NORGE
(19) [NO]

STYRET FOR DET
INDUSTRIELLE RETTSVERN

[B] (12) UTLEGNINGSSKRIFT (11) Nr. 166107

(51) Int. Cl.[5] G 06 K 19/06, G 07 F 7/12

(21) Patentsøknad nr. 840178
(22) Inngivelsesdag 18.01.84
(24) Løpedag 18.01.84
(62) Avdelt/utskilt fra søknad nr.

(86) Internasjonal søknad nr. -
(86) Internasjonal inngivelsesdag -
(85) Videreføringsdag -
(41) Alment tilgjengelig fra 23.07.84
(44) Utlegningsdag 18.02.91

(71)(73) Søker/Patenthaver CII HONEYWELL BULL,
B.P. 33, 94 Avenue Gambetta,
F-75960 Paris Cedex 20, FR

(72) Oppfinner MIHCEL UGON, Maurepas, FR

(74) Fullmektig Bryn & Aarflot AS, Oslo.

(30) Prioritet begjært 20.01.83, FR, nr. 8300884.

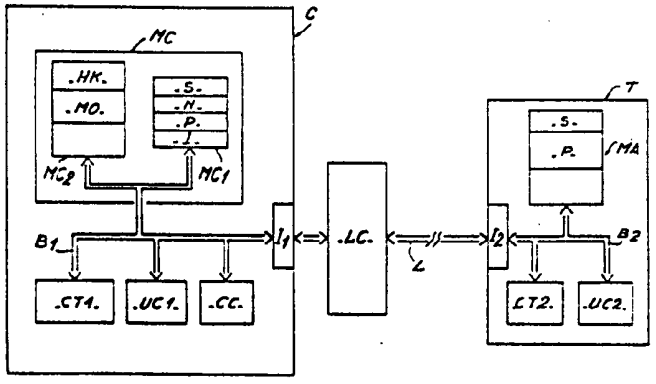
(54) Oppfinnelsens benevnelse FREMGANGSMÅTE OG SYSTEM FOR Å KLARERE EN INNEHAVER AV ET BÆRBART OBJEKT, F.EKS. ET KORT, TIL Å FÅ ADGANG TIL I DET MINSTE EN TJENESTE.

(57) Sammendrag

Fremgangsmåte og system for å klarere innehaveren av et bærbart objekt, f.eks. et kort, til å få adgang ved hjelp av dette kort til i det minste en tjeneste tilbudt av i det minste en autoriserende instans eller organisasjon. Fremgangsmåten tillater at brukeren av et kort (C) får adgang til en bestemt tjeneste ved å bevirke innskrivning av en autoriserende informasjon på kortet (C) av et autoriserende system (T), at kortet (C) og systemet bringes til å beregne et resultat som i det minste tar i betraktning en hemmelig informasjon (S), for sammenligning i en komparator (CC) på kortet, av de beregnede resultater og å validere den autoriserende informasjon hvis resultatene er identiske. Oppfinnelsen har anvendelse i forbindelse med kredittkort.

(56) Anførte publikasjoner

Europeisk (EP) patentsøknad, publ.nr. 028965,
USA (US) patent nr. 3806874.



2/2

Denne oppfinnelse angår generelt problemer som oppstår ved anvendelse av et bærbart objekt for å oppnå adgang til tjenester beskyttet som konfidensielle. Mer spesielt er det et formål med oppfinnelsen å tilveiebringe en fremgangsmåte og et apparat for å autorisere eller klarere innehaveren av et bærbart objekt, f.eks. et kort, til med dette kort å få adgang til i det minste en tjeneste som stilles til disposisjon av en autoriserende instans (i det følgende til dels bare betegnet "instans").

Utviklingen av datakommunikasjon har ført til et nytt problem: Hvordan skal man gjenkjennes enten på avstand eller uten avstand, av en annen part som ikke kjenner vedkommende personlig eller av et databehandlingssystem som man ønsker å kommunisere med, f.eks. fra en terminal.

Denne utvikling har antatt konkret form ved fremkomsten av bærbare og ikke-bærbare elektroniske media eller enheter, f.eks. kort, som innbefatter en ikke-flyktig beskyttet hukommelse, hvilket kan ha tallrike anvendelser og særlig er beregnet for det vanlige publikum. Det kan henvises til US patentene 4.211.919, 4.264.912 og 4.310.897 som gjelder typiske bærbare dataenheter eller -bærere. Andre former for slike innretninger er selvsagt også kjent.

Takket være individualiseringen av disse kort ved hjelp av data som på forhånd er registrert i deres hukommelser, har det vært mulig å planlegge og sette ut i praksis systemer som gjør det mulig å autorisere eller klarere personer eventuelt juridiske personer til å utføre beskyttede operasjoner som er spesifikke for de påtenkte anvendelser.

Alle disse anvendelser medfører en utveksling av informasjon i form av en dialog mellom i det minste et kort og en terminal. Fra det øyeblikk en utveksling av informasjon finner sted, spesielt konfidensiell informasjon, har det avgjørende betydning å foreta kontroller som hovedsaklig tar sikte på å verifisere gyldigheten av den informasjon som er utvekslet. Dette er desto mer viktig fordi tanken på svindel nødvendigvis må tas i betraktning i forbindelse med tanken om beskyttet adgang eller en beskyttet tjeneste.

Det eksisterer allerede systemer hvor et kort muliggjør adgang til beskyttede områder. Se f.eks. US patentene 4.211.919, 4.224.666, 4.271.482 og 4.295.041. For å gjøre disse systemer

bedre med hensyn til motstandsevne mot svindel er det iverksatt en dialog som tar i betraktning vilkårlig utvalgte passord på en slik måte at en svindler blir hindret i å reprodusere en sekvens av tidligere dialog som har autorisert til lovlig adgang til det beskyttede område. Et slikt system er spesielt beskrevet i fransk patent nr. 2.469.760.

Andre systemer tillater at et kort blir brukt til finansielle transaksjoner. I utgangspunktet må kortet krediteres med en viss pengesum av en behørlig autorisert utstedende instans. For å hindre forsøk på svindel, spesielt ved å modifisere det beløp som kortet er kreditert med, vil den utstedende instans beskytte seg selv ved å bruke et passord til å sikre kontrollen av operasjonene eller transaksjonene. Det er gjort en forbedring i disse systemer for å øke motstandsevnen mot svindel, ved å bruke et spesifikt passord hvis verdi er korrelert med en referanse som er spesifikk for kortet, ved hjelp av en algoritme som bare er kjent for den utstedende instans.

Etter å være blitt brukt flere ganger kan kreditten på kortet bli brukt opp og innehaveren må få en ny kreditt innskrevet på dette. På det nåværende tidspunkt er det bare to mulige måter å gi et kort ny kreditt på: Enten blir kortet ganske enkelt ikke lenger brukbart, og det må utstedes et nytt kort; eller man må få kortet gjenkredittert av den utstedende instans som alene er autorisert til å foreta en slik operasjon. I begge tilfeller må innehaveren av kortet således reise til det sted hvor den utstedende instans holder til.

Hittil har kortinnehaverne ikke vært i stand til å få slike kort gjenkredittert over avstand, og spesielt ikke fra sitt hjem. I virkeligheten ville en slik operasjon nødvendiggjøre overføring av konfidensiell informasjon på den kommunikasjonslinjen som forbinder en terminal plassert i kortbrukerens hjem, med et system som befinner seg hos den utstedende instans. Denne konfidensielle informasjon omfatter hovedsaklig en kundenøkkel som gjør det mulig for transaksjonsutstyr hos instansen å få bekreftet kortinnehaverens legitimitet og videre en nøkkel som er spesiell for instansen overført til kortet for å gjøre det mulig i kortet å få bekreftet at det virkelig er i kommunikasjon med terminalen i den autori-

serende instans. Fra det øyeblikk da det foregår kommunikasjon av konfidensiell informasjon eksisterer muligheten for svindel.

Fra US patent 3.806.874 er kjent en fremgangsmåte for å autorisere brukeren av et bærbart objekt til å få adgang til en tjeneste som leveres av en eneste autoriserende instans. Beregningen av et første resultat bevirkes inne i det bærbare objektet, og beregningen av et andre resultat foregår inne i et autoriserende system som det bærbare objektet er forbundet med, og beregningen foretas under styring av den autoriserende instans. Disse resultatene tar i betraktning i det minste en hemmelig nøkkel (eller referanse) som er registrert på forhånd både i kortet og i systemet. De må passe sammen for at systemet skal autentisere det bærbare objektet. Det bevirkes altså to sammenligninger: En første inne i en krets på kortet, og en andre sammenligning inne i en krets i terminalen. Resultatene fra hver av disse sammenligningene er nødvendig for å tillate innskrivingen (av en ny kredittsum) i kortets lagerenhet. Noen validering av en innskriving forekommer ikke i US 3.806.874. Dessuten finnes det i US patentets beskrivelse intet som viser eller antyder muligheten for å eliminere en av sammenligningene, fortrinnsvis den som foregår i terminalen, uten at dette skulle lede til forstyrrelser i driften av systemet.

Fra europeisk patentsøknad 28.965 er også kjent en metode der det bærbare objekt og den autoriserende instans begge foretar en beregning som senere blir sammenlignet slik at kortbrukeren eventuelt kan få adgang til en tjeneste. Imidlertid omfatter systemet ifølge EP 28.965 bl.a. det trekk å avlese en identifikasjonskode inneholdt i kortets lagerenhet, og å se om denne "matcher" de koder som er mulige for systemet, dvs. at en forutgående sertifisering må foretas. Et slikt trekk er ikke aktuelt i foreliggende oppfinnelse. Et annet avvikende trekk stammer fra det faktum at et vilkårlig tall skal benyttes i beregningen av resultatene for å få forskjellige resultater mellom de beregninger som foretas med et gitt kort. Noe slikt tilfeldig tall benyttes heller ikke i foreliggende oppfinnelse.

Foreliggende oppfinnelse har til formål å overvinne ulempene ved den kjente teknikk ved å tillate at den spesielle

innehaver eller bruker av et kort gir sitt kort ny kreditt fra hjemmet ved å eliminere overføringen av de konfidensielle nøkler som er spesifikke for en gitt anvendelse. Denne eliminering gjør det mulig å ta sikte på bruk av ett og det samme kort til å gi adgang til tjenester som samtidig deles blant et flertall instanser. Dette problem kan ikke løses ved å bruke et unikt passord fordi det ville tillate innføring av informasjon som er særegen for ulike tjenester på korthukommelsesnivå, og simulering av slik informasjon av en svindler.

Ved å eliminere løsningen med et passord som er spesifikt for en spesiell tjeneste og å erstatte dette med en utveksling av vilkårlig informasjon som direkte tolkes av kortet, gjør denne oppfinnelse det derfor mulig for kortet å virke under selvstyring og å validere de forskjellige resultater av beregninger som utføres på vegne av de forskjellige instanser.

I dette øyemed foreslår oppfinnelsen en fremgangsmåte for å autorisere eller klarere brukeren av et bærbart objekt, f.eks. et kort, til å få adgang med dette kort til minst en tjeneste som leveres av minst en autoriserende instans, og fremgangsmåten er nøyaktig definert i det vedføyde patentkrav 1. Vanligvis opprettes forbindelse mellom kortet og et autoriserende system som tilhører vedkommende instans, og en autoriserende referanse bevirkes innskrevet av dette system på anmodning fra kortbrukeren, inn i kortets hukommelse for å gi adgang til denne tjeneste, og kortet og systemet bringes til å beregne et resultat (R) som fremkommer ved utførelse av ett og samme program (P) som tar i betraktning i det minste en hemmelig referanse (S) som på forhånd er registrert både på kortet og i systemet. Fremgangsmåten omfatter også sammenligning i kortet av de på forhånd beregnede resultater (R) og at kortet validerer den autoriserende informasjon hvis denne sammenligning tilfredsstiller en forutbestemt betingelse.

Andre fordeler, særegne trekk og detaljer ved denne oppfinnelse vil fremgå av den følgende beskrivelse under henvisning til tegningene som viser et foretrukket utførelseseksempel ifølge oppfinnelsen:

Figurene 1a og 1b illustrerer skjematisk forbindelser som kan eksistere mellom forskjellige autoriserende instanser som kortbrukeren kan oppnå adgang til,

figur 2 er et blokkskjema som viser nødvendige anordninger og midler til å utføre fremgangsmåten ifølge oppfinnelsen, og

figur 3 forklarer arten av den autoriserende informasjon som skrives inn i kortets hukommelse, og identifisering av de tilsvarende autoriserende instanser.

Før beskrivelsen av fremgangsmåten ifølge oppfinnelsen skal det først forklares hva som er å forstå med betegnelsen "autoriserende instans". En autoriserende instans er en instans som vanligvis er offisielt anerkjent og som tilbyr i det minste en tjeneste som hvilken som helst person, enten en naturlig person eller en "kunstig" person, kan få adgang ved å bruke et kort utstedt av vedkommende instans.

Det henvises nå til figur 1a. Det er der skjematisk vist en autoriserende instans BANK, så som et banketablissement som er autorisert til å utstede kredittkort. En person som har et kredittkort av denne type ihende, kan henvende seg til en annen autoriserende instans (H1 på figur 1b) for å oppnå tjenester tilbudt av denne, og om mulig bruke det kort som allerede er utstedt til vedkommende person av den autoriserende instans BANK. Det er derved fremkommet et flertjenestekort.

Det er likeledes mulig å forbinde de autoriserende instanser med hverandre i en kjede for å gjøre disse avhengig av hverandre, slik som vist på figurene 1a og 1b. Instansen BANK, eller den prinsipale autoriserende instans, kan gi adgang til en autoriserende instans TELEFON som på sin side gir adgang til en instans KATALOG. Under disse betingelser kan en person ikke oppnå den tjeneste som leveres av instansen KATALOG uten at vedkommende allerede har adgang til instansen TELEFON, og for å disponere over instansen TELEFON må vedkommende allerede ha adgang til instansen BANK.

I dette eksempel autoriserer instansen TELEFON til bruk av telefonkiosker som mottar kortene for automatisk å sikre at samtaleenheter blir registrert for avregning, og instansen KATALOG tillater konsultering av telefonkataloger på en skjerm, fra kortbrukerens hjem.

Figur 1b viser et mer generelt eksempel på en mulig forgrening blant et flertall instanser. En instans H1 eller en hovedinstans tillater adgang til enhetene H2 eller H3, og instansen H2 tillater adgang til enhetene H4 eller H5. Følgelig må en person som ønsker adgang til instansen H5 nødvendigvis allerede ha adgang til instansene H2 og H1.

På figur 2 er det vist et bærbart objekt så som et kort C. Dette kort C omfatter i det minste en hukommelse MC, prosesseringskretser CT1, en komparatorkrets CC og en kommandoenhet UCL. (Et typisk kort er vist i US patent 4.211.919.) Alle disse elementer kommuniserer med hverandre gjennom en forbindelsesbuss B1.

Hukommelsen MC er oppdelt i minst to hukommelsessoner MC1, MC2. I sonen MC1 er det registrert i det minste en hemmelig referanse S som er ukjent for kortbrukeren, et tall N som er særegent for kortet og en algoritme for en spesiell beregning, oversatt av et program P.

I hukommelsessonen MC2 er det i det minste innlest autoriserende ord HK tilforordnet åpningsord MO og beregnet til å motta informasjon som identifiserer de autoriserende instanser og informasjon vedrørende data som er spesifikke for de tjenester som tilbys av disse autoriserende instanser.

Et typisk autoriserende system er vist i US patent nr. 4.211.919.

Et autoriserende system T som er særegent for en spesiell anvendelse omfatter i det minste følgende:

En hukommelse MA hvor den samme hemmelige informasjon S og det forannevnte program P blir registrert,

prosesseringskretser CT2 særlig for utførelse av programmet P,

og en kommandoenhet UC2 for synkronisering av utvekslingene av informasjon mellom kortet C og systemet T. Alle disse elementer er forbundet med hverandre gjennom en forbindelsesbuss B2.

For å konversere med systemet T kan kortet C forbindes med en kortleser LC gjennom en mellomkobling I_1. Denne kortleser LC er gjennom en kommunikasjonskanal L forbundet med systemet T gjennom en mellomkobling I_2.

Som eksempel kan kortleseren LC være plassert i den individuelle kortbrukers hjem, mens kommunikasjonskanalen I f.eks. tilveiebringes gjennom en telefonlinje, og systemet T er plassert i lokalene for den autoriserende instans med sikte på å levere en spesiell tjeneste.

For at brukeren av et kort C skal få adgang til den tjeneste som tilbys av en instans, må dette kort C inneholde et autoriserende ord HK som er særegent for denne instans.

Et autoriserende ord HK for en hovedinstans inneholder i det minste en sone ZK som identifiserer den autoriserende instans, og komplementære soner ZA, ZB, ZD hvis rolle skal forklares lenger nedenfor.

I tilfelle av en kjede av forskjellige autoriserende instanser vil det autoriserende ord HK for hver instans avhengig av en autoriserende instans som er innskrevet foran dette, i tillegg inneholde en sone ZM som inneholder den samme informasjon som sonen ZK for det autoriserende ord til instansen som forut er innskrevet.

Til det autoriserende ord HK svarende til hver instans er det tilforordnet i det minste et åpningsord MO som er innlest i hukommelsen på kortet C. Dette åpningsord MO inneholder informasjon, spesielt informasjon som er spesifikk for den tjeneste som tilbys av instansen. Et åpningsord MO omfatter en sone ZK som identifiserer instansen og som således svarer til sonen ZK i det tilforordnede autoriserende ord HK, sonen ZD for data som vedrører den tjeneste som tilbys av instansen, og komplementære soner ZA, ZB som er identiske med dem i det tilforordnede autoriserende ord HK.

Anta at en person, enten naturlig person eller kunstig person, ønsker å benytte seg av den tjeneste som leveres av hovedinstansen, dvs. en som ikke er avhengig av noen annen autoriserende instans. Tar man tilfellet på figur 1a som eksempel er denne hovedinstans instansen BANK.

Personen går til denne instans, så som et banketablissement som er spesielt autorisert til å utstede kredittkort. Etter innledende standardkontroller vedrørende f.eks. identiteten av personen, og tilstanden på dennes bankkonto eller etter at denne konto er blitt åpnet, utsteder instansen BANK et kredittkort i hvis hukommelsessone MC2 det er innskrevet et autoriserende ord HK1 i adressen a1 og et åpningsord MO1

er innskrevet i adressen a10. Disse skriveoperasjoner utføres i banklokalet ved bruk av et behørig beskyttet informasjons-behandlingssystem som anvendes for autorisering og som et kort C er knyttet til.

Under henvisning til figur 3 blir sonene ZK, ZD, ZA og ZB fylt som følger:

- sone ZK inneholder informasjonen BANK,
- sone ZD inneholder sikkerhetsdata,
- sone ZA kan ganske enkelt omfatte en enkelt binær bit som har verdien "1", og
- sone ZB kan likeledes omfatte en enkelt binær bit som har verdien "1".

Sone ZK, ZD, ZA,ZB i åpningsordet MO1 blir fylt som følger:

- sone ZK inneholder informasjonen BANK,
- sone ZD inneholder en kreditt av størrelse f.eks. 1.000 kroner, og
- sonene ZA, ZB inneholder den samme informasjon som sonene ZA, ZD på det tilhørende autoriseringsord HK1.

I hukommelsessonen MCL på kortet C er det også registrert parametre S, N, P som definert ovenfor, samt en kode I som er kjent for kortbrukeren for å muliggjøre verifisering gjennom kortet på i og for seg kjent måte, av legitimiteten av brukeren av dette kort forut for utførelsen av noen operasjon.

Den person som er utstyrt med et slikt kort C kan så befinne seg i en av tre situasjoner:

Den første, eller normale situasjon, svarer til det tilfelle at kortbrukeren benytter dette til å foreta banktransaksjoner som er godkjent av den autoriserende instans BANK, og hvor det etter hver transaksjon foretas debetering av den kreditt som er innskrevet i sone ZD av åpningsordet MO1 med det beløp som transaksjonen gjelder. Det system som tar hånd om skrivingen av det nye kredittbeløp søker i hukommelsessonen MC2 på kortet C etter et åpningsord hvis sone ZK inneholder den autoriserende instans BANK og verifiserer før innskrivning at bitposisjonene i sonene ZA og ZB virkelig har verdien "1".

Den annen situasjon opptrer når det kredittbeløp som er innskrevet på kortet ikke er tilstrekkelig til å muliggjøre nye transaksjoner. Hittil har kortbrukeren ikke hatt noe annet valg enn å gå til instansen BANK for å få kortet fornyet eller gjenkredittert, eller det måtte utstedes et nytt kort

til brukeren ved hjelp av den tidligere beskrevne prosess.

I motsetning til dette kan kortbrukeren ifølge oppfinnelsen gjenkreditere dette uten å gå til instansen BANK, ved å foreta en operasjon fra sitt hjem som vist på figur 2. For å gjøre dette blir kortet C innsatt i kortleseren LC og så oppkalles gjennom telefon en operatør i det autoriserende system T som befinner seg i lokalene for instansen BANK. Når denne forbindelse er etablert og kortleseren LC er forbundet med systemet T, skjer følgende operasjoner i rekkefølge:

Kortbrukeren ber operatøren om å skrive et nytt åpningsord MO10 inn i hukommelsessonen MC2 på kortet C med følgende informasjon: Den autoriserende instans er instansen BANK (sone ZK) og den ønskede kreditt med beløp f.eks. 5.000 kroner (sone ZD). Operatøren beordrer det autoriserende system T til å skrive dette åpningsord MO10 etter å ha funnet en disponibel adresse (an) i hukommelsessonen MC2.

Systemet T eller kortet C forlanger så utførelse av programmet P på nivå av systemet T og på nivå av kortet C. Dette program P tar i betraktning fire parametre: adressen (an), de hemmelige data S, det autoriserende ord HK1 for instansen BANK - et ord som normalt allerede må ha vært skrevet på kortet, og referansen N som er særegen for kortet og omfatter f.eks. en produsents serienummer overført til systemet T.

Før utførelse av programmet P verifiserer kortet C at det virkelig inneholder det autoriserende ord HK for den autoriserende instans opptatt i sone ZK av åpningsordet M10 som nå skal skrives. I dette eksempel kontrollerer så kortet om det inneholder det autoriserende ord HK1 for den autoriserende instans BANK. Hvis kortet C ikke finner det autoriserende ord HK1, stopper dialogen og kortet C gjør åpningsordet MO10 ugyldig ved å gi bitposisjonen i sone ZB av åpningsordet MO10 verdien "0". Hvis kortet derimot finner det autoriserende ord HK1, dvs. hvis det finner informasjonen BANK i sone ZK av et autoriserende ord HK, og videre etter å ha verifisert at bitposisjonene i sonene ZA, ZB av dette ord virkelig har verdien "1", utfører kortet C programmet P ved hjelp av sine prosesseringskretser CT1.

For sin del vil systemet T også utføre programmet P. Det autoriserende ord HK1 som er nødvendig for denne beregning

og som kan være kjent for operatøren av systemet T, blir innført under kontroll av systemet T, men blir ikke overført av kortet C.

Det resultat R som beregnes av systemet T blir så overført til kortet C, som i sin komparatorkrets C sammenligner dette resultat R med det som kortet selv har beregnet.

Hvis de to resultater tilfredsstiller en forutbestemt betingelse (f.eks. at de to resultater er like), validerer kortet C åpningsordet MO10 ved å sette bitposisjonen i sone ZB av dette ord på verdien "1". Det er viktig å bemerke her at det er kortet selv som validerer eller bekrefter et åpningsord. Så verifiserer systemet T at innholdet av åpningsordet MO10 virkelig svarer til innholdet av det ord som det har sørget for å få skrevet og så settes bitposisjonen i sone ZA av åpningsordet MO10 på verdien "1".

Hvis alle disse operasjoner skjer normalt, blir i virkeligheten kortet gitt kreditt.

Den tredje situasjon angår det tilfelle at brukeren av kortet C ønsker å få en ny autoriserende instans HK innskrevet.

Hvis denne instans er en ny hovedinstans blir prosedyren som allerede beskrevet ovenfor. Hvis på den annen siden denne nye autoriserende instans er avhengig av en annen instans hvis autoriserende ord allerede er blitt innskrevet på kortet, kan brukeren av dette kort selv utløse innskrivningsoperasjonen for denne nye autoriserende instans i henhold til det som er vist på figur 2.

Når forbindelsen er blitt etablert med systemet T, beordrer kortbrukeren skriving av et autoriserende ord HK. Anta at situasjonen er som vist på figur 1a, hvor kortbrukeren ønsker adgang til den autoriserende instans TELEFON HK2. Brukeren ber da terminalen T om et autoriserende ord HK2 med informasjonen "TELEFON" i sone ZK og informasjonen "BANK" i sone ZM. Når det autoriserende ord HK2 er skrevet, f.eks. i adressen a2 i hukommelsessonen MC2 på kortet C, verifiserer så kortet om det allerede har et autoriserende ord HK1 svarende til den autoriserende instans BANK. For å gjøre dette undersøker det i sonene ZK for autoriserende ord som allerede er blitt innskrevet om en av disse soner inneholder informasjonen "BANK". Hvis det ikke finner denne informasjon, blir dialogen avbrutt. Hvis det finner denne informasjon, verifiserer

det dessuten om bitposisjonene i sonene ZA og ZB av det autoriserende ord som er blitt funnet, har verdien "1". Hvis dette er slik, så utfører kortet C og systemet T det ovenfor beskrevne program med en validering av det autoriserende ord HK2 under de samme betingelser som fastsatt for å skrive et åpningsord MO slik som beskrevet for den forannevnte situasjon.

Det skal bemerkes at den sikkerhetsinformasjon som er nevnt ovenfor og som er tilstede i sone ZD av hvert autoriserende ord HK utelukkende er beregnet til å gjøre beregningsprosessen for å komme til resultatet R, komplisert og således hindre en svindler i lett å kunne forutberegne et slikt resultat R. Denne informasjon kan f.eks. innbefatte de data som den autoriserende instans ble innskrevet på i kortet. For ytterligere å forbedre sikkerheten i systemet er det mulig å kombinere adresseparameteret (a) og parameteret (N) i henhold til en forutbestemt relasjon.

Når det autoriserende ord HK2 er validert, sørger kortbrukeren for at et åpningsord MO2 blir skrevet inn ved en adresse a20 ved hjelp av den samme prosess som allerede beskrevet ovenfor ved innskrivning av åpningsordet MO10.

Det bemerkes også at sonene ZA og ZB som nevnt ovenfor, ikke er tilgjengelige utenfra.

Det vil forstås at det bærbare objekt kan være noe annet enn et kort og at de autoriserende instanser som det er tale om, ikke trenger å tilby utelukkende finansielle tjenester. Slike tjenester kan vedrøre abonnement på blader, filmer som kan vises på en kundes fjernsynsapparat osv.

P A T E N T K R A V

1. Fremgangsmåte for å autorisere eller klarere brukeren av et bærbart objekt (C), f.eks. et kort, omfattende et lager (MC), behandlingskretser (CT1), komparatorkretser (CC) og styrekretser (UC1), til å få adgang med dette objekt til minst en tjeneste som leveres av minst en autoriserende instans, hvor fremgangsmåten omfatter:

- at det bærbare objekt (C) forbindes med et autoriserende system (T) som tilhører den autoriserende instans, idet nevnte system innbefatter en hukommelse (MA), prosesseringskretser (CT2) og kontrollkretser (UC2);

- at det bevirkes en beregning av et første resultat i det bærbare object (C), og samtidig en beregning av et andre resultat i systemet (T), hvor det første og det andre resultat fremkommer ved en utførelse av det samme program (P) i begge tilfeller, hvor det i beregningene medtas minst en hemmelig referanse (S) som er registrert på forhånd i både det bærbare objekt (C) og i systemet (T);

- at det andre resultat, beregnet av systemet (T), overføres til det bærbare objekt (C);

- og at for å validere eller bekrefte innskrivingen av en autoriserende referanse fra systemet (T) i lageret (MC) til det bærbare objektet (C), bevirkes det sammenligning i det bærbare objektet (C) av de to resultater som er beregnet tidligere;

k a r a k t e r i s e r t v e d at systemet (T) på anmodning fra kort-brukeren først skriver inn nevnte autoriserende referanse i det bærbare objektets (C) lager (MC), og at videre objektet (C) innskriver i sitt lager (MC) en valideringsreferanse dersom ovennevnte sammenligning tilfredsstiller en forutbestemt betingelse.

2. Fremgangmåte ifølge krav 1, k a r a k t e r i s e r t v e d at:

- det preliminært defineres hvilke forskjellige autoriserende instanser som brukeren av et bærbart objekt kan få adgang til for å oppnå tjenesten;

- de forskjellige autoriserende instanser sammenkjedes i samsvar med en forutbestemt sammenkjedings-betingelse;

- hver autoriserende instans identifiseres ved hjelp av en autoriserende referanse med forutbestemt format, innbefattende minst en referanse for identifikasjon av den aktuelle autoriserende instans;

- det verifiseres, på det tidspunkt hvor en autoriserende referanse for en ny autoriserende instans innskrives i det bærbare objektet (C), at sammenkjedings-betingelsen som tilsvarer denne nye autoriserende instans allerede er skrevet inn i det bærbare objektet (C); og

- deretter igangsettes beregningen av de ovennevnte resultatene (R).

3. Fremgangsmåte ifølge krav 2, k a r a k t e r i s e r t v e d at den autoriserende referanse for den første autoriserende instans, eller hoved-instansen, innskrives av en behørig autorisert instans ved utstedelse av det bærbare objekt (C) til brukeren, idet de autoriserende data vedrørende de andre autoriserende instanser innskrives i det bærbare objektet (C) på ordre fra bæreren av dette objektet og utelukkende under kontroll av objektet (C).

4. Fremgangsmåte ifølge krav 1, 2 eller 3, k a r a k t e r i s e r t v e d at de autoriserende data for de autoriserende instanser utenom hoved-instansen kan innskrives i objektet over avstand, spesielt fra objekt-brukerens hjem.

5. Fremgangsmåte ifølge krav 1, 2 eller 3, k a r a k t e r i s e r t v e d at ved beregningen av det ovenenvnte resultat (R) tas det i betraktning hva som er den autoriserende referanse for den autoriserende instans som den autoriserende instans avhenger av, hvis autoriserende referanse ønskes innskrevet.

6. Fremgangsmåte ifølge krav 1, 2 eller 3, k a r a k t e r i s e r t v e d at ved beregningen av resultatet (R) nevnt ovenfor, tas det i betraktning i hvilken adresse i lageret den autoriserende referanse er innskrevet.

7. Fremgangmåte ifølge krav 6, k a r a k t e r i s e r t v e d at ved beregning av resultatet (R) nevnt ovenfor, tas det i betraktning den ovennevnte adresse i lageret, kombinert med en referanse som er særegen for objektet, slik som objektets serienummer som ble påført da objektet ble fremstilt.

8. Fremgangsmåte ifølge krav 1, k a r a k t e r i s e r t v e d at validering bevirkes av objektet når det gjelder innskriving av en autoriserende referanse dersom det eksisterer identitet mellom de resultater (R) som beregnes av objektet og de som beregnes av det autoriserende systemet.

9. Fremgangsmåte ifølge krav 1, k a r a k t e r i s e r t v e d at

- minst ett åpningsord tilordnes hver autoriserende referanse som er særegen for en autoriserende instans, hvilket åpningsord inneholder i det minste referansen for identifisering av den autoriserende instans og en referanse som er særegen for den tjeneste som leveres av denne autoriserende instans;

- det bevirkes innskriving av et nytt åpningsord på ordre fra objekt-brukeren og via det autoriserende system som er spesifikt for den aktuelle autoriserende instans;

- det undersøkes om den autoriserende instans som er identifisert i åpningsordet, allerede har sin autoriserende referanse innskrevet på objektet; og

- derpå igangsettes beregningen av de ovennevnte resultater (R).

10. System for å autorisere eller klarere brukeren av et bærbart objekt, f.eks. et kort, til å få adgang med dette objekt til minst en tjeneste som leveres av minst en autoriserende instans, av en type hvor objektet omfatter minst ett lager (MC) hvor i det minste en hemmelig informasjon (S) og ett program (P) er lagret, idet nevnte program utfører en forutbestemt algoritme som tar i betraktning i det minste den hemmelige informasjon (S), hvor nevnte objekt (C) forbindes med et autoriserende system (T) som er spesifikt for en gitt autoriserende instans, idet nevnte system (T) innbefatter i det minste en hukommelse (MA) hvor i det minste den ovennevnte hemmelige kode og det ovennevnte program også er registrert, hvor nevnte objekt videre omfatter en komparatorkrets for sammenligning av to resultater (R), hvilke resultater beregnes samtidig i objektet (C) og i systemet (T), k a r a k t e r i s e r t v e d at autoriserende data som identifiserer de autoriserende instanser og autoriserer objekt-brukeren til å få adgang til de tjenester som leveres av disse autoriserende instanser, er registrert i objektets (C) lager (MC), og ved at resultatet av den ovenfor refererte sammenligning benyttes for validering i objektet av en autoriserende referanse innskrevet i objektet (C) av systemet (T).

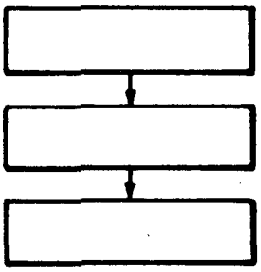


FIG.1a

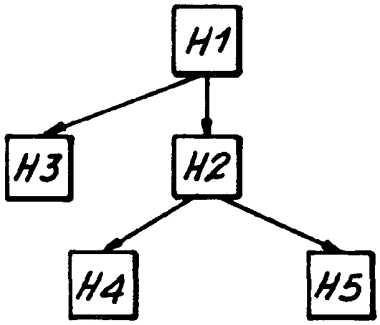


FIG.1b

FIG.3

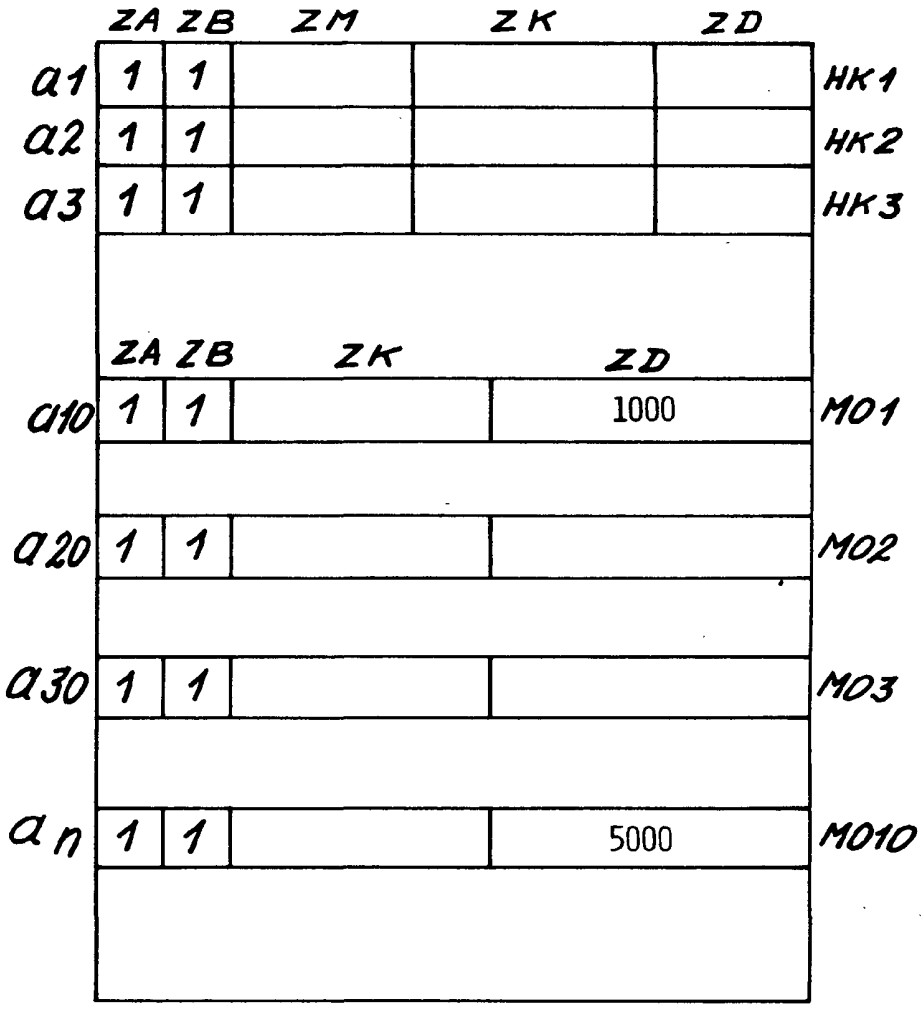


FIG.2