



F1000100621B

(12) PATENTTIJULKAISU
PATENTSKRIFT

(10) FI 100621 B

(45) Patentti myönnetty - Patent beviljats 15.01.98

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

G 07F 7/10

(21) Patenttihakemus - Patentansökning 912215

(22) Hakemispäivä - Ansökningsdag 08.05.91

(24) Alkupäivä - Löpdag 08.05.91

(41) Tullut julkiseksi - Blivit offentlig 11.11.91

(32) (33) (31) Etuoikeus - Prioritet

10.05.90 FR 9005830 P

SUOMI-FINLAND

(FI)

Patentti- ja rekisterihallitus
Patent- och registerstyrelsen

(73) Haltija - Innehavare

1. Dassault Electronique, 55, quai Marcel Dassault, 92214 Saint-Cloud, France, (FR)

(72) Keksijä - Uppfinnare

1. Besson, Richard, 13, rue Gabriel Fauré, 78960 Voisins-Le-Bretonneux, France, (FR)

(74) Asiamies - Ombud: Seppo Laine Oy, Lönnrotinkatu 19 A, 00120 Helsinki

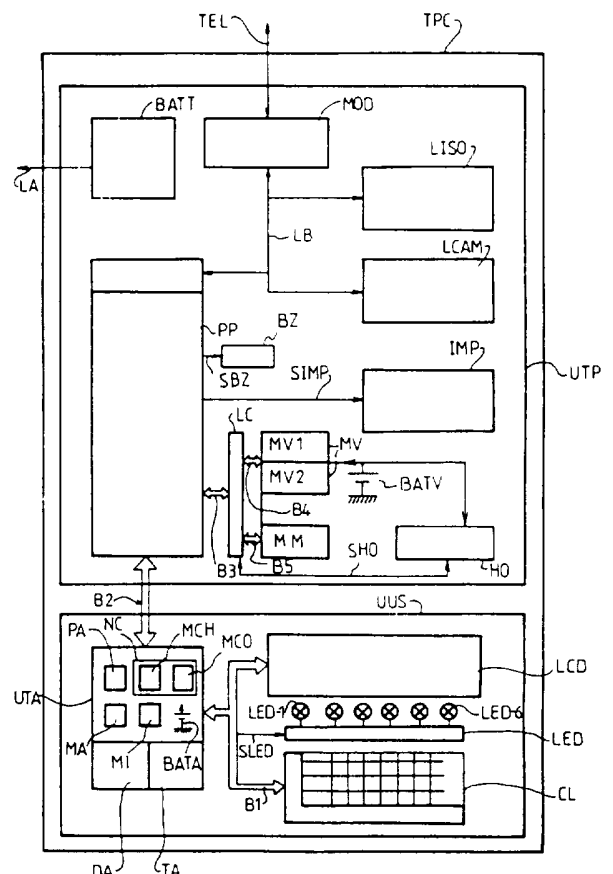
(54) Keksinnön nimitys - Uppfinningens benämning

Laitte salaisten tietojen käsittelymiseksi
Anordning för behandling av hemliga data

(56) Viitejulkaisut - Anförda publikationer

(57) Tiivistelmä - Sammandrag

Keksintö on tietojenkäsittelylaite, joka käsittää käyttäjäyksikön (UUS) tietojen ulosottamiseksi (CL) ja/tai esittämiseksi (VS), ja keskusyksikön (UTP) tietojen käsittelymiseksi tietyn käsittelyalgoritmin (AT) mukaan. Keksinnön mukaan laite käsittää lisäksi erittäin luotettavan lisäkäsittely-yksikön (UTA), joka on yhdistetty laitteeseen varmistamaan kokonaistiedonvaihto käyttäjäyksikön (UUS) ja keskusyksikön välillä (UTP). Lisäkäsittely-yksikkö (UTA) käsittää välineet (MC) tietojen salaamiseksi, tiedonsiirtovälineet (B2), joilla on normaalitila ja salaustila, jossa salataan ainakin yhteen suuntaan siirrettävät tiedot, ja keskusyksikön (UTP) käsittelyalgoritmi (AT) määrää tiedonsiirtovälineiden (B2) toimintatilan, välineet (MA), jotka on sovitettu tarkistamaan mainitun käsittelyalgoritmin (AT) aitous ja jotka toimivat itsenäisesti, ja välineet (MI), jotka on sovitettu kokonaan estämään tiedonsiirtovälineitä (B2) toimimasta siinä tapauksessa, että mainittu tarkistus ei vahvista aitoutta.



Uppfinningen avser en anordning för behandling av data omfattande en användarenhet (UUS) för utskrivning och/eller åskådliggörande (VS) av data och en centralenhet (UTP) för behandling av data enligt en bestämd algoritm (AT). Enligt uppfinningen omfattar anordningen därtill en synnerligen pålitlig tilläggsbehandlingsenhet (UTA), som är kopplad till anordningen för tryggnade av allt utbyte av data mellan användarenheten (UUS) och centralenheten (UTP). Tilläggsbehandlingsenheten (UTA) omfattar organ för hemlighållande av data (MC), organ för överföring av data (B2) med ett normalläge och ett hemlighållningsläge i vilket åtminstone i en riktning överförda data är tryggade, varvid centralenhetens (UTP) behandlingsalgoritm (AT) bestämmer dataöverföringsorganens (B2) funktionstillstånd, självständigt fungerande organ (MA) för kontroll av äktheten hos sagda behandlingsalgoritm (AT), och organ (MI) för att helt förhindra överföringsorganens (B2) funktion i fall att äktheten inte kunnat bekräftas vid sagda kontroll.

Laite salaisten tietojen käsittelemiseksi

Keksintö koskee tietojen salaamista.

5

Se soveltuu maksukorttikauppaan kauppoihin asennetuilla elektronisilla maksulaitteilla, joita kutsutaan myös myymäläpääätteiksi tai kassapääätteiksi.

10

Nykyisin kauppias ottaa tapahtuman loppusumman ulos myyntipisteen päätteen näppäimistöltä, kun taas asiakas voi vahvistaa tapahtuman tunnisteellaan, tai muodostamalla luottamuksellisen koodinsa erillisellä pikku laitteella, ns. asiakaspäätteellä.

15

Useimmiten ryhdytään tehokkaisiin varotoimenpiteisiin asiakaspäätteen suhteen koodisalaisuuden säilyttämiseksi ja siis erittäin suuren luotettavuuden saavuttamiseksi.

20

Nyt hakija ehdottaa toteutettavaksi myymäläpäätteen, joka tyydyttää kaksi tarvetta:

25

1) antaa mahdollisuuden samalla näppäimistöllä yhdellä kertaa muodostaa luottamuksellinen koodi (salainen informaatio) ja ottaa ulos ei-salaisia, tapahtumaan liittyviä tietoja, kuten sen loppusumma, ja

30

2) salata näin otettujen ja/tai muodostettujen tietojen, varsinkin luottamuksellisen koodin, käsittely.

35

Tällainen pääte toteutetaan lähtemällä tietojenkäsittelylaitteesta, joka käsittää käyttäjäyksikön tietojen ulosottamiseksi ja/tai esittämiseksi ja keskusyksikön tietojen käsittelemiseksi tietyn käsittelyalgoritmin mukaan.

Keksinnön yleismääritelmän mukaan tietojenkäsittelylaite käsittää lisäksi:

- erittäin luotettavan lisäkäsittely-yksikön, joka on yh-

distetty laitteeseen varmistamaan kokonaistiedonvaihto
käyttäjäyksikön ja keskusyksikön välillä, ja se käsittää

. välineet tietojen salaamiseksi,

5 . tiedonsiirtovälineet, joilla on normaalitila ja
salaustila, jossa salataan ainakin yhteen suuntaan siirret-
tävät tiedot, ja keskusyksikön käsittelyalgoritmi määrää
tiedonsiirtovälineiden toimintatilan,

10 . välineet, jotka on sovitettu tarkastamaan maini-
tun käsittelyalgoritmin aitous ja jotka toimivat itsenäi-
sesti, ja

. välineet, jotka on sovitettu kokonaan estämään
tiedonsiirtovälineitä toimimasta siinä tapauksessa, että
mainittu tarkastus ei vahvista aitoutta.

15 Tällaisessa laitteessa käyttäjän ulosottamia ja/tai näyttä-
miä tietoja voidaan näin toisaalta käsitellä niiden luon-
teen mukaan joko julkisesti tai koodattuina, ja toisaalta
näitä tietoja käsitellään ainoastaan silloin, kun käsitte-
lyalgoritmi on aito. Se johtaa parantuneeseen luotettavuus-
20 teen käyttäjän ulosottamien ja/tai esittämien tietojen
käsittelyssä.

Keksinnön erään erityistoteutusmuodon mukaan keskusyksikkö
käsittää prosessorin, joka suorittaa kahden muistin osoi-
25 tuksen, joista muisteista ainakin toinen on pysyvä, ja si-
sältää mainitun käsittelyalgoritmin perusohjelmat, joka
algoritmi hoitaa osoitteen jakamisen näiden kahden muistin
välillä, ja aitouden tarkistusvälineet todentavat tunnis-
teen näiden kahden muistin sisällöstä.

30 Edullisesti toinen muisti on dynaaminen tai haihtuva.

Keksinnön erään toisen erityistoteutusmuodon mukaan aitou-
den tarkistusvälineet todentavat tunnisteen ainakin osit-
35 tain molempien muistien sisällöstä näennäishajasaannilla.

Mieluiten tietojen suojausvälineet käsittävät tietojen
koodausvälineet ja/tai tietojen pakkaamisvälineet.

Käytännössä tunniste molempien muistien kokonais- tai osittaissisällöstä toteutetaan pakkaamisvälineillä.

5 Keksinnön eräässä erityistoteutusmuodossa käsittelyalgoritmin perusohjelmat samoinkuin suojatussa, ei-julkisessa paikassa oleva, ennalta laskettu tunniste ladataan pysyvään muistiin paikkaan, joka niinikään on suojattu, ei-julkinen.

10 Keksinnön erään aspektin mukaan on laite varustettu yhteysliittymällä, esimerkiksi modemilla.

15 Keksinnön eräässä toisessa toteutusmuodossa käsittelyalgoritmin perusohjelmat samoinkuin sen ennalta laskettu, suojatussa, ei-julkisessa paikassa oleva tunniste ladataan yhteysliittymän kautta dynaamiseen muistiin paikkaan, joka voi olla suojaamaton, ja pakkaamisvälineet laskevat tunnisteen näin ladatuista perusohjelmista, kun taas aitouden tarkistusvälineet vertaavat näin laskettua tunnistetta yhteysliittymän kautta ladattuun tunnisteeseen.

20 Silloin kun käsittelyalgoritmi on todettu vääräksi, mainittu käsittelyalgoritmi voidaan korvata täydentävällä käsittelyalgoritmillä, joka ladataan yhteysliittymän kautta dynaamiseen muistiin yhdessä suojatussa, ei-julkisessa
25 paikassa olevan, ennalta lasketun tunnisteensa kanssa, ja pakkausvälineet laskevat täydentävään algoritmiin liittyvän tunnisteeseen, kun taas aitouden tarkistusvälineet vertaavat näin laskettua tunnistetta yhteysliittymän kautta ladattuun tunnisteeseen. Vääräksi todetun käsittelyalgoritmin korvaaminen täydentävällä algoritmillä voi tapahtua suojaamattomassa paikassa.
30

35 Silloin kun keksintöä käytetään maksukorttikaupassa, käsiteltäviin tietoihin kuuluu luottamuksellisen koodin tapaisia tietoja.

Keksinnön erään aspektin mukaan käyttäjäyksikkö käsittää riveittäin ja sarakkeittain tapahtuvaan matriisilukuun soveltuvan näppäimistön, kun taas lisäkäsittely-yksikkö

kykenee syöttämään kyselypulsseja näppäimistön kuhunkin riviin samalla tarkistaen näppäimistön sarakkeet, yksi painallus tuottaa tietyn rivi-sarake-kontaktin, ja lisäkäsittely-yksikkö on varustettu ainakin näppäimistön tiettyihin sarakkeisiin ja riveihin kohdistetuilla kaksisuuntaisilla liitännöillä, ja käsittää välineet väärrien painallusten jäljittelemiseksi, jolloin ainakin kyselyimpulssit kohdistuvat samanaikaisesti ainakin yhteen riviin ja yhteen sarakkeeseen, mikä poistaa mahdollisuuden siepata luottamuksellinen koodi näppäimistön rivien ja sarakkeiden tilaa vakoilemalla.

Keksinnön erään toisen aspektin mukaan tietojen salaamisvälineet kykenevät todentamaan aidoiksi etäpääteltä modeemin kautta saadut tiedot, tai varmistamaan mainittuun etäpäätteeseen modeemin kautta lähetetyt tapahtumatiedot.

Keksinnön erään toisen tärkeän tunnusmerkin mukaan laite sijaitsee kädessä pidettävässä kotelossa.

Edullisesti keksinnönmukainen laite on käyttökelpoinen sellaisen teleteknisen ja automaattisen laitteiston aitouden todentamisessa, joka käsittää keksinnönmukaisen etäpäätteeseen yhdistetyn laitteen (ääripäiden aidoksi todentaminen).

Keksinnön muut tunnusmerkit ja edut käyvät selville jäljempänä seuraavasta yksityiskohtaisesta kuvauksesta, ja mukaan liitetyistä piirustuksista, joissa

kuvio 1 esittää keksinnönmukaisen kädessäpidettävän tietojenkäsittelylaitteen päältä,

kuvio 2 on kuva kuvion 1 laitteesta sivultapäin, ja

kuvio 3 on lohkokaavio keksinnönmukaisen tietojenkäsittelylaitteen sisällä olevista piireistä.

Liitteenä olevissa piirustuksissa on useita tietäntyyppisiä

osia. Tästä syystä ne on otettu mukaan selitykseen, ei ainoastaan, jotta tämä ymmärrettäisiin paremmin, vaan myös tarvittaessa keksinnön määrittelyn auttamiseksi.

5 Muutoin jäljempänä olevassa yksityiskohtaisessa selityksessä tarkastellaan ainoastaan pankkipäätettä, vaikkakin ottaen huomioon sen, että keksintö soveltuu myös yleisempään käyttöön.

10 Kuviossa 1 viitenumero TPC merkitsee kädessä pidettävää päätettä, joka voi olla elektroninen maksupääte (hakijan myymän E 232-sarjan pääte).

15 Tämä pääte on muodoltaan yleisesti suuntaissärmiö, ja siinä on varsi MH, johon käyttäjän on tarkoitus tarttua kädellä, ja paksumpi osa RN, johon on tarkoitus sijoittaa kirjoitusyksikkö IMP. Pääte muodostuu yläosasta PS ja alaosasta PI, jotka liittyvät tiiviisti toinen toisiinsa muodostaakseen kotelon.

20 Näppäimistöyksikkö CL sijaitsee varren MH yläosassa PS. Näppäimistön näppäimet sijaitsevat yläosan PS ulkopinnalla. Näppäimistössä on esimerkiksi kaksikymmentä näppäintä, joista kahdeksantoista on järjestetty kuuden rivin ja kolmen sarakkeen taulukoksi ja kaksi on vapaana. Samalla tavoin voidaan määritellä kuusi toimintonäppäintä F1, F2, F3, FN, ON/OFF ja vaakanuoli, kymmenen numeronäppäintä nollasta yhdeksään, poistonäppäin CORR ja pilkkunäppäin 00. Kaksi
25 vapaata näppäintä merkitsevät esimerkiksi peruutusta ja
30 hyväksymistä.

Näyttömoduli VS on niinikään sijoitettu varren MH yläosaan PS. Näyttömoduliin kuuluu nestekidenäyttö LCD ja valodiodinäyttö LED. Näyttömoduli sijaitsee näppäimistön CL ja
35 paksumman osan RN välissä. Edullisesti näyttömodulin ulkopinta on hieman viisto, jotta modulin näytöt näkyisivät paremmin.

Näyttölaite LCD käsittää esimerkiksi kaksi kuudentoista

kuvaelementin riviä. Valodiodinäyttö taas käsittää kuusi erillistä diodia LED-1:stä LED-6:een. Nämä diodit antavat mahdollisuuden osoittaa päätteen eri elementtien toimintatilan.

5

Kuten kuviossa 2 on esitetty, päätteen poikki koko sen leveydeltä menee ura F, joka sijaitsee näyttömodulin VS ja paksumman osan RN välissä. Kortinlukija LISO ympäröi uraa F mahdollistaakseen perinteisen tapaisen maksukortin lukemisen kun tämä viedään uraan ja kuljetetaan sitä pitkin suuntaan tai toiseen.

10

Paksumpaan osaan RN on sijoitettu kirjoitinmoduli IMP. Kysymyksessä on esimerkiksi neulakirjoitin. Paperinauha repäistään irti esimerkiksi leikkaavan reunan BT avulla, joka reuna on koholla paksumman osan RN yläosaan PS nähden.

15

Tehonsyöttöliitäntä LA on järjestetty päätteen ulkopuolisen syötön mahdollistamiseksi.

20

Samoin on järjestetty (esittämättä jätetty) liitäntä, joka mahdollistaa päätteen kytkemisen teleteknisesti ulkopuolisiin käsittely-yksiköihin.

25

Päätteen mitat ovat esimerkiksi seuraavat.

Päätteen kokonaispituus on 270 mm. Varren MH pituus, leveys ja paksuus ovat 110 mm, 90 mm ja vastaavasti 50 mm. Paksumman osan RN pituus, leveys ja paksuus ovat 120 mm, 110 mm ja vastaavasti 70 mm.

30

Kuvion 3 lohkokaaviossa näkyvät kohdassa TPC päätteen ulkorajat.

35

Keksinnön mukaan on pääte TPC jaettu suojattuun käyttäjäyksikköön UUS ja keskusyksikköön UTP.

Kuten edellä mainittiin kuvioihin 1 ja 2 viitaten, on käyttäjäyksikössä kaksikymmentä näppäintä käsittävä näppäimistö

CL, valoilmaisinlaite LED ja näyttölaite LCD.

5 Keksinnön yleismääritelmän mukaan on järjestetty erittäin luotettava lisäkäsittelylaite UTA, joka on kytketty mukaan tietojen kokonaisvaihdon varmistamiseksi käyttäjäyksikön UUS ja keskusyksikön UTP välillä.

10 Lisäkäsittelylaite muodostuu esimerkiksi integroidusta hybridi- tai monoliittipiiristä, joka on valettu hartsiin.

15 Keksinnönmukaisen päätteen rakenneyksiköiden selitys sisältää riittävästi teknistä informaatiota, jotta alan ammattimies voi sen toteuttaa, varsinkin mitä tulee lisäkäsittelylaitteen rakenteellisiin elementteihin, vaikkakin viime-
mainitut on kuvattu suppeammin ottaen huomioon niiden suo-
jauskäyttö.

20 Lisäkäsittely-yksikkö UTA käsittää mikroprosessorin PA ja sisäiset muistit DA ja TA, jotka ovat ainakin osittain pysyväismuisteja ja yhdistetty sisäisellä väylällä mikroprosessoriin PA. Sisäiset muistit DA ja TA ovat esimerkiksi CMOS RAM-tyyppisiä, joita varten on varalla hartsiin valettu paristo BATA päätteen verkkosyötön pudotessa pois.

25 Suojapiiri MC, joka on varustettu koodausvälineillä MCH ja kompressointivälineillä MCO, sijaitsee integroidussa hybridipiirissä. Juuri tämä antaa lisäkäsittely-yksikölle erittäin hyvän luotettavuuden. Se käsittää salaiset avaimet, jotka kykenevät koodaamaan tiedot kansainvälisen tietojenkoodausstandardin, kuten esimerkiksi "Data Encryption Standardin" (DES), mukaan.

30 Ulkoinen väylä B1 mahdollistaa tietojen siirtämisen käyttäjäyksikön rakenteellisten elementtien CL ja LCD ja lisäkäsittely-yksikön UTA vastaavien välillä.

Komentolinja SLED, joka on asennettu lisäkäsittely-yksikön ja valomerkkilaitteen LED väliin antaa mahdollisuuden ohjata mainitun valomerkkilaitteen diodeja.

Samoin on järjestetty ulkoinen väylä B2, joka mahdollistaa tietojen siirron lisäkäsittely-yksikön ja keskusyksikön välillä. Suojauspiiri MC on järjestetty lisäkäsittely-yksikön sisäisen väylän ja ulkoisen väylän B2 väliin. Samoin
5 lisäkäsittely-yksikkö kykenee siirtämään mainitun suojauspiirin MC kautta koodatut ja varastoidut tiedot sisäisiin muisteihin DA ja TA.

Keskusyksikkö puolestaan käsittää mikroprosessorin PP.

- 10 Keskusyksikön osoiteväylä B3 menee komentologiikan LC kautta tullakseen kohdassa B4 dynaamiselle muistille MV, joka on jaettu kahdeksi dynaamiseksi muistiksi MV1 ja MV2, samoin kuin kohdassa B5 pysyväismuistille MM.

- 15 Molemmat muistit MM ja MV muistavat sisältönsä: pysyväismuisti MM pysyvästi, ja dynaaminen muisti MV parin (tai pariston) BATV varmistuksen ansiosta. Keksinnön mukaan muuttumaton muisti MM sisältää käsittelyalgoritmin perusohjelmat ja hoitaa molempien muistien osoitteiden jakamisen.
20 Dynaaminen muisti MV sisältää ohjelmat ja tiedot, jotka voidaan kaukoladata, kuten näemme yksityiskohtaisemmin jäljempänä.

- Dynaamiset muistit MV1 ja MV2 ovat esimerkiksi CMOS RAM-
25 muisteja, MV1:n ja vastaavasti MV2:n kapasiteetti on arvoltaan esimerkiksi 32 - 128 kilotavua. Muuttumaton muisti MM on esimerkiksi EPROM-muisti. Sen kapasiteetti on arvoltaan esimerkiksi 64 - 128 kilotavua.

- 30 Havaitaan, että pari tai paristo BATT, joka on yhdistetty liitäntään LA, varmistaa päätteen toiminnot. Edullisesti BATV-syöttö turvaa CMOS RAM-muisteissa olevan informaation säilyvyyden päätteeseen tulevan virran syötön katketessa.
CMOS RAM-muisteissa olevat tiedot menetetään heti siinä
35 tapauksessa, että syöttöön BATV kohdistuu mekaanisia iskuja.

Paristo BATV varmistaa samoin ajastimen HO toiminnan, jota ajastinta ohjaa ohjauslogiikka LC ohjaussignaalin SHO kaut-

ta.

5 Prosessori PP voi myös ohjata summerin tapaista soittokel-
loa BZ prosessorista PP tulevan ohjaussignaalin SBZ väli-
tyksellä.

10 Keskusyksikön UTP käsittelyalgoritmi AT määrää ulkoisen
väylän B2 toimintatilan, ts. sen väylän, joka välittää joko
normaalin toimintatilan mukaiset tai salaustilan mukaiset
tiedot, jossa salaustilassa luottamuksellinen koodi kooda-
taan.

15 Hakiija on kuitenkin havainnut, että rikolliset saattaisivat
vilpillisesti muuttaa käsittelyalgoritmia syöttääkseen
luottamuksellisen koodin julkisesti näppäimistöltä kes-
kusyksikköön ja yrittääkseen siepata mainitun luottamuksel-
lisen koodin hetkellä, jolloin keskusyksikkö käsittelee
sitä.

20 Siitä syystä hakiija on ennalta varustanut lisäkäsittely-
yksikön välineillä, jotka soveltuvat tarkistamaan käsit-
telyalgoritmin AT aitouden, ja jotka toimivat itsenäisesti.
Tarkistusvälineiden vuoksi on järjestetty välineet M1,
jotka ovat soveliaat estämään tiedonsiirtovälineitä B2
25 kokonaan toimimasta siinä tapauksessa, että mainittu tar-
kistusväline ei vahvista aitoutta.

30 Keksinnön erään erityistoteutusmudon mukaan tehdään käsit-
telyalgoritmi henkilökohtaiseksi, ts. mainittuun käsittely-
algoritmiin liitetään tunniste.

35 Käytännössä nimenomaan käsittelyalgoritmin määrittelevät
ohjelmat sisältävien muistien MV1, MV2 ja MM kokonaissisäl-
lölle lasketaan tunniste. Tämä tunniste toteutetaan pakkaa-
misvälineillä MCO, jotka ovat lisäkäsittely-yksikössä.
Siitä seuraa, että käsittelyalgoritmin aitouden tarkistami-
nen tarkoittaa muistien MV1, MV2 ja MM kokonaissisällössä
olevan tunnisteiden vertaamista tästä sisällöstä näin lasket-
tuun tunnisteeseen.

Käsittelyalgoritmin tunniste lasketaan esimerkiksi "Data Encryption Standard" (DES) tyyppisellä pakkaamismenetelmällä tai kansainvälisen koodausnormin "Message Authentication Algorithm" (MAA), viitenumero ISO 8731 mukaan.

5

Kun on kyse keksinnönmukaisen päätteen asentamisesta kauppiaille, tapahtuu käsittelyalgoritmin personalisointi seuraavalla tavalla.

10

Ei-julkisessa suojatussa paikassa, kuten suojatussa huoneessa, viedään salatut avaimet suojauspiiriin MC. Pääte on estotilassa, ts. se ei pysty varmistamaan suojaustoimintaa, kuten luottamuksellisen koodin ulosottamista.

15

Jonkinlaisella lataustoiminnolla, esimerkiksi kaukolatauksella, ohjelmoimalla PROM tai sarjaliitännällä ladataan käsittelyalgoritmi samoinkuin mainitussa suojatussa paikassa ennalta laskettu tunniste muuttuviin muisteihin MV1 ja MV2. Tunniste täyttää muistit MV1 ja MV2, jotta välttyttäisiin vapaaksi jääneen muistitilan vilpilliseltä käytöltä.

20

Mikroprosessori PA laskee sitten pakkaamisvälineiden MCO välityksellä tunnisteiden keskusyksikköön näin ladatusta algoritmista ketjutetun pakkaamismenetelmän DES tai MAA mukaan. Kontrollointivälineet MA vertaavat lopuksi näin laskettua tunnistetta jo ladattuun tunnisteeseen.

25

Siinä tapauksessa, että tunnisteet ovat yhtäläiset, on pääte käyttövalmis, ts. se ei ole enää estotilassa ja hyväksyy asiakaskäyttäjän ja myyjäkäyttäjän välisen käytön. On todettava, että ennen tämän yhtäläisyyden saavuttamista ei pääte salaa toimintoja.

30

Kun pääte kerran on asennettu kauppiaille ja omistettu asiakaskäyttäjälle, se hyväksyy luottamuksellisen koodin ulosoton ja sen DES-koodauksen VISA-, ISO- tai erityispankkiformaatin mukaan.

35

Asiakaskäyttäjän pankkikortin lukeminen tapahtuu maksukort-

5 tilukijan LISO välityksellä tai muistikorttilukijan LCAM välityksellä. Nämä lukijat on yhdistetty kaksisuuntaisilla komentolinjoilla LB keskusmikroprosessoriin PP. Tavallisesti pääte on yhdistetty etäpääätteisiin teleteknisen liitännän TEL kautta. Tässä tapauksessa modemi MOD on sijoitettu teleteknisen liitännän ja prosessorin PP väliin suojatun luottamuksellisen koodin siirron mahdollistamiseksi mainittuihin etäpääätteisiin.

10 Lisäksi on järjestetty ohjaussignaali, joka välitetään keskusprosessorin kirjoitusyksikköön IMP yhdistävän ohjauslinjan SIMP kautta tapahtuman tietojen painamiseksi paperille.

15 Edellä mainitun estotilan poistumisvaiheen jälkeen, joka tila on antanut mahdollisuuden todentaa aitous päätteeseen ladatusta käsittelyalgoritmista, on pääte käyttövalmis, ts. se sallii samalla kertaa tapahtuman tietojen ulosottamisen ja luottamuksellisen koodin muodostamisen.

20 Kauppiaalle tapahtuneen asentamisen jälkeen on pääte vielä herkkä sellaisille vilpillisille ohjelmistomuutoksille, joita rikolliset voisivat tehdä siepatakseen luottamuksellisen koodin.

25 Hakija on keksinnön mukaisesti kehittänyt menetelmän aitouden todentamiseen tosiajassa käsittelyalgoritmista päätteen ei-suojattuun paikkaan asentamisen jälkeen, joka menetelmä tuo ratkaisun ongelmaan.

30 Edellä mainitun päätteen estotilan poistovaiheen aikana lisäkäsittely-yksikön mikroprosessori PA pilkkoo käsittelyalgoritmien tavut, jotka sijaitsevat muisteissa MV1, MV2 ja MM (esimerkiksi jakaa kunkin 128:aan tavuun) ja laskee kuhunkin jakoon liittyvän aidoksitodennuksen ketjutetun
35 pakkaamismenetelmän DES tai MAA mukaan. Näin lasketut aidoksitodennukset varastoidaan lopulta lisäkäsittely-yksikön sisäisiin muisteihin.

Lisäkäsittely-yksikkö laskee samoin yleistunnisteen laske-

misen käsittelyalgoritmista ja varastoi mainitun yleistunnisteen sisäiseen muistiin DA, TA. Ohjausvälineet MA todentavat lopuksi näin lasketun yleistunnisteen ja aiemmin ladatun tunnisteen. Jos ohjausvälineet pitävät todennusta
5 aitona, on pääte käyttövalmis.

Tästä hetkestä lähtien lisäkäsittely-yksikkö voi siis ottaa yhteyttä keskusyksikköön, jotta tämä toimittaisi sille tietojenjaon tavut suojatusta muistista näennäissatunnaisesti.
10

Tässä tapauksessa lisäkäsittely-yksikkö laskee tämän jaon tavuihin liittyvän tunnisteen ja vertaa näin laskettua tunnistetta päätteen estotilan poistamisen aikana varastoituu.
15

Siinä tapauksessa, että tunnisteet ovat yhtäläiset, pysyy pääte käyttövalmiina, koska tämä yhtäläisyys merkitsee, että käsittelyalgoritmia ei ole muutettu vilpillisesti kauppiaille tapahtuneen asennuksen jälkeen.
20

Siinä tapauksessa, että aitoutta ei ole todettu, asettuu lisäkäsittely-yksikkö jompaan kumpaan kahdesta seuraavasta tilasta:

25 1) pyyhkii pois salatut avaimet suojauspiiristä ja lukitsee näppäimistön, tai

2) odottaa käsittelyalgoritmin oikeaa uudelleenalustamista kaukolatauksella.

20 On ilmeistä, että ensimmäinen tila estää jatkokäytön, koska se tekee välttämättömäksi tehtaalle palautuksen uusien salaisten avaimien asentamista varten, kun taas toinen tila on joustavampi, koska alustus voidaan tehdä paikan päällä
35 uudelleenalustustoimintojen kaukosiirtona.

Tarkemmin sanoen algoritmin uudelleenalustaminen, toisin sanoen korvaaminen täydentävällä algoritmilla, tapahtuu seuraavalla tavalla.

Kun käsittelyalgoritmi on tarkistuksessa havaittu vääräksi, korvataan käsittelyalgoritmi täydentävällä käsittelyalgoritmilla, joka on ladattu modeemin MD kautta muuttuviin muisteihin MV1, MV2 yhdessä etukäteen julkisessa, suojamattomassa paikassa lasketun tunnisteiden kanssa.

Kompressoitivälineet MCO laskevat sitten täydentävään käsittelyalgoritmiin liittyvän tunnisteiden.

10 Lopuksi oikeellisuuden tarkastusvälineet MA vertaavat näin laskettua tunnistetta modemin välityksellä ladattuun tunnisteeseen.

15 Hakija on havainnut, että rikolliset voisivat yrittää siepata luottamuksellisen koodin hetkellä, jolloin se siirtyy käyttäjäyksiköstä lisäkäsittely-yksikköön.

20 Tämä ongelma on ratkaistu asettamalla väliin lisäkäsittely-yksikkö, joka antaa mahdollisuuden estää luottamuksellisen koodin sieppausmahdollisuus näppäimistön rivien ja sarakkeiden tilaa vakoilemalla.

25 Ranskalaisessa patenttihakemuksessaan 86 07901, joka on pantu vireille 2. kesäkuuta 1986, on hakija jo suojannut varmistetun näppäimistöyksikön, joka antaa mahdollisuuden parantaa näppäimistöyksikön suojausta varsinkin luottamuksellisen koodin muodostamisen suhteen.

30 Kuten yllämainitussa hakemuksessa on kuvattu, kykenee keksinnön mukainen lisäkäsittely-yksikkö syöttämään kyselypulsseja näppäimistön kuhunkin riviin samalla tarkastaen näppäimistön sarakkeita, jolloin yksi painallus tuottaa tietyn rivi-sarake-kontaktin.

35 Lisäkäsittely-yksikkö on varustettu lisäksi ainakin näppäimistön tiettyihin sarakkeisiin ja riveihin kohdistetuilla kaksisuuntaisilla liitännöillä, ja käsittää välineet väärin painallusten jäljittelemiseksi, jolloin ainakin kyse-lyimpulssit kohdistuvat samanaikaisesti ainakin yhteen

riviin ja yhteen sarakkeeseen, mikä poistaa mahdollisuuden siepata luottamuksellllinen koodi näppäimistön rivien ja sarakkeiden tilaa vakoilemalla.

- 5 Alan ammattimies voi etsiä muita näppäimistön suojaukseen liittyviä teknisiä osia yllämainitusta patenttihakemuksesta, koska tämä muodostaa selityksen olennaisen osan.

- 10 Keksinnön mukaan voi lisäkäsittely-yksikkö myös varmistaa päätteen suojaustoimenpiteet, esimerkiksi todentaa aidoiksi sellaiset yhteen etäpääätteeseen lähetetyt tiedot, kuten pankkitapahtumaan liittyvät tiedot, tai todentaa aidoiksi sellaiset etäpääätteestä vastaanotetut tiedot, kuten pankkikorttien protestilista, joka on lähetetty päätteeseen
- 15 etäpääätteen kautta.

- Käyttämällä näin samaa aitouden tarkistuskaaviota, jota on käytetty käsittelyalgoritmin tietoja varten, lasketaan tunniste johonkin pankkitapahtumaan liittyviin kaikkiin
- 20 tietoihin.

Senjälkeen pääte lähettää tunnisteiden etäpääätteelle, joka kykenee hoitamaan pankkitapahtuman modeemin kautta.

- 25 Etäpääte vastaanottaa pankkitapahtumaan liittyvät tiedot ja siihen liittyvän tunnisteiden. Senjälkeen se laskee näin vastaanotettuihin pankkitapahtumatietoihin liittyvän tunnisteiden ja todentaa näin lasketun tunnisteiden aitouden näin vastaanotetun tunnisteiden suhteen.

- 30 Samantapaista suojaa voidaan soveltaa vastakkaiseen suuntaan jostain etäpääätteestä vastaanotettujen tietojen aidoksi todentamiseen.

- 35 Edullisesti voidaan myös pääte todentaa aidoksi menetelmällä, jota nimitetään "ääripäiden aidoksi todentaminen".

Päätteen todentamiseksi aidoksi lähetetään satunnainen avainsana etäpäättteen kautta päätteeseen teleteknisen liittännän kautta. Päätteessä avainsana koodataan koodausvälineillä. Sitten koodattu avainsana lähetetään etäpäätteseen, joka suorittaa vastaanotetun koodatun avainsanan ja mainitun etäpäättteen koodaaman avainsanan vertailun ja todentaa näin päätteen aidoksi.

Toisen ääripään, ts. etäpäättteen aidoksi todentaminen tapahtuu kääntäen edellä mainitulla menetelmällä.

Edellä kuvattuja, keksinnönmukaisia ohjelmistosuojauksia voidaan täydentää fyysisillä suojauksilla, joiden tarkoituksena on parantaa päätteen luotettavuutta.

Pääte varustetaan esimerkiksi sellaisella fyysisellä suojauksella, joka on selostettu ranskalaisessa patenttihakemuksessa 86 03945, jonka hakija on pannut vireille 19. maaliskuuta 1986.

Tämä patenttihakemus muodostaa tämän selityksen olennaisen osan.

Samalla tavoin päätteen suojausta etäpäätteiden suhteen parannetaan laitteistolla, joka on kuvattu ranskalaisessa patenttihakemuksessa 86 17485, jonka hakija on pannut vireille 15. joulukuuta 1986.

Tämä patenttihakemus muodostaa samoin tämän selityksen kiinteän osan.

Lyhyesti sanottuna suojattujen tietojen sieppaus estetään keksinnön ansiosta mainittujen tietojen ulosotosta aina vastaanottajalle asti, joka usein on etäällä, toisaalta varsinkin sijoittamalla paikoilleen lisäkäsittely-yksikkö, joka tarkistaa päätteen käsittelyalgoritmin aitouden ja toisaalta käyttämällä luottamuksellisen koodin ulosottomat-

riisista ohjelmallisesti tuotettua häirintää päätteen näppäimistön ja lisäkäsittely-yksikön välillä.

5 Keksintö tuo näin tehokkaan ratkaisun salaisiksi mainittujen tietojen, kuten luottamuksellisen koodin suojaukseen.

10

15

20

25

30

35

Patenttivaatimukset:

1. Tietojenkäsittelylaite, joka käsittää

5 - käyttäjäyksikön (UUS) tietojen ulosottamiseksi
(CL) ja/tai esittämiseksi (VS), ja

 - keskusyksikön (UTP) tietojen käsittelemiseksi
tietyn käsittelyalgoritmin (AT) mukaan,

10

t u n n e t t u siitä, että se käsittää lisäksi

15

- erittäin luotettavan lisäkäsittely-yksikön
(UTA), joka on yhdistetty laitteeseen varmistamaan
kokonaistiedonvaihto käyttäjäyksikön (UUS) ja kes-

kusyksikön välillä (UTP), ja se käsittää
. välineet (MC) tietojen salaamiseksi,
. tiedonsiirtovälineet (B2), joilla on normaaliti-
la ja salaustila, jossa salataan ainakin yhteen suuntaan
siirrettävät tiedot, ja keskusyksikön (UTP) käsittelyalgo-
ritmi (AT) määrää tiedonsiirtovälineiden (B2) toimintati-
lan,

20

. välineet (MA), jotka on sovitettu tarkistamaan
mainitun käsittelyalgoritmin (AT) aitous ja jotka toimivat
itsenäisesti, ja

25

. välineet (MI), jotka on sovitettu kokonaan estä-
mään tiedonsiirtovälineitä (B2) toimimasta siinä tapaukses-
sa, että mainittu tarkistus ei vahvista aitoutta.

30

2. Patenttivaatimuksen 1 mukainen laite, t u n n e t t u
siitä, että keskusyksikkö (UTP) käsittää prosessorin (PP),
joka suorittaa kahden muistin (MV1, MV2 ja MM) osoituksen,
joista muisteista ainakin toinen (MM) on pysyvä, ja sisäl-
tää mainitun käsittelyalgoritmin (AT) perusohjelmat, joka
algoritmi hoitaa osoitteen jakamisen kahden muistin (MV1,
MV2 ja MM) välillä, ja että aitouden tarkistusvälineet (MA)
todentavat tunnisteen molempien muistien (MV1, MV2 ja MM)

35

sisällöstä.

3. Patenttivaatimuksen 2 mukainen laite, t u n n e t t u
siitä, että toinen muisteista (MV1 ja MV2) on dynaaminen
5 tai haihtuva.

4. Jonkin edellisen patenttivaatimuksen mukainen laite,
t u n n e t t u siitä, että tietojen aitouden tarkistusvä-
lineet (MC) todentavat tunnisteen ainakin osittain molempi-
10 en muistien sisällöstä näennäishajasaannilla.

5. Jonkin edellisen patenttivaatimuksen mukainen laite,
t u n n e t t u siitä, että tietojen salausvälineet (MC)
käsittävät tietojen koodausvälineet (MCH) ja/tai tietojen
15 pakkaamisvälineet (MCO).

6. Jonkin edellisen patenttivaatimuksen mukainen laite,
t u n n e t t u siitä, että tunniste molempien muistien
kokonais- tai osittaissisällöstä tapahtuu pakkaamisväli-
20 neillä (MCO).

7. Jonkin edellisen patenttivaatimuksen mukainen laite,
t u n n e t t u siitä, että laite on varustettu yhteys-
liittymällä, esimerkiksi modeemilla (MD).
25

8. Jonkin patenttivaatimuksen 1 - 7 mukainen laite, t u n -
n e t t u siitä, että käsittelyalgoritmin (AT) perusoh-
jelmat samoin kuin suojatussa, ei-julkisessa paikassa oleva,
ennakolta laskettu tunniste on ladattu pysyvään muistiin
30 paikkaan, joka niinikään on suojattu, ei-julkinen.

9. Patenttivaatimuksen 7 mukainen laite, t u n n e t t u
siitä, että käsittelyalgoritmin (AT) perusohjelmat samoin
kuin ennalta laskettu, suojatussa, ei-julkisessa paikassa
35 oleva tunniste on ladattu yhteysliittymän (MD) kautta dy-
naamiseen muistiin (MV1 ja MV2) paikkaan, joka voi olla
suojaamaton, ja pakkaamisvälineet (MCO) laskevat tunnisteen

näin ladatuista perusohjelmista, kun taas aitouden tarkistusvälineet (MA) vertaavat näin laskettua tunnistetta yhteysliitännän (MD) kautta ladattuun tunnisteeseen.

5 10. Patenttivaatimuksen 7 mukainen laite, t u n n e t t u
siitä, että kun käsittelyalgoritmi on todettu vääräksi,
mainittu käsittelyalgoritmi korvataan täydentävällä käsit-
telyalgoritmilla, joka ladataan yhteysliittynän (MD) kautta
dynaamiseen muistiin (MV1 ja MV2) yhdessä suojatussa, ei-
10 julkisessa paikassa olevan, ennalta lasketun tunnisteensa
kanssa, ja että pakkaamisvälineet (MCO) laskevat täydentä-
vään algoritmiin liittyvän tunnisteeseen, kun taas aitouden
tarkistusvälineet (MA) vertaavat näin laskettua tunnistetta
yhteysliitännän kautta ladattuun tunnisteeseen.

15 11. Jonkin edellisen patenttivaatimuksen mukainen laite,
t u n n e t t u siitä, että käsiteltäviin tietoihin kuuluu
tyypiltään luottamuksellisia kooditietoja.

20 12. Jonkin edellisen patenttivaatimuksen mukainen laite,
t u n n e t t u siitä, että käyttäjäyksikkö käsittää

riveittäin ja sarakkeittain tapahtuvaan matriisilukuun
soveltuvan näppäimistön (CL), kun taas lisäkäsittely-yksik-
25 kö kykenee syöttämään kyselypulsseja näppäimistön kuhunkin
riviin samalla tarkastaen näppäimistön sarakkeet, yksi pai-
nallus tuottaa tietyn rivi-sarake-kontaktin, ja lisäkäsit-
tely-yksikkö (UTA) on varustettu ainakin näppäimistön (CL)
tiettyihin sarakkeisiin ja riveihin kohdistetuilla kak-
30 sisuuntaisilla liitännöillä, ja käsittää välineet väärrien
painallusten jäljittelemiseksi, jolloin ainakin jotkut
kyselyimpulssit kohdistuvat samanaikaisesti ainakin yhteen
riviin ja yhteen sarakkeeseen, mikä poistaa mahdollisuuden
siepata luottamuksellinen koodi näppäimistön rivien ja
35 sarakkeiden tilaa vakoilemalla.

13. Jonkin edellisen patenttivaatimuksen mukainen laite,
t u n n e t t u siitä, että tietojen salaamisvälineet (MC)
kykenevät todentamaan aidoiksi etäpäätteeltä modeemin (MD)
kautta saadut tiedot, tai varmistamaan mainittuun etäpää-
5 teeseen modeemin (MD) kautta lähetetyt tapahtumatiedot, tai
todentamaan päätteen aidoksi.

14. Jonkin edellisen patenttivaatimuksen mukainen laite,
t u n n e t t u siitä, että laite sijaitsee kädessä pidet-
10 tävässä kotelossa.

15. Jonkin edellisen patenttivaatimuksen mukaisen laitteen
käyttö sellaisen teleteknisen ja automaattisen laitteiston
aitouden todentamisessa, joka käsittää mainitun laitteen
15 ainakin yhteen etäpäätteeseen yhdistettynä.

20

25

30

35

Patentkrav:

1. Anordning för behandling av data, omfattande

- 5 - en användarenhet (UUS) för utskrivning (CL)
 och/eller åskådliggörande (VS) av data, och
- en centralenhet (UTP) för behandling av data
 enligt en viss behandlingsalgoritm (AT),

10

k ä n n e t e c k n a d av att den vidare omfattar

- en synnerligen pålitlig tilläggsbehandlingsenhet
 (UTA) kopplad till anordningen för tryggnad av
15 totalutbytet av data mellan användarenheten (UUS)
 och centralenheten (UTP), och att den omfattar
- organ (MC) för hemlighållande av data,
 - dataöverföringsorgan (B2) med ett normalläge och
ett hemlighållningsläge, i vilket åtminstone i en riktning
20 överförda data hemlighålles, varvid centralenhetens (UTP)
 behandlingsalgoritm (AT) bestämmer dataöverföringsorganens
 (B2) funktionstillstånd,
 - självständigt fungerande organ (MA) anordnade
 för kontroll av äktheten hos nämnda behandlingsalgoritm
25 (AT), och
 - organ (MI) anordnade för total förhindring av
 överföringsorganens (B2) funktion, ifall äktheten inte
 bekräftats vid nämnda kontroll.

30

2. Anordning enligt patentkrav 1, k ä n n e t e c k n a d
av att centralenheten (UTP) omfattar en processor (PP), som
utför adressering för två minnen (MV1, MV2 och MM), av

vilka åtminstone det ena (MM) är permanent och innehåller
basprogrammen för den nämnda behandlingsalgoritmen (AT),
som ombesörjer adressfördelningen mellan de två minnena
(MV1, MV2 och MM), och att organen för äkthetskontrollen
5 (MA) verifierar ett identifieringstecken för innehållet i
bägge minnen (MV1, MV2 och MM).

3. Anordning enligt patentkrav 2, k ä n n e t e c k n a d
av att det andra minnet (MV1 och MV2) är dynamiskt eller
10 flyktigt.

4. Anordning enligt något av de föregående patentkraven,
k ä n n e t e c k n a d av att organen (MC) för
äkthetskontroll av data verifierar identifieringstecknet
15 för åtminstone en del av innehållet i bägge minnen medelst
en skenbar direktåtkomst.

5. Anordning enligt något av de föregående patentkraven,
k ä n n e t e c k n a d av att organen (MC) för
20 hemlighållande av data omfattar organ (MCH) för kodning av
data och/eller organ (MCO) för packning av data.

6. Anordning enligt något av de föregående patentkraven,
k ä n n e t e c k n a d av att tecknet för total- eller
25 delinnehållet i bägge minnen verkställs medelst
packningsorganen (MCO).

7. Anordning enligt något av de föregående patentkraven,
k ä n n e t e c k n a d av att anordningen är försedd med
30 en kontaktanslutning, till exempel ett modem (MD).

8. Anordning enligt något av patentkraven 1 - 7, k ä n n e -

t e c k n a d av att basprogrammen för
behandlingsalgoritmen (AT) liksom det på förhand beräknade
identifieringstecknet på ett skyddat, icke-offentligt
ställe är laddade i det permanenta minnet på ett likväl
5 skyddat och icke-offentligt ställe.

9. Anordning enligt patentkrav 7, k ä n n e t e c k n a d
av att basprogrammen för behandlingsalgoritmen (AT) liksom
det på förhand beräknade tecknet på ett skyddat, icke-
10 offentlig ställe är laddade via kontaktanslutningen (MD) i
det dynamiska minnet (MV1 och MV2) på ett ställe, som kan
vara oskyddat, och packningsorganen (MCO) beräknar
identifieringstecknet ur de så laddade basprogrammen, medan
organen (MA) för äkthetskontroll jämför det så beräknade
15 tecknet via kontaktanslutningen (MD) med det laddade
tecknet.

10. Anordning enligt patentkrav 7, k ä n n e t e c k n a d
av att när behandlingsalgoritmen har befunnits vara falsk,
20 ersätts den nämnda behandlingsalgoritmen med en
kompletterande behandlingsalgoritm, som laddas via
kontaktanslutningen (MD) i det dynamiska minnet (MV1 och
MV2) tillsammans med det på förhand beräknade tecknet på
ett skyddat, icke-offentligt ställe, och att
25 packningsorganen (MCO) beräknar ett identifieringstecken,
som ansluter sig till den kompletterande algoritmen, medan
organen (MA) för äkthetskontroll jämför det så beräknade
identifieringstecknet med det via kontaktanslutningen
laddade tecknet.

30

11. Anordning enligt något av de föregående patentkraven,
k ä n n e t e c k n a d av att behandlingsuppgifterna

innefattar koddata av konfidentiell typ.

12. Anordning enligt något av de föregående patentkraven,
k ä n n e t e c k n a d av att användarenheten omfattar

5

ett tangentbord (CL) lämpat för matrisläsning rad- och
kolumnvis, medan tilläggsbehandlingsenheten kan frammata
förfrågningspulser till varje rad i tangentbordet under
samtidig kontroll av kolumnerna i tangentbordet, en
10 tryckning åstadkommer en bestämd rad-kolumn -kontakt, och
tilläggsbehandlingsenheten (UTA) är försedd med
dubbelriktade anslutningar riktade mot åtminstone bestämda
kolumner och rader i tangentbordet (CL), och medel för
imitering av oriktiga tryckningar, varvid åtminstone några
15 förfrågningsimpulser riktas samtidigt mot en rad och en
kolumn, vilket eliminerar möjligheten att fånga en
konfidentiell kod genom spionering av tillståndet för
raderna och kolumnerna i tangentbordet.

20 13. Anordning enligt något av de föregående patentkraven,
k ä n n e t e c k n a d av att organen (MC) för
hemlighållande av data kan verifiera uppgifter erhållna
från en fjärrterminal via ett modem (MD) som äkta, eller
trygga transaktionsuppgifter till fjärrterminalen via
25 modemmet (MD), eller verifiera terminalen som äkta.

14. Anordning enligt något av de föregående patentkraven,
k ä n n e t e c k n a d av att anordningen befinner sig i
ett fodral, som hålles i handen.

30

15. Användning av en anordning enligt något av de
föregående patentkraven vid kontroll av äktheten hos sådan

teleteknisk och automatisk utrustning, som omfattar nämnda anordning ansluten till åtminstone en fjärrterminal.

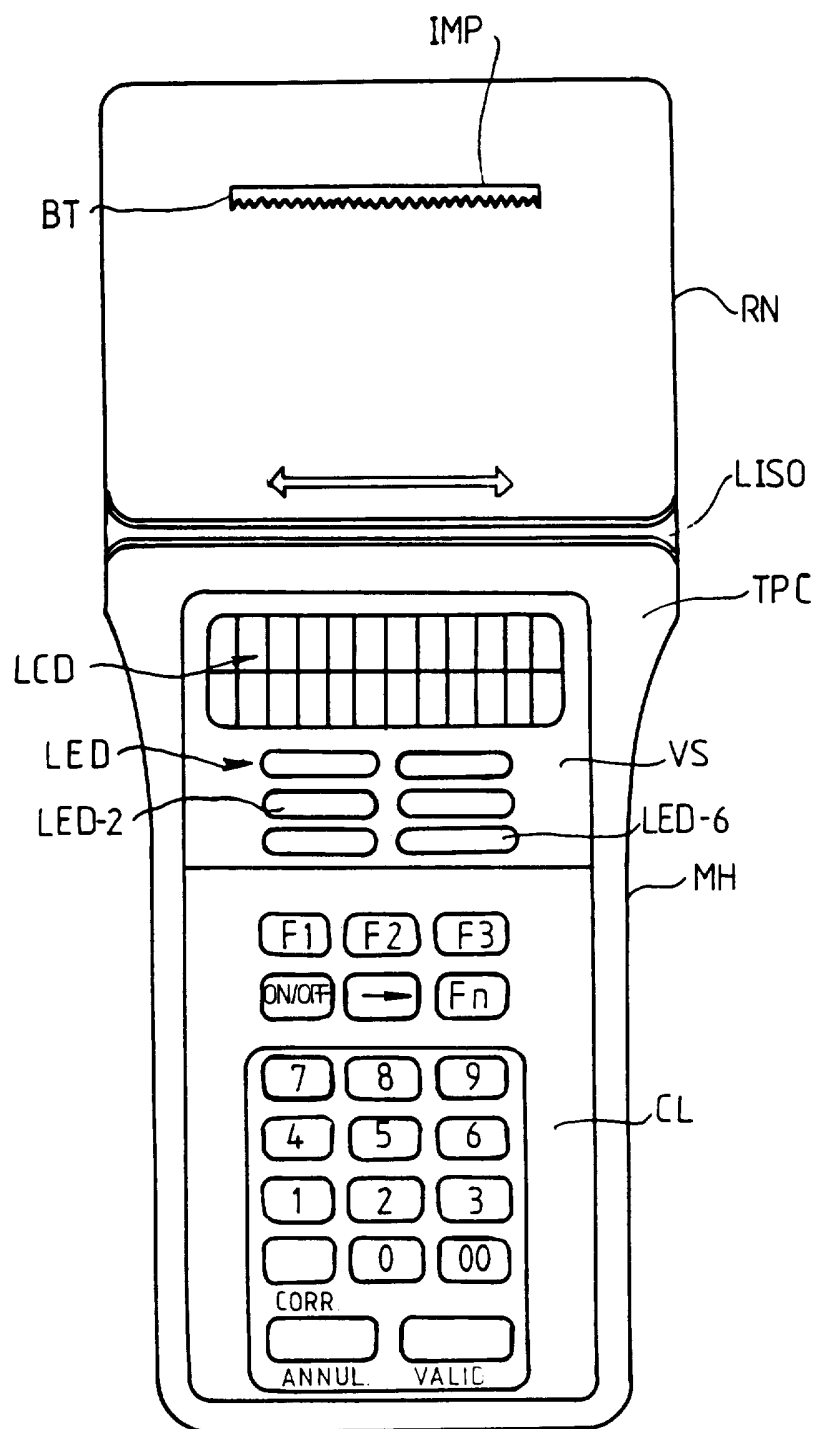
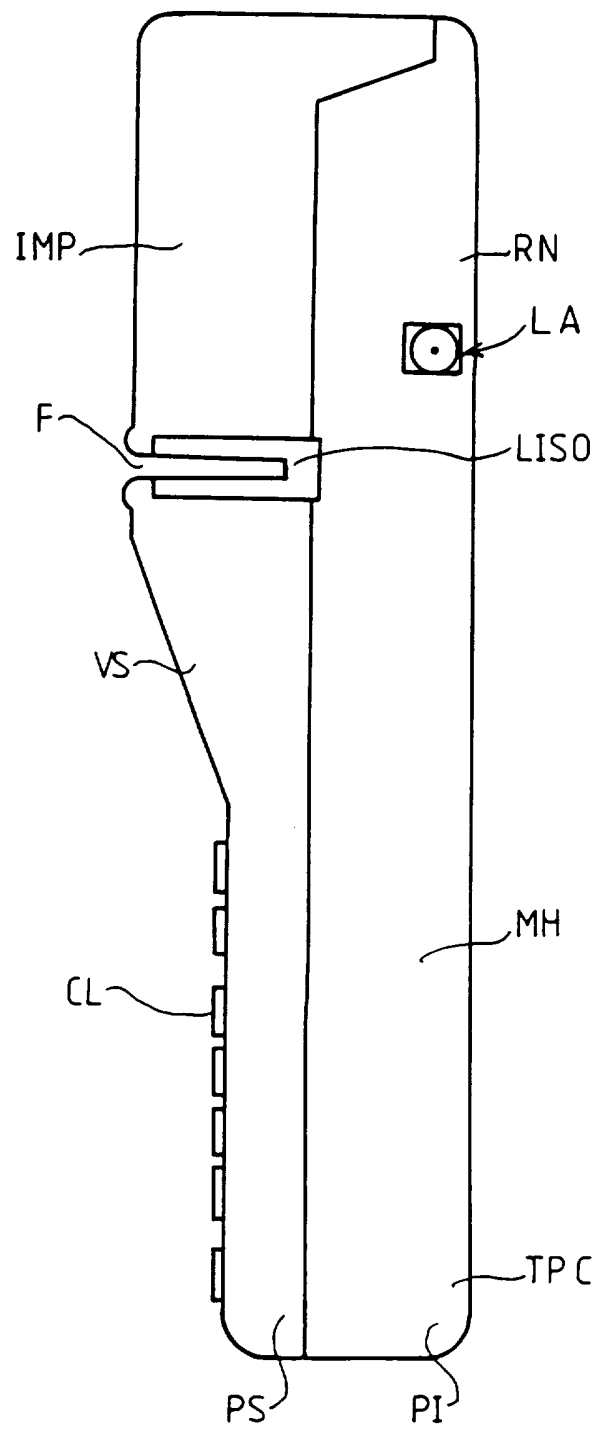


FIG.1

FIG. 2

