[A] TIIVISTELMÄ - SAMMANDRAG

(11) (21) **Patenttihakemus - Patentansökan** 971620

(51) Kv.lk.6 - Int.kl.6

H 04Q 7/38, H 04L 9/32

(22) Hakemispäivä - Ansökningsdag **16.04.1997**

(24) Alkupäivä - Lopdag **16.04.1997**

(41) Tullut julkiseksi - Blivit offentlig **17.10.1998**

SUOMI-FINLAND

(FI)

Patentti- ja rekisterihallitus
Patent- och registerstyrelsen

(71) Hakija - Sökande

1. **Nokia Telecommunications Oy**, Helsinki, Keilalahdentie 4, 02150 Espoo, (FI)

(72) Keksijä - Uppfinnare

1. **Aura, Tuomas**, Jämeräntaival 11 L 232, 02150 Espoo, (FI)

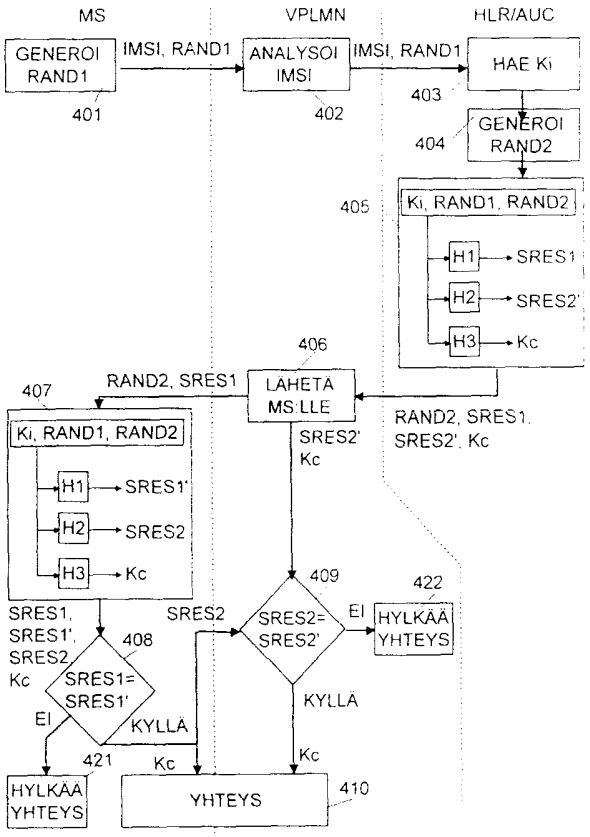
(74) Asiamies - Ombud: **Patenttitoimisto Compatent Oy**, Teollisuuskatu 33, PL 156, 00511 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning

Autentikointimenetelmä
Autenticeringsförfarande

(57) Tiivistelmä - Sammandrag

Tietoliikennejärjestelmissä voidaan liikenteen suojaamiseksi salakuuntelulta ja väärällä identiteetillä esiintymisen estämiseksi yhteyden päätelaitteiden oikeellisuus tarkistaa autentikointimenettelyllä. Erityisen tärkeää päätelaitteiden oikeellisuuden tarkistamien on matkaviestinjärjestelmissä. Autentikointimenettelyssä verkko tarkistaa tilaajalaitteen sille antaman identiteetin oikeellisuuden. Lisäksi tilaajalaite voi tarkistaa verkon identiteetin oikeellisuuden. Tekniikan tason mukaisissa järjestelmissä autentikoinnin suorittamiseen vaadittavia salaisia tietoja joudutaan siirtämään turvattomia siirtoverkkoja pitkin ja antamaan niitä vierailtavien verkkojen haltuun. Tiedot mahdollistavat rajoittamattoman määrän autentikointeja rajoittamattoman ajan kuluessa. Tällöin aktiivinen salakuuntelija voi joissain tapauksissa saada ne tietoonsa, ja jatkossa suorittaa autentikointiprosessin muodostamatta yhteyttä tilaajan autentikointikeskukselle. Tässä keksinnössä esitetään menetelmä, joissa jokainen yksittäinen autentikointiprosessi on matkaviestimen ja autentikointikeskuksen välinen toiminnallisuus. Tällöin verkon luotettavuus tulee tarkistetuksi jokaisen autentikoinnin yhteydessä, eikä onnistuneeseen väärällä identiteetillä esiintymiseen riittäviä tietoja kuljeteta verkkoelementtien välillä.



Jatkuu seur. sivulla
Forts. nästa sida

I telekommunikationssystem är det möjligt att för att skydda trafiken mot avlyssning och för att förhindra uppträdande med en oriktig identitet kontrollera riktigheten av terminaler som uppkopplar en förbindelse genom autenticeringsförfarandet. Att riktigheten av terminaler kontrolleras är särskilt viktigt i mobilkommunikationssystem. Autenticeringsförfarandet innebär att nätet kontrollerar riktigheten av den identitet som abonnentapparaten meddelat därtill. Dessutom kan abonnentapparaten kontrollera riktigheten av nätets identitet. I systemen enligt teknikens ståndpunkt är man tvungen att överföra den hemliga information som krävs för en autenticitetskontroll genom skyddslösa överföringsnät och att ställa den till förfogande för de nät som besöks. Informationen möjliggör ett obegränsat antal autenticitetskontroller under en obegränsad tidsperiod, varvid en aktiv avlyssnare i vissa fall kan få tag på den och därefter utföra en autenticeringsprocess utan att uppkoppla en förbindelse till abonnentens autenticeringscentral. I denna uppfinning presenteras ett förfarande vid vilket varje enskild autenticeringsprocess är verksamhet mellan mobilteleapparat och autenticeringscentral. Nätets pålitlighet kontrolleras alltså i samband med varje autenticitetskontroll och mellan nätelement överförs ingen information som möjliggör lyckat uppträdande med en oriktig identitet.