(19) SUOMI - FINLAND
(FI)

PATENTTI- JA REKISTERIHALLITUS
PATENT- OCH REGISTERSTYRELSEN
FINNISH PATENT AND REGISTRATION OFFICE

(10) **FI 955307 A7**

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

(21) Patenttihakemus - Patentansökan - Patent application 955307

(51) Kansainvälinen patenttiluokitus - Internationell patentklassifikation - International patent classification
G07F 7/10 (2006.01)
G06K 19/073 (2006.01)

(22) Tekemispäivä - Ingivningsdag - Filing date **07.03.1994**

(23) Saapumispäivä - Ankomstdag - Reception date **06.11.1995**

(41) Tullut julkiseksi - Blivit offentlig - Available to the public **06.11.1995**

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

(86) Kansainvälinen hakemus - Internationell ansökan - International application **07.03.1994 PCT/IB1994/000031**

(71) Hakija - Sökande - Applicant

1 • **CP8 Technologies,** 36-38, rue de la princesse, 78430 Louveciennes, RANSKA, (FR)

(72) Keksijä - Uppfinnare - Inventor

1 • **Holtey, Thomas O.,** Newton, MA 02162, AMERIKAN YHDYSVALLAT, (US)
2 • **Wilson, Peter J.,** TX 78641, AMERIKAN YHDYSVALLAT, (US)

(74) Asiamies - Ombud - Agent

Berggren Oy Ab, Antinkatu 3 C, 00100 Helsinki

(54) Keksinnön nimitys - Uppfinningens benämning - Title of the invention
Turvallinen muistikortti
Säkert minneskort

Turvallinen muistikortti - Säkert minneskort

Esillä olevan keksinnön kohteena ovat kannettavat mikrotietokoneet ja erityisesti järjestelmä tietojen suojaamiseksi kannettavassa digitaalitietoympäristössä.

Henkilökohtaisten tietojen turvallisuus on aina ollut tärkeä asia. Sitä on varmistettu lukkojen, koodien ja salataskujen avulla. Tiedon saatua uusia muotoja, tarvitaan uusia menetelmiä, jotka vastaavat muuttuneita olosuhteita.

Historiallisesti katsottuna tietoa on turvattu nimikirjoituksilla, valtakirjoilla ja valokuvilla. Elektronisten laitteiden, kuten esim. pankkiautomaattien myötä turvallisuustyökalujen joukkoon on lisätty koodatut kortit ja henkilökohtaiset tunnistenumerot (PIN). Tietokonejärjestelmissä käytetään edelleen salasanoja.

Viime aikoina älykortti on yleistynyt turvallisuustyökaluna. Älykortti on pieni mikrotietokone, jossa on haihtumaton muisti, johon voi kirjoittaa ja yksinkertainen syöttö/tulostusliittymä, joka on valmistettu yhtenä siruna ja sijoitettu muoviseen "luottokorttiin". Se käsittää ulkoiset liitäntäalueet, joiden avulla se voidaan kytkeä erikoislaitteistoihin. Kortin mikrotietokoneeseen sisältyvä ohjelma on vuorovaikutuksessa kyseisen laitteiston kanssa ja antaa sen lukea tai muuntaa haihtumatonta muistiaan halutun algoritmin mukaisesti, joka voi vaihtoehtoisesti sisältää myös salasanojen vaihdon. Muistitiedon suojaamiseksi on kehitetty erityisiä menetelmiä, jotka tilanteen mukaan sallivat erilaisia lupia. Esim. US-patentti 4 328 279 esittää arkkitehtuurin, joka sallii käsittely- ja ohjausyksikön kanssa samalla sirulla olevan haihtumattoman muistin automaattisen ohjelmoinnin. Samoin kuin muissa järjestelmissä mikroprosessori suojaa vain samalla sirulla olevaa muistia.

Älykorttia on käytetty sekä tunnistusprosessin helpottamiseksi että arvokkaan tiedon varsinaisena säilytyspaikkana. Tässä tapauksessa, kuten useimmissa aikaisemmissa tapauksessa, on käytetty fyysistä "avainta" sekä jotain erityistietoa osana varmennus- tai todennusprosessia. Tällaisissa tapauksissa tunnistus on ollut pääsyn haluavan henkilön ja tietyn osapuolen, esim. turvallisuusvartijan tai pankkiautomaatin välinen keskustelu.

Erillisten tietokonelaitteiden nykyinen kannettavuus mahdollistaa sekä fyysisen avaimen että todennusvälineen pienen koon ja kannettavuuden, jolloin ne myös helpommin häviävät tai varastetaan. Lisäksi laskentalaitteet tekevät mahdolliseksi monta kertaa yrittää arvata tai päätellä tunnistusprosessiin liittyvä erityinen tieto tai

salasana. Tämä pätee erityisesti sellaisissa tapauksissa, joissa varas saa haltuunsa myös todennusvälineen. Asioiden pahentamiseksi nykytekniikka tekee mahdolliseksi kantaa mukanaan valtavia määriä arkaluontoista tietoa taskussa tai käsilaukussa, josta se helposti häviää.

Nykyään salkkumikrot ja vieläkin pienemmät mikrot tarjoavat pystyvän erillisen ympäristön, joka käsittää merkittävän laskentakapasiteetin, jolloin tarvitaan lisää tietojen tallennuskykyä. Ongelma on aluksi ratkaistu pienoiskovalevylaitteilla, jotka sisältävät sekä ohjelmat että tiedot. Vaikka nämä järjestelmät on usein suojattu salasanoilla, eivät ne kuitenkaan suojele arkaluontoisia tietoja täydellisesti, koska ensinnäkin todennusväline itsessään on haavoittuva. Sitä paitsi tiedot sisältävä levyasema voidaan siirtää ja siihen on mahdollista päästä sisään ympäristössä, joka edistää tietojen analysointia. Tässä tapauksessa ainoastaan jonkinlainen salakirjoitus pystyy suojelemaan tietoja. Levysaanti mahdollistaa sen ilman kohtuuttomia suorituksia tai kustannusrajoja. Esimerkki tämän tyyppisestä järjestelmästä esitetään US-patentissa 4 985 920.

Hiljattain markkinoille tulleen pikamuistin ja poistettavien "muistikorttien" ansiosta kannettavien tietokoneiden kokoa ja virtatarvetta on voitu pienentää huomattavasti. Pikamuistissa yhdistyy suorasaantimuistin (RAM) joustavuus ja levyjen kestävyys. Näiden tekniikoiden avulla pystytään nykyään sisällyttämään luottokortin kokoiseen poistettavaan pakkaukseen jopa 20 miljoona bittiä tietoa ilman virtaa. Tiedot voidaan saada esille isäntäjärjestelmässä, joko niin kuin ne sisältyisivät tavanomaiseen levyasemaan tai isäntäjärjestelmän muistin jatkeena. Nämä tekniset kehitysaskeleet ovat edelleen mahdollistaneet järjestelmien pienemmän koon siten, että nyt niitä voi pikemminkin kantaa taskussa kuin käsilaukussa tai salkussa.

Täten on helpompaa hävittää tai varastaa tiedot ja niiden isäntäjärjestelmä ja samanaikaisesti on vaikeampaa suojata muistitietoa salakirjoituksella, koska se aiheuttaa suuria kustannuksia ja suoritusesteitä.

Voidaan vielä todeta, että julkaisusta EP-A-0 212 655 tunnetaan muistikortti, joka sisältää salauksen purkuvälineet. Lisäksi se sisältää välineet (järjestelmän ohjaimen, koodivertailijan, osoitevertailijan) muistin turvaamiseksi, mutta nämä välineet ovat muistiin nähden ulkoisia, eikä näin ollen ole kysymys muistisirusta, joka voitaisiin turvata sisäisin keinoin, jos se poistetaan kortista.

Täten esillä olevan keksinnön ensisijaisena tavoitteena on aikaansaada kannettava digitaalinen järjestelmä, jossa on turvallinen alamuistijärjestelmä.

Keksinnön toinen tavoite on aikaansaada muistikortti, joka voidaan suojata, jos se poistetaan kannettavasta digitaalisesta järjestelmästä. Lisäksi keksinnön tavoitteena on aikaansaada muistikortti, jossa kortin sirut on suojattu, jos ne poistetaan kyseisestä kortista.

Edellä mainittujen tavoitteiden saavuttamiseksi on keksinnön mukaiselle muistikortille tunnusomaista se, mikä on esitetty patenttivaatimuksessa 1. Keksinnön kohteena on samalla menetelmä tällaisen kortin rakentamiseksi ja menetelmän tunnusmerkit selviävät vaatimuksesta 18. Keksinnön mukainen turvallinen muistikortti käsittää edullisessa suoritusmuodossa mikroprosessorin yhdessä puolijohdesirussa ja yhden tai useamman haihtumattoman osoitettavan muistisirun. Mikroprosessorisiru ja haihtumaton muistisiru liittyvät yhdessä sisäiseen korttitietoväylään osoite-, data- ja ohjaustietojen välittämiseksi haihtumattomiin muistisiruihin. Mikroprosessori sisältää osoitettavan haihtumattoman muistin tiedon tallentamiseksi käsittäen useita avainarvoja, kokoonpanotietoja ja ohjelmakäskytietoja osoitteen, datan ja ohjaustietojen siirron ohjaamiseksi sisäisessä tietoväylässä. Sirumuisti on organisoitu useampaan jaksoon tai kosketinkenttään, jolloin kukin jakso käsittää useita osoitettavia sijainteja.

Esillä olevan keksinnön mukaisesti jokainen muistisiru on rakennettu sisältämään loogiset turvallisuustarkastuspiirit. Edullisessa sovellutusesimerkissä piirit sisältävät haihtumattoman lukittavan muistin, haihtumattoman, lukittavan varastoinnin mahdollistavan elementin ja haihtuvan, pääsyä ohjaavan muistin, jotka kaikki voidaan kuormittaa mikroprosessorin ohjauksessa. Lähemmin tarkasteltuna mikroprosessori ensin lataa tunnusarvon haihtumattomaan lukittavaan muistiin ja palauttaa pääsyn lukittavan varastoinnin mahdollistavaan elementtiin. Tämän jälkeen mikroprosessori lataa pääsyn ohjausmuistin kokoonpanotietojen mukaisesti. Tiedot ladataan vasta sitten, kun mikroprosessori on päätellyt, että käyttäjä on onnistunut suorittamaan ennalta määrätyn todennusmenettelyn isäntäkoneessa. Kunkin muistin loogiset turvallisuuspiirit mahdollistavat pikamuistin valittuihin osoitettuihin lohkoihin tallennettujen tietojen lukemisen osana muistisirun pääsyn ohjausmuistiin tallennetun kokoonpanotiedon toimintoa. Käyttäjän on jaksoittain suoriuduttava todennusmenettelystä isäntäkoneessa, ja käyttäjä saa jatkaa pääsyn ohjausmuistin sallimien tietojen lukemista. Edullisessa sovellutusmuodossa isäntäkone on liitetty muistikorttiin standardiliitännän kautta, joka voi olla esim. PCMCIA-järjestön standardit täyttävä liitäntä.

Esillä olevassa keksinnössä yhdistetään älykortti- ja muistikorttitekniikat, mikä on ratkaisevan tärkeätä, jotta pystytään suojaamaan pikamuistitekniikan mahdollista-

mia suuria tietomääriä elektroniikan kutistamisen luomissa "huonosti suojelluissa" ympäristöissä. Lisäksi esillä oleva keksintö pystyy hyödyntämään kummassakin tekniikassa tapahtuvat parannukset.

Lisäksi esillä olevan keksinnön loogiset turvallisuuspiirit on sisällytetty pikamuistiin ja toimivat sen yhteydessä siten, että se minimoi pikamuistin loogisiin peruspiireihin tehtävien muutosten määrän. Sitä paitsi pikamuisti pystyy toimimaan turvallisella tavalla ja ei-turvatulla tavalla, jolloin loogiset turvallisuuspiirit ohitetaan siten, että pikamuisti pystyy toimimaan ikään kuin tällaisia piirejä ei olisi asennettu. Ei-turvattuun tilaan siirrytään yleensä silloin, kun pikamuistin haihtumattoman lukittavan muistin tiedot on tarkastettu. Tämä viittaa yleisesti ohjelmoimattomaan tai täysin tyhjennettyyn pikamuistiin, joka luonnollisesti tyhjenee ennalta määrättyyn tilaan (eli tilaan, jossa kaikki arvot ovat YKSI).

Lisäämällä pieni määrä logiikkaa pikamuistiin ja "pääsyn ohjausprosessorin" (ACP), turvataan pikamuistin tiedot ilman, että salakirjoitus on välttämätöntä. Tällöin keksintö eliminoi kustannukset, jotka aiheutuvat tietojen salakirjoituksesta ja niiden tulkitsemisesta, mikä voi olla varsin pitkäaikainen prosessi suurten tietolohkojen kohdalla.

Käytössä ACP määräajoin kysyy järjestelmän käyttäjältä todennusta. Kyseessä voi olla salasana, PIN, erityinen kynätietokoneliike, joka suoritetaan kirjoituspinnan tietyssä kohdassa, käyttäjän ääneen lausuma käsky tai "äänijäljennös". Menetelmä vaihtelee eri järjestelmien välillä. Ohjelmoitavan ACP:n avulla käyttäjä pystyy muuttamaan todennuksen tarkoin määrättyä sisältöä ja kehotuksen toistoja. Todennuskoodi ja lukitus- ja pääsyn ohjausmuistien vaatimat tiedot on tallennettu ACP:n haihtumattomaan muistiin, joka on samalla sirulla kuin ACP, jolloin se on suojattu.

Kuten mainittiin, sallii ACP onnistuneen todennuksen seurauksena pääsyn pikamuistin kaikkiin tai valittuihin lohkoihin. Epäonnistuminen katkaisee pääsyn pikamuistiin. Täten epäonnistunut todentaminen johtaa siihen, että pikamuistin tiedot suojataan. Lisäksi käyttäjän alustama komento voi myös johtaa siihen, että pääsy estetään. Edelleen, kun virta kytketään ensimmäisen kerran päälle seisakin jälkeen, estyy pääsy suojattuihin muistiosiin kunnes ensimmäinen todennus on onnistuneesti suoritettu.

Tällöin, jos joko muistikortti tai sen isäntäprosessori katoavat, varastetaan, niistä katkaistaan virta tai ne jätetään ilman valvontaa, muistin sisältämät tiedot on suo-

jattu pääsyltä joko välittömästi tai heti, kun voimassaoleva jaksoittainen todennus umpeutuu. Varkaustapauksissa muistin tiedot on suojattu pääsyltä vaikka muistikortti avattaisiin ja koettaisiin elektronisesti tai muistisirut poistettaisiin ja sijoitettaisiin toiseen laitteeseen.

Esillä olevan keksinnön edellä esitetyt tavoitteet ja edut selviävät paremmin seuraavasta selityksestä yhdessä oheisten piirrosten kanssa.

Kuvio 1 esittää yleisen lohkokaavion järjestelmästä, johon sisältyy esillä olevan keksinnön mukaisesti rakennettu muistikortti.

Kuvio 2 esittää yksityiskohtaisemmin kuvion 1 mukaisen pääsyn ohjausprosessorin (ACP) sisältäen piirroksen sen haihtumattomasta muistista.

Kuvio 3 esittää yksityiskohtaisen lohkokaavion kuvion 1 mukaisesta vakiopikamuistista, joka on muunnettu esillä olevan keksinnön mukaisesti.

Kuviot 4 ja 5 esittävät vuokaaviot, joita käytetään esillä olevan keksinnön mukaisen muistikortin toiminnan selittämiseksi sen suorittaessa eri todennustoimia.

Kuvio 1 esittää lohkokaavion turvallisesta kannettavasta käsinpidettävästä laskentajärjestelmästä 1, jota käytetään mikrona tai tapahtumaprosessorina. Järjestelmä 1 sisältää esillä olevan keksinnön mukaisesti rakennetun muistikortin 3, joka yhdistyy isäntäprosessoriin 5 tietoväylän 102 avulla. Isäntäprosessori 5 voi olla kämmenmikro, kuten Hewlett-Packardin valmistama HP 95LX. Isäntäprosessori 5 sisältää nestekidenäytön (LCD) 5-2, näppäimistön 5-4, mikroprosessorin 5-6, muistin 5-8 ja sarjaliitännän 5-10, jotka ovat kaikki yhdessä liitetty tietoväylään 106. Muisti 5-8 sisältää yhden megatavun lukumuistia (ROM) ja 512 Ktavua työmuistia (RAM).

Muistikortin 3 ja isäntäprosessorin 5 välinen yhteys luodaan standarditietoväyläliitännän kautta. Edullisessa sovellusmuodossa tietoväylä 102 vastaa PCMCIA-liiton standardeja. Liitäntä 102 tarjoaa polun osoite-, ohjaus- ja datatietojen siirtämiseksi isäntäprosessorin 5 ja muistikorttijärjestelmän 3 välillä standardiliitäntäsirun 104 ja muistikorttitietoväylän 105 kautta. Kukin tietoväylistä 102, 105 ja 106 sisältää dataväylän, ohjausväylän ja osoiteväylän ja tarjoavat jatkuvat signaalipolut kaikkien samanlaisten tietoväylien kautta. Esim. tietoväylä 105 sisältää osoiteväylän 105a, dataväylän 105b ja ohjausväylän 105c.

PCMCIA-tietoväylästandardi on kehittynyt standardista, joka tukee levyn emulointia muistikorteissa, olennaisesti erilaiseen standardiin, joka sallii satunnaisen pääsyn muistitietoihin. Esillä olevan keksinnön mukainen muistikortti tarjoaa suojamenetelmän, joka tukee uutta standardia tarjoamalla nopean pääsyn satunnaismuistiin turvautumatta salakirjoitukseen. Kontrolloimalla tietopolut, jotka kuljettavat tiedot muistijonosta isäntään, esillä olevan keksinnön mukainen muistikortti suojaa tietoja käyttämättä aikaavievää puskurointia, salakirjoitusta tai muuta sarjakäsittelyä polulla.

Yleensä käyttäjä käyttää järjestelmää 1 näppäimistöltä 5-4 suorittaakseen yleiset toiminnot, kuten taulukkolaskentaa ja tietokantatoimintoja, jotka esittävät tietoja näytöllä 5-2 ja päivittävät muistikortin 3 tiedostoihin tallennettuja tietoja. Isäntäprosessori 5 lähettää osoitetiedot tietoväylää 102 pitkin hakeakseen tietoja, ja haluttaessa päivittää tiedot ja lähettää ne yhdessä välttämättömien osoite- ja ohjaustietojen kanssa takaisin muistikorttiin 3.

Kuviossa 1 esitetyllä tavalla esillä olevan keksinnön mukainen muistikortti 3 sisältää pääsyn ohjausprosessorin (ACP) 10, joka on kytketty tietoväylään 105 ja määrän (n) CMOS-pikamuistisiruja 103a-103n, jotka on kaikki liitetty tietoväylään 105. ACP 10 on tyypillisesti saman tyyppinen käsittelyelementti, jota käytetään älykortissa. CMOS-pikamuistit 103a-103n voivat Intel Co:n valmistamia pikamuistisiruja. Ne voivat olla esim. Intel 28F001BX-pikamuistisiruja, jotka sisältävät kahdeksan 128 Ktavu x 8 CMOS pikamuistia. Täten 4-Mtavun pikamuistikortti voi sisältää 32 CMOS-pikamuistia, eli "n" = 32.

PÄÄSYN OHJAUSPROSESSORI 10

Kuviossa 2 esitetään lohkokaaviona edullisen sovellutusmuodon mukainen pääsyn ohjausprosessori (ACP). ACP 10 sisältää suojatun haihtumattoman muistin 10-2, työmuistin (RAM) 10-4, mikroprosessorin 10-6, intervallilaskurin 10-8 ja liitäntälohkon 10-10, joka on liitetty tietoväylään 105. Haihtumaton muisti 10-2 tarjoaa useita osoitettuja paikkoja, joihin todennustietoa ja -ohjelmia voidaan tallentaa. Tarkemmin muistipaikat 10-2a sisältävät yhden tai useamman henkilökohtaisen tunnusluvun (PIN), yhteyskäytäntösekvenssin tai muita tunnistustietoja sen varmistamiseksi, että käyttäjällä on pääsyoikeus järjestelmään ja pikamuistien 103a-103n niiden lohkojen tunnistamiseksi, joihin käyttäjällä on pääsy sekä aikaväliarvo, jota käytetään uudelleen todentamiseen.

Muistipaikat 10-2b sisältävät avainarvot, joita käytetään kunkin pikamuistin 103a-103n tai kunkin pikamuistin 103a-103n yksittäisten lohkojen suojaamiseksi käytettyjen koodien suojaamiseksi.

Muistipaikat 10-2c sisältävät ohjelmaohjesekvenssit haluttujen todentamistoimintojen suorittamiseksi ja järjestelmän nollaamiseksi, jos etukäteen annetut epäonnistumisehdot täyttyvät. Tietyt ohjelmaohjeet antavat käyttäjän ohjata uudelleen todennuksen ajankohdan määräävän intervallilaskurin 10-8 asettamista. Uudelleentodennuusintervalli määrittää keskeytysten välisen ajan ja keskeytyksen lähettämisen isäntäprosessorille 5 vaatien käyttäjän identiteetin vahvistamista pyytämällä käyttäjää antamaan uudestaan PIN-koodinsa tai muun salasanan. Intervallilaskuri 10-8 vastaanottaa kellopulsseja isäntäprosessorista 5 tietoväylän 102 kautta ja käyttäjä voi asettaa sen työympäristön mukaisesti. Käyttäjä voi esim. kotona kytkeä ajastimen pois päältä (eli asettaa sen maksimiarvoon), tai asettaa aikaväliksi yksi tunti. Lentokoneessa käyttäjä voi asettaa aikaväliksi kymmenen minuuttia paremman suojan aikaansaamiseksi. Kuten edellä kuvattiin, käyttäjää pyydetään tarkistamaan aikaväli uudelleen joka kerta, kun virta kytketään päälle, jolloin tapahtuu uudelleentodennus säännöllisin aikavälein turvallisuuden parantamiseksi.

PIKAMUISTIT 103a-103n

Kuviossa 3 esitetään yksityiskohtainen lohkokaavio pikamuisteista 103a-103n. Siinä näytetään pelkästään muistin 103a yksityiskohtaiset loogiset piirit, koska muistit 103b-103n ovat identtisiä muistin 103a kanssa.

Pikamuisti 103a käsittää perusmuodossa kaksi osaa, joista toinen käsittää esillä olevan keksinnön mukaiset turvapääsyn ohjauspiirit ja toinen pikamuistin loogiset perus- tai standardipiirit.

Turvapääsyn ohjausosa

Kuvion 3 osoittamalla tavalla esillä olevan keksinnön mukaiset turvaohjauspiirit sisältävät 32-bittisen avainrekisterin, 32-bittisen haihtuvan lukittavan rekisterin 33, 12-bittisen viivelaskurin 32, vertailupiirin 39, YKSI arvon yksi ilmaisevan signaalipiirin 38, haihtumattoman lukittavan muistin 35, yhden bitin haihtumattoman lukittavan varastoinnin mahdollistavan elementin 36, haihtuvan pääsyn ohjausmuistin 43, esitetyllä tavalla sovitetun pääsyn muuntamisen sallivan JA-portin 34 ja TAI-antoportin 45. Huomautetaan, että tämä osa vastaanottaa useiden heksadesimaaliarvojen määräämiä käskyn ohjaussignaaleja (esim. 31H-38H) loogiseen perusosaan sisältyvästä käskyrekisteristä 50. Nämä signaalit osoittavat eri data-arvot

käskysarjassa, jonka käskyrekisteri 50 vastaanottaa ACP:stä 10 dataväylän 105b kautta. Käskyt ovat niiden käskysarjojen tärkeä jatke, joita pikamuisti yleensä käyttää. Tavalliset pikamuistikäskyt ovat samassa muodossa kuin ne, joita 28F001BX pikamuisti yleensä käyttää. Käskyjä kuvataan julkaisussa "Memory Products", jonka Intel Corporation on julkaissut. Esillä olevan keksinnön käyttämät käskyt kuvataan taulukossa 1.

Viitaten kuvioon 1 ensimmäinen käsky, joka esitetään on käsky muistin lukituksen lataamiseksi, jota käytetään satunnaisen numeron kehittämän lukitusarvon lataamiseksi haihtumattomaan lukkomuistiin (LM) 35 kussakin muistissa 103a-103n. Kullakin muistilla 103a-103n saattaa olla eri tai sama lukitusarvo riippuen käyttäjän turvallisuusvaatimuksista. Lukitusarvo ladataan lukitusmuistiin 35 avainrekisterin (K) 31 kautta yksibittisen, haihtumattoman varastoelementin 36 ohjauksessa. Taulukon 1 mukaista käskyä, joka mahdollistaa lukitusmuistin palauttamisen, käytetään muistielementin 36 palauttamiseksi. Tämä estää lukitusmuistiin 35 tallennetun lukitusarvon muuttamisen, koska kun lukitusmuistin palauttamisen mahdollistava käsky on kerran palauttanut muistielementin 36, ei sitä voi enää asettaa. Lukitusmuistin 35 haihtumaton sisältö siirretään L-rekisteriin 3, kun virta kytketään päälle. On syytä huomioida, että lukitusmuistin 35 paikka tai sijainti riippuu suunnittelusta. Muisti 35 voidaan esim. toteuttaa muistijonon 54 jatkeena.

Taulukon 1 mukaista avainrekisterin latauskäskyä käytetään avainrekisterin 31 lataamiseksi ja viivelaskurin 32 asettamiseksi. ACP 10 käyttää viivelaskurin vähennyskäskyä viivelaskurin 32 sisällön vähentämiseksi yhdellä. ACP 10 käyttää lukemisen sallivia ja lukemisen estäviä muistipankkikäskyjä mahdollistamaan tai estämään pääsyn muistijonon 54 eri muistilohkoihin pääsyn ohjausmuistia 43 ladattaessa.

Taulukko 1

	Käsky	1. tietoväylän toimintajakso		Osoitetietoja	2. tietoväylän toimintajakso	Data
5	Lataa lukitusmuisti	Kirjoita		31H	Kirjoita	N/A
	Palauta lukitusmuisti mahdollistus	Kirjoita		33H	N/A	N/A
10	Lataa avainrekisteri	Kirjoita		32H	Kirjoita	Avaintieto
	Vähennä viivelaskuri	Kirjoita		35H	N/A	N/A
15	Lukemisen mahdollistava muistipankki	Kirjoita	MBA	34H	Kirjoita	MBA
	Lukemisen estävä muisti-pankki	Kirjoita	MBA	38H	Kirjoita	MBA

Lataa lukitusmuisti (31H)

Tämä käsky kopioi avainrekisterin 31 sisällön haihtumattomaan lukitusmuistiin 35, jos ja vain jos muistin lukituksen päälle asettava 36 antosignaali on TOSI.

Palauta muistin lukituksen päälleasetus (33H)

Tämä käsky palauttaa muistin lukituksen päälle asettavan loogisen elementin 36 estäen lukitusmuistin 35 lataamisen tai muuttamisen.

Lataa avainrekisteri (32H)

Tämä käsky siirtää avainrekisterin aikaisempaa sisältöä yhden bitin (LSB kohti MSB) ja lataa "avainarvon" ACP:stä 10 avainrekisteriin LSB.

Lisäksi se asettaa viivelaskurin 32 maksimiarvoonsa, esim. kaikki arvot YKSI.

Vähennä viivelaskuri (35H)

Tämä käsky vähentää viivelaskurin 32 YHDELLÄ. Viivelaskurin on oltava yhtä suuri kuin NOLLA, jotta muistijonoa 54 voitaisiin myöhemmin lukea.

Lukemisen mahdollistava muistipankki (34H)

Tämä käsky asettaa muistipankkiosoitetta (MBA) vastaavan bitin pääsyn ohjausmuistiin 43, jos ja vain jos signaali (37), joka kertoo pääsyn muuntamisen päälle asettamisesta, on TOSI. Tällöin valittua pankkia on mahdollista lukea.

Lukemisen estävä muistipankki (38H)

Tämä käsky palauttaa bitin, joka vastaa pääsyn ohjausmuistin 43 muistipankkiosoitetta.

Tarkisteltaessa taulukkoa 1 yksityiskohtaisemmin nähdään, että taulukko 1 esittää myös kaikkien lisäkäskyjen tietoväyläjaksotoiminnot. Kutakin kahta tietoväyläjaksoa vaativaa käskyä kohden käskyrekisteri 50 vastaanottaa ensimmäisen tietoväyläjakson aikana 8-bittisen käskyn, jonka ACP 10 on kehittänyt, ja joka on lähetetty tietoväylän 105 dataväylän 105 a ja syöttöpuskurin 51 kautta. Käskyrekisteri 50 määrää valitun loogisen elementin vastaanottamaan dataväylästä 105b käskyn suorittamiseksi toisen tietoväyläjakson aikana tarvittavan tiedon. Osoitetulla tavalla toinen tietoväyläjakso on määrätty ei soveltuvaksi (N/A), koska lukitusmuistin palauttamisen mahdollistamista ja viivelaskurin vähentämistä koskevien käskyjen toteuttaminen tarvitsee vain yhden jakson.

Normaalitoiminnassa K-rekisteri 31 on ladattu avainarvolla, joka on saatu muistipaikoista 10-2b avainrekisterin lataamista koskevalla käskyllä ja viivelaskuri 32 on asetettu maksimiarvoonsa. Toistuviin ACP:stä 10 tuleviin viivelaskurin vähentämistä koskeviin käskyihin vastataan vähentämällä viivelaskurin arvot NOLLIIN ja kehitetään nollalaskuriantosignaali 41, jota sovelletaan syöttönä JA-porttiin 34.

Jokainen viivelaskuri 32 rajoittaa yritysten määrää, joilla voidaan yrittää päästä pikamuisteihin 103a-103n sellaisessa tapauksessa, kun varas poistaa sirut ja sijoittaa ne "laittomaan korttiin" ja ohjelmoi prosessorin tai laitteiston toistuvasti arvaamaan kunkin muistisirun avainta. Toisella tavalla ilmaistuna laskuri 32 varmistaa, että on yritettävä huomattavan monta kertaa laittomaa pääsyä pikamuisteihin. Avain ja viivelaskuri on mitoitettu siten, että tällainen kokeileminen vie suhteettoman paljon aikaa.

Lähemmin tarkasteltuna avainrekisteri 31 sisältää n. 4 biljoona (232) erilaista yhdistelmää. Edullisessa sovellusmuodossa viivelaskuri 32 on 12-bittinen laskuri. Jos oletetaan, että viivelaskuria 32 vähennetään mikrosekunnin välein, vaatii jokainen yritys arvata avainarvoa 212 tai 4 millisekuntia. ACP 10, joka tietää oikean avainarvon, aiheuttaa vain neljä millisekuntia pitkän viiveen alkuasetukseen. Satunnaiset yritykset arvata avainarvo vaativat 231 yritystä, jolloin onnistumismahdol-

lisuus on 50 %. Avainarvon arvaaminen veisi silloin 231 x 212 mikrosekuntia tai 102 päivää. Tässä ajassa useimmat varkaat luopuvat. Pidempi tai lyhyempi aika aikaansaadaan luonnollisesti muuntamalla avaimen ja viivelaskurin 32 kokoa.

Jos esillä olevan keksinnön mukainen muistikortti varastetaan ja sijoitetaan "laittomaan isäntään", ACP 10 rajoittaa varkaan yrityksiä ratkaista PIN-koodi tunnettujen menetelmien avulla. Tällaiset menetelmät saattavat käsittää pääsyn lukitsemisen tai tietojen tuhoamisen, jos väärien arvausten kynnys ylittyy.

Pikamuistin 103a ensimmäisen todennustoiminnon aikana avainarvo ladataan 32-bittiseen K-rekisteriin 31 neljän perättäisen avainrekisterin lataamista koskevan käskyn jälkeen (dataväylä 105b on bitin levyinen tietoväylä). Viivelaskuri 32 pakotetaan maksimilaskuunsa (kaikki arvot YKSI) ja ACP 10 vähentää sen lähettämällä viivelaskurin vähentämistä koskevia käskyjä perättäisillä ensimmäisen tietoväylän jaksoilla. Kun viivelaskuri 32 on vähennetty arvoon NOLLA se kehittää nollalaskusignaalin 41, jota sovelletaan JA-portin 34 yhteen syöttöön.

Jos K-rekisteriin 31 tallennettu avainarvo on yhtä suuri kuin L-rekisteriin 33 tallennettu lukitusarvo, mikä osoittaa, että käyttäjä antoi oikean tunnistuksen isäntäprosessorille 5, vertaileva logiikka 39 sovittaa yhtä suuria arvoja vertailevan signaalin 42 JA-portin 34 toiseen syöttöön. Tällöin JA-portti 34 kehittää pääsyn muuntamisen päälle asettavan signaalin 37 annossaan, jolloin on mahdolista kirjoittaa ja päästä ohjausmuistiin 43 ACP:n 10 valvonnassa. Tämä puolestaan sallii myöhemmin muistijonon 54 lukemisen.

Pääsyn ohjausmuisti 43 sisältää yhden bitin haihtuvan varastoinnin muistijonon 54 kunkin lohkon/pankin kohdalla. Nämä bitit nollataan osana pikamuistin virta päälle -sekvenssiä. Jotta tiedot luettaisiin muistista 103a osoitettua muistilohkoa vastaavan bitin on oltava loogisesti YKSI. ACP 10 asettaa bitit antaen muistipankin lukemisen sallivia käskyjä jos, ja vain jos pääsyn muuntamisen salliva signaali 37 on TOSI.

Kuten taulukossa 1 esitetään, lukemisen päälle asettavan muistipankkikäskyn toisen tietoväyläjakson aikana muistijonon 54 valitun muistipankin kolme (3) ylintä osoitebittiä lähetetään osoiteväylää 105c pitkin ja heksadesimaalikäskytunnistimen toisto lähetetään dataväylää 105a pitkin käskyrekisteriin 50. Tämän tuloksena kirjoitetaan YKSI pääsyn ohjausmuistin 43 osoitettuun bittisijaintiin. Edullisessa sovellutusmuodossa muistipankin lukemisen salliva käskysekvenssi toistetaan kahdeksan kertaa, koska muistijono 54 on järjestetty kahdeksaan pankkiin, jotka

kaikki käsittävät 16 Ktavua. ACP 10 voi rajoittaa pääsyä valittuihin pankkeihin antamalla vastaavalla tavalla sekvenssin muistipankin lukemisen estäviä käskyjä.

Esillä olevan keksinnön mukaisen pääsyn ohjausmuistin 43 antoa sovelletaan päälle asettavana ottona antopuskuriin 52 pikamuistin jokaisen lukujakson aikana, kun muistijonon 54 jonkin pankin sijainnin sisältöä luetaan. Toisin sanoen saattaa lukujakso esiintyä, vaikka luettavia tietoja on estetty kulkemasta antopuskurin 52 läpi sopivan pankin pääsyn ohjausmuistin avainnusignaalin puuttuessa. Tarkemmin edullisessa sovellusmuodossa pääsyn ohjausmuisti 43 sisältää kahdeksan yksitellen osoitettavaa bittimuistielementtia, 8-bittisen dekooderin otto-osoitteen 3, joka dekooderi on liitetty kunkin muistielementin ottoon ja 1-8 antokanavointilaitepiirin, joka on liitetty kunkin muistielementin antoon. Kunkin osoitteen kolmen ylimmän osoitebitin koodit tulkitaan ja niitä käytetään sen lohkon muistielementin valitsemiseksi, jonka sisältöä muutetaan. Vastaavalla tavalla näitä kolmea bittiä käytetään sen lohkon muistielementin annon valitsemiseksi, joka sisältää luettavan pikamuistipaikan.

Jos lukitusmuisti 35 tyhjennetään täysin, eli jos L-rekisterin 33 sisällön osoittamat arvot ovat YKSI ovat kaikki YKSI, antopuskuri 52 on aina päällä. Eli kun lukitusrekisteri 33 sisältää arvot "KAIKKI YKSI", tämä kehittää signaalin KAIKKI YKSI ilmaisinelementistä 38 TAI-porttiin 45 antopuskurin 52 kytkemiseksi päälle. Tämä asettaa pikamuistin 103a tehokkaasti ei-turvattuun tilaan. Tällöin on mahdollista ohittaa kaikki esillä olevan keksinnön mukaiset loogiset turvallisuuspiirit. Täten samaa pikamuistisirua voidaan käyttää sekä turvallisiin että ei-turvattuihin sovelluksiin, mikä säästää tuotantokustannuksia.

Pikamuistin loogiset peruspiirit

Kuten kuviossa 3 esitetään nämä piirit sisältävät muistijonon 54, komentorekisterin 50, loogiset otto/anto-piirit 60, osoitesalvan 56, kirjoitustilakoneen 61, järjestelmän 62 pyyhkimisen suorittamiseksi jännitteellä, antokanavointilaitteen 53, tietorekisterin 55, ottopuskurin 51, antopuskurin 52 ja tilarekisterin 58. Edellä mainitulla tavalla pikamuistin 103a loogiset peruspiirit ovat usein samantyyppisiä kuin Intel Corporationin valmistamassa pikamuistissa 28F001BX. Koska tällaiset piirit ovat tavanomaisia, niitä kuvataan vain välttämättömiltä osilta. Lisätietoa tällaisista piireistä saa julkaisusta "Memory Products", sivut 3-109 - 3-134, tilausnro 210830, julkaisija Intel Corporation vuonna 1992. Kuviossa 3 esitetyllä tavalla pikamuistin peruspiirit vastaanottavat useita syöttösignaaleja (AO-A16), osoite-, datasignaaleja

(D00-D07) sekä ohjaussignaaleja (CE, WE, OE, PWD ja VPP). Signaalit kuvataan seuraavassa taulukossa 2.

Taulukko 2. Signaalien kuvaus

Symboli	Nimi ja toiminto
AO-A16	Muistiosoitteiden OSOITESYÖTÖT. Osoitteet lukitaan sisäisesti kirjoitusjakson aikana.
D00-D07	TIETOJEN SYÖTTÖ/TULOSTUS: Syöttää tiedot ja käskyt muistin kirjoitusjaksojen aikana; tulostaa tietoja muistin ja tilan kirjoitusjaksojen aikana. Dataneulat ovat aktiivisia ylhäällä ja kulkeutuvat tilanteessa pois, jos sirua ei valita tai annot estetään. Tiedot lukitaan sisäisesti kirjoitusjakson aikana.
CE	SIRUN ASETTAMINEN PÄÄLLE: Aktivoi laitteen ohjauslogiikan, ottopuskurit, dekooderit ja linjailmaisimet. CE on aktiivinen alhaalla, CE ylhäällä jättää muistilaitteen valitsematta ja vähentää virran kulutuksen valmiustasolle.
PWD	VIRTATILAN LASKU: Asettaa laitteen virtatilan alas. PWD on aktiivinen alhaalla; PWD korkealla johtaa normaalitoimintaan. PWD=VHH mahdollistaa muistilohkojen ohjelmoimisen. Lisäksi PWD lukitsee pois tyhjennys- tai kirjoitustoiminnot ollessaan aktiivinen alhaalla suojaten tietoja virtasiirtojen aikana.
OE	ANNON ASETTAMINEN PÄÄLLE: Ohjaa laitteen annot tietopuskureiden läpi lukujakson aikana. OE on aktiivinen alhaalla.
WE	KIRJOITUKSEN ASETTAMINEN PÄÄLLE: Ohjaa kirjoituksia komentorekisteriin ja jonolohkoihin. WE on aktiivinen alhaalla. Osoitteet ja tiedot lukitaan WE-pulssin nousevaan reunaan.
Vpp	POISTA/OHJELMAN VIRTALÄHDE kunkin lohkon jonon tai ohjelmointibittien lohkojen poistamiseksi. Huomaa: Kun Vpp < Vppl Max, muistin sisältöä ei ole mahdollista muuttaa.

Taulukossa 2 esitetyllä tavalla sirun (CE), kirjoituksen (WE) ja annon (OE) päälle asettavia signaaleja sovelletaan komentorekisteriin 50 ja I/O-logiikkaan 60 isäntäprosessorista tietoväylän 102 ja ohjausväylän 105b kautta ja ne hajotetaan mää-

rättyjen logiikkalohkojen ohjaamiseksi. Virtatilan laskevaa signaalia (PWD) sovelletaan myös komentorekisteriin 50, jotta pikamuisti pystyisi suorittamaan taulukossa 2 määritetyt toiminnot. Tätä signaalia voidaan käyttää pikamuistin turvallisuusohjausalueen haihtuvien muistielementtien tyhjentämiseksi halutulla tavalla, jolloin käyttäjä pakotetaan uudestaan todentamaan henkilöllisyytensä normaalien toimintojen jatkuessa.

Pikamuistin loogiset peruselementit toimivat yleisesti seuraavalla tavalla. Tietoja tallennetaan muistijonoon 54 dataväylän 105a, ottopuskurin 51 ja tietorekisterin 55 kautta osoitettuun paikkaan yhdessä muistilohkoista, jonka määrittää osoitelogiikka 56 osoiteväylästä 105c saamansa osoitteen avulla. Muistijonon 54 pankki lukee tietoja määrätystä osoitepaikasta, jotka tiedot lähetetään isäntäprosessoriin 5 antokanavointilaitteen 53, antopuskurin 52, dataväylän 105a ja tietoväylän 102 kautta. Statusrekisteriä 58 käytetään kirjoitustilakoneen, virheen erottavan tilan, poistotilan, ohjelmatilan ja Vpp-tilan tallentamiseksi.

Kirjoitustilakone 61 ohjaa lohkojen tyhjentämistä ja ohjelman algoritmejä. Ohjelma/poistojännitejärjestelmää 62 käytetään muistijonon 54 tai kunkin lohkon ohjelmointibittien lohkojen poistamiseksi Vpp-tason funktiona (eli kun Vpp on korkealla ohjelmointi voi tapahtua; jos Vpp on alhainen, muistijono 54 toimii lukumuistina.

Seuraavassa kuvataan esillä olevan keksinnön mukaisen turvallisen muistikortin toimintaa viitaten erityisesti kuvioiden 4 ja 5 mukaiseen vuokaavioon. Ennen kuin toimintoja kuvataan yksityiskohtaisemmin kuvataan ensin muistikortin valmistukseen, toiveiden mukaan muokkaamiseen ja toimintaan liittyvät vaiheet.

Kortin valmistuksen ensimmäisessä vaiheessa ACP 10 asettaa muistikortin jokaisen muistisirun lukitusarvon. Tämän se tekee lataamalla avainarvon kuviossa 3 esitettyyn lukitusmuistiin. Arvot tallennetaan ACP:n suojattuun haihtumattomaan muistiin 10-2 (eli kuvion 2 avaimet 1-n). Tämän jälkeen lukitusmuistin päälle asettavat elementit 36 asetetaan arvoon NOLLA lukitusmuistin tietojen edelleen muuttamisen tai lukemisen estämiseksi. Koska nämä elementit ovat haihtumattomia, niitä ei ole mahdollista muuttaa ellei koko pikamuistisirua tyhjennetä.

Toisessa vaiheessa toiveiden mukaan muokkaamisen yhteydessä, muistikorttiin voidaan ladata sen tiedot tai ohjelmasovellus, koska suojatoiminta ei vaikuta kirjoitukseen. Tämän jälkeen ACP:hen 10 ladataan muistin pankkirakenteeseen liittyviä tietoja sekä kuhunkin muistipankkiin sovellettavat suoja-asteet.

Kolmannessa vaiheessa toiveiden mukaan muokkaamisen yhteydessä, käyttäjä perustaa parametrit taajuudelle ja todennustoiminnolle ja tarvittaville erityistiedoille (esim. henkilökohtaiset tunnistenumerot PIN). Kyseiset tiedot tallennetaan ACP:n muistiin.

Neljännessä vaiheessa, kun virta on päällä "avainrekisteri", "pääsyn muuntamisen päälle asettava" signaali ja "pääsyn ohjausmuisti" alustetaan siten, että ne estävät pääsyn tietoihin tai kirjoittamisen pääsyn ohjausmuistiin 43. Ensimmäinen todennusdialogi käynnistyy.

Ensimmäisessä todennusdialogissa ACP 10, isäntäprosessorin 5 palveluja hyväksikäyttäen kehottaa käyttäjää ja vastaanottaa todennustietoja. Jos todennus epäonnistuu ei toimintoa suoriteta; jos todennus onnistuu kunkin muistisirun avainrekisteriin ladataan ACP:n muistiin tallennettu arvo. Tämän toiminnon aikana viivelaskuria 32 käytetään estämään sirun toiminta tietyksi ajaksi latauksen jälkeen, jolloin satunnaisista yrityksistä tehdään tulokseton prosessi. Avainrekisterien lataaminen saa "pääsyn muuntamisen päälle asettavan" signaalin olemaan tosi kussakin sirussa. Tämän jälkeen ACP 10 perustaa pääsyn lataamalla pääsyn ohjausmuistit tallennetun tietokokoonpanon mukaisesti.

Kuudennessa vaiheessa, edellistä seuraavan todennusdialogin yhteydessä, ACP 10 aika ajoin käyttäjän kokoonpanon mukaisesti kehottaa käyttäjää uudestaan todentamaan henkilöllisyytensä (uudelleen todennus). Jos todennus epäonnistuu, ACP 10 pakottaa kaikki muistisirut virta päälle -tilaan, jolloin pääsy muistien tietoihin estyy, koska pääsyn ohjausmuisti 43 tyhjenee ja avainrekisterin 31 sisältö tyhjenee. Seuraavassa kuvion 1 mukaisen järjestelmän toimintaa selitetään viitaten kuvioihin 4 ja 5.

Päivän alkutoiminnot

Kuvio 4 esittää lohkokaavion muodossa eri toimintamuodot. Lohkot 402 ja 401 esittävät kaksi käynnistystilaa. Lohkossa 402 käyttäjä vie muistikortin 3 sisään aikaisemmin käynnistettyyn isäntäprosessoriin 5. Lohkossa 401 käyttäjä käynnistää isäntäprosessorin 5, kun muistikortti 3 on jo asennettu siihen.

Kummassakin käynnistystoiminnossa lohkon 402 aikana ACP 10 ja sen liittymät alustetaan tavanomaisella tavalla, ja lohko 403 tyhjentää kaikki 'n' K-rekisterit 31 ja 'n' pääsyn ohjausmuistit 43 osana pikamuistien 103a-103n sisäistä alustamissekvenssiä. Tämä estää tietojen lukemisen muisteista 103a-103n, koska jokaisen

muistin antopuskuri 52 on pois päältä. Lukitusarvo ladataan 'n' L-rekistereihin 33 kultakin LM:ltä 35, kun virta kytketään päälle.

Lohkossa 404 ACP 10 lähettää keskeytyssignaalin isäntäprosessoriin 5, joka vastaa vaatimalla käyttäjältä PIN-koodia tai muuta tunnistustietoa. Lohkossa 405 ACP 10 muistipaikkoihin 10-2a tallennetun ohjelman avulla tarkistaa, että PIN-koodi tai muut tunnistustiedot vastaavat muistipaikkoihin 10-2a tallennettuja tietoja. Mikäli ne eivät vastaa, päätöksentekolohko 406 laskee virheen ja ACP 10 haarautuu lohkoon 407 saadakseen ACP:n 10 joko lukitsemaan tai tuhoamaan muistien 103a-103n sisällöt.

Ensimmäinen käyttäjän todennus onnistuu

Jos päätöksentekolohko 406 sisältää vastaavan tiedon, joka osoittaa todennuksen onnistuneen, ACP 10 lohkossa 408 avainrekisterin lataamista koskevan käskyn kautta lataa jokaisen K-rekisterin 31 muistipaikoista 10-2b sopivalla avainarvolla. Lisäksi lohko 409 toistuvasti vähentää viivelaskurin 32 sisältöä antaen peräkkäin viivelaskurin vähentämistä koskevat käskyt tavoitteena binäärinollalasku, mikä johtaa kuvion 3 nollalaskusignaalin 41 luomiseen.

Lohkossa 410 jokainen pääsyn ohjausmuistin 43 paikka on ladattu tiedoilla muistipankin lukemisen käynnistävällä käskyllä, jolloin on mahdollista päästä vastaavan pikamuistin 103a-103n valittuihin pankkeihin.

Ajoittainen uudelleen todennus

Lohkossa 411 ACP 10 odottaa, että intervallilaskurin 10-8 viestittämä ennaltamäärätty aikaväli, jonka muistipaikkoihin 10-2a tallennetut tiedot ovat perustaneet, päättyy ennen kuin se pyytää käyttäjältä uudelleen todennusta. Tämän jälkeen ACP 10 lohkossa 412 keskeyttää isäntäprosessorin 5 pyytääkseen käyttäjää antamaan uudestaan PIN-koodin tai muun pyydetyn tunnisteen.

Päätöksentekolohko 413 tarkistaa PIN-koodin tai muun prosessorilta 5 saadun tiedon ja vertaa sitä muistipaikkoihin 10-2a tallennettuihin tietoihin ja intervalliajastimen 10-8 anto tallennetaan. Käyttäjällä on etukäteen asetettu aikaväli, joka on yleensä 30 sekuntia pitkä, jonka aikana hänen on syötettävä todennustiedot isäntäprosessoriin 5. Sillä aikaa, kun kello käy, lohko 414 rekisteröi kokeen virheeksi, jos päätöksentekolohkon 413 testi epäonnistuu. Tällöin se tarkistaa vastaanotettiinko maksimaalinen virhemäärä ja haarautuu toistaakseen lohkot 412 ja 413. Jos virheiden lukumäärä vastaa maksimimäärää, APC 10 lohkossa 415 tyhjentää pi-

kamuistin K-rekisterin 31 peräkkäisillä avainrekisterin latauskäskyillä ja tyhjentää pääsyn ohjausmuistit 43 peräkkäisillä muistin lukemisen estävillä käskyillä. Tämän jälkeen lohko 415 haarautuu lohkoon 404 mahdollistaakseen uuden "ensimmäisen todennustapahtuman".

Jos päätöksentekolohkossa 413 suoritettava koe onnistuu, K-rekisteri 31 pysyy muuttumattomana (eli se sisältää ACP:n aikaisemmin lataaman avainarvon), jolloin käyttäjä pystyy jatkamaan järjestelmän 1 käyttämistä. Siinä tapauksessa, että 30 sekuntia kuluu ilman, ett päätöksentekolohko 413 vastaanottaa PIN-koodin tai muun tiedon, ACP 10 tyhjentää K-rekisterin 31 ja pääsyn ohjausmuistin 43 samalla tavalla kuin aikaisemmin.

Kuvio 5 esittää vuokaavion, joka kuvaa miten isäntäprosessori 5 reagoi APC:n 10 todennusta varten esittämään keskeytyspyyntöön vastauksena kuvion 4 lohkoihin 404 ja 412. Esitetyllä tavalla päätöksentekolohko 501 odottaa keskeytystä ACP:ltä 10 ja pyyntöä, että käyttäjä syöttäisi uudelleen PIN-koodin tai muun tiedon. Päätöksentekolohko 501 haarautuu lohkoon 502, kun se vastaanottaa keskeytyksen lohkoilta 404 tai 412. Lohko 502 esittää PIN-koodia tai muuta tietoa koskevan pyynnön isäntänäytöllä 5-2. Lohko 503 hyväksyy näppäimistöltä tulleet tiedot ja lohko 504 keskeyttää ACP:n 10. Lohko 5 lähettää PIN-koodin ACP:lle 10.

Alan ammattimies ymmärtää, että esilä olevan keksinnön edullista sovellutusmuotoa voidaan muuttaa monella tavalla poikkeamatta sen piiristä. Keksintöä voidaan esimerkiksi käyttää yhdessä eri tyyppisten haihtumattomien muistien, liittymien jne. kanssa.

Vaikka ehtojen ja sääntöjen mukaisesti on kuvailtu ja selitetty keksinnön paras muoto siihen voidaan tehdä tiettyjä muutoksia poikkeamatta keksinnön piiristä siten, kuin se on oheisissa patenttivaatimuksissa esitetty ja joissakin tapauksissa voidaan keksinnön tiettyjä ominaisuuksia käyttää edullisesti käyttämättä vastaavalla tavalla sen muita ominaisuuksia.

Patenttivaatimukset

1. Turvallinen muistikortti, jota käytetään kannettavassa isäntätietokoneessa, joka muistikortti käsittää:

mikroprosessorin (10-6), joka on liitetty välittämään osoite-, data- ja ohjaustietoja isäntäkoneelle (5) ja vastaanottamaan niitä siltä, ja joka mikroprosessori sisältää ensimmäisen osoitettavan haihtumattoman muistin (10-2) tietojen tallentamiseksi, jotka sisältävät avainarvoja ja kokoonpanotietoja;

sisäisen tietoväylän (105), joka on liitetty mainittuun mikroprosessoriin osoite-, data- ja ohjaustietojen välittämiseksi, jotka määrittävät muistitoimintoja, jotka kortin on tarkoitus suorittaa; ja

joukon toisia osoitettavia haihtumattomia muisteja, joista ainakin yksi osoitettava haihtumaton muisti (103a) on liitetty sisäiseen tietoväylään yhdessä mikroprosessorin kanssa osoite-, data- ja ohjaustietojen vastaanottamiseksi, jolloin sanottu muisti sisältää haihtumattoman muistiosan ja turvallisuustarkistusosan, joista muistiosa käsittää toisaalta muistijonon (54), joka on organisoitu useaksi lohkoksi, joista jokaisella lohkolla on lukuisia osoitettavia paikkoja, ja toisaalta loogisen ohjausvälineen (50) muistitoimintojen suorittamiseksi, turvallisuustarkistusosan ollessa liitetty mainittuun sisäiseen tietoväylään, loogiseen ohjausvälineeseen ja muistijonoon, jolloin turvallisuustarkistusosa sisältää:

useita haihtumattomia (31, 35) ja haihtuvia (33, 43) tallennuslaitteita ainakin yhden avainarvon tallentamiseksi ja lohkoihin liittyviä kokoonpanotietoja; ja

loogisen pääsynohjausvälineen (32, 34, 39), joka on liitetty mainittuun loogiseen ohjausvälineeseen (50) ja tallennuslaitteisiin, jolloin looginen pääsynohjausväline mahdollistaa muistijonon osoitettuihin lohkoihin tallennettujen tietojen lukemisen kokoonpanotietojen määrittämällä tavalla vasta sitten, kun mikroprosessori on määritellyt, että ennalta määrätty todennustoimenpide on suoritettu isäntäkoneessa ja se on asettanut loogisen pääsynohjausvälineen päälle, jolloin tämä sallii tietojen lukemisen muistijonosta kokoonpanotietojen mukaisesti.

2. Patenttivaatimuksen 1 mukainen muistikortti, **tunnettu** siitä, että mikroprosessori (10-6) ja haihtumaton muisti (103a) sisältyvät erillisiin puolijohdesiruihin.

3. Patenttivaatimuksen 1 mukainen muistikortti, **tunnettu** siitä, että kortti sisältää edelleen liitäntäpiirivälineen (104), joka kytkee kortin (13) isäntäkoneeseen (5) ja että liitäntäpiiriväline ja mikroprosessori sisältyvät samaan puolijohdesiruun.

4. Patenttivaatimuksen 1 mukainen muistikortti, **tunnettu** siitä, että haihtumaton muisti (103a) ja haihtumattomat tallennuslaitteet (31, 35) ovat pikamuisteja.

5. Patenttivaatimuksen 1 mukainen muistikortti, **tunnettu** siitä, että yksi haihtumattomista tallennuslaitteista on lukitusmuisti (35) lukitusarvon tallentamiseksi, joka vastaa yhtä avainarvoista, ja toinen haihtumattomista laitteista on lukitustallennuksen päälleasettamiselementti (36), joka on liitetty lukitusmuistiin (35), jolloin lukitusmuistiin alunperin on ladattu lukitusarvo ja lukitustallennuksen päälleasettamiselementti on kytketty tilaan, joka estää lukitusarvon muuntamisen mikroprosessorin valvonnan alla.

6. Patenttivaatimuksen 2 mukainen muistikortti, **tunnettu** siitä, että lukitusarvon tallennus ja lukitustallennuksen päälleasettamiselementin (36) kytkeminen tapahtuu muistikortin alkuperäisessä valmistusvaiheessa.

7. Patenttivaatimuksen 5 mukainen muistikortti, **tunnettu** siitä, että yksi haihtuvista tallennuslaitteista on osoitettava pääsyn ohjausmuisti (43), jossa on lukuisia paikkoja, jotka lukumäärältään vastaavat muistijonon (54) lohkojen lukumäärää kokoonpanotietojen tallentamiseksi, pääsyn ohjausmuisti on liitetty sisäiseen tietoväylään (105) ja loogiseen pääsynohjausvälineeseen (32, 34, 39), pääsyn ohjausmuisti ladataan mikroprosessorin (10-6) valvonnan alla vasta sitten, kun mikroprosessori on määrittänyt, että ennalta määritetty todennustoimenpide on ensin suoritettu onnistuneesti isäntäkoneessa (5), jolloin looginen pääsynohjausväline asettaa pääsyn ohjausmuistin (43) päälle.

8. Patenttivaatimuksen 7 mukainen muistikortti, **tunnettu** siitä, että lukitusmuistiin (35) ladattu lukitusarvo käsittää vain arvoja YKSI ja että turvallisuustarkastusosa edelleen sisältää pelkästään arvoja YKSI käsittävän ilmaisinpiirin (38), joka on liitetty lukitusmuistiin, jolloin ilmaisinpiiri pelkästään arvoja YKSI sisältävän lukitusarvon perusteella luo signaalin, joka tehokkaasti ohittaa turvallisuustarkastusosan ja mahdollistaa mainitun haihtumattoman muistin (103a) toiminnan ikään kuin turvallisuustarkastusosaa ei olisi.

9. Patenttivaatimuksen 7 mukainen muistikortti, **tunnettu** siitä, että ennalta määrätty todennustoimenpide aluksi suoritetaan, kun muistikortti (3) ensimmäiseen kerran liitetään kommunikoimaan isäntäkoneen (5) kanssa.

10. Patenttivaatimuksen 9 mukainen muistikortti, **tunnettu** siitä, että pääsyn ohjausväline sisältää lukitusrekisterin (33), joka on liitetty vastaanottamaan lukitusarvo lukitusmuistista (35), vertailupiirin (39), avainrekisterin (31) mikroprosessorin avainrekisteriin siirtämän avainarvon tallentamiseksi, viivelaskurin (32) ennalta määrätyn aikavälin määrittävän laskun tallentamiseksi ja veräjävälineen (34), joka on liitetty pääsyn ohjausmuistiin (43), vertailijaan ja viivelaskuriin, jolloin vertailupiiri on liitetty lukitus- ja avainrekistereihin ja veräjävälineeseen ja veräjäväline on liitetty viivelaskuriin pääsyn muuntamisen päälle asettavan signaalin kehittämiseksi, kun vertailupiiri viestittää identtisestä vertailusta lukituskoodiarvon välillä, joka on ladattu lukitusrekisteriin (33), kun viivelaskuri (32) on viestittänyt ennalta määrätyn aikavälin päättyvän, pääsyn muunneltavuuden päälle asettavan signaalin ehdollistaen pääsyn ohjausmuistin (43) kokoonpanotietojen lataamiseksi.

11. Patenttivaatimuksen 10 mukainen muistikortti, **tunnettu** siitä, että looginen ohjausväline (50) sisältää piirit komentosignaalien luomiseksi ennalta määrätyn komentosarjan perusteella, jota mikroprosessori käyttää kunkin muistisirun turvallisuustarkastusosan toiminnan ohjaamiseksi.

12. Patenttivaatimuksen 11 mukainen muistikortti, **tunnettu** siitä, että looginen ohjausväline (50) mikroprosessorin luoman ensimmäisen ennalta määrätyn käskysarjan perusteella luo ensimmäisen signaalin lukituskoodiarvon lataamiseksi lukitusmuistiin (35), jolloin ensimmäinen ennalta määrätyistä käskyistä on luotu kortin alkuperäisessä valmistusvaiheessa.

13. Patenttivaatimuksen 12 mukainen muistikortti, **tunnettu** siitä, että looginen ohjausväline (50) mikroprosessorin luoman toisen ennalta määrätyn käskysarjan perusteella luo toisen signaalin lukitustallennuksen päälleasettamiselementin (35) kytkemiseksi ennalta määrättyyn tilaan, joka estää lukitusmuistiin (35) tallennetun lukitusarvon lukemisen tai muuntamisen.

14. Patenttivaatimuksen 12 mukainen muistikortti, **tunnettu** siitä, että looginen ohjausväline (50) mikroprosessorin luoman kolmannen ennalta määrätyn käskysarjan perusteella luo kolmannen signaalin, joka lataa avainrekisteriin (31) ennalta määrätyn avainarvon, jolloin mikroprosessori luo kolmannen ennalta määrätyistä käskysarjoista vasta sitten, kun mikroprosessori on määritellyt, että ennalta määrätty todennustoimenpide on suoritettu onnistuneesti.

15. Patenttivaatimuksen 14 mukainen muistikortti, **tunnettu** siitä, että loogisen ohjausvälineen (50) luoma kolmas signaali samanaikaisesti pakottaa viivelaskurin

(32) ennalta määrättyyn laskuun ennalta määrätyn aikajakson alun perustamiseksi ja että looginen ohjausväline mikroprosessorin luoman ennalta määrätyn käskysarjan joka neljännen sarjan perusteella vähentää yhdellä ennalta määrätyn laskun, jolloin viivelaskuri viestittää sen aikajakson päättymisen, joka tulee, kun ennalta määrätty määrä ennalta määrättyjen käskyjen joka neljänsiä käskyjä on suoritettu.

16. Patenttivaatimuksen 11 mukainen muistikortti, **tunnettu** siitä, että looginen ohjausväline (50) mikroprosessorin kehittämän ennalta määrätyn käskysarjan viidensien ja kuudensien käskysarjojen perusteella luo viidennen ja kuudennen signaalin paikkojen asettamiseksi ja uudelleen asettamiseksi pääsyn ohjausmuistissa (43) kokoonpanotietojen mukaisesti niiden lohkojen määrittämiseksi, joista tietoja saa lukea.

17. Patenttivaatimuksen 11 mukainen muistikortti, **tunnettu** siitä, että tallennuslaitteet käsittävät

haihtumattoman lukitusmuistin (35) ennalta määrätyn lukitusarvon vastaanottamiseksi ja tallentamiseksi pysyvästi, joka arvo vastaa yhtä avainarvoa määrätystä määrästä avainarvoja;

että mikroprosessori (10-6) on sovitettu lähettämään toiselle haihtumattomalle muistille (103a) yhden mainituista avainarvoista sisäistä väylää käyttäen, mikäli ennalta määrätty todennustoimenpide on suoritettu onnistuneesti isäntäkoneessa (5);

loogisen pääsyn ohjausvälineen (32, 34, 36) ollessa sovitettu ilmaisemaan, milloin mainittu lähetetty avainarvo vastaa lukitusarvoa, sekä mahdollistamaan muistijonon (54) lukemisen kun vastaavuus on todettu.

18. Menetelmä turvallisen muistikortin rakentamiseksi, joka asennetaan isäntäkoneeseen (5), joka käsittää useita haihtumattomia muistisiruja (103a, 103b,... 103n), jokainen muistisiru sisältää muistijonon (54), joka on organisoitu osoitettavia paikkoja sisältäväksi lohkoksi, ja loogiset ohjauspiirit (50) komentosignaalien luomiseksi, jotka signaalit suorittavat muistitoimintoja, joka menetelmä käsittää seuraavat vaiheet:

(a) mikroprosessori (10) sisällytetään korttiin ja yhdistetään olemaan yhteydessä isäntäkoneeseen, kun se asennetaan siihen, mikroprosessori sisältää osoitettavan haihtumattoman muistin (10-2) tietojen tallentamiseksi mukaan lukien useita

avainarvoja, jotka määrittävät käyttäjän pääsyn muistialueille ja muistikokoonpanotietoja, jotka määrittävät pääsyn muistialueille;

(b) loogiset turvallisuuspiirit sisällytetään jokaiseen haihtumattomaan muistisiruun, jolloin loogiset turvallisuuspiirit sisältävät haihtumattoman lukitusmuistin (35) ennalta määrätyn lukitusarvon tallentamiseksi, joka vastaa yhtä avainarvoa, loogisen pääsyn ohjausvälineen (32, 34, 39), joka on liitetty lukitusmuistiin ja osoitettavan haihtuvan pääsyn ohjausmuistin (43), joka käsittää lukuisia paikkoja, joiden määrä vastaa niiden lohkojen määrää, joihin tallennetaan pääsyä koskevaa bittitietoa kokoonpanotietojen mukaisesti;

(c) yhdistetään mikroprosessori jokaiseen muistisiruun osoite-, data- ja ohjaustietojen välittämiseksi kuhunkin muistisiruun;

(d) muunnellaan loogisia ohjauspiirejä (50) siten, että ne reagoivat lukuisiin käskyihin loogisten turvallisuuspiirien käyttämiseksi;

(e) sovitetaan mikroprosessori (10-6) niin, että se suorittaa ennalta perustetun käyttäjän alkutodennuksen isäntäkoneessa (5); kun käyttäjä pyytää pääsyä lohkoihin; ja

(f) sovitetaan mikroprosessori (10-6) niin, että se sallii loogisten turvallisuuspiirien siirtävän tietyt lukuisista käskyistä kuhunkin siruun vasta sitten, kun vaiheen (e) mukainen todennustoimenpide on onnistuneesti suoritettu, sallien eri lohkoihin tallennettujen tietojen lukemisen pääsyn ohjausmuistiin tallennetun pääsyä koskevan bittitiedon mukaisesti.

19. Patenttivaatimuksen 18 mukainen menetelmä, **tunnettu** siitä, että mikroprosessorin haihtumaton muisti (10-2) käsittää useita osia ja että vaihe (a) edelleen käsittää vaiheet, joissa mikroprosessori luo avainarvoille satunnaisarvot ja avainarvot ladataan ensimmäiseen (10-2b) useista osista.

20. Patenttivaatimuksen 18 mukainen menetelmä, **tunnettu** siitä, että mikroprosessori edelleen sisältää intervallilaskurin (10-8), joka on liitetty mikroprosessorin haihtumattomaan muistiin (10-2), ja että vaihe (a) edelleen käsittää vaiheet, joissa mikroprosessori luo käyttäjän valitseman aikavälin sekä lataa tätä valittua aikaväliarvoa vastaavan arvon intervallilaskuriin, ja että menetelmä edelleen käsittää seuraavat vaiheet:

(g) mikroprosessori määräajoin alustaa vaiheen (e) mukaisen käyttäjän todennustoimenpiteen käyttäjän valitsemalla aikavälillä; ja

(h) sallitaan edelleen lohkoihin tallennettujen tietojen lukeminen pääsyä määrittelevän bittitiedon mukaisesti niin kauan, kuin vaiheen (b) mukainen todennus suoritetaan onnistuneesti.

Patentkrav L 18

1. Säkert minneskort för användning i en portabel värddator, vilket minneskort innefattar:

en mikroprocessor (10-6) kopplad för sändning och mottagning av adress-, data- och styrinformation till och från nämnda värddator (5) samt innehållande ett första adresserbart beständigt minne (10-2) för att lagra information som inkluderar ett antal nyckelvärden och konfigurationsinformation;

en intern bussledning (105) kopplad till sagda mikroprocessor för överföring av adress-, data- och styrinformation som definierar minnesoperationer som skall utföras av nämnda kort: och

ett antal andra adresserbara beständiga minnen inkluderande åtminstone ett andra beständigt minne (103a) som är anslutet till sagda interna bussledning tillsammans med mikroprocessorn för att mottaga sagda adress-, data- och styrinformation, varvid sagda minne innefattar en beständig minnessektion och en säkerhetskontrollsektion, där sagda minnessektion innehåller å ena sidan en minnesrad (54) anordnad till ett antal block där vart och ett block har ett flertal adresserbara positioner, och å andra sidan styrlogikdon (50) för att utföra sagda minnesoperationer, och sagda säkerhetskontrollsektion är ansluten till sagda interna bussledning, till sagda styrlogikdon och sagda minnesrad, varvid säkerhetskontrollsektionen innefattar:

ett antal beständiga (31, 35) och obeständiga (33, 43) lagringsdon för att lagra åtminstone ett av sagda nyckelvärden och konfigurationsinformationen som ansluter sig till sagda block; och

access-styrlogikdon (32, 34, 39) anslutna till sagda styrlogikdon (50) och sagda lagringsdon, varvid access-styrlogikdonen möjliggör utläsning av informationen som lagrats i addresserade av sagda block i minnesraden (54) såsom specificeras genom konfigurationsinformationen, endast efter det sagda mikroprocessor har

fastställt att en bestämd autentikationsprocedur har utförts med värddatorn och har påkopplat access-styrlogiken för att medge utläsning av sagda information från minnesraden i enlighet med konfigurationsinformationen.

2. Minneskort enligt patentkravet 1, **kännetecknat** av att mikroprocessorn (10-6) och det beständiga minnet(103a) befinner sig på separata halvledarchips.

3. Minneskort enligt patentkravet 1, **kännetecknat** av att kortet därtill innefattar interfacekretsdon (104) som kopplar nämnda kort (13) till värddatorn (5) och där interfacekretsdonet och sagda mikroprocessor är inkluderade på samma halvledarchips.

4. Minneskort enligt patentkravet 1, **kännetecknat** av att sagda beständiga minne (103a) och sagda beständiga lagringsdon (31, 35) utgörs av snabbminnen.

5. Minneskort enligt patentkravet 1, **kännetecknat** av att ett av sagda beständiga lagringsdon utgörs av ett låsminne (35) för att lagra ett låsvärde motsvarade sagda ena nyckelvärde, och ett andra av sagda beständiga lagringsdon är ett påkopplingselement (36) för låslagring som är anslutet till sagda låsminne (35), varvid låsminnet inledningsvis är lagrat med sagda låsvärde och påkopplingselementet för låslagringen är kopplat till ett läge som förhindrar modifikation av sagda låsvärde under styrning av mikroprocessorn.

6. Minneskort enligt patentkravet 2, **kännetecknat** av att lagring av sagda låsvärde och omkoppling av sagda element (36) för påkoppling av låslagringen sker under kortets ursprungliga framställningsskede.

7. Minneskort enligt patentkravet 5, **kännetecknat** av att sagda obeständiga lagringsdon utgörs av adresserbart access-styrminne (43) med ett flertal minnesplatser vars antal motsvarar antalet block i sagda minnesrad (54) för lagring av konfigurationsinformationen, varvid sagda access-styrminne är kopplat till den interna bussledningen (105) och till sagda access-styrlogikdon (32, 34, 39), access-styrminnet laddas under kontroll av mikroprocessorn (10-6) endast efter att mikroprocessorn fastställt att sagda på förhand bestämda autentikationsprocedur ursprungligen utförts framgångsrikt, varvid värddatorn (5) åstadkommer påkoppling av sagda access-styrminne (43) via access-styrlogikdonet.

8. Minneskort enligt patentkravet 7, **kännetecknat** av att sagda låsvärde som lagrats i låsminnet (35) alla har värdet ETT och där sagda säkerhetskontrollsektion ytterligare innehåller en detektorkrets (38) för alla värden ETT vilken är anslu-

ten till sagda låsminne, varvid detektorkretsen som svar på låsvärdet ETT för alla genererar en signal som effektivt förbikopplar sagda säkerhetskontrollsektion och påkopplar sagda andra beständiga minne (103a) för att fungera som om sagda säkerhetskontrollsektion icke existerade.

9. Minneskort enligt patentkravet 7, **kännetecknat** av att utförandet av sagda på förhand bestämda autentikationsprocedur ursprungligen äger rum när sagda minneskort (3) först kopplas att kommunicera med värddatorn (5).

10. Minneskort enligt patentkravet 9, **kännetecknat** av att sagda access-styrdon innefattar ett låsregister (33) kopplat för att motta sagda låsvärde från låsminnet (35), en jämförelsekrets (39), ett nyckelregister (31) för att lagra ett nyckelvärde som överförts till nyckelregistret via sagda mikroprocessor, en fördröjningsräknare (32) för att lagra ett räknetal som definierar ett bestämt tidsintervall, samt grindorgan (34) som kopplats till sagda access-styrminne (43), till sagda jämförelsekrets och sagda fördröjningsräknare, varvid jämförelsekretsen är kopplad till sagda lås- och nyckelregister och till sagda grindorgan, och grindorganen är kopplade till fördröjningsräknaren för att generera en signal som påkopplar modifikation av accessen då jämförelsekretsen signalerar en identisk jämförelse med sagda låskodsvärde som är lagrat i låsregistret (33), när fördröjningsräknaren (32) signalerat ett slut på det på förhand bestämda tidsintervallet, varvid sagda signal som påkopplar accessmodifikationen färdigställer access-styrminnet (43) för lagring av konfigurationsinformationen.

11. Minneskort enligt patentkravet 10, **kännetecknat** av att sagda styrlogikdon (50) innefattar kretsar för att generera kommandosignaler såsom svar på en bestämd kommandoserie som används av mikroprocessorn för att styra funktionen av sagda säkerhetskontrollsektion i vart och ett minneschips.

12. Minneskort enligt patentkravet 11, **kännetecknat** av att sagda styrlogikdon (50) såsom svar på ett första av sagda på förhand bestämd serie av kommandon som genererats av mikroprocessorn genererar en första signal för att ladda sagda låskodsvärde i låsminnet (35), varvid sagda första av den bestämda serien av kommandon genereras under kortets ursprungliga tillverkningsskede.

13. Minneskort enligt patentkravet 12, **kännetecknat** av att styrlogikdonet (50) såsom svar på ett andra av sagda serie av på förhand bestämda kommandon genererat av mikroprocessorn genererar en andra signal för att koppla sagda ele-

ment (36) som påkopplar låslagringen till ett bestämt läge som blockerar inläsningen eller modifikationen av låsvärdet som lagrats i låsminnet (35).

14. Minneskort enligt patentkravet 12, **kännetecknat** av att sagda styrlogikdon (50) såsom svar på ett tredje av sagda serie av kommandon genererar en tredje signal för att i nyckelregistret (31) ladda ett bestämt av sagda nyckelvärden, varvid sagda tredje av den bestämda serien av kommandon genereras av mikroprocessorn endast efter det att mikroprocessorn fastställt att den bestämda autentikationsprocessen utförts framgångsfullt.

15. Minneskort enligt patentkravet 14, **kännetecknat** av att sagda tredje signal som genereras av styrlogikdonet (50) samtidigt tvingar fördröjningsräknaren (32) till ett bestämt räknetal för att fastställa starten av det bestämda tidsintervallet, och varvid styrlogikdonet såsom svar på vart och ett fjärde av sagda bestämda serie av kommandon genererade av mikroprocessorn minskar det bestämda räknetalet med ett, varvid fördröjningsräknaren signalerar slutet på tidsintervallet till följd av ett bestämt antal av sagda fjärde av den bestämda serien av kommandon.

16. Minneskort enligt patentkravet 11, **kännetecknat** av att styrlogikdonet (50) såsom svar på ett antal femte och sjätte av nämnda serie kommandon från mikroprocessorn genererar femte och sjätte signaler för att ställa och återställa positioner i sagda access-styrminne (43) i enlighet med konfigurationsinformationen för att definiera från vilka av sagda block informationen är tillåten att bli utläst.

17. Minneskort enligt patentkravet 11, **kännetecknat** av att lagringsdonen innefattar ett beständigt låsminne (35) för att inledningsvis motta och permanent lagra ett bestämt låsvärde som motsvarar sagda nyckelvärde; att mikroprocessorn (10-6) är anpassad att till sagda beständiga minne (103a) över den interna bussledningen sända sagda ena av nyckelvärdena, ifall autentikationsproceduren med sagda värddator (5) utförts framgångsrikt; varvid access-styrdonen (32, 34, 39) anpassats att detektera huruvuda sagda ena nyckelvärde motsvarar låsvärdet, och för att möjliggöra läsning av minnesraden (54) då motsvarighet fastställts.

18. Förfarande för att åstadkomma ett säkert minneskort att installeras i en värddator (5) innefattande ett antal beständiga minneschips (103a, 103b,...103n), varvid vart och ett minneschips innehåller en minnesrad (54) som organiserats i block av addresserbara positioner, samt styrlogikkretsar (50) för att generera kommandosignaler för att utföra minnesoperationer, där sagda förfarande innefattar stegen att:

(a) i kortet inkorporeras en mikroprocessor (10) kopplad att kommunicera med nämnda värddator efter installering i densamma, varvid mikroprocessorn inkluderar ett addresserbart beständigt minne (10-2) för att lagra information som innefattar ett antal nyckelvärden definierande användaråtkomlighet till minnesområden samt minneskonfigurationsinformation som definierar access till sagda minnesområden;

(b) inkorporering av säkerhetslogikkretsar i vart och ett beständigt minneschips, varvid säkerhetslogikkretsarna innefattar ett beständigt låsminne (35) för att lagra ett bestämt låsvärde som motsvarar ett av sagda nyckelvärden, access-styrlogikdon (32, 34, 39) kopplade till låsminnet, och ett adresserbart obeständigt access-styrminne (43) med ett flertal positioner motsvarande antalet sagda antal block för lagring av access-bitinformation i enlighet med sagda konfigurationsinformation;

(c) kopplande av mikroprocessorn till vart och ett minneschips för överföring av adress-, data- och styrinformation till sagda vart och ett minneschips:

(d) modifiering av styrlogikkretsarna (50) att svara på ett flertal kommandon för att sätta säkerhetslogikkretsarna i funktion:

(e) anpassning av mikroprocessorn (10-6) så att den utför en första bestämd användarautentikationsoperation med sagda värddator (5) då access till sagda block begärts av en användare; och

(f) anpassning av mikroprocessorn (10-6) så att den medger att sagda säkerhetslogikkretsar överför valda av sagda serie av kommandon till sagda vart och ett chips endast när autentikationsoperationen i steget (e) utförts framgångsrikt, för att tillåta att information som lagrats i olika av sagda block läses ut i enlighet med access-bitinformationen som lagrats i access-styrminnet.

19. Förfarande enligt patentkravet 18, **kännetecknat** av att sagda beständiga minne (10-2) hos mikroprocessorn har ett antal sektioner och där steget (a) ytterligare innefattar stegen att mikroprocessorn bringas att generera godtyckliga värden såsom sagda nyckelvärden och att ladda nyckelvärdena i en första (10-2b) av sagda antal sektioner.

20. Förfarande enligt patentkravet 18, **kännetecknat** av att sagda mikroprocessor ytterligare innefattar en intervallräknare (10-8) kopplad till mikroprocessorns beständiga minne (10-2) och där steget (a) vidare innefattar stegen att bringa mikroprocessorn att generera ett användarselektivt tidsintervall och att ladda ett värde

motsvarande det användarselektiva tidsintervallet i sagda intervallräknare, och där förfarandet vidare innehåller stegen att:

(g) mikroprocessorn anpassas att periodiskt igångsätta sagda användarautentikationsoperation i steget (e) med sagda valda tidsintervall; och

(h) fortsätta att tillåta utläsning av informationen som lagrats i sagda block i enlighet med access-bitinformationen så länge autentikationsoperationen i steget (b) utförs framgångsrikt.

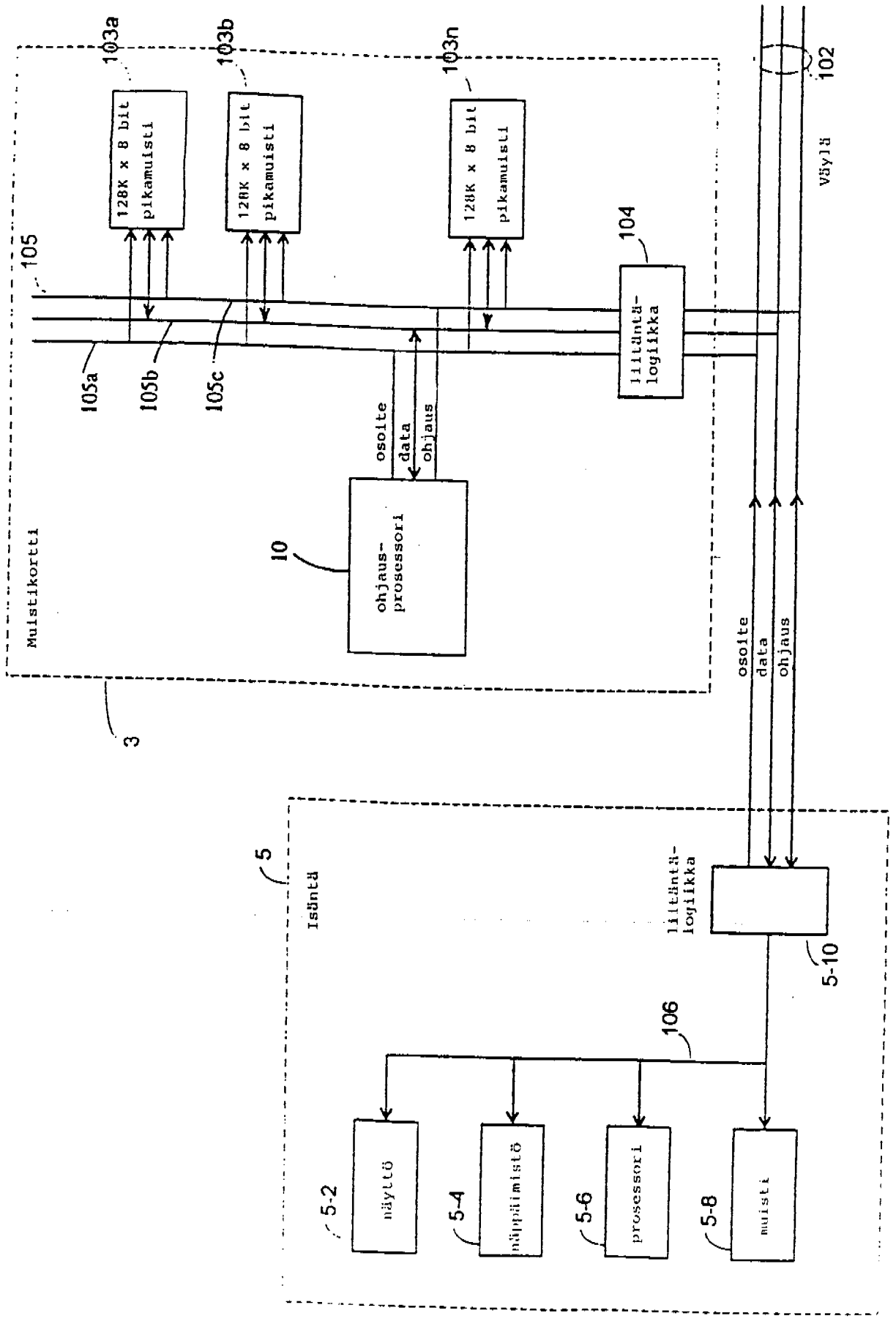
103a
103b
103n
128K x 8 bit pikamuisti
128K x 8 bit pikamuisti
128K x 8 bit pikamuisti
105
105a
105b
105c
104
liitäntä-logiikka
102
väylä
osoite
data
ohjaus
Muistikortti
10
ohjaus-prosessori
3
5
Isäntä
liitäntä-logiikka
5-10
106
5-2
näyttö
5-4
näppäimistö
5-6
prosessori
5-8
muisti

Figure 1

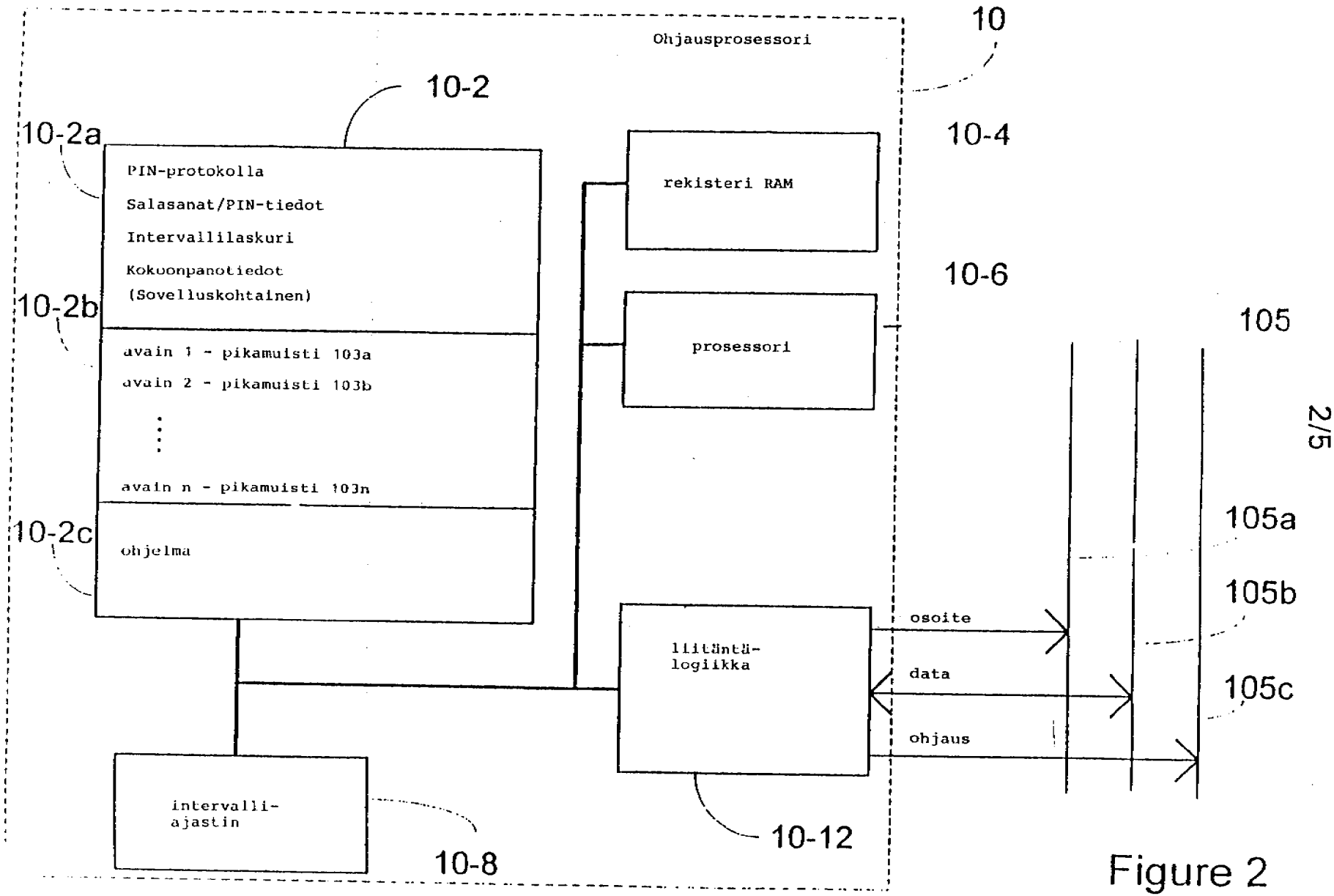
Ohjausprosessori
10
10-2
10-2a
PIN-protokolla
Salasanat/PIN-tiedot
Intervallilaskuri
Kokoonpanotiedot
(Sovelluskohtainen)
10-2b
avain 1 - pikamuisti 103a
avain 2 - pikamuisti 103b
avain n - pikamuisti 103n
10-2c
ohjelma
rekisteri RAM
10-4
prosessori
10-6
105
105a
105b
105c
osoite
data
ohjaus
liitäntä-
logiikka
10-12
intervalli-
ajastin
10-8

Figure 2

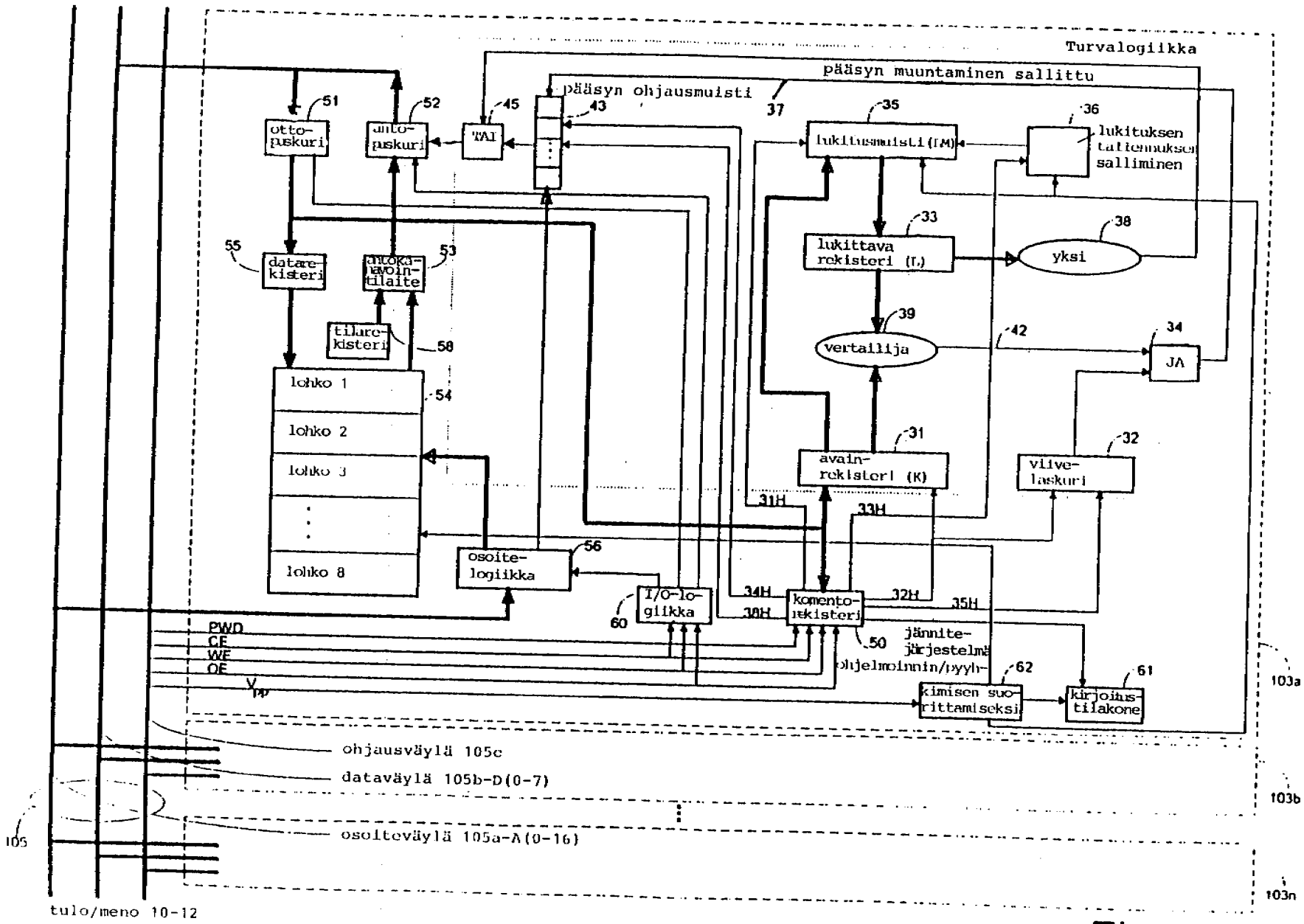
Turvalogiikka
pääsyn muuntaminen sallittu
pääsyn ohjausmuisti
37
43
45
TAI
51
otto-puskuri
52
anto-puskuri
55
datare-kisteri
53
antoka-navoin-tilaite
tilare-kisteri
58
lohko 1
lohko 2
lohko 3
lohko 8
54
osoite-logiikka
56
I/O-lo-giikka
60
35
lukitusmuisti (LM)
36
lukituksen tallennuksen salliminen
33
lukittava rekisteri (L)
38
yksi
39
vertailija
42
34
JA
31
avain-rekisteri (K)
32
viive-laskuri
31H
33H
34H
38H
32H
35H
komento-rekisteri
50
jännite-järjestelmä
ohjelmoinnin/pyyh-
62
kimisen suo-rittamiseksi
61
kirjoitus-tilakone
PWD
CE
WE
OE
V_{pp}
ohjausväylä 105c
dataväylä 105b-D(0-7)
osoiteväylä 105a-A(0-16)
105
tulo/meno 10-12
103a
103b
103n

Figure 3

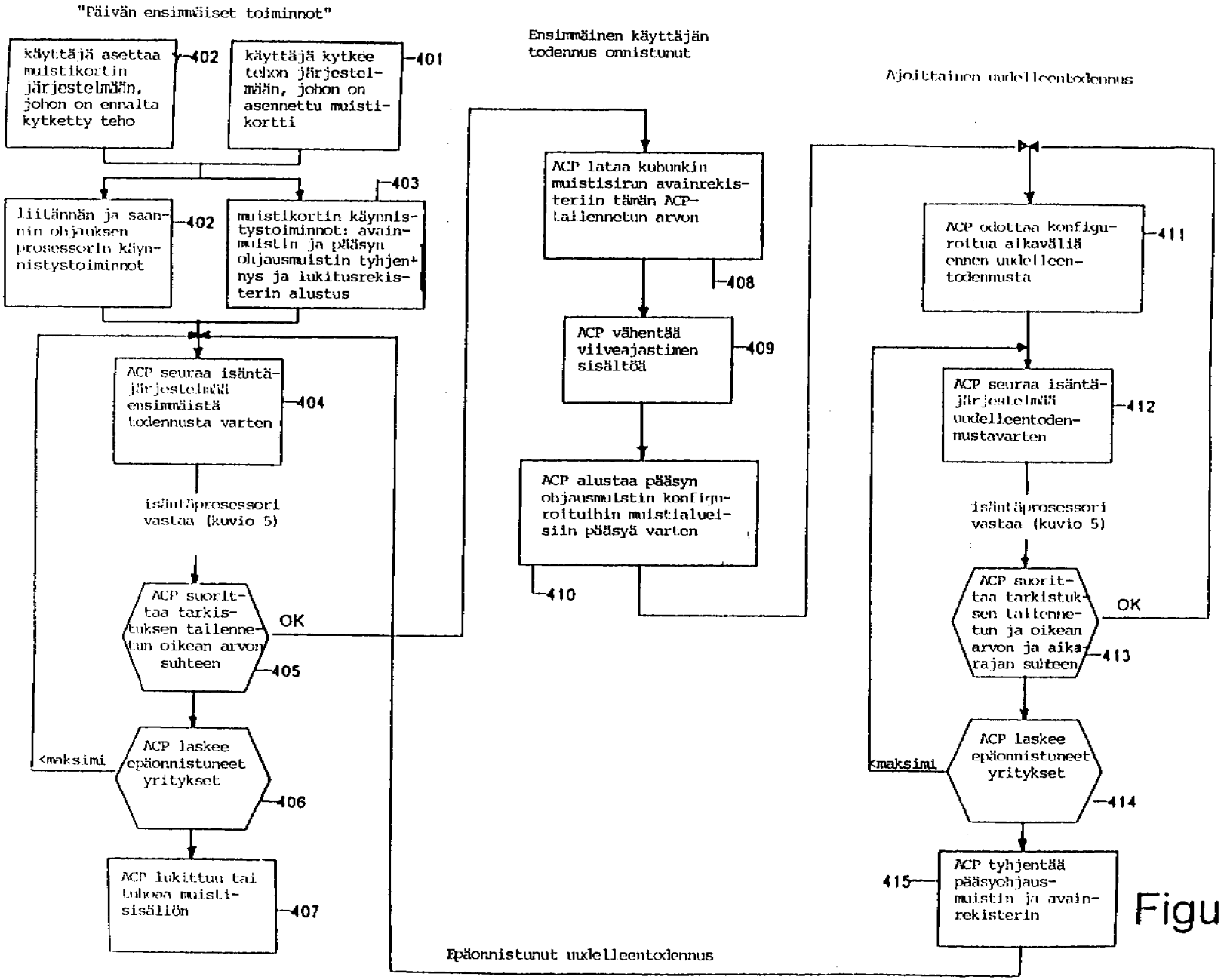
"Päivän ensimmäiset toiminnot"
käyttäjä asettaa muistikortin järjestelmään, johon on ennalta kytketty teho
402
käyttäjä kytkee tehon järjestelmään, johon on asennettu muistikortti
401
liitännän ja saannin ohjauksen prosessorin käynnistystoiminnot
402
403
muistikortin käynnistystoiminnot: avainmuistin ja pääsyn ohjausmuistin tyhjennys ja lukitusrekisterin alustus
ACP seuraa isäntäjärjestelmää ensimmäistä todennusta varten
404
isäntäprosessori vastaa (kuvio 5)
ACP suorittaa tarkistuksen tallennetun oikean arvon suhteen
OK
405
<maksimi
ACP laskee epäonnistuneet yritykset
406
ACP lukittuu tai tuhoaa muistisisällön
407
Ensimmäinen käyttäjän todennus onnistunut
ACP lataa kubunkin muistisirun avainrekisteriin tämän ACP-tallennetun arvon
408
ACP vähentää viiveajastimen sisältöä
409
ACP alustaa pääsyn ohjausmuistin konfiguroituihin muistialueisiin pääsyä varten
410
Epäonnistunut uudelleentodennus
Ajoittainen uudelleentodennus
ACP odottaa konfiguroitua aikaväliä ennen uudelleentodennusta
411
ACP seuraa isäntäjärjestelmää uudelleentodennustavarten
412
isäntäprosessori vastaa (kuvio 5)
ACP suorittaa tarkistuksen tallennetun ja oikean arvon ja aikarajan suhteen
OK
413
<maksimi
ACP laskee epäonnistuneet yritykset
414
415
ACP tyhjentää pääsyohjausmuistin ja avainrekisterin

Figure 4

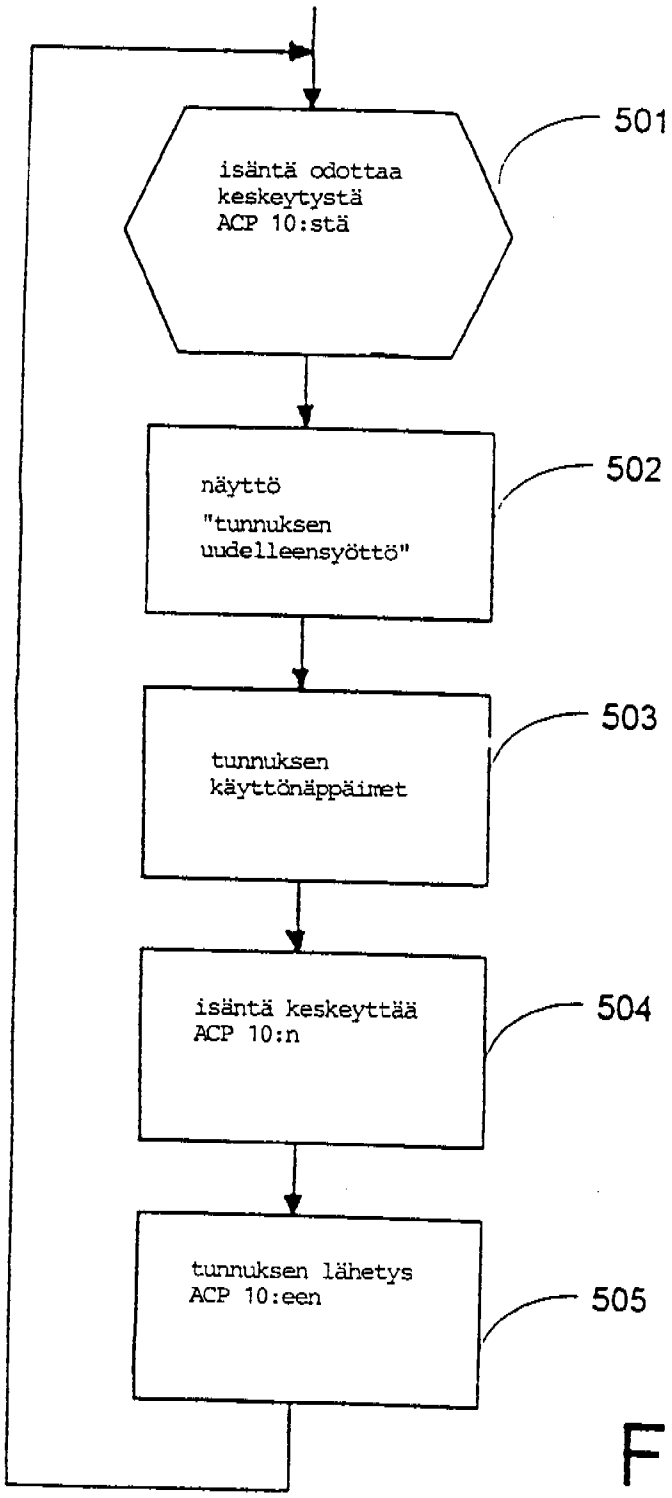
isäntä odottaa
keskeytystä
ACP 10:stä
501
näyttö
"tunnuksen
uudelleensyöttö"
502
tunnuksen
käyttönäppäimet
503
isäntä keskeyttää
ACP 10:n
504
tunnuksen lähetys
ACP 10:een
505

Figure 5