

(19)



**SUOMI - FINLAND**

**(FI)**

**PATENTTI- JA REKISTERIHALLITUS**

**PATENT- OCH REGISTERSTYRELSEN**

**FINNISH PATENT AND REGISTRATION OFFICE**

**(10) FI 981902 A7**

**(12) JULKISEKSI TULLUT PATENTTIHAKEMUS  
PATENTANSÖKAN SOM BLIVIT OFFENTLIG  
PATENT APPLICATION MADE AVAILABLE TO THE  
PUBLIC**

(21) Patentihakemus - Patentansökan - Patent application **981902**

(51) Kansainvälinen patenttiluokitus - Internationell patentklassifikation -  
International patent classification  
**H04K 1/00**

(22) Tekemispäivä - Ingivningsdag - Filing date **04.09.1998**

(23) Saapumispäivä - Ankomstdag - Reception date **04.09.1998**

(41) Tullut julkiseksi - Blivit offentlig - Available to the public **05.03.2000**

(43) Julkaisupäivä - Publiceringsdag - Publication date **13.06.2019**

(71) Hakija - Sökande - Applicant

**1 • Sonera Smarttrust Oy**, Elimäenkatu 17-19, 00510 Helsinki, SUOMI - FINLAND, (FI)

(72) Keksijä - Uppfinnare - Inventor

**1 • Vatanen, Harri**, Sonera, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud - Agent

**Papula Oy**, Mechelininkatu 1 a, 00180 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning - Title of the invention

**Turvamoduuli, turvajärjestelmä ja matkaviestin**

**Säkerhetsmodul, säkerhetssystem och mobilteleapparater**

## **TURVAMODUULI, TURVAJÄRJESTELMÄ JA MATKAVIESTIN KEKSINNÖN ALA**

Keksintö koskee turvamoduulia. Erityisesti keksinnön kohteena on uusi ja parannettu turvamoduuli ja turvajärjestelmä erilaisten korkeaa tietoturvaa vaativien sanomien käsittelemiseksi ja välittämiseksi. Lisäksi keksinnön kohteena on turvamoduulia hyväksi käyttävä matkaviestin.

### **10 TEKNIIKAN TASO**

Matkaviestinverkoissa, esimerkiksi GSM-verkoissa (GSM, Global System for Mobile communications) käytetään puheen siirron yhteydessä voimakasta salausta radiotiellä matkaviestimen ja tukiaseman välillä. Puheviestinnän ohella myös teksti- tai datamuotoinen matkaviestimillä tapahtuva viestiminen on lisääntynyt. Palvelutason nousun myötä teksti- tai datamuotoiseen viestintään tukeutuvat palvelut ovat yleistyneet. Tekstimuotoista viestintää voidaan käyttää hyväksi erilaisissa palvelutoiminteissa, palveluiden maksamisessa ja niin edelleen.

Tällä hetkellä sanomien mahdollista salausta hankaloittaa se, että nykyisen matkaviestinstandardin mukaisiin matkapuhelimeen ei voida tehdä salaamista helpottavia muutoksia, koska puhelimen käyttöliittymät ovat valmistajakohtaisia. Ainoa riittävästi standardoitu ja salauksen kannalta riittävän avoin komponentti on tilaajaidentiteettimoduuli (SIM, Subscriber Identity Module).

Nykyisen matkaviestinstandardin, kuten GSM-standardin mukaiset matkapuhelimet eivät sellaisenaan suo mahdollisuutta salata matkaviestimillä tapahtuvaa tekstimuotoista viestintää. Tekstimuotoisella viestinnällä voidaan toteuttaa palveluja, kuten pankkipalveluja, jotka vaativat korkeaa tietoturvasoaa. Korkeaa tietoturvaa vaativat palvelut eivät kuitenkaan voi

yleistyä ennen kuin sanomaliikenteen riittävä salaus on mahdollista.

Lisäksi ongelmana matkaviestinverkon käytössä on, että siinä toteutettavat sanomavälityspalvelut eivät välttämättä ole reaaliaikaisia ja viestien välittäminen saattaa kestää. Tämä voi muodostua ongelmaksi esimerkiksi silloin, kun käyttäjä haluaa maksaa ostoksensa kaupan kassalla. Tällöin pienikin viive sanomavälityksessä hidastaa merkittävästi maksutapahtuman suorittamista. Mikään matkaviestinstandardin osa ei tällä hetkellä tue paikallista liikennöintiä matkaviestimen ja kassapäätteen välillä.

Ryhmä maailman johtavia tietoliikenne- ja tietotekniikkayrityksiä on kehittänyt tekniikan, jonka avulla matkapuhelimen ja esimerkiksi kannettavan tietokoneen välille voidaan muodostaa langaton yhteys. Tämä tekniikka on nimetty "Bluetoothiksi" ja se perustuu lyhyen kantaman radioteknologiaan, jolloin sen avulla voidaan yhdistää toisiinsa monenlaisia päätelaitteita. Tarkempaa kuvausta tekniikasta esitetään esimerkiksi WWW-sivulla [www.bluetooth.com](http://www.bluetooth.com).

Bluetooth -tekniologia mahdollistaa laitteiden kytkemisen toisiinsa lyhyen kantaman radiolinkillä. Bluetooth -tekniologian avulla voidaan esimerkiksi matkaviestin ja kannettava tietokone yhdistää toisiinsa ilman hankalaa kaapelointia. Tulostimet, työasemat, telekopiolaitteet, näppäimistöt ja virtuaalisesti mitkä tahansa digitaaliset laitteet voivat olla osana Bluetooth -järjestelmää tai -verkkoa. Tekniologia muodostaa universaalin sillan olemassa oleviin dataverkoihin, oheislaitteisiin ja tarjoaa mahdollisuuden pienten yksityisten ryhmien muodostamiseen toisiinsa kytkettyjen laitteiden avulla ilman kiinteää verkkoinfrastruktuuria. Lisäksi laitteiden välillä voidaan käyttää salausta ja autentikointia esimerkiksi siten, että vain tietyn käyttäjän matkapuhelinta voidaan käyttää tietyn kannettavan tietokoneen yhteydessä.

Edelleen entuudestaan tunnetaan älykortti, joka mahdollistaa varman henkilökohtaisen autentikoinnin sekä väärentämättömän allekirjoituksen. Sen sovel-

5 voidaan mainita kansallinen sähköinen henkilöllisyys-

todistus (EID) tiedostojen, tietoliikenteen ja sähkö-

postin salaaminen, dokumenttien allekirjoitusväline, elektroninen maksuväline, ajokortti, äänestyslipuke ja niin edelleen.

10 Vaikka älykorttia voidaan käyttää edellä kuvatulla on ongelmana edelleen se, että älykortti vaatii kuitenkin erillisen lukulaitteen, jolla ollaan yhteydessä älykorttiin. Lisäksi älykortti ei kuitenkaan pysty kommunikoimaan yksinään minkään tietoliikenne-

15 verkon yli, jolloin tietojen päivittäminen esimerkiksi lyhytsanomaviestein ei ole mahdollista.

Lisäksi vaikka matkaviestin voitaisiinkin yhdistää Bluetooth -teknologian avulla paikallisesti kassapäätteeseen ja käyttää tätä matkaviestintä maksuvälineenä, on edelleen ongelmana maksutoiminnan tarvitsema salattu ja tietoturvallinen tietoliikenne.

20

Entuudestaan ei tunneta yleiskäyttöistä turvamoduulia, joka voitaisiin kytkeä erilaisiin kassa- ja automaattijärjestelmiin, matkaviestimeen tai muihin

25 mukana kannettaviin laitteisiin ja joka pystyisi kommunikoimaan esimerkiksi toisaalta isäntälaitteen ja toisaalta palveluntarjoajan laitteen kanssa esimerkiksi Bluetooth -teknologiaa hyödyntäen salatusti ja turvallisesti siten, että pankkien ja viranomaisten asettamat korkeat tietoturvallisuusvaatimukset tulisivat täytetyiksi.

30

Esillä olevan keksinnön tarkoituksena on poistaa edellä mainitut ongelmat.

35 Erityisesti esillä olevan keksinnön tarkoituksena on tuoda esiin uudentyyppinen ja yleiskäyttöinen turvamoduuli, jota voidaan käyttää monenlaisissa sovellusympäristöissä paikallisen salatun ja turvalli-

sen yhteyden muodostamiseen. Lisäksi keksinnön kohteena on tuoda esiin turvajärjestelmä, jossa tarjotaan välineet käyttäjän ja palveluntarjoajan väliseen salattuun tietoliikenteeseen.

5 Edelleen esillä olevan keksinnön tarkoituksena on tuoda esiin uudenlainen matkaviestin, jota voidaan käyttää paikalliseen ja tietoturvalliseen yhteydenpitoon palveluntarjoajan päätelaitteen kanssa. Tällä ratkaisulla yhdessä turvamoduulin kanssa voidaan  
10 toteuttaa yleiskäyttöinen turvalaitteisto, jonka liittäminen ja käyttäminen on mahdollista missä tahansa ympäristössä.

Lisäksi keksinnön tarkoituksena on tuoda esiin laite, jonka valmistaja voidaan suoraan sertifioida niin sanotuksi luotettavaksi kolmanneksi osapuoleksi. Tällöin ei erikseen tarvita laitevalmistajaa, kuten matkapuhelinvalmistajaa tai operaattoria, jonka valmistamaan laitteeseen luotettava kolmas osapuoli  
15 lisääisi salausominaisuuden.

20

#### KEKSINNÖN YHTEENVETO

Esillä oleva keksintö kohdistuu turvamoduuliin, johon kuuluu kytkentävälineet turvamoduulin yhdistämiseksi päätelaitteeseen, kuten matkaviestimeen,  
25 kassapäätteeseen, pankkiautomaattiin, kannettavaan tietokoneeseen, puhelimeen tai mihin tahansa muuhun vastaavaan päätelaitteeseen. Tarkoituksena on, että turvamoduuli on yleiskäyttöinen tietoliikenneverkkoihin ja tietoliikennepäätelaitteisiin kytkettävä moduuli, jonka avulla voidaan toteuttaa tarvittavat salaus-  
30 toimenpiteet korkeaa tietoturvaa vaativien sovellusten toteuttamiseksi.

Keksinnön mukaisesti turvamoduuliin kuuluu salausvälineet turvamoduulin sähköisen tiedonsiirron salaamiseksi, salauksen purkamiseksi ja sähköisen al-  
35 lekirjoituksen toteuttamiseksi. Edullisesti salausvälineisiin kuuluu prosessori, joka salaa, purkaa sala-

uksen ja toteuttaa sähköisen allekirjoituksen. Lisäksi välineisiin kuuluu muisti, joka on yhdistetty prosessoriin sen tarvitsemien avaimien ja parametrien tallentamiseksi.

5 Edelleen keksinnön mukaisesti turvamoduuliin kuuluu ensimmäinen liityntärajapinta turvamoduulin yhdistämiseksi sähköistä tiedonsiirtoa varten ulkoiseen laitteeseen ja teholähde tehonsyötön järjestämiseksi turvamoduulin tehoa tarvitseville osille eli prosessorille ja muistille. Teholähde voidaan myös korvata  
10 isäntälaitteen, johon turvamoduuli yhdistetään, tehollähteellä järjestämällä tehonsyöttö turvamoduuliin suoraan isäntäkoneesta. Liityntärajapinta voidaan toteuttaa esimerkiksi Bluetooth -teknologialla, joka on  
15 sinänsä tunnettu teknologia ja jonka standardointityö on vielä kesken. Kuitenkaan emme kuvaa sitä tässä tarkemmin, koska se on entuudestaan tunnettua.

Lisäksi turvamoduuliin voi kuulua älykorttiosa, joka on järjestetty älykorttitoimintojen toteuttamiseksi turvamoduulilla. Älykorttiosa voi käyttää  
20 liityntärajapintaa kommunikoidessaan ulkopuolisten laitteiden, kuten kassapäätteiden, pankkiautomaattien ja vastaavien kanssa sähköisen rahan käyttämiseksi ja lataamiseksi. Näin keksinnön ansiosta älykortin käyttäminen on entistä helpompaa ja houkuttelevampaa asi-  
25 akkaan ja käyttäjän kannalta.

Turvamoduuli voidaan integroida esimerkiksi matkaviestimen tehollähteeseen, jolloin turvamoduuliin edullisesti kuuluu runko, joka on sovitettu vastaamaan  
30 esimerkiksi matkaviestimen tehollähteen muotoja, ja liitin, joka on yhdistetty runkoon ja jolla turvamoduuli kytketään sähköisesti matkaviestimeen sen tehollähteen paikalle. Tällöin turvamoduuli on kytketty matkaviestimeen tehon syöttämiseksi siihen ja kommuni-  
35 koinnin toteuttamiseksi matkaviestimen avulla. Tällöin turvamoduulia voidaan käyttää matkaviestimen näppäimistöä ja näyttöä apuna käyttäen.

Keksinnön kohteena on lisäksi turvajärjestelmä, johon kuuluu palveluntarjoajan päätelaite, kuten pankkiautomaatti, kassa, myyntiautomaatti tai vastaava, ja palvelunkäyttäjän päätelaite, kuten matkaviestin. Järjestelmässä päätelaitteet on yhdistetty toisiinsa sähköisesti ennalta valitun tiedonsiirtoyhteyden avulla, esimerkiksi Bluetooth -teknologialla.

Keksinnön mukaisesti turvajärjestelmään kuuluu palveluntarjoajan päätelaitteeseen kytketty ensimmäinen turvamoduuli ja palvelunkäyttäjän päätelaitteeseen kytketty toinen turvamoduuli. Tällöin turvamoduuleilla salataan ja puretaan salaus päätelaitteiden välillä. Edullisesti turvamoduuleihin kuuluu salausvälineet, ensimmäinen liitäntärajapinta ja teholähde, kuten edellä kuvattiin turvamoduulin yhteydessä.

Turvajärjestelmään voi kuulua myös palveluntarjoajan palvelin, joka on sähköisesti yhteydessä palveluntarjoajan päätelaitteeseen. Tämä yhteys voidaan muodostaa esimerkiksi tietoliikenneverkon, kuten GSM-matkaviestinverkon avulla tai jollain muulla sopivalla verkolla. Ensimmäinen turvamoduuli voidaan yhdistää edelleen tietoliikenneverkon välityksellä palveluntarjoajan palvelimeen palvelunkäyttäjän päätelaitteella suoritettujen toimintojen päivittämiseksi ja tallentamiseksi palvelimelle. Tällä tarkoitetaan niin sanottuja clearing-toimintoja, jolloin palvelunkäyttäjän palveluista tai ostoksista maksama sähköinen raha siirretään palveluntarjoajan tilille.

Keksinnön kohteena on myös matkaviestin, jolla tarkoitetaan sinänsä tunnettua päätelaitetta, johon kuuluu näppäimistö, näyttö, radio-osa ja teholähde. Eräs edullinen esimerkki tällaisesta matkaviestimestä on GSM-yhteensopiva päätelaite tai GSM-matkapuhelin (GSM, Global Standard for Mobile Communication).

Keksinnön mukaisesti tehollähteeseen on integroitu turvamoduuli, johon kuuluu salausvälineet ja ensimmäinen liityntärajapinta, kuten edellä turvamoduu-

lin yhteydessä on kuvattu. Edullisesti turvamoduuli on järjestetty käsittelemään matkaviestimellä tietoliikenneverkon ja/tai matkaviestimen paikallisen tiedonsiirtoliitännän kautta välitettävää informaatiota.

- 5 Turvamoduuli voi kommunikoida matkaviestimen ja/tai ulkopuolisen päätelaitteen kanssa Bluetooth -teknologialla.

- Esillä olevan keksinnön etuna tunnettuun tekniikkaan verrattuna on, että nykyisiä olemassa olevia  
10 matkapuhelimia ei välttämättä tarvitse muuttaa mitenkään haluttaessa käyttää niitä tietoturvalliseen yhteydenpitoon. Edelleen keksinnön etuna on, että turvamoduuli on yleiskäyttöinen, jolloin se voidaan kytkeä miltei mihin tahansa päätelaitteeseen, jossa salattua  
15 tiedonsiirtoa tarvitaan.

Lisäksi keksinnön ansiosta voidaan toteuttaa tietoturvallisia järjestelmiä, joiden avulla palveluntarjoajat voivat tarjota korkeaa tietoturvaa vaativia palveluitaan, kuten pankkipalveluitaan.

20

#### KUVALUETTELO

Seuraavassa keksintöä selostetaan edullisten sovellusesimerkkien avulla viitaten oheiseen piirustukseen, jossa

- 25 kuvio 1 esittää erästä esillä olevan keksinnön mukaista turvamoduulia;

kuvio 2 esittää erästä esillä olevan keksinnön mukaista edullista turvajärjestelmää; ja

- 30 kuvio 3 esittää erästä esillä olevan keksinnön mukaista edullista matkaviestintä, johon on integroitu eräs keksinnön mukainen turvamoduuli.

#### KEKSINNÖN YKSITYISKOHTAINEN SELOSTUS

- 35 Kuviossa 1 esitettyyn turvamoduuliin kuuluu kytkentävälineet 1 turvamoduulin yhdistämiseksi päätelaitteeseen SP, MS. Päätelaite voi olla matkaviestin,

kassapäätte, pankkiautomaatti tai mikä tahansa vastaava laite, jolla halutaan toteuttaa korkeaa tietoturvaa vaativia sovelluksia. Lisäksi turvamoduuliin kuuluu salausvälineet 2, joilla salataan turvamoduulin sähköinen tiedonsiirto, puretaan salaus ja muodostetaan tarvittaessa sähköinen allekirjoitus.

Paikallisverkkoliitännän tai vastaavan toteuttamiseksi turvamoduuliin kuuluu edelleen ensimmäinen liityntäraajapinta RP1, jolla turvamoduuli voidaan yhdistää esimerkiksi radioteitse sähköistä tiedonsiirtoa varten päätelaitteeseen. Liityntäraajapinnan yhteyteen voidaan järjestää niin sanottu Bluetooth -osa, kuten kuviossa 1 esitetään, jolla toteutetaan kyseisen teknologian vaatimat toimenpiteet. Turvamoduuliin on järjestetty myös teholähde 3, joka voi olla ladattava akku, verkkomuuntaja tai vastaava, jolla järjestetään tehonsyöttö turvamoduulin tehoa tarvitseville osille.

Edelleen kuviossa 1 esitettyihin salausvälineisiin kuuluu prosessori 4, joka voidaan suunnitella ja optimoida erityisesti salaustoimintoja varten ja joka salaa, purkaa salauksen ja toteuttaa sähköisen allekirjoituksen, ja muisti 5, joka on yhdistetty prosessoriin sen tarvitsemien avaimien ja parametrien tallentamiseksi. Muistiin voidaan tallentaa turvamoduulin käyttäjän henkilökohtainen avain, käytetyn salausalgoritmin parametrejä ja muita tarpeellisia tietoja. Edullinen esimerkki salausalgoritmista on RSA-menetelmä, mutta myös muita epäsymmetrisiä algoritmeja voidaan sovelluksesta riippuen käyttää.

Edelleen turvamoduuliin kuuluu älykorttiosa SC, joka on järjestetty älykorttitoimintojen toteuttamiseksi turvamoduulilla. Älykortti-osa voi hyödyntää turvamoduulin muita osia, esimerkiksi liityntäraajapintaa RP1 tietoliikenneyhteyksissään.

Turvamoduulin prosessoriin 4 tai älykortti-osaan SC kuuluu edelleen kello, jolla turvamoduulin toimintoja synkronoidaan ja kellotetaan. Kello synkro-

noituu sen laitteen kelloon, johon turvamoduuli kytketään. Myös on mahdollista, että kello synkronoituu Bluetooth -järjestelmän kelloon.

Turvamoduulin runko 6 on sovitettu vastaamaan  
 5 matkapuhelimen teholähteen muotoja. Lisäksi runkoon 6 on yhdistetty liitin 7, jolla turvamoduuli kytketään matkapuhelimeen. Liittimen 7 kautta voidaan kytkeä teho ja tietoliikenne turvamoduulin ja matkapuhelimen välillä. Tässä sovelluksessa turvamoduulin teholähde  
 10 vastaa kapasiteetiltaan olennaisesti matkaviestimen teholähdettä ja on siten myös ladattava. Tällöin turvamoduuli voidaan helposti mekaanisesti ja sähköisesti kiinnittää matkapuhelimeen.

Kuviossa 2 on esitetty eräs esimerkki keksinnön mukaisesta turvajärjestelmästä. Kuviossa 2 esitettyyn turvajärjestelmään kuuluu palveluntarjoajan päätelaite SP eli tässä esimerkissä pankkiautomaatti ja palvelunkäyttäjän päätelaite MS eli tässä esimerkissä GSM-matkapuhelin, jotka on yhdistetty toisiinsa sähköisesti ennalta valitun tiedonsiirtoyhteyden avulla.  
 20 Tässä esimerkissä tiedonsiirtoyhteys muodostetaan käyttäen Bluetooth -teknologiaa.

Lisäksi kuviossa 2 esitettyyn turvajärjestelmään kuuluu palveluntarjoajan päätelaitteeseen kytketty ensimmäinen turvamoduuli SM1 ja palvelunkäyttäjän päätelaitteeseen kytketty toinen turvamoduuli SM2, jotka turvamoduulit on järjestetty käsittelemään päätelaitteiden välisellä tietoliikenneyhteydellä siirrettävää informaatiota. Tällöin turvamoduulien SM1 ja  
 30 SM2 muisteihin on järjestetty sopivat avaimet ja muut parametrit. Julkisen avaimet voidaan ladata ennalta esimerkiksi erityisiltä tarkoitukseen varatuilta julkisten avainten palvelimilta.

Lisäksi kuviossa 2 esitettyyn turvajärjestelmään kuuluu palveluntarjoajan palvelin 8. Ensimmäinen turvamoduuli on yhdistetty tietoliikenneverkon, tässä esimerkissä puhelinverkon, välityksellä palveluntarjo-

ajan palvelimeen 8. Tällöin palvelunkäyttäjän päätelaitteella suoritettut toiminnot voidaan päivittää ja tallentaa palvelimelle. Toisaalta palveluntarjoajan päätelaite SP ja palvelin 8 voivat olla fyysisesti sama asia.

Kuviossa kolme esitetään kaaviomaisesti eräs edullinen keksinnön mukainen matkaviestin. Kuviossa 3 esitettyyn matkaviestimeen kuuluu näppäimistö (9), näyttö 10, radio-osa 11 ja tehrolähde 12 ja luonnollisesti muut tarpeelliset osat, joita tässä ei mainita. Teholähteeseen 12 on integroitu turvamoduuli SM, johon kuuluu, kuten edellä, salaussäilyneet 2 turvamoduulin sähköisen tiedonsiirron salaamiseksi, salauksen purkamiseksi ja sähköisen allekirjoituksen toteuttamiseksi ja ensimmäinen liityntärajapinta RP1 turvamoduulin yhdistämiseksi sähköistä tiedonsiirtoa varten matkaviestimeen MS ja/tai ulkoiseen laitteeseen SP.

Edullisesti turvamoduuli SM on järjestetty käsittelemään matkaviestimellä tietoliikenneverkon ja/tai matkaviestimen paikallisen liitännän 13 kautta välitettävä informaatio. Tällöin myös turvamoduuli voi käyttää hyväkseen matkaviestimen tiedonsiirtoominaisuuksia esimerkiksi siten, että Bluetooth -teknologialla turvamoduuli muodostaa yhteyden ensin matkaviestimeen ja siitä edelleen samalla teknologialla palveluntarjoajan päätelaitteeseen SP.

Vielä esitetään eräs edullinen sovellus turvajärjestelmän, turvamoduulin ja matkaviestimen käytöstä viitaten kuvioon 2. Käyttäjä haluaa ladata pankkitililtään sähköiseen rahalaitteeseensa eli matkaviestimeensä rahaa. Käyttäjä käynnistää matkaviestimen esimerkiksi pankkimoodissa, jolloin turvamoduuli aktivoituu ja aloittaa yhteydenmuodostuksen ympäristössä oleviin toisiin Bluetooth -teknologiaa tukeviin laitteisiin. Tämä voidaan toteuttaa Bluetooth -kuvauksissa määritellyllä tavalla. Kun käyttäjän matkaviestimeen MS kytketty turvamoduuli SM1 ja sen rahakortti- tai

älykorttiosa SC havaitsevat pankin automaatin SP, ne alustavat turvatus yhteyden automaattiin lähettämällä oman julkisen avaimensa ja vastaanottamalla pankin julkisen avaimen. Näin käyttäjän turvamoduuli SM1 ja  
5 automaatin turvamoduuli SM2 voivat käyttää salausta välittäessään keskenään viestejään. Käyttäjä ilmoittaa matkaviestimen MS näppäimistön 9 ja näytön 10 avulla haluamansa lataussumman, joka lähetetään automaattiin SP salattuna. Tämän jälkeen automaatti pyytää vielä  
10 käyttäjän sähköistä allekirjoitusta, jonka käyttäjä antaa turvamoduulinsa SM1 kautta.

Automaatin SP hyväksyttyä latauksen, se lähettää ladattavan summan käyttäjän älykortille SC turvamoduulien SM1 ja SM2 kautta ja päivittää kyseisen  
15 tapahtuman pankin palvelimelle 8. Vaikka tässä ei kuvatakaan, on selvää, että edellä kuvattua toimintoa voidaan muunneltuna sovittaa useisiin -erilaisiin palvelu- ja myyntiautomaattitoimintoihin.

Keksintöä ei rajata pelkästään edellä esitettyjä sovellusesimerkkejä koskevaksi, vaan monet muunnokset ovat mahdollisia pysyttäessä patenttivaatimusten määrittelymään keksinnöllisen ajatuksen puitteissa.  
20

## PATENTTIVAATIMUKSET

1. Turvamoduuli, johon kuuluu kytkentävälineet (1) turvamoduulin yhdistämiseksi päätelaitteeseen (SP), kuten matkaviestimeen, kassapääätteeseen, pankkiautomaattiin tai vastaavaan, tunnettu siitä, että turvamoduuliin kuuluu

salausvälineet (2) turvamoduulin sähköisen tiedonsiirron salaamiseksi, salauksen purkamiseksi ja sähköisen allekirjoituksen toteuttamiseksi;

ensimmäinen liityntäraajapinta (RP1) turvamoduulin yhdistämiseksi langatonta sähköistä tiedonsiirtoa varten ulkoiseen laitteeseen, ja

teholähde (3) tehonsyötön järjestämiseksi turvamoduulin tehoa tarvitseville osille.

2. Patenttivaatimuksen 1 mukainen turvamoduuli, tunnettu siitä, että salausvälineisiin kuuluu prosessori (4), joka salaa, purkaa salauksen ja toteuttaa sähköisen allekirjoituksen, ja muisti (5), joka on yhdistetty prosessoriin sen tarvitsemien avaimien ja parametrien tallentamiseksi.

3. Patenttivaatimuksen 1 tai 2 mukainen turvamoduuli, tunnettu siitä, että turvamoduuliin kuuluu älykorttiosa (SC), joka on järjestetty älykorttitoimintojen toteuttamiseksi turvamoduulilla.

4. Jonkin edeltävistä patenttivaatimuksista 1 - 3 mukainen turvamoduuli, tunnettu siitä, että ensimmäisen liityntäraajapinta on toteutettu Bluetooth-tekniologialla.

5. Jonkin edeltävistä patenttivaatimuksista 1 - 4 mukainen turvamoduuli, tunnettu siitä, että turvamoduuliin kuuluu runko (6), joka on sovitettu vastaamaan matkaviestimen tehonlähteen muotoja, ja liittin (7), joka on yhdistetty runkoon, turvamoduulin kytkemiseksi matkaviestimeen olennaisesti matkaviestimen tehonlähteen paikalle ja tehon syöttämiseksi tehonlähteestä (3) matkaviestimelle.

6. Turvajärjestelmä, johon kuuluu palveluntarjoajan päätelaite (SP) ja palvelunkäyttäjän päätelaite (MS), jotka on yhdistetty toisiinsa sähköisesti ennalta valitun tiedonsiirtoyhteyden avulla, t u n n e t t u siitä, että turvajärjestelmään kuuluu palveluntarjoajan päätelaitteeseen kytketty ensimmäinen turvamoduuli (SM1) ja palvelunkäyttäjän päätelaitteeseen kytketty toinen turvamoduuli (SM2), jotka turvamoduulit on järjestetty käsittelemään päätelaitteiden välisellä tietoliikenneyhteydellä siirrettävää informaatiota; ja että ensimmäiseen ja toiseen turvamoduuliin kuuluu

salausvälineet (2) turvamoduulin sähköisen tiedonsiirron salaamiseksi, salauksen purkamiseksi ja sähköisen allekirjoituksen toteuttamiseksi;

ensimmäinen liityntärajapinta (RP1) turvamoduulin yhdistämiseksi sähköistä tiedonsiirtoa varten päätelaitteeseen, ja

teholähde (3) tehonsyötön järjestämiseksi turvamoduulin tehoa tarvitseville osille.

7. Patenttivaatimuksen 6 mukainen turvajärjestelmä, t u n n e t t u siitä, että palveluntarjoajan päätelaite (SP1) on pankkiautomaatti, kassa, myyntiautomaatti tai vastaava.

8. Patenttivaatimuksen 6 tai 7 mukainen turvajärjestelmä, t u n n e t t u siitä, että palvelunkäyttäjän päätelaite (SP2) on matkaviestin, kannettava tietokone tai vastaava.

9. Jonkin edeltävistä patenttivaatimuksista 6 - 8 mukainen turvajärjestelmä, t u n n e t t u siitä, että turvajärjestelmään kuuluu palveluntarjoajan palvelin (8); ja että ensimmäinen turvamoduuli on yhdistetty tietoliikenneverkon välityksellä palveluntarjoajan palvelimeen (8) palvelunkäyttäjän päätelaitteella suoritettujen toimintojen päivittämiseksi ja tallentamiseksi palvelimelle.

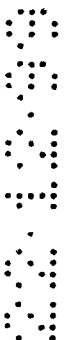
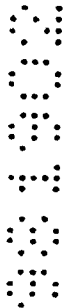
10. Matkaviestin, johon kuuluu näppäimistö (9), näyttö (10), radio-osa (11) ja teholähde (12), tunnettu siitä, että teholähteeseen on integroitu turvamoduuli (SM), johon kuuluu

5           salausvälineet (2) turvamoduulin sähköisen tiedonsiirron salaamiseksi, salauksen purkamiseksi ja sähköisen allekirjoituksen toteuttamiseksi; ja

          ensimmäinen liityntärajapinta (RP1) turvamoduulin yhdistämiseksi sähköistä tiedonsiirtoa varten  
10 matkaviestimeen (MS) ja/tai ulkoiseen laitteeseen (SP).

          11. Patenttivaatimuksen 10 mukainen matkaviestin, tunnettu siitä, että turvamoduuli (SM) on järjestetty käsittelemään matkaviestimellä tietoliikenneverkon ja/tai matkaviestimen paikallisen liitännän (13) kautta välitettävä informaatio.

          12. Patenttivaatimuksen 10 tai 11 mukainen matkaviestin, tunnettu siitä, että turvamoduuli (SM) on järjestetty kommunikoidaan matkaviestimen (MS)  
20 ja/tai palveluntarjoajan päätelaitteen (SP) kanssa Bluetooth -teknologialla.



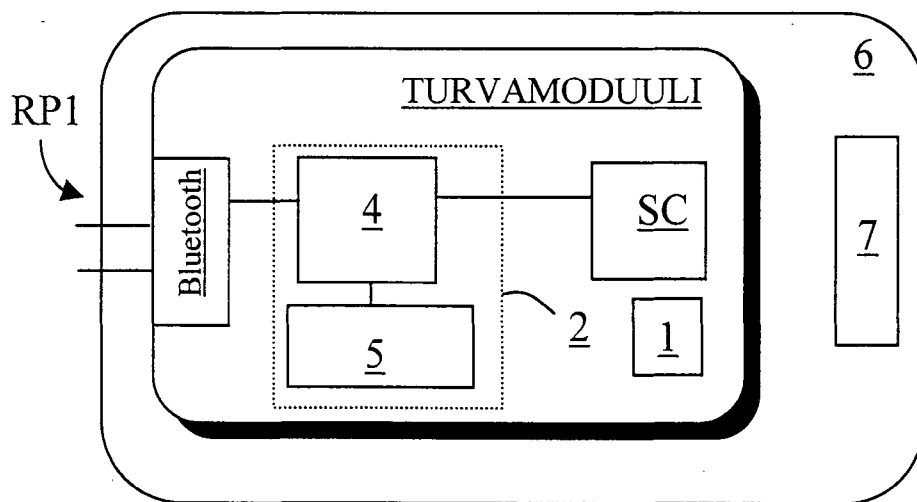


Fig. 1

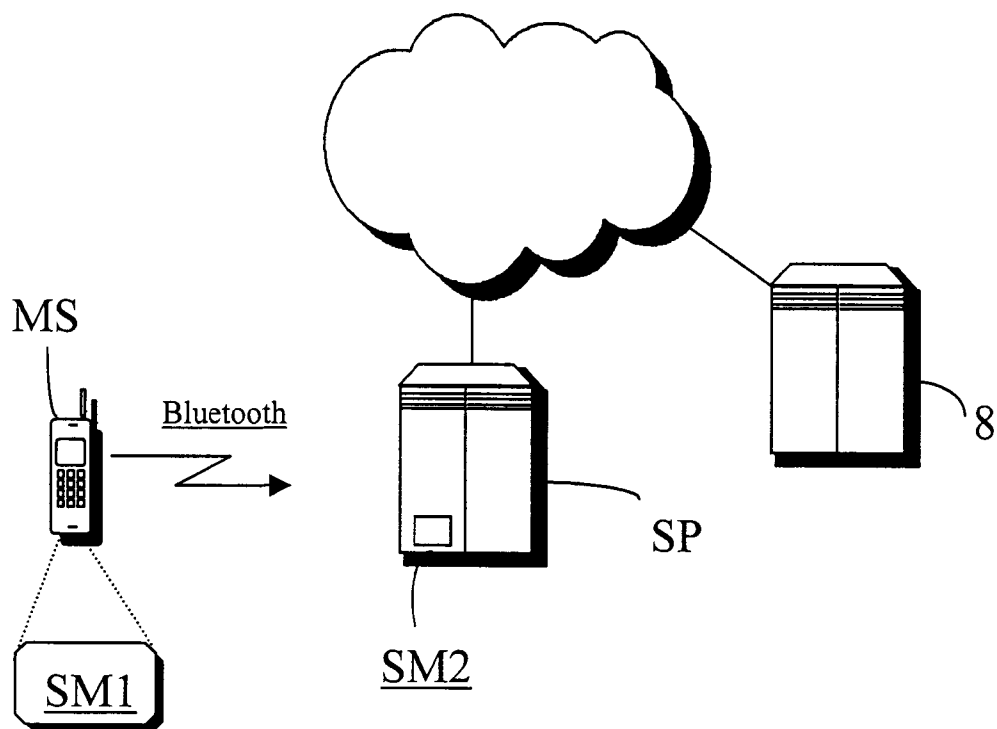


Fig. 2

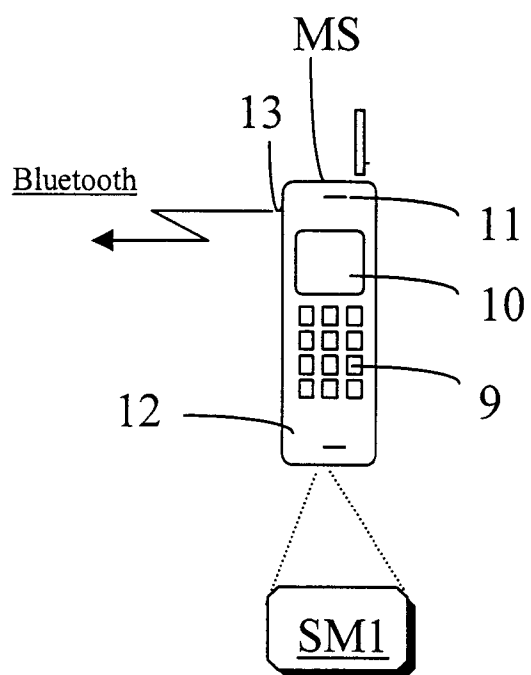


Fig. 3

|                                |                 |
|--------------------------------|-----------------|
| <b>PATENTTIHAKEMUS<br/>NRO</b> | <b>LUOKITUS</b> |
| 981902                         | H04K 1/00       |

|                                                                                                     |
|-----------------------------------------------------------------------------------------------------|
| <b>TUTKITTU AINEISTO</b>                                                                            |
| <b>Patenttijulkaisukokoelma (FI, SE, NO, DK, DE, CH, EP, WO, GB, US), tutkitut luokat</b><br>H04K 1 |
| <b>Tiedonhaut ja muu aineisto</b><br>WPI, USCLAIMS, JAPIO, INSPEC, EPOQUE 2                         |

|                                                                                                                                                                                                                                                                                                                |                                 |                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|---------------------------|
| <b>VIITEJULKAISUT</b>                                                                                                                                                                                                                                                                                          |                                 |                           |
| <b>Kategoria<sup>*)</sup></b>                                                                                                                                                                                                                                                                                  | <b>Julkaisun tunnistetiedot</b> | <b>Koskee vaatimuksia</b> |
| X                                                                                                                                                                                                                                                                                                              | US A 5 742 756 (H04K 1/00)      | 1                         |
| A                                                                                                                                                                                                                                                                                                              | - “ -                           | 6, 10                     |
| P,A                                                                                                                                                                                                                                                                                                            | WO A 98/01848 (G07F 7/08)       | 1,6,10                    |
| A                                                                                                                                                                                                                                                                                                              | WO A 98/16080 (H04Q 7/38)       | 1,6,10                    |
| A                                                                                                                                                                                                                                                                                                              | FI A 956022 (H04Q 7/32)         | 1,6,10                    |
| A                                                                                                                                                                                                                                                                                                              | DE A 197 32 762 (G07F 7/08)     | 1,6,10                    |
| A                                                                                                                                                                                                                                                                                                              | DE A 195 26 730 (H04M 1/00)     | 10                        |
| <sup>*)</sup> X Patentoitavuuden kannalta merkittävä julkaisu yksinään tarkasteltuna<br>Y Patentoitavuuden kannalta merkittävä julkaisu, kun otetaan huomioon tämä ja yksi tai useampi samaan kategoriaan kuuluva julkaisu<br>A Yleistä tekniikan tasoa edustava julkaisu, ei kuitenkaan patentoitavuuden este |                                 |                           |
| <b>Päiväys</b><br>22.6.1999                                                                                                                                                                                                                                                                                    | <b>Tutkija</b><br>Juha Jukanen  |                           |