NORGE

(12) **PATENT**

(19) NO (11) **315490** (13) B1

(51) Int Cl[7] H 04 L 9/32

Patentstyret

(21) Søknadsnr	19941216	(86) Int. inng. dag og søknadsnummer	
(22) Inng. dag	1994.04.05		
(24) Løpedag	1994.04.05	(85) Videreføringsdag	
(41) Alm. tilgj.	1994.10.07	(30) Prioritet	1993.04.06, FR, 9304073
(45) Meddelt dato	2003.09.08		

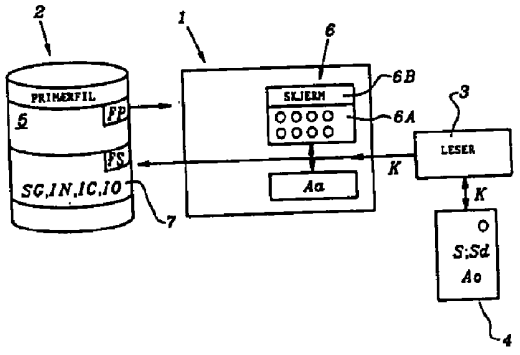
(71) Patenthaver Bull CP8, BP 45, F-78430 Louveciennes, FR
(72) Oppfinner Michel Ugon, F-78310 Maurepas, FR
(74) Fullmektig Bryn Aarflot AS, 0104 Oslo

(54) Benevnelse **Fremgangsmåte for signering av et informasjonsbehandlings-dokument, og anordning for utførelse av fremgangsmåten**

(56) Anførte publikasjoner EP 0281225

(57) Sammendrag

Oppfinnelsen vedrører en fremgangsmåte for signering av en primær informasjons-behandlingsfil (FP), av typen som består av å få kretser i en informasjons-behandlingsenhet (1, 3, 4) til å beregne minst en signatur (SG) for filen, ved å benytte minst ett hemmelig dataelement (S, Sd) spesifikk for undertegneren, men ukjent for ham, arkivert i en hemmelig minnesone i et flyttbart elektronisk objekt (4), som har et minne og behandlingskretser, og som er tilgjengelig for undertegneren, og å knytte den beregnede signaturen til den primære filen. Oppfinnelsen er også kjennetegnet ved at når hver signatur er beregnet, kan den videre bestå av å håndtere minst en del av den primære filen, slik at signaturen er en funksjon av det hemmelige dataelementet til undertegneren og av hver behandlet del av filen, og å lage en sekundærfil (FS) hvor det i hvert fall skrives informasjon (IN) som muliggjør identifikasjon av hver del av den primære filen som ble benyttet til å beregne denne signaturen, og å knytte den sekundære filen sammen med den tilhørende signaturen på den ene siden, og med den signerte filen på den andre.



Oppfinnelsen vedrører en fremgangsmåte for signering av et informasjonbehandlings-dokument, også kalt en elektronisk fil, en fremgangsmåte for signaturverifisering, og en anordning for utførelse av fremgangsmåten.

I økende grad utveksles informasjon av en hvilken som helst type mellom ulike samtalepartnere ved hjelp av informasjonsbehandlingsmidler. Dette er for eksempel tilfellet med elektronisk post, som består av å overføre dokumenter i form av digital informasjon.

Avhengig av type og/eller viktigheten til informasjonen som dokumentet inneholder kan det være nødvendig at utstederen av dokumentet, eller med andre ord dokumentets forfatter, identifiseres tilfredsstillende, eller å verifisere at en autorisert person har gitt sin godkjennelse eller validert en slik fil, og på en slik måte at den er enda sikrere med et manuskript eller maskinskrevet dokument. Faktisk kan forfatteren av et maskinskrevet dokument eller enhver person autorisert til å handle på grunnlag av et slikt dokument, kan identifiseres ved hver håndskrevne signatur påført dokumentet.

Begrepet å validere et dokument oppstår når dokumenter som signeres eller initialiseres av en eller flere personer, for eksempel for å tillate visse handlinger, blir sirkulert. Dette er tilfellet spesielt for offisielle papirer, trykte administrative eller regnskapsformularer, ett hvilket som helst dokument som gir fullmakt til en eller flere personer, eller et hvilket som helst dokument (som for eksempel kontrakter) brukt for å leie mer enn en person.

Fra et papirdokument (håndskrevet eller maskinskrevet er det relativt enkelt å finne identiteten til forfatteren eller til personer som har validert det, fordi hver signatur er påført papiret selv). Dette er ikke tilfellet med en elektronisk fil. En elektronisk fil består av en sekvens av bits som hver har logisk verdi "0" eller "1". Som en følge av dette er enhver indikasjon vedheftet en slik fil på identiteten til dens forfatter eller til personene som har validert den ikke tilstrekkelig til å bevise at filen, i den formen den foreliggende ved et gitt øyeblikk, er i samme tilstand som den var da disse personene signerte eller validerte dem.

Dette er årsaken til at konseptet med elektronisk signering av slike filer har oppstått. Dette gjøres ved å benytte behandlingskretsene til å beregne en elektronisk signatur for hver undertegner som er en funksjon av innholdet i filen, og av minst en parameter som er spesifikk for en undertegner eller en gruppe av undertegnere, og knytte hver signatur beregnet på denne måten til filen. Verifisering av identiteten til en undertegner består av å benytte behandlingskretsene til å rekalkulere signaturen, og å sammenligne denne rekalkulerte signaturen med den tilknyttede signaturen.

En mulig bedrager, d.v.s. en person som ikke er autorisert til å signere kan ikke modifisere en fil og knytte en koherent signatur med den, fordi han ikke har kontroll med parameteren eller parametrene som er spesifikk for den originale undertegneren eller undertegnerne. Ved sirkulasjon av dokumenter som skal signeres av mer enn en person, betyr tilsvarende enhver modifikasjon av filen etter at minst en person allerede har signert den at det er umulig å erstatte hver allerede beregnede signatur med en koherent signatur.

En slik fremgangsmåte for å beregne og verifisere signaturer er beskrevet i fransk patent 2 514 593, som svarer til US-patent 4 656 474 og til europeisk patentnummer 077238.

Denne fremgangsmåten består i å utstyre hver potensiell undertegner med et flyttbart objekt, så som et mikroprosessorkort (også kalt smartkort), hvis minne inneholder en hemmelig nøkkel som kun er tilgjengelig for behandlingskretsene i objektet. Den hemmelige nøkkelen er diversifisert. D.v.s. at den er forskjellig fra ett objekt til et annet, slik at to ulike objekter ikke kan signere den samme meldingen på samme måte.

Signatursteget består i seg selv av å kople objektet til en informasjonsbehandlingsanordning (som kan være anordningen hvor filen behandles), og/eller fra hvilken anordning den blir sendt til en annen anordning, og signere filen ved å forårsake at beregningsalgoritmer kjøres i anordningen og i objektet, slik at signaturen er en funksjon av den hemmelige nøkkelen og av innholdet i filen.

For å unngå at den hemmelige nøkkelen blir kjent utenfor objektet, blir enten signaturen beregnet i sin helhet inne i objektet av dettes behandlingskretser, eller et delresultat blir beregnet av objektet og overført til kretsene i behandlingsanordningen, som fullfører beregningen. Eventuelt kan behandlingsanordningen begynne beregningen, for eksempel ved å benytte en datakompresjonsalgoritme, og objektet beregner selve signaturen. Etter at signaturen er beregnet blir den overført med filen sammen med et dataelement forbundet med undertegnerens identitet.

Verifisering består av å rekalkulere signaturen til en fil, uten å røpe den, ved å benytte behandlingskretsen i en passende anordning, og deretter sammenligne denne rekalkulerte signaturen med den som ble tilknyttet filen, og endelig indikere kun resultatet av sammenligningen (d.v.s. om signaturene stemmer overens eller ikke). Rekalkulasjonen er mulig fordi behandlingskretsene i verifiseringsanordningen inneholder en algoritme som setter dem i stand til først å rekalkulere, uten å røpe, undertegnerens diversifiserte hemmelige nøkkel fra det

dataelementet forbundet med hans identitet som blir overført sammen med filen, og deretter fra denne rekalkulerte nøkkel å rekalkulere signaturen. Den rekalkulerte nøkkel blir ikke røpet utenfor kretsene i verifiseringsanordningen, slik at nøkkelens hemmelige natur blir bevart. Den rekalkulerte signaturen blir ikke røpet for å hindre en person som ønsker å forfalske dokumentet og som observerer verifiseringsoperasjonene, i å forsøke å benytte resultatene av rekalkulasjonen for sine egne formål.

Imidlertid er det en særlig ulempe ved de kjente fremgangsmåtene for signering at de krever behandling av hele filen ved kalkulasjon og verifisering av en signatur. Dette kan være upraktisk av flere årsaker.

En første årsak, som er viktig når filen må signeres av en enkelt person eller av mer enn en person uten at noen av dem har gjort noen endringer, er at dersom filen er svært lang, så kan prosessen med å kalkulere og verifisere signaturen ta en viss tid, hvilket er i konflikt med målene for informasjonsbehandling.

En fil inneholder både informasjon som kan kalles sensitiv, og annen informasjon som ikke er det. Den sensitive informasjonen er den som vedrører grunnlagsdata. Dette kan omfatte numeriske verdier når filen er en regnskapsfil, eller bestemte avsnitt i en rapport eller et brev. Den ikke-sensitive informasjonen er den som vedrører format. Dette omfatter for eksempel ledetekst eller noter som når de er til stede øker lesbarheten i filen uten å endre grunnlagsdata, og som det følgelig er uviktig å beholde eller å beholde uendret.

En andre årsak er når mer enn en person skal signere filen, mens de er autorisert til å endre visse soner av den, eller å legge til informasjon. Med de kjente fremgangsmåtene kan i dette tilfellet kun signaturen til den siste undertegneren kalles autentisk, siden hver endring av eller tillegg til filen betyr at parametrene som ble benyttet til å beregne de foregående signaturene er endret.

På den annen side oppviser publikasjonen EP-A-0 281 225 en fremgangsmåte for å gi adressaten for en melding tillatelse til å verifisere at meldingens innhold ikke er forandret ved en overføring, ved hjelp av tidligere kryptering av blokker i meldingen for å frembringe meldings-autentiseringskoder (MAC) som i seg selv er tidligere kjente.

Et første formål med oppfinnelsen er å gjøre det mulig å redusere mengden av tid som er nødvendig for å beregne og verifisere signaturen, sammenlignet med fremgangsmåtene ifølge tidligere kjent teknikk.

Et andre formål med oppfinnelsen er å gjøre det mulig at den samme filen signeres av mer enn en person selv om den muligens kan ha blitt endret eller fått tillegg etter at en første undertegner har validert den.

Disse målene nås ved den foreliggende oppfinnelsen, som foreslår en fremgangsmåte for signatur av en primær informasjonsbehandlingsfil, av den typen som består av å forårsake at kretser i en informasjonsbehandlingsanordning beregner minst en signatur for filen, ved å behandle minst ett hemmelig dataelement spesifikt for undertegneren, men ukjent for ham, hvilket dataelement er lagret i en hemmelig minnesone i et flyttbart elektronisk objekt med minnet og behandlingskretser, som er tilgjengelig for undertegneren, og å lenke den beregnede signaturen til den primære filen, som er karakterisert ved at når hver signatur blir beregnet, består den videre av å behandlet minst en del av den primære filen, slik at signaturen er en funksjon av undertegnerens hemmelige dataelement, og av hver behandlet del av filen, og lage en sekundærfil hvor det i hvert fall skrives informasjon som muliggjør identifikasjon av hver del av den primære filen som ble benyttet til å kalkulere denne signaturen, og å lenke den sekundære filen med den korresponderende signaturen på den ene side, og med den signerte filen på den andre.

Et annet trekk ved den foreliggende oppfinnelsen er at for å lenke den sekundære filen til den korresponderende signaturen, blir denne signaturen skrevet inn i den sekundære filen.

Et annet trekk ved den foreliggende oppfinnelsen er at det hemmelige dataelementet til hver undertegner er lagret i en hemmelig minnesone i et flyttbart elektronisk objekt, med minne og behandlingskretser, som er tilgjengelig for undertegneren.

Et annet trekk ved den foreliggende oppfinnelse er at dataelementet som er spesifikt for en undertegner er diversifisert, slik at to ulike undertegnere ikke kan signere samme filen på samme måte. Dette trekket gjør det mulig å identifisere hver undertegner, for eksempel gjenfinne navnet hans ved å benytte fremgangsmåtene beskrevet i de ovennevnte patentene. Det er imidlertid mulig å benytte et felles dataelement, d.v.s. ett som er felles for flere enn en undertegner, når man ønsker å verifisere at filen er signert av en autorisert person, uten å vite eksakt hvem det er.

En fremgangsmåte for å verifisere en forhåndsbestemt signatur i en fil beregnet ifølge den foreliggende oppfinnelsen er karakterisert ved at den består av å identifisere, ved hjelp av den sekundære filen, hver del av den signerte filen som ble benyttet til å oppnå den aktuelle signaturen; benytte behandlingskretsene til å rekalkulere signaturen ved å behandle parametere som antas å svare til den benyttet i den opprinnelige kalkulasjonen; sammenligne den rekalkulerte signaturen med den lenkede signaturen; og indikere resultatet av sammenligningen.

Oppfinnelsen er særlig fordelaktig fordi den bevarer sikkerheten ved de tidligere kjente fremgangsmåtene samtidig som den har større fleksibilitet og flere fordeler.

Spesielt gjelder det at så snart en undertegner velger å signere hele filen, fordi han antar at hele innholdet består av sensitiv informasjon, så vil informasjonen i den sekundære filen lenket til den korresponderende signaturen indikere at denne signaturen ble beregnet ved å benytte hele filen. Hvis en senere undertegner i dette tilfellet endrer filen, blir den foregående signaturen inkoherent. Omvendt kan han enten signere den i sin tur, helt eller delvis, eller legge til informasjon og deretter beregne sin egen signatur basert på all eller noe av informasjonen som er lag til og/eller all eller noe av informasjonen som filen inneholdt før han gjorde tilføyelsen.

Beregningen av hver ny signatur fører dermed til at det dannes en ny sekundær fil eller en ny tilføyelse i den sekundære filen hvor denne nye signaturen blir skrevet, sammen med informasjonen som gjorde det mulig å beregne den.

En annen fordel ved fremgangsmåten et at den setter en person, som må validere en fil etter at den er signert av forfatteren, i stand til å godkjenne kun visse deler av innholdet. For å gjøre dette kan personen som skal validere filen velge å behandle kun de delene av filen han er enig i når han skal beregne sin egen signatur.

Ytterligere karakteristika og fordeler ved oppfinnelsen vil tre klarere frem fra den følgende beskrivelsen, sammen med de vedføyde tegningene, hvor:

Fig. 1 viser den grunnleggende oppbygningen av et foretrukket system for å virkeliggjøre oppfinnelsen;

Fig. 2 -7 viser et foretrukket arrangement for hver av skjermbildene for dialog mellom brukerne og systemet i løpet av fasene for signatur og/eller verifisering.

I figur 1 vises den grunnleggende oppbygningen til en foretrukket anordning for å virkeliggjøre oppfinnelsen. Det viste systemet kan benyttes for både behandling og/eller verifisering av signaturer.

Anordningen omfatter en informasjonsbehandlingsenhet 1, så som en datamaskin, som er i stand til å behandle informasjonsbehandlingsdokumenter. Enheten omfatter på kjent måte midler 2 for masselagring av data eller dokumenter/filer. Disse midlene kan være magnetiske disketter, optiske disker, eller enhver tenkelig lagringsenhet.

I den foretrukne utførelsesformen er enheten videre forbundet med en leser 3 for et elektronisk objekt 4 som kan fjernes eller flyttes, også kjent som et utbyttbart elektronisk medium, så som et mikroprosessorkort, som på kjent måte omfatter behandlingskretser og en hemmelig minnesone hvor det er lagret data som er

tilgjengelig kun for behandlingskretsene. Den hemmelige minnesonen inneholder minst ett hemmelig dataelement Sd, som er diversifisert i hvert kort, eller med andre ord er forskjellig fra ett kort til et annet. Dette gjør det mulig å utføre den samme beregningsalgoritmen (kryptering, signatur, o.s.v.) i begge kort, og ved å behandle samme inngangsdata tilført begge kortene og det diversifiserte dataelementet i hvert kort får forskjellige resultater fra ett kort til et annet. Enheten og objektet utgjør følgelig til sammen signatur- eller verifiserings-anordningen.

I en variant inneholder den hemmelige minnesonen i det utbyttbare elektroniske mediet 4 ikke et diversifisert dataelement, men kun et hemmelig dataelement S, som er identisk i alle kortene beregnet til en bestemt anvendelse, eller som er identisk for alle kortene beregnet til bruk i en bestemt anvendelse som er utdelt til personer med identiske tilgangsrettigheter til denne anvendelsen. Diversifisering er faktisk kun nødvendig når det må være mulig å skille mellom alle eller noen av brukerne.

For den samme anvendelsen kan det hemmelige dataelementet altså være felles for potensielle undertegnere som har den samme hierarkiske rang, eller med andre ord samme myndighet til å signere eller de samme tilgangsrettighetene. Omvendt eksisterer diversifisering mellom ulike hierarkiske nivåer. Denne utførelsen er tilstrekkelig ved sirkulasjon av dokumenter og alt som er nødvendig er enkel verifikasjon av at en fil er blitt signert av personer på ulike hierarkiske nivå, uten å bestemme deres identitet presis. Det er også mulig at alle potensielle undertegnere, uavhengig av deres rang, kan ha et identisk hemmelig dataelement. I dette tilfellet kan man ganske enkelt verifisere at filen er signert av en autorisert person.

Det er underforstått ønskelig at data diversifiseres mellom ulike informasjonsbehandlingsanvendelser.

Enheten 1 omfatter behandlingskretser i stand til å utføre beregningsalgoritmer, særlig en algoritme Aa for signering av minst deler av en primær fil FP inneholdt i en del 5 av dens masselager 2. På utførelsestidspunktet er algoritmen Aa for eksempel lagret i en hurtigminnesone (RAM) i enheten 1.

Videre omfatter enheten midler 6 for grensesnitt mot og dialog med brukere, nærmere bestemt et tastatur 6A og en skjerm 6B. Enheten kan omfatte andre, ikke viste, midler, så som en mus, en talegjenkjenningsenhet, o.s.v.

Rollen til det utbyttbare elektroniske mediet 4 er å tilveiebringe en nøkkel K, som er en funksjon av det hemmelige dataelementet, d.v.s. enten det diversifiserte hemmelige dataelementet Sd eller det ikke-diversifiserte hemmelige dataelementet S som objektets minne inneholder til enheten 1 ved hjelp av leseren 3. Måten denne nøkkelen K utvikles på, vil bli forklart id et følgende.

Når signaturalgoritmen Aa utføres, blir nøkkelen K behandlet av behandlingskretsene i enheten, slik at signaturen SG vil være en funksjon av denne nøkkelen K, og av i hvert fall deler av den primære filen P.

Som det vil gå frem av det følgende, velges delen eller delene av den primære filen som skal behandles for å beregne signaturen enten av undertegneren eller automatisk av systemet.

For å muliggjøre verifisering av signaturen SG fører ifølge den foreliggende oppfinnelsen beregning av hver signatur til at det blir dannet en ny sekundær fil FS, eller av en tilføyelse i den sekundære filen som ikke bare inneholder denne signaturen SG, men også parametere eller informasjon som gjør det mulig å identifisere data som blir brukt til å beregne den. Denne sekundære filen FS lages av enheten 1, og blir deretter skrevet til en del 7 av enhetens masselager 2.

Mer spesielt inneholder den sekundære filen FS blant annet informasjon IN som gjør det mulig å gjenskape delene av den primære filen FP som blir benyttet til å beregne signaturen. Dette kan være informasjon forbundet med minneadressene til disse delene, eller enhver informasjon som gjør det mulig å rekonstruere disse delene i den primære filen.

I tillegg til denne informasjonen IN som muliggjør rekonstruksjon av deler av den primære filen FP som blir benyttet til å beregne signaturen, kan den sekundære filen FS også inneholde tilleggsinformasjon IC.

For det første er det tenkelig at algoritmen Aa for beregning av signatur er forskjellig fra en enhet til en annen. Som nevnt ovenfor, må den samme enheten kunne benyttes like godt til å beregne som til å verifiserer signaturer. På et gitt tidspunkt, for eksempel på grunn av programvareutvikling, kan det hende at enheten som blir benyttet til å beregne signaturen benyttet en eldre programvareversjon enn det enheten benyttet til verifisering ville benyttet dersom den skulle signere nor. Uavhengig av programvareversjonen, kan det hende at de to enhetene benyttet fullstendig ulik programvare for beregningen. I tilfelle med flere undertegnede kan det også hende at signaturene i samme fil er beregnet på ulike enheter med ulike programvarer. Med andre ord kan ulike anordninger benyttes til å beregne signaturene.

Av denne grunn omfatter tilleggsinformasjonen IC i den sekundære filen FS i dette tilfellet data som muliggjør identifikasjon av anordningen, eller med andre ord enheten og/eller algoritmen, som faktisk ble benyttet ved beregning av signaturen.

Som nevnt, blir nøkkelen K beregnet av det flyttbare objektet 4, på bakgrunn av det diversifiserte hemmelige dataelementet Sd eller ikke-diversifiserte hemmelige dataelementet S som objektet inneholder. Et objekt som inneholder et diversifisert

hemmelig dataelement Sd må benyttes hver gang det er nødvendig å identifisere undertegneren entydig. Omvendt er det ikke nødvendig å diversifisere det hemmelige dataelementet når det kun er nødvendig å verifisere at undertegneren er en autorisert person, som tilhører en begrenset gruppe. I dette tilfellet er det tilstrekkelig at det hemmelige dataelementet er felles for alle personene i denne gruppen. Disse prinsippene er kjent fra tidligere kjente fremgangsmåter for signering.

Beregning av nøkkelen K består av å uføre en algoritme Ao i objektet, hvilken algoritme er lagret i objektets behandlingskretser, og hvilken algoritme betjener på den ene siden det diversifiserte hemmelige dataelementet Sd eller ikke-diversifiserte hemmelige dataelementet S inneholdt i objektets minne, og på den andre siden et eksternt dataelement E laget i enheten og deretter overført fra enheten til objektet, på en slik måte at nøkkelen K er en funksjon av både det hemmelige dataelementet Sd eller S, og det eksterne dataelementet E.

Når det hemmelige dataelementet i objektet er diversifisert, må enheten som skal benyttes til verifisering være i stand til å rekonstruere det, uten å røpe det, slik at enheten deretter kan rekalkulere nøkkelen K.

Dette kan for eksempel gjøres ved å iverksette og tilpasse fremgangsmåten beskrevet i ett av patentene nevnt tidligere id en foreliggende søknaden. Fremgangsmåten i patentfamilien er med dette inntatt ved referanse. Alternativt kan man benytte enhver kjent fremgangsmåte som gjør det mulig å rekalkulere et diversifisert hemmelig dataelement Sd for et objekt, uten å røpe elementet, og uten at objektet som ble benyttet til signering er tilgjengelig.

Fremgangsmåten beskrevet i den tidligere nevnte patentfamilien. og som er tilpasset den foreliggende oppfinnelsen består av å knytte sammen data Io som identifiserer objektet med den primære filen FP og med signaturen SG. Dette kan for eksempel gjøres ved å skrive opplysningene blant tilleggsinformasjonen i den sekundære filen FS, slik at det er mulig å rekalkulere eller rekonstruere det diversifiserte dataelementet uten å røpe det, ved å benytte de spesifikke kretsene i verifiseringsenheten. Disse identifikasjonsdataene kan for eksempel bestå av p parametere, som representerer adressene til p av de q mulige grunn-nøklene som er arkivert i mediets hemmelige minnesone. I dette tilfellet blir det diversifiserte hemmelige dataelementet deretter stilt sammen som en kombinasjon av informasjonen arkivert ved disse p adressene.

Som nevnt utfører objektet også en algoritme Ao. Vanligvis er denne algoritmen arkivert i et permanent minne av ROM eller PROM type, og kan variere fra en objekttype til en annen. Av denne grunn kan objektets identifikasjonsdata IO

også representerer algoritmen som utføres av objektet, eller kan med andre ord representere hvilken objekttype som er benyttet.

I dette tilfellet knyttes en spesifikk kontrollmodul sammen med en verifikasjonsenhet når signaturene verifiseres. Oppbygningen av denne modulen vil bli detaljert beskrevet i det følgende, sammen med den følgende detaljerte beskrivelsen av stegene i signaturverifiseringsprosessen.

Dataelementet E kan på signeringstidspunktet lages på ulike måter avhengig av algoritmen Aa arkivert i behandlingskretsene til signeringsenheten.

I en utførelsesform lages det eksterne dataelementet E automatisk av behandlingskretsene i enheten 1. Det kan for eksempel være et tilfeldig dataelement. For dette formålet ville enheten omfatte en generator for tilfeldige tall.

I et slikt tilfelle hvor dataelementet lages automatisk, vil dette eksterne dataelementet E bli skrevet blant tilleggsinformasjonen IC i den sekundære filen FS, slik at verifiseringsenheten kan rekonstruere nøkkelen K.

I en annen utførelsesform er det eksterne dataelementet E en funksjon av, eller utgjort av, dato og/eller tiden filen ble signert. I dette tilfellet blir enten dataelementet E selv, eller informasjon som muliggjør rekalkulasjon ved verifiseringstidspunktet, eller med andre ord informasjon korrelert med dato og/eller tid, skrevet blant tilleggsinformasjon IC i den sekundære filen FS.

I en annen utførelsesform utgjøres det eksterne dataelementet E av informasjon uttrukket fra og/eller forbundet med den primære filen FP selv. Plassering og øvrige egenskaper ved denne informasjonen kan være kjent på forhånd, eller det kan bestemmes tilfeldig av behandlingskretsene i enheten samtidig som signaturen blir beregnet.

En variant er således at det eksterne dataelementet E er sammensatt av et forhåndsbestemt antall n av oktetter valgt blant de første oktettene i filene, eller av de første oktettene av den første delen av filen som behandles ved beregning av signaturen.

Dette antallet n og plasseringen av oktettene som skal benyttes kan fastsettes en gang for alle. I dette tilfellet kan dataelementet E enkelt utelates fra den sekundære filen, siden verifiseringsenheten kan utlede hvordan dette dataelementet E ble bygget opp så snart enheten vet hvilken algoritme Aa som ble benyttet.

I en annen variant er det eksterne dataelementet E forbundet med filens navn, og/eller hode, og/eller størrelse, og/eller generelt enhver informasjon utledet fra filen.

I en annen variant blir tallet n og/eller plasseringen av de oktettene som skal benyttes bestemt på tilfeldig måte av enheten på det tidspunktet det eksterne

dataelementet E lages. I dette tilfellet blir enten dataelementet E eller informasjon som muliggjør rekonstruksjon av dette dataelementet, for eksempel tallet n og/eller plasseringen av oktettene som skal benyttes, skrevet blant tilleggsinformasjonen IC i den sekundære filen FS.

For å oppsummere:

- når det eksterne dataelementet E er laget, blir nøkkelen K beregnet i undertegnerens flyttbare medium 3, som en funksjon av hvilket dataelement E og av det hemmelige dataelementet S eller Sd som dette mediet inneholder;

- avhengig av sammenhengen blir dataelementet E, eller informasjon som setter verifiseringsenheten i stand til å rekonstruere dataelementet E, skrevet inn i den sekundære filen FS;

- hvis mediets hemmelige dataelement er et diversifisert dataelement Sd, så overføres en identifikasjon eller informasjon IO, som setter verifiseringsenheten i stand til å rekonstruere identifikasjonen IO, fra mediet til signeringsenheten, som deretter skriver identifikasjonen inn i den sekundære filen FS;

- signaturen SG blir beregnet fra nøkkelen K og fra minst en del av filen, og deretter skrevet inn i den sekundære filen;

- informasjon som gjør det mulig å bestemme hvilken del eller hvilke deler av filen som blir benyttet å beregne signaturen blir skrevet inn i den sekundære filen.

Det er klart at i tilfeller hvor mer enn en undertegner er involvert, så blir en sekundærfil eller separate poster laget for hver og en av dem. Som et resultat, kan flere sekundære filer være knyttet til den samme primære filen, eller den sekundære filen kan ha like mange poster som det er signaturer.

En eller flere signaturer kan verifiseres av en og/eller de andre av undertegnerne, og/eller av tredjeparter, betinget av at de har tilgang til utstyr tilpasset til en slik verifisering. Faktisk må dette utstyret være likt det som ble benyttet til å beregne hver signatur. Det kan også være det samme utstyret som ble benyttet til beregningen.

Verifiseringen består av å rekalkulere hver signatur ved bruk av de samme parametere som ble brukt ved den opprinnelige signeringen, og å sammenligne den rekalkulerte signaturen med den tilsvarende signaturen skrevet i den sekundære filen. For å gjøre dette, omfatter verifiseringsutstyret behandlings- og sammenligningskretser.

For å hindre en potensiell bedrager, som studerer verifiseringsprosessen, i å dra fordeler fra resultatene, har verifiseringsutstyret fortrinnsvis behandlings- og minnekretser ordnet slik at en rekalkulert signatur aldri blir røpet utenfor disse kretsene, og slik at kun resultatet av sammenligningen blir vist. Data som er

nødvendig for rekalkulasjonen blir deretter behandlet i en hemmelig minnesone i verifiseringsutstyret, og den rekalkulerte signaturen blir slettet så snart resultatet av sammenligningen er vist.

Hvis verifiseringsutstyret skal kunne rekalkulere signaturen, må det som nevnt først kunne rekalkulere nøkkelen K som ble benyttet til å alge signaturen. Som nevnt blir denne nøkkelen beregnet fra et diversifisert hemmelig dataelement Sd, eller et ikke-diversifisert hemmelig dataelement S lagret i en hemmelig minnesone i et flyttbar objekt som tilhører undertegneren.

Når det hemmelige dataelementet er diversifisert, ved tilpasningen beskrevet ovenfor av fremgangsmåten beskrevet i de før nevnte patentene, så kan utstyret omfatte en enhet med en spesifikk kontrollmodul, som omfatter en hemmelig minnesone og kretser for å behandle informasjon lagret i denne sonen, for å hindre at denne informasjonen blir kjent utenfor modulen.

I en utførelsesform er denne modulen beregnet til å ligge inne i enheten.

I en variant utgjøres modulen av et flyttbart minne og mikroprosessor-objekt 4, tilsvarende det som benyttes av undertegnerne.

I en foretrukket utførelsesform er noen eller hver ac undertegnernes bærbare objekter brukbare som moduler for verifisering av signaturer.

Ett objekt gjør det således mulig, både å signere, og å verifisere alle signaturene beregnet av kort fra samme familie. Det vil for eksempel si slike som har diversifiserte hemmelige data Sd som er laget fra enten det samme hemmelige grunnelementet, eller på måten som er beskrevet i de nevnte patentene.

I dette tilfellet kan det diversifiserte dataelementet av ett hvilket som helst objekt rekalkuleres eller rekonstrueres av noen eller hvert av objektene i den samme familien for å verifisere signaturene. Det er klart at i dette tilfellet vil et objekt benyttet til verifisering aldri tilby en rekalkulerbar signatur eller det rekonstruerte diversifiserte dataelementet.

Dette setter enhver i stand til å signere og verifisere ved å bruke det samme objektet, men hindrer en undertegner i å reprodusere signaturen til en annen.

Ved å anvende fremgangsmåten i de nevnte patentene, er det således tilstrekkelig at kontrollmodulens hemmelige sone inneholder de q mulige parametrene og å lese identifikasjonsinformasjonen IO knyttet til en signatur SG i den sekundære filen, for at modulen skal kunne bruke behandlingskretsene til å rekonstruere det hemmelige dataelementet Sd til objektet som ble benyttet til å kalkulere signaturen, men uten noen gang å røpe dette hemmelige dataelementet, ved å lese innholdet i adressene spesifisert i identifikasjonsinformasjonen.

Hvis dataelementet ikke er diversifisert, er det tilstrekkelig at enheten forbindes med en modul som har en hemmelig minnesone hvor det hemmelige dataelementet S er reprodusert, og behandlingskretser tilpasset slik at data i denne hemmelige sonen vil være tilgjengelige utelukkende for disse behandlingskretsene. I en utførelsesform er en slik modul beregnet til å bygges inn i enheten, og behandlingskretsene kan være de samme som enhetens. I en variant er modulen bygget på basis av et flyttbart objekt. I en foretrukket utførelsesform kan hvert flyttbare objekt som er tilgjengelig for en undertegner benyttes som en verifiserings-modul.

Verifiseringsenheten er til å rekonstruere det eksterne dataelementet E fra informasjonen (dataelementet E selv, dato og/eller tid, o.s.v.) som er skrevet med dette for øyet i den sekundære filen FS i løpet av signaturfasen.

Deretter ble nøkkelen K rekalkulert fra det eksterne dataelementet E og fra det diversifiserte eller ikke-diversifiserte hemmelige dataelementet, rekonstruert av modulen, og følgelig antatt å korrespondere med det som ble benyttet ved beregning av signaturen. Rekalkulering av denne koden K krever at det hemmelige dataelementet ikke røpes, og gjøres derfor av kretsene forbundet med denne hemmelige sonen, eller med andre ord, avhengig av utførelsesformen, kretsene i enheten eller kretsene i et flyttbart objekt.

Behandlingskretsene i enheten bestemmer deretter, fra den sekundære filen FS, hvilken del eller hvilke deler av den primære filen som ble benyttet til å beregne den opprinnelige signaturen, og rekalkulerer deretter en signatur SG', som ikke røpes utenfor behandlingskretsene, ved å behandle den rekalkulerte nøkkelen K og den nevnte delen eller delene av den primære filen.

Til slutt sammenligner sammenligningskretsene den rekalkulerte signaturen SG' med signaturen SG lest fra den sekundære filen, hvoretter kun resultatet av sammenligningen vises på enheten fremvisningsmidler for personen som utfører verifiseringen.

Den foretrukne utførelsesformen beskrevet ovenfor består følgelig av å få en nøkkel K kalkulert i objektet, og deretter få signaturen kalkulert av enhetens behandlingskretser, som en funksjon av denne nøkkelen K og minst en til av den primære filen FP.

I en variant blir signaturen beregnet i objektet, hvilket gjør det unødvendig å generere det eksterne dataelementet E. I dette tilfellet er algoritmen Aa, som er lagret i enheten, laget på en slik måte at behandlingskretsen er dens behandler og sender til objektet hver del valgt fra filen, og valgfritt en eller flere parametere som er passende å behandle, så som dato og/eller tid, og/eller navn og størrelse, o.s.v. I

den endelige analysen gjenvinner objektets kretser signaturen SG, som er en funksjon av delene av filen og andre parametere som kretsene har mottatt fra enheten, og de overfører deretter denne signaturen til enheten slik at den vil bli skrevet i den sekundære filen FS. Man oppnår på denne måten et sammenlignbart resultat uten at det er nødvendig å overføre koder til enheten. Hvis en eller flere ytterligere parametere blir behandlet, må også informasjon som gjør det mulig å rekonstruere disse parametrene skrives i den sekundære filen.

I dette tilfellet, hvor signaturen beregnes av objektet, er forutsetningen at kretsene i enheten har grunnleggende funksjoner. Algoritmen Aa, som er lagret i enheten, er redusert til en minimum for å muliggjøre utvekslinger med objektet og med filene som finnes i enhetens masselagre.

Denne varianten krever imidlertid bruk av flyttbare objekter med større beretningskapasitet og kraftigere algoritmer enn den foretrukne fremgangsmåten. Den foretrukne fremgangsmåten beskrevet ovenfor, krever faktisk kun at objektets behandlingskretser er i stand til å reagere på en innkommende ordre med å tilveiebringe et resultat som er en funksjon av objektenes hemmelige dataelement S eller SD og et eksternt dataelement.

Realisering av oppfinnelsen i maskinvare eller programvare er innenfor kompetansen til en fagmann på området, og behøver ingen videre, detaljert beskrivelse.

Signaturen eller signaturene i en primærfil FP kan verifiseres mens den primære filen og den sekundære fil eller filer FS er i samme enhet som den som ble benyttet til beregningen, eller etter at den primære filen og dens sekundære fil eller filer FS er overført til en annen enhet.

Overføringen er ikke tema i den foreliggende oppfinnelsen. Den kan gjøres ved hjelp av alle kjente midler eller fremgangsmåter. Den kan omfatte en elektronisk overføring over en datalinje, en overføring ved hjelp av et maskinvaremedium som en diskett, eller en hvilken som helst annen type dataoverføring. Det bør være ganske klart at den primære filen og den sekundære filen eller filene som er knyttet til den bør overføres til en enhet som er i stand til å utføre signaturverifiseringene, dersom man ønsker å utføre denne operasjonen, eller med andre ord spesielt til en enhet som har en passende programvarestruktur.

Hvis oppfinnelsen skal virkeliggjøres på en enkelt måte, er det ønskelig å tilveiebringe et system som muliggjør enkel dialog med brukeren av systemet, enten han er undertegneren eller personen som verifiserer signaturen, d.v.s. et system som er ergonomisk og brukervennlig.

Dette er grunnen til at oppfinnelse fortrinnsvis bør virkeliggjøres ved å benytte filbehandlingsmaskinvare som tillater bruk av dialogvinduer, slik som den som virker i et Microsoft Windows-miljø.

Figur 2 viser et grunnleggende dialogvindu som kan åpnes for å starte enten beregningen eller verifiseringen av en signatur eller signaturer knyttet til en fil.

Anvendelsens tittel 8 fremtrer på en tittellinje 9 ved toppen av vinduet, og de tilgjengelige menyene går frem av en menylinje 10.

En første meny, "MODUS", gjør det mulig å velge enten "signatur" modus eller "signaturverifisering" modus.

En andre meny "PIL", gjør det mulig å velge en hvilken som helst filtype som er lagret i enheten, og som brukeren ønsker å signere eller som man ønsker å verifisere signaturen eller signaturene til. Dette kan omfatte tekstfiler, datafiler, tegninger, o.s.v.

En tredje meny, "UTVALG", er tilgjengelig i hvertfall når "signatur" modus er aktiv. Den gir tilgang til en enten "manuell utvalg" modus eller til en "automatisk utvalg" funksjon, som begge vil bli detaljert beskrevet sendere.

En fjerde meny "OPPSETT", gjør det mulig for eksempel å velge et medium som allerede er benyttet til en signatur, eller å tilordne karakteristika til et nytt medium. Disse begrepene vil bli nærmere beskrevet senere.

Endelig kan en hjelpemeny, "?", være til stede.

Figurene 3 og 4 viser to varianter av vinduer som kan åpnes når en fil er aktivert av "FIL" menyen, og når signaturverifiseringsmodusen er aktivert av "MODUS" menyen. Disse variantene inneholder kun minimale forskjeller, som bli bli belyst hver gang det blir nødvendig.

Når verifiseringsmodus er aktiv er det en fordel, og ikke nødvendig, at "UTVALG" menyen er tilgjengelig. Omvendt må "FIL" og "MODUS" menyene være tilgjengelige.

En første ramme, "KILDE" 11, kommer opp, og inneholder informasjon om status for den validerte filen og indikerer filens navn, om den er signert eller ikke, dens størrelse, filens dato og katalogen hvor den er plassert.

Videre indikerer en andre ramme, "SIGNATUR" 12, antall og/eller navnet til signaturene som muligens kan være knyttet til denne filen.

I varianten på figur 3, er hver av signaturene i denne andre rammen 12 markert med et navn, indikert i en første sone 13, i dette tilfellet "Pierre", "Paul", o.s.v. I varianten på figur 4, er hver av signaturene i denne andre rammen 12 markert av et ordenstall, "sign 1", "sign 2", gitt som standardverdier av enheten, og vist i den første sonen 13.

En andre sone 14 viser den aktive signaturen, ved navn (figur 3) eller nummer (figur 4).

I en tredje ramme på figur 3, "informasjon" 15, vises ordene "hele dokumentet", hvilket indikerer at signaturen "Pierre", som nå verifiseres, ble beregnet på grunnlag av hele filen. I den tilsvarende rammen på figur 4, vises ordene "manuelt utvalg", hvilket indikerer at signaturen "sign 1", som nå verifiseres, ble beregnet på grunnlag av end el av filen.

I tillegg viser en sone 16 i denne tredje rammen 15 navnet til mediet som ble benyttet til å beregne signaturen som nå verifiseres.

"OK" eller "AVBRYT" knapper, som er tilgjengelige, for eksempel ved hjelp av en markør som kan flyttes omkring ved å bruke en mus eller tastaturet 6a, er plassert i denne rammen 15. Disse knappene gjør det mulig å starte eller avbryte verifiseringen.

I en annen sone 17 i denne rammen 15, vises fremgangen i verifiseringsberegningen som et prosenttall etter at start av verifiseringen er bekreftet med "OK" knappen. Videre gjør sonen 17 det mulig å vise en stolpe, hvor stolpens lengde indikerer fremgangen.

Vinduer som kan åpnes når en signatur lages eller legges til, er vist på figurene 5 og 6. Valg av "signatur" gjøres fra "MODUS" menyen, som er tilgjengelig ved oppstart av applikasjonen eller fra "verifiserings" modus, eller naturligvis når "signatur" modus selv er bekreftet.

Når signaturmodus er aktiv, velges fortrinnsvis hele dokumentet eller filen dersom ikke annet blir spesifisert. D.v.s. at signaturen vil bli beregnet på grunnlag av hele filen. Imidlertid kan en eller flere deler av filen velges manuelt som beskrevet nedenfor.

Når "signatur" modus er aktiv, er samtlige menyer tilgjengelige.

Figur 5 viser et vindu som åpnes når signatur modus og manuelt utvalg er aktivert.

Det åpne vinduet er tilsvarende dem på figurene 3 eller 4, bortsett fra at det i informasjonsrammen 15 er indikert at den aktive modus er modusen for signaturberegning, og at ordene "manuelt utvalg" er skrevet i rammen.

Det skal bemerkes at dersom utvalget gjøres uten spesielle valg, så åpnes et vindu (ikke vist i tegningene), som kun har en enkelt forskjellig utseende fra vinduet på figur 5. I informasjonsrammen 15 står ordene "hele dokumentet" i stedet for "manuelt utvalg".

Videre vises navnet og informasjon vedrørende den filen som nå signeres i den første rammen "kilde", og navnet eller nummeret til signaturen som nå lages vises i den andre sonen 14 i den andre rammen 12.

Endelig er navnet til mediet, som benyttes til å beregne signaturen som nå lages, skrevet i den spesifikke sonen 16 i den tredje rammen 15.

I en fortrukket utførelsesform startes signaturberegningen ved å trykke på "OK" knappen i informasjonsrammen 15, når hele dokumentet er valgt enten frivillig eller ved at intet annet er spesifisert.

I denne foretrukne utførelsesformen åpnes imidlertid vinduet vist i figur 6 ved manuelt utvalg. Dette vinduet gjør det mulig å vise innholdet i filen, og å velge visse soner i den ved å bruke en markør, også kjent som cursor, som for eksempel en markør som beveges omkring av en mus eller av taster på tastaturet 6a forbundet med behandlingsenheten.

"KILDE" og "SIGNATUR" rammene som opptrer i de foregående vinduene er erstattet av en enkelt ramme 18, hvor filinnholdet blir vist frem, mens rammen 15 "INFORMASJON", fortsatt er til stede.

Valg av en eller flere deler av filen kan gjøres manuelt ved å bruke en markør som beveges av en mus eller av taster på tastaturet. Eksempelet på figur 6 viser valg av en enkelt del 19, også kalt en blokk, av en tekstfil som består av 37 oktetter. Informasjonsrammen indikerer antall blokker, og totalt antall oktetter som er valgt.

Dette vinduet kan omfatte en eller flere lineære slektrør 20, 21, slik at filen kan rulles på skjermen på vanlig måte for å gjøre det mulig å søke etter spesielle deler av filen. En første selektor 20 gjør det for eksempel mulig å rulle innen den aktive siden, og en andre selektor 21 gjør det mulig å rulle side for side.

Til slutt manipuleres "OK" knappen for å bekrefte valget, og starte signaturberegningen.

"OPPSETT" menyen gjør det mulig å spesifisere egenskapene for et nytt medium til systemet, for eksempel ved signering, eller å søke etter egenskapene til et medium som allerede er spesifisert når noe skal verifiseres.

Av denne grunn må en ny undertegner som ønsker å bruke systemet bekrefte korttypen han benytter til signeringen.

Hvis en ny undertegner bruker et medium som for eksempel et kort med egenskaper som allerede er lastet inn fra et annet kort, er det denne menyen han bruker for å oppgi dette.

Brukerens bekreftelse åpner et "KORT" vindu tilsvarende det på figur 7. Dette inneholder bokser som gjør det mulig å taste inn ulike parametere som definerer et nytt medium benyttet til beregning av en ny signatur. Det er med denne

menyen medier som inneholder ulike algoritmer og/eller forskjellig diversifiserte nøkler kan identifiseres på beregningstidspunktet, slik at verifisering kan utføres senere.

Således kan denne menyen blant annet benyttes til å indikere applikasjonene "ref appli" (tekstbehandler, regneark, o.s.v.), som mediet kan ha tilgang til. I tillegg kan man presis identifisere den involverte medietypen og nøkkelversjonene ("ref nøkkel", "nøkkelversjon") som mediet inneholder, slik at systemet kan virke som det skal. Mer generelt gjør denne menyen det mulig å gi systemet alle nødvendige parametere som vedrører et medium, slik at det blir tilgjengelig for beregning og verifisering.

PATENTKRAV

1. Fremgangsmåte for signering av en datamaskin-hovedfil (FP) av en person, hvilken fremgangsmåte består i å få minst en signatur (SG) for filen beregnet ved hjelp av kretser i en informasjonsbehandlingsenhet (1, 3, 4), å benytte en signaturalgoritme (Aa, Ao) og ta hensyn til minst ett hemmelig dataelement (S; Sd) som er spesifikt for undertegneren, men ukjent for ham, og som er lagret i en hemmelig minnesone i en bærbar elektronisk gjenstand (4) med et minne og behandlingskretser, og som er tilgjengelig for denne undertegneren, og i å knytte den beregnede signaturen til hovedfilen,
k a r a k t e r i s e r t v e d at, når hver signatur beregnes, består fremgangsmåten videre i:

- å utvelge minst en valgt del (19) av hovedfilen som undertegneren ønsker å hefte sin signatur til, slik at signaturen er en funksjon av undertegnerens hemmelige dataelement og av hver valgt del av filen;

- å lage en sekundærfil (FS) og registrere i denne i det minste noe informasjon (IN) som tillater identifisering av hver del av hovedfilen som ble benyttet ved beregning av denne signaturen; og

- å knytte sekundærfilen på den ene side til den tilsvarende signatur, og på den annen side til den signerte fil.

2. Fremgangsmåte ifølge krav 1,
k a r a k t e r i s e r t v e d at et stykke med algoritme-informasjon (IC) som definerer en type signatur-algoritme som benyttes til å beregne den nevnte signaturen, registreres i sekundærfilen (FS).

3. Fremgangsmåte ifølge krav 1,
k a r a k t e r i s e r t v e d at et stykke med informasjon (IO) om den bærbare gjenstanden, med definisjon av en type bærbar gjenstand og som benyttes til å beregne den nevnte signaturen, registreres i sekundærfilen (FS).

4. Fremgangsmåte ifølge krav 1,
k a r a k t e r i s e r t v e d at hovedfilen (FP) signeres av en rekke undertegnere med forskjellige hemmelige dataelementer (S, Sd) som befinner seg henholdsvis i forskjellige bærbare gjenstander (4), gjennom de følgende trinn:

- å utvelge fra hovedfilen like mange valgte fildeler (19) som det finnes undertegnere, og som de respektive undertegnere akter å beregne sin signatur for;

- å beregne hver signatur ved å benytte en informasjonsbehandlingsenhet (1) som omfatter en signaturalgoritme, og eksekvere en beregning med denne algoritmen på grunnlag av undertegnernes henholdsvise, hemmelige dataelement, tatt fra den tilsvarende, bærbare gjenstand og på grunnlag av den tilsvarende, valgte fildel, for å oppnå et resultat som definerer hver signatur;

- å benytte en sekundærfil (FS) til å registrere et stykke med filidentifiserings-informasjon (IN) som identifiserer, i hovedfilen, alle de valgte fildeler som er benyttet til å beregne signaturen; og

- å sammenknytte hovedfilen, signaturene og sekundærfilen.

5. Fremgangsmåte ifølge krav 1,
karakterisert ved at beregningen av signaturer omfatter de følgende trinn;

- å tilveiebringe en første signaturalgoritme (Aa) i informasjonsbehandlingsenheten;

- å tilveiebringe en beregningsalgoritme (Ao) for en andre nøkkel i den bærbare gjenstanden;

- å frembringe og overføre et variabelt dataelement (E) fra kretsene i behandlingsenheten til gjenstandens kretser;

- å beregne en nøkkel (K) i gjenstandens kretser ved å eksekvere algoritmen for den andre nøkkelen i gjenstandens kretser og ved å benytte det variable dataelementet og det hemmelige dataelementet;

- å overføre nøkkelen fra gjenstandens kretser til behandlingsenhetens kretser;

- å beregne signaturen ved å eksekvere den første signaturalgoritmen i behandlingsenhetens kretser og benytte nøkkelen og den valgte fildelen (19); og

- å registrere det variable dataelementet i sekundærfilen (FS).

6. Fremgangsmåte ifølge krav 1,
karakterisert ved at beregningen av signaturer omfatter de følgende trinn:

- å eksekvere signaturalgoritmen (Ao) i den bærbare gjenstanden;

- å overføre den valgte fildelen (19) fra behandlingsenhetens kretser til gjenstandens kretser; og

- å beregne signaturen ved å benytte denne valgte fildelen og det hemmelige dataelementet ved å eksekvere signaturalgoritmen i gjenstandens kretser.

7. Fremgangsmåte ifølge krav 1,

k a r a k t e r i s e r t v e d at signaturen som er knyttet til hovedfilen, verifiseres, idet signatur-verifiseringstrinnet omfatter:

- å identifisere den valgte fildelen (19) i hovedfilen (FP) ved å bruke filidentifiserings-informasjonen (IN) i sekundærfilen (FS);
- å benytte en informasjonsbehandlingsenhet (1) som omfatter signatur-algoritmen og, i en hemmelig minnesone, det hemmelige dataelementet (S, Sd);
- å beregne på nytt signaturen i enheten ved å eksekvere en beregning med signaturalgoritmen, basert på det hemmelige dataelementet i den hemmelige minnesonen og på den identifiserte, valgte fildelen, og å ta hensyn til eventuell annen informasjon som er registrert tidligere i sekundærfilen for å beregne signaturen, idet resultatet av beregningen utgjør signaturen som er beregnet på nytt;
- å sammenligne signaturen som er beregnet på nytt, med signaturen (SG) som er knyttet til hovedfilen; og
- å indikere et resultat av sammenligningen uten å avsløre signaturen som er beregnet på nytt.

8. Anordning for å gi en person tillatelse til å signere en datamaskin-hovedfil (FP) for implementering av fremgangsmåten i henhold til et av kravene 1-7, omfattende:

- en bærbar gjenstand (4) med et minne og behandlingskretser, hvilken bærbar gjenstand er dedikert til en undertegner og er tilgjengelig for ham, idet en hemmelig sone i dette minnet lagrer et hemmelig dataelement (S, Sd) som er spesifikt for en identitet for minst en undertegner;
- informasjonsbehandlingsmidler (1);
- midler for beregning av en signatur (SG) ved benyttelse av en signaturalgoritme (Aa, Ao) og ved å eksekvere en beregning med denne algoritmen, basert på den bærbare gjenstandens hemmelige dataelement og filen, idet et resultat av denne beregningen utgjør signaturen;

k a r a k t e r i s e r t v e d at anordningen videre omfatter:

- midler (6) for å fremvise hovedfilens innhold;
- midler for å gi undertegneren tillatelse til å utvelge fra hovedfilen en valgt fildel (19) slik at signaturen (SG) baseres på denne delen;
- midler for å bruke en sekundær fil (FS) til å registrere et stykke med filidentifiserings-informasjon (IN) sin identifiserer i hovedfilen den valgte fildelen som benyttes til å beregne signaturen; og
- midler for å sammenknytte hovedfilen, signaturen og sekundærfilen.

9. Anordning ifølge krav 8,
karakterisert ved at den omfatter:
- midler (13) for å fremvise et navn eller en rang for en signatur som allerede er knyttet til en fil;
- midler for utvelgelse av minst en signatur som skal verifiseres; og
- midler (14) for å fremvise rangen eller navnet til en signatur som beregning eller verifisering foregår for.

10. Anordning ifølge krav 8,
karakterisert ved at den omfatter midler for å spesifisere overfor informasjonsbehandlingsenheten (1), de egenskaper (IO) ved den bærbare gjenstanden som benyttes for en signatur som beregning foregår for, eller som er benyttet for en signatur som verifisering foregår for.

11. Anordning ifølge krav 8,
karakterisert ved at den omfatter en verifiseringsenhet forbundet med en verifiseringsmodul anordnet for å finne og/eller beregne på nytt parametrene som er benyttet for beregning av signaturen, idet disse parametrene er annerledes enn delene (19) av hovedfilen (FP) som er benyttet til å beregne signaturen, men uten å avsløre parametrene.

12. Anordning ifølge krav 8,
karakterisert ved at modulen er en bærbar elektronisk gjenstand (4) med et minne og behandlingskretser, hvilken bærbare gjenstand er i stand til å bli forbundet med verifiseringsenheten.

13. Anordning ifølge krav 12,
karakterisert ved at de bærbare elektroniske gjenstandene (4) som er tilgjengelige for undertegnerne, er tilpasset for å innbefatte verifiseringsmodulen, idet gjenstandene tjener både til å signere filene og til å verifisere de beregnede signaturene, ved bruk av et ikke-diversifisert eller diversifisert dataelement.

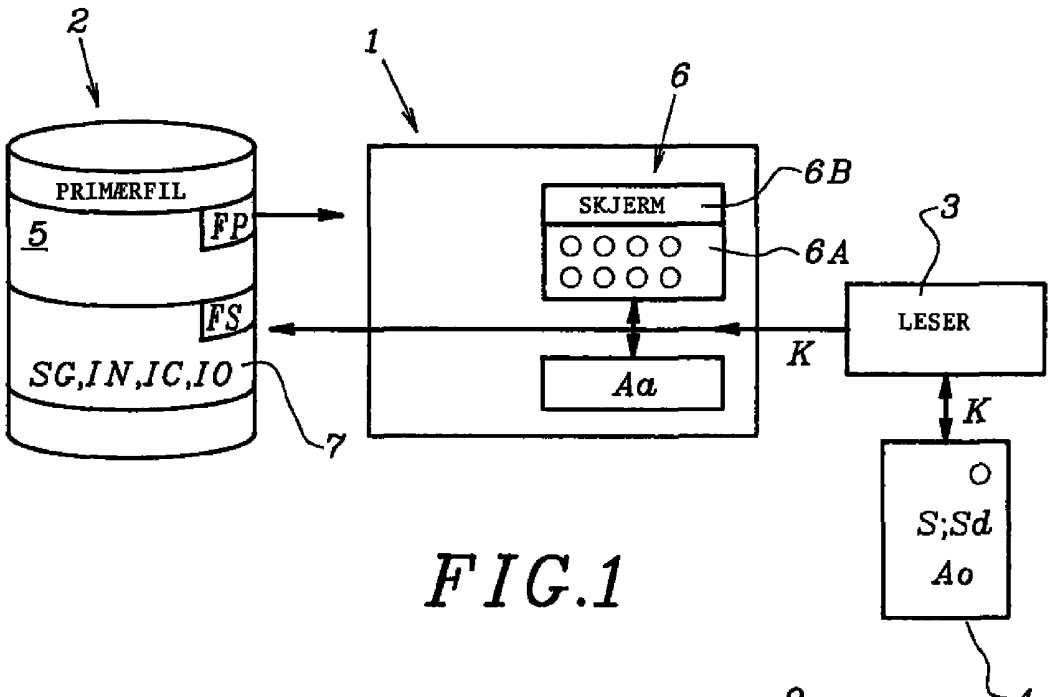

2
1
6
PRIMÆRFIL
5
FP
FS
SG,IN,IC,IO
7
SKJERM
6B
6A
Aa
3
LESER
K
K
S;Sd
Ao
4

FIG.1

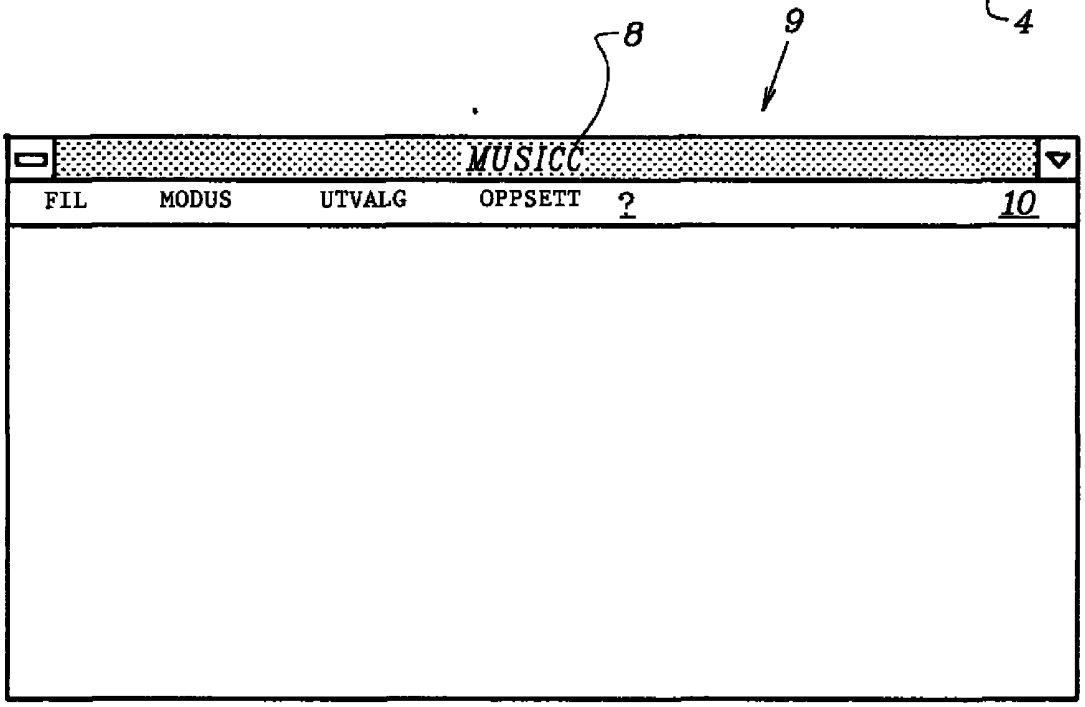

8
9
MUSICC
FIL
MODUS
UTVALG
OPPSETT
?
10

FIG.2

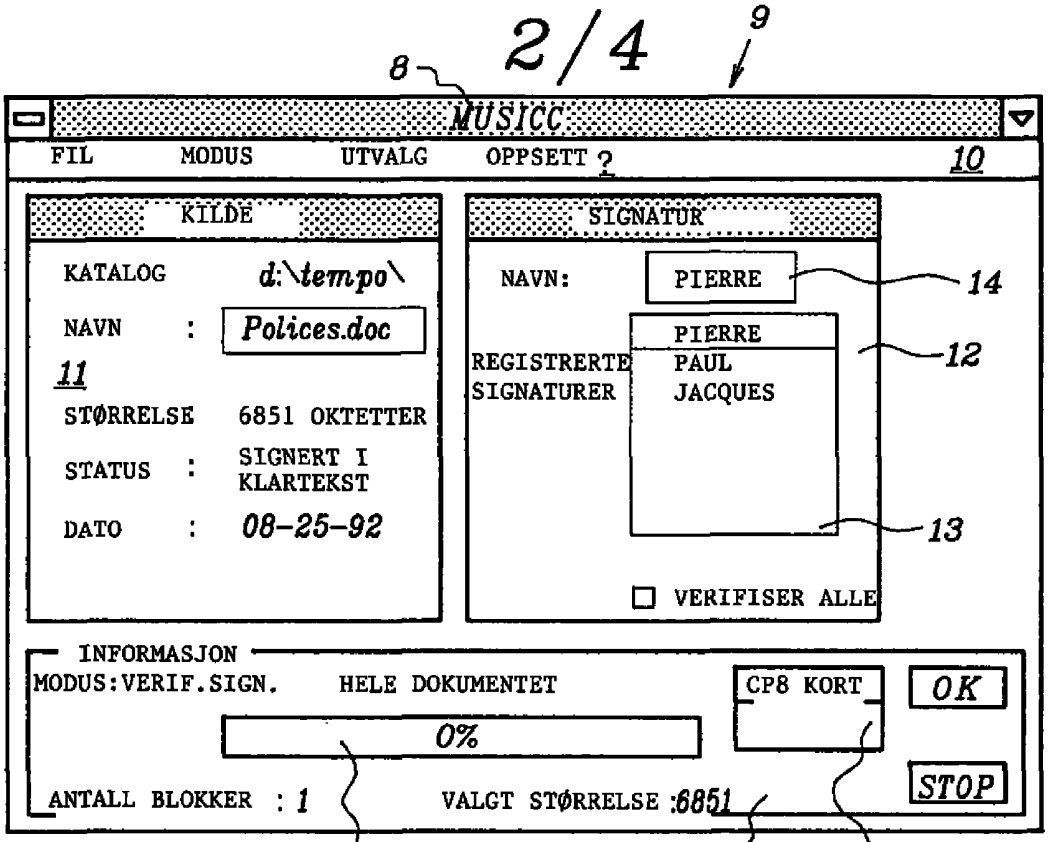

8
9
MUSICC
FIL
MODUS
UTVALG
OPPSETT ?
10
KILDE
KATALOG
d:\tempo\
NAVN :
Polices.doc
11
STØRRELSE
6851 OKTETTER
STATUS :
SIGNERT I KLARTEKST
DATO :
08-25-92
SIGNATUR
NAVN:
PIERRE
14
PIERRE
PAUL
JACQUES
REGISTRERTE SIGNATURER
12
13
VERIFISER ALLE
INFORMASJON
MODUS:VERIF.SIGN.
HELE DOKUMENTET
CP8 KORT
OK
0%
STOP
ANTALL BLOKKER : 1
VALGT STØRRELSE :6851
17
15
16

FIG.3

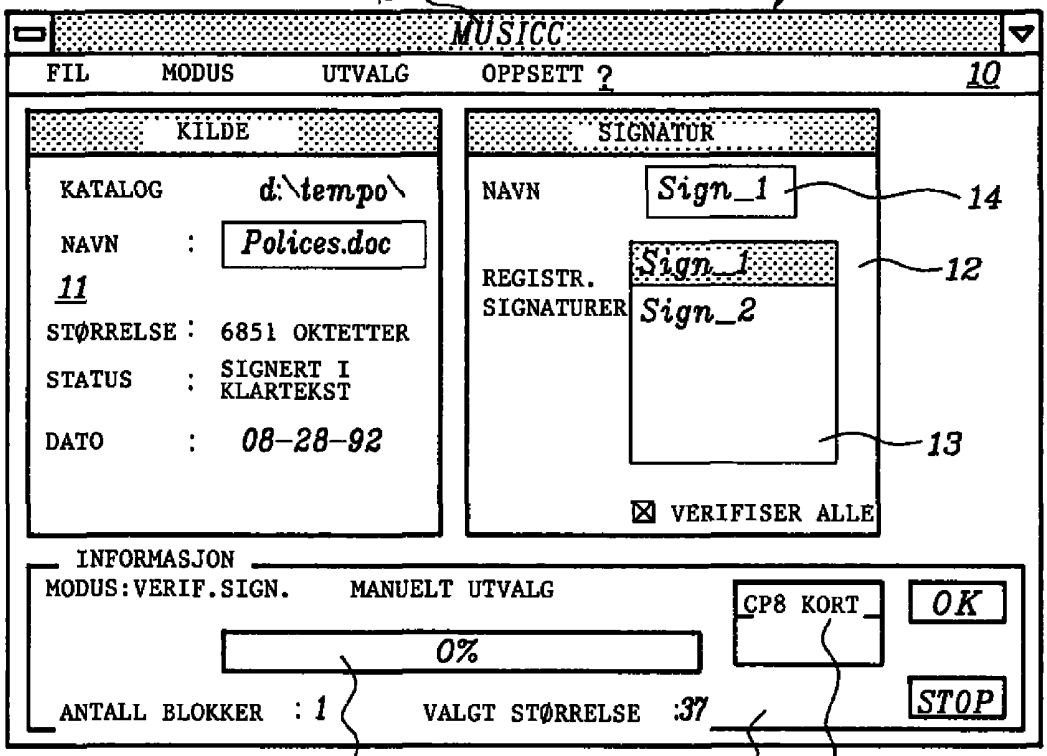

8
9
MUSICC
FIL
MODUS
UTVALG
OPPSETT ?
10
KILDE
KATALOG
d:\tempo\
NAVN :
Polices.doc
11
STØRRELSE :
6851 OKTETTER
STATUS :
SIGNERT I KLARTEKST
DATO :
08-28-92
SIGNATUR
NAVN
Sign_1
14
Sign_1
Sign_2
REGISTR. SIGNATURER
12
13
VERIFISER ALLE
INFORMASJON
MODUS:VERIF.SIGN.
MANUELT UTVALG
CP8 KORT
OK
0%
STOP
ANTALL BLOKKER : 1
VALGT STØRRELSE :37
17
15
16

FIG.4

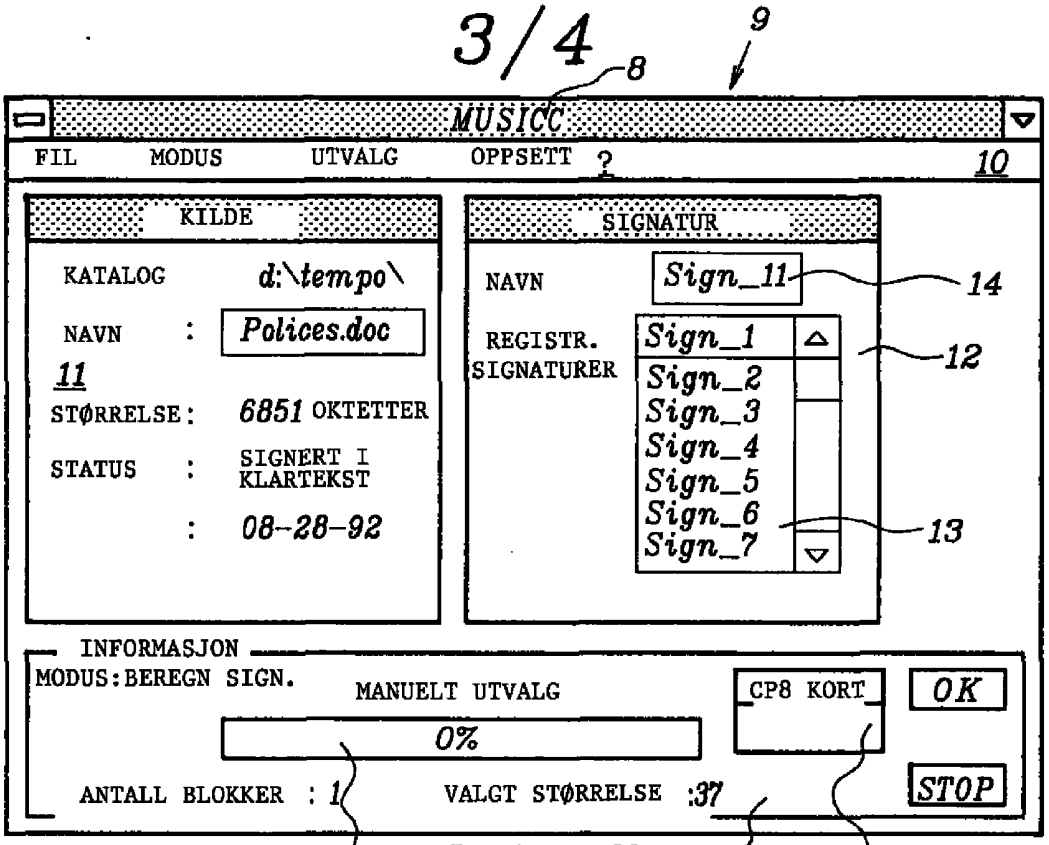

9
8
MUSICC
FIL
MODUS
UTVALG
OPPSETT ?
10
KILDE
KATALOG
d:\tempo\
NAVN :
Polices.doc
11
STØRRELSE :
6851 OKTETTER
STATUS :
SIGNERT I KLARTEKST
: 08-28-92
SIGNATUR
NAVN
Sign_11
14
REGISTR. SIGNATURER
Sign_1
Sign_2
Sign_3
Sign_4
Sign_5
Sign_6
Sign_7
12
13
INFORMASJON
MODUS:BEREGN SIGN.
MANUELT UTVALG
0%
CP8 KORT
OK
STOP
ANTALL BLOKKER : 1
VALGT STØRRELSE :37
17
15
16

FIG.5

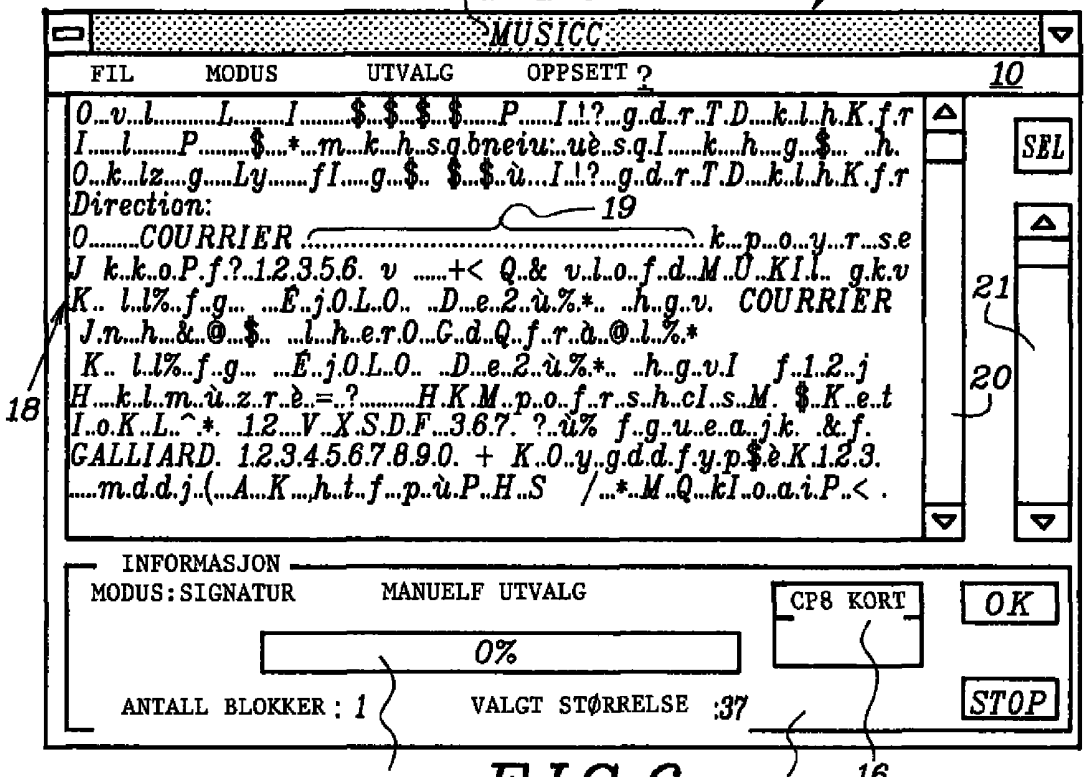

8
9
MUSICC
FIL
MODUS
UTVALG
OPPSETT ?
10
SEL
Direction:
19
COURRIER
21
20
18
INFORMASJON
MODUS:SIGNATUR
MANUELF UTVALG
CP8 KORT
OK
0%
STOP
ANTALL BLOKKER : 1
VALGT STØRRELSE :37
17
15
16

FIG.6

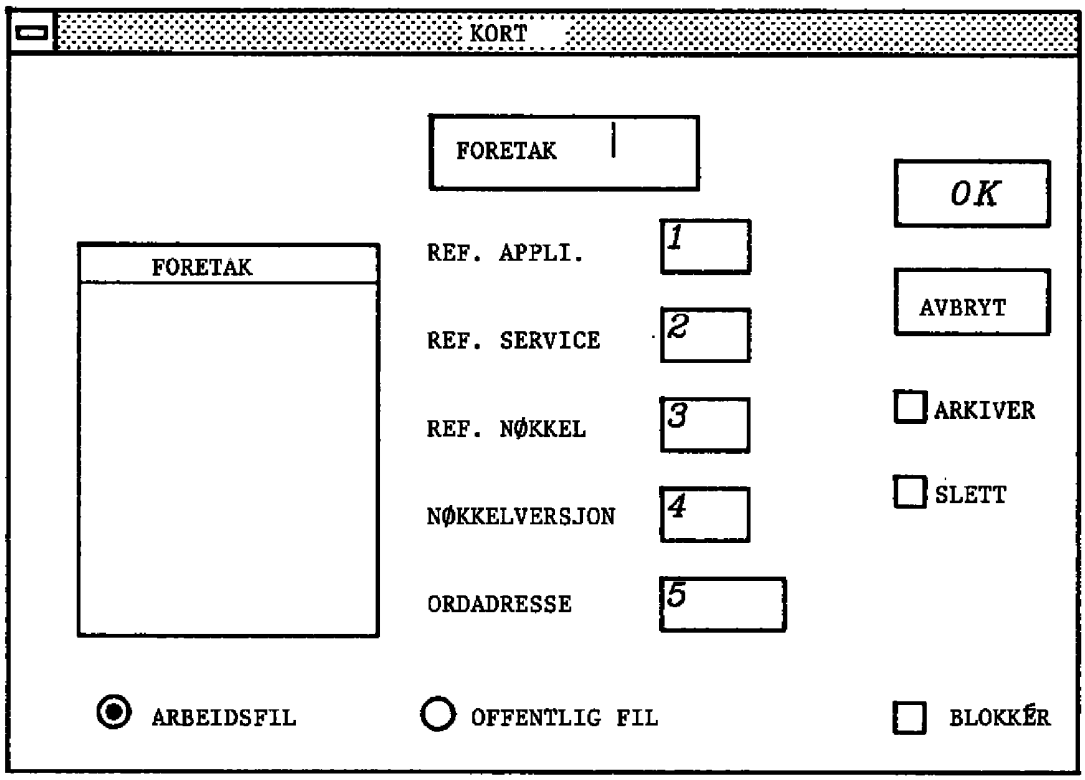

KORT
FORETAK
OK
FORETAK
REF. APPLI.
1
AVBRYT
REF. SERVICE
2
REF. NØKKEL
3
ARKIVER
NØKKELVERSJON
4
SLETT
ORDADRESSE
5
ARBEIDSFIL
OFFENTLIG FIL
BLOKKÉR

FIG.7