FI000120174B

(12) PATENTTIJULKAISU
PATENTSKRIFT

(10) FI 120174 B

(45) Patentti myönnetty - Patent beviljats 15.07.2009

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

H04L 9/30 (2006.01)

(21) Patenttihakemus - Patentansökning 20045089

(22) Tekemispäivä - Ingivningsdag 19.03.2004

(24) Alkupäivä - Löpdag 19.03.2004

(41) Tullut julkiseksi - Blivit offentlig 20.09.2005

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 • **Honkanen, Jukka-Pekka,** Pyynikintie 23 A 13, 33230 Tampere, SUOMI - FINLAND, (FI)
2 • **Mikkonen, Jouni,** Kotimäenkatu 5, 33820 Tampere, SUOMI - FINLAND, (FI)
3 • **Haverinen, Henry,** Riuttamäentie 77, 41120 Puuppola, SUOMI - FINLAND, (FI)

(74) Asiamies - Ombud

Tampereen Patenttitoimisto Oy, Hermiankatu 1 B, 33720 Tampere

(54) Keksinnön nimitys - Uppfinningens benämning

Tietojen tallentaminen laitteen yhteydessä
Lagring av information i samband med en anordning

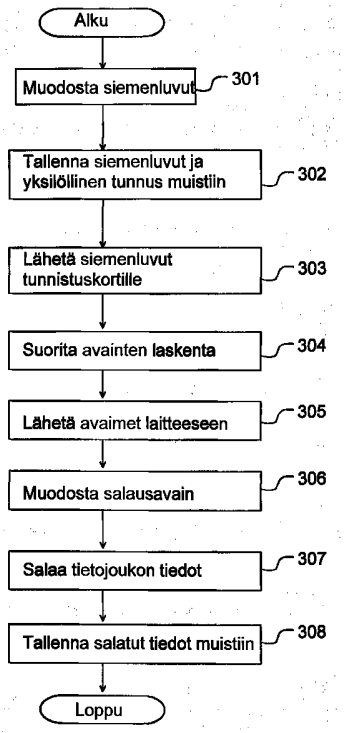
(56) Viitejulkaisut - Anförda publikationer

EP 1059761 A1, US 2001041593 A1, WO 99/25086 A2

(57) Tiivistelmä - Sammandrag

Keksintö kohdistuu menetelmään tietojen tallentamiseksi elektroniikkalaitteen (1) muistiin (1.2), jossa suoritetaan tallennettavien tietojen salaaminen salausavaimella (Ks). Elektroniikkalaitteen (1) yhteyteen on asennettu tunnistuskortti (2), johon on muodostettu kryptografinen algoritmi ja yksilöllinen tunnus (ID). Elektroniikkalaitteessa (1) muodostetaan ainakin yksi siemenarvo (RAND1, RAND2, RAND3), ja välitetään mainittu ainakin yksi siemenarvo tunnistuskortille (2). Tunnistuskortilla (2) suoritetaan mainittu kryptografinen algoritmi, jonka syötteenä käytetään mainittua siemenarvoa (RAND1, RAND2, RAND3), jolloin algoritmissa muodostetaan ainakin yksi johdettu arvo(Kc1, Kc2, Kc3). Mainittu ainakin yksi johdettu arvo (Kd, Kc2, Kc3) välitetään elektroniikkalaitteeseen (1), jolloin mainitun salausavaimen (Ks) muodostuksessa käytetään mainittua ainakin yhtä johdettua arvoa (Kc1, Kc2, Kc3). Keksintö kohdistuu myös elektroniikkalaitteeseen (1), moduuliin sekä tietokoneohjelmatuotteeseen.

Uppfinningen avser ett förfarande för att lagra information i ett minne (1.2) av en elektronikanordning, varvid informationen som skall lagras krypteras med en krypteringsnyckel (Ks). I förbindelse med elektronikanordningen (1) har installerats ett identifieringskort (2) som är försett med en kryptografisk algoritm och en individuell identifierare (ID), I elektronikanordningen (1) genereras åtminstone ett frövärde (RAND1, RAND2, RANDS), och sagda åtminstone ett frövärde förmedlas till identifieringskortet (2). På identifieringskortet (2) utförs sagda kryptografiska algoritm, varvid sagda frövärde (RAND1, RAND2, RAND3) används som indata och i algoritmen bildas åtminstone ett härlett värde (Kd, Kc2, Kc3). Sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3) förmedlas till elektronikanordningen (1), varvid sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3) används vid bildningen av sagda krypteringsnyckel (Ks). Uppfinningen avser även en elektronikanordning (1), en modul samt en datorprogramvara.



Tietojen tallentaminen laitteen yhteydessä

Nyt esillä oleva keksintö kohdistuu menetelmään tietojen tallentamiseksi elektroniikkalaitteen muistiin, jossa suoritetaan tallennettavien tietojen salaaminen salausavaimella, ja jonka elektroniikkalaitteen yhteyteen on asennettu tunnistuskortti, johon on muodostettu kryptografinen algoritmi, jossa elektroniikkalaitteessa muodostetaan ainakin yksi siemenarvo, välitetään mainittu ainakin yksi siemenarvo tunnistuskortille, jossa suoritetaan mainittu kryptografinen algoritmi, jonka syötteenä käytetään mainittua siemenarvoa, jolloin kryptografisessa algoritmissa muodostetaan ainakin yksi johdettu arvo. Keksintö kohdistuu lisäksi elektroniikkalaitteeseen, joka käsittää muistia, ja tunnistuskorttiliitännän, ja jonka yhteyteen on asennettu tunnistuskortti, johon on muodostettu kryptografinen algoritmi ja elektroniikkalaitteessa on välineet ainakin yhden siemenarvon muodostamiseksi, välineet mainitun ainakin yhden siemenarvon välittämiseksi tunnistuskortille, jossa on välineet mainitun kryptografisen algoritmin suorittamiseksi, jonka syötteenä on järjestetty käytettäväksi mainittua siemenarvoa, jolloin kryptografisessa algoritmissa on järjestetty muodostettavaksi ainakin yksi johdettu arvo. Keksintö kohdistuu myös moduuliin käytettäväksi elektroniikkalaitteen yhteydessä, joka elektroniikkalaite käsittää muistia, ja tunnistuskorttiliitännän, ja jonka yhteyteen on asennettu tunnistuskortti, johon on muodostettu kryptografinen algoritmi, ja jossa moduulissa on välineet ainakin yhden siemenarvon muodostamiseksi, välineet mainitun ainakin yhden siemenarvon välittämiseksi tunnistuskortille, jossa on välineet mainitun kryptografisen algoritmin suorittamiseksi, jonka syötteenä on järjestetty käytettäväksi mainittua siemenarvoa, jolloin algoritmissa on järjestetty muodostettavaksi ainakin yksi johdettu arvo. Keksintö kohdistuu vielä tietokoneohjelmatuotteeseen, joka käsittää koneellisesti suoritettavissa olevia ohjelmakäskyjä tietojen tallentamiseksi elektroniikkalaitteen muistiin, ja tallennettavien tietojen salaamiseksi salausavaimella, ja jonka elektroniikkalaitteen yhteyteen on asennettu tunnistuskortti, johon on muodostettu kryptografinen algoritmi.

Nykyisissä kannettavissa elektronisissa laitteissa voidaan säilyttää monenlaista tietoa. Osa tiedoista voi olla luonteeltaan sellaisia, että käyttäjä ei toivo niiden joutuvan tuntemattomien tietoon. Tätä varten on tarpeen salata jollakin tavalla kyseisiä tietoja. Tällaisia tietoja voivat olla mm. käyttäjätunnukset, salasanat, osoitteet, henkilökohtaiset tiedot, asiakasrekisterit, sovellusohjelmat, tietokannat jne. Nykyiset tietojen salausmenetelmät perustuvat yleensä salasanaan. Lisäksi voi olla mahdollista siirtää salatut tiedot toiseen laitteeseen ja avata ne myös siellä, jos oikea salasana on saatu tietoon. Joissakin laitteissa voidaan käyttää laitteistolla suoritettavaa tietojen salaamista, jolloin laitteessa on tarvittavat toiminnot tietojen salassa pitämiseksi. Kaikissa laitteissa tällaisen järjestelyn toteuttaminen ei kuitenkaan ole mahdollista tai järkevää, jolloin voidaan mahdollisesti käyttää ohjelmallisesti toteutettua salausta. Ohjelmallisessa salauksessa käytetään jotakin salausalgoritmia, johon esim. laitteen käyttäjä syöttää salausavaimen (salasanan), minkä jälkeen salausalgoritmilla suoritetaan tietojen salaaminen. Salattujen tietojen salauksen purkaminen voidaan tällöin toteuttaa vastaavasti salauksen purkuavaimella ja salauksen purkavalla algoritmilla. Symmetrisessä salauksessa salausavain ja salauksen purkuavain ovat samat kuten usein myös salausalgoritmi ja salauksen purkava algoritmi. Epäsymmetrisessä salauksessa sen sijaan käytetään eri avainta salauksessa ja salauksen purkamisessa.

Tyypillisesti käyttäjät valitsevat turvallisuusmielessä huonoja salasanoja, jotka on helppo muistaa, mutta samalla ne ovat haavoittuvia erilaisia hyökkäyksiä vastaan. Lisäksi salasanat ovat usein jonkin kielen mukaisia sanoja, erisnimiä, päiväyksiä tms. Tällöin salasana voi olla selvitettävissä esimerkiksi ns. sanakirjahyökkäyksellä, jossa käytetään yhden tai useamman kielen sanakirjaa ja sieltä löytyviä sanoja kokeilemalla yritetään selvittää oikea salasana. Eräs toinen vaihtoehto salasanan selvittämiseksi on suuren joukon satunnaisia salasanoja kokeileminen (”brute force” –menetelmä). Jos salasanan pituus on vain muutama merkki, saattaa edellä mainittu menetelmä onnistua löytämään oikean salasanan suhteellisen nopeasti nykyisin käytettävissä olevilla tietokoneilla tai vastaavilla.

Patenttihakemusjulkaisussa EP1059761 esitetään menetelmä tiedon salaamiseksi ja salauksen purkamiseksi salausavaimella, joka muodostetaan salattavaksi tarkoitetusta tiedosta käyttämällä salausavaimen generointiarvoa. Tieto salataan salausavaimella ja tallennetaan salausavaimen generointiarvon kanssa ensimmäiseen paikkaan ja alkuperäinen salaamaton tieto toiseen. Salatun tiedon salauksen purkamista varten toimitetaan ensimmäisestä paikasta toiseen salausavaimen generointiarvo, jonka avulla toisessa paikassa tallennetusta tiedosta muodostetaan salausavain, joka toimitaan ensimmäiseen paikkaan salauksen purkamiseksi.

Kansainvälinen hakemusjulkaisu WO 99/25086 esittää kaksi menetelmää salausavaimen generoimiseksi salausalgoritmia varten kahden eri laitteen välillä siirrettävien tietojen salaamisessa. Ensimmäisessä menetelmässä käytetään matkaviestimen SIM-korttia, johon välitetään matkaviestinverkossa generoitu siemenluku. SIM-kortti laskee tallennetulla algoritmilla salausavaimen käyttämällä syötteenä siemenlukua sekä SIM-kortille tallennettua tilaajan tunnistusavainta tai lasketaan salausavain toisella algoritmilla käyttämällä ensimmäisessä laskentavaiheessa muodostettu arvoa sekä tilaajan tunnistusavainta.

Nyt esillä olevan keksinnön eräänä tarkoituksena on aikaansaada parannettu tietojen salaaminen elektroniikkalaitteen yhteydessä. Keksintö perustuu siihen ajatukseen, että käytetään salausavaimen muodostamisessa tunnistuskorttia, jossa on tallennettuna salausalgoritmi. Täsmällisemmin ilmaistuna nyt esillä olevan keksinnön mukaiselle menetelmälle on pääasiassa tunnusomaista se, että elektroniikkalaitteessa muodostetaan ainakin yksi siemenarvo, välitetään mainittu ainakin yksi siemenarvo tunnistuskortille, jossa suoritetaan mainittu kryptografinen -algoritmi, jonka syötteenä käytetään mainittua siemenarvoa, jolloin algoritmissa muodostetaan ainakin yksi johdettu arvo, ja välitetään mainittu ainakin yksi johdettu arvo elektroniikkalaitteeseen, jolloin mainitun salausavaimen muodostuksessa käytetään mainittua ainakin yhtä johdettua arvoa, ja että elektroniikkalaitteeseen on tallennettu yksi tai useampia tietojoukkoja, ja tietojoukon yhteyteen on tallennettu tieto yksilöivästä tunnuksesta, jolloin tietojen salauksen purkamisvaiheessa

etsitään mainituista yhdestä tai useammasta tietojoukosta se, jonka yksilöivä tunnus vastaa tunnistuskortille tallennettua sisäistä avainta, ja mikäli tietojoukko löytyi, suoritetaan löydetyn tietojoukon tietojen salauksen purkaminen käyttämällä mainittua salausavainta. Nyt esillä olevan keksinnön mukaiselle elektroniikkalaitteelle on pääasiassa tunnusomaista se, että elektroniikkalaitteessa on välineet ainakin yhden siemenarvon muodostamiseksi, välineet mainitun ainakin yhden siemenarvon välittämiseksi tunnistuskortille, jossa on välineet mainitun kryptografisen algoritmin suorittamiseksi, jonka syötteenä on järjestetty käytettäväksi mainittua siemenarvoa, jolloin algoritmissa on järjestetty muodostettavaksi ainakin yksi johdettu arvo, ja elektroniikkalaitteessa on välineet mainitun ainakin yhden johdetun arvon vastaanottamiseksi, ja välineet mainitun ainakin yhden johdetun arvon käyttämiseksi mainitun salausavaimen muodostuksessa, ja että elektroniikkalaitteeseen on tallennettu yksi tai useampia tietojoukkoja, ja tietojoukon yhteyteen on tallennettu tieto sisäisestä avaimesta, jolloin elektroniikkalaite käsittää etsimisvälineet mainituista yhdestä tai useammasta tietojoukosta sen tietojoukon etsimiseksi, jonka yksilöivä tunnus vastaa tunnistuskortille tallennettua sisäistä avainta tietojoukon tietojen salauksen purkamiseksi. Keksinnön mukaiselle moduulille on pääasiassa tunnusomaista se, että moduulissa on välineet ainakin yhden siemenarvon muodostamiseksi, välineet mainitun ainakin yhden siemenarvon välittämiseksi tunnistuskortille, jossa on välineet mainitun kryptografisen algoritmin suorittamiseksi, jonka syötteenä on järjestetty käytettäväksi mainittua siemenarvoa, jolloin algoritmissa on järjestetty muodostettavaksi ainakin yksi johdettu arvo, ja moduulissa on välineet mainitun ainakin yhden johdetun arvon vastaanottamiseksi, ja välineet mainitun ainakin yhden johdetun arvon käyttämiseksi mainitun salausavaimen muodostuksessa, ja että elektroniikkalaitteeseen on tallennettu yksi tai useampia tietojoukkoja, ja tietojoukon yhteyteen on tallennettu tieto sisäisestä avaimesta, jolloin moduuli käsittää etsimisvälineet mainituista yhdestä tai useammasta tietojoukosta sen tietojoukon etsimiseksi, jonka yksilöivä tunnus vastaa tunnistuskortille tallennettua sisäistä avainta tietojoukon tietojen salauksen purkamiseksi. Keksinnön mukaiselle ohjelmatuotteelle on vielä pääasiassa tunnusomaista se, että tietokoneohjelmatuote käsittää koneellisesti suoritettavissa olevia ohjelmakäskyjä:

- mainitun ainakin yhden johdetun arvon vastaanottamiseksi tunnistuskortilta, ja

mainitun ainakin yhden johdetun arvon käyttämiseksi mainitun salauksen purkuavaimen muodostuksessa,

johon elektroniikkalaitteeseen on tallennettu yksi tai useampia tietojoukkoja, ja tietojoukon yhteyteen on tallennettu tieto yksilöivästä tunnuksesta, jolloin tietokoneohjelmatuote käsittää lisäksi koneellisesti suoritettavissa olevia ohjelmakäskyjä:

- tietojen salauksen purkamisvaiheessa sen tietojoukon etsimiseksi mainituista yhdestä tai useammasta tietojoukosta, jonka yksilöivä tunnus vastaa tunnistuskortille tallennettua sisäistä avainta, ja
- löydetyn tietojoukon tietojen salauksen purkamiseksi käyttämällä mainittua salausavainta.

Keksinnöllä saavutettavia etuja ovat mm. seuraavat. Keksinnön mukainen salausjärjestely mahdollistaa suhteellisen luotettavan tietojen salauksen sellaisessakin elektroniikkalaitteessa, jossa ei ole laitteistopohjaista tietojen salausta käytettävissä. Keksinnön mukainen salaus on erittäin hankala purkaa ilman salauksessa käytetyn tunnistuskortin asentamista elektroniikkalaitteen yhteyteen. Keksinnöllä on mahdollista estää myös luvattomasti toiseen elektroniikkalaitteeseen kopioitujen salattujen tietojen salauksen purkaminen tässä toisessa elektroniikkalaitteessa. Keksinnön mukaisessa salausjärjestelyssä on mahdollista käyttää vahvoja, riittävän pitkiä salausavaimia, jolloin salauksen purkaminen voi olla käytännössä lähes mahdotonta. Keksinnön etuna on myös se, että salausjärjestelyn toteuttamisessa voidaan käyttää nykyisiä tunnistuskortteja kuten matkaviestimien SIM-kortti (Subscriber Identity Module), joissa on jo olemassa ominaisuudet salausavainten muodostamiseksi siemenluvuista. Keksinnön mukaisen salauksen käyttö ei kuitenkaan vaadi mitään toimenpiteitä siltä taholta, jolta tunnistuskortti on hankittu, vaikka käytettäisiin olemassa olevia tunnistuskortteja.

Keksintöä selostetaan seuraavassa tarkemmin viitaten samalla oheisiin piirustuksiin, joissa

kuva 1 esittää keksinnön erään suoritusmuodon mukaista elektroniikkalaitetta pelkistettynä lohkokaaviona, ja

kuva 2 esittää keksinnön erään suoritusmuodon mukaisen elektroniikkalaitteen yhteydessä käytettävää tunnistuskorttia pelkistettynä lohkokaaviona, ja

kuva 3a esittää keksinnön erään suoritusmuodon mukaisen menetelmän tietojen salaamiseksi eri vaiheita pelkistettynä vuokaaviona, ja

kuva 3b esittää keksinnön erään suoritusmuodon mukaisen menetelmän salattujen tietojen purkamiseksi eri vaiheita pelkistettynä vuokaaviona.

Nykyisissä matkaviestinjärjestelmissä, kuten GSM-järjestelmässä, käytetään matkaviestinjärjestelmän mukaisten langattomien viestintälaitteiden tunnistamisessa tunnistekorttina ns. SIM-korttia (Subscriber Identity Module), johon on tallennettu käyttäjäkohtaista tietoa. Matkaviestinjärjestelmässä tätä SIM-kortin sisältämää tietoa käytetään langattomien viestintälaitteiden tunnistamiseksi ja väärinkäytösten estämiseksi. Tunnistekortille on tallennettu salausavainten muodostusalgoritmi, joka GSM-järjestelmässä on ns. A8-algoritmi. Tunnistuskortille on lisäksi tallennettu tunnistuskorttikohtainen sisäinen avain Ki. Matkaviestin syöttää tunnistuskortille ns. siemenluvun (siemenarvon) RAND, jonka se on saanut GSM-verkosta. Siemenluvun valitsee GSM-verkon tunnistuskeskus (Authentication Centre, AuC), ja siemenluku on yleensä valesatunnaisluku. Tunnistuskortilla siemenluku ja tunnistuskorttikohtainen avain Ki syötetään salausavainten muodostusalgoritmiin A8, jolla muodostetaan istuntokohtainen salausavain Kc. Salausavainta Kc matkaviestin käyttää salatessaan tukiasemalle lähetettävää tietoa sekä purkaessaan tukiasemalta vastaanotetun salatun tiedon salauksen. Mainittakoon tässä yhteydessä se, että edellä mainittu siemenluku ei välttämättä ole numeerinen tieto vaan se voi olla muunkinlainen merkkijono.

Seuraavassa keksintöä selostetaan käyttämällä esimerkkinä elektroniikkalaitteesta 1 GSM-matkaviestinjärjestelmän matkaviestintä ja tunnistuskortista 2 GSM-matkaviestimen SIM-korttia, mutta on selvää, että keksintöä ei ole rajoitettu ainoastaan GSM-matkaviestimissä käytettäväksi, vaan keksintöä voidaan soveltaa lukuisissa erilaisissa elektroniikkalaitteissa, joiden yhteydessä voidaan käyttää jotakin tunnistuskorttia. Kuvan 1 mukainen elektroniikkalaite 1 käsittää mm. ohjauslohkon 1.1 elektroniikkalaitteen 1 toimintojen ohjaamiseksi. Lisäksi elektroniikkalaitteessa 1 on muistia 1.2 tietojen, ohjelmien yms. tallentamiseksi, tunnistuskorttiliitäntä 1.3 tunnistuskortin 2 liittämiseksi elektroniikkalaitteen 1 yhteyteen, matkaviestinvälineet 1.4 sekä käyttöliittymä 1.5. Elektroniikkalaitteen muistista 1.2 voidaan varata muistialue salattujen tietojen tallentamista varten.

Kuvassa 2 on esitetty eräs esimerkki tunnistuskortista 2, joka tässä esimerkissä on SIM-kortti. Tunnistuskortti 2 käsittää myös ohjauslohkon 2.1 tunnistuskortin 2 toimintojen ohjaamiseksi ja muistia 2.2 tietojen ja ohjelmakoodien tallentamiseksi. Muistiin 2.2 on tallennettu mm. algoritmi eli käytännössä ohjelmakäskyjä algoritmin mukaisen laskennan suorittamiseksi. Muistiin 2.2 on tallennettu myös yksilöllinen tunnus ID, kuten käyttäjän kansainvälinen matkaviestintilaajatunnus IMSI. Tunnistuskortissa 2 on vielä liitäntä 2.3, jonka välityksellä tietoja voidaan välittää elektroniikkalaitteen 1 ja tunnistuskortin 2 välillä. Lisäksi liitännän 2.3 kautta voidaan välittää tunnistuskortille 2 sen tarvitsema käyttöjännite.

On selvää, että tunnistuskorttia 2 ei välttämättä tarvitse liittää elektroniikkalaitteeseen 1 fyysisesti, vaan voidaan käyttää myös langatonta tiedonsiirtoa elektroniikkalaitteen 1 ja tunnistuskortin 2 välillä keksinnön toimintaperiaatteiden pysyessä silti pääpiirteissään samankaltaisina. Tällöin elektroniikkalaitteen 1 tunnistuskorttiliitäntä 1.3 ja tunnistuskortin liitäntä 2.3 käsittävät langattoman tiedonsiirron mahdollistavat lähetinvastaanottimet sinänsä tunnetusti.

Seuraavaksi kuvataan keksinnön erään suoritusmuodon mukaisen menetelmän eri vaiheita viitaten samalla kuvan 3a vuokaavioon. Siinä vaiheessa kun on tarve suorittaa tietojen salaaminen, muodostetaan elektroniikkalaitteessa 1 yksi tai useampi siemenluku, esimerkiksi kolme siemenlukua RAND1, RAND2, RAND3, jotka ovat satunnaislukuja tai valesatunnaislukuja. Tätä esittää lohko 301 kuvan 3a vuokaaviossa. Siemenluvut voidaan muodostaa usealla eri periaatteella siten, että siemenluvut ovat mahdollisimman satunnaisia. Muodostetut siemenluvut tallennetaan muistiin 1.2, johon tallennetaan myös tunnistuskortilta 2 luettu yksilöllinen tunnus IMSI (lohko 302). Siemenluvut RAND1, RAND2, RAND3 lähetetään 303 elektroniikkalaitteesta 1 tunnistuskortille 2 tunnistuskorttiliitännän 1.3 kautta. Lisäksi elektroniikkalaite 1 lähettää tunnistuskortille 2 komennon algoritmin laskemiseksi tai jollakin muulla tavoin ohjaa tunnistuskorttia 2 suorittamaan algoritmin laskenta kullekin siemenluvulle RAND1, RAND2, RAND3. Tunnistuskortti 2 vastaanottaa siemenluvut ja suorittaa algoritmin laskennan 304 siemenlukuja vastaavien avainten Kc1, Kc2, Kc3 muodostamiseksi. Algoritmina on esim. GSM-järjestelmässä käytettävä A8-algoritmi. Algoritmin laskennassa käytetään siemenluvun lisäksi yksilöllistä sisäistä avainta Ki, joka on tallennettu tunnistuskortin muistiin 2.2. GSM-verkon tunnistuskeskuksessa AuC on tallennettuna kutakin tilaajatunnusta (IMSI) vastaava sisäinen avain Ki, joten tunnistuskeskus osaa käyttää kullekin tilaajalle oikeaa sisäistä avainta Ki. Laskenta suoritetaan esimerkiksi tunnistuskortin 2 ohjauslohkossa 2.1. Laskennan tuloksena saadaan kutakin siemenlukua kohden yksi avain, tässä esimerkissä siis kolme avainta Kc1, Kc2, Kc3. Kukin avain Kc1, Kc2, Kc3 lähetetään 305 elektroniikkalaitteeseen 1. Elektroniikkalaitteessa 1 näitä avaimia Kc1, Kc2, Kc3 käytetään tietojen salaamisessa käytettävän salausavaimen Ks muodostamisessa 306 esim. yksisuuntaisen funktion avulla. Tämä yksisuuntainen funktio muodostaa avainten Kc1, Kc2, Kc3, yksilöllisen tunnuksen ID ja mahdollisesti käyttäjän syöttämän salasanan avulla salausavaimen Ks. Tämän jälkeen tietojen salaamien voidaan suorittaa esim. seuraavasti.

Tallennettavat tiedot syötetään salausalgoritmiin, jossa salausavaimen Ks avulla muodostetaan 307 salattu tietojoukko eli suoritetaan tietojou-

kon tietojen salaaminen. Salausalgoritmina on esim. symmetrinen salausalgoritmi, jolloin alkuperäiset tiedot saadaan selville käyttämällä salauksen purkamiseen samaa avainta Ks. Salatut tiedot tallennetaan 308 elektroniikkalaitteen 1 muistiin 1.3. Lisäksi näiden tietojen yhteyteen tallennetaan tieto siemenluvuista sekä yksilöllisestä tunnuksesta. Siemenluvut sekä yksilöllinen tunnus voidaan tarvittaessa tallentaa salattuna esim. käyttäjän määrittämän salasanan avulla. Tietojen tallentamisessa voidaan tarvittaessa käyttää hyväksi elektroniikkalaitteen 1 käyttöjärjestelmätoimintoja, mikäli elektroniikkalaitteessa 1 on tällainen asennettuna. Käyttöjärjestelmätoiminnoissa on tavallisesti tiedostonhallintatoiminnot, jolloin tietojoukko voidaan tallentaa tiedostoksi käyttöjärjestelmän huolehtiessa tiedoston tallennustoiminnosta. Tiedosto voidaan vastaavasti noutaa käsiteltäväksi tiedostotoimintojen avulla. Jos käyttäjän salasanalla salataan vain siemenluvut, on etuna se, että jälkeenpäin käyttäjän määrittämää salasanaa ei voida selvittää ns. brute force tai sanakirjahyökkäyksillä, koska salattavat siemenluvut ovat satunnaisia. Hyökkääjä ei voi tällöin tarkistaa salasanan arvauksen onnistumista, koska satunnaisista siemenluvuista ei voida suoraan sanoa, onko salauksen purkaminen onnistunut.

Siinä vaiheessa kun elektroniikkalaitteessa 1 on tarve käsitellä salattuja tietoja salaamattomassa muodossa, suoritetaan salauksen purkaminen esim. seuraavasti viitaten samalla kuvan 3b vuokaavioon. Elektroniikkalaitteessa 1 suoritetaan yksilöllisen tunnuksen lukeminen 310 tunnistuskortilta 2 elektroniikkalaitteen muistiin 1.2 tarvittaessa. Tämän jälkeen tutkitaan 311, löytyykö muistista 1.2 kyseistä yksilöllistä tunnusta vastaava tietojoukko, kuten tiedosto. Tietojoukkoa voidaan etsiä sisällön ja/tai otsikkotietojen (esim. tiedoston nimi, jossa voi olla mukana yksilöllinen tunnus) avulla. Kun oikea tietojoukko on löydetty, luetaan 312 tietojoukosta sen salauksen yhteydessä käytetty yksi tai useampi siemenluku RAND1, RAND2, RAND3.

Mikäli tietojoukon tallennuksen yhteydessä on suoritettu siemenlukujen ja mahdollisesti myös yksilöllisen tunnuksen salaus, suoritetaan näiden tietojen salauksen purkaminen. Tätä varten elektroniikkalaite 1 esim.

pyytää käyttäjää syöttämään salasanan, jolla siemenlukujen ja yksilöllisen tunnuksen salaus voidaan purkaa.

Siinä vaiheessa kun yksilöllinen tunnus ja siemenluvut ovat tiedossa, välitetään 313 siemenluvut tunnistuskortille 2 ja suoritetaan tunnistuskortilla 2 siemenlukuja vastaavien avaimien Kc1, Kc2, Kc3 laskenta 314, kuten edellä tietojen salauksen yhteydessä on esitetty. Avaimet Kc1, Kc2, Kc3 välitetään 315 elektroniikkalaitteeseen 1, jossa avainten ja yksilöllisen tunnuksen perusteella muodostetaan 316 tietojoukon salauksen purkuavain salausalgoritmia vastaavalla salauksen purkualgoritmilla. Jos kyseessä on symmetrinen salaus, salausalgoritmina ja salauksen purkualgoritmina käytetään samaa algoritmia.

Mikäli elektroniikkalaitteessa 1 on asennettuna sellainen tunnistuskortti 2, johon tallennettu yksilöllinen tunnus täsmää jonkin tietojoukon yhteyteen tallennettua yksilöllistä tunnusta, voidaan suorittaa tämän tietojoukon tietojen salauksen purkaminen 317, minkä jälkeen tietojoukon tiedot ovat elektroniikkalaitteessa 1 käytettävissä.

Mikäli elektroniikkalaitteessa 1 on asennettuna sellainen tunnistuskortti 2, johon tallennettu yksilöllinen tunnus ei täsmää minkään tietojoukon yhteyteen tallennettua yksilöllistä tunnusta, ei mitään salattua tietojoukkoa tällöin käsitellä ja tiedot pysyvät salassa. Keksinnöllä mahdollistetaan tällä tavoin se, että elektroniikkalaitteessa 1 voidaan tiettyä tunnistuskorttia 2 käyttämällä käsitellä vain sellaisia tämän keksinnön mukaisesti salattua tietojoukkoja, joiden salaus on suoritettu kyseisen tunnistuskortin 2 ollessa asennettuna elektroniikkalaitteen 1 yhteyteen. Keksinnön mukainen järjestely estää myös sen, että mikäli tietojoukko kopioidaan elektroniikkalaitteesta 1 johonkin toiseen elektroniikkalaitteeseen (ei esitetty kuvissa), ei tietojoukon salausta voi purkaa muutoin kuin asentamalla oikea tunnistuskortti 2 tähän toiseen elektroniikkalaitteeseen. Keksinnön erään toisen suoritusmuodon mukaisessa järjestelmässä tämäkin voidaan estää käyttämällä yhtenä salausavaimen Ks muodostustietona elektroniikkalaitteen 1 yksilöllistä laitetunnusta tai vastaavaa. Tämä estää siis suhteellisen tehokkaasti saman tietojoukon tietojen samanaikaisen käytön useammassa elektroniikkalaitteessa 1.

Keksinnön vielä erään suoritusmuodon mukaisessa menetelmässä suoritetaan vielä avainten Kc1, Kc2, Kc3 salaaminen ja tallentaminen tietojoukon yhteyteen tietojoukon salauksen yhteydessä. Tällöin näiden avainten salauksessa käytetään samaa salausavainta Ks, jolla tietojoukon muut vahvalla salauksella salattavaksi tarkoitetut tiedot salataan. Tällöin tietojoukon tietoja käsiteltäessä muodostetaan tunnistuskortilla 2 avaimet Kc1, Kc2, Kc3 ja näiden sekä yksilöllisen tunnuksen perusteella lasketaan salauksen purkuavain, kuten edellä on esitetty. Tämän jälkeen, ennen tietojoukon varsinaisten tietojen salausta, suoritetaan vielä tietojoukkoon salatussa muodossa tallennettujen avainten salauksen purkaminen. Avaimia verrataan tunnistuskortilta 2 luettuihin avaimiin Kc1, Kc2, Kc3 ja mikäli avaimet ovat samat, voidaan tietojoukon muiden tietojen salaus purkaa. Jos avaimet eivät täsmää, on todennäköistä, että tunnistuskortti 2 ei ole sama jota käytettiin tietojoukon tietojen salauksessa. Tällä järjestelyllä voidaan vähentää sitä mahdollisuutta, että joku saisi selville esim. elektroniikkalaitteen 1 toimintaa tutkimalla avaimet Kc1, Kc2, Kc3 siinä vaiheessa, kun avaimia käsitellään salaamattomassa muodossa.

Keksinnössä hyödynnetään siis tunnistuskorttia 2, johon on muodostettu yksi tai useampi algoritmi ja jota tunnistuskorttia 2 ja algoritmia käytetään jossakin muussakin tarkoituksessa, kuten käyttäjän tunnistuksessa matkaviestinverkossa. Keksinnön soveltamiseksi ei esim. matkaviestimen käyttäjän kuitenkaan tarvitse ottaa yhteyttä matkaviestinverkon operaattoriin, vaikka hyödynnettäisiinkin kyseisen operaattorin myöntämää tunnistuskorttia ja siihen tallennettua algoritmia ja muita tunnistustoimintoja. Kyseessä on tässä mielessä operaattorista riippumaton järjestelmä.

Siemenlukujen pituus valitaan siten, että saavutetaan kulloiseenkin sovellukseen riittävän vahva salaus. Toisaalta tunnistuskortti 2 voi määrätä sen, kuinka pitkä ja minkä muotoinen on siemenluvun oltava. Esimerkiksi voidaan käyttää 128-bittistä siemenlukua, mutta keksintöä ei ole rajoitettu ainoastaan 128-bittisten siemenlukujen käyttöön.

Eräässä CDMA-tekniikkaan perustuvassa matkaviestinjärjestelmässä käytetään matkaviestimissä ns. R-UIM –korttia, jolloin myös tämän tyyppistä tunnistuskorttia voidaan käyttää nyt esillä olevan keksinnön yhteydessä. Muina ei-rajoittavina esimerkkeinä tunnistuskorteista mainittakoon vielä UMTS-matkaviestinjärjestelmän USIM-kortti, sähköinen henkilökortti, sekä tunnistuspiirillä varustettu pankkikortti ja luottokortti (ns. sirukortti). Näissä tapauksissa käytetään salausavaimen Ks muodostamiseen jotakin siemenarvosta tunnistuskortilla 2 kryptografisesti muodostettua johdettua arvoa. Kaikissa tapauksissa siemenarvon ei tarvitse olla satunnaisluku, eikä kortilla muodostetun arvon tarvitse olla salausavain. Keksinnön kannalta oleellista on, että elektroniikkalaitteen 1 muodostamasta siemenarvosta voidaan tunnistuskortilla 2 muodostaa joku johdettu arvo, jonka laskemiseen käytetään tunnistuskortille 2 tallennettua sisäistä avainta Ki. Sisäinen avain Ki voi olla symmetrinen avain tai asymmetristä (julkisen avaimen) kryptografiaa käytettäessä sisäinen avain Ki voi olla tunnistuskortille 2 tallennetun avainparin yksityinen avain. Esimerkiksi julkisen avaimen menetelmiä käytettäessä siemenarvona voi toimia joku selväkielinen merkkijono, joka esimerkiksi sisältää elektroniikkalaitteen 1 valitseman satunnaisen tai valesatunnaisen osan. Tämä merkkijono salataan tai allekirjoitetaan tunnistuskortilla 2 käyttämällä tunnistuskortille 2 tallennettua yksityistä avainta. Tunnistuskortin 2 palauttama salattu merkkijono tai digitaalinen allekirjoitus toimii tällöin tunnistuskortilla 2 johdettuna arvona, jota voidaan käyttää edelleen salausavaimen Ks johtamisessa. Tässäkään tapauksessa johdettua arvoa ei voida jälkeenpäin selvittää ilman, että kyseinen tunnistuskortti 2 on käytettävissä, joten elektroniikkalaitteeseen 1 salattuna tallennetut tiedot on tällöin suojattu kopioimiselta ja käytöltä.

Vaikka edellä on esitetty, että salausavain Ks muodostetaan tunnistuskortin 2 muodostaman yhden tai useamman avaimen Kc1, Kc2, K3 ja yksilöllisen tunnuksen ID avulla, voidaan salausavaimen Ks muodostuksessa lisäksi käyttää esim. yksilöllistä laitetunnusta, kuten IMEI (International Mobile Equipment Identifier), elektroniikkalaitteelle 1 mahdollisesti muodostettua lähiverkko-osoitetta, kuten WLAN MAC –osoite, langattoman lyhyen kantaman laiteosoitetta, kuten Bluetooth MAC –osoite jne.

Nyt esillä olevan keksinnön mukaiset toiminnot voidaan toteuttaa pääosin ohjelmallisesti elektroniikkalaitteen 1 ohjauslohkon 1.1, kuten suorittimen, ohjelmakomentoina. Keksintö voidaan toteuttaa myös moduulina, joka liitetään elektroniikkalaitteeseen 1 suorittamaan halutut toiminnot.

Lisäksi mainittakoon se, että tässä keksinnössä käytettävän tunnistuskortin 2 ei välttämättä tarvitse olla muodostettu kortin muotoon, vaan tunnistuskortti 2 voi käytännön toteutukseltaan poiketa korttimuodosta.

On selvää, että nyt esillä olevaa keksintöä ei ole rajoitettu ainoastaan edellä esitettyihin suoritusmuotoihin, vaan sitä voidaan muunnella oheisten patenttivaatimusten puitteissa.

Patenttivaatimukset:

1. Menetelmä tietojen tallentamiseksi elektroniikkalaitteen (1) muistiin (1.2), jossa suoritetaan tallennettavien tietojen salaaminen salausavaimella (Ks), ja jonka elektroniikkalaitteen (1) yhteyteen on asennettu tunnistuskortti (2), johon on muodostettu kryptografinen algoritmi, jossa elektroniikkalaitteessa (1) muodostetaan ainakin yksi siemenarvo (RAND1, RAND2, RAND3), välitetään mainittu ainakin yksi siemenarvo tunnistuskortille (2), jossa suoritetaan mainittu kryptografinen algoritmi, jonka syötteenä käytetään mainittua siemenarvoa (RAND1, RAND2, RAND3), jolloin kryptografisessa algoritmissa muodostetaan ainakin yksi johdettu arvo (Kc1, Kc2, Kc3), **tunnettu** siitä, että mainittu ainakin yksi johdettu arvo (Kc1, Kc2, Kc3) välitetään elektroniikkalaitteeseen (1), jolloin salausavaimen (Ks) muodostuksessa käytetään mainittua ainakin yhtä johdettua arvoa (Kc1, Kc2, Kc3), ja että elektroniikkalaitteeseen (1) on tallennettu yksi tai useampia tietojoukkoja, ja tietojoukon yhteyteen on tallennettu tieto yksilöivästä tunnuksesta (ID), jolloin tietojen salauksen purkamisvaiheessa etsitään mainituista yhdestä tai useammasta tietojoukosta se, jonka yksilöivä tunnus vastaa tunnistuskortille (2) tallennettua sisäistä avainta (Ki), ja mikäli tietojoukko löytyi, suoritetaan löydetyn tietojoukon tietojen salauksen purkaminen käyttämällä mainittua salausavainta (Ks).

2. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että tunnistuskortille (2) on muodostettu sisäinen avain (Ki), jolloin mainitun salausavaimen (Ks) muodostuksessa käytetään lisäksi mainittua sisäistä avainta (Ki).

3. Patenttivaatimuksen 2 mukainen menetelmä, **tunnettu** siitä, että mainitun salausavaimen (Ks) muodostuksessa käytetään yksisuuntaista funktiota, johon syötteenä käytetään mainittua yhtä tai useampaa johdettua arvoa (Kc1, Kc2, Kc3) ja sisäistä avainta (Ki).

4. Patenttivaatimuksen 2 tai 3 mukainen menetelmä, **tunnettu** siitä, että elektroniikkalaitteeseen (1) on tallennettu laitekohtainen tunnus,

jolloin mainitun salausavaimen (Ks) muodostuksessa käytetään lisäksi elektroniikkalaitteen (1) laitekohtaista tunnusta.

5. Patenttivaatimuksen 2, 3 tai 4 mukainen menetelmä, **tunnettu** siitä, että tietojoukon tietojen salauksen purkamiseksi muodostetaan salauksen purkuavain (Ks), jonka muodostamiseksi etsitään tietojoukon tiedoista tieto salausvaiheessa käytetystä ainakin yhdestä siemenarvosta (RAND1, RAND2, RAND3), välitetään mainittu ainakin yksi siemenarvo tunnistuskortille (2), jossa suoritetaan mainittu kryptografinen algoritmi, jonka syötteenä käytetään mainittua siemenarvoa (RAND1, RAND2, RAND3) ja mainittua sisäistä avainta (Ki), jolloin kryptografisessa algoritmissa muodostetaan yksi tai useampi johdettu arvo (Kc1, Kc2, Kc3), ja välitetään mainittu ainakin yksi johdettu arvo (Kc1, Kc2, Kc3) elektroniikkalaitteeseen (1), jolloin mainitun salauksen purkuavaimen (Ks) muodostuksessa käytetään mainittua ainakin yhtä johdettua arvoa (Kc1, Kc2, Kc3).

6. Jonkin patenttivaatimuksen 1—5 mukainen menetelmä, **tunnettu** siitä, että tunnistuskorttina (2) käytetään matkaviestinjärjestelmän matkaviestimien tunnistuksessa käytettävää tunnistuskorttia, jolloin mainittuna kryptografisena algoritmina käytetään matkaviestimen tunnistuksessa käytettävää algoritmia.

7. Jonkin patenttivaatimuksen 1—6 mukainen menetelmä, **tunnettu** siitä, että tunnistuskorttina (2) käytetään jotakin seuraavista

- SIM-kortti,
- USIM-kortti,
- R-UIM –kortti,
- sähköinen henkilökortti,
- pankkikortti,
- luottokortti.

8. Jonkin patenttivaatimuksen 1—7 mukainen menetelmä, **tunnettu** siitä, että ainakin osa siemenarvosta (RAND1, RAND2, RAND3) muodostetaan satunnaisesti tai valesatunnaisesti.

9. Elektroniikkalaite (1), joka käsittää muistia (1.2), ja tunnistuskorttiliitännän (1.3), ja jonka yhteyteen on asennettu tunnistuskortti (2), johon on muodostettu kryptografinen algoritmi, ja elektroniikkalaitteessa (1) on välineet (1.1) ainakin yhden siemenarvon (RAND1, RAND2, RAND3) muodostamiseksi, välineet (1.3) mainitun ainakin yhden siemenarvon välittämiseksi tunnistuskortille (2), jossa on välineet (2.1) mainitun kryptografisen algoritmin suorittamiseksi, jonka syötteenä on järjestetty käytettäväksi mainittua siemenarvoa (RAND1, RAND2, RAND3), jolloin kryptografisessa algoritmissa on järjestetty muodostettavaksi ainakin yksi johdettu arvo (Kc1, Kc2, Kc3), **tunnettu** siitä, että elektroniikkalaitteessa (1) on välineet (1.3) mainitun ainakin yhden johdetun arvon (Kc1, Kc2, Kc3) vastaanottamiseksi, ja välineet (1.1) mainitun ainakin yhden johdetun arvon (Kc1, Kc2, Kc3) käyttämiseksi mainitun salausavaimen (Ks) muodostuksessa, ja että elektroniikkalaitteeseen (1) on tallennettu yksi tai useampia tietojoukkoja, ja tietojoukon yhteyteen on tallennettu tieto sisäisestä avaimesta (Ki), jolloin elektroniikkalaite (1) käsittää etsimisvälineet mainituista yhdestä tai useammasta tietojoukosta sen tietojoukon etsimiseksi, jonka yksilöivä tunnus vastaa tunnistuskortille (2) tallennettua sisäistä avainta (Ki) tietojoukon tietojen salauksen purkamiseksi.

10. Patenttivaatimuksen 9 mukainen elektroniikkalaite (1), **tunnettu** siitä, että tunnistuskortille (2) on muodostettu sisäinen avain (Ki), jolloin mainitun salausavaimen (Ks) muodostuksessa on järjestetty käytettäväksi lisäksi mainittua sisäistä avainta (Ki).

11. Patenttivaatimuksen 10 mukainen elektroniikkalaite (1), **tunnettu** siitä, että mainitun salausavaimen (Ks) muodostuksessa on järjestetty käytettäväksi yksisuuntaista funktiota, jonka syötteenä on mainittu yksi tai useampi johdettu arvo (Kc1, Kc2, Kc3) ja sisäinen avain (Ki).

12. Patenttivaatimuksen 10 tai 11 mukainen elektroniikkalaite (1), **tunnettu** siitä, että elektroniikkalaitteeseen (1) on tallennettu laitekohtainen tunnus, jolloin mainitun salausavaimen (Ks) muodostuksessa on järjestetty käytettäväksi lisäksi elektroniikkalaitteen (1) laitekohtaista tunnusta.

13. Patenttivaatimuksen 10, 11 tai 12 mukainen elektroniikkalaite (1), **tunnettu** siitä, että se käsittää välineet (1.1) salauksen purkuavaimen muodostamiseksi käytettäväksi tietojoukon tietojen salauksen purkamisessa, välineet tiedon salausvaiheessa käytetystä ainakin yhdestä siemenarvosta (RAND1, RAND2, RAND3) etsimiseksi tietojoukon tiedoista, välineet (1.3) mainitun ainakin yhden siemenarvon välittämiseksi tunnistuskortille (2), jossa on järjestetty suoritettavaksi mainittu kryptografinen algoritmi, jonka syötteenä on järjestetty käytettäväksi mainittua siemenarvoa (RAND1, RAND2, RAND3) ja mainittua sisäistä avainta (Ki), jolloin algoritmissa on järjestetty muodostettavaksi yksi tai useampi johdettu arvo (Kc1, Kc2, Kc3), jolloin elektroniikkalaitteessa (1) on välineet (1.3) mainitun ainakin yhden johdetun arvon (Kc1, Kc2, Kc3) vastaanottamiseksi tunnistuskortilta (2), jolloin mainitun salauksen purkuavaimen (Ks) muodostuksessa on järjestetty käytettäväksi mainittua yhtä tai useampaa johdettua arvoa (Kc1, Kc2, Kc3).

14. Jonkin patenttivaatimuksen 9—13 mukainen elektroniikkalaite (1), **tunnettu** siitä, että tunnistuskorttina (2) on matkaviestinjärjestelmän matkaviestimien tunnistuksessa käytettävä tunnistuskortti, jolloin mainittuna algoritmina on matkaviestimen tunnistuksessa käytettävä algoritmi.

15. Jonkin patenttivaatimuksen 9—14 mukainen elektroniikkalaite (1), **tunnettu** siitä, että tunnistuskorttina (2) on jokin seuraavista

- SIM-kortti,
- USIM-kortti,
- R-UIM –kortti,
- sähköinen henkilökortti,
- pankkikortti,
- luottokortti.

16. Moduuli käytettäväksi elektroniikkalaitteen yhteydessä (1), joka elektroniikkalaite (1) käsittää muistia (1.2), ja tunnistuskorttiliitännän (1.3), ja jonka yhteyteen on asennettu tunnistuskortti (2), johon on

muodostettu kryptografinen algoritmi, ja jossa moduulissa on välineet (1.1) ainakin yhden siemenarvon (RAND1, RAND2, RAND3) muodostamiseksi, välineet (1.3) mainitun ainakin yhden siemenarvon välittämiseksi tunnistuskortille (2), jossa on välineet (2.1) mainitun kryptografisen algoritmin suorittamiseksi, jonka syötteenä on järjestetty käytettäväksi mainittua siemenarvoa (RAND1, RAND2, RAND3), jolloin algoritmissa on järjestetty muodostettavaksi ainakin yksi johdettu arvo (Kc1, Kc2, Kc3), **tunnettu** siitä, että moduulissa on välineet (1.3) mainitun ainakin yhden johdetun arvon (Kc1, Kc2, Kc3) vastaanottamiseksi, ja välineet (1.1) mainitun ainakin yhden johdetun arvon (Kc1, Kc2, Kc3) käyttämiseksi salausavaimen (Ks) muodostuksessa, ja että elektroniikkalaitteeseen (1) on tallennettu yksi tai useampia tietojoukkoja, ja tietojoukon yhteyteen on tallennettu tieto sisäisestä avaimesta (Ki), jolloin moduuli käsittää etsimisvälineet mainituista yhdestä tai useammasta tietojoukosta sen tietojoukon etsimiseksi, jonka yksilöivä tunnus vastaa tunnistuskortille (2) tallennettua sisäistä avainta (Ki) tietojoukon tietojen salauksen purkamiseksi.

17. Tietokoneohjelmatuote, joka käsittää koneellisesti suoritettavissa olevia ohjelmakäskyjä:

- tietojen tallentamiseksi elektroniikkalaitteen (1) muistiin (1.2), ja
- tallennettavien tietojen salaamiseksi salausavaimella (Ks),

ja jonka elektroniikkalaitteen (1) yhteyteen on asennettu tunnistuskortti (2), johon on muodostettu kryptografinen algoritmi, tietokoneohjelmatuote käsittää koneellisesti suoritettavissa olevia ohjelmakäskyjä:

- ainakin yhden siemenarvon (RAND1, RAND2, RAND3) muodostamiseksi,
- tiedon salausvaiheessa käytetystä ainakin yhdestä siemenarvosta (RAND1, RAND2, RAND3) etsimiseksi tietojoukon tiedoista,
- mainitun ainakin yhden siemenarvon välittämiseksi tunnistuskortille (2), jossa on järjestetty suoritettavaksi mainittu kryptografinen algoritmi, jonka syötteenä on järjestetty käytettäväksi mainittua siemenarvoa (RAND1, RAND2, RAND3), jolloin algoritmissa on järjestetty muodostettavaksi ainakin yksi johdettu arvo (Kc1, Kc2, Kc3),

tunnettu siitä, että tietokoneohjelmatuote käsittää koneellisesti suoritettavissa olevia ohjelmakäskyjä:

- mainitun ainakin yhden johdetun arvon (Kc1, Kc2, Kc3) vastaanottamiseksi tunnistuskortilta (2), ja
- mainitun ainakin yhden johdetun arvon (Kc1, Kc2, Kc3) käyttämiseksi mainitun salauksen purkuavaimen (Ks) muodostuksessa,

johon elektroniikkalaitteeseen (1) on tallennettu yksi tai useampia tietojoukkoja, ja tietojoukon yhteyteen on tallennettu tieto yksilöivästä tunnuksesta (ID), jolloin tietokoneohjelmatuote käsittää lisäksi koneellisesti suoritettavissa olevia ohjelmakäskyjä:

- tietojen salauksen purkamisvaiheessa sen tietojoukon etsimiseksi mainituista yhdestä tai useammasta tietojoukosta, jonka yksilöivä tunnus vastaa tunnistuskortille (2) tallennettua sisäistä avainta (Ki), ja
- löydetyn tietojoukon tietojen salauksen purkamiseksi käyttämällä mainittua salausavainta (Ks).

18. Patenttivaatimuksen 17 mukainen tietokoneohjelmatuote, **tunnettu** siitä, että tietojoukon tietojen salauksen purkamiseksi tietokoneohjelmatuote käsittää koneellisesti suoritettavissa olevia ohjelmakäskyjä:

- tietojoukon tiedoista tiedon salausvaiheessa käytetystä ainakin yhdestä siemenarvosta (RAND1, RAND2, RAND3) etsimiseksi,
- mainitun ainakin yhden siemenarvon välittämiseksi tunnistuskortille (2), jossa suoritetaan mainittu kryptografinen algoritmi, jonka syötteenä käytetään mainittua siemenarvoa (RAND1, RAND2, RAND3), jolloin algoritmissa muodostetaan ainakin yksi johdettu arvo (Kc1, Kc2, Kc3),

jolloin tietokoneohjelmatuote käsittää koneellisesti suoritettavissa olevia ohjelmakäskyjä:

- mainitun ainakin yhden johdetun arvon (Kc1, Kc2, Kc3) vastaanottamiseksi tunnistuskortilta (2), ja
- mainitun yhden tai useamman johdetun arvon (Kc1, Kc2, Kc3) käyttämiseksi mainitun salauksen purkuavaimen (Ks) muodostuksessa, ja

- tietojoukon salauksen purkamiseksi mainitulla salauksen purkuavaimella (Ks).

19. Patenttivaatimuksen 18 mukainen tietokoneohjelmatuote, **tunnettu** siitä, että elektroniikkalaitteeseen (1) on tallennettu kaksi tai useampia tietojoukkoja, ja kunkin tietojoukon yhteyteen on tallennettu tieto sisäisestä avaimesta (Ki), jolloin tietokoneohjelmatuote käsittää koneellisesti suoritettavissa olevia ohjelmakäskyjä mainituista tietojoukoista sen tietojoukon etsimiseksi, jonka yksilöivä tunnus vastaa tunnistuskortille (2) tallennettua sisäistä avainta (Ki), ja mikäli tietojoukko löytyi, suoritetaan löydetyn tietojoukon tietojen salauksen purkaminen.

Patentkrav:

1. Förfarande för att lagra information i ett minne (1.2) av en elektronikanordning (1), varvid informationen som skall lagras krypteras med en krypteringsnyckel (Ks), och i förbindelse med vilken elektronikanordning (1) har installerats ett identifieringskort (2) som är försett med en kryptografisk algoritm, i vilken elektronikanordning (1) genereras åtminstone ett frövärde (RAND1, RAND2, RAND3), sagda åtminstone ett frövärde förmedlas till identifieringskortet (2), på vilket sagda kryptografiska algoritm utförs, varvid sagda frövärde (RAND1, RAND2, RAND3) används som indata, varvid i den kryptografiska algoritmen bildas åtminstone ett härlett värde (Kc1, Kc2, Kc3), **kännetecknat** av, att sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3) förmedlas till elektronikanordningen (1), varvid sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3) används vid bildningen av den sagda krypteringsnyckeln (Ks), och att i elektronikanordningen (1) har lagrats en eller flera datamängder, och i förbindelse med datamängden har lagrats information om ett identifierande kännetecken (ID), varvid man vid dekrypteringsskedet av data söker bland de sagda en eller flera datamängderna den datamängd, vars identifierande kännetecken motsvarar en på identifieringskortet (2) lagrad inre nyckel (Ki), och om datamängden hittades, utförs dekryptering av den upphittade datamängden genom att använda den sagda krypteringsnyckeln (Ks).

2. Förfarande enligt patentkrav 1, **kännetecknat** av, att på identifieringskortet (2) har bildats en inre nyckel (Ki), varvid den sagda inre nyckeln (Ki) används ytterligare vid genereringen av den sagda krypteringsnyckeln (Ks).

3. Förfarande enligt patentkrav 2, **kännetecknat** av, att vid bildningen av den sagda krypteringsnyckeln (Ks) används en enkelriktad funktion, i vilken sagda ett eller flera härledda värden (Kc1, Kc2, Kc3) och den inre nyckeln (Ki) används som indata.

4. Förfarande enligt patentkrav 2 eller 3, **kännetecknat** av, att i elektronikanordningen (1) har lagrats ett anordningsspecifikt

kännetecken, varvid elektronikanordningens (1) anordningsspecifika kännetecken används ytterligare för generering av den sagda krypteringsnyckeln (Ks).

5. Förfarande enligt patentkrav 2, 3 eller 4, **kännetecknat** av, att för dekryptering av data i datamängden genereras en dekrypteringsnyckel (Ks), för vars bildning man söker bland data i datamängden information om åtminstone ett i krypteringsskedet använt frövärde (RAND1, RAND2, RAND3), sagda åtminstone ett frövärde förmedlas till identifieringskortet (2), på vilket man utför den sagda kryptografiska algoritmen, i vilken det sagda frövärdet (RAND1, RAND2, RAND3) och den sagda inre nyckeln (Ki) används som indata, varvid i den kryptografiska algoritmen bildas ett eller flera härledda värden (Kc1, Kc2, Kc3), och sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3) förmedlas till elektronikanordningen (1), varvid sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3) används vid bildningen av den sagda dekrypteringsnyckeln (Ks).

6. Förfarande enligt något av patentkraven 1–5, **kännetecknat** av, att som identifieringskortet (2) används ett identifieringskort som används för identifiering av mobila stationer i ett mobilt kommunikationssystem, varvid som den sagda kryptografiska algoritmen används en algoritm som används för identifiering av en mobil station.

7. Förfarande enligt något av patentkraven 1–6, **kännetecknat** av, att som identifieringskortet (2) används ett av de följande:

- ett SIM-kort,
- ett USIM-kort,
- ett R-UIM-kort,
- ett personligt elektroniskt identifieringskort,
- ett bankkort,
- ett kreditkort.

8. Förfarande enligt något av patentkraven 1–7, **kännetecknat** av, att åtminstone en del av frövärdet (RAND1, RAND2, RAND3) bildas på ett slumpmässigt eller pseudo-slumpmässigt sätt.

9. Elektronikanordning (1), som omfattar ett minne (1.2) och en identifieringskortanslutning (1.3), och i förbindelse med vilken har installerats ett identifieringskort (2) som är försett med en kryptografisk algoritm, och elektronikanordningen (1) omfattar medel (1.1) för att generera åtminstone ett frövärde (RAND1, RAND2, RAND3), medel (1.3) för att förmedla sagda åtminstone ett frövärde till identifieringskortet (2), som omfattar medel (2.1) för att utföra den sagda kryptografiska algoritmen, i vilken det sagda frövärdet (RAND1, RAND2, RAND3) är anordnat att användas som indata, varvid i den kryptografiska algoritmen har anordnats att bildas åtminstone ett härlett värde (Kc1, Kc2, Kc2), **kännetecknad** av, att elektronikanordningen (1) omfattar medel (1.3) för att motta sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3), och medel (1.1) för att använda sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3) för bildning av en krypteringsnyckel (Ks), och att i elektronikanordningen har lagrats en eller flera datamängder, och i förbindelse med datamängden har lagrats information om en inre nyckel (Ki), varvid elektronikanordningen (1) omfattar medel för att söka bland sagda en eller flera datamängder en datamängd, vars identifierande kännetecken motsvarar den på identifieringskortet (2) lagrade inre nyckeln (Ki) för dekryptering av data i datamängden.

10. Anordning (1) enligt patentkrav 9, **kännetecknad** av, att på identifieringskortet (2) har bildats en inre nyckel (Ki), varvid den sagda inre nyckeln (Ki) är ytterligare anordnad att användas vid genereringen av den sagda krypteringsnyckeln (Ks).

11. Elektronikanordning (1) enligt patentkrav 10, **kännetecknad** av, att vid bildningen av den sagda krypteringsnyckeln (Ks) är anordnad att användas en enkelriktad funktion, i vilken sagda ett eller flera härledda värden (Kc1, Kc2, Kc3) och den inre nyckeln (Ki) används som indata.

12. Elektronikanordning (1) enligt patentkrav 10 eller 11, **kännetecknad** av, att i elektronikanordningen (1) har lagrats ett anordningsspecifikt kännetecken, varvid elektronikanordningens (1)

anordningsspecifika kännetecken är anordnad att används ytterligare vid bildningen av den sagda krypteringsnyckeln (Ks).

13. Elektronikanordning (1) enligt patentkrav 10, 11 eller 12, **kännetecknad** av, att den omfattar medel (1.1) för att bilda en dekrypteringsnyckel för att användas för dekryptering av data i en datamängd, medel för att söka bland data i datamängden information om åtminstone ett frövärde (RAND1, RAND2, RAND3) som använts vid krypteringsskedet, medel (1.3) för att förmedla sagda åtminstone ett frövärde till identifieringskortet (2), på vilket den sagda kryptografiska algoritmen är anordnad att utföras, i vilken algoritm det sagda frövärdet (RAND1, RAND2, RAND3) och den sagda inre nyckeln (Ki) är anordnade att användas som indata, varvid i algoritmen har anordnats att bildas ett eller flera härledda värden (Kc1, Kc2, Kc3), varvid elektronikanordningen (1) omfattar medel (1.3) för att motta sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3) från identifieringskortet (2), varvid sagda ett eller flera härledda värden (Kc1, Kc2, Kc3) är anordnade att användas vid bildningen av den sagda dekrypteringsnyckeln (Ks).

14. Elektronikanordning (1) enligt något av patentkraven 9–13, **kännetecknad** av, att identifieringskortet (2) är ett identifieringskort som används för identifiering av mobila stationer i ett mobilt kommunikationssystem, varvid den sagda kryptografiska algoritmen är en algoritm som används för identifiering av en mobil station.

15. Elektronikanordning enligt något av patentkraven 9–14, **kännetecknad** av, att identifieringskortet (2) är ett av de följande:

- ett SIM-kort,
- ett USIM-kort,
- ett R-UIM-kort,
- ett personligt elektroniskt identifieringskort,
- ett bankkort,
- ett kreditkort.

16. Modul för att användas i förbindelse med en elektronikanordning (1), vilken elektronikanordning (1) omfattar ett minne (1.2) och en identifieringskortanslutning (1.3), och i förbindelse med vilken har installerats ett identifieringskort (2) som är försett med en kryptografisk algoritm, och elektronikanordningen (1) omfattar medel (1.1) för att generera åtminstone ett frövärde (RAND1, RAND2, RAND3), medel (1.3) för att förmedla sagda åtminstone ett frövärde till identifieringskortet (2), som omfattar medel (2.1) för att utföra den sagda kryptografiska algoritmen, i vilken det sagda frövärdet (RAND1, RAND2, RAND3) är anordnat att användas som indata, varvid i den kryptografiska algoritmen har anordnats att bildas åtminstone ett härlett värde (Kc1, Kc2, Kc2), **kännetecknad** av, att modulen (1) omfattar medel (1.3) för att motta sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3), och medel (1.1) för att använda sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3) för bildning av en krypteringsnyckel (Ks), och att i elektronikanordningen har lagrats en eller flera datamängder, och i förbindelse med datamängden har lagrats information om en inre nyckel (Ki), varvid elektronikanordningen (1) omfattar medel för att söka bland sagda en eller flera datamängder en datamängd, vars identifierande kännetecken motsvarar den på identifieringskortet (2) lagrade inre nyckeln (Ki) för dekryptering av data i datamängden.

17. Datorprogramprodukt som omfattar maskinellt utförbara program-instruktioner:

- för lagring av data i minnet (1.2) av en elektronikanordning (1), och
- för kryptering av data som skall lagras med en krypteringsnyckel (Ks),

och i förbindelse med elektronikanordningen (1) har installerats ett identifieringskort (2), som är försett med en kryptografisk algoritm, varvid datorprogramprodukten omfattar maskinellt utförbara programinstruktioner:

- för att bilda åtminstone ett frövärde (RAND1, RAND2, RAND3),
- för att söka bland data i datamängden information om åtminstone ett frövärde (RAND1, RAND2, RAND3) som använts vid krypteringsskedet,

- för förmedling av sagda åtminstone ett frövärde till identifieringskortet (2), i vilket den sagda kryptografiska algoritmen är anordnad att utföras, i vilket det sagda frövärdet (RAND1, RAND2, RAND3) är anordnat att användas som indata, varvid i algoritmen har anordnats att bildas åtminstone ett härlett värde (Kc1, Kc2, Kc3),

kännetecknad av, att datorprogramprodukten omfattar maskinellt utförbara programinstruktioner:

- för att motta sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3) från identifieringskortet (2), och
- för att använda sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3) för bildning av den sagda dekrypteringsnyckeln (Ks),

i vilken elektronikanordning (1) har lagrats ett eller flera datamängder, och i förbindelse med datamängden har lagrats information om ett identifierande kännetecken (ID), varvid datorprogramprodukten omfattar ytterligare maskinellt utförbara programinstruktioner:

- för att söka vid dekrypteringsskedet av data bland sagda en eller flera datamängder den datamängd, vars identifierande kännetecken motsvarar den inre nyckeln (Ki) som lagrats på identifieringskortet (2), och
- för att dekryptera data i den upphittade datamängden genom att använda den sagda dekrypteringsnyckeln (Ks).

18. Datorprogramprodukt enligt patentkrav 17, **kännetecknad** av, att för att dekryptera data i den upphittade datamängden datorprogramprodukten omfattar maskinellt utförbara programinstruktioner:

- för att söka bland data i datamängden information om åtminstone ett frövärde (RAND1, RAND2, RAND3) som använts vid krypteringsskedet,
- för förmedling av sagda åtminstone ett frövärde till identifieringskortet (2), i vilket den sagda kryptografiska algoritmen utföras, i vilket det sagda frövärdet (RAND1, RAND2, RAND3) användas som indata, varvid i algoritmen bildas åtminstone ett härlett värde (Kc1, Kc2, Kc3),

varvid datorprogramprodukten omfattar maskinellt utförbara programinstruktioner:

- för att motta sagda åtminstone ett härlett värde (Kc1, Kc2, Kc3) från identifieringskortet (2), och
- för att använda sagda åtminstone ett eller flera härledda värden (Kc1, Kc2, Kc3) för bildning av den sagda dekrypteringsnyckeln (Ks), och
- för dekryptering av datamängden med den sagda dekrypteringsnyckeln (Ks).

19. Datorprogramprodukt enligt patentkrav 18, **kännetecknad** av, att i elektronikanordningen (1) har lagrats två eller flera datamängder, och i förbindelse med varje datamängd har lagrats information om en inre nyckel (Ki), varvid datorprogramprodukten omfattar maskinellt utförbara programinstruktioner för att söka bland sagda datamängder den datamängd, vars identifierande kännetecken motsvarar den på identifieringskortet (2) lagrade inre nyckeln (Ki), och om datamängden upphittades, utförs dekryptering av data i den upphittade datamängden.

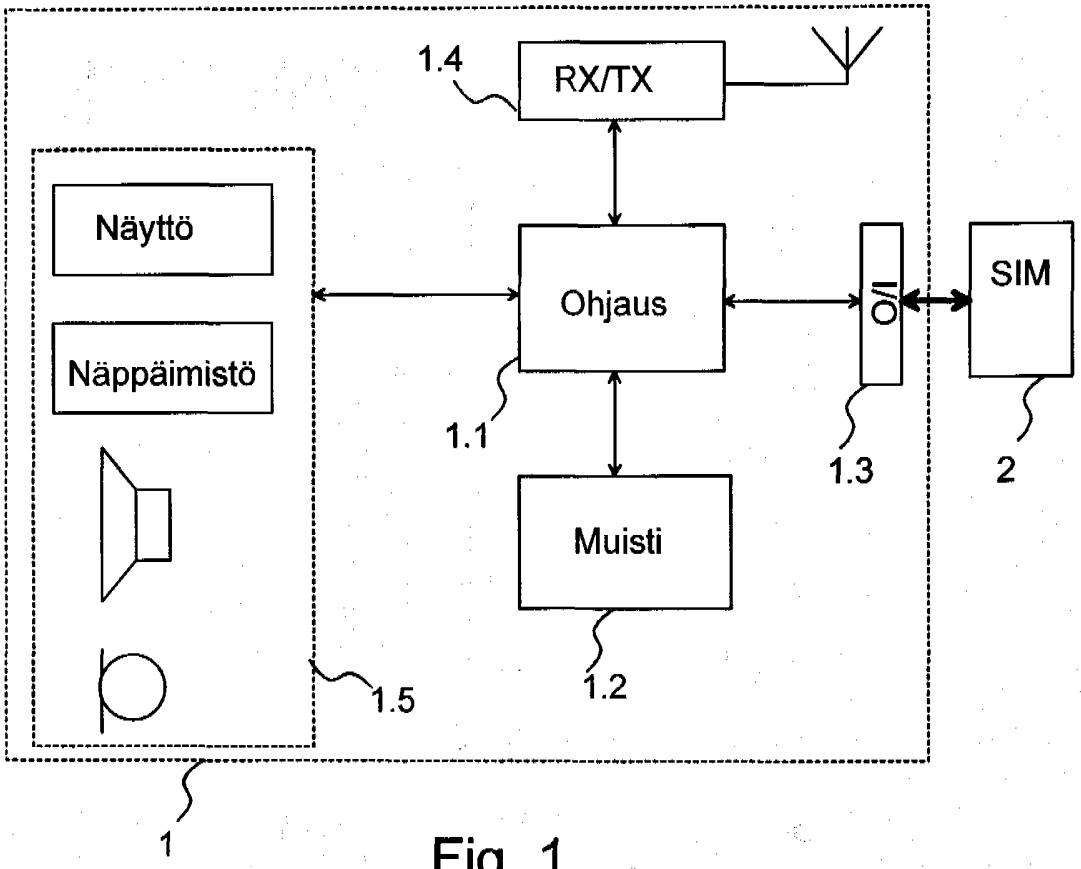

1.4
RX/TX
Näyttö
Näppäimistö
Ohjaus
O/I
SIM
1.1
1.3
2
Muisti
1.2
1.5
1

Fig. 1

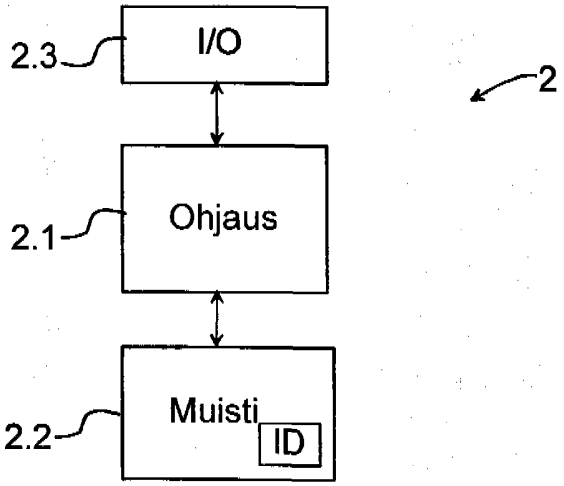

2.3
I/O
2
2.1
Ohjaus
2.2
Muisti
ID

Fig. 2

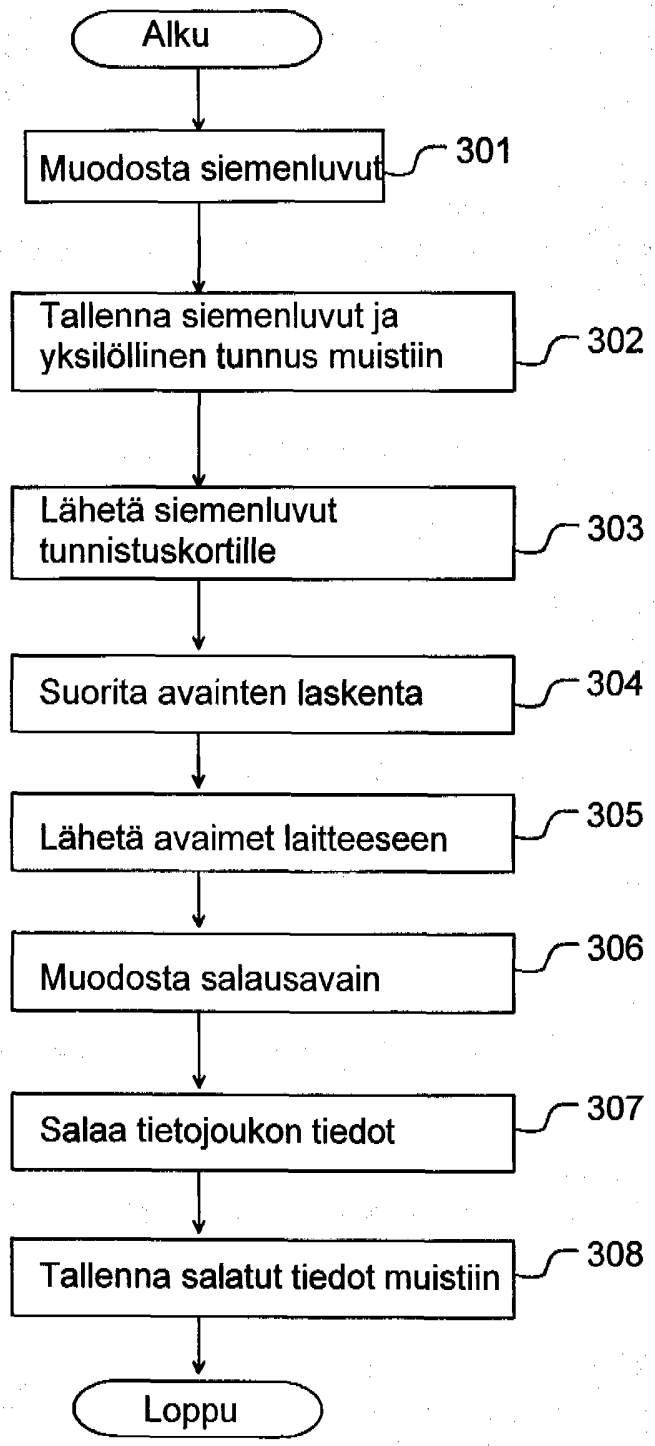

Alku
Muodosta siemenluvut
301
Tallenna siemenluvut ja yksilöllinen tunnus muistiin
302
Lähetä siemenluvut tunnistuskortille
303
Suorita avainten laskenta
304
Lähetä avaimet laitteeseen
305
Muodosta salausavain
306
Salaa tietojoukon tiedot
307
Tallenna salatut tiedot muistiin
308
Loppu

Fig. 3a

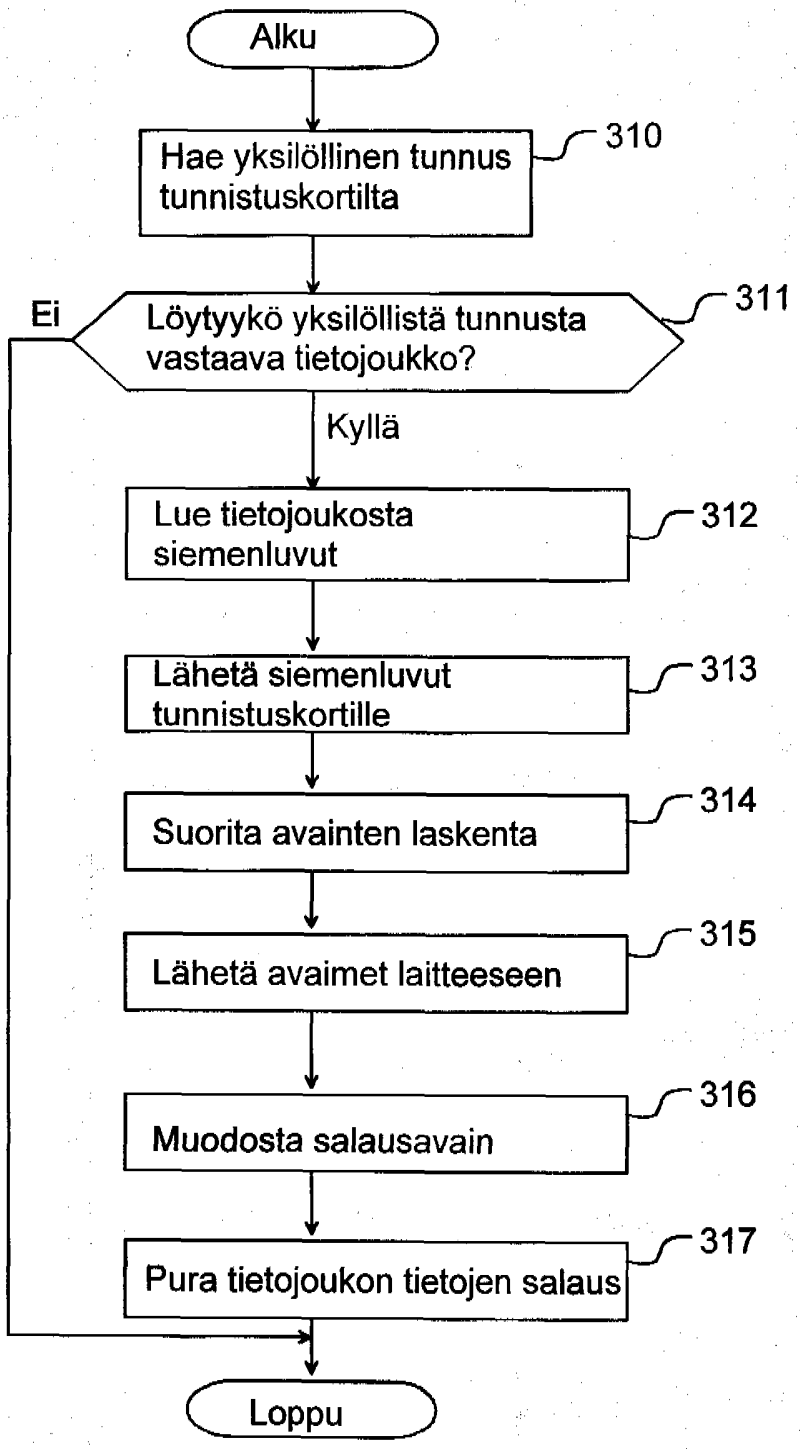

Alku
Hae yksilöllinen tunnus tunnistuskortilta
310
Ei
Löytyykö yksilöllistä tunnusta vastaava tietojoukko?
311
Kyllä
Lue tietojoukosta siemenluvut
312
Lähetä siemenluvut tunnistuskortille
313
Suorita avainten laskenta
314
Lähetä avaimet laitteeseen
315
Muodosta salausavain
316
Pura tietojoukon tietojen salaus
317
Loppu

Fig. 3b