NORGE

(12) **PATENT**

(19) NO (11) **304458** (13) B1

(51) Int Cl[6] G 06 F 9/44

Patentstyret

(21) Søknadsnr	19923239	(86) Int. inng. dag og søknadsnummer	
(22) Inng. dag	18.08.1992		
(24) Løpedag	18.08.1992	(85) Videreføringsdag	
(41) Alm. tilgj.	22.02.1993	(30) Prioritet	19.08.1991, FR, 9110404
(45) Meddelt dato	14.12.1998		

(73) Patenthaver France Télécom, 6, place d'Alleray, F-75015 Paris, FR
Telediffusion de France, 10 rue d'Oradour sur Glane, F-75015 Paris, FR

(72) Oppfinner Françoise Coutrot, Cesson-Sevigne, FR
Pierre Fevrier, St. Sulpice la Foret, FR

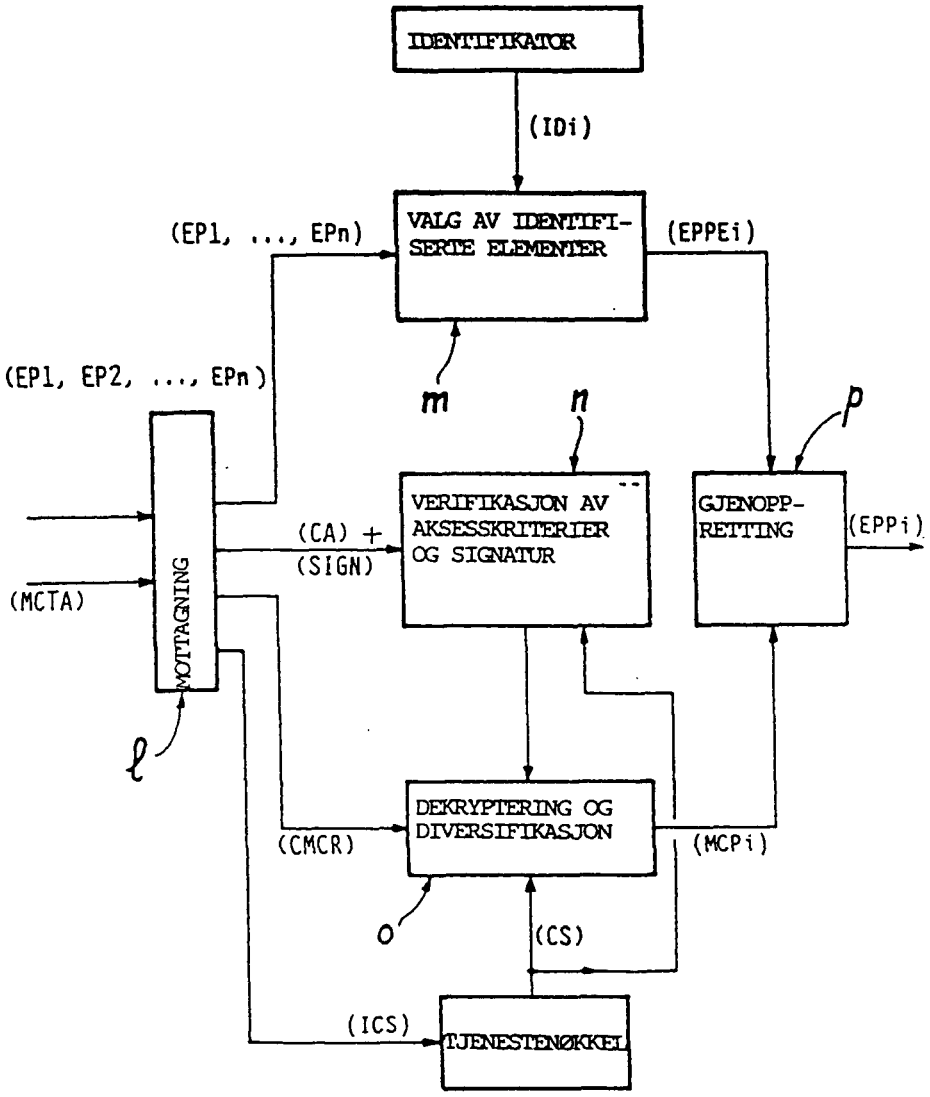
(74) Fullmektig Onsagers Patentkontor - Defensor AS, 0103 Oslo

(54) Benevnelse **Fremgangsmåte til utsendelse og mottagelse av personlige programmer**

(56) Anførte publikasjoner EP A3 317101, JP A 2-157710

(57) Sammendrag

Programmet består av personlige programelementer som inneholder en identifikasjon av mottageren eller adressaten, idet aksessen til hvert programelement er reservert for den enkelte mottager og betinget av beskyttelsen av en aksesstillatelse som dekker aksesskriteriene for tjenesten og besittelsen av en individuell identifikasjon for hver mottagers del. Kontrollmeldingen for adgangstillatelse tillater brukeren av tjenesten å beregne, på basis av det enkelte kryptogram og et rotkontrollord og identifikasjonen av mottageren, samtlige personlig kontrollord som vil sette mottageren, og ham alene, i stand til å gjenopprette elementene som angår ham.


IDENTIFIKATOR
(IDi)
VALG AV IDENTIFI-SERTE ELEMENTER
(EP1, ..., EPn)
(EPPEi)
(EP1, EP2, ..., EPn)
m
n
p
VERIFIKASJON AV AKSESSKRITERIER OG SIGNATUR
GJENOPP-RETTING
(EPPi)
(CA) +
(SIGN)
(MCTA)
MOTTAGNING
l
DEKRYPTERING OG DIVERSIFIKASJON
(CMCR)
(MCPi)
o
(CS)
(ICS)
TJENESTENØKKEL

Oppfinnelsen angår en fremgangsmåte til overføring og mottagning av personlige programmer.

Den store økning i antallet overførings- eller kringkastingsbærere (satellitter, kabler, mikrobølger) har fått programoperatørene til i stort omfang å øke tilbudet av tjenester for å aksessere kontrollprogrammer som kan være i form av audiovisuelle programmer, lydprogrammer eller dataoverførings-programmer.

Prinsippet for aksesskontroll til slike tjenester er basert på omkasting av et program ved overføring og gjenoppretting av budskapet mottatt under styring av en aksesstillatelse. Omkastings- og gjenopprettingssystemene initialiseres av data som varieres på slumpmessig måte og som er kjent som et kontroll-ord. Informasjonen som skriver aksesskriteriene til programmet og en beskyttet form av kontrollordet er innbefattet i kontrollmeldingene for adgangstillatelsene som ledsager det omkastede program.

For å få aksess til et omkastet program er det nødvendig for den betingede aksessinnretning å være i stand til å utnytte en av kontrollmeldingene om aksesstillatelsene som er forbundet med programmet. I tilfelle av "personlige" tjenester for hvilke programmet består av en rekke program-elementer (videosekvenser og/eller lyd og/eller data) adressert til samme antall forskjellige adressater eller mottagere, må hvert programelement bare restaureres på ukodet form for den enkelte mottager som er involvert og kontrollmeldingene om aksesstillatelsene må gjøre det mulig å garantere beskyttelse for hvert av programelementene.

Oppfinnelsen angår en fremgangsmåte til overføring og mottagning av kontrollmeldinger for aksesstillatelser som gjør enhver mottager, (men bare den alene) til å motta programelementer sendt til ham innenfor rammen av en personlig overføringstjeneste.

Anvendelsene av en slik fremgangsmåte er alle personlige program-overførings- eller kringkastingstjenester som er multiplekset på samme bærer, f.eks. talebudskap, datatransmisjon (teleks, nedlasting av data, faks, radiomeldinger såsom operatør- eller alfapersonsøking), overføring av faste eller levende bilder (videooverføring) osv.

Eksisterende fremgangsmåter som gjør det mulig å beskytte aksess til et kringkastet program, består i å allokere til hvert programelement en kontrollmelding om aksesstillatelse. Denne fremgangsmåten er sterkt utbredt i betalingsfjernsynstjenester hvor hvert program eller programelement leveres til en stor seerskare og for hvilke det er tilstrekkelig å forbinde ett eller flere, typisk tre eller fire meldinger om aksesstillatelse med det fullstendige kringkastede program. Informasjonsraten som er spesifikke for aksesskontroll relativt til et kringkastet program er da meget liten (typisk noen få hundre byte/s for å styre en informasjonsrate på flere megabyte/s).

Hver kontrollmelding om aksesstillatelse har generelt fire felter:

- en identifikator for tjenestenøkkelen som skal benyttes,
- et felt som definerer aksessbetingelsene som skal tilfredsstilles for å ha rett til å benytte en slik tjenestenøkkel,
- kryptogrammet eller kryptogrammene for ett eller begge kontrollord,
- et redundant felt som hensiktsmessig kan tilføyes for at sikkerhetsprosessoren ikke kan benyttes utenfor sin tiltenkte sammenheng.

Når sikkerhetsprosessoren inneholder en korrekt aksesstillatelse, dvs. når den holder tjenestenøkkelen angitt av identifikatoren og denne tjenestenøkkelen er gitt en status som samsvarer med visse betingelser angitt i aksesskriterie-feltet, dekrypterer eller dechiffrerer sikkerhetsprosessoren kryptogrammet eller kryptogrammene for å rekonstituere kontrollordet eller -ordene. Kontrollordet tillater terminalen å gjenopprette programmet eller program-elementene som den forbindes med.

I tilfelle av personlige kringkastingstjenester, ville utvidelsen av den foregående metode som ville bestå i å forbinde samme antall kontroll-meldinger om aksesstillatelse som det er programelementer som kan aksesseres på en bestemt måte, gjøre det nødvendig i visse tilfeller å redusere informasjonsresurssen med to, under antagelse av at innholdet av informasjonen som skal overføres, har omtrent samme omfang som den aktuelle kontrollmelding om aksesstillatelse (f.eks. radiomeldinger som viser 40 karakterer). Denne betydelige reduksjon i den resterende nyttbare ressurs, dvs. informasjonen, motvirker den økonomiske lønnsomhet som tilstrebes for kringkastingstjenesten.

Hensikten med den foreliggende oppfinnelse er å avbøte denne ulempe. For dette formål skaffer den foreliggende oppfinnelse en fremgangsmåte hvor programmet deles i samme antall programelementer som det er personlige sekvenser (video og/eller lyd og/eller data), idet elementene identifiseres av en identifikasjon som er individuell for deres mottager eller adressat og har et omkastet innhold basert på kontrollord som er spesifikt for hver mottager eller adressat og som garanterer hemmeligholdelsen av programsekvensene.

En kontrollmelding om en aksesstillatelse er forbundet med det kringkastede program og gjør det mulig for samtlige sikkerhetsprosessorer hos autoriserte brukere og på basis av kryptogrammet å rekonstituere et generelt kontrollord kjent som rotkontrollordet og identifikasjonen av hver mottager, idet det spesifikke kontrollord vil muliggjøre gjenoppretting av programelementene identifisert av den samme identifikasjon av mottageren.

Samtidig som den garanterer en total hemmeligholdelse for hvert av programelementene, gjør oppfinnelsen det mulig å kringkaste bare en enkelt kontrollmelding om adgangstillatelse på basis av hvilken alle mottagere programsekvenser kunne beregne det personlige kontrollord benyttet til den forutgående omkasting av informasjonen som angår dem.

En slik prosess gjør det mulig å vende tilbake til informasjonsrater som er identiske med de for betalingsfjernsynstjenester, nemlig noen få hundre byte/s.

Mer bestemt angår den foreliggende oppfinnelse en fremgangsmåte til overføring av programmer hvor programmene omkastes av et kontrollord og aksesskontrollmeldinger dannes og spesielt inneholder aksesskriterier og et kryptogram av kontrollordet, kjennetegnet ved at:

- for å adressere personlige programmer til forskjellige mottagere identifisert av identifikatorer, skaffes kontrollordet som benyttes til omkasting av programmer tiltenkt den bestemte mottager ved personliggjøring ved hjelp av identifikatoren for mottageren, av et enkelt kontrollord kalt rotkontrollordet og som gjelder alle mottagerne og bare en enkelt aksesskontrollmelding overføres for alle mottagerne, idet meldingen mer bestemt inneholder et kryptogram av rotkontrollordet.

Oppfinnelsen skal nå forklares nærmere i det følgende og med henvisning til den ledsagende tegning.

Fig. 1 viser på generell form de forskjellige operasjoner som utføres ved overføring.

Fig. 2 viser den generelle struktur av et kringkastet program.

Fig. 3 viser strukturen av kontrollmeldingen for en adgangstillatelse.

Fig. 4 viser på generell form de forskjellige operasjoner utført ved mottagning hos en aksessinnretning.

Fig. 5 viser den spesielle struktur av kontrollmeldingen for en aksesstillatelse.

Fig. 6 viser formatet av en melding om den alminnelige anvendbare dataprotokoll (GPD).

Fig. 7 viser strukturen av en meldingstittel.

Fig. 8 viser utvidelsen av en meldingstittel.

Fig. 9 viser et utvidet adressefelt.

Fig. 10 viser en første variant av anordningen som gjør det mulig å skaffe et personlig kontrollord ved overføring.

Fig. 11 viser en annen variant av anordninger som gjør det mulig å skaffe et personlig kontrollord.

Fig. 12 viser en første variant av anordningen som ved mottagning gjør det mulig å restaurere et personlig kontrollord når den første variant er blitt benyttet ved overføring for å skaffe det personlige kontrollord.

Fig. 13 viser en annen variant av anordningen som ved mottagning gjør det mulig å restaurere et personlig kontrollord når den annen variant er blitt benyttet ved overføringen for å skaffe det personlige kontrollord.

På fig. 1 og i andre generelle figurer såsom gjengivelser som fig. 4, 10, 11, 12, 13 etc. svarer de forskjellige blokkene som er vist til forskjellige operasjoner. Det må ikke forstås slik at disse operasjoner utføres av det samme antall uavhengige kretser. Fagmannen vil vite at disse operasjoner

vanligvis utføres på en generell basis av mikroprosessorer, både ved overføring og mottagning. Fig. 1 viser de vesentlige operasjoner som utføres ved overføring.

Henvisningsbokstavene (a, b, c, etc.) benyttet på fig. 1 svarer til følgende avsnitt:

a) programmet som skal overføres er delt i (n) programelementer kalt "personlige programelementer" (EPP1, EPP2, ... EPPn) tiltenkt (n) forskjellige adressater eller mottagere (D1, D2, ... Dn);

b) til hver mottager (D1, D2, ... Dn) allokeres en identifikator (ID1, ID2, ... IDn);

c) på slumpmessig måte dannes et kontrollord som gjelder alle mottagere og som kalles "rotkontrollordet" (MCR);

d) en tjenestenøkkel (CS) identifiseres av en tjenestenøkkelindentifikator (ICS);

e) på basis av kontrollordet (MCR) og tjenestenøkkelen (CS) dannes en algoritme, kjent som en krypterings- eller chiffreringsalogritme (AC) for å skaffe et kryptogram (CMCR) av rotkontrollordet;

f) på basis av rotkontrollordet (MCR), identifikasjon av mottagere (ID1, ID2, ... IDn) og tjenestenøkkelen (CS), dannes av en såkalt diversifikasjons-algoritme (AD) som leverer rotkontrollord individuelt til hver mottager (D1, D2, ... Dn) og som er kjent som "personlige kontrollord" (MCP1, MCP2, ... MCPn);

g) på basis av de personlige programelementer (EPP1, EPP2, ..., EPPn) og personlige kontrollord (MCP1, MCP2, ..., MCPn) svarende til forskjellige mottagere (D1, D2, ..., Dn) som det tas sikte på, omkastes de personlige programelementer (EPP1, EPP2, ..., EPPn) ved hjelp av henholdsvis de personlige kontrollord (MCP1, MCP2, ..., MCPn) for å skaffe omkastede personlige programelementer (EPPE1, EPPE2, ..., EPPEn);

h) til de omkastede personlige programelementene tilføyes identifikatorene for mottagerne (ID1, ID2, ..., IDn) for å konstituere programelementer (EP1, EP2, ..., EPn) individuelle for disse forskjellige mottagere;

i) aksesskriteriene (CA) som må tilfredsstilles for å ha rett til å benytte tjenestenøkkelen (CS) defineres;

j) på basis av identifikatoren for tjenestenøkkelen (ICS), kryptogrammet til kontrollordet (CMCR), aksesskriteriene (CA) og etter valg en signatur for kryptogrammet og aksesskriteriene (SIGN) dannes kontrollmeldinger (MCTA) for aksesstillatelse;

k) de omkastede programelementer (EP1, EP2, ..., EPn) og kontroll-meldingen (MCTA) for aksesstillatelse overføres.

Fig. 2 viser den generelle struktur av programelementer (EP1....EPn) med deres respektive mottageridentifikatorer (ID1, ..., IDn) forbundet med de respektive omkastede personlige programelementer (EPP1, ..., EPPEn). Det er til de (n) blokker mulig å tilføye en tjenestedatablokk (DS) som ikke er personlig (kringkastingstjeneste for et stort antall brukere) eller tjenestedata som gjør det mulig å beskrive tjenestens iboende struktur.

Kontrollmeldingen (MCTA) for aksesstillatelse som innbefatter aksess-kriteriene for programinformasjon som inneholder kryptogrammet av rotkontrollordet (CMCR), kan ha en struktur lik den på fig. 3, hvor det er mulig å se en tjenestenøkkelidentifikator (ICS) etterfulgt av aksesskriterier til tjenesten (CA), fulgt av kryptogrammet (CMCR) av rotkontrollordet og endelig og valgfritt signaturen (SIGN) for kriteriene for aksess og kryptogrammet av rotkontrollordet.

Sekvensen av operasjoner som utført i terminalen til en av mottagerne, dvs. en mottager av rang "i" (hvor "i" er et helt tall mellom 1 og n) er skjematisk vist på fig. 4. Disse operasjoner er definert i de følgende avsnitt hvor avsnittsnummeret igjen henviser til henvisningsbokstaven benyttet til å identifisere blokkene på tegningen.

l) hver mottager mottar de omkastede programelementer (EP1, EP2, ..., EPn) med deres mottageridentifikatorer (ID1, ID2, ..., IDn) og deres omkastede personlige programelementer (EPPE1, EPPE2, ..., EPPEn) og mottar også kontrollmeldinger (MCTA) for aksesstillatelse;

m)den bestemte mottager (Di) beholder blant programelementene som han mottar, dem som inneholder hans identifikator (IDi) som gir ham de omkastede personlige programelementer (EPPEi) tiltenkt ham;

n) denne bestemte mottager (Di) sjekker på basis av kontrollmeldingene (MCTA) for aksesstillatelse hvorvidt aksesskriteriene (CA) er oppfylt ved hans aksesstillatelse og hvis så, sjekker han integriteten av meldingen ved analyse av signaturen (SIGN) hvis denne er dannet ved overføring;

o) på basis av kryptogrammet (CMCR) av rotkontrollordet, tjenestenøkkelen (CS) og sin identifikator (IDi) danner mottageren (Di) en omvendt algoritme (AC^{-1}) av krypteringsalgoritmen (AC) dannet ved overføring i operasjon e) og danner også en algoritme (AD) som er diversifikasjonsalgoritmen (AD) dannet ved overføring i operasjon f) og endelig finner han sitt individuelle personlige kontrollord (MCPi);

p) mottageren (Di) gjenoppretter deretter de omkastede personlige programelementer (EPPEi) tiltenkt ham, mottatt etter operasjon m) på basis av det personlige kontrollord (MCPi), mottatt etter operasjon o) og får på ukodet form de personlige programelementer (EPPi) tiltenkt ham.

En utførelse skal nå beskrives og gjelder signaler av familien MAC/pakke-EUROCRYPT (innbefattet i fullkanal-datakringkastingsmetoden).

Strukturen av kontrollmeldingene for aksesstillatelse er som definert i spesifikasjonen for det betingede aksessystem EUROCRYPT som gjelder signaler i MAC/pakke-familien. Det er vist på fig. 5. Tjenestenøkkel-0identifikatoren (ICS) angir en hemmelig nøkkel (CS) og omfatter tre byter aksesskriterier (CA) og et variabelt bytetall, kryptogrammet eller kryptogrammene (CMCR) av rotkontrollordet funnet ved hjelp av den hemmelige nøkkel (CS) strekker seg over 8 eller 16 byter og signaturen strekker seg over 8 byter. Denne signaturen er resultatet av en kompresjons-algoritme anvendt på informasjonen som foreligger i kontrollmeldingen for aksesstillatelse (kontrollordkryptogrammet eller -kryptogrammene og aksesskriteriene) ved bruk av den hemmelige nøkkel (CS).

Formatene på meldingene som svarer til kringkastingen av de digitale data (teletekst, lyd, etc.) er beskrevet i del 4C av spesifikasjonsdokumentet for en MAC/pakke-signal under overskriften "General Purpose Data Protocol (GPD)". Strukturen av disse meldingene er vist på fig. 6, hvor meldingen omfatter totalt 45 byter med en variabel meldingstittel, et variabelt datasegment og et feildeteksjonskodefelt "Cyclic Redundancy Code" (CRC) på valgfri form.

Meldingsoverskriften eller "hodet" er vist på fig. 7 med en formatkatalog eller -deskriptor på en byte og en meldingstittelutvidelse av variabel lengde. Deskriptoren definerer hvorvidt meldingstittelutvidelsesfeltet foreligger, om segmenttelleren foreligger og om adressefeltet foreligger.

Fig. 8 viser utvidelsen av meldingstittelen med et variabelt utvidet adressefelt, en valgfri segmentteller på fire byter og en valgfri segmentlengde på tre byter.

Endelig viser fig. 9 det utvidede adressefelt med en adresselengde på en byte og en utvidet adresse med variabel lengde.

Det foreslås å identifisere meldinger i GPD-format ved i det "utvidede adressefelt" å definere den enkelte fem byters adresse (UA) såsom beskrevet i EUROCRYPT-spesifikasjonen. Denne adressen definerer på en entydig måte hver av sikkerhetsprosessorene til brukerne.

Det skal bemerkes at identifikasjonsprosessen for meldingen også kan integreres på meldingens "applikasjonsnivå", dvs. avhengig av arten av informasjonene som utveksles innenfor datasegmentene.

Fig. 10 og 11 viser to av de mulige varianter for å skaffe et personlig kontrollord på basis av enten rotkontrollordet eller kryptogrammet av rotkontrollordet. Disse to varianter benyttes ved overføring. Til dem svarer de to viste varianter ved mottagning og som vil beskrives i forbindelse med fig. 12 og 13.

I varianten vist på fig. 10 benyttes for i den ovennevnte operasjon f) å danne personlige kontrollord (MCP1, MCP2, ..., MCPn) på basis av rotkontrollordet (MCR) for å identifisere mottagere definert av en enkelt adresse (UA) og tjenestenøkkelen (CS), diversifikasjonsalgoritmen (AD) på rotkontrollordet med den enkelte adresse (UA) for mottageren som diversifikasjonsparameteren. For å skaffe kryptogrammet av rotkontrollordet finner det sted en benyttelse av krypteringsalgoritmen (AC) på rotkontrollordet (MCR) med bruk av tjenestenøkkelen (CS) som krypteringsparameteren.

I varianten på fig. 11 benyttes diversifikasjonsalgoritmen (AD) på tjenestenøkkelen (CS) med den enkelte eller entydige adresse som diversifikasjonsparameter, hvilken gir den personlige tjenestenøkkelen (CSP). Dette etterfølges av bruken av dekrypteringsalgoritmen (AC^{-1}) på kryptogrammet

av rotkontrollordet (CMCR) med den personlige tjenestenøkkel (CSP) som krypteringsparameter.

For på basis av kryptogrammet (CMCR) av rotkontrollordet, tjenestenøkkelen (CS) og adressen (UA) å skaffe det personlige kontrollord (MCPi) individuelt for mottageren (Di), er i tilfelle av den første variant vist på fig. 12 er det første trinn ved mottagning å benytte den omvendte dekrypteringsalgoritme (AC^{-1}) på kryptogrammet av rotkontrollordet (CMCR), med bruk av tjenestenøkkelen som dekrypteringsparameter, hvilket gir rotkontrollordet (MCR) fulgt av bruken på det siste av det omvendte diversifikasjonsalgoritme (AD) med bruk av den enkelte adresse (UA) som diversifikasjonsparameter, hvilket endelig gir det personlige kontrollord (MCPi) individuelt for mottageren.

For fra kryptogrammet (CMCR) for rotkontrollordet, tjenestenøkkelen (CS) og den individuelle adresse (UA) å skaffe et personlig kontrollord individuelt for mottageren, er i den annen variant vist på fig. 13 er det første trinn å anvende diversifikasjonsalgoritmen (AD) på tjenestenøkkelen (CS) med adressen (UA) som diversifikasjonsparameteren, hvilket gir den personlige tjenstenøkkel (CSP). Dette følges av bruken av dekrypteringsalgoritmen (AC^{-1}) på kryptogrammet (CMCR) for rotkontrollordet med den personlige tjenestenøkkel (CSP) som dekrypteringsparameteren, hvilket til slutt gir det personlige kontrollord (MCPi) individuelt for mottageren (Di).

Uansett hvilken variant som benyttes, tas etter at det personlige kontrollord er skaffet, i bruk en pseudoslumpgenerator som leverer dekrypteringssekvenser svarende til krypteringssekvensene brukt ved overføring.

Anordningen for omkasting og gjenoppretting av datasegmentene kan konvensjonelt bestå av eksklusiv-ELLER-porter, hvorav en inngang mottar enkrypterings/dekrypteringssekvensene og den andre ukodede/omkastede data og hvis utgang leverer de omkastede/ukodede data.

I en praktiske utførelse blir behandlingen utført av den betingede overførings/mottagningsaksessinnretning integrert utført av en sikkerhetsprosessor (smartkort) med en rate lik eller mindre enn 2400 baud (ved eksisterende smartkortteknologier). Prosessoren leverer enkrypterings/-dekrypteringssekvensene som skal anvendes på dataene som skal omkastes/gjenopprettes. I tilfelle av den høyere rate blir den pseudoslump-

messige genererende funksjon overført til terminalen og prosessoren leverer de personlige kontrollord.

PATENTKRAV

1. Fremgangsmåte til overføring av programmer hvor programmene omkastes av et kontrollord og aksesskontrollmeldinger dannes og spesielt inneholder aksesskriterier og et kryptogram av kontrollordet, hvor fremgangsmåten er
karakterisert ved at for å adressere personlige programmer til forskjellige mottagere identifisert av identifikatorer, skaffes kontrollordet som benyttes til omkasting av programmer tiltenkt den bestemte mottager ved personliggjøring ved hjelp av identifikatoren for mottageren, av et enkelt kontrollord kalt rotkontrollordet og som gjelder alle mottagerne og bare en enkelt aksesskontrollmelding overføres for alle mottagerne, idet meldingen mer bestemt inneholder et kryptogram av rotkontrollordet.

2. Fremgangsmåte i henhold til krav 1,
karakterisert ved at den omfatter følgende operasjoner:

a) å dele programmet som skal overføres i (n) programelementer kalt personlige programelementer (EPP1, EPP2, ..., EPPn) tiltenkt samme antall (n) av forskjellige mottagere (D1, D2, ..., Dn);

b) å allokere til hver mottager (D1, D2, ..., Dn) en identifikator (ID1, ID2, ..., IDn);

c) å danne på en slumpmessig måte et kontrollord som gjelder alle mottagere og som kalles rotkontrollord (MCR);

d) å definere en tjenestenøkkel (CS) defineres av en tjenestenøkkelidentifikator (ICS);

e) å danne på basis av rotkontrollordet (MCR) og tjenestenøkkelen (CS) en krypteringsalgoritme (AC) for å skaffe et kryptogram (CMCR) av rotkontrollordet,

f) å danne på basis av rotkontrollordet (MCR) eller kryptogrammet (CMCR) av rotkontrollordet, identifikasjonen av mottagerne (ID1, ID2, ..., IDn) og tjenestenøkkelen (CS), en diversifikasjonsalgoritme (AD) som for hver mottager (D1, D2, ..., Dn) leverer individuelle kontrollord kalt personlige kontrollord (MCP1, MCP2, ..., MCPn);

g) å omkaste på basis av de personlige programelementene (EPP1, EPP2, ..., EPPn) og personlige kontrollord (MCP1, MCP2, ..., MCPn) svarende til de forskjellige mottagere (D1, D2, ..., Dn) som det tas sikte på, de personlige programelementer (EPP1, EPP2, ..., EPPn) ved hjelp av henholdsvis de personlige kontrollord (MCP1, MCP2, ..., MCPn) for å skaffe omkastede personlige programelementer (EPP1, EPP2, ..., EPPn);

h) å tilføye til disse omkastede personlige programelementer identifikatoren (ID1, ID2, ..., IDn) for mottagerne for å danne programelementer (EP1, EP2, ..., EPn) individuelle for de forskjellige mottagere;

i) å definere aksesskriterier (CA) som må tilfredsstilles for å ha rett til å benytte tjenstenøkkelen (CS);

j) å danne på basis av kryptogrammet (CMCR) for rotkontrollordet, tjenestenøkkelidentifikatoren (ICS), aksesskriteriene (CA) og etter valg en signatur (SIGN) for kryptogrammet og aksesskriteriene, kontrollmeldinger (MCTA) for aksesstillatelse;

k) å overføre programelementene (EP1, EP2, ..., EPn) og kontrollmeldingen (MCTA) for aksesstillatelsen.

3. Fremgangsmåte i henhold til krav 2,
k a r a k t e r i s e r t v e d at for i operasjonen f) å skaffe personlige kontrollord (MCP1, MCP2, ..., MCPn) på basis av rotkontrollordene (MCR), identifikasjon av mottagerne (ID1, ID2, ..., IDn) og tjenestenøkkelen (CS), benyttes diversifikasjonsalgoritmen (AD) på rotkontrollordet med tjenestenøkkelen (CS) og den enkelte adresse (UA) for mottageren som diversifikasjonsparameter.

4. Fremgangsmåte i henhold til krav 2,
k a r a k t e r i s e r t v e d at for i operasjon f) å skaffe personlige kontrollord (MCP1, MCP2, ..., MCPn) fra rotkontrollordet (MCR), mottageridentifikatorene (ID1, ID2, ..., IDn) og tjenestenøkkelen (CS), benyttes diversifikasjonsalgoritmen (AD) på tjenestenøkkelen (CS) med den enkelte eller entydige adresse som diversifikasjonsparameter, hvilket gir en personlig tjenestenøkkel (CSP) og deretter benyttes dekrypteringsalgoritmen (AC^{-1}) for rotkontrollordkryptogrammet (CMCR) med bruk av den personlige tjenestenøkkel (CSP) som dekrypteringsparameter.

5. Fremgangsmåte til mottagning av programmer overført i henhold til fremgangsmåten som angitt i krav 1, hvor det gjøres en sjekk for å finne ut hvorvidt aksesskriteriene er oppfylt, kontrollordet benyttet til omkasting rekonstitueres og de mottatte programmer gjenopprettes, og hvor fremgangsmåten er
k a r a k t e r i s e r t v e d at hver mottager ved hjelp av sin identifikator og aksesskontrollmeldingen på basis av rotkontrollordet rekonstituerer sitt eget personlige kontrollord som setter ham, og ham alene, i stand til å gjenopprette programmet tiltenkt ham.

6. Fremgangsmåte for mottagning av programmer overført i henhold til fremgangsmåten som angitt i krav 2,
k a r a k t e r i s e r t v e d at:

l) hver mottager mottar programelementene (EP1, EP2, ..., EPn) med deres mottageridentifikatorer (ID1, ID2, ..., IDn) og deres omkastede personlige programelementer (EPPE1, EPPE2, ..., EPPEn) og som mottar en kontrollmelding (MCTA) for adgangstillatelse; hvor

m)en bestemt mottager (Di) av de mottatte programelementer beholder dem som inneholder identifikatoren (IDi) som svarer til ham og som gir ham de personlige programelementer (EPPEi) tiltenkt ham;

n) på basis av kontrollmeldingene (MCTA) for aksesstillatelser sjekker mottageren (Di) hvorvidt aksesskriteriene (CA) er oppfylt ved hans aksesstillatelse og hvis så, sjekker han integriteten av meldingen ved å analysere signaturen hvis den siste er blitt dannet ved overføring;

o) på basis av kryptogrammet (CMCR) av rotkontrollordet, tjenestenøkkelen (CS) og sin identifikator (IDi) danner mottageren (Di) den ovendte algoritme (AC^{-1}) av krypteringsalgoritmen (AC) dannet ved overføring i operasjonen e) og danner diversifikasjonsalgoritmen (AD) dannet ved overføring i operasjonen f) for igjen å finne sitt personlige kontrollord (MCPi);

p) mottageren (Di) gjenoppretter deretter de omkastede personlige programelementer (EPPEi) tiltenkt ham og dannet etter operasjonen m) på basis av det personlige kontrollord (MCPi) dannet etter operasjon o) og får på ukodet form de personlige programelementer.

7. Fremgangsmåte i henhold til krav 6, karakterisert ved at for i operasjon o) fra kryptogrammet (CMCR) av rotkontrollordet, tjenestenøkkel (CS) og identifikatoren (Idi) å danne det personlige kontrollord individuelt for ham, starter mottageren (Di) med å benytte på kryptogrammet (CMCR) for rotkontrollordet, dekrypteringsalgoritmen (AC^{-1}) som er den omvendte av krypteringsalgoritmen (AC) med bruk av tjenestenøkkelen (CS) som parameter, hvilket gir ham rotkontrollordet (MCR) og han benytter deretter diversifikasjonsalgoritmen (AD) på den sistnevnte med bruk av den enkelte adresse (UA) som diversifikasjonsparameter, hvilket til slutt gir ham hans individuelle personlige kontrollord (MCPi) (fig. 12).

8. Fremgangsmåte i henhold til krav 6, karakterisert ved at for i operasjon o) fra kryptogrammet (CMCR) for rotkontrollordet, tjenestenøkkelen (CS) og identifikatoren (IDi) å danne det personlige kontrollord (MCPi) som er individuelt for ham, starter mottageren (Di) med å benytte diversifikasjonsalgoritmen (AD) på tjenestenøkkelen (CS) med adressen (UA) som diversifikasjonsparameter, hvilket gir ham den personlige tjenestenøkkel (CSP) og han benytter deretter dekrypteringsalgoritmen (AC^{-1}) på kryptogrammet (CMCR) for rotkontrollordet med den personlige tjenestenøkkel (CSP) som dekrypteringsparameteren, hvilket til slutt gir ham det personlige kontrollord (MCPi) som er individuelt for ham (fig. 13).

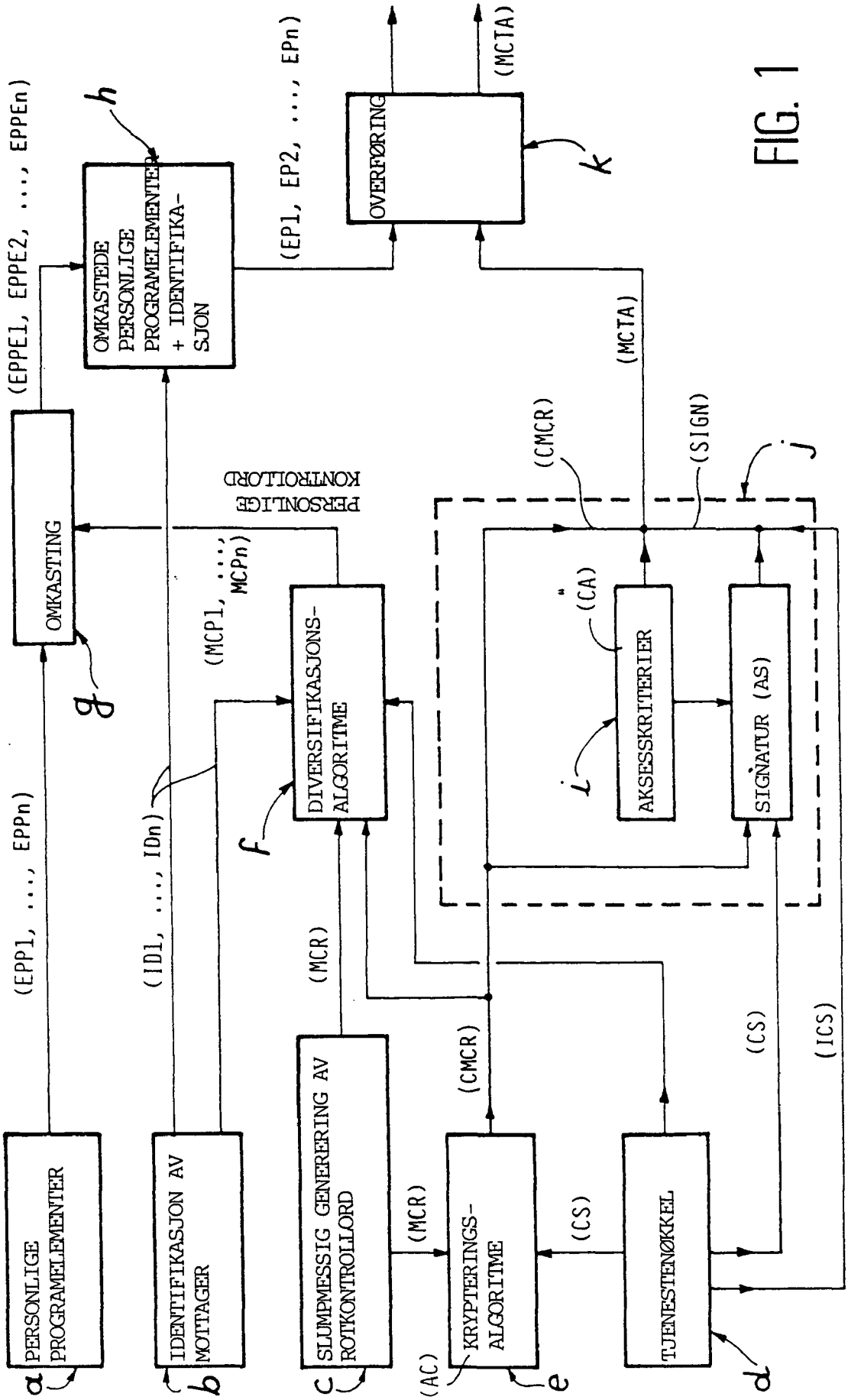

PERSONLIGE PROGRAMELEMENTER
IDENTIFIKASJON AV MOTTAGER
SLUMPMESSIG GENERERING AV ROTKONTROLLORD
KRYPTERINGS-ALGORITME
TJENESTENØKKEL
DIVERSIFIKASJONS-ALGORITME
AKSESSKRITERIER
SIGNATUR (AS)
OMKASTING
OMKASTEDE PERSONLIGE PROGRAMELEMENTER + IDENTIFIKA-SJON
OVERFØRING
PERSONLIGE KONTROLLORD
(EPP1, ..., EPPn)
(ID1, ..., IDn)
(MCR)
(AC)
(CS)
(ICS)
(CMCR)
(MCP1, ..., MCPn)
(CA)
(SIGN)
(MCTA)
(EP1, EP2, ..., EPn)
(EPPE1, EPPE2, ..., EPPEn)
a
b
c
d
e
f
g
h
i
j
k

FIG. 1

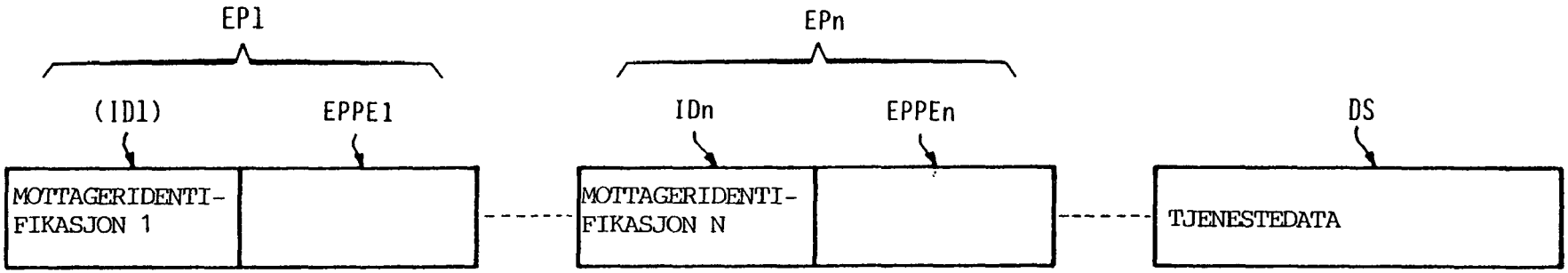

EP1
EPn
(ID1)
EPPE1
IDn
EPPEn
DS
MOTTAGERIDENTI-
FIKASJON 1
MOTTAGERIDENTI-
FIKASJON N
TJENESTEDATA

FIG. 2

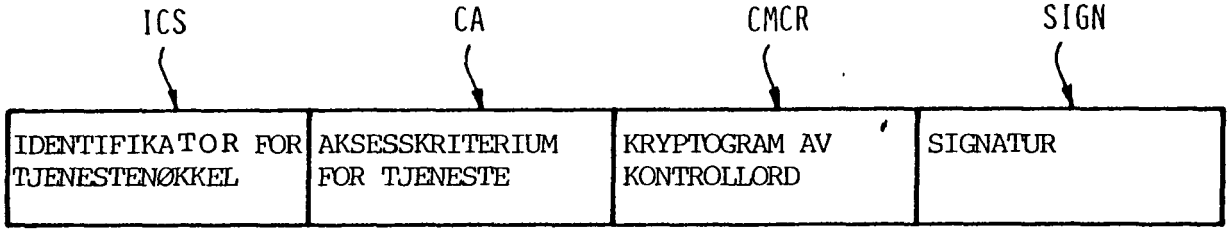

ICS
CA
CMCR
SIGN
IDENTIFIKATOR FOR
TJENESTENØKKEL
AKSESSKRITERIUM
FOR TJENESTE
KRYPTOGRAM AV
KONTROLLORD
SIGNATUR

FIG. 3

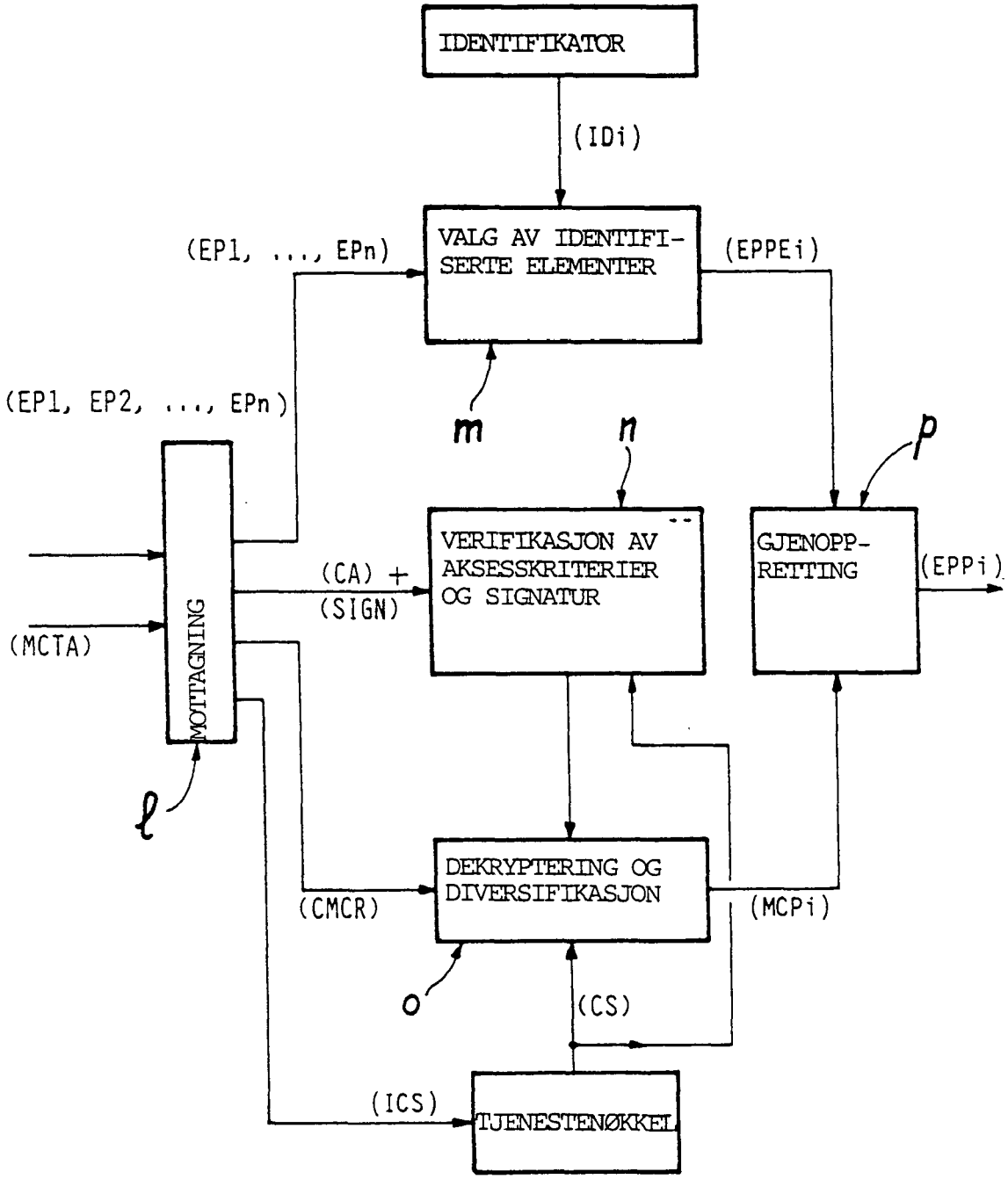

IDENTIFIKATOR
(IDi)
VALG AV IDENTIFI-SERTE ELEMENTER
(EP1, ..., EPn)
(EPPEi)
(EP1, EP2, ..., EPn)
m
n
p
VERIFIKASJON AV AKSESSKRITERIER OG SIGNATUR
GJENOPP-RETTING
(EPPi)
(CA) +
(SIGN)
(MCTA)
MOTTAGNING
l
DEKRYPTERING OG DIVERSIFIKASJON
(CMCR)
(MCPi)
o
(CS)
(ICS)
TJENESTENØKKEL

FIG. 4

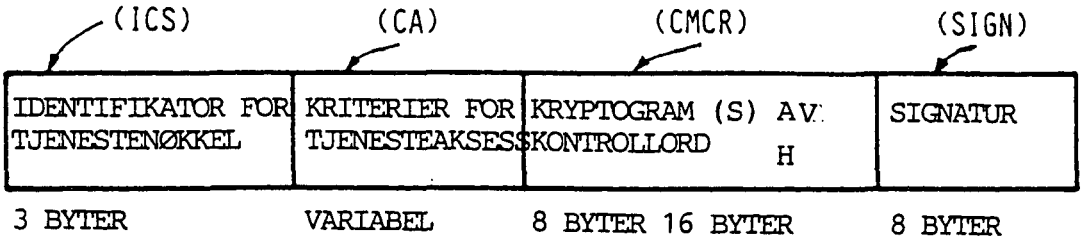


FIG. 5

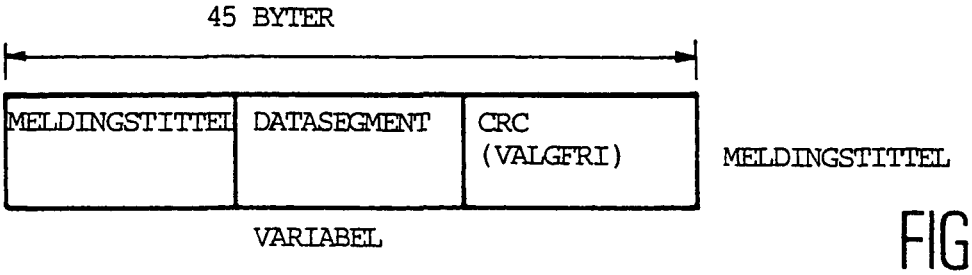


FIG. 6

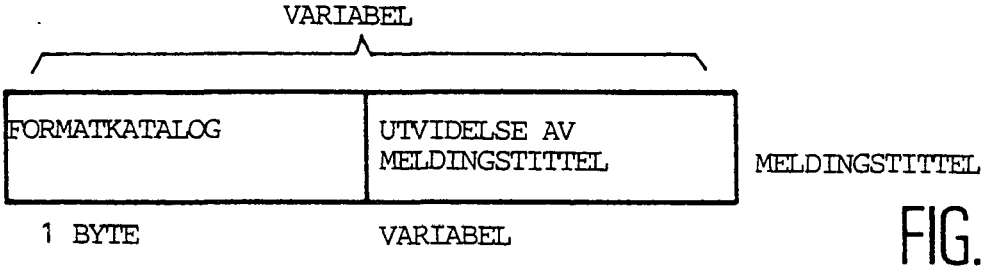


FIG. 7

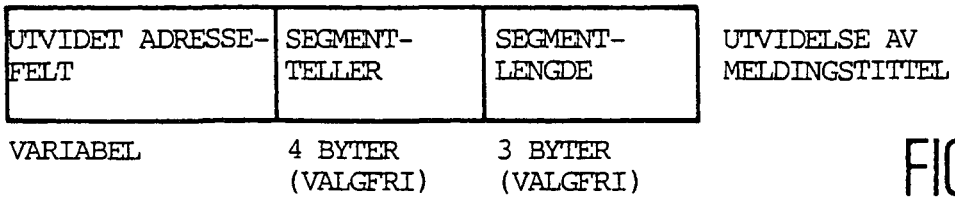


FIG. 8

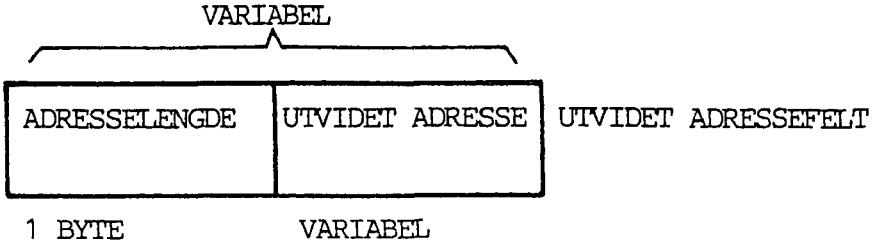


FIG. 9

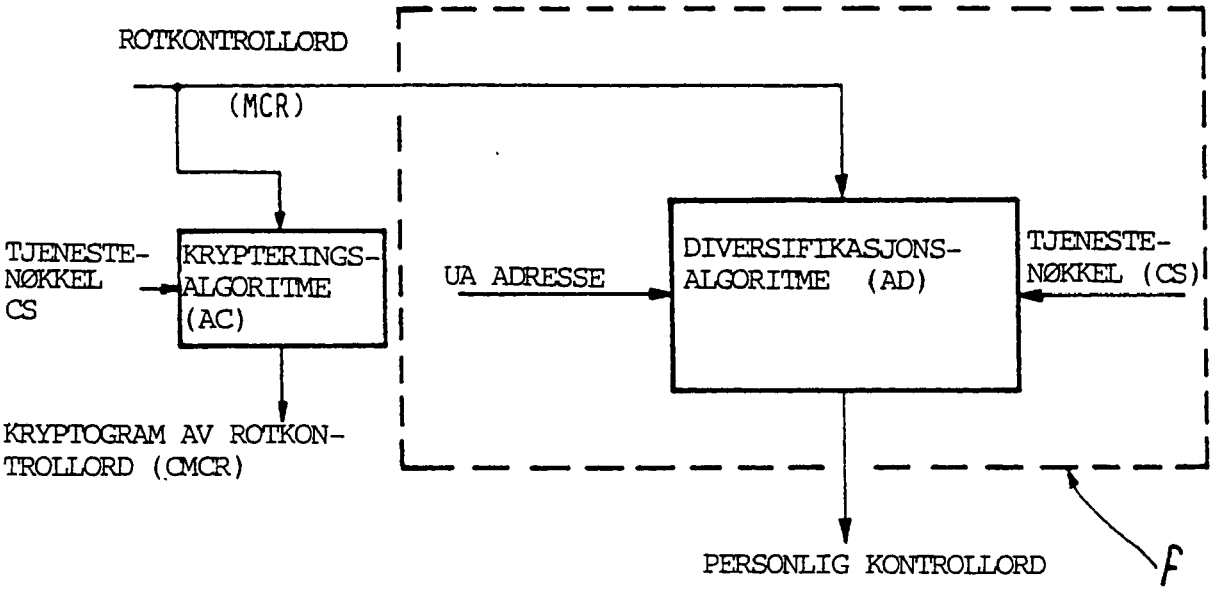

ROTKONTROLLORD
(MCR)
TJENESTE-
NØKKEL
CS
KRYPTERINGS-
ALGORITME
(AC)
KRYPTOGRAM AV ROTKON-
TROLLORD (CMCR)
UA ADRESSE
DIVERSIFIKASJONS-
ALGORITME (AD)
TJENESTE-
NØKKEL (CS)
PERSONLIG KONTROLLORD
F

FIG. 10

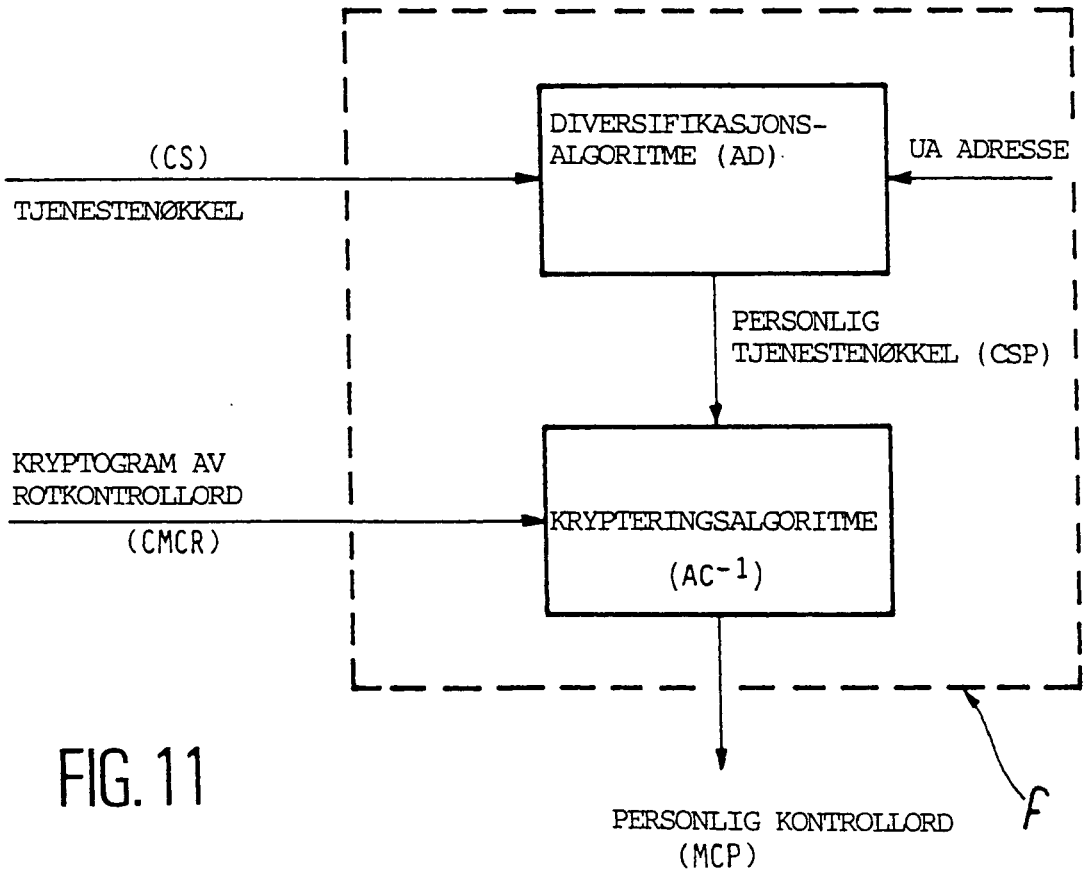

(CS)
TJENESTENØKKEL
DIVERSIFIKASJONS-
ALGORITME (AD)
UA ADRESSE
PERSONLIG
TJENESTENØKKEL (CSP)
KRYPTOGRAM AV
ROTKONTROLLORD
(CMCR)
KRYPTERINGSALGORITME
(AC-1)
PERSONLIG KONTROLLORD
(MCP)
F

FIG. 11

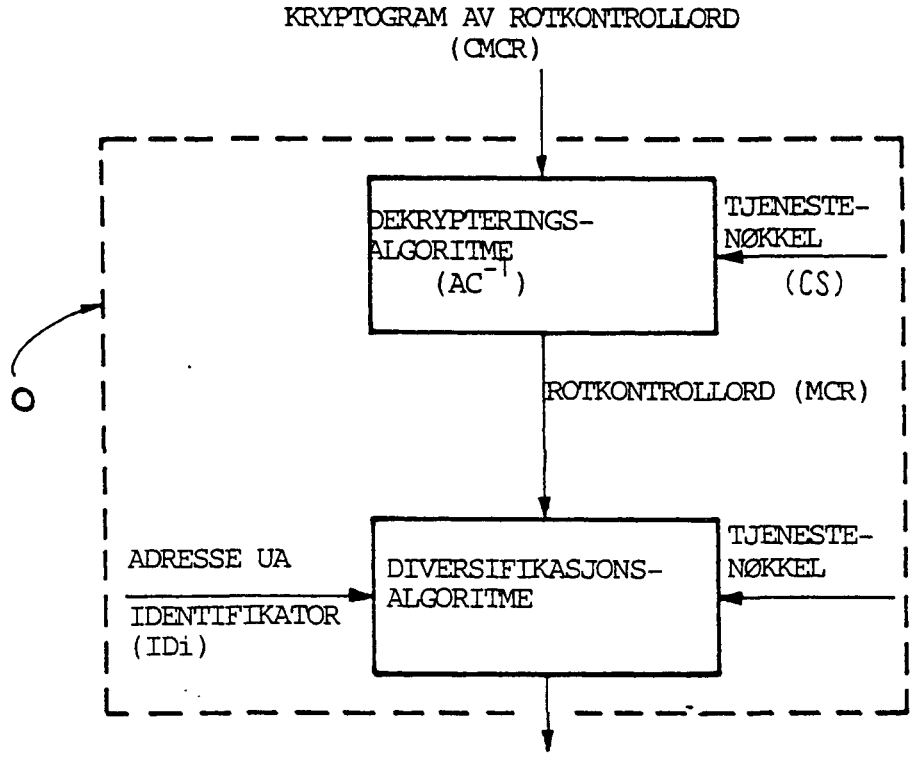

KRYPTOGRAM AV ROTKONTROLLORD
(CMCR)
DEKRYPTERINGS-
ALGORITME
(AC⁻¹)
TJENESTE-
NØKKEL
(CS)
ROTKONTROLLORD (MCR)
ADRESSE UA
IDENTIFIKATOR
(IDi)
DIVERSIFIKASJONS-
ALGORITME
TJENESTE-
NØKKEL
PERSONLIG KONTROLLORD (MCPi)

FIG. 12

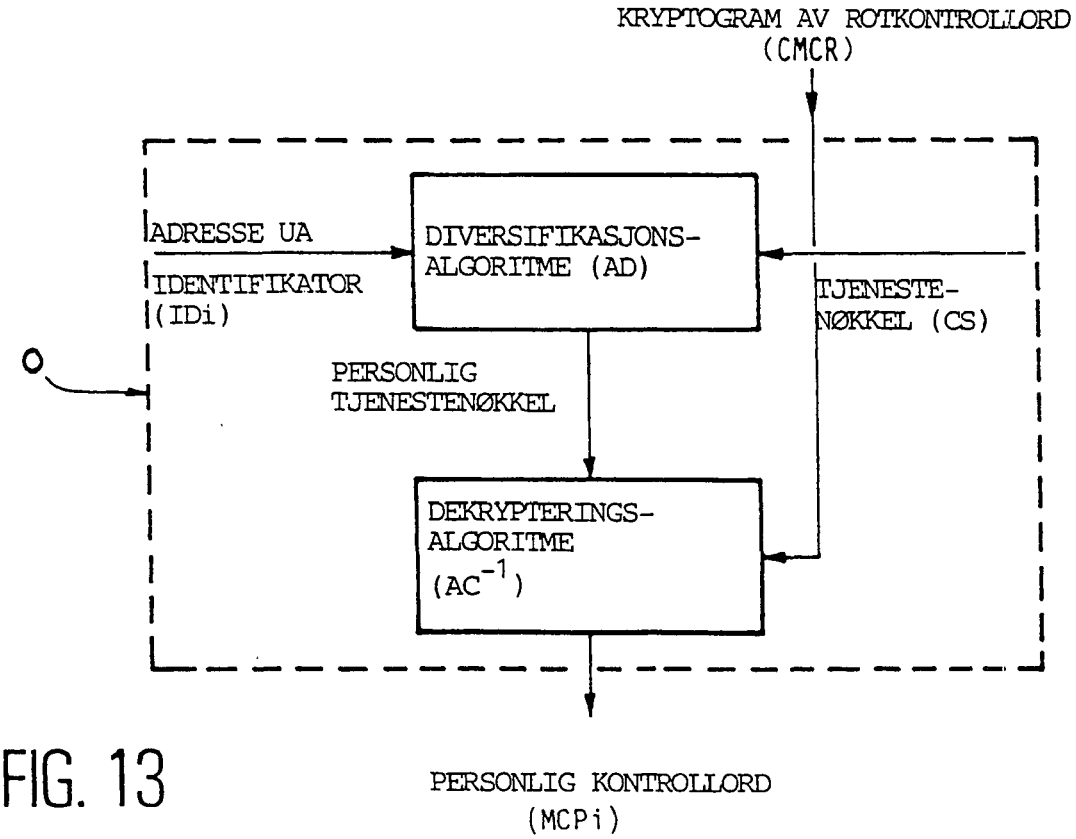

KRYPTOGRAM AV ROTKONTROLLORD
(CMCR)
ADRESSE UA
IDENTIFIKATOR
(IDi)
DIVERSIFIKASJONS-
ALGORITME (AD)
TJENESTE-
NØKKEL (CS)
PERSONLIG
TJENESTENØKKEL
DEKRYPTERINGS-
ALGORITME
(AC⁻¹)
PERSONLIG KONTROLLORD
(MCPi)

FIG. 13