



(12) PATENT

(19) NO

(11) 330751

(13) B1

NORGE

(51) Int Cl.

G06K 17/00 (2006.01)

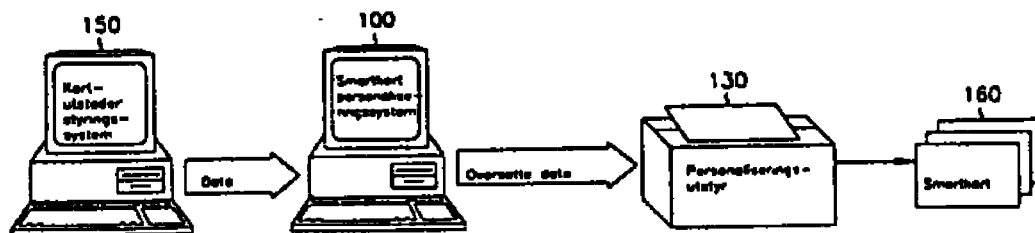
G07F 7/10 (2006.01)

Patentstyret

(21)	Søknadsnr	19984821	(86)	Int.inng.dag og søknadsnr	1997.04.14 PCT/US1997/06204
(22)	Inng.dag	1998.10.15	(85)	Videreføringdag	1998.10.15
(24)	Løpedag	1997.04.14	(30)	Prioritet	1996.04.15, US, 15743 1996.11.22, US, 755459
(41)	Alm.tilgj	1998.12.15			
(45)	Meddelt	2011.07.04			
(73)	Innehaver	Ubij Inc, 5909 Baker Road, Suite 580, Minneapolis, MN 55345, USA			
(72)	Oppfinner	David R. Tushie, Eden Prairie, MN, USA William W. Haeuser, Chaska, MN, USA			
(74)	Fullmektig	Onsagers AS, Postboks 6963 St Olavs Plass, 0130 OSLO, Norge			

(54)	Benevnelse	Frengangsmåte og system for personifisering av et smartkort
(56)	Anførte publikasjoner	US 4874935 A, US 4747706 A, JOLIET C: An integrated personalization workshop for smart Cards, PROCEEDINGS OF THE FOURTH ESCAT CONFERENCE. (EUROPEAN SMART CARD APPLICATIONS AND TECHNOLOGY), HELSINKI, FINLAND, 4-6 SEPT. 1991, pages 99-108.
(57)	Sammendrag	

Et smartkort-personaliseringssystem vedlikeholder en database omfattende kortutsleder-dataformatmal, kortapplikasjoner, kortoperativsystemordre, og personaliseringsutstyrsesifikasjoner, og tilveiebringer et sentralisert grensesnitt av innganger og utganger mot et kortutstedelsesprosess som dynamisk tilpasses endringer i utstedelsesprosessen for å tillate at en kortutsteder endrer formatene, kortapplikasjonene, kortoperativsystemene og/eller personaliseringsutstyret (130) i en kortutstedelsesprosess. Systemet har et grensesnitt til et hvilket som helst utsteder-styringssystem (150), styrer overføringen av kortutstederdata, og kortapplikasjoner til det spesielle personaliseringsutstyr som anvendes, og vedlikeholder statistikker for reel-tids- og frakoblet (offline) forespørsler for å støtte kritisk styring- og rapporteringsfunksjoner. Ytterligere virker systemet med flere sikkerhetsmetoder for å hindre svik.



Den foreliggende oppfinnelse vedrører datalagringsanordninger og nærmere bestemt fremstilling av bærbare, programmerte databærere slik som kredittkort, betalingskort, identifikasjonskort, og andre transaksjonskort.

Økende antall organisasjoner som utsteder transaksjonskort for deres brukere, kunder, eller ansatte krever kort som er skreddersydde for å oppfylle kravene til deres spesielle tjeneste eller applikasjon. Disse organisasjoner vil også at kortene skal inneholde data om kortets innehaver. Kjente transaksjonskort koder slike data i en magnetstripe på baksiden av kortet, men mengden data som kan bæres av en magnetstripe er begrenset. En ny type transaksjonskort har innstøpt en mikroprosessorfabrikke i kortets plast for å øke kortets datalagringskapasitet betraktelig. I tillegg kan sofistikerte kortapplikasjoner, spesielle for kortets utsteder utføres i noen varianter av brikkene, og brikken kan også omfatte en type operativsystem. Transaksjonskort med innstøpte brikker er omtalt i industrien som bærbare, programmerte databærere, mer vanlig kalt «smartkort». Brikken i et smartkort er programmert med initialiserings- og/eller personaliseringsdata samtidig som overflaten av kortet preges og/eller trykkes.

Initialiseringsdataene omfatter tre hoved-informasjonstyper: applikasjonsdata, sikkerhetsdata, og trykte data. Applikasjonsdata er felles for alle kortene, for en gitt kortapplikasjon og omfatter applikasjons-programkode og variabler. Sikkerhetsdataene forhindrer ulovlig anvendelse av kortet og er vanligvis tilveiebrakt i form av «sikre nøkler». Trykte data, slik som logo, strekkode, og forskjellige typer numerisk informasjon, plasseres på kortets overflate. Noen av de samme data eller alle disse kan også preges på overflaten. Optisk teknologi kan også anvendes for å gjøre hele eller en del av kortets flate til et lagringsmedium med data som er tilgjengelige ved hjelp av en egnet optisk leser.

Smartkortet programmeres også med informasjon som er spesiell for en enkelt kortinnehaver ved hjelp av en prosess kalt personalisering. Personaliseringsinformasjon for et smartkort er lik personaliseringsinformasjon vanligvis omfattet i ikke-smartkort, slik som kortinnehaverens navn, kontonummer, kortets utløpsdato og et bilde. På grunn av den økede lagringskapasitet kan brikken i et smartkort omfatte flere data enn basisinformasjonen på standard-transaksjonskortet, omfattende en grafisk representasjon av personens signatur, data som definerer type tjenester som kortinnehaveren er berettiget til, og kontogrenser for disse tjenester.

Smartkortets utstedelsesprosess må kontrollere og avgi rapport om hvert personalisert kort og om resultatene av personaliseringsprosessen. Omfattende rapportering- og revisjonsfiler må opprettholdes for å støtte kortets oppfølgingskrav.

Vanligvis må et smartkort-utstedelsessystem være skreddersydd for å oppfylle kravene for en spesifikk kortapplikasjon som vil programmeres på en spesifikk type smartkort under kontroll av et operativt system spesifikt for kortet, og for å

formatere dataene på kortet til å være kompatible med en spesiell type personaliseringsutstyr som er valgt for å utstede kortet. Hele utstedelsessystemet må konfigureres når noen av disse variabler (utsteder-applikasjon, smartkort-/kortoperativsystem, og/eller personaliseringsutstyr) er endret, og dette øker tidsforbruk og kostnadene for kortets utsteder tilknyttet levering av personaliserte smartkort til kundene. I tillegg mangler mange av de kjente utstedelsessystemer levedyktige midler for å gi kortets utsteder en dynamisk tilbakemelding angående status av en spesiell gruppe kort i prosessen.

Ytterligere anvender systemene for utstedelse av smartkort som er i bruk for tiden, en "eier-tilnæringsform" (proprietary approach) utviklet av kortets produsent eller produsenten av personaliseringsutstyret. For å oppmuntre salget av deres respektive kort eller utstyr, utvikler hver produsent en unik personaliseringsløsning for en spesiell kortapplikasjon, og hver løsning er spesiell for en bestemt kortutsteder. Disse unike løsningene er ment å optimere ytelsen av kortene eller utstyret og tillater således ikke en mer inklusiv, generalisert personaliseringsprosess som aksepterer et hvilket som helst kortoperativsystem og/eller virker med et hvilket som helst personaliseringsutstyr.

Artikkelen "JOLIET C: An integrated personalization workshop for smart Cards" publisert i "Proceedings of the fourth ESCAT conference (European smart cart applications and technology)", Helsinki, Finland, 4-6 september 1991 beskriver et programmeringsverktøy for personalisering av smartkort bestående av en kortholderdatabase med midler for å prege smartkortet.

US 4747706 beskriver en fremgangsmåte og system for å prege tegn på et kort som anvender en krets som beregner en tegnbevegelsestid og en kortbevegelsestid for hvert tegn.

US 4,874,935 beskriver en fremgangsmåte for klargjøring av en mikroprosessorbrikke i et smartkort til å holde et styringsprogram, applikasjonsdata, brukerinformasjon (kortinnehaverinformasjon), transaksjonsinformasjon og også dataordlister som beskriver ulike felter og lagersteder for data i brikken.

Siden etterspørselen for smartkort øker, vil et smartkort-utstedelsessystem som tillater at kortutstederne anvender et hvilket som helst type personaliseringsutstyr for å håndtere flere typer smartkort, og deres ledsagende operativsystemer, og for å innlemme utstederens spesielle kortapplikasjoner sammen med de krevde kortinnehaverdata i et hvilket som helst av de forskjellige typer smartkort, være nødvendig.

Et smartkort-personaliseringsystem vedlikeholder en database som omfatter kortapplikasjonsdata, utstederens formatmaldata, kortoperativsystemdata, og personaliseringsutstyrdata for å tillate at en kortutsteder dynamisk endrer

kortapplikasjoner, kort- og kortoperativsystemer, og/eller personaliseringsutstyr i en kortutstedelsesprosess uten behov for å endre kortutstederens grensesnitt mot utstedelsesprosessen.

5 Systemet for personalisering av smartkortet utsteder bærbare, programmerte databærere, eller smartkort, ved først å innhente et dataformat-kjennemerke, et kortoperativsystem-kjennemerke, et personaliseringsutstyr-kjennemerke, et applikasjonsprogram-kjennemerke eller kjennemerker, og personaliseringsdata for en kortinnehaver fra et kortutsteder-styringssystem. Kjennemerkene tillater at systemet adresserer data som er lagret i en datastruktur, slik som en database, og 10 spesifiserer de spesielle data som systemet krever for at hvert kort skal utstedes. På grunn av at hver kortutsteder formaterer personaliseringsdata på forskjellig måte og kan ha flere dataformater, har systemet for personalisering av smartkort en database med dataformatmaler som kan ha et grensesnitt mot flere kortutstedelsesstyringssystemer. Systemet innhenter formatmalen som definerer 15 personaliseringsdata anvendt ved en spesiell kortutsteder fra en post i databasen identifisert ved dataformat-kjennemerket. Systemet anvender dataformatmaler for å oversette personaliseringsdata fra kortutstederformat til et internt format som gjenkjennes av systemets komponenter. Systemet anvender kortets operativsystem-kjennemerket og applikasjonsprogram-kjennemerket(-ne) for å innhente 20 programmeringskontrollordre for et operativsystem som er lastet på forhånd i en mikroprosessorbrikke innstøpt i kortet, og applikasjonsdata, i form av kode og/eller variabler, for applikasjonsprogramtype(r) fra databasen. Systemet innhenter også utstyrets karakteristiske data for personaliseringsutstyret som skal anvendes for å utstede smartkortet ved anvendelse av personaliseringsutstyr-kjennemerket. Når 25 systemet har innhentet alle data som er nødvendige for å utstede smartkortet overfører det programkontrollordrene, applikasjonskoden, variablene, og de oversatte personaliseringsdata til personaliseringsutstyret som spesifisert ved utstyrets karakteristiske data.

30 Som et alternativ, sender kortets utsteder ikke noe dataformat-kjennemerke fordi dataformatmalen avledes fra data i applikasjonsdata-posten eller fordi personaliseringsformatet tilsvarer i en en-til-en-basis med det interne format som anvendes i systemet. Kortets utsteder kan også erstatte dataformatmal-posten med dataformat-kjennemerket slik at systemet ikke behøver å referere til dets format-post-database.

35 Et annet trekk ved smartkort-personaliseringssystemet er kortstyringsfunksjonen. Smartkort-personaliseringssystemet samler opplysninger vedrørende kortets utstedelsesprosess og rapporterer disse opplysninger til styringssystemet for kortutstedelse.

Smartkort kan omfatte en eller flere «sikre nøkler» som er programmert i brikken for å hindre ulovlig anvendelse av kortet. De egnede sikker nøkkeldata fremskaffes ved smartkort-personaliseringssystemet fra sikker nøkkel-post som vedlikeholdes av kortets utsteder, eller en annen sikkerhetskilde, og deretter overføres til

5 personaliseringsutstyret. Sikkerhetskilden leverer også sikkerhetsfunksjoner som anvendes ved smartkort-personaliseringssystemet for å sikre integriteten og hemmeligheten til dataene under overføring av data til og fra systemet og innenfor systemet under smartkortets personaliseringsprosess.

Smartkort-styringssystemet utfører funksjonene beskrevet ovenfor gjennom en serie

10 programvaremoduler som utføres på en eller flere datamaskiner. En modul er et kortutstedelses-styringssystem-grensesnittet som innhenter dataformat-kjennemerket, kortoperativsystem-kjennemerket, personaliseringsutstyr-kjennemerket, applikasjonsprogram-kjennemerket(-ne), og personaliseringsdata for en kortinnehaver fra kortutstedelses-styringssystemet. Kortutstedelses-

15 styringssystem-grensesnittet anvender deretter dataformat-kjennemerket for å innhente formatmaler som definerer personaliseringsdata og oversetter personaliseringsdataene til det vanlige interne dataformat. En kortoperativsystem-grensesnittmodul innhenter programmeringskontrollordene for kortets operativsystem-type spesifisert ved kortets operativsystem-kjennemerke. En

20 kortapplikasjons-grensesnittmodul anvender applikasjonsprogram-kjennemerket (-ne) for å bestemme hvilken type (hvilke typer) applikasjonsprogram som skal plasseres på kortet og innhenter de spesifiserte applikasjonskoder og variabler. En personaliseringsutstyr-grensesnittmodul er ansvarlig for innhenting av utstyrets karakteristiske data for personaliseringsutstyr-typen spesifisert ved

25 personaliseringsutstyr-kjennemerket, og ytterligere for å overføre programmeringskontroll-ordene, applikasjonskoden og variablene, og de oversatte personaliseringsdata til personaliseringsutstyret ifølge kravene angitt ved utstyrets karakteristiske data.

Rapportering og sikkerhetsfunksjoner er tilveiebragt ved en oppfølging/

30 rapportmodul og ved en modul for styring av sikker nøkkel.

Systemet for personalisering av smartkortene anvender en underliggende datastruktur, slik som en database, som ligger i et datamaskin-lagringsmedium for å organisere data som er nødvendige for å utstede smartkortene. Datastrukturen omfatter flere forskjellige typer data-elementer og anvender indekser eller

35 kjennemerker for hurtig aksessere spesifikke data. Det finnes fire hoveddata-elementer i systemet: et dataformat-element, et kortoperativsystem-element, et applikasjonsprogram-element, og et personaliseringsutstyr-element.

Dataformat-elementet omfatter en mal som definerer formatet for personaliseringsdataene som anvendes ved kortets utsteder. Dataformat-elementet

- kan være lagret i en database som omfatter dataformat-elementer for flere kortutstedere og informasjonen lagret i dataformat-elementet aksesseres gjennom dataformat-kjennemerket. Som et alternativ kan dataformat-elementet avledes ved det tidspunkt kortet utstedes fra data i applikasjonsprogram-elementet(-ne) slik at
- 5 applikasjonsprogram-kjennemerket som sendes av kortets utsteder identifiserer dataformatet. Når dataformatet for personaliseringsdataene tilsvareer nøyaktig det interne format ved smartkortets personaliseringssystem, er dataformatmaler som danner et virtuelt dataformat-element for utstedelsesprosessen logisk medført.
- Kortoperativsystem-elementer holder programmeringskontrollordre som leder
- 10 kortets operativsystemer og som kontrollerer en smartkortbrikke og aksesseres gjennom kortets operativsystem-kjennemerke.
- Applikasjonsprogram-elementene omfatter applikasjonsdata, slik som programkode og variabler, som kreves ved applikasjonene tilknyttet flere kortutstedere; applikasjonsdata aksesseres gjennom applikasjonsprogram-kjennemerket(-ne).
- 15 Driftsparametrene for flere typer personaliseringsutstyr anvendt for å utstede smartkort lagres i personaliseringsutstyr-elementet og aksesseres ved hjelp av et personaliseringsutstyr-kjennemerke tilsvarende typen personaliseringsutstyr som skal anvendes under utstedelsen.
- Spesielle konfigurasjoner for smartkort-personaliseringssystemet støtter
- 20 kortutstedere som ikke trenger full systemfleksibilitet som beskrevet ovenfor.
- Smartkort-personaliseringssystemet adresserer svakhetene i den kjente teknikk ved å tilveiebringe et sentralisert grensesnitt med inngangssignaler og utgangssignaler til smartkort-personaliseringsprosessen som er utformet for dynamisk å innrette seg til endringer i utstedelsesprosessen. Systemet har et grensesnitt mot et hvilket som
- 25 helst utstedelses-styringssystem, det styrer overføring av kortinnehaverens data og kortapplikasjoner til det spesielle personaliseringsutstyr som er anvendt, samler statistikker for reell tids- og frakoblede (off-line) forespørsler og støtter kritisk styrings- og rapporteringsfunksjoner. Systemet vedlikeholder en database med utstedelsesdataformat, kortoperativsystemer, kortapplikasjonsprogrammer, og typen
- 30 personaliseringsutstyr. Denne database tillater at systemet håndterer en hvilken som helst kombinasjon eller permutasjon av dataene, og således forbedrer kostnadene og tid-til-markedet for utstederen. Ytterligere har systemet et grensesnitt mot flere kortsikkerhetsfremgangsmåter for å redusere svindel.
- Oppfinnelsen vil nå beskrives med henvisning til de vedlagte tegninger, hvor
- 35 Fig. 1A er et blokkdiagram som representerer en prosess for utstedelse av et smartkort som har innlemmet et smartkort-personaliseringssystem.

- Fig. 1B er et funksjons-blokkdiagram for inngangs- og utgangskoplinger for smartkort-personaliseringssystemet vist i fig. 1A.
- Fig. 1C er et funksjons-blokkdiagram som viser programvaremoduler og datastrukturer som omfatter en utførelse av smartkort-personaliseringssystemet vist i fig. 1B.
- 5 Fig. 2 er et funksjons-blokkdiagram for utførelsen i fig. 1C med tilføyelse av en sikkerhetsmodul for å styre nøklene anvendt for smartkort.
- Fig. 3 er et funksjons-blokkdiagram av en annen utførelse av smartkort-personaliseringssystemet som viser en minimal konfigurasjon for å styre flere typer kort og personaliseringsutstyr.
- 10 Fig. 4 er funksjons-blokkdiagrammet for utførelsen i fig. 3 med tilføyelse av en modul for å styre flere kortoperativsystemer.
- Fig. 5 er funksjons-blokkdiagrammet for utførelsen i fig. 4 med sikkerhetsmodulen.
- 15 Fig. 6 er funksjons-blokkdiagrammet for utførelsen i fig. 3 med tilføyelse av en modul for å styre flere kortapplikasjoner.
- Fig. 7 er funksjons-blokkdiagrammet for utførelsen i fig. 6 med tilføyelse av sikkerhetsmodulen.
- 20 Fig. 8 er et høyt nivå-flytskjema for datamaskinprogramvare som implementerer funksjonene til smartkort-personaliseringssystemet.
- Fig. 9 er et funksjons-blokkdiagram av en alternativ utførelse av smartkort-personaliseringssystemet med anvendelse av programvaremoduler og data-poster.
- 25 Fig. 10 er et høyt nivå-flytskjema for datamaskinprogramvarer som implementerer funksjonene i utførelsen av smartkort-personaliseringssystemet vist i fig. 9.
- Fig. 11 er et datafeltskjema for en korttrammemal-post anvendt ved utførelsen av smartkort-personaliseringssystemet vist i fig. 9.
- 30 Fig. 12 er et datafeltskjema for en dataformatmal-post anvendt ved utførelsen av smartkort-personaliseringssystemet vist i fig. 9.
- Fig. 13 er et datafeltskjema for et kortapplikasjonsdata-post anvendt ved utførelsen av smartkort-personaliseringssystemet vist i fig. 9.

Fig. 14 er en rapportmal som viser utvalgs-poster som oppfølges ved smartkort-personaliseringssystemet.

I den følgende detaljerte beskrivelse av utførelsene, refererer man til de vedlagte tegningene som danner en del herav, og hvor det vises som illustrasjon spesielle utførelser hvor oppfinnelsen kan anvendes. Disse utførelser er beskrevet i tilstrekkelig detalj for å tillate at fagmannen på området skal kunne utføre oppfinnelsen, og man skal forstå det slik at andre utførelser kan anvendes, og at strukturelle, logiske og elektriske endringer kan foretas uten å komme bort seg fra ånden og rammen ved den foreliggende oppfinnelse. Den følgende detaljerte beskrivelse skal derfor ikke betraktes på en begrenset måte og rammen for den foreliggende oppfinnelsen er definert bare ved de vedlagte krav.

Det første siffer (de første sifrene) i henvisningtallene i figurene tilsvarer vanligvis figur-nummer, med det unntak at identiske komponenter som er tilstede i flere figurer identifiseres med samme henvisningstall.

15 Utstedelse av smartkort

Standard transaksjonskort slik som vanlige kredittkort er kjent for de fleste mennesker. Et transaksjonskort inneholder vanligvis informasjon angående kort-innehaveren, slik som navn og kortnummer, trykket eller preget på kortets overflate. Transaksjonskort omfatter vanligvis en magnetstripe som også er kodet med kortinnehaverens data. Prosessen for trykking/preging/koding av kortinnehaverens data på hvert transaksjonskort er kjent som "personalisering". Hvert transaksjonskort underkastes også en prosess kjent som "initialisering" hvor noen typer informasjon som er felles for alle kort i en gruppe, slik som utsteder-kjennemerke og gruppenummer, plasseres i kortet.

Et smartkort skiller seg fra et standard transaksjonskort i at en datamaskin-mikroprosessorbrikke er innstøpt i kortets plast for å øke kortets datalagringskapasitet betraktelig. I noen varianter av smartkort vil kortets produsent laste brikken på forhånd med en av flere mulige kortoperativsystemer, og operativsystemet kontrollerer brikkens programmering under personaliseringsprosessen.

I tillegg kan sofistikerte kortapplikasjoner som er spesielle for kortutstederen utføres i noen varianter av brikkene.

Initialiseringsdata for et smartkort omfatter tre hoved-informasjontyper: applikasjonsdata, sikkerhetsdata og trykkede data. Applikasjonsdata er felles for alle kort med en gitt kortapplikasjon og omfatter applikasjonsprogramkode og variabler som er programmert i brikken. Sikkerhetsdata, vanligvis tilveiebragt i form av sikre nøkler eller sikkerhetsfunksjoner, validerer data på kortet og hindrer

ulovlig anvendelse av kortet. Trykkede data, slik som logo, strekkode og flere typer numerisk informasjon, trykkes på kortets overflate. Noen av de samme data eller alle de kan også preges på overflaten. Optisk teknologi kan også anvendes for å gjøre danne en del av overflaten til smartkortet til et lagringsmedium med data som er tilgjengelige ved hjelp av en egnet optisk leser.

Personaliseringsinformasjon for et smartkort er tilsvarende personaliseringsinformasjonen som vanligvis er omfattet i ikke-smartkort, slik som kortinnehaverens navn, kortnummer, kortets utløpsdato, og et bilde. På grunn av den økede lagringskapasitet kan brikken i et smartkort omfatte ytterligere data i tillegg til basisinformasjonen tilstedet på standard transaksjonskort, omfattende en grafisk representasjon av individets signatur, data som definerer type tjenester som kortinnehaveren er berettiget til, og kontogrenser for slike tjenester.

Smartkort-personaliseringsystem

Fig. 1A viser komponentene i en smartkort-utstedelsesprosess som omfatter en utførelse av smartkort-personaliseringsystemet ifølge den foreliggende oppfinnelse. Smartkort-personaliseringsystemet 100 mottar data fra et kortutstederstyringssystem 150 (vanligvis eieren til kortets utsteder), oversetter dataene til en datastrøm og mater ut datastrømmen til personaliseringsutstyret 130 som personaliserer smartkortene 160. Kortutstederstyringssystemet 150 styrer kortinnehaverens data og fastsetter type kort som skal utstedes, kortapplikasjoner som skal innstøpes i kortet, og hvilket personaliseringsutstyr som skal anvendes for å utstede kortet for en spesiell kortinnehaver. Kortutstederens styresystem er vanligvis et datamaskinprogram som vist i fig. 1A, men smartkort-personaliseringsystemet 100 kan motta data fra alternative innmatinger, slik som f.eks. en person som mater inn data fra et telefontastatur.

Smartkort-personaliseringsystemet 100 vises i fig. 1A som et datamaskinprogram som utføres i en datamaskin. Som beskrevet nedenfor, aksesserer smartkort-personaliseringsystemet 100 database-poster som definerer flere typer kort og kortoperativsystemer, kortapplikasjoner, og personaliseringsutstyr.

De logiske funksjoner for programvaren og databasen kan være fordelt blant datamaskiner i et klient/server-nettverk eller sentralisert i en enkelt prosessor. Funksjonene kan også være fordelt på prosessorer som er koplet gjennom et standard lokalt nett (LAN), et fjernnett (WAN), dediserte telefonlinjer eller andre kommunikasjonsmidler som anvendes for løs kopling av prosessorer. Programvareprogrammet utføres under et operativsystem slik som Unix, Windows 95, eller Windows NT, og på en industristandard-arbeidsstasjon og/eller personlig datamaskinutstyr.

Systemet 100 kontrollerer kortprintere, pregingsanordninger, og integrerte eller tilføyde smartkort-grensesnittanordninger som representeres i fellesskap i fig. 1A ved personaliseringssystemet 130. Personaliseringsutstyret 130 representerer også slike anordninger som korttrykking/pregingsanordninger for store antall, korttrykking/pregingsanordninger for små antall, automatiske tellemaskiner (ATMer), salgspunktterminaler, ubemannede kiosker, person-datamaskiner, nettverks-datamaskiner, og on-line telekommunikasjonsanordninger. På grunn av investeringen i eksisterende ikke-smartkort-personaliseringsutstyr, vil flere kortutstedere ikke kjøpe et fullstendig nytt smartkort-personaliseringssystem, men vil i stedet øke det eksisterende personaliseringsutstyr med en smartkort-grensesnittanordning som programmerer brikken i kortet mens den eldre anordning utfører trykkings- og pregings-funksjonene. I en slik konfigurasjon kan datamaskin-systemet som utfører smartkort-personaliseringssystemet 100, eller verten, være fysisk koplet til begge anordningene eller til bare den ene. I det siste tilfelle kontrollerer verten denne direkte-kopledede anordningen og den har en logisk kopling til den andre. Den fysiske kopling mellom anordningene og verten varierer med produsenten og med anordningens modell. Vanlige industri-standardkoplinger omfatter serie RS232, SCSI (Small Computer System Interface), Ethernet, og serie TTL (Transistor-Transistor Logic). I tillegg krever noen anordninger en eier-busskopling.

Koplingene mellom smartkort-personaliseringssystemet 100 og kortets styresystem 150 og anordningen 130 kan også implementeres ved standard lokalnett, fjernnett, dediserte telefonlinjer eller annen fjernkommunikasjon-infrastruktur for å overføre data. Anvendelse av slike fjernkoplinger ved personalisering av smartkort er beskrevet i US-patent nr. 5.524.857, utstedt 9. juli 1996, Laing, m.fl. Alternative koplinger vil være åpenbare for fagmannen på området og ligger innenfor oppfinnelsens ramme.

Fig. 1B er et blokkdiagram av en utførelse av smartkort-personaliseringssystemet som illustrerer de logiske koplinger mellom smartkort-personaliseringssystemet 100 og funksjonene anvendt av en kortutstedelsesorganisasjon for å utstede smartkort. Kortinnehaverens data som vedlikeholdes av kortutstedelsesorganisasjonen omfatter informasjon om hver enkelt kortinnehaver, slik som navn, kontonummer, kortets utløpsdato, og tjenester som kan anvendes. Flere måter å mate inn kortinnehaverens data til kortutsteder-styringssystem 150 vises i fantomtegning slik som kortinnehaverens data 152 i fig. 1B. Kortutsteder-styringssystemet 150 kan motta kortinnehaverens data på datamaskinmedia, slik som magnetbånd, floppy-disc eller CD-ROM. Alternativt kan kortinnehaverens data 152 mates inn gjennom en on-line-kobling, slik som et generelt svitsjet-telefonnettverk, et pakkesvitsjet-nettverk, f.eks. Internett, en dedisert linje, eller et kabel/satellitt-TV-signal. Ytterligere måter

for innmating av kortinnehaverens data 152 til systemet 150 vil være åpenbare for fagmannen på området.

I tillegg til kortutsteder-styringssystemet 150, har vanligvis kortutstederen en eksisterende rapporteringsanordning 154, mot hvilken smartkort-personaliseringssystemet 100 har et grensesnitt, slik at kortutstederen kan gjennomgå statistisk informasjon vedlikeholdt ved systemet 100. En ekstern sikkerhetskilde, også tilveiebragt ved kortutstederen og henvist som styringsanordning for sikker-nøkkel 111 og database for sikker-nøkkel 128, tilveiebringer sikkerhetsfunksjoner som samvirker med kortutsteder- styringssystemet 150 og smartkort-personaliseringssystemet 100. Fig. 1B illustrerer også en alternativ utførelse av smartkort-personaliseringssystemet 100 som støtter en kortutsteder som har tilleggs- (add-on)smartkort-grensesnittanordninger. Systemet 100 sender et parti av personaliseringsinformasjonen til det gamle personaliseringsutstyr 130 og resten av data til en postprosessor 132 i smartkort-grensesnittanordningen 132 som programmerer brikken. Disse funksjoner forklares i detalj nedenfor.

Utførelser av datamaskin-programvareprogrammet for smartkort-personaliseringssystemet 100 vist i de følgende tegninger, virker som kombinasjoner av kodemoduler hvor hver modul utfører en spesifikk del av utstedelsesprosessen. I disse utførelser koples modulene ved hjelp av definerte innmatings- og utmatingsprogramanrop og de er også koplet til datastrukturene gjennom standard data-spørreordre som tilveiebringer tilgang til dataene lagret i datastrukturene. Kommunikasjonsprotokollene mellom modulene, og mellom modulene og datastrukturene, varierer avhengig av språket i hvilket modulene er skrevet, og av det underliggende datastyringssystem som anvendes for å støtte databasen.

Fig. 1C er et mer detaljert funksjons-blokkdiagram for smartkort-personaliseringssystemet 100 i fig. 1B uten de eksterne sikkerhetsfunksjoner. Fig. 1C viser de interne koplinger mellom programvaremoduler og database-poster som tillater at smartkort-personaliseringssystemet 100 kombinerer flere typer utstederdataformater, kortoperativsystemer, kortapplikasjoner og personaliseringsutstyr ved utstedelse av smartkortet.

Smartkort-personaliseringssystemet 100 tilveiebringer et brukertilpasset kortutsteder-styringssystem-grensesnitt 101 mot et kortutsteder-styringssystem 150. I denne utførelse, sender kortutsteder-styringssystemet 150 personaliseringsdata fra en kortinnehaver database 152 til systemet 100. Hver programvaremodul innenfor systemet 100 forventer at personaliseringsdata passerer til den i et spesielt internt format. Siden personaliseringsdata har et eksternt format definert ved kortutstederen, og som ofte er forskjellig fra det interne format (de interne formater) forventet ved programvaremodulene, oversettes personaliseringsdata ved systemet 100 til det interne format (de interne formater) ved anvendelse av dataformatmalen.

Systemet 100 kan innhente dataformatmalen gjennom et dataformat-kjennemerke som sendes av kortutstederen og som systemet 100 anvender for å hente en eventuell dataformatmal-post 120 (vist i fantomtegning i fig. 1C), som illustrert ved en valgfri kobling mellom posten 120 og kortutsteder-styringssystem-grensesnitt 102. Som et alternativ sender kortutstederen dataformatmal-posten til systemet 100 istedenfor dataformat-kjennemerket. I en annen utførelse, kan dataformatmalen avledes fra datakort-applikasjons-posten 124 som er spesifisert ved et applikasjonsprogram-kjennemerke som sendes ved utstederen som illustrert ved en valgfri kobling mellom kortapplikasjons databasen 124 og kortutsteder-styringssystem-grensesnittet 101.

I en ytterligere, alternativ utførelse av fig. 1C, tilveiebringes sikkerhetsfunksjoner internt ved smartkort-personaliseringssystemet 100 ved å sende sikkerhetsfunksjoner i systemet som en del av kortapplikasjons-posten.

En ytterligere alternativ utførelse, hvor personaliseringsdataformatet tilsvarer det interne format, er også vist i fig. 1C. Siden ingen oversettelse mellom det eksterne og interne format er nødvendig i denne utførelse, behøves ingen dataformatmal, slik at dataformat-posten 120 og kodingene mellom kortutsteder-styringssystem-grensesnittet 101 og dataformat-posten 120 og kortapplikasjons databasen 124 ikke er tilstede. Dataformat-posten 120 kan bestå av flere tabeller som gir instruksjoner til systemet 100 angående den egnede spalting av personaliseringsdata eller en enkelt liste som angir rekkefølgen i hvilken feltene i kortinnehaverdata-posten er tilstede, som det vil være åpenbart for fagmannen på området. De forskjellige alternative prosedyrer for å fastsette formatet for personaliseringsdataene beskrevet ovenfor er implisitt i alle utførelser av smartkort-personaliseringssystemet 100 beskrevet her.

Ved anvendelse av et kort-kjennemerke levert ved kortutstedelses-styringssystemet 150, gjenfinner en kortoperativsystem-grensesnittsmodul 103 programmeringskontrollordre som er spesielle for operativsystemet 120 for mikroprosessorbrikken som er innstøpt i den type kort som utstedes. Programmeringskontrollordrene styrer kodingen av brikken med personaliseringsdata og kortapplikasjonene valgt av kortets utsteder.

Hver kortapplikasjon omfatter programkode- og variabledata som er lagret i databasen som applikasjonsdata 124 og som er identifisert ved et applikasjonsprogram-kjennemerke. Kortutsteder-styringssystemet 150 sender en eller flere programapplikasjons-kjennemerker til systemet 100 som anvendes ved en kortapplikasjons-grensesnittsmodul 105 for å innhente de tilsvarende applikasjonsdata 124.

Personaliseringsutstyret som kortutstederen planlegger å anvende for å utstede kortgruppen er definert ved et personaliseringsutstyr-kjennemerke. En

personaliseringsutstyr-grensesnittmodul 107 innhenter utstyrets karakteristiske data 126 som er spesielle for den type personaliseringsutstyr 130 som tilsvarende personaliseringsutstyr-kjennemerke. Personaliseringsutstyr-grensesnittet 107 innhenter også programmeringskontrollordre, applikasjonskode og variabler, og de
 5 oversatte personaliseringsdata, og overfører all denne data til personaliseringsutstyret 130 som spesifisert ved de utstyrets karakteristiske data 126 for utstedelse av smartkortet.

En alternativ utførelse av systemet 100 støtter en kortutsteder som har økt sitt eksisterende personaliseringsutstyr med en smartkortprogrammeringsanordning, ved
 10 at personaliseringsutstyr-grensesnittet 107 sender en sub-gruppe av den oversatte personaliseringsinformasjon til det eldre personaliseringsutstyr 130 og resten av dataene til en post-prosessor 132 i smartkort-programmeringsanordningen.

Smartkort-personaliseringsutstyret 100 tilveiebringer også en oppfølgings-/rapportmodul eller -maskin 109, som samler statistisk informasjon fra de andre
 15 moduler i systemet 100 og formaterer den statistiske informasjon for utmating som hardkopi-rapporter 154 eller som innmating til en rapporteringsfunksjon i kortutsteder-styringssystemet 150. På grunn av at denne statistiske informasjon samles i reell tid, kan kortutsteder-styringssystemet 150 interaktivt be oppfølgings-/rapportmodulen 109 å fremskaffe statistikker om smartkort-
 20 personaliseringssystemet under driften. Eksempler på punkter som overvåkes ved oppfølgings-/rapportmodulen 109 vises i fig. 14.

I en alternativ utførelse vist i fig. 2, omfatter smartkort-personaliseringssystemet 100 en sikkerhetskilde i form av en sikkerhetsnøkkel-styringsanordning 111 og sikkerhetsnøkkel database 128. Når et smartkort er fremstilt, inkluderer selgeren
 25 sikkerhetsarkitektur for brikken for å hindre ikke-autorisert programmering. Sikkerhetsarkitektur-implementeringen er vanligvis avhengig av applikasjonen programmert på brikken. For eksempel vil sikkerhetsnøkklene programmert i en lagretverdi-applikasjon være forskjellig fra sikkerhetsnøkklene programmert i en helsevesen-applikasjon. Sikkerhetsarkitektur-implementeringen varierer også
 30 avhengig av typen kort: noen kort krever en enkelt sikkerhetsnøkkel som tillater brikkeprogrammering mens andre krever flere sikkerhetsnøkler for å tillate brikkeprogrammering og for å utføre flere ytterligere sikkerhetsfunksjoner. Fig. 2 illustrerer grunnfunksjonene for sikkerhetsnøkkel-styringsanordningen når den har et grensesnitt med sikkerhetsarkitektur på et kort som krever flere sikkerhetsnøkler.

Som vist i fig. 2, lagres sikkerhetsnøkkeldata i sikkerhetsnøkkel-databasen 128 som er ekstern til smartkort-personaliseringssystemet 100 og som vedlikeholdes av kortutstederen eller av en annen sikkerhetskilde. Utvidelse av sikkerhetsnøkkel-styringsanordningen 111 for å håndtere flere eller færre sikkerhetsnøkler, og for å ha et grensesnitt mot en sikkerhetsnøkkel database som styres ved selve smartkort-

personaliseringssystem er avhengig av applikasjonen, operativsystemet og personaliseringsutstyret som anvendes i den spesifikke kortutstedelses-applikasjon, og vil være åpenbar for fagmannen på området.

5 Sikkernøkkel-styringsanordningen 111 tilveiebringer også ytterligere mekanismer for å sikre sikkernøkkel-dataautentisering, dataintegritet og datahemmeligholdelse. I en utførelse utføres sikkernøkkel-dataautentiseringen ved implementering av flere dekrypteringsmetoder. Sikkernøkkel-dataintegriteten oppnås ved digital signurmekanismer som anvender offentlige nøkler for å sikre at sikkernøkkeldata overføres og mottas fra gyldige kilder. Sikkernøkkeldatahemmeligholdelse sikres 10 ved å dekryptere de overførte data med en privat nøkkel som deles med datamottakeren og som datamottakeren anvender for å dekryptere dataene ved mottakelse.

Etter at systemet 100 mottar en sikkernøkkel-post fra sikkernøkkel-databasen 128, vil sikkernøkkel-styringen, sammen med kortoperativsystem-grensesnittet 103 og 15 kortapplikasjons-grensesnittet 105, utføre sikkernøkkel-autentisering-, dataintegritet- og datahemmeligholdelsesfunksjonene. Systemet 100 overfører da sikkernøkkel-data til personaliseringsutstyret 130 sammen med de andre dataene for kortet gjennom personaliseringsstyr-grensesnittet 107.

I en alternativ utførelse, sender sikkernøkkel-styringsanordningen 111 sikkerhets- 20 informasjon til de andre moduler på smartkort-personaliseringssystemet 100. For eksempel kan deler av kortinnhaverdataene, slik som PIN- (personlig identifikasjonsnummer) kode dekrypteres ved utsteder-styringssystemet 150 før data sendes til smartkort-personaliseringssystemet 100. Kortutsteder-styringssystem-grensesnittet 101 gjenfinner den krypteringsnøkkelen i sikkernøkkel-databasen 128 25 ved sikkernøkkel-styringsanordningen 111, og dekrypterer data før koding eller programmering av PIN-kode i magnetstripen og/eller brikken.

I en ytterligere alternativ utførelse, er sikkernøkkel-styringsanordningen 111 en kode-«krok» i smartkort-personaliseringssystemet 100 som tilveiebringer en portkopling for en ekstern sikkerhetskilde som leverer de ønskede 30 sikkerhetsfunksjoner. Et eksempel av en slik ekstern sikkerhetskilde er et sikkerhets-styringsprogram som er skrevet av en tredje part som styrer en sikkerhets database av sikkernøkler og/eller sikkerhetsfunksjoner tilsvarende sikkernøkkel-databasen 128. Sikkerhetsfunksjonene kan være enten eksterne rutiner utført ved sikkerhetsstyring, eller kodemoduler sendt ved sikkerhetsstyringen som er utført 35 ved smartkort-personaliseringssystemet 100 for å tilveiebringe de ønskede sikkerhetsfunksjoner, eller en kombinasjon av begge.

Fig. 3 viser en minimal konfigurasjon av smartkort-personaliseringssystemet 100. I denne utførelse er bare kortutsteder-styringssystem-grensesnittmodulen 101 og personaliserings-grensesnittmodulen 107 virksomme i programvaren. Denne

utførelse tillater at kortutstederen anvender systemet 100 for å personalisere ikke-smartkort og således spares kostnadene ved å ha to separate personaliseringssystemer, mens man tillater at kortutstederen anvender flere dataformater og flere typer personaliseringsutstyr. Fig. 3 illustrerer også en ytterligere alternativ utførelse som omfatter oppfølgings-/rapporteringsmodulen 109 som beskrevet ovenfor i forbindelse med fig. 1C.

I en ytterligere alternativ utførelse, koder smartkort-personaliseringssystemet 100 vist i fig. 3 data til et optisk transaksjonskort når optisk kodeutstyr anvendes som personaliseringsutstyr 130.

Fig. 4 og 5 viser enda ytterligere alternative utførelser som implementeres når kortutstederen ikke programmerer inn kortapplikasjonen i smartkortets brikke. Disse utførelsene tillater at kortutstederen utsteder flere korttyper med deres ledsagende flertall av operativsystemer på flere typer personaliseringsutstyr uten å måtte rekonfigurere smartkort-personaliseringssystemet 100. Som beskrevet ovenfor i forbindelse med fig. 1C, omfatter fig. 4 moduler som støtter rapporteringen og postprosesseringen. Fig. 5 illustrerer utførelsene i fig. 4 med tilføyelse av sikker nøkkel-styringsmodulen 111 som tilveiebringer sikkerhet til dataoperativsystem-grensesnittet 103 for overføring til personaliseringsutstyret 130.

På samme måte illustrerer fig. 6 og 7 utførelsen for å støtte en kortutsteder som anvender brikken på et smartkort bare som datalagringsanordning for en kortapplikasjon, og derfor ikke har et operativsystem som utføres på brikken. Smartkort-personaliseringssystemet 100 støtter flere kortapplikasjoner for flere korttyper utstedt ved flere typer personaliseringsutstyr. Fig. 6 og 7 er tilsvarende fig. 4 og 5 bortsett fra at sikker nøkkel-styringsanordningen 111 tilveiebringer sikker nøkler og/eller funksjoner til kortapplikasjons-grensesnittet 105 istedenfor til kortoperativ-grensesnittet 103.

Fig. 8 er et høyt nivå-flytskjema for utførelse av programvaren som implementerer funksjonene til smartkort-personaliseringssystemet 100 beskrevet ovenfor. Programvaren innhenter et personaliseringsutstyr-kjennemerke for en gruppe transaksjonskort som skal utstedes fra kortutsteder-styringssystemet ved blokk 801. Avhengig av type kort som skal utstedes, innhenter programvaren samtidig også et programapplikasjon-kjennemerke og/eller et kortoperativsystem-kjennemerke. Programvaren innhenter da den spesielle dataformatmal tilsvarende formatet til personaliseringsdata ved en av prosedyrene beskrevet ovenfor (blokk 803). Ved blokk 805 innhenter systemet utstyrets karakteristikk for personaliseringsutstyret som skal anvendes for å utstede kortgruppen fra personaliseringsutstyr-posten spesifisert ved personaliseringsutstyr-kjennemerket.

Hvis et kortoperativsystem-kjennemerke var plassert ved kortutsteder-styringssystemet (blokk 807), gjenfinner programvaren programmeringskontrollordene fra

kortets operativsystem database-post tilsvarende kortoperativsystem-kjennemerket ved blokk 809. Blokk 811 og 813 utfører samme logikk for en kortapplikasjon, med gjenfinning av applikasjonsdata, slik som kode og/eller variabler fra databasen. Ved dette punktet har programvaren innhentet de felles data som er nødvendige for alle kort i gruppen og begynner å gå i sløyfe gjennom logikken som utsteder kortene for de enkelte kortinnehavere.

Kortutsteder-styringssystemet sender personaliseringsdata for en enkelt kortinnehaver til programvaren (blokk 815) som oversetter data-postene fra formatet definert ved dataformatmalen til et internt format anvendt ved modulene på smartkort-personaliseringsystemet (blokk 817). Hvis kortbrikken omfatter sikkerhetsarkitektur som krever sikkernøkler (blokk 819), innhenter programvaren sikkernøkkeldataene som er nødvendige for å utføre sikkernøkkel-funksjonene fra de egnede sikkernøkkel-kilder ved blokk 821.

Programvaren er nå klar for å overføre data til personaliseringsutstyret for å programmere kortet. Hvis kortet er beskyttet ved sikkernøkler, er sikkernøkkel-funksjonene utført og sikkernøkkel-dataene overført ved blokk 823. Deretter overføres programmerings-kontrollkodene for brikkens operativsystem, hvis de anvendes (blokkene 825 og 827), og deretter er applikasjonskode og/eller variablene overført hvis de er nødvendige (blokk 829 og 831). Til slutt overføres kortinnehaverens personaliseringsdata som var oversatt til det interne format (blokk 833).

Etter at dataene er overført til kortet, tilføyer programvaren de egnede verdier til statistikkene som den samler for kortutsteder-styringssystemet ved blokk 839. Hvis flere kort i samme gruppe fortsatt skal utstedes (blokk 841), kommer programvaren tilbake til blokk 815 og innhenter personaliseringsdata for neste kortinnehaver. Ellers fastsetter programvaren om kortutsteder-styringssystemet har et annet gruppekort for utstedelse (blokk 843) eller ikke og den kommer tilbake til blokk 801 for å innhente den nødvendige informasjon for å gjenta syklusen for den nye gruppe. Hvis ingen ytterligere kort skal utstedes, går programvaren ut.

Mekanismene ved hvilke kortutsteder-styringssystemet 150 sender de nødvendige data til smartkort-personaliseringsystemet 100 og rekkefølgen i hvilken smartkort-personaliseringsystemet prosesserer data fra kortutsteder-styringssystemet kan endres uten å overskride rammen for oppfinnelsen. Forskjellige montasjer er krevd ved det spesielle miljø hvor systemet 100 opererer, som vist ved den alternative utførelsen vist i fig. 9 og 10.

I fig. 9 virker en sikkerhetsmodul 911 som port til smartkort-personaliserings-systemet 100 for en sikkerhetskilde slik som sikkerhetsstyring 940 og sikkerhets databasen 942 vist i fig. 1B som 111 og 128 respektivt. Sikkerhetsstyringen 940 kontrollerer tilgang til sikkerhets databasen 942 og kopler til sikkerhetsporten 911

for å utføre de nødvendige sikkerhetsfunksjoner for smartkort-personaliseringssystemet 100. Sikkerhetsporten 911 er koplet til kortutstederstyringssystem-grensesnittet 901 som tillater at grensesnittet 901 krever at sikkerhetsstyringen 940 dekrypterer personaliseringsdata sent i et krypteringsformat ved kortutstederstyringssystemet 950. Sikkerhetsporten 911 er også koplet til kortapplikasjons-grensesnittet 903 og kortapplikasjons-grensesnittet 905, slik at den kan levere de nødvendige sikkerhetsnøkler og/eller sikkerhetsfunksjoner til grensesnittene som forklart ovenfor i forbindelse med fig. 2.

Ytterligere innhenter utførelsen av smartkort-personaliseringssystemet 100 vist i fig. 9 applikasjonsdata 922 spesifisert ved applikasjonsprogram-kjennemerket, før programmeringskontroll-ordrene spesifikke for kortoperativsystemet 924 innhentes ved hjelp av kort-kjennemerket. Denne utførelse tillater at personaliseringsdata og applikasjonsdata oversettes til det interne format før man gjenfinner programmeringsordre fra kortoperativsystemet 924 og utstyrets karakteristiske data 926, og således økes hastigheten til prosessering av hvert smartkort.

Standard transaksjonskort har data trykket eller preget på kortets overflate og/eller datakoder i en magnetstripe på kortet. Med et smartkort kan også data lagres i et internt minneområde innenfor mikroprosessen. Samme data kan plasseres på kortets overflate, i magnetstripen og også i brikkeminnet. Den nøyaktige konfigurering til data inne og på kortet vil variere avhengig av typen smartkort som utstedes og av kravene stilt av kortets utsteder.

Fig. 10 er et høyt nivå-flytskjema av utførelsen vist i fig. 9 og, sammen med fig. 11, 12 og 13, illustrerer ytterligere hvordan forskjellige mekanismer kan anvendes for å implementere smartkort-personaliseringssystemet 100. Kortutstederstyringssystemet 950 sender en korttrammemal som definerer konfigureringen til smartkort-personaliseringssystemet 100 ved blokk 1001.

Fig. 11 illustrerer en utførelse av dataanlegget for korttrammemal-posten 1100. Mikroprosessorbrikke-kjennemerket 1101 og kortoperativsystem-kjennemerket 1102 (hvis tilstede) er spesifikke for den type smartkort som skal utstedes. Hovedfil-definisjonen 1103 omfatter kontrollinformasjon slik som brikkekilde og siste dato brikken ble endret. Systemfil-definisjonene 1104, 1105, 1107 omfatter adresser for beliggenheten av systemfilene innenfor brikkens minne. Systemfilene anvendes ved kortoperativsystemet og inneholder informasjon slik som PIN-kode(r) for kort og applikasjoner og algoritmetabeller. I utførelsen vist i fig. 11, er hovedfil- og systemfil-definisjonene tilpasset den internasjonale standard-organisasjon (ISO), direktiv nr. 7816-4.

De neste tre deler av korttrammemal-posten 1100 definerer plassering av data på kortets overflate og magnetstripen. Hvis informasjonen skal trykkes på kortet, slik som kortinnhaverens bilde 1109, sendes beliggenheten på kortets overflate hvor

slike data skal trykkes til kortutsteder-styringssystemet 905 i trykkmalen til kortrammemal-posten 1100. På samme måte, sendes beliggenhetene på kortets overflate for preging av data i pregingsmalen, og anordningen av data som skal kodes i magnetstripen sendes i magnetstripemalen. PREGINGSDATA illustreres i

5 kortrammemal-posten 1100 som kortinnehaver-navn (EMNavn) 1111, kontonummer (EMAkonto) 1113, og utløpsdato (EMXdat) 1115 og magnetstripedataene som kontonummer (MSAkonto) 1117 og utløpsdato (MSXdat) 1119. Antall data-poster i trykkings- pregings- og magnetstripemalene vil variere avhengig av

10 konfigurasjonen til smartkortet som ønsket ved kortutstederen, som det vil være åpenbart for fagmannen på området.

Hvis kortutstederen vil ha kortapplikasjoner programmert i brikken i smartkortet, sender kortutstederen applikasjonsprogram-kjennemerkene til smartkort-personaliseringssystemet 100 i delene 1121, 1123, 1125 i kortrammemal-posten 1100. Hver applikasjon kan ha spesifikke sikkerhetsfunksjoner tilknyttet til den

15 (1127, 1129, 1131) og den informasjonen er også sendt ved kortutsteder-styringssystemet 950. Kortrammemal-posten 1100 omfatter også personaliseringsutstyr-kjennemerket 1123 for personaliseringsutstyret som anvendes for å utstede smartkortene.

I en alternativ utførelse, lagrer smartkort-personaliseringssystemet 100 vanligvis

20 anvendte kortrammemal-poster i en intern database, slik at kortutsteder-styringssystemet 950 bare trenger å sende et kortrammemal-kjennemerke som identifiserer hvilken kortrammemal-post som skal anvendes for en spesiell gruppe kort.

Smartkort-personaliseringssystemet 100 innhenter dataformatmalen for

25 personaliseringsdata fra en forhåndsdefinert beliggenhet spesifisert av kortutstederen ved blokk 1003. Hvis kortutstederen har sendt et dataformat-kjennemerke til systemet 100, gjenfinnes dataformatmal-posten tilsvarende dataformat-kjennemerket i dataformat databasen 920. Som et alternativ kan kortutstederen sende dataformatmal-posten selv. Når verken dataformat-

30 kjennemerket eller dataformatmal-posten sendes til systemet 100, fastsettes formatet til personaliseringsdata ved kortapplikasjonsdataene som forklart i større detalj nedenfor.

Et eksempel av en dataformatmal-post er vist i fig. 12. Dataformatmal-posten 1200

35 definerer en hypotetisk anordning av personaliseringsdata-postene i kortinnehaverens database 950 hvor kontonummeret 1201 er det første felt, kortinnehaverens navn 1202 er det andre felt, og utløpsdato for kortet 1205 er et tredje felt. I en utførelse er personaliseringsdata-postene komma-begrensede poster slik at ingen datafelt-lengder er nødvendige for å definere postenes format. Således definerer dataformatmal-posten 1200 vist i fig. 12 strukturen til det følgende

eksempel av en komma-begrenset personaliseringsdata-post til smartkort-personaliseringsystemet 100 fullstendig: 133444999922,Mary Jane Smith,0299.

Smartkort-personaliseringsystemet 100 innhenter applikasjonsdata for kortapplikasjonen, eller applikasjonene 922, tilsvarende applikasjonsprogram-
 5 kjennemerkene, hvis de er tilstede, som var sendt av kortutsteder-styringssystemet 950 ved blokk 1007. Hvis ikke noe applikasjonsprogram-kjennemerke er sendt, innhenter smartkort-personaliseringsystemet 100 standard (default) applikasjonsdata (blokk 1008). De standard og/eller applikasjonsdata i kort-
 10 applikasjons-posten(e) tilsvarende applikasjonsprogram-kjennemerkene innføres i de tilsvarende partier, dvs. 1121, 1123, 1125, i kortrammemal-posten 1100.

En utførelse av anordningen av en kortapplikasjons-post vises i fig. 13. Det første felt i kortapplikasjons-data-posten 1300 er applikasjonsnavn 1301. På samme måte som ved andre datamaskinbaserte applikasjonsprogrammer, prosesserer en
 15 kortapplikasjon data fra eksterne kilder slik som en automatisk tellemaskin eller interne kilder slik som datafiler kodet til mikroprosessorens minne. Anvendelse av smartkortet forårsaker at den egnede applikasjon utføres ved mikroprosessoren og applikasjonen, i sin tur, aksesserer de interne filer for å gjenfinne eller lagre data. For å aksessere interne data, omfatter kortapplikasjonsdata-posten pekere til
 20 applikasjonsfiler i brikkeminnet (1302, 1305, 1037) og også beliggenheten av feltene innenfor applikasjonsfilene. Noen av feltene er initialisert med data fra kortinnehaver databasen 952 når kortet utstedes. Applikasjonsdataene 1300 omfatter en adresse 1303 til en kortinnehaverfil plassert i brikkens minne og definerer kortinnehaverfilen som omfatter tre felt: kortinnehaverens navn (ICNavn) 1309, kontonummer (ICKonto) 1311 og utløpsdato (ICXdat) 1313. Videre lagres interne
 25 data i andre applikasjonsfiler og anordningen av disse ytterligere filer er også definert ved applikasjonsdata 1300.

Hvis brikken som er innstøpt i smartkortet omfatter et operativsystem som spesifisert ved kortrammemal-posten, innhenter smartkort-personaliseringsystemet 100 et sett av programmeringskontrollordre for operativsystemet fra kortoperasjons
 30 databasen 924 ved blokk 1011. Programmeringskontroll-ordrene for hvert operativsystem omfatter ordre for funksjoner slik som å danne og aksessere filer i brikkens minne, å lese og skrive poster i filene plassert i brikkeminnet, sammen med sikkerhetsordre som autentiserer PIN- (personlig identifikasjonsnummer) koder og kontrolltransaksjoner som endrer pengemengder lagret i brikken.

Smartkort-personaliseringsystemet 100 innhenter utstyrets karakteristiske data tilsvarende personaliseringsutstyr-kjennemerket i kortrammemal-posten fra personaliseringsutstyr-databasen 926 ved blokk 1013. Omfattet i utstyrets karakteristiske data er et sett av personaliseringsprogrammerings-kontrollordre som kontrollerer driften av personaliseringsutstyret. På samme måte som ved tilfellet

med kortoperativsystemene er personaliserings-kontrollordre eiendom til selgeren av utstyret, men de omfatter vanligvis ordrer som er rettet mot administrasjon, formatering og fremstilling av smartkort.

5 Når smartkort-personaliseringssystemet 100 har innhentet alle data som er nødvendige for å definere smartkortet, er det klart til å akseptere personaliseringsdata-poster 952 fra kortutsteder-styringssystemet 950. Når hver personaliseringsdata-post 952 passerer ved blokk 1015, anvender smartkortpersonaliseringssystemet 100 dataformatmalen, hvis den er tilstede, for å
10 oversette personaliseringsdata til et internt format, og kortapplikasjonsdata og kortrammemalen for å avbilde personaliseringsdata til variabler i et command-skript, som er skrevet i et internt skriptspråk ved blokk 1017. Oversettelsen og avbildningsprosessen beskrives ytterligere nedenfor. Alternative utførelser som anvender et standard programmeringsspråk slik som Basic, Java eller C istedenfor det interne skriptspråket ligger innenfor oppfinnelsens ramme.

15 Smartkort-personaliseringssystemet 1019 kontrollerer sikkerhetskravene for de forskjellige komponenter i smartkort-utstedelsesprosessen. Ved utførelsen av kortrammemalen vist i fig. 11, er sikkerhetskrav for applikasjonene spesifisert ved kortrammemal-posten 1100 i blokk 1019. Hvis det finnes sikkerhetskrav innhenter smartkort-personaliseringssystemet 100 sikre data og/eller funksjoner fra
20 sikkerhetsstyringen 940 og tilføyer funksjonene til det interne skript ved blokken 1021. En alternativ utførelse av smartkort-personaliseringssystemet 100 sender kjennemerkene for kortoperativsystemet og personaliseringsutstyret, sammen med applikasjonsprogram-kjennemerket til sikkerhetsstyringen 940 som gjenfinner de egnede sikkerhetsdata og/eller funksjoner fra sikkerhets databasen 942. Sikkerhets-
25 funksjonene anvender vanligvis data fra ytterligere kilder, omfattende data lagret i interne brikkefiler, personaliseringsdata 952, operativsystem databasen 924, kortapplikasjons databasen 922, kombinert med algoritme-tabeller lagret i brikken eller kommende fra en ekstern sikkerhetsmodul, slik som sikkerhetsstyringen 940, for å utføre sikkerhetsnøkkel-autentiserings-, dataintegritets-, datahemmeligholdelses-
30 og andre sikkerhetsprosesser beskrevet ovenfor i forbindelse med fig. 2.

Når det interne ordreskript er utført, må det oversettes til eierprogrammerings-kontrollordre som er de opprinnelige for kortoperativsystemet (hvis tilstede) og til personaliseringsutstyret slik at personaliseringsdata kan overføres til smartkortet. I
35 denne utførelse utøves oversettelsen ved en skriptspråk-tolk ved blokk 1025 og 1027 med anvendelse av informasjonen innhentet fra kortoperativsystem databasen 924 og personaliseringsutstyr databasen 926.

Ved blokk 1029, sender smartkort-operativsystemet 100 det tolkede skrift til personaliseringsutstyret som da utfører programmerings-kontrollordre for å prege/trykke, kode og programmere de egnede personaliseringsdata respektivt på

overflaten, i magnetstripen og i brikken i smartkortet. Som tidligere, hvis kortutsteder har valgt å kjøpe en tilleggs-smartkort-programmeringsanordning for å tilføye den til det eksisterende personaliseringsutstyr, sender en alternativ utførelse av smartkort-personaliseringsystemet 100 kontrollordene for preging og koding til personaliseringsutstyret 930, og kontrollordre for brikken til postprosessen 132 i smartkort-programmeringsanordningen.

Når utstedelsesprosessen er fullført for et kort, innhenter smartkort-personaliseringsystemet 100 neste personaliseringsdata-post hvis det finnes ytterligere kort av samme type som venter på utstedelse (blokk 1033). Ellers fastsetter smartkort-personaliseringsystemet om det er en annen gruppe smartkort av en annen type som venter på utstedelse (blokk 1001) og utstedelsesprosessen begynner på nytt ved å innhente en ny korttrammemal-post fra kortutstederen.

Det følgende eksempel anvender prøve-data for å beskrive ytterligere prosesseringen utøvet ved utførelsen av smartkort-personaliseringsystemet 100 vist i fig. 9 og 10. Kortutsteder-styringssystemet 950 krever initialiseringen av utstedelsesprosessen ved å sende en korttrammemal-post, applikasjonsprogram-kjennemerke(r), et kortoperativsystem-kjennemerke, et personaliseringsutstyr-kjennemerke og, om ønskelig, et dataformatmal-kjennemerke eller en dataformatmal-post til smartkort-personaliseringsystemet 100. I dette eksemplet sender kortutsteder-styringssystemet 950 en applikasjonsressursmal-post som vist nedenfor og som omfatter kjennemerkene. Systemet 100 innhenter en dataformatmal ved anvendelse av en av prosedyrene beskrevet ovenfor og forklart i større detalj nedenfor i forbindelse med prøve-kortinnehaverdata-postene.

Applikasjonsressursmal-post

[A1]

DFT=CARD1.DFT

CAT=CARD1.CAT

CID=CHIPX.CID

CPT=CARD1.CPT/

SOURCE=A1

25

Den første setning i posten markerer begynnelsen av informasjonen for en spesiell applikasjon, i dette tilfellet applikasjon «A1». De neste fire setninger definerer kjennemerker for korttrammemal-post (DFT), kortapplikasjons-post (CAT), kortoperativsystem-post (CID) og personaliseringsutstyrs-post (CPT). Den siste

5 setning er navnet til en fil som dannes ved kortutstedelses-styringssystemet 950 og som omfatter kortinnehaverdata-post(er). Kortutstedelses-styringssystemet 950 innfører kortinnehaverdata enten som en enkelt forespørsel eller som en gruppe forespørsler for kort som skal utstedes. Systemet 100 gjenfinner postene som tilsvare kjennemerkene fra databasen.

10 Systemet 100 anvender deretter informasjonen som er omfattet i kortrammemalen og dataformatmalen for å sette opp et internt «skript» som det Æ senere tolker til spesielle ordre omfattet i kortoperativsystemet og personaliseringsutstyrs-poster som instruerer pesonaliseringsutstyret for å prosesserere personaliseringsdata og utstede kortet for hver kortinnehaver.

To prøver på -kortinnehaverdata-poster 952 vises nedenfor.

Kortinnehaverdata-poster
Smith,James^12653683091245^0998^041052^mmmm
Anderson,Sue^39485003984138^0297^110248^mmmm

15 I disse poster plasserer formatet definert ved kortutstederen kontonavn (kortinnehaverens navn) i det første felt fulgt av kontonummer, utløpsdato, fødselsdato, og medisinske data.

20 Systemet 100 anvender dataformatmalen for å tolke hver kortinnehaverdata-post 952 mens den prosesseres. Systemet 100 anvender også dataformatmalen og kortapplikasjons-postene 922 for å validere dataene 952 og å sikre egnede data og format. Et eksempel på en dataformatmal som tilsvare formatet for prøve-kortinnehaver-postene vist ovenfor, vises i den første linje i tabellen nedenfor. James Smiths personaliseringsdata-posten inkluderes i tabellen for å vise overensstemmelse mellom dataformatmalen og feltene i kortinnehaverdata-posten. Dataformatmalen bringer hvert felt i kortinnehaver-posten i overensstemmelse med en intern etikett, %1, %2, osv. som tilsvare den interne rekkefølge anvendt
25 innenfor systemet 100.

Dataformatmal-post
%1 %2 %3 %4 %5
Smith,James^12653683091245^0998^041052^mmmm

Eksemplet vist ovenfor representerer det enkleste tilfelle hvor feltene i en kortinnehaverdata-post 952 er anordnet i den interne rekkefølge anvendt ved smartkort-personaliseringssystemet 100. Denne én-til-én overensstemmelse betyr at systemet 100 ikke behøver å oversette kortinnehaverdatafeltene til den interne feltrekkefølge. I et slikt tilfelle er dataformatmal-posten unødvendig. Således i en ytterligere alternativ utførelse, sender ikke kortutstederen et dataformat-kjennemerke til smartkort-personaliseringssystemet 100, men istedenfor sender den et kjennemerke, slik som et flagg, som opplyser systemet 100 om at ingen dataformatmal er nødvendig, fordi kortinnehaverdatafeltene er i en én-til-én overensstemmelse med den interne feltrekkefølge. Systemet 100 retter seg etter kjennemerket ved å gå forbi oversettelsestrinnet.

Et mer komplisert eksempel vist nedenfor, er et hvor feltene til kortinnehaverdata-posten 952 og data innenfor feltene ikke er i en rekkefølge i samsvar med den interne system-rekkefølgen. I dette tilfelle er oversettelse nødvendig.

Kortinnehaverdata i utstederformat

1234567891245 James Smith 0998 041052 mmmm

Kortholderdata oversatt til internt format

Smith,James^12653683091245^0998^041052^mmmm

15

Systemet 100 anvender dataformatmalen for å oversette datafeltene til den interne rekkefølge som vist ovenfor. Oversettelsen kan resultere i fysisk omplassering av datafeltene eller logisk omplassering hvor dataformatmalen kalles som en nøkkel hver gang et felt fra kortinnehaverdata-posten refereres ved systemet 100. Flere dataformatmaler utformet for å oversette forskjellige oppstillinger av kortinnehaverdata vil være åpenbare for en fagmann på området på samme måte som erstatningen av tabeller med feltlikninger eller med et sett spaltningsordre eller andre mekanismer for den enkelte tabell anvendt ovenfor for å illustrere dette eksempel.

25 Kortrammemal-posten beskriver strukturen til brikken på kortet. I prøven vist nedenfor, vil \$MF-posteringen definere en rotkatalog (3F00), mens \$DF-posteringen definerer en medisinsk applikasjon (5F20), og en kontoapplikasjon (5F10). Innenfor hver katalog finnes det applikasjonsspesifikke filer definert ved \$EF-posteringer, slik som 6F00 som omfatter kontonavn og 6F10 som omfatter kontonummer. Alle filbeskrivelsesdata ligger i kortrammemalen og defineres ved forskjellige tidspunkter under smartkort-utstedelsesprosessen.

30

 Korttrammemal-post

```

$CHIP=3101,MEM=8192,SIZE=N10
$SMF PATH=x3F00,TAG=ROOT,TITLE='Root Directory',SIZE=D7194
$SDF PATH=x3F005F10,TAG=ACCT,TITLE='Acct Data',SIZE=D2048
  $SDF PATH=x3F00F20,TAG=MED,TITLE='Medical',SIZE=D1024
    $SEF PATH=x3F003100,TAG=ICCID,TITLE='Issuer
      ID',FORMAT=T,SIZE=D10
      $SEF PATH=x3F005F205E00,TAG=MED1,TITLE='Medical
        profile',FORMAT=T,SIZE=D80
        $SEF PATH=x3F005F106F00,TAG=NAME,TITLE='Acct
          Name',FORMAT=T,SIZE=A30
          $SEF PATH=x3F005F106F10,TAG=ACCTID,TITLE='Account
            No.',FORMAT=T,SIZE=N14
            $SEF PATH=x3005F106F20,TAG=EXPIRE,TITLE=Expire
              Date',FORMAT=T,SIZE=N4
              $SEF PATH=x3F005F106F30,TAG=BIRTH,TITLE='Account Holder
                Birthdate',FORMAT=T,SIZE=N6
  
```

- 5 Kortapplikasjons-posten 922 avbilder kortinnehaverdataene 952 til datafeltene anvendt ved applikasjonen. Prøve-kortapplikasjons-posten 922 vist nedenfor har dens data-posteringer anordnet i sekvensen i hvilken de er prosessert ved smartkort-personaliseringssystemet 100.

 Kortapplikasjons-post

```

$VL ICCID VALUE=1234509876

$VL MEDI %5,TYPE=A

$VL NAME %1,TYPE=A

$VL ACCTID %2,TYPE=N

$VL EXPIRE %3,TYPE=N

$VL BIRTH %4,TYPE=N

$VL FM TACT %2(1-4)-%2(5-9)-%2(10-14)
  
```

5 ICCID-posteringen omfatter brikkens kjennemerke. Hver av de resterende posteringer, bortsett fra FMTACCT, avbilder en etikett til feltet i kortinnehaverens data-post 952 som omfatter informasjon (som definert i dataformatmalen vist ovenfor) og spesifiserer type data i feltet. Således representerer MED1-etiketten det femte felt i kortinnehaverdata-posten 952 og dataene er i alfabetisk format. FMTACCT-posteringen deler det andre felt i kortinnehaverdata-posten 952, dvs., kontonummer, i seksjoner og innfører bindestrek mellom delene.

10 Kortoperativsystem-posten 924 omfatter programmeringskontrollordrene som er nødvendige for å programmere brikken på kortet. Prøve-kortoperativsystem-programmeringskontrollordrene vist nedenfor er tatt fra ISO-direktiv nummer 7816-4 og er ikke de interne eiendoms-ordre av en hvilken som helst spesielt kortoperativsystem.

Kortoperativsystem-post

```
SELECT A0A4000002%F
```

```
WRITE A0D0%O%L%D
```

```
READ A0B0%O%L%D
```

```
RESET VALUE=xFF
```

15 Hver postering i eksempel-posten ovenfor omfatter en etikett fulgt av den tilsvarende ordre i kortoperativsystemets opprinnelige språk. Variable parameterfelter angis ved % fulgt av en bokstav og fylles med de egnede kortinnehaverdata når hvert enkelt kort er prosessert.

20 Personaliseringsutstyrs-posten 926 omfatter personaliseringsutstyrets karakteristiske data, slik som ordre som definerer den virkelige sekvens og trinnene som er nødvendige for å utstede et fullstendig kort på et spesifikt sett av personaliseringsutstyr. Prøveinstruksjonene anvendt i dette eksempel er fiktive og representerer ikke de interne eiendomsinstruksjoner for et hvilket som helst spesielt personaliseringsutstyr.

25

 Personaliseringsutstyrs-post

```

$EMBOSS
    #EMB#%FMTACCT%^%NAME%
$ENCODE
    #ENC#%%%ACCTID%^%NAME%
$IC
    #\@#
    @ICCID
    WRITE ICCID
    @NAME
    SELECT ACCT
    SELECT NAME
    WRITE NAME
    @ACCTID
    SELECT ACCTID
    WRITE ACCTID
    @EXPIRE
    SELECT EXPIRE
    WRITE EXPIRE
$PR
  
```

Når hvert kort utstedes, prosesseres personaliseringsutstyrets karakteristiske dataene vist ovenfor serielt i fire trinn definert ved posteringene innledet av et «\$»-tegn.

- 5 Kortapplikasjons-posten 922 anvendes for å fastsette verdien av de variable parameterfelt i hver ordre.

\$EMBOSS-ordren er en enkelt datastrøm som begynner med kontrollsekvensen #EMB# som meddeler personaliseringsutstyret at data som følger bør preges på kortet. Hvert datafelt i ordren er innesluttet i et par prosenttegn. I dette tilfellet er det første datafelt MFTACCT, eller det formaterte kontofelt som definert i 10 kortapplikasjons-posten 922. Systemet 100 søker i kortapplikasjons-posten 922 etter FMTACCT-posteringen og danner strengen «1265-36830-91245» utfra det andre datafelt i den første prøve-kortinnehaver-post 952. Neste felt, NAME, tas fra det første datafelt i kortinnehaver-posten 952. Således blir pregingsordre for den første 15 prøve-kortinnehaver 952 #EMB%1265-36830-91245%%%Smith,James%.

\$ENCODE-ordren forårsaker at systemet 100 prosesserer kortinnehaverdataene som skal kodes på magnetstripen på kortet på samme måte som pregingsordren. Ytterligere kontrolltegn i samsvar med følgende IATA (International Air Travel Association) og ISO-standarder innføres i ordren. Den resulterende ordre er 20 #ENC#%%%12653683091245%%%Smith,James%.

\$IC-ordren spesifiserer informasjonen som skal lagres i brikkens minne. Kortoperativsystem-posten 924 anvendes for å oversette instruksjonene i

personaliseringsutstyrs-posten til programmeringskontrollordre for operativsystemet. En kontrollsekvens, #@#, anvendes for å melde til personaliseringsutstyret at de data som kommer etter er brikke-data. Det første felt som skal lagres er brikkens kjennemerke, ICCID. Systemet 100 tolker WRITE (SKRIV)-etiketten i personaliseringsutstyrs-posten 926 ifølge ordre-kjennemerket med WRITE-etiketten i operativsystem-posten 924. Siden ingen avviksverdi er spesifisert i applikasjons-posten 922 for brikke-kjennemerke-posteringen, lastes standard (default) på «0000» til %O-variabel parameterfeltet. %L-variabel parameterfeltet settes til verdien til SIZE-(STØRRELSE) feltet i \$CHIP- (BRIKKE) posteringen i korttrammemalen dvs. «10» eller hexadesimal «0A». %D-variabel parameterfeltet settes til verdien av ICCID, «1234509876». Den resulterende ordre er A0D000000A1234509876.

De neste ordre forårsaker at kortoperativsystemet lagrer kortinnehaverens navn i kontonavn-filen i kontokatalogen på brikken. Systemet 100 oversetter SELECT ACCT-ordre (VELG KONTO) til den tilsvarende kortoperativsystem-ordre. Systemet 100 lokaliserer SELECT-posteringen i kortoperativsystem-posten 924, ACCT-inngangen i korttrammemal-posten, og erstatter den spesifiserte katalogbane for kontokatalogen definert i ACCT-posteringen, dvs. «5F10» for det %F-variabel parameterfelt i ordren definert i SELECT-inngangen. Den resulterende ordre er A040000025F10. På samme måte forårsaker SELECT NAME- (VELG NAVN) ordren at systemet 100 erstatter kontonavnfilen «6F00» med %F-variabel parameterfeltet. Den resulterende ordre er A040000026F00. Den siste ordre i denne serie er WRITE- (SKRIV) ordre. Systemet tolker WRITE-ordren ved å erstatte standard-avviket på «0000» med %O, verdien av SIZE-feltet, «30» eller hex «1E», som definert ved NAME-posteringen i korttrammemal-posten med %L, og kortinnehaverens navn, «Smith,James» for den første prøve-kortinnehaverdata-post 952 for %D, for å danne ordren A0D000001Smith,James~~~~~ hvor hver «~» representerer et sløfjekontroll-mellomrom innført for å fylle ut navnet med opptil tretti tegn.

Systemet 100 prosesserer de resterende ordre i personaliseringsutstyrs-posten 926 på tilsvarende måte for å tilveiebringe en kontinuerlig streng av data omfattende ordrene for å utstede et kort for den første prøve-kortinnehaverdata-post 952:

```
#\@\#A0D000000A123459876A0A40000025F10A0A40000026F
00A0D000001Esmith,James~~~~~ A040000
026F10A0A4000002E12653683091245A0A40000026F2040998.
```

\$PR-ordren forårsaker at systemet 100 sender ordredatatrømmen til personaliseringsutstyret.

De datalayout vist i fig. 11, 12 og 13 og prøvedataene drøftet sammen med det ovennevnte eksempel er bare eksempler som anvendes for å illustrere virkningen av

flere utførelser av smartkort-personaliseringssystemet 100. Innretningene og dataene er nødvendigvis definert ved omgivelsene hvor de anvendes. Dette vil være åpenbart for fagmannen på området.

- 5 Som det også vil være åpenbart for fagmannen på området, omfatter smartkort-personaliseringssystemet alternative utførelser av programvare-programmet hvor systemets funksjoner er utført ved moduler som er forskjellige fra de som vises i figurene. Systemet 100 kan prosessere data i serie eller i parallell eller en kombinasjon av de to, uten å fjerne seg fra ånden eller rammen ved oppfinnelsen.
- 10 Programvare-programmet kan være skrevet i ett eller flere av de lett tilgjengelige programmeringsspråk og modulene kan være kodet som subrutiner, subsystemer, eller objekter, avhengig av språket som velges. På samme måte er dataene anvendt ved systemet 100 beskrevet og representert som logiske poster tilveiebragt i en database, men oppfinnelsen er ikke begrenset til den beskrevne innretning av data-poster og anvendelse av en spesiell type datastyringssystem er ikke forutsatt heller.
- 15 Relasjons database-systemer fra leverandører slik som Oracle, Sybase, Informix, eller Microsoft tilveiebringer den nødvendige infrastruktur for å styre de underliggende data i systemet, enten det er sentralisert eller fordelt, men andre organisasjonsdata-strukturer, dvs., indekserte flate filer, kan erstattes uten å overskride oppfinnelsens ramme.
- 20 Ytterligere vil alternative utførelser av oppfinnelsen implementere systemet i maskinvare, fastvare, eller en kombinasjon av både maskinvare og fastvare, og også fordeling av modulene og/eller dataene på forskjellig måte vil være åpenbar for fagmannen på området og er også innenfor oppfinnelsens ramme.
- 25 Man skal forstå at den ovennevnte beskrivelse er ment å være forklarende og ikke begrensende. Mange andre utførelser vil være åpenbare for fagmannen på området ved betraktning av beskrivelsen ovenfor. Oppfinnelsesrammen vil derfor være fastsatt med henvisning til de vedlagte krav, sammen med hele utstrekningen av ekvivalenter til hvilke disse krav er berettiget.

PATENTKRAV

1. Fremgangsmåte for utstedelse av bærbare, programmerte databærere omfattende følgende trinn:
 - 5 å innhente et personaliseringsutstyr-kjennemerke og personaliseringsdata for en kortinnehaver fra et kortutsteder-styringssystem;
 - å innhente utstyrets karakteristiske data for en personaliseringsutstyr-type fra en post i en database identifisert ved personaliseringsutstyr-kjennemerket;
 - 10 å overføre personaliseringsdata til personaliseringsutstyret som spesifisert ved utstyrets karakteristiske data for den type personaliseringsutstyr som skal utstede databæreren;
 - å oversette personaliseringsdata til internt format slik at de oversatte personaliseringsdata overføres til personaliseringsutstyret;
 - 15 k a r a k t e r i s e r t v e d at personaliseringsdata oversettes fra et format definert ved kortutsteder-styringssystemet til det interne format ifølge formatmaldata.

2. Fremgangsmåte ifølge krav 1,
 - 20 k a r a k t e r i s e r t v e d at den ytterligere omfatter trinnet å innhente formatmaldata fra en post i databasen identifisert ved et dataformat-kjennemerke levert ved kortutsteder-styringssystemet.

3. Fremgangsmåte ifølge krav 1,
 - 25 k a r a k t e r i s e r t v e d at den ytterligere omfatter trinnet å innhente formatmaldata fra kortutsteder-styringssystemet.

4. Fremgangsmåte ifølge krav 1,
 - 30 k a r a k t e r i s e r t v e d at den ytterligere omfatter trinnet å innhente formatmaldata fra en applikasjonsdata-post i databasen identifisert ved et applikasjonsprogram-kjennemerke levert ved kortutsteder-styringssystemet.

5. Fremgangsmåte ifølge krav 1,
 - 35 k a r a k t e r i s e r t v e d at den ytterligere omfatter trinnene:
 - å samle informasjon vedrørende utstedelse av databærere; og
 - å rapportere statistikker avledet fra den samlede informasjon til kortutsteder-styringssystemet.

6. Fremgangsmåte ifølge krav 1,
 - k a r a k t e r i s e r t v e d at den ytterligere omfatter følgende trinn:

- å innhente et applikasjonsprogram-kjennemerke fra kortutsteder-
styringssystemet;
- å innhente applikasjonsdata fra en post i databasen identifisert ved
applikasjonsprogram-kjennemerket;
- 5 å overføre applikasjonsdata til personaliseringsutstyret som spesifisert ved
utstyrets karakteristiske data.
7. Fremgangsmåte ifølge krav 1,
k a r a k t e r i s e r t v e d at den ytterligere omfatter trinnet:
- 10 å innhente sikkerhetsdata fra en sikkerhetskilde; og
å overføre sikkerhetsdata til personaliseringsutstyret som spesifisert ved
utstyrets karakteristiske data.
8. Fremgangsmåte ifølge krav 7,
k a r a k t e r i s e r t v e d at den ytterligere omfatter trinnet:
- 15 å innhente et kortoperativsystem-kjennemerke fra kortutsteder-
styringssystemet;
- å innhente programmeringskontrollordre fra en post i databasen identifisert
ved operativsystem-kjennemerket; og
- 20 å overføre programmeringskontrollordre til personaliseringsutstyret som
spesifisert ved utstyrets karakteristiske data.
9. Fremgangsmåte ifølge krav 8,
k a r a k t e r i s e r t v e d at den ytterligere omfatter følgende trinn:
- 25 å innhente et applikasjonsprogram-kjennemerke fra kortutsteder-
styringssystemet;
- å innhente applikasjonsdata fra en post i databasen identifisert ved
applikasjonsprogram-kjennemerket; og
- å overføre applikasjonsdata til personaliseringsutstyret som spesifisert ved
- 30 utstyrets karakteristiske data.
10. System for utstedelse av bærbare programmerte databærere, omfattende:
et kortutsteder-styringssystem-grensesnitt for å innhente et
personaliseringsutstyr-kjennemerke og personaliseringsdata for en kortinnehaver fra
- 35 et kortutsteder-styringssystem;
- et personaliseringsutstyr-grensesnitt for å innhente utstyrets karakteristiske
data for en personaliseringsutstyr-type fra en post i en database identifisert ved
personaliseringsutstyr-kjennemerket; og
- et personaliseringsutstyr-grensesnitt for ytterligere å overføre
- 40 personaliseringsdataene til personaliseringsutstyret som spesifisert ved utstyrets
karakteristiske data for type personaliseringsutstyr som skal utstede databæreren;
k a r a k t e r i s e r t v e d at systemet ytterligere innhenter formatmaldata fra en

post i databasen identifisert ved et dataformat-kjennemerke levert ved kortutstederstyringssystemet og oversetter personaliseringsdata til et internt format fra et format definert ved formatmaldata slik at personaliseringsutstyr-grensesnittet overfører de oversatte personaliseringsdata til personaliseringsutstyret.

5

11. System ifølge krav 10, karakterisert ved at det ytterligere omfatter en oppfølgings-/rapportmaskin for å samle data fra systemet vedrørende utstedelse av databærere og for å rapportere de samlede data til kortutstederstyringssystemet.

10

12. System ifølge krav 10, karakterisert ved at det ytterligere omfatter:
et kortapplikasjons-grensesnitt for å innhente applikasjonsdata fra en post i databasen identifisert ved et applikasjonsprogram-kjennemerke innhentet ved kortutstederstyringssystem-grensesnittet; og
et personaliseringsstyringssystem-grensesnittet for ytterligere å overføre applikasjonsdata til personaliseringsutstyret som spesifisert ved utstyrets karakteristiske data.

15

20

13. System ifølge krav 10, karakterisert ved at det ytterligere omfatter en sikkerhetsstyring for å innhente sikkerhetsdata fra en sikkerhetskilde og å overføre sikkerhetsdata til personaliseringsutstyr-grensesnittet.

25

14. System ifølge krav 10, karakterisert ved at det ytterligere omfatter:
et kortoperativsystem-grensesnitt for å innhente programmeringskontrollordre fra en post i en database identifisert ved et kortoperativsystem-kjennemerke innhentet ved kortutstederstyringssystem-grensesnittet; og
et personaliseringsutstyr-grensesnitt for ytterligere å overføre programmeringskontrollordre til personaliseringsutstyret som spesifisert ved utstyrets karakteristiske data.

30

35

15. System ifølge krav 10, karakterisert ved at det ytterligere omfatter:
et kortapplikasjons-grensesnitt for å innhente applikasjonsdata fra en post i databasen identifisert ved et applikasjonsprogram-kjennemerke innhentet ved kortutstederstyringssystem-grensesnittet; og

40

et personaliseringsutstyr-grensesnitt for ytterligere å overføre applikasjonsdata til personaliseringsutstyret som spesifisert ved utstyrets karakteristiske data.

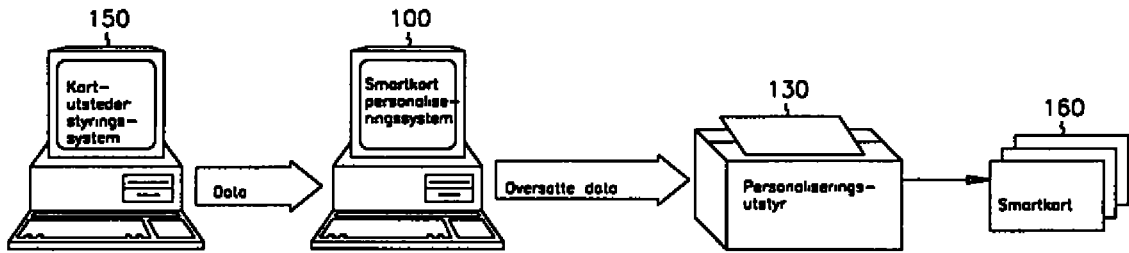


FIG 1A

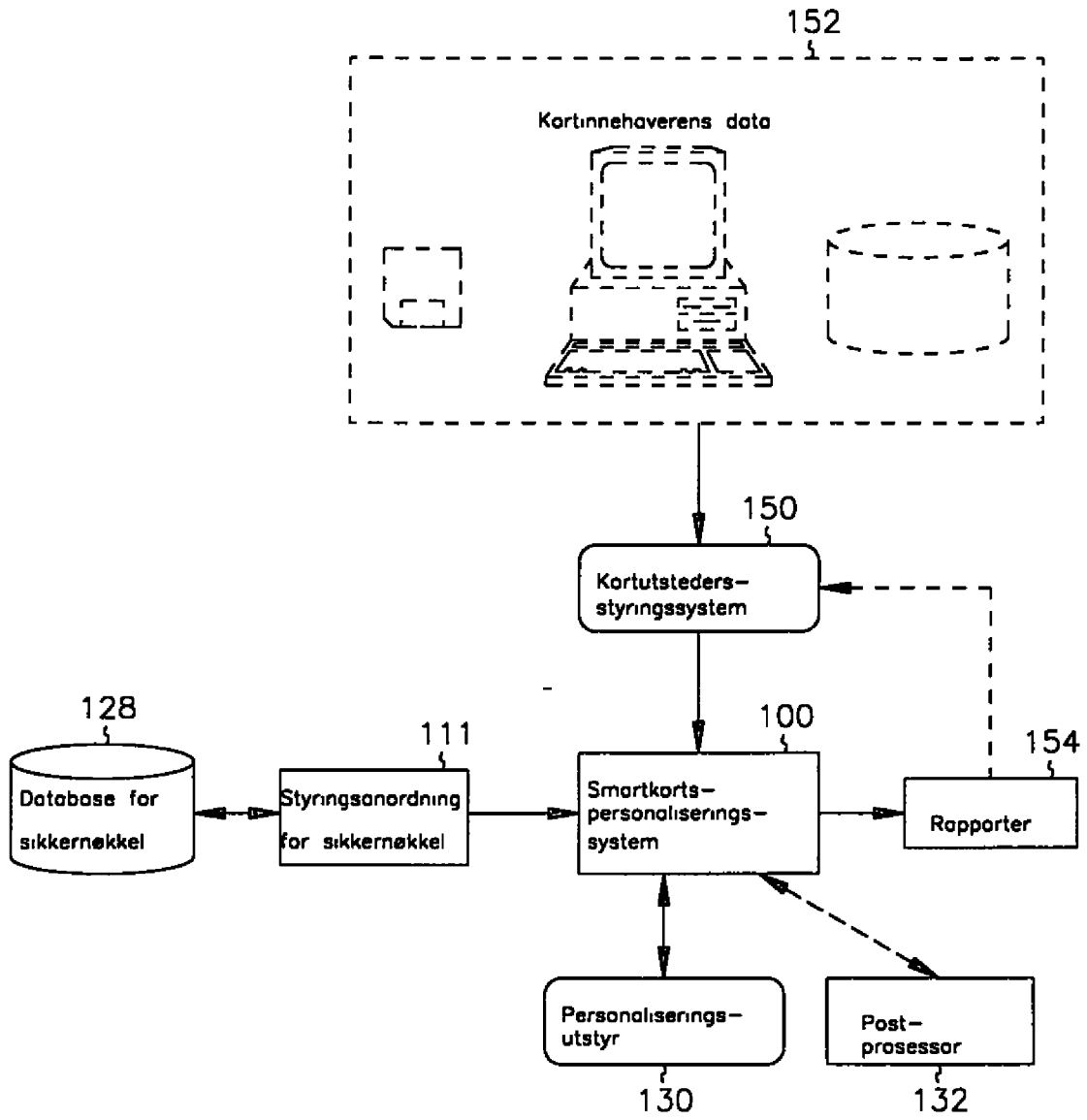


FIG 1B

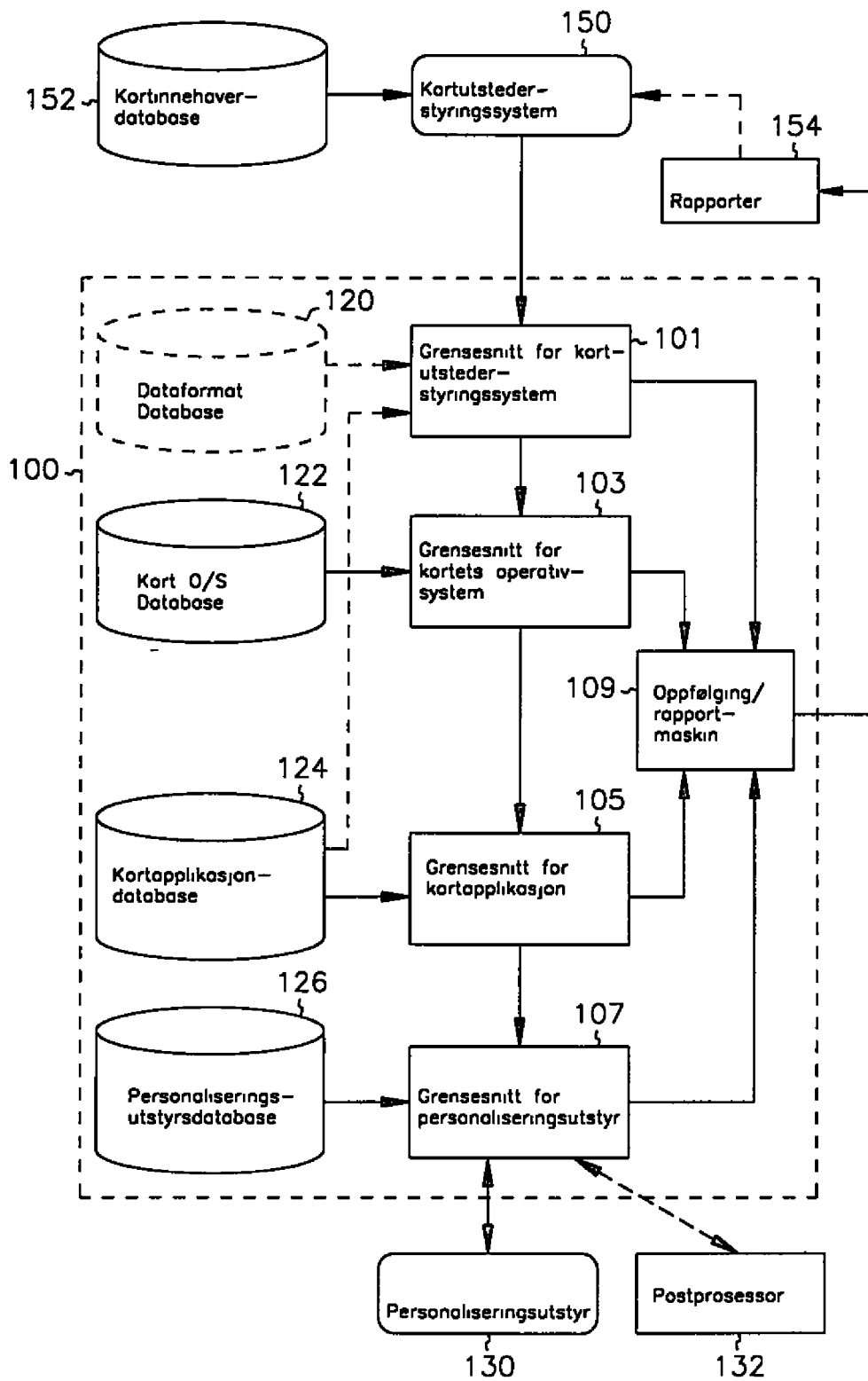


FIG 1C

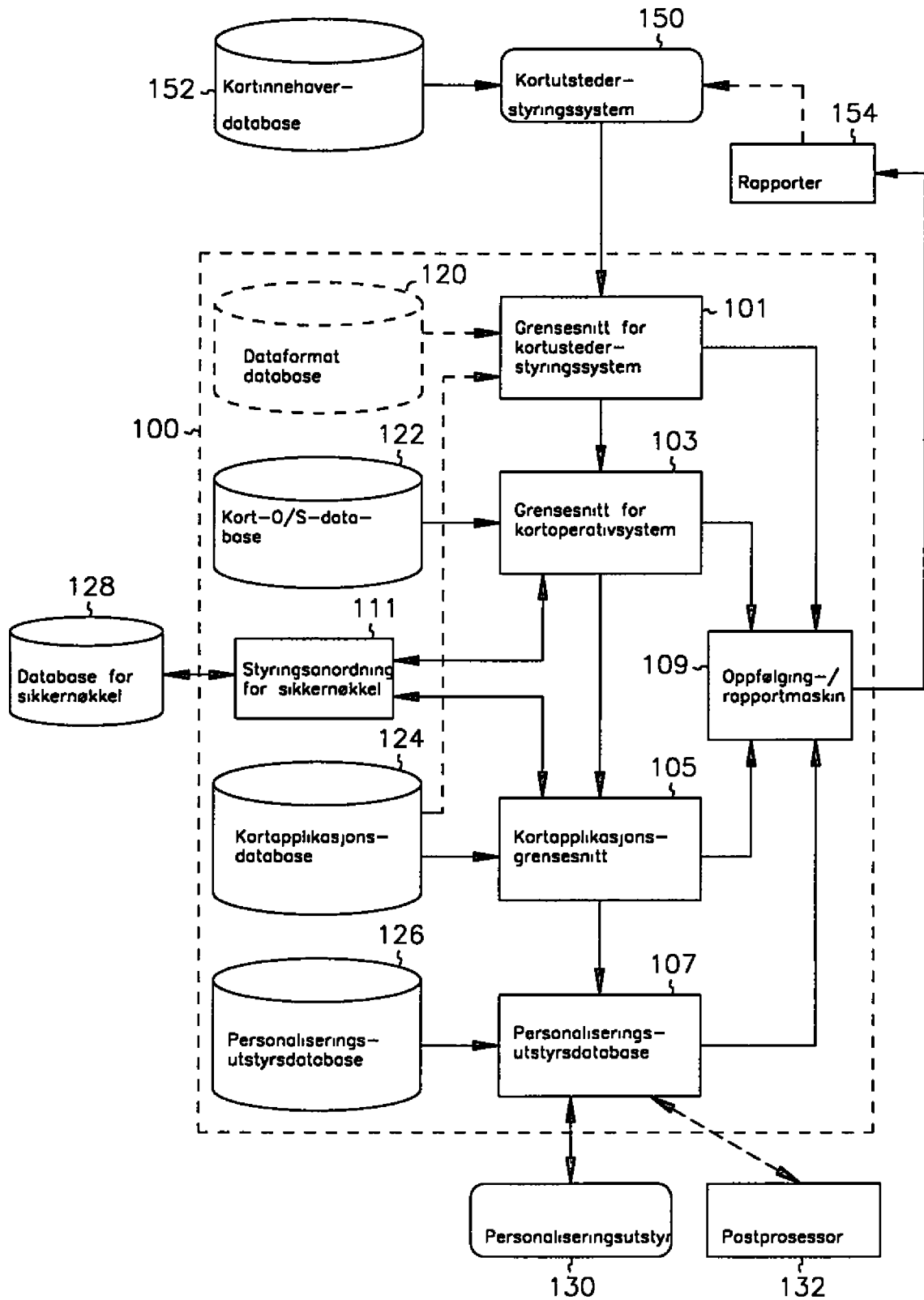


FIG 2

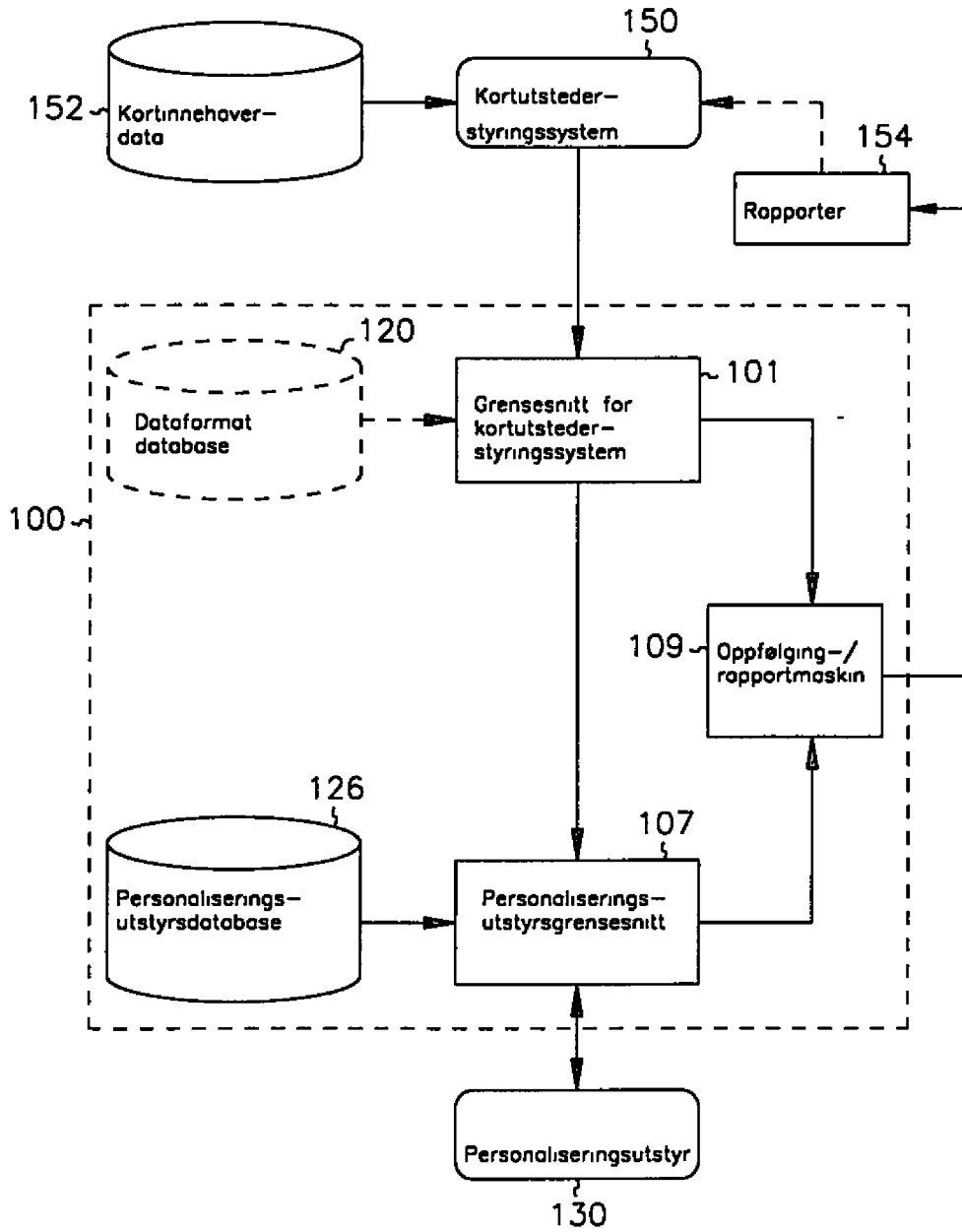


FIG 3

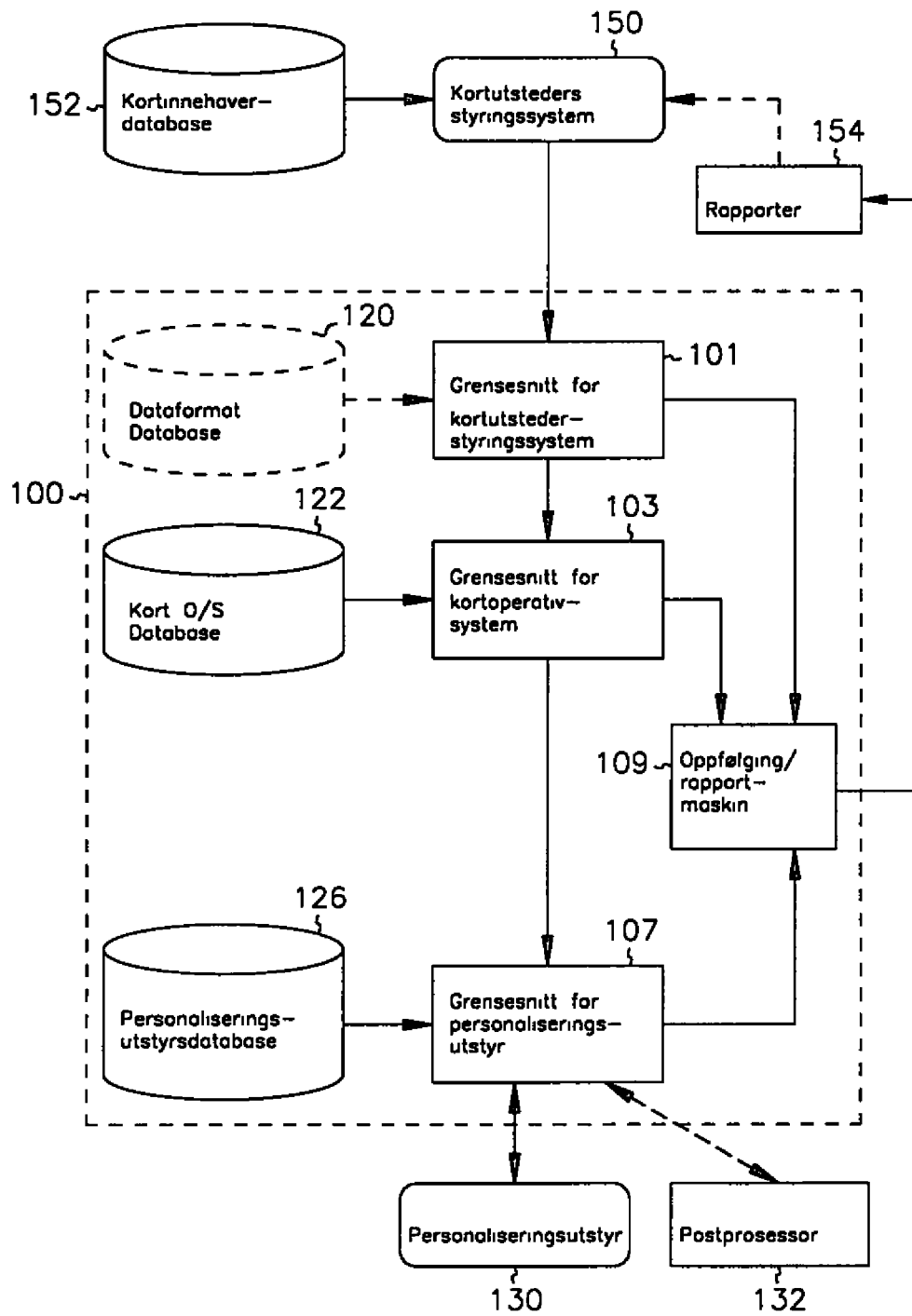


FIG 4

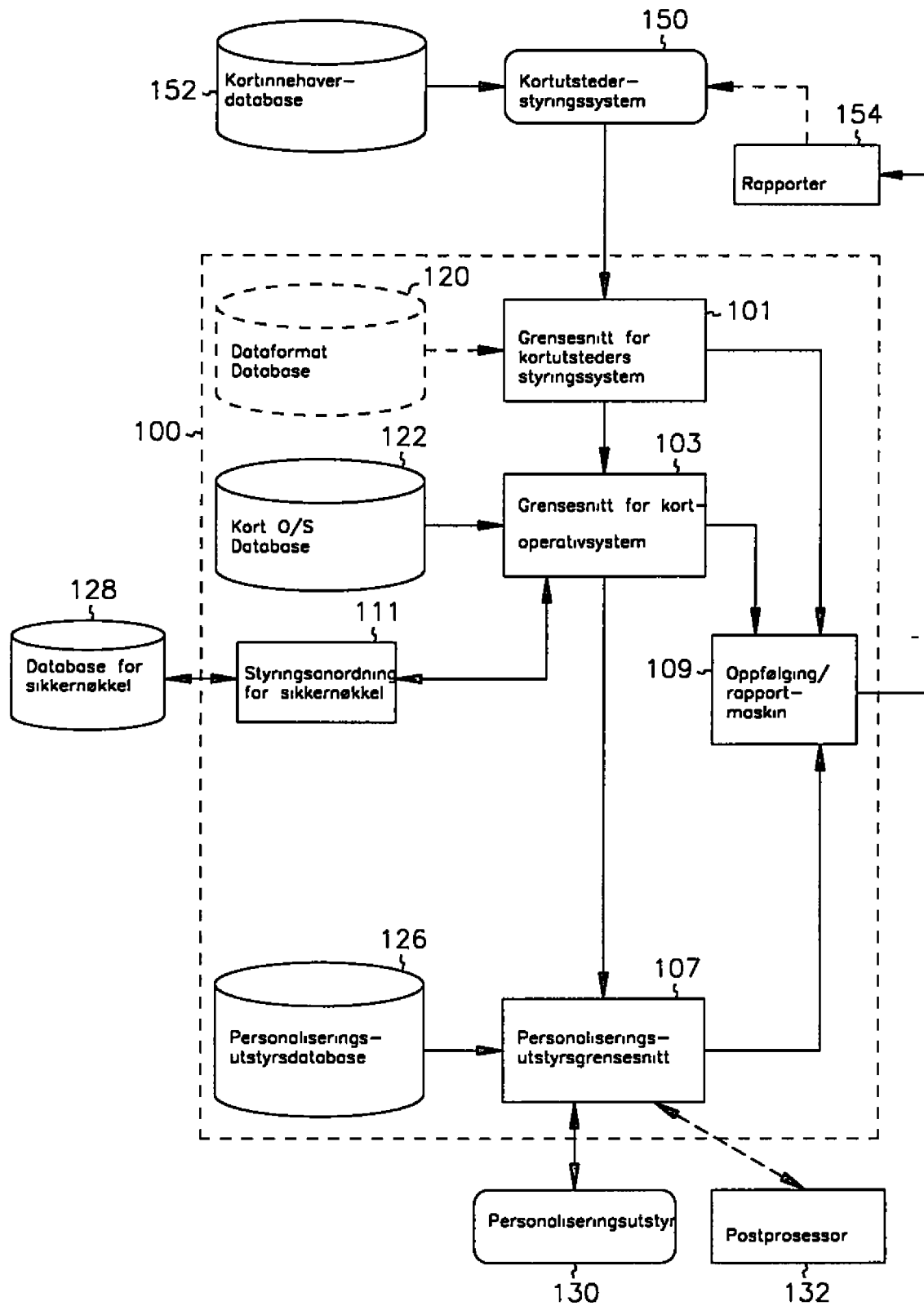


FIG 5

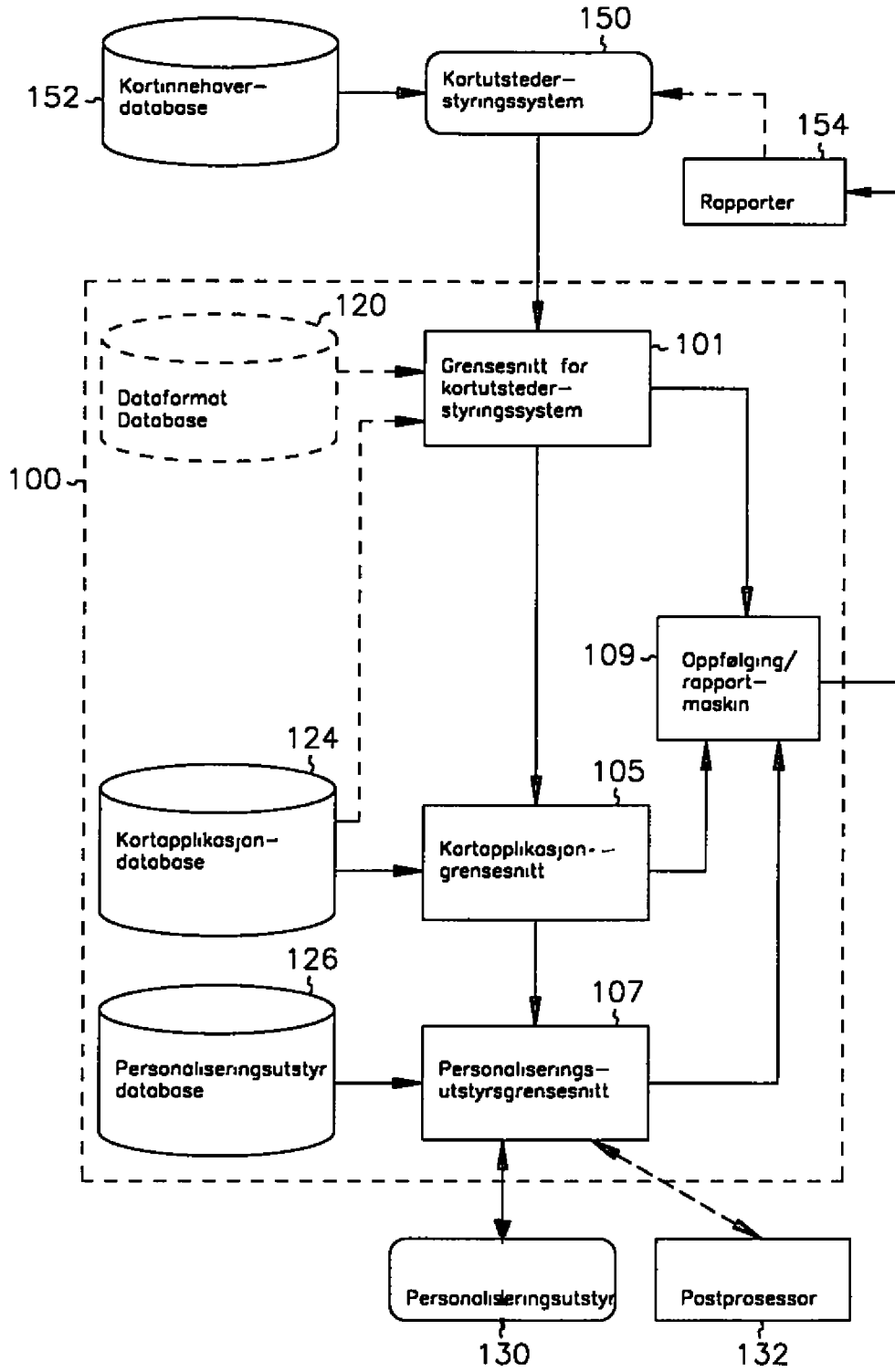


FIG 6

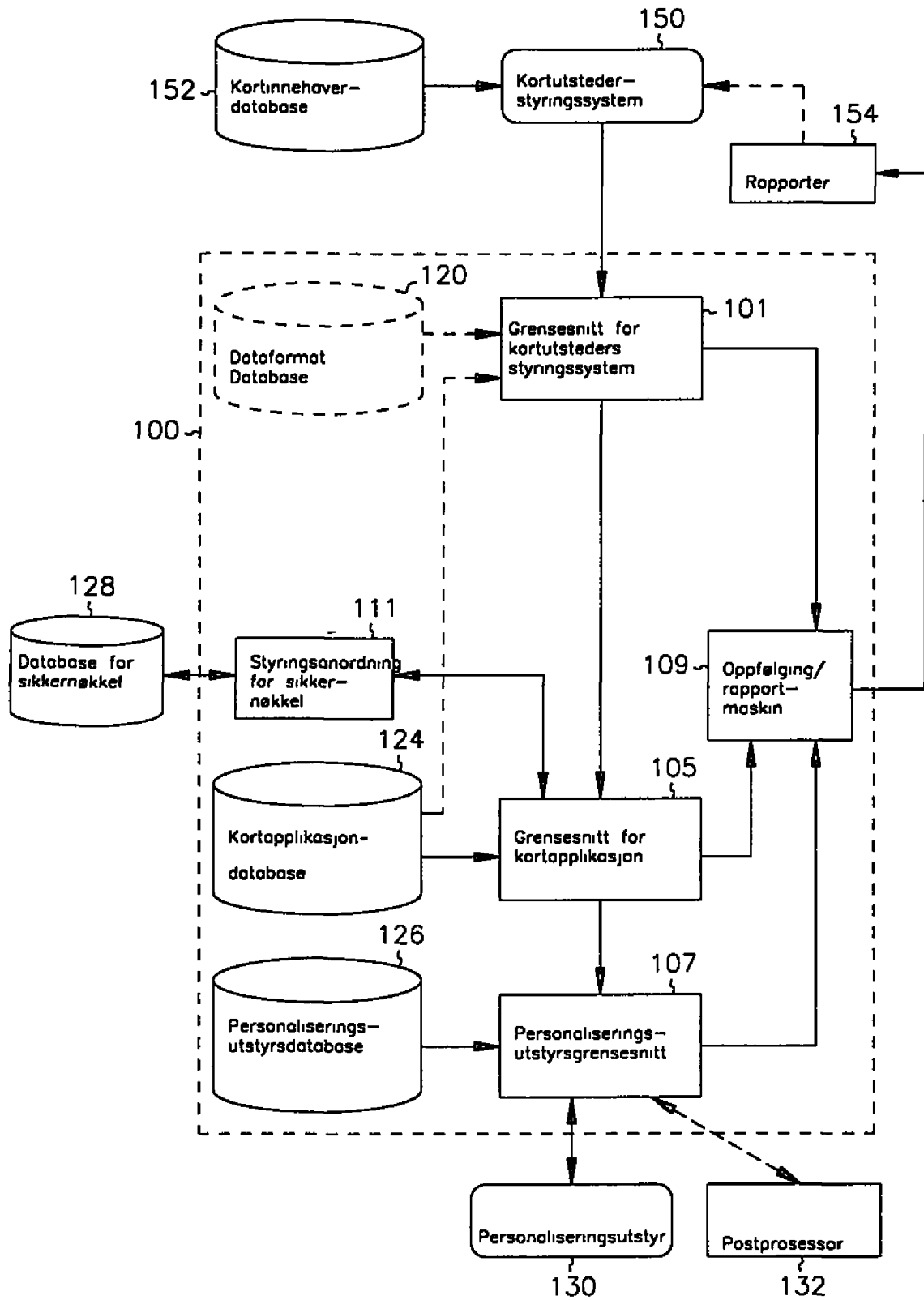
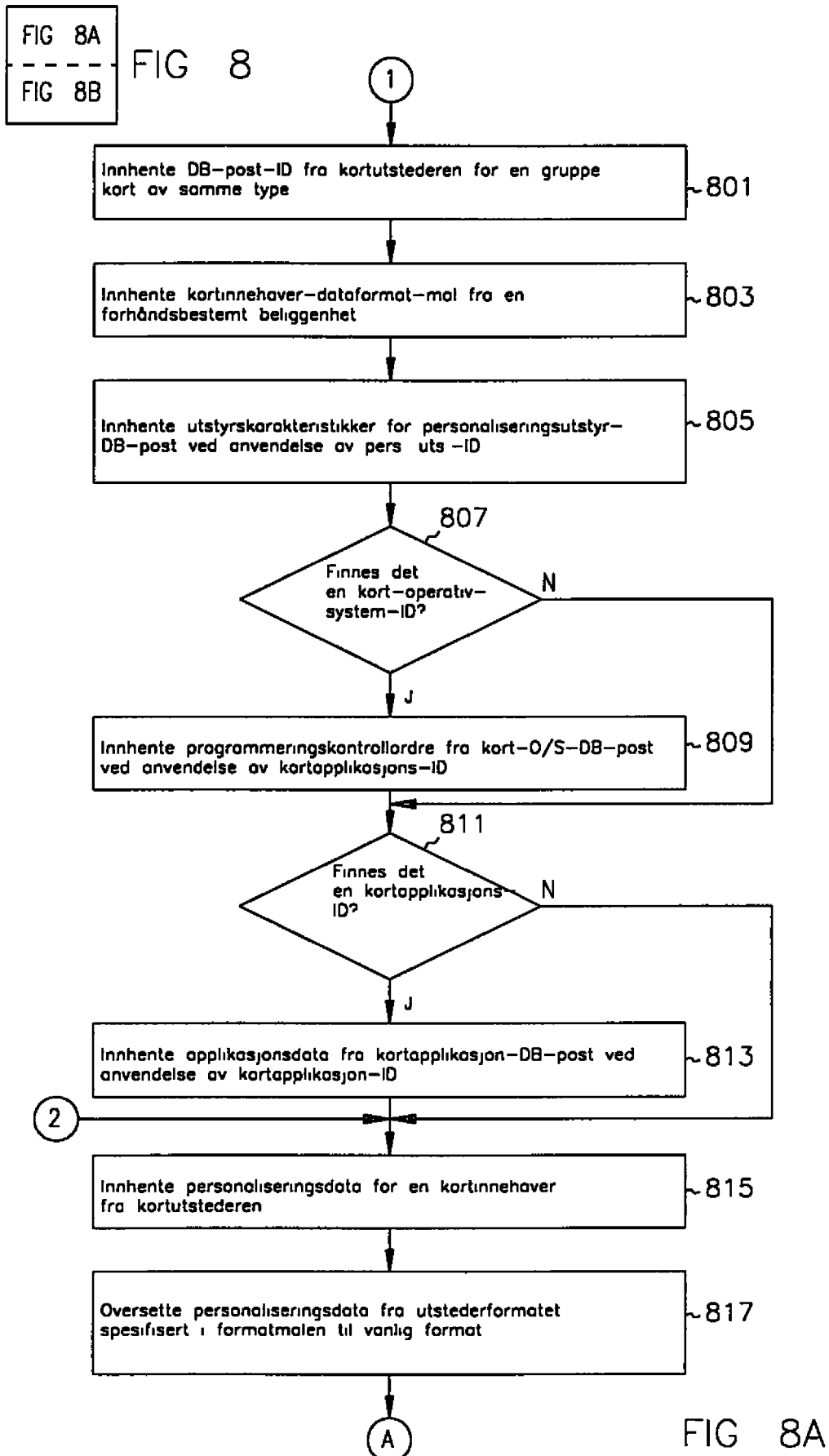


FIG 7



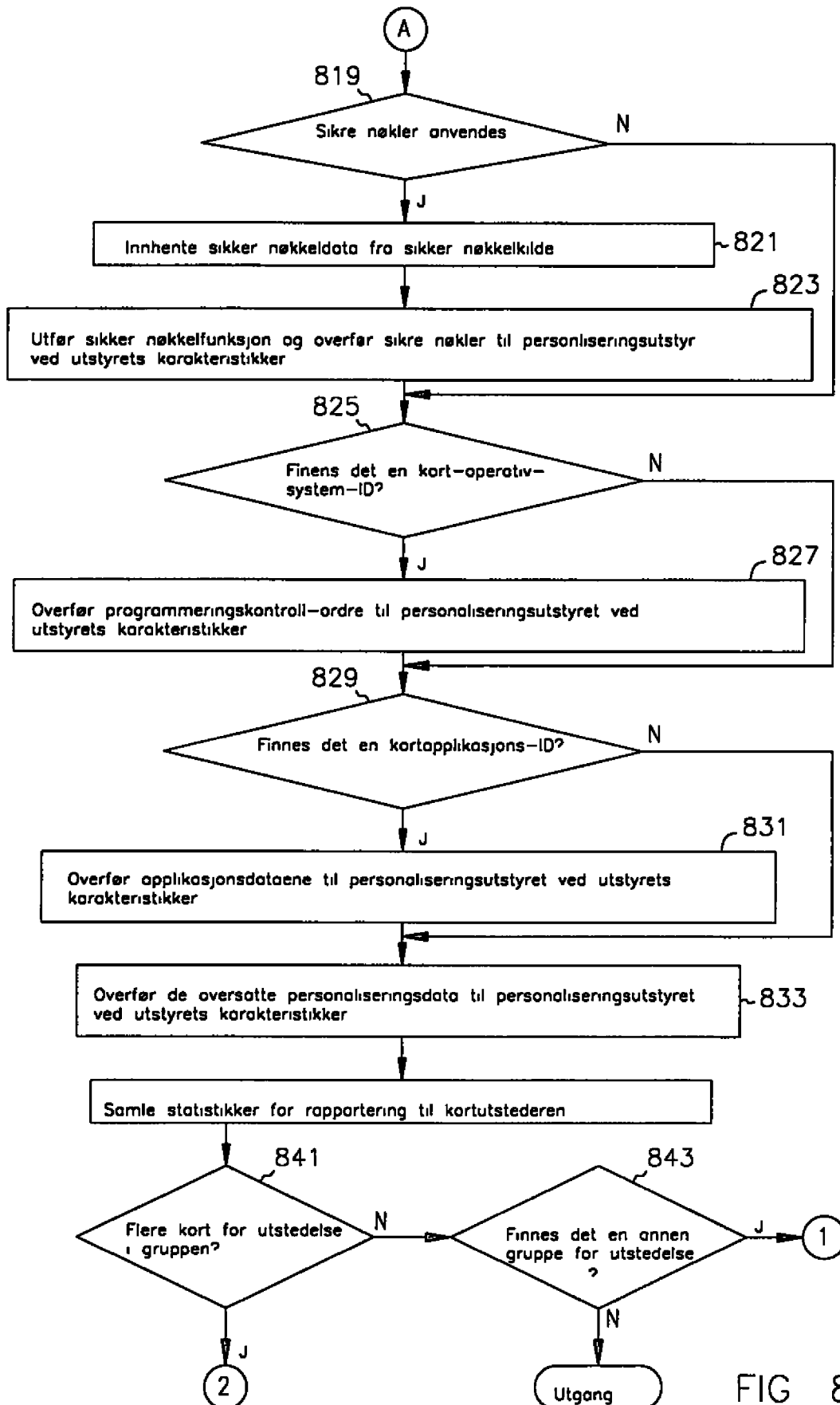


FIG 8B

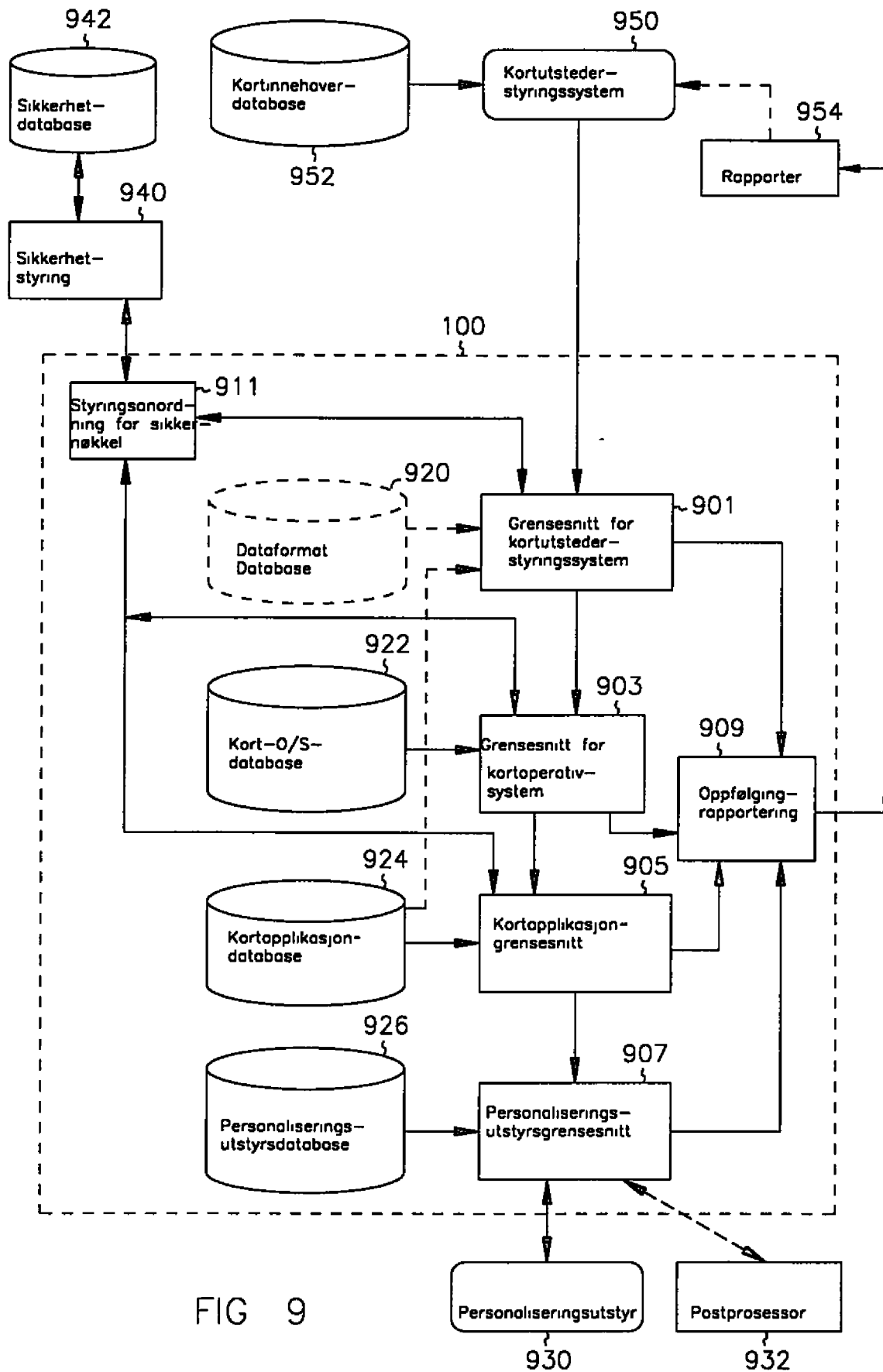
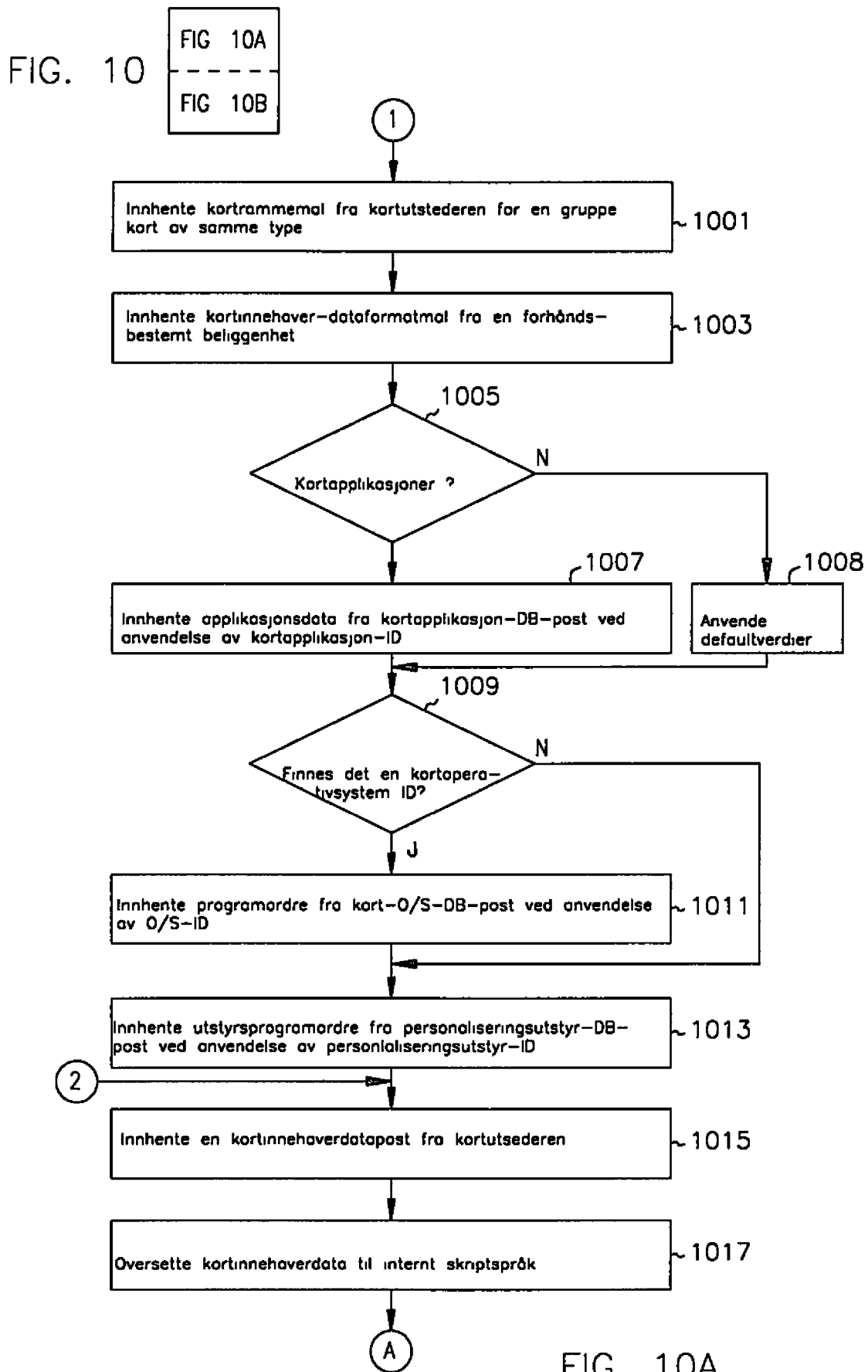


FIG 9



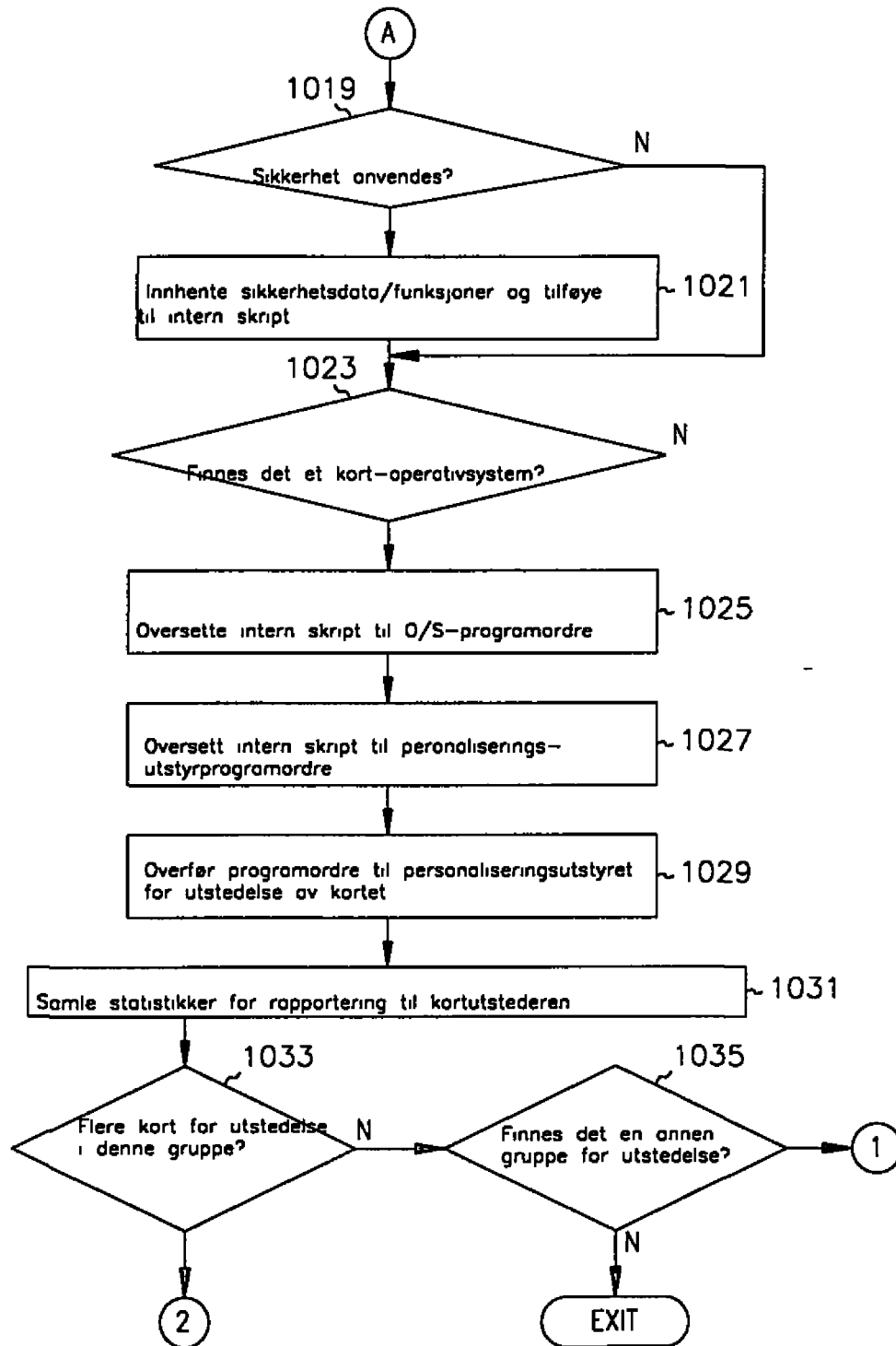
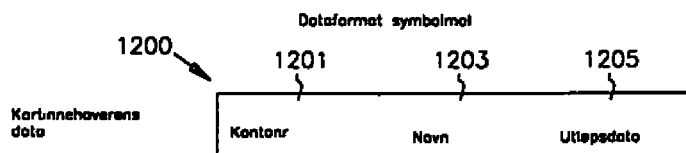
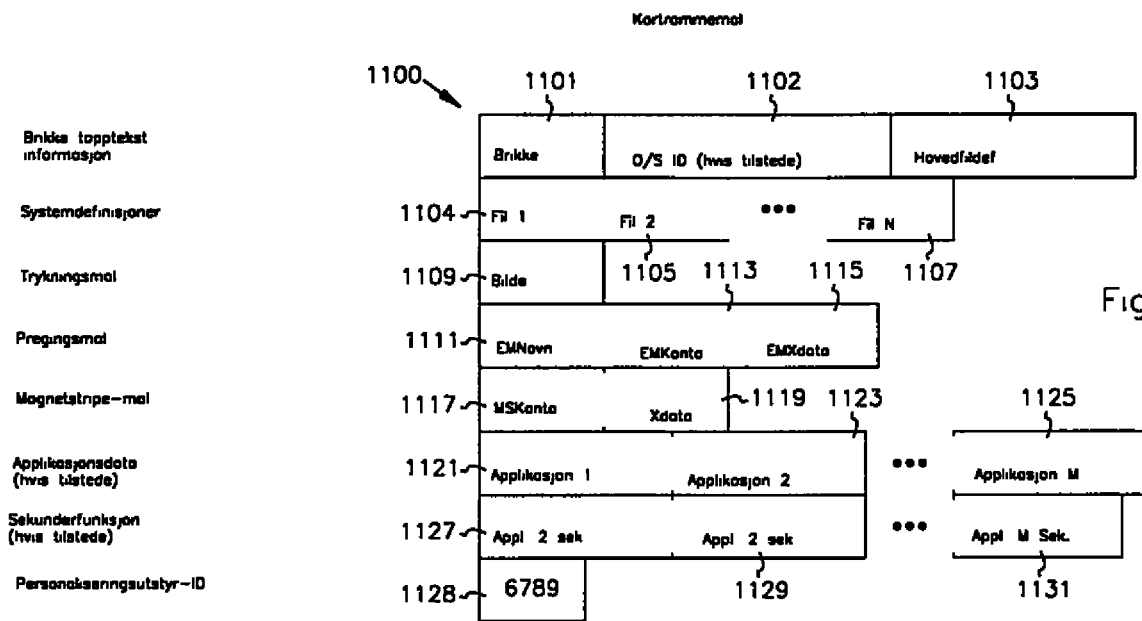


FIG 10B



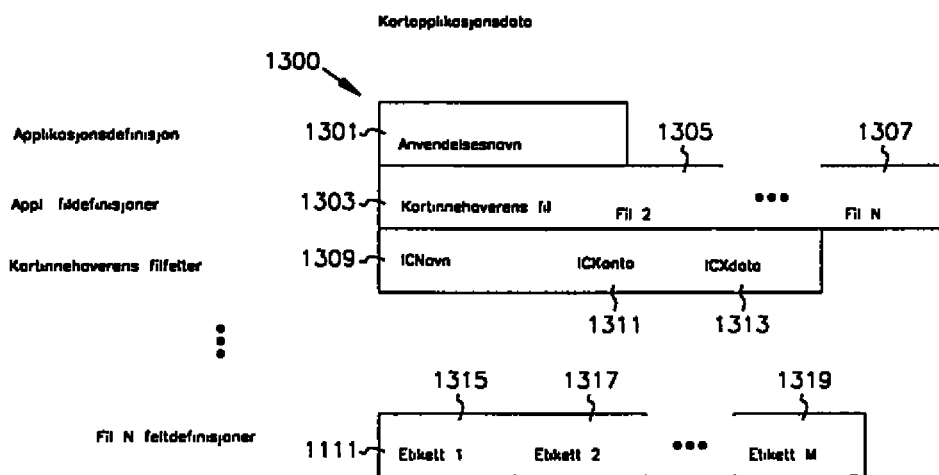


Figure 13