FI0001046668

(12) **PATENTTIJULKAISU**
PATENTSKRIFT

(10) **FI 104666 B**

(45) Patentti myönnetty - Patent beviljats **15.03.2000**

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

(21) Patenttihakemus - Patentansökning **974186**

(22) Hakemispäivä - Ansökningsdag **10.11.1997**

(24) Alkupäiva - Löpdag **10.11.1997**

(41) Tullut julkiseksi - Blivit offentlig **11.05.1999**

SUOMI – FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN

(73) Haltija - Innehavare

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

(72) Keksijä - Uppfinnare

1 •Immonen, Olli, Tuohuskuja 16 A 5, 00670 Helsinki, SUOMI - FINLAND, (FI)

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

(54) Keksinnön nimitys - Uppfinningens benämning

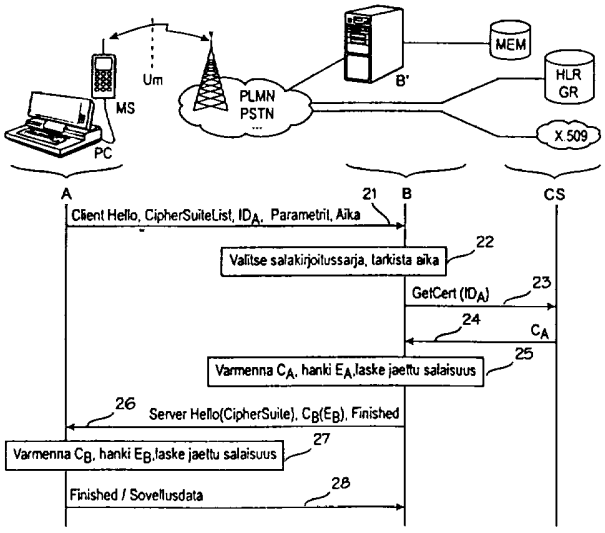
Varma kättelyprotokolla
Säkert handskakningsprotokoll

(56) Viitejulkaisut - Anförda publikationer

EP A 0532231 (H 04L 9/32, American Telephone and Telegraph Company, p. 8, r. 38 - p. 9, r. 55)
US A 5371794 (H 04L 9/00, Sun Microsystems Inc., p. 6, r. 67 - p. 9, r. 16)

(57) Tiivistelmä - Sammandrag

Menetelmä varmaa kättelyprotokollaa varten hitaan kanavan (Um) kautta A:n ja B:n välillä. A lähettää ensimmäisen sanoman (21), joka osoittaa salakirjoitussarjojen joukon parametreineen sekä tunnisteensa (ID_A). B valitsee salakirjoitussarjan, saa A:n sertifikaatin (C_A) nopean yhteyden kautta, varmentaa A:n sertifikaatin (C_A) ja saa A:n julkisen avaimen (E_A). Seuraavaksi B lähettää toisen sanoman (26), joka käsittää B:n sertifikaatin (C_B), osoituksen siitä, että B on varmentanut A:n sertifikaatin (C_A), ja osoituksen valitusta salakirjoitussarjasta. A alkaa käyttää valittua salakirjoitussarjaa; varmentaa B:n sertifikaatin (C_B) ja saa B:n julkisen avaimen (E_B). Seuraavaksi A lähettää kolmannen sanoman (28), joka osoittaa että A on varmentanut B:n sertifikaatin (C_B). Sovellusdataa voidaan lähettää A:lta B:lle kolmannessa sanomassa (28), jolloin saavutetaan kaksisuuntainen avaintenvaihto ja keskinäinen varmennus kahden A:n ja B:n välisen sanoman (21, 26) suuruisella tehollisella lisäkuormalla.



Förfarande för ett säkert handskakningsprotokoll mellan A och B förenade med en långsam kanal (Um). A sänder ett första meddelande (21) vilket anger en uppsättning av chifferserier med parametrar, och dess identifierare (ID_A). B väljer en chifferserie, erhåller A:s certifikat (C_A) genom en snabb förbindelse, bekräftar A:s certifikat (C_A) och erhåller A:s allmänna nyckel (E_A). Därefter sänder B ett andra meddelande (26) vilket omfattar B:s certifikat (C_B), en indikation om att B har bekräftat A:s certifikat (C_A), och en indikation om den valda chifferserien. A börjar använda den valda chifferserien, bekräftar B:s certifikat (C_B) och erhåller B:s allmänna nyckel (E_B). Sedan sänder A ett tredje meddelande (28) vilket anger att A har bekräftat B:s certifikat (C_B). Tillämpningsdata kan sändas från A till B i det tredje meddelandet (28) varvid ett dubbelriktat nyckelutbyte och en inbördes bekräftelse utförs med en effektiv extra last av två meddelanden (21, 26) mellan A och B.

Varma kättelyprotokolla

Keksinnön tausta

Keksinnön kohteena on yleisesti varma kättelyprotokolla tietoliikenneverkkoja varten. Täsmällisemmin sanottuja keksintö liittyy menetelmään ja laitteistoon varman kättelyn tuottamiseksi puhelun osapuolten välillä siten, että varsinaista datasiirtoa edeltävä lisäkuorma on minimaalinen.

Tämän hakemuksen puitteissa "TLS" tarkoittaa "Transport Layer Security". Eräs tällainen protokolla kuvataan julkaisussa *"The TLS Protocol"*, toukokuu 21, 1997, kirjoittajina Tim Dierks ja Christopher Allen, Consensus Development. Tämä dokumentti on julkaistu nimellä "draft-ietf-tls-protocol-03.txt", ja se sisältyy tähän hakemukseen viittauksena. Täsmällisemmin sanottuja keksintö ehdottaa parannettua kättelyprotokollaa, joka on sovellettavissa mm. TLS:n kaltaisissa protokollissa.

TLS-tyyppinen protokolla käsittää useita kerroksia, kuten:

Ylemmän tason protokollat

Kättelyprotokolla/hälytysprotokolla (alert ~)/sovellusprotokolla

Tietueprotokolla

Kuljetusprotokolla

Alemman tason protokollat

Kuvio 1 perustuu mainitun TLS ehdotusprotokollan lukuun 7.3, ja se esittää tunnettua kättelymenetelmää. Selostuksen pitämiseksi yhdenmukaisena mainitun ehdotuksen kanssa osapuolia A ja B kutsutaan myös vastaavasti nimillä "asiakas" ja "palvelin". (Sellaisia termejä kuten "hello" (tervehdys) ja "finished" (loppu) käytetään myös yhdenmukaisesti mainitun TLS-ehdotuksen kanssa. Vaiheessa 11 asiakas A lähettää client hello -sanoman. Tämä client hello -sanoma käsittää listan asiakkaan tukemista salakirjoitussarjoista (cipher suite) ja pakkaus- eli kompressiomenetelmistä. Vaiheessa 12 palvelin B valitsee salakirjoitussarjan ja pakkausmenetelmän. (B voi valinnaisesti myös tarkistaa aikaleiman varmistaakseen, että sanoma ei ole vanha, uudelleenlähetettävä sanoma.)

Vaiheessa 13 palvelin B vastaa server hello -sanomalla. Sanomat client hello 11 ja server hello 13 perustavat turvallisuuden osapuolten välille, tyypillisesti perustamalla seuraavat attribuutit: protokollaversio, istunnon tunniste, salakirjoitussarja ja pakkausmenetelmä. Server hello -sanoman yhteydessä palvelin B lähettää oman sertifikaattinsa C_B asiakkaalle ja pyytää asiakasta A lähettämään asiakassertifikaattinsa C_A palvelimelle B. Vasteena tälle,

vaiheessa 14 asiakas A varmentaa B:n sertifikaatin ja saa B:n julkisen avaimen E_B. Vaiheessa 15 asiakas A lähettää B:lle finished -sanoman, joka osoittaa että A on kyennyt varmentamaan B:n identiteetin. Lisäksi A lähettää oman sertifikaattinsa C_A B:lle. Vaiheessa 16 B käyttää C_A:ta saadakseen A:n julkisen avaimen E_A. Vaiheessa 17 B lähettää oman finished -sanomansa asiakkaalle A. Vastapuolensa identiteetin varmennuksen yhteydessä kumpikin osapuoli laskee itsenäisesti jaetun salaisen avaimen tätä istuntoa varten. Nyt molemmat osapuolet ovat vaihtaneet avaimia, sopineet salakirjoitussarjasta/pakkausmenetelmästä ja varmentaneet toisen osapuolen identiteetin. Vaiheessa 18 asiakas A voi aloittaa sovellusdatan lähettämisen.

Sertifikaatit C_A ja C_B ovat yllä selostetun protokollan olennainen osa. Osapuolten keskenään luottaman auktoriteetin allekirjoittamilla sertifikaateilla kumpikin osapuoli voi varmentaa vastapuolensa identiteetin. Sertifikaatti käsittää ainakin omistajansa identiteetin (A/B) ja julkisen avaimen tai avaimet (E_A/E_B), voimassaoloajan, sertifikaatin myöntäjän ja tämän digitaalisen allekirjoituksen. Se voi myös käsittää sen omistajalle myönnetyt oikeudet. Sopiva digitaalisten allekirjoitusten mekanismi on käänteinen julkisen avaimen salakirjoitus: myöntäjä allekirjoittaa sertifikaatin yksityisellä avaimellaan ja kuka tahansa haluaakin varmentaa sertifikaatin, tekee sen käyttämällä myöntäjän julkista avainta. Sertifikaatin sopiva rakenne määritellään ISO-standardissa X.509.

Ongelmana tässä tunnetussa kättelyprotokollassa on sen vaatima suuri lisäkuorma. Kuten kuviosta 1 nähdään, varsinainen datasiirto alkaa vasta vaiheessa 18, eli sen jälkeen kun osapuolten välillä on lähetetty neljä sanomaa. Langattomassa monipääsyjärjestelmässä, missä osapuolia erottaa ilmarajapinta Um ja yleinen matkapuhelinverkko PLMN, todellinen sanomanvälitys on paljon monimutkaisempaa kuin kuviossa 1 näytetään. Tämä johtuu siitä, että kuviossa 1 näytetään vain todelliset sanomat ja (selvyyden vuoksi) siitä on jätetty pois resurssien varaus- ja vapautusvaiheet, jotka ovat alan ammattilaiselle rutiinia, mutta silti elintärkeitä.

Keksinnön lyhyt selostus

Yllä olevan selostuksen perusteella keksinnön tavoitteena on siten kehittää menetelmä ja sopivat verkkoelementit (solmut ja päätelaitteet) sellaisen kättelyprotokollan tuottamiseksi, jolla on pieni lisäkuormitus, eli vähäinen sanomien määrä ilmarajapinnan yli. Tämä tavoite saavutetaan menetelmällä ja verkkoelementeillä, joille on tunnusomaista se, mitä sanotaan itsenäisissä

patenttivaatimuksissa. Keksinnön edulliset suoritusmuodot ovat epäitsenäisten patenttivaatimusten kohteena.

Keksintö perustuu uudentyyppiseen toimintojen jakamiseen osapuolten A ja B välillä. Lisäksi joitakin ilmarajapinnan ylittäviä sanomia voidaan eliminoida käyttämällä maaperustaista sertifikaattivarastoa tai -palvelua ja toteuttamalla kysely tähän varastoon. Lisäksi keksintö perustuu näkemykseen, että varsinaisen kättelyn viimeinen sanoma tulisi lähettää A:lta B:lle, jolloin varsinainen datan lähetys voidaan ketjuttaa viimeisen kättelysanoman yhteyteen, jolloin nettolisäkuormitus minimoituu.

Keksintö soveltuu tietoliikennejärjestelmiin, joilla on osapuolten välillä pullonkaulana toimiva hidas ja/tai epäluotettava lähetyskanava.

Kuvioiden lyhyt selostus

Keksintöä selostetaan seuraavassa edullisten suoritusmuotojen yhteydessä, viitaten oheisiin piirroksiin, joista:

Kuvio 1 esittää signalointikaaviota, joka esittää tunnettua kättelyprotokollaa; ja

Kuvio 2 on yhdistelmä, jossa alaosa on lomitettu signalointikaavio/vuokaavio, joka esittää keksinnön erästä suoritusmuotoa ja yläosa on lohkokaavio, joka esittää kuinka keksinnön mukainen toiminnallisuus voidaan sijoittaa eri verkkoelementteihin.

Keksinnön yksityiskohtainen selostus

Viitaten nyt kuvioon 2 selostetaan keksinnön eräs suoritusmuoto. Kuvion 2 alaosa on lomitettu signalointikaavio/vuokaavio, joka esittää keksinnön erästä suoritusmuotoa. Kuvion 2 yläosa on siihen liittyvä lohkokaavio, joka esittää erästä mahdollista kartoitusta puhelun osapuolten ja fyysisten verkkoelementtien kesken.

Vaiheessa 21 asiakas A lähettää ensimmäisen osapuolten välisen sanoman, joka käsittää kaikki vaiheen 11 sanoman elementit. (Osapuolten välinen sanoma on sanoma A:lta B:lle tai päinvastoin.) Lisäksi vaiheen 21 sanoma käsittää myös asiakkaan A tunnisteen ID_A ja salakirjoitusparametreja (kuten satunnaislukuja ja/tai alustusvektoreita), mikäli jokin osoitettu salakirjoitussarja tätä vaatii. Tunnistetta ID_A tarkastellaan myöhemmin lähemmin. Vasteena client hello -sanomalle vaiheessa 22 palvelin B valitsee salakirjoitussarjan. Edullisesti se myös tarkistaa A:n lähettämän sanoman aikaleiman. Vaiheessa 23, sen sijaan että palvelin B pyytäisi A:n sertifikaattia C_A A:lta itsel-

tään, palvelin B käyttää A:n lähettämää tunnistetta ID_A noutaakseen A:n sertifikaatin C_A sertifikaattivarastosta CS (certificate store). B:n ja CS:n välisen yhteyden tulisi olla huomattavasti nopeampi kuin ilmarajapinnan Um. Vaiheessa 24 luotettu osapuoli CS palauttaa A:n sertifikaatin C_A. Vaihtoehtoisesti tai tämän lisäksi B voi myös ylläpitää sertifikaattien paikallista muistia MEM ja ohittaa kyselyn CS:ään, jos A:n sertifikaatti löytyy paikallisesta muistista. Vaiheessa 25 B varmentaa C_A:n, saa A:n julkisen avaimen E_A ja laskee jaetun salaisen avaimen. Vaiheessa 26 B lähettää A:lle toisen osapuolten välisen sanoman. Toinen osapuolten välinen sanoma käsittää B:n sertifikaatin C_B. Se myös osoittaa, että B on kyennyt varmentamaan A:n sertifikaatin. (Tämä osoitus voi kuitenkin olla implisiittinen, mikä tarkoittaa että B lähettää sertifikaattinsa vain mikäli se on varmentanut A:n sertifikaatin.) vaiheessa 27 A varmentaa B:n sertifikaatin C_B, saa B:n julkisen avaimen E_B ja laskee jaetun salaisen avaimen. Vaiheessa 28 A lähettää B:lle kolmannen osapuolten välisen sanoman, joka käsittää finished -sanoman, joka osoittaa että se on kyennyt varmentamaan B:n sertifikaatin.

Selvyyden vuoksi kuviossa 2 näytetään vain mitä tapahtuu, kun kättely onnistuu, eli molemmat osapuolet toimivat protokollan mukaisesti. Jos protokollasta poikkeamista havaitaan, tämä on yleensä kohtalokas virhe, ja kättely päättyy.

On syytä huomata, että viimeinen osapuolten välinen sanoma (joka käsittää finished -sanoman vaiheessa 28) osoittaa A:sta B:hen. Tämä poikkeaa selkeästi kuviossa 1 näytetystä tunnetusta protokollasta. Keksinnön tämän ominaisuuden etu on, että vaiheessa 28 sovellusdataa voidaan ketjuttaa kolmannen osapuolten välisen sanoman kanssa. Keksinnön mukaisen kättelyprotokollan tehollinen lisäkuormitus on siis vain kaksi osapuolten välistä sanomaa, verrattuna tunnetun kättelyn neljän sanoman lisäkuormaan. Tämän saavuttamiseksi on käytettävä soveltuvaa avaintenvaihtomekanismia. Sopiviin avaintenvaihtoalgoritmeihin kuuluu Diffie-Hellman (DH) kiinteillä parametreilla ja varmennettuna digitaalisella allekirjoitusalgoritmilla (Digital Signature Algorithm, DSA). DH-algoritmi löytyy useimmista salakirjoituksen oppikirjoista. Lisäksi alkuperäinen Diffie-Hellman -algoritmi kuvataan US-patentissa 4 200 770 ja Digital Signature Algorithm on yhdysvaltalainen standardi ja tosiasiallinen kansainvälinen standardi. Toinen hyvä yhdistelmä on Elliptic Curve Diffie-Hellman (ECDH) kiinteillä parametreilla ja varmennettuna algoritmilla Elliptic Curve Digital Signature Algorithm (ECDSA). DH-standardin ja ECDH:n välinen

ero on vain erilainen matematiikka salakirjoitus- ja purkuavaimia saataessa ja käytettäessä. Tällaiset erot eivät ole keksinnön kannalta oleellisia.

Lisäksi RSA (Rivest-Shamir-Adlemann) ja ECES (Elliptic Curve Encryption Scheme) -algoritmeja voidaan käyttää sopivin muutoksin. Näillä algoritmeilla palvelinavaimen vaihto (Server Key Exchange) tapahtuu seuraavasti. B kehittää satunnaisluvun, joka on esisalaisuus (pre-master secret), salakirjoittaa sen A:n julkisella avaimella ja lähettää tuloksen A:lle. Vaiheen 26 sanoma siis käsittäisi osat ServerHello, C_B, ServerKeyExhange, Finished. Nyt A purkaa tämän pääavainta edeltävän salaisuuden salakirjoituksen. Tämä palvelinavaimen vaihto muistuttaa TLS:ssä käytetyn proseduurin peilikuvaa, jolloin kättely voidaan edelleen suorittaa vain kahdella ilmarajapinnan ylittävällä sanomalla.

Yllä selostettu kättelymenetelmä käyttää julkisia avaimia. Kuten hyvin tiedetään, julkisen avaimen salakirjoitus on paljon hitaampaa kuin symmetrinen salakirjoitus. Sen vuoksi on edullisempaa käyttää julkisen avaimen salakirjoitusta vain vaihtamaan parametreja, joita käytetään jaetun avaimen laskemiseen symmetristä salakirjoitusta, kuten DES:ää varten. Sanomassa 21 lähetettyjä parametreja (satunnaislukuja) voidaan käyttää tähän tarkoitukseen.

Vaikka keksinnön mukainen kättely jossakin määrin rajoittaa käytettävissä olevia avaimenvaihtomekanismeja varsinaisen kättelyn aikana, keksintö ei rajoita käytettävissä olevia mekanismeja, joita käytetään todelliseen datasiirtoon. Toisin sanoen keksintö ei rajoita käytössä olevia vaihtoehtoja symmetristä salakirjoitusta varten, vaikka se vaatii että ensin käytettävät parametrit symmetristä salakirjoitusta varten vaihdetaan käyttäen kiinteiden parametrien avaimenvaihtomekanismia. Sanomassa 21 (ja 26) lähetetyt salakirjoitusparametrit voidaan yhdistää yksityisten avainten kanssa luomaan esisalaisuuksia (pre-master secret), joita puolestaan käytetään luomaan pääsalaisuuksia (master secret), jne. Jokaiseen sanomaa 28 seuraavaan sovellusdatasanomaan voidaan siis ketjuttaa erillinen sanoma. Tätä erillistä sanomaa voidaan käyttää vaihtamaan valittua salakirjoitusmekanismia.

Asiakkaan A tunnisteen ID_A tulisi olla yksilöllinen kullekin A:lle. Sopivia tunnisteita ovat esimerkiksi verkkonumero, kuten MSISDN- tai X.509 -numero. Varsinainen kättelyprotokolla ei suojaa tunnistetta ID_A, vaikka se voidaankin suojata alemman tason protokollalla. Sen vuoksi on edullista kehittää ID_A käyttäen yksisuuntaista funktiota, kuten hash-funktiota. Yksisuuntaiset funktiot ovat funktioita, jotka ovat huomattavasti (ainakin useita kertaluokkia)

helpompia suorittaa yhteen suuntaan kuin käänteiseen suuntaa. Esimerkkejä yksisuuntaisista funktioista on suurten alkulukujen kertominen, diskreetti potenssiinkorotus, elliptiset funktiot ja hash-funktiot. Yksisuuntaisten funktioiden etuna on, että ne kätkevät A:n identiteetin mahdollisilta salakuuntelijoilta. Kuten hyvin tiedetään, hash-funktiot vähentävät informaatiota. Hash-koodatut numerot eivät siis välttämättä ole uniikkeja. Hyvä yhdistelmä saavutetaan kuitenkin käyttämällä asiakkaan julkisen avaimen E_A hash-koodia ja osoittamalla julkiset avaimet siten, että ne eivät tuota identtisiä hash-arvoja.

Kuvion 2 yläosa näyttää, kuinka keksinnön mukainen toiminnallisuus voidaan kartoittaa eri verkkoelementeille. Keksintöä voidaan käyttää langattomassa tietoliikennejärjestelmässä kuten matkaviestinjärjestelmässä. Asiakas A voi olla matkaviestin MS (Mobile Station), johon mahdollisesti on kytketty tai integroitu kannettava tietokone PC (Personal Computer). Palvelin B voi olla tietokone B', joka tuottaa taloudellisia palveluja tai myöntää pääsyn luottamukselliseen tietoon, jne. A ja B voivat liikennöidä ilmarajapinnan Um ja yleisen langoitetun matkapuhelinverkon PLMN (Public Land based Mobile Network) kautta, mahdollisesti myös langoitetun puhelinverkon PSTN (Public Switched Telephone Network) kautta.

Luotettu osapuoli CS voidaan toteuttaa jossakin PLMN:n rekisterissä, kuten kotirekisterissä (Home Location Register, HLR) tai GPRS-rekisterissä GR. Vaihtoehtoisesti luotetun osapuolen palvelut voidaan toteuttaa mainitussa ISO-standardissa X.509 esitetyllä tavalla.

Sen sijaan, että A:n sertifikaatti noudetaan CS:stä, tai tämän lisäksi, B voi ylläpitää sertifikaattien paikallista muistia MEM ja ohittaa CS-kyselyn, jos A:n sertifikaatti löytyy paikallisesta muistista. B voi olla kytkettynä lähiverkkoon ja kaikkien asiakkaiden sertifikaatteja voidaan ylläpitää lähiverkon yli. Paikallista muistia MEM voidaan käyttää myös välimuistina (cache) tallentamaan hiljattain käytettyjä sertifikaatteja. Tosiaikaisissa sovelluksissa, jos sertifikaatti peruutetaan, tietokonetta B' on informoitava ja tämän on myös poistettava peruutettu sertifikaatti välimuististaan.

Eräs keksinnön tärkeä etu on, että lisäkuorma ilmarajapinnan kaltaisen hitaan tiedonsiirtokanavan yli voidaan puolittaa tunnettuihin protokolliin verrattuna. Toinen etu on, että asiakkaan sertifikaattia C_A ei tarvitse tallentaa asiakkaassa itsessään. Koska asiakas A on tyypillisesti matkaviestin, sen muistikapasiteetti on rajoittunut. Näin myös vähennetään vilpillisten kolmansien osapuolten saamaa informaatiota siinä tapauksessa, että asiakkaan lait-

teisto katoaa tai varastetaan tai joutuu valtuuttamattomien henkilöiden käyttöön. Vielä, koska asiakkaan sertifikaattia C_A ei lähetetä ilmarajapinnan yli, vähemmän informaatiota vuotaa mahdollisille salakuuntelijoille.

Keksintö on selostettu edullisten suoritusmuotojen yhteydessä. Tietoliikennetekniikan määritykset muuttuvat kuitenkin nopeasti. Tällaiset kehitykset saattavat vaatia keksintöön lisämuutoksia. Sen vuoksi kaikki sanat ja ilmaukset tulisi tulkita laajasti, ja ne on tarkoitettu havainnollistamaan eikä rajoittamaan oheisissa patenttivaatimuksissa kuvattua keksintöä.

Patenttivaatimukset

1. Menetelmä varmaa kättelyprotokollaa varten tietoliikennekanavan (Um, PLMN) kautta yhdistettyjen ensimmäisen osapuolen (A) ja toisen osapuolen (B) välillä, missä kumpikin osapuoli tukee vastaavaa joukkoa salakirjoitussarjoja, ja kullekin osapuolelle on määritelty vastaava sertifikaatti (C_A, C_B), joista kukin sertifikaatti (C_A, C_B) käsittää vastaavan omistajansa julkisen avaimen (E_A, E_B); menetelmän ollessa, t u n n e t t u siitä, että:

- ensimmäinen osapuoli (A) lähettää ensimmäisen osapuolten välisen sanoman (21), joka osoittaa sen tukemien salakirjoitussarjojen joukon, salakirjoitussarjojen vaatimat parametrit sekä ensimmäisen osapuolen (A) tunnisteen (ID_A);

vasteena ensimmäiselle osapuolten väliselle sanomalle (21), toinen osapuoli (B);

- valitsee jonkin mainituista osoitetuista salakirjoitussarjoista, jota myös toinen osapuoli (B) tukee;

- käyttää mainittua tunnistetta (ID_A) saadakseen ensimmäisen osapuolen (A) sertifikaatin (C_A) sellaisen yhteyden kautta, joka on merkittävästi nopeampi kuin mainittuja osapuolia yhdistävä tietoliikennekanava (Um, PLMN);

- varmentaa mainitun saadun ensimmäisen osapuolen (A) sertifikaatin (C_A) ja saa ensimmäisen osapuolen (A) julkisen avaimen (E_A);

- lähettää toisen osapuolten välisen sanoman (26), joka käsittää toisen osapuolen (B) sertifikaatin (C_B), osoituksen siitä, että toinen osapuoli (B) on varmentanut ensimmäisen osapuolen (A) sertifikaatin (C_A), sekä osoituksen mainitusta valitusta salakirjoitussarjasta;

vasteena toiselle osapuolten väliselle sanomalle (26), ensimmäinen osapuoli (A):

- alkaa käyttää valittua salakirjoitussarjaa;

- varmentaa toisen osapuolen (B) sertifikaatin (C_B) ja saa toisen osapuolen (B) julkisen avaimen (E_B);

- lähettää kolmannen osapuolten välisen sanoman (28), joka osoittaa että ensimmäinen osapuoli (A) on varmentanut toisen osapuolen (B) sertifikaatin (C_B);

jolloin informaatio, joka ei ole yllä mainituille vaiheille välttämätön, voidaan lähettää ensimmäiseltä osapuolelta (A) toiselle osapuolelle (B) kolmannessa osapuolten välisessä sanomassa (28), mikä toteuttaa kaksisuuntai-

sen avaintenvaihdon ja keskinäisen varmentamisen kahden osapuolten välisen sanoman (21, 26) suuruisella tehollisella lisäkuormalla.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että mainittu vaihe ensimmäisen osapuolen (A) sertifikaatin (C_A) saamiseksi käsittää sen noutamisen toisen osapuolen (B) ulkopuolisesta lähteestä, edullisesti tietoliikenneverkon rekisteristä (HLR, GR) tai olennaisesti ISO-standardia X.509 vastaavasta hakemistopalvelusta.

3. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että mainittu vaihe ensimmäisen osapuolen (A) sertifikaatin (C_A) saamiseksi käsittää sen noutamisen paikallisesta muistista (MEM).

4. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että mainittu ensimmäisen osapuolen (A) tunniste (ID_A) muodostetaan yksisuuntaisen funktion, edullisesti hash-funktion avulla.

5. Jonkin edellisen patenttivaatimuksen mukainen menetelmä, t u n n e t t u siitä, että mainittu toinen sanoma (26) käsittää esisalaisuuden, jonka toinen osapuoli (B) saa kehittämällä satunnaisluvun ja salakirjoittamalla sen ensimmäisen osapuolen (A) julkisella avaimella (E_A).

6. Tietoliikennelaitteisto (A), joka on sovitettu toimimaan ensimmäisenä osapuolena varmassa kättelyprotokollassa mainitun laitteiston (A) ja toisen osapuolen (B) välillä, t u n n e t t u siitä, että laitteisto on sovitettu:

- lähettämään toiselle osapuolelle (B) ensimmäisen sanoman (21), joka osoittaa salakirjoitussarjojen joukon, salakirjoitussarjojen vaatimat parametrit sekä laitteiston (A) tunnisteen (ID_A);
- vastaanottamaan toiselta osapuolelta toisen sanoman (26), joka käsittää osoituksen mainitun toisen osapuolen (B) valitsemasta salakirjoitussarjasta, toisen osapuolen (B) sertifikaatin (C_B), osoituksen siitä, että toinen osapuoli (B) on käyttänyt mainittua laitteiston tunnistetta (ID_A) saadakseen ja varmentaakseen laitteiston (A) sertifikaatin (C_A);
- käyttämään toisen sanoman (26) osoittamaa salakirjoitussarjaa;
- varmentamaan toisen osapuolen (B) sertifikaatin (C_B) ja saamaan toisen osapuolen (B) julkisen avaimen (E_B);

- lähettämään toiselle osapuolelle (B) kolmannen sanoman (28), joka osoittaa että laitteisto (A) on varmentanut toisen osapuolen (B) sertifikaatin (C_B); ja

- lisäämään informaatiota, joka ei ole yllä mainituille toiminnoille välttämätön, mainittuun kolmanteen sanomaan (28).

7. Tietoliikennelaitteisto (B), joka on sovitettu vastaamaan ensimmäisen osapuolen (A) aloittamaan varmaan kättelyprotokollaan, laitteiston (B) ollessa kytkettävissä mainittuun ensimmäiseen osapuoleen (A) tietoliikennekanavan (Um, PLMN) kautta, t u n n e t t u siitä, että laitteisto (B) on sovitettu:

- vastaanottamaan ensimmäiseltä osapuolelta (A) ensimmäisen sanoman (21), joka osoittaa salakirjoitussarjojen joukon, salakirjoitussarjojen vaatimat parametrit sekä ensimmäisen osapuolen (A) tunnisteen (ID_A);

- valitsemaan yhden mainituista salakirjoitussarjoista;

- käyttämään tunnistetta (ID_A) saadakseen ensimmäisen osapuolen (A) sertifikaatin (C_A) sellaisen yhteyden kautta, joka on merkittävästi nopeampi kuin mainittu tietoliikennekanava (Um, PLMN);

- varmentamaan mainitun saadun ensimmäisen osapuolen (A) sertifikaatin (C_A) ja saamaan ensimmäisen osapuolen (A) julkisen avaimen (E_A);

- lähettämään ensimmäiselle osapuolelle (A) toisen sanoman (26), joka käsittää laitteiston (B) sertifikaatin (C_B) ja osoittaa, että laitteisto (B) on varmentanut ensimmäisen osapuolen (A) sertifikaatin (C_A), ja osoittaa mainitun valitun salakirjoitussarjan; ja

- vastaanottamaan ensimmäiseltä osapuolelta (A) kolmannen sanoman (28), joka osoittaa että ensimmäinen osapuoli (A) on varmentanut laitteiston (B) sertifikaatin (C_B), ja joka käsittää informaatiota, joka ei ole yllä mainituille toiminnoille välttämätöntä.

Patentkrav

1. Förfarande för ett säkert handskakningsprotokoll mellan en första part (A) och en andra part (B) förenade via en telekommunikationskanal (Um, PLMN), varvid båda parterna stöder ett respektive antal chifferserier, och ett respektive certifikat (C_A, C_B) har definierats för vardera parten, varav bägge certifikaten (C_A, C_B) omfattar en allmän nyckel (E_A, E_B) av sin respektive innehavare (A, B), varvid förfarandet är k ä n n e t e c k n a t av att

den första parten (A) sänder ett första meddelande (21) mellan parterna vilket anger en uppsättning av chifferserier som stöds av den första parten, parametrar som krävs av chifferserierna samt den första partens (A) identifierare (ID_A),

som gensvar på det första meddelandet (21) mellan parterna:

- väljer den andra parten (B) en av nämnda angivna chifferserier som också stöds av den andra parten (B),

- använder den andra parten (B) nämnda identifierare (ID_A) för att erhålla den första partens (A) certifikat (C_A) genom en sådan förbindelse som är betydligt snabbare än telekommunikationskanalen (Um, PLMN) som förenar nämnda parter,

- bekräftar den andra parten (B) den första partens (A) nämnda erhållna certifikat (C_A) och erhåller den första partens (A) allmänna nyckel (E_A),

- sänder den andra parten (B) ett andra meddelande (26) mellan parterna vilket omfattar den andra partens (B) certifikat (C_B), en indikation om att den andra parten (B) har bekräftat den första partens (A) certifikat (C_A), samt en indikation om nämnda valda chifferserie,

som gensvar på det andra meddelandet (26) mellan parterna:

- börjar den första parten (A) använda den valda chifferserien,

- bekräftar den första parten (A) den andra partens (B) certifikat (C_B) och erhåller den andra partens (B) allmänna nyckel (E_B),

- sänder den första parten (A) ett tredje meddelande (28) mellan parterna som anger att den första parten (A) har bekräftat den andra partens (B) certifikat (C_B),

varvid information som inte är nödvändig för ovannämnda steg kan sändas från den första parten (A) till den andra parten (B) i det tredje meddelandet (28) mellan parterna, och sålunda utföra dubbelriktad nyckelutbyte och en inbördes bekräftelse med en effektiv extra last i storlek av två meddelanden

(21, 26) mellan parterna.

2. Förfarande enligt patentkrav 1, k ä n n e t e c k n a t av att nämnda steg för att erhålla den första partens (A) certifikat (C_A) omfattar dess hämtning från en källa utanför den andra parten (B), företrädesvis ett register (HLR, GR) i ett telekommunikationsnät eller från en registerservice som väsentligen motsvarar ISO-standard X.509.

3. Förfarande enligt patentkrav 1, k ä n n e t e c k n a t av att nämnda steg för att erhålla den första partens (A) certifikat (C_A) omfattar dess hämtning från ett lokalt minne (MEM).

4. Förfarande enligt något av de föregående patentkraven, k ä n n e t e c k n a t av att den första partens (A) nämnda identifierare (ID_A) bildas med hjälp av en enkelriktad funktion, företrädesvis en hash-funktion.

5. Förfarande enligt något av de föregående patentkraven, k ä n n e t e c k n a t av att nämnda andra meddelande (26) omfattar en förhandshemlighet som den andra parten (B) erhåller genom att bilda ett slumptal och genom att kryptera det med den första partens (A) allmänna nyckel (E_A).

6. Telekommunikationsanordning (A) anordnad att fungera som en första part i ett säkert handskakningsprotokoll mellan nämnda anordning (A) och en andra part (B), k ä n n e t e c k n a d av att anordningen är anordnad att

- sända till den andra parten (B) ett första meddelande (21) som anger en uppsättning av chifferserier, parametrar som chifferserierna kräver samt anordningens (A) identifierare (ID_A),
- motta från den andra parten ett andra meddelande (26) som omfattar en indikation om en chifferserie vald av nämnda andra part (B), den andra partens (B) certifikat (C_B), en indikation om att den andra parten (B) har använt anordningens nämnda identifierare (ID_A) för att erhålla och bekräfta anordningens (A) certifikat (C_A),
- använda den av det andra meddelandet (26) angivna chifferserien,
- bekräfta den andra partens (B) certifikat (C_B) och erhålla den andra partens (B) allmänna nyckel (E_B),
- sända till den andra parten (B) ett tredje meddelande (28) som anger att anordningen (A) har bekräftat den andra partens (B) certifikat (C_B), och
- tillägga information, som inte är nödvändig för ovannämnda funk-

tion, i nämnda tredje meddelande (28).

7. Telekommunikationsanordning (B) anordnad att svara på ett säkert handskakninsprotokoll inlett av en första part (A) då anordningen (B) kan kopplas till nämnda första part (A) via en telekommunikationskanal (Um, PLMN), k ä n n e t e c k n a d av att anordningen (B) är anordnad att:

- motta från den första parten (A) ett första meddelande (21) som anger en uppsättning av chifferserier, parametrar som chifferserierna kräver samt den första partens (A) identifierare (ID_A),
- välja en av nämnda chifferserier,
- använda identifieraren (ID_A) för att erhålla den första partens (A) certifikat (C_A) genom en sådan förbindelse som är betydligt snabbare än nämnda telekommunikationskanal (Um; PLMN),
- bekräfta den första partens (A) nämnda erhållna certifikat (C_A) och erhålla den första partens (A) allmänna nyckel (E_A),
- sända till den första parten (A) ett andra meddelande (26) som omfattar anordningens (B) certifikat (C_B) och anger att anordningen (B) har bekräftat den första partens (A) certifikat (C_A) och anger nämnda valda chifferserie, och
- motta från den första parten (A) ett tredje meddelande (28) som anger att den första parten (A) har bekräftat anordningens (B) certifikat (C_B) och som omfattar information som inte är nödvändig för ovannämnda funktioner.

Fig. 1

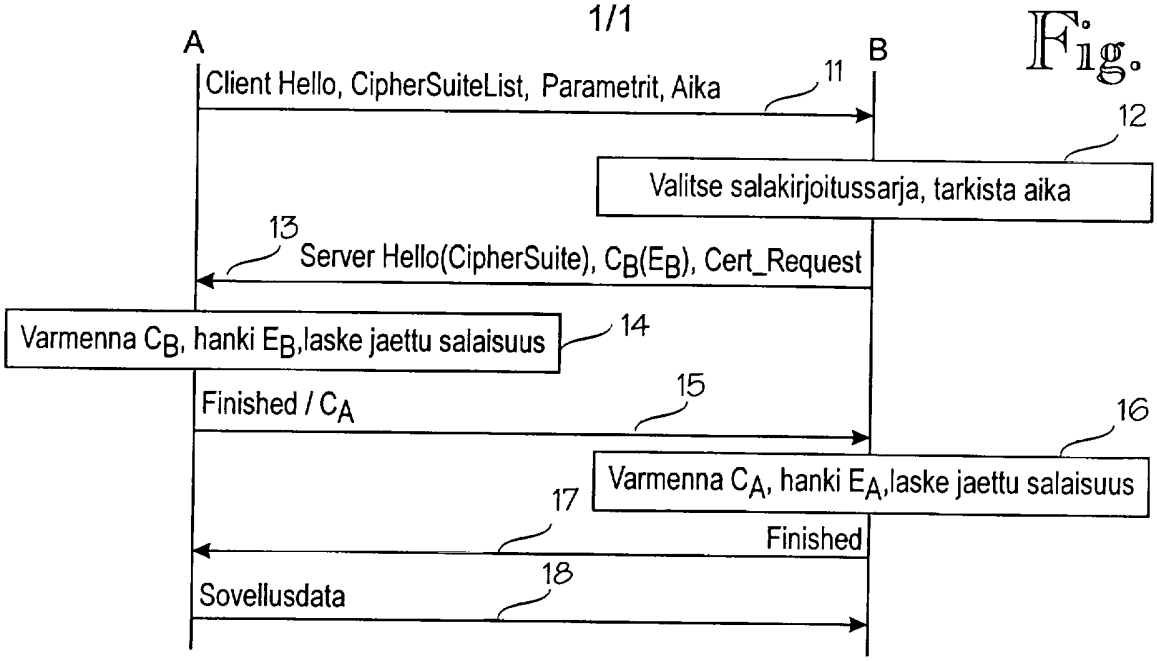
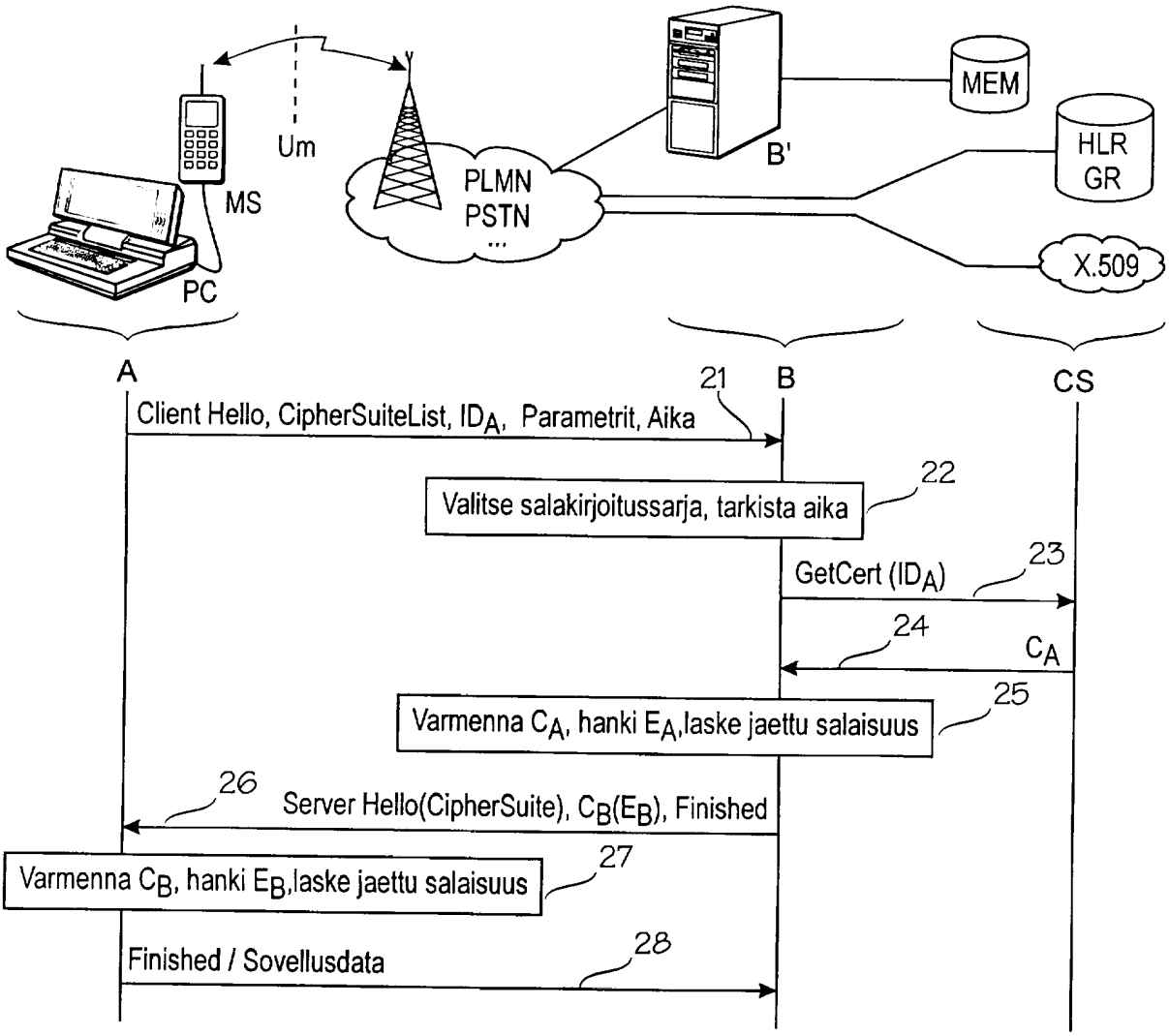

A
B
Client Hello, CipherSuiteList, Parametrit, Aika
11
12
Valitse salakirjoitussarja, tarkista aika
13
Server Hello(CipherSuite), $C_B(E_B)$, Cert_Request
Varmenna C_B, hanki E_B,laske jaettu salaisuus
14
Finished / C_A
15
16
Varmenna C_A, hanki E_A,laske jaettu salaisuus
17
Finished
Sovellusdata
18

Fig. 2


Um
MS
PC
PLMN
PSTN
...
B'
MEM
HLR
GR
X.509
A
B
CS
21
Client Hello, CipherSuiteList, ID_A, Parametrit, Aika
22
Valitse salakirjoitussarja, tarkista aika
23
GetCert (ID_A)
24
C_A
25
Varmenna C_A, hanki E_A,laske jaettu salaisuus
26
Server Hello(CipherSuite), $C_B(E_B)$, Finished
Varmenna C_B, hanki E_B,laske jaettu salaisuus
27
Finished / Sovellusdata
28