authentication_result) vastauksen MT:lle.

Jos AP on hyväksynyt MT:n verkkoonsa, MT pyytää 303 (Association_request) assosiaatiota verkkoon WLAN. AP vastaa 304 (Association_response) pyyntöön. Assosiaatio suoritetaan, jotta WLAN-verkossa WLAN tiedetään, mille liityntäpisteelle AP lähettää MT:lle kohdistuva data. Päätelaitteen MT täytyy olla assosioitu kerrallaan yhdessä liityntäpisteessä AP, jotta se voi lähettää dataa AP:n kautta.

Tämän jälkeen suoritetaan edullisesti kuvion 2 yhteydessä havainnollistetulla tavalla autentikaatio ja toisen salausavaimen K laskeminen matkaviestinverkon GSMNW avulla. Tällöin päätelaitteessa MT lasketaan 305 (Calculation of K) toinen salainen avain K. Jos autentikaatio on hyväksyttävä, PAC vastaanottaa 306 (Reception of K) GAGW:n laskeman toisen salaisen avaimen K. PAC lähettää 307 (Authentication_information) AP:lle toisen salaisen avaimen K ja tiedon autentikaatiosta onnistumisesta, jolloin AP linkittää K:n päätelaitteen MT MAC-osoitteeseen. PAC:lta lähetetään 308 AP:n kautta edullisesti samaa viestiä hyödyntäen myös MT:lle tieto autentikaation onnistumisesta (PAC_MT_AUTHANSWER_RESP_OK).

Saatuaan toisen salaisen avaimen K, AP lähettää 309 (Put_WEP_on) MT:lle pyynnön WEP-algoritmin käyttämisestä data salaukseen. MT kuittaa 310 (Put_WEP_on_ack) pyynnön, jotta datan salaamisen alkamiskohta saadaan oikein ajoitettua. Tämän jälkeen toinen salainen avain K viedään MT:n MAC-kerrokselle ja MT salaa lähetettävän datan ja purkaa vastaanotetun datan salauksen 311 (Cipher data with K and WEP) K:n ja WEP-algoritmin avulla. AP alkaa myös käyttämään 312 (Cipher data with K and WEP) K:ta ja WEP-algoritmia MT:lle kohdistuvan datan salaamisessa ja MT:ltä vastaanotetun datan salauksen purkamisessa. AP tarkkailee vastaanotetun datan MAC-osoitteita ja suorittaa MT:n MAC-osoitteesta tulevalle datalle salauksen purkamisen ja vastaavasti salaa MT:n MAC-osoitteeseen kohdistuvan datan. Tällöin saadaan K nopeasti käyttöön ja data salaus voidaan aloittaa.

Eräs vaihtoehtoinen tapa toteuttaa toisen salausavaimen K käyttöönotto viestin 308 (223) jälkeen on hyödyntää muita IEEE802.11-protokollan viestejä: MT voi suorittaa autentikoinnin poistamisen (Deauthentication) avoi-

men järjestelmän autentikaatiolle (301, 302) viestien 309 ja 310 sijaan. Kun autentikaation poistaminen on suoritettu, MT voi pyytää IEEE802.11-standardin jaetun avaimen autentikaatiota (Shared Key Authentication) liityntäpisteeltä AP. Tämän jälkeen suoritetaan sinänsä jo IEEE802.11-standardista tunnetun neljän kehyksen (first, second, third, final) lähettäminen, jotta voidaan todeta molempien käsittävän saman jaetun avaimen. Jaettuna avaimena on tässä tapauksessa toinen salausavain K. Jos jaetun avaimen autentikaatio onnistuu, voidaan siirtyä salaukseen 311, 312. Tästä saavutetaan se etu, että voidaan käyttää jo IEEE802.11-protokollassa olevia viestejä.

Jos päätelaitteen yhteysvastuu siirtyy (handover) uudelle liityntäpisteelle, vanha liityntäpiste voi välittää toisen salausavaimen K uudelle liityntäpisteelle. Näin voidaan tarjota datan salaus myös handoverin jälkeen.

Kuviossa 4 on havainnollistettu keksinnön erään edullisen suoritusmuodon mukaisen liityntäpisteen AP ja päätelaitteen MT käsittämiä salausvälineitä ECM (Enciphering means) datan salaamiseksi (enciphering) käyttämällä toista salausavainta K ja WEP-algoritmia. Sekä MT että AP suorittavat kehyksien salaamisen kuviossa 4 esitetyllä tavalla. Toinen salausavain K konkatenoidaan 24-bittisen aloitusvektorin IV (Initialization Vector) kanssa, joten niistä muodostuu syöte 401 WEP-satunnaislukugeneraattoria WPRNG (WEP Pseudorandom Number Generator) varten. WPRNG tuottaa avainsekvenssin 402 (Key Sequence), joka on yhtä pitkä kuin siirrettävien dataoktettien määrä + 4. Tämän sen takia, että eheysalgoritmin IA (Integrity Algorithm) suojaamattomasta datasta 403 (Plaintext) muodostama eheyden tarkastusarvo ICV (Integrity Check Value) 404 suojataan myös. Suojaamaton data 403 yhdistetään eheyden tarkastusarvon ICV 404 kanssa ja tulos 405 (Plaintext+ICV) viedään yhdistettäväksi avainsekvenssin 402 kanssa. Avainsekvenssi 402 yhdistetään tämän jälkeen suojaamattoman datan ja ICV:n 405 kanssa käyttämällä XOR-operaatiota. Salattu data (Enciphered data) 406 voidaan tämän jälkeen viedä radiotielle lähettäväksi.

Aloitusvektori IV välitetään myös salatun datan 406 ohella lähetettävässä viestissä. IV:n arvo muutetaan edullisesti jokaiselle lähetettävälle paketille, koska tämä vaikeuttaa salakuuntelijan toimintaa. WEP-algoritmin käyttö datan salaamiseen laajentaa lähetettävää MPDU-yksikköä (MAC Protocol Data Unit) 8 oktetilla: 4 aloitusvektoria IV varten ja 4 oktettia eheyden tarkastusarvoa ICV varten.

Kuviossa 5 on esitetty liityntäpisteen AP ja päätelaitteen MT käsittämiä salausvälineitä DCM (Deciphering means) salatun datan salauksen purkamiseksi toista salausavainta K ja WEP-algoritmia käyttämällä. Kun AP tai MT vastaanottaa radiotien yli lähetetyn salatun viestin MPDU, kuviossa 4 kuvatut operaatiot suoritetaan käänteisenä. Vastaanotetun viestin MPDU aloitusvektorin IV 502 ja salaisen avaimen K 503 yhdiste 504 (K+IV) syötetään WEP-satunnaislukugeneraattoriin WPRNG, jolloin saadaan avainsekvenssi KS 505. Avainsekvenssille KS 505 ja salatulle datalle 501 (Enciphered data) suoritetaan XOR-operaatio. Tästä saadaan alkuperäinen suojaamaton data 506 (Plaintext) ja eheyden tarkastusarvo ICV 507. Suojaamattomalle datalle 506 voidaan suorittaa eheyden tarkistus algoritmilla IA. Saatua tarkastuarvoa ICV' 508 voidaan verrata 509 (ICV'=ICV?) ICV:n. Jos ne eivät ole samoja, vastaanotettu MAC-protokollayksikkö on virheellinen.

Keksintöä voidaan soveltaa myös IP-liikkuvuusprotokollaa (Mobile IP) tukevassa tietoliikennejärjestelmässä. IP-liikkuvuusprotokollaa tukeva tietoliikennejärjestelmä käsittää päätelaitteen IP-liikkuvuutta tukevia liikkuvuusagentteja, eli kotiagentteja HA (Home Agent) ja etäagentteja (Foreign Agent). Kotiagentit tunneloivat päätelaitteelle kohdistuvat paketit päätelaitteen vierailevassa verkossa rekisteröitymään etäagenttiin, joka välittää paketit edelleen päätelaitteelle.

Erään edullisen suoritusmuodon mukaisesti päätelaitteen MT vierailevassa langattomassa lähiverkossa voi olla käytössä yksi tai useampi liikkuvuusagentti. MT kommunikoi liikkuvuusagentin kanssa, joka puolestaan on yhteydessä GAGW:n. Tällöin voidaan suorittaa samoja toimenpiteitä kuten kuvion 2 yhteydessä on havainnollistettu, korvaamalla kuitenkin PAC liikkuvuusagentilla (HA tai FA). MT:n ja liikkuvuusagentin välinen tiedonsiirto hoidetaan laajennuksen (extension) käsittävällä IP-liikkuvuusviesteillä: MT voi pyytää (204) autentikointia verkkotunnisteen NAI käsittävällä rekisteröintipyyntöviestillä (Registration request). GAGW voi toimia kuten kuvion 2 yhteydessä on esitetty. Liikkuvuusagentti vastaa edullisesti autentikointipyyntöön vastaamalla (211) haasteet (RAND) käsittävällä vastausviestillä (Registration Reply). MT puolestaan voi lähettää tarkistusvasteen SIGNsres käsittävän uuden rekisteröintipyyntöviestin liikkuvuusagentille. Myöhemmin MT:lle voidaan vastata autentikaation onnistumisesta vastausviestillä. Jos autentikaatio on onnistunut, laskettu toinen salausavain K voidaan ottaa käyttöön päätelaitteessa MT ja liityntäpisteessä AP.

Edellä kuvattu keksinnöllinen toiminnallisuus voidaan toteuttaa päätelaitteen MT ja verkkoelementtien (AP, PAC, GAGW) käsittämissä prosessoreissa edullisesti ohjelmallisesti. On myös mahdollista käyttää kovo-ratkaisuja, kuten ASIC-piirejä (Application Specific Integrated Circuit) tai erillislogiikkaa.

Alan ammattilaiselle on ilmeistä, että tekniikan kehittyessä keksinnön perusajatus voidaan toteuttaa monin eri tavoin. Keksintö ja sen suoritusmuodot eivät siten rajoitu yllä kuvattuihin esimerkkeihin vaan ne voivat vaihdella patenttivaatimusten puitteissa.

Patenttivaatimukset

1. Menetelmä datan salauksen (ciphering) järjestämiseksi tietoliikennejärjestelmässä, joka käsittää ainakin yhden langattoman päätelaitteen, langattoman lähiverkon ja yleisen matkaviestinverkon, jonka menetelmän mukaisesti

tarjotaan päätelaitteelle tunniste ja tunnisteelle spesifinen salainen avain, joka salainen avain on myös tallennettu matkaviestinverkkoon,

lähetetään päätelaitteelta matkaviestinverkolle päätelaitteen tunniste,

lasketaan matkaviestinverkossa matkaviestinverkon mukainen ainakin yksi ensimmäinen salausavain tunnisteelle spesifisen salaisen avaimen ja ensimmäistä salausavainta varten valitun haasteen avulla,

lähetetään ainakin yksi haaste päätelaitteelle,

lasketaan päätelaitteessa matkaviestinverkon mukainen ainakin yksi ensimmäinen salausavain salaisen avaimen ja ainakin yhden haasteen avulla,

t u n n e t t u siitä, että:

hoidetaan tiedonsiirto matkaviestinverkon ja päätelaitteen välillä langattoman lähiverkon kautta,

lasketaan päätelaitteessa ja matkaviestinverkossa toinen salausavain mainitun ainakin yhden ensimmäisen salausavaimen avulla,

lähetetään mainittu toinen salausavain matkaviestinverkosta langattomaan lähiverkkoon, ja

salataan päätelaitteessa ja langattomassa lähiverkossa päätelaitteen ja verkon välinen data mainittua toista salausavainta käyttäen.

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

lasketaan päätelaitteessa ja matkaviestinverkossa matkaviestinverkon mukainen ainakin yksi autentikaatiovaste ainakin yhden haasteen ja salaisen avaimen perusteella,

lasketaan päätelaitteessa tarkistusvaste ainakin yhden autentikaatiovasteen ja ensimmäisen salausavaimen perusteella,

lähetetään tarkistusvaste matkaviestinverkkoon,

lasketaan matkaviestinverkossa tarkistusvaste ainakin yhden autentikaatiovasteen ja ainakin yhden ensimmäisen salausavaimen perusteella

verrataan päätelaitteen lähettämää tarkistusvastetta matkaviestinverkon laskemaan tarkistusvasteeseen, ja

lähetetään mainittu toinen salausavain matkaviestinverkosta langattomaan lähiverkkoon vasteena sille, että päätelaitteen lähettämä ja matkaviestinverkon laskema tarkistusvaste vastaavat toisiaan.

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

lähetetään päätelaitteesta suojakoodi matkaviestinverkolle,

lasketaan matkaviestinverkossa tarkistussumma suojakoodin ja ainakin yhden ensimmäisen salausavaimen avulla,

lähetetään tarkistussumma päätelaitteelle,

tarkastetaan tarkistussumma päätelaitteessa, ja

lasketaan mainittu toinen salausavain päätelaitteessa vasteena sille, että tarkistussumma on oikea.

4. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

lähetetään mainittu toinen salausavain langattoman lähiverkon liityntäpisteelle, joka tarjoaa päätelaitteelle langattoman yhteyden,

lähetetään liityntäpisteeltä päätelaitteelle pyyntö WEP-algoritmin käytöstä, ja

salataan liityntäpisteessä ja päätelaitteessa lähetettävä data ja puretaan vastaanotetun datan salaus WEP-algoritmin ja mainitun toisen salausavaimen avulla.

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

syötetään mainittu toinen salausavain ja aloitusvektori (Initialization Vector) WEP-satunnaislukugeneraattoriin (WEP Pseudorandom Number Generator), joka tuottaa avainsekvenssin,

salataan lähetettävä data suorittamalla XOR-operaatio salaamattomalla datalle ja avainsekvenssille, ja

puretaan vastaanotetun datan salaus suorittamalla XOR-operaatio salatulle datalle ja avainsekvenssille.

6. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että

päätelaite käsittää GSM-järjestelmän tilaajan tunnistusyksikön SIM,

langaton lähiverkko tukee IEEE802.11-standardia, ja

matkaviestinverkko tukee GSM-standardia.

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

lasketaan mainittu toinen salausavain suorittamalla hash-funktio ainakin osalle seuraavista parametreistä: ainakin yksi ensimmäinen salausavain (Kc), ainakin yksi haaste (RAND), tilaajatunniste (IMSI) ja päätelaitteen laskema suojakoodi (MT_RAND).

8. Tietoliikennejärjestelmä, joka käsittää ainakin yhden langattoman päätelaitteen, langattoman lähiverkon ja yleisen matkaviestinverkon, jossa järjestelmässä

matkaviestinverkko käsittää ensimmäiset laskemisvälineet (AuC) matkaviestinverkon mukaisen ainakin yhden ensimmäisen salausavaimen laskemiseksi päätelaitteen lähettämän tunnisteen mukaisen salaisen avaimen ja ensimmäistä salausavainta varten valitun haasteen avulla,

matkaviestinverkko on järjestetty lähettämään ainakin yhden haasteen päätelaitetta varten,

päätelaite käsittää tunnistusyksikön (SIM) matkaviestinverkon mukaisen ainakin yhden ensimmäisen salausavaimen laskemiseksi tunnistusyksikköön (SIM) tallennetun salaisen avaimen ja ainakin yhden haasteen avulla,

t u n n e t t u siitä, että:

langaton lähiverkko käsittää välineet (PAC, AP) tiedonsiirron hoitamiseksi matkaviestinverkon ja päätelaitteen välillä,

päätelaite ja matkaviestinverkko käsittävät toiset laskemisvälineet (CM, GAGW) toisen salausavaimen laskemiseksi mainitun ainakin yhden ensimmäisen salausavaimen avulla,

matkaviestinverkko käsittää välineet (GAGW) mainitun toisen salausavaimen lähettämiseksi langattomaan lähiverkkoon, ja

päätelaite ja langaton lähiverkko käsittävät salausvälineet (ECM, DCM) päätelaitteen ja langattoman lähiverkon välisen datan salaamiseksi (en/deciphering) mainittua toista salausavainta käyttäen.

9. Patenttivaatimuksen 8 mukainen tietoliikennejärjestelmä, t u n n e t t u siitä, että

päätelaitteen tunnistusyksikkö (SIM) ja matkaviestinverkon ensimmäiset laskemisvälineet (AuC) on järjestetty laskemaan matkaviestinverkon mukainen ainakin yksi autentikaatiovaste haasteen ja salaisen avaimen perusteella,

päätelaitteen toiset laskemisvälineet (CM) on järjestetty laskemaan tarkistusvaste ainakin yhden autentikaatiovasteen ja ainakin yhden ensimmäisen salausavaimen perusteella,

päätelaite käsittää välineet (CM, TxRx) tarkistusvasteen lähettämiseksi matkaviestinverkkoon,

matkaviestinverkon toiset laskemisvälineet (GAGW) on järjestetty laskemaan tarkistusvaste ainakin yhden autentikaatiovasteen ja ensimmäisen salausavaimen perusteella

matkaviestinverkon toiset laskemisvälineet (GAGW) on järjestetty vertaamaan päätelaitteen lähettämää tarkistusvastetta laskemaansa tarkistusvasteeseen, ja

matkaviestinverkon toiset laskemisvälineet (GAGW) on järjestetty lähettämään mainittu toinen salausavain matkaviestinverkosta langattomaan lähiverkkoon vasteena sille, että päätelaitteen lähettämä ja matkaviestinverkossa laskettu tarkistusvaste vastaavat toisiaan.

10. Patenttivaatimuksen 8 tai 9 mukainen tietoliikennejärjestelmä, t u n n e t t u siitä, että

langaton lähiverkko ja päätelaite tukevat IEEE802.11-standardia,

matkaviestinverkko tukee GSM-standardia, ja

salausvälineet (ECM, DCM) on järjestetty salaamaan data käyttämällä WEP-algoritmia.

11. Langaton päätelaite, joka käsittää lähetinvastaanottimen (TxRx) langattoman yhteyden muodostamiseksi langattoman lähiverkon liityntäpisteeseen ja tunnistusyksikön (SIM) matkaviestinverkon mukaisen ainakin yhden ensimmäisen salausavaimen laskemiseksi tunnistusyksikköön (SIM) tallennetun salaisen avaimen ja matkaviestinverkon lähettämän ainakin yhden haasteen avulla, t u n n e t t u siitä, että:

päätelaite käsittää toiset laskemisvälineet (CM) toisen salausavaimen laskemiseksi mainitun ainakin yhden ensimmäisen salausavaimen avulla, ja

päätelaite käsittää salausvälineet (ECM, DCM) päätelaitteen ja liityntäpisteen välisen datan salaamiseksi (en/deciphering) mainittua toista salausavainta käyttäen.

12. Patenttivaatimuksen 11 mukainen langaton päätelaite, t u n n e t t u siitä, että

päätelaitteen tunnistusyksikkö (SIM) on järjestetty laskemaan matkaviestinverkon mukainen ainakin yksi autentikaatiovaste haasteen ja salaisen avaimen perusteella,

päätelaitteen toiset laskemisvälineet (CM) on järjestetty laskemaan tarkistusvaste ainakin yhden autentikaatiovasteen ja mainitun ainakin yhden ensimmäisen salausavaimen perusteella, ja

päätelaite käsittää välineet (CM, TxRx) tarkistusvasteen lähettämiseksi matkaviestinverkkoon.

13. Patenttivaatimuksen 11 tai 12 mukainen langaton päätelaite, t u n n e t t u siitä, että

päätelaite tukee IEEE 802.11-standardia ja salausvälineet (ECM, DCM) on järjestetty salaamaan data käyttämällä WEP-algoritmia.

14. Langattoman lähiverkon liityntäpiste, joka käsittää salausvälineet (ECM, DCM) päätelaitteen ja liityntäpisteen välisen datan salaamiseksi (en/deciphering), t u n n e t t u siitä, että

salausvälineet (ECM, DCM) on järjestetty salaamaan lähetettävä data ja purkamaan vastaanotetun datan salaus yleisen matkaviestinverkon laskemaa päätelaitekohtaista toista salausavainta käyttäen, joka mainittu toinen salausavain on laskettu päätelaitteelle spesifisen salaisen avaimen avulla lasketun ainakin yhden ensimmäisen salausavaimen avulla.

15. Patenttivaatimuksen 14 mukainen liityntäpiste, t u n n e t t u siitä, että

liityntäpiste tukee IEEE 802.11-standardia ja salausvälineet (ECM, DCM) on järjestetty salaamaan lähetettävä data ja purkamaan vastaanotetun datan salaus käyttämällä WEP-algoritmia.

Patentkrav

1. Förfarande för att arrangera chiffrering av data (ciphering) i ett telekommunikationssystem, som omfattar åtminstone en trådlös terminalanordning, ett trådlöst lokalnät och ett allmänt mobilnät, enligt vilket förfarande

terminalanordningen erbjuds en identifierare och en specifik hemlig nyckel för identifieraren, vilken hemlig nyckel även är lagrad i mobilnätet,

terminalanordningens identifierare sänds från terminalanordningen till mobilnätet,

i mobilnätet beräknas åtminstone en första chiffreringsnyckel enligt mobilnätet med hjälp av den för identifieraren specifika hemliga nyckeln och ett anrop som valts för den första chiffreringsnyckeln,

åtminstone ett anrop sänds till terminalanordningen,

i terminalanordningen beräknas åtminstone en första chiffreringsnyckel enligt mobilnätet med hjälp av den hemliga nyckeln och åtminstone ett anrop,

k ä n n e t e c k n a t av att:

dataöverföring mellan mobilnätet och terminalanordningen utförs via det trådlösa lokalnätet,

i terminalanordningen och mobilnätet beräknas en andra chiffreringsnyckel med hjälp av nämnda åtminstone en första chiffreringsnyckel,

nämnda andra chiffreringsnyckel sänds från mobilnätet till det trådlösa lokalnätet och

data mellan terminalanordningen och nätet chiffreras i terminalanordningen och det trådlösa lokalnätet genom att använda nämnda andra chiffreringsnyckel.

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

åtminstone ett autenticeringssvar enligt mobilnätet beräknas i terminalanordningen och mobilnätet på basis av åtminstone ett anrop och den hemliga nyckeln,

ett kontrollsvar beräknas i terminalanordningen på basis av åtminstone ett autenticeringssvar och den första chiffreringsnyckeln,

kontrollsvaret sänds till mobilnätet,

ett kontrollsvar beräknas i mobilnätet på basis av åtminstone ett autenticeringssvar och åtminstone en första chiffreringsnyckeln,

kontrollsvaret som terminalanordningen sänt jämförs med kontroll-

svaret som mobilnätet beräknat, och

nämnda andra chiffreringsnyckel sänds från mobilnätet till det trådlösa lokalnätet i gensvar på att kontrollsvaret som terminalanordningen sänt motsvaras av kontrollsvaret som mobilnätet beräknat.

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

en säkerhetskod sänds från terminalanordningen till mobilnätet,

en kontrollsumma beräknas i mobilnätet med hjälp av säkerhetskoden och åtminstone en första chiffreringsnyckel,

kontrollsumman sänds till terminalanordningen,

kontrollsumman kontrolleras i terminalanordningen och

nämnda andra chiffreringsnyckel beräknas i terminalanordningen i gensvar på att kontrollsumman är korrekt.

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

nämnda andra chiffreringsnyckel sänds till en anslutningspunkt i det trådlösa lokalnätet, vilken anslutningspunkt erbjuder en trådlös förbindelse för terminalanordningen,

en begäran sänds från anslutningspunkten till terminalanordningen om användning av en WEP-algoritm och

data som skall sändas chiffreras i anslutningspunkten och terminalanordningen och mottagen chiffrerad data dechiffreras med hjälp av WEP-algoritmen och nämnda andra chiffreringsnyckel.

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

nämnda andra chiffreringsnyckel och en initieringsvektor (Initialization Vector) matas i en WEP-slumptalsgenerator (WEP Pseudorandom Numer Generator) som genererar en nyckelsekvens,

data som skall sändas chiffreras genom att utföra en XOR-operation för ochiffrerad data och nyckelsekvensen och

mottagen chiffrerad data dechiffreras genom att utföra XOR-operationen för chiffrerad data och nyckelsekvensen.

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

terminalanordningen omfattar en abonnentidentifierarenhet SIM för GSM-systemet,

det trådlösa lokalnätet stöder IEEE802.11-standard och

mobilnätet stöder GSM-standard.

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

nämnda andra chiffreringsnyckel beräknas genom att utföra en hash-funktion för åtminstone en del av följande parametrar: åtminstone en första chiffreringsnyckel (Kc), åtminstone ett anrop (RAND), en abonnentidentifierare (IMSI) och den av terminalanordningen beräknade säkerhetskoden (MT_RAND).

8. Telekommunikationssystem, som omfattar åtminstone en trådlös terminalanordning, ett trådlöst lokalnät och ett allmänt mobilnät, i vilket förfarande

mobilnätet omfattar första beräkningsmedel (AuC) för beräkning av åtminstone en första chiffreringsnyckel enligt mobilnätet med hjälp av hemlig nyckel enligt en identifierare som terminalanordningen sänt och ett anrop som valts för den första chiffreringsnyckeln,

mobilnätet är anordnat att sända åtminstone ett anrop för terminalanordningen,

terminalanordningen omfattar en identifierarenhet (SIM) för beräkning av åtminstone en första chiffreringsnyckel enligt mobilnätet med hjälp av den i identifierarenheten (SIM) lagrade hemliga nyckeln och åtminstone ett anrop,

k ä n n e t e c k n a t av att:

det trådlösa lokalnätet omfattar medel (PAC, AP) för att utföra dataöverföring mellan mobilnätet och terminalanordningen,

terminalanordningen och mobilnätet omfattar andra beräkningsmedel (CM, GAGW) för beräkning av en andra chiffreringsnyckel med hjälp av nämnda åtminstone en första chiffreringsnyckel,

mobilnätet omfattar medel (GAGW) för att sända nämnda andra chiffreringsnyckel till det trådlösa lokalnätet och

terminalanordningen och det trådlösa lokalnätet omfattar chiffreringsmedel (ECM, DCM) för chiffrering (enciphering/deciphering) av data mellan terminalanordningen och det trådlösa lokalnätet genom att använda nämnda andra chiffreringsnyckel.

9. Telekommunikationssystem enligt patentkrav 8, k ä n n e t e c k n a t av att

terminalanordningens identifierarenhet (SIM) och mobilnätets första beräkningsmedel (AuC) är anordnade att beräkna åtminstone ett autentice-

ringssvar enligt mobilnätet på basis av anropet och den hemliga nyckeln,

de andra beräkningsmedlen (CM) i terminalanordningen är anordnade att beräkna ett kontrollsvar på basis av åtminstone ett auteniceringssvar och åtminstone en första chiffreringsnyckel,

terminalanordningen omfattar medel (CM, TxRx) för sändning av kontrollsvaret till mobilnätet,

de andra beräkningsmedlen (GAGW) i mobilnätet är anordnade att beräkna ett kontrollsvar på basis av åtminstone ett autenticeringssvar och den första chiffreringsnyckeln,

de andra beräkningsmedlen (GAGW) i mobilnätet är anordnade att jämföra kontrollsvaret som terminalanordningen sänt med kontrollsvaret som de beräknat, och

de andra beräkningsmedlen (GAGW) i mobilnätet är anordnade att sända nämnda andra chiffreringsnyckel från mobilnätet till det trådlösa lokalnätet i gensvar på att kontrollsvaret som terminalanordningen sänt motsvaras av kontrollsvaret som beräknats i mobilnätet.

10. Telekommunikationssystem enligt patentkrav 8 eller 9, k ä n n e t e c k n a t av att

det trådlösa lokalnätet och terminalanordningen stöder IEEE802.11-standard och

mobilnätet stöder GSM-standard och

chiffreringsmedlen (ECM, DCM) är anordnade att chiffrera data genom att använda en WEP-algoritm.

11. Trådlös terminalanordning, som omfattar en sändtagare (TxRx) för etablering av en trådlös förbindelse med en anslutningspunkt i ett trådlöst lokalnät och en identifierarenhet (SIM) för beräkning av åtminstone en första chiffreringsnyckel enligt mobilnätet med hjälp av en i identifierarenheten (SIM) lagrad hemlig nyckel och åtminstone ett anrop som mobilnätet sänt, k ä n n e t e c k n a d av att:

terminalanordningen omfattar andra beräkningsmedel (CM) för beräkning av en andra chiffreringsnyckel med hjälp av nämnda åtminstone en första chiffreringsnyckel, och

terminalanordningen omfattar chiffreringsmedel (ECM, DCM) för chiffrering (enciphering/deciphering) av data mellan terminalanordningen och anslutningspunkten genom att använda nämnda andra chiffreringsnyckel.

12. Trådlös terminalanordning enligt patentkrav 11, k ä n n e -

tecknad av att

terminalanordningens identifierarenhet (SIM) är anordnad att beräkna åtminstone ett auteniceringssvar enligt mobilnätet på basis av ett anrop och den hemliga nyckeln,

de andra beräkningsmedlen (CM) i terminalanordningen är anordnade att beräkna ett kontrollsvar på basis av åtminstone ett auteniceringssvar och nämnda åtminstone en första chiffreringsnyckel och

terminalanordningen omfattar medel (CM, TxRx) för sändning av kontrollsvaret till mobilnätet.

13. Trådlös terminalanordning enligt patentkrav 11 eller 12, kännetecknad av att

terminalanordningen stöder IEEE 802.11-standard och chiffreringsmedlen (ECM, DCM) är anordnade att chiffrera data genom att använda en WEP-algoritm.

14. Anslutningspunkt i ett trådlöst lokalnät, vilken anslutningspunkt omfattar chiffreringsmedel (ECM, DCM) för chiffrering av data mellan en terminalanordning och anslutningspunkten, kännetecknad av att

chiffreringsmedlen (ECM, DCM) är anordnade att chiffrera data som skall sändas och dechiffrera mottagen chiffrerad data genom att använda en terminalspecifik andra chiffreringsnyckel som ett allmänt mobilnät beräknat, vilken andra chiffreringsnyckel beräknats med hjälp av åtminstone en första chiffreringsnyckel som beräknats med hjälp av en för terminalanordningen specifik hemlig nyckel.

15. Anslutningspunkt enligt patentkrav 14, kännetecknad av att

anslutningspunkten stöder IEEE 802.11-standard och chiffreringsmedlen (ECM, DCM) är anordnade att chiffrera data som skall sändas och dechiffrera mottagen chiffrerad data genom att använda en WEP-algoritm.

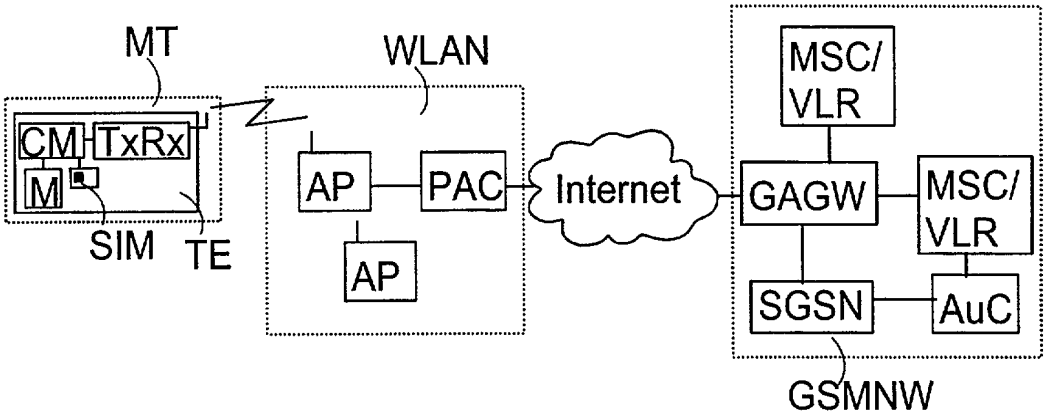

MT
WLAN
MSC/
VLR
CM
TxRx
M
AP
PAC
Internet
GAGW
MSC/
VLR
SIM
TE
AP
SGSN
AuC
GSMNW

Fig. 1

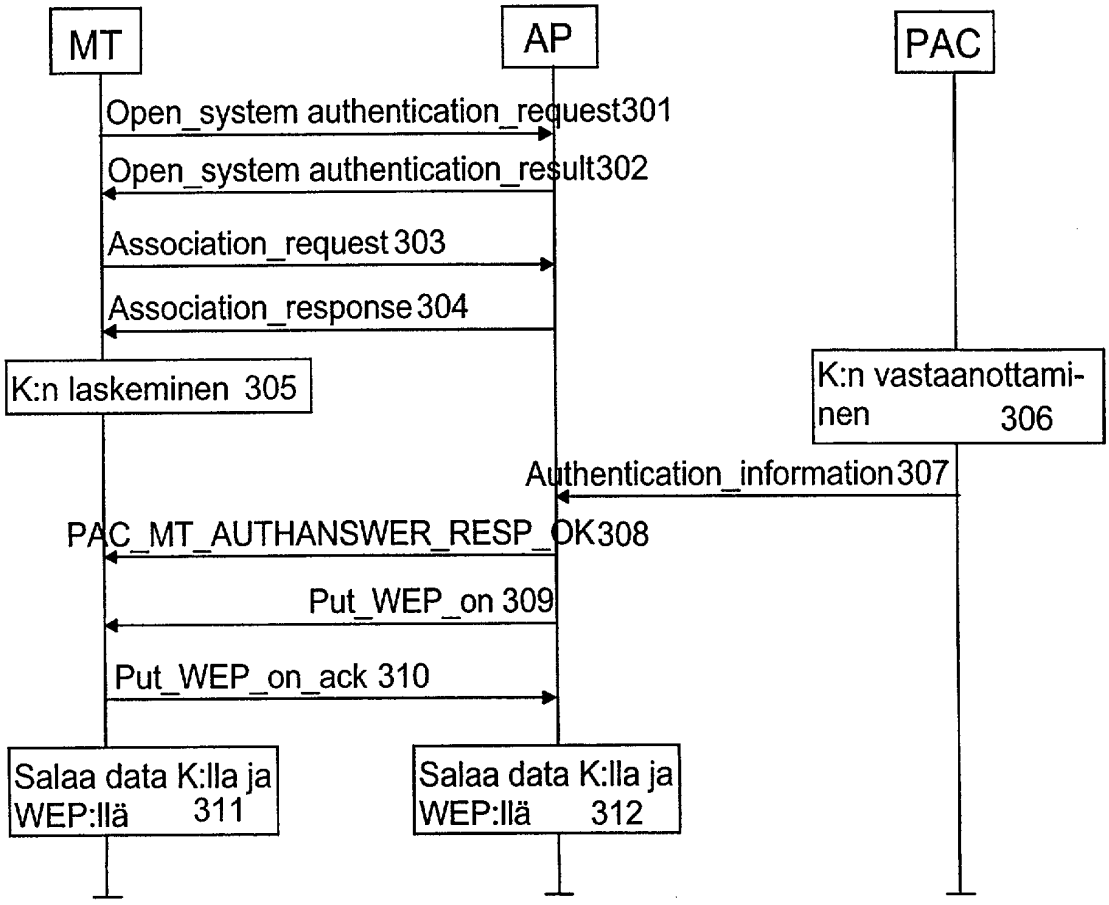

MT
AP
PAC
Open_system authentication_request 301
Open_system authentication_result 302
Association_request 303
Association_response 304
K:n laskeminen 305
K:n vastaanottami-
nen 306
Authentication_information 307
PAC_MT_AUTHANSWER_RESP_OK 308
Put_WEP_on 309
Put_WEP_on_ack 310
Salaa data K:lla ja
WEP:llä 311
Salaa data K:lla ja
WEP:llä 312

Fig. 3

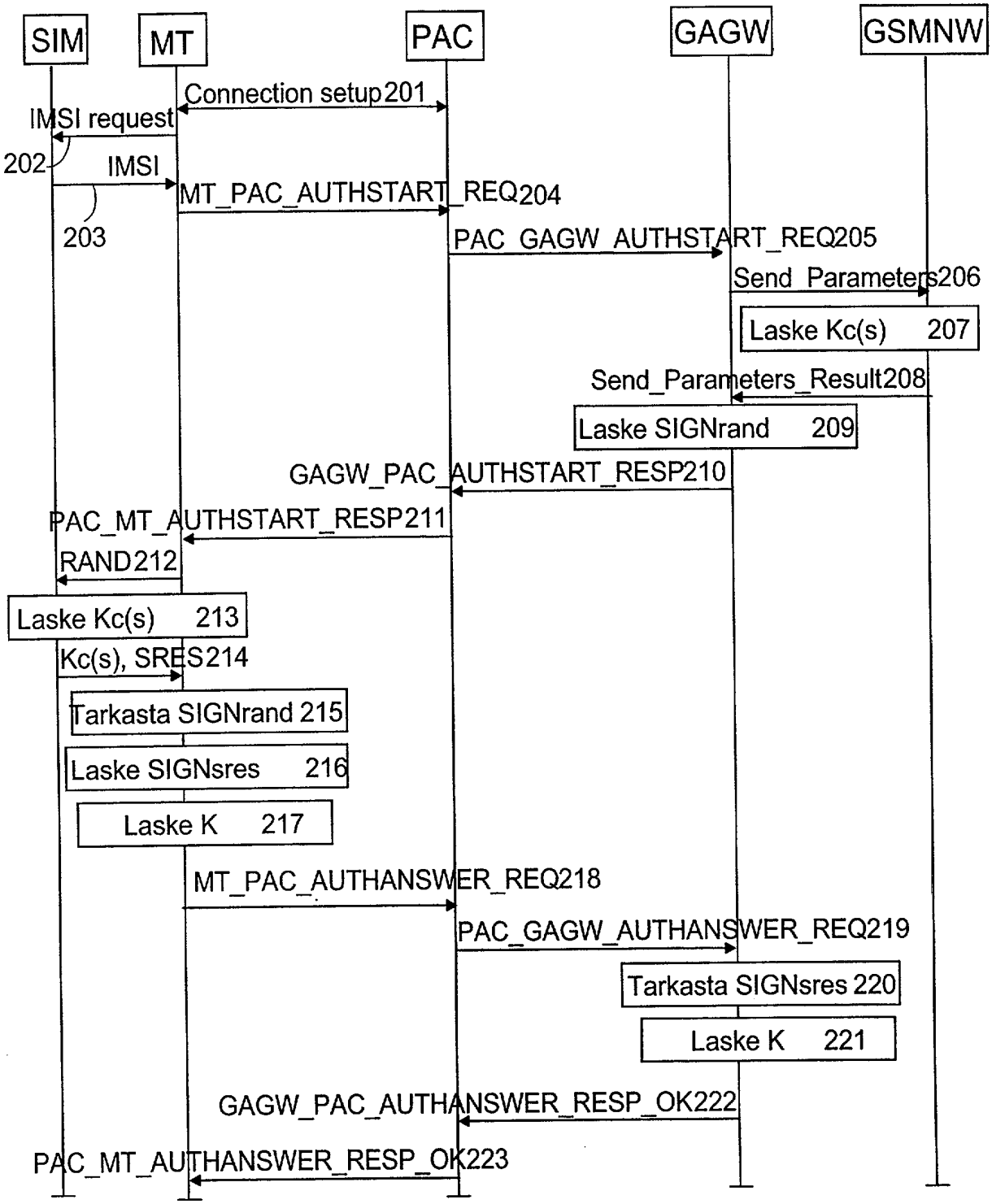

SIM
MT
PAC
GAGW
GSMNW
Connection setup 201
IMSI request
202
IMSI
MT_PAC_AUTHSTART_REQ 204
203
PAC_GAGW_AUTHSTART_REQ 205
Send_Parameters 206
Laske Kc(s) 207
Send_Parameters_Result 208
Laske SIGNrand 209
GAGW_PAC_AUTHSTART_RESP 210
PAC_MT_AUTHSTART_RESP 211
RAND 212
Laske Kc(s) 213
Kc(s), SRES 214
Tarkasta SIGNrand 215
Laske SIGNsres 216
Laske K 217
MT_PAC_AUTHANSWER_REQ 218
PAC_GAGW_AUTHANSWER_REQ 219
Tarkasta SIGNsres 220
Laske K 221
GAGW_PAC_AUTHANSWER_RESP_OK 222
PAC_MT_AUTHANSWER_RESP_OK 223

Fig. 2

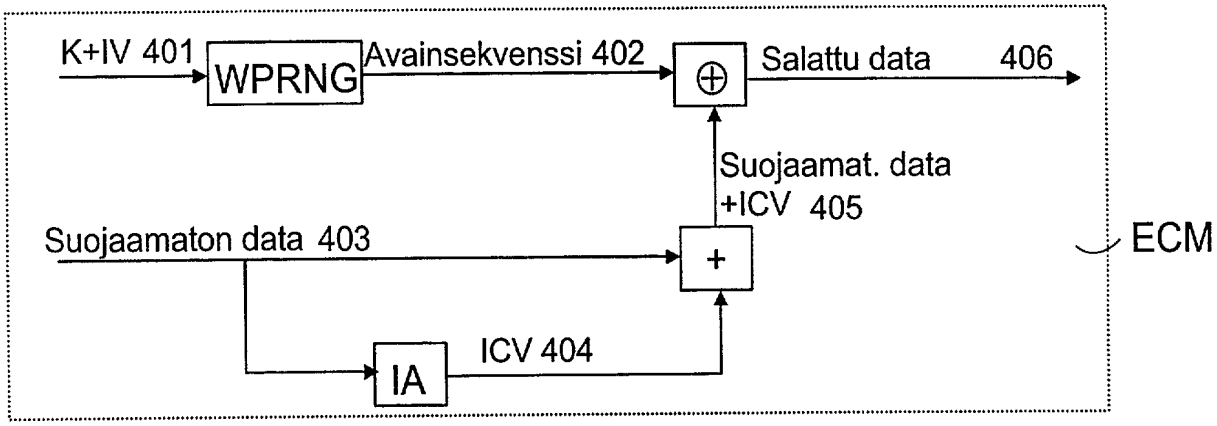

K+IV 401
WPRNG
Avainsekvenssi 402
Salattu data
406
Suojaamat. data
+ICV 405
Suojaamaton data 403
ECM
IA
ICV 404

Fig. 4

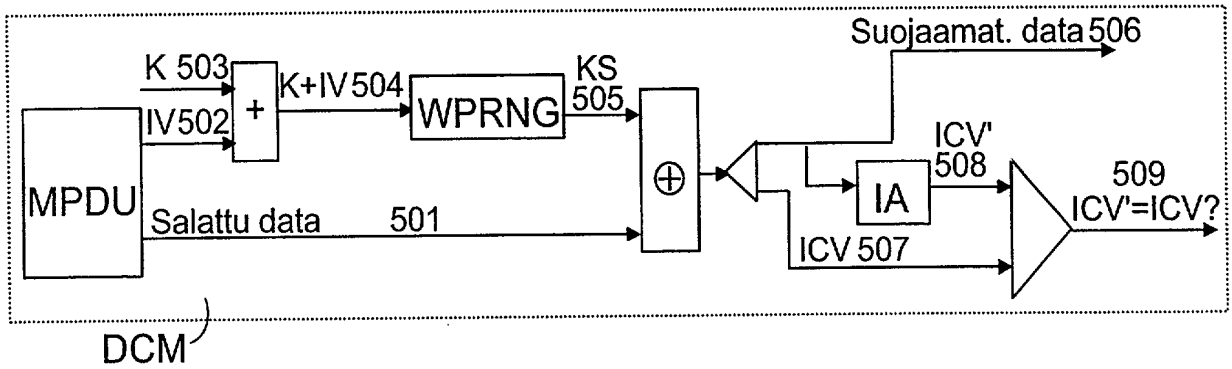

Suojaamat. data 506
K 503
IV502
K+IV504
WPRNG
KS
505
MPDU
Salattu data
501
ICV'
508
IA
509
ICV'=ICV?
ICV 507
DCM

Fig. 5