(19) DANMARK

(11) **DK 174885 B1**

(12) PATENTSKRIFT

Patent- og
Varemærkestyrelsen

(51) Int.Cl[7].: **H 04 L 9/32** **H 04 N 7/14**

(21) Patentansøgning nr: **PA 1988 02547**

(22) Indleveringsdag: **1988-05-09**

(24) Løbedag: **1987-09-08**

(41) Alm. tilgængelig: **1988-05-09**

(45) Patentets meddelelse bkg. den: **2004-01-19**

(86) International ansøgning nr: **PCT/US87/02301**

(86) International indleveringsdag: **1987-09-08**

(85) Videreførelsesdag: **1988-05-10**

(30) Prioritet: **1986-09-10 US 905775**

(73) Patenthaver: **The Titan Corporation, 3033 Science Park Road, San Diego, California 92121, USA**
General Instrument Corporation, 101 Tournament Drive, Horsham, Pennsylvania 19044, USA

(72) Opfinder: **Ron D. Katznelson, 3913 Caminito Del Mar Surf, San Diego, California 92130, USA**

(74) Fuldmægtig: **Chas. Hude A/S, H.C. Andersens Boulevard 33, 1780 København V, Danmark**

(54) Benævnelse: **Brugerterminal for dataudtag og anordninger til at regulere et sådant udtag**

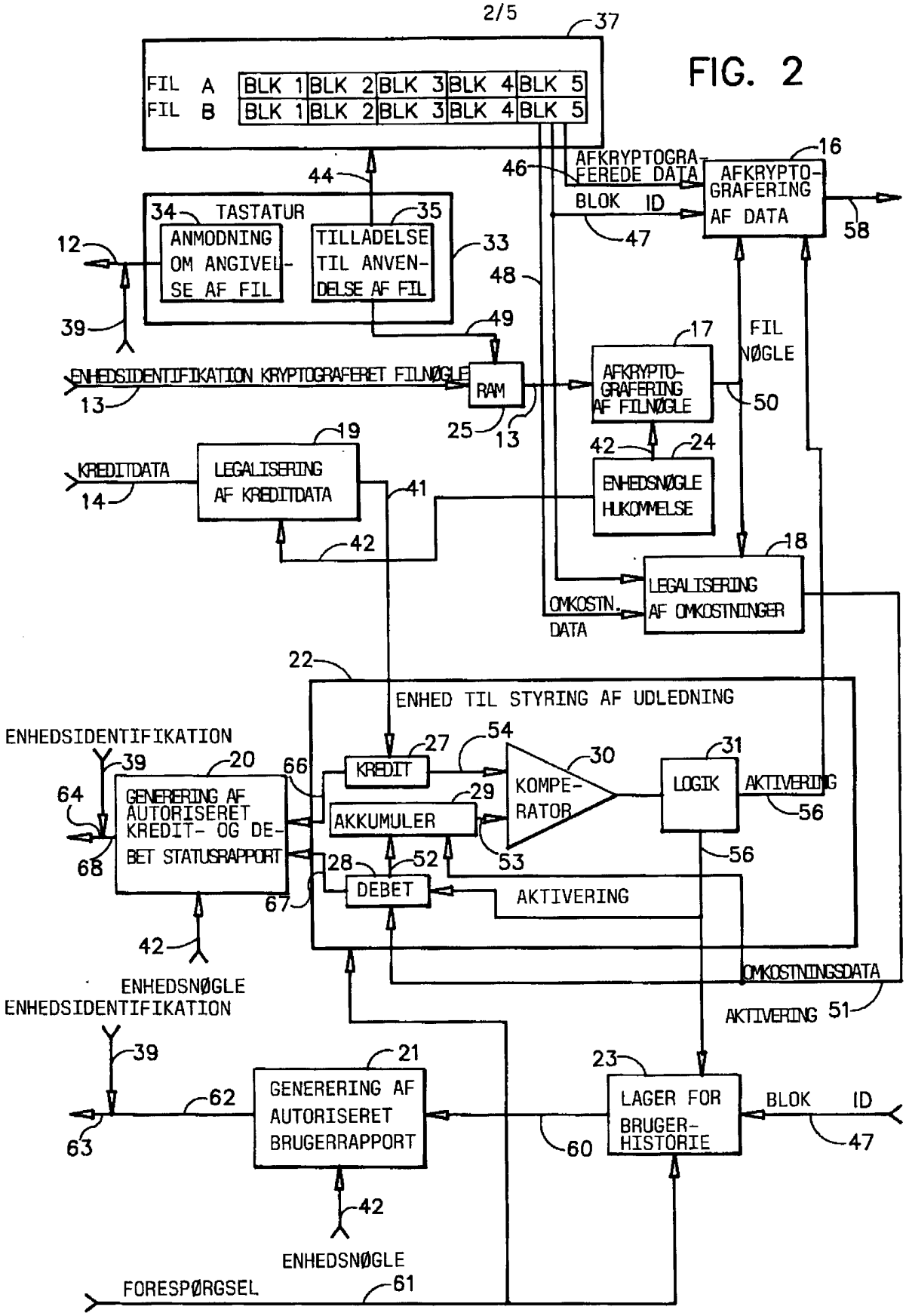
(56) Fremdragne publikationer:
GB A 2136175
EP A1 0135422

(57) Sammendrag:

System til styring og administration for udledning af data fra en CD-ROM hukommelse indeholdende kryptograferede datafiler, hvorfra udledningen må være autoriseret. Systemet omfatter en autorisations- og nøglefordelingsterminal og et antal kundedataudledningsterminaler med sådanne hukommelser (37). Autorisationsterminalen autoriserer en udledning af data ved autoriserede kundeterminaler, ved at der til de autoriserede kundeterminaler tilføres en kryptogfrafinøgle (13), der muliggør en udledning af data, og et autoriseret kreditsignal (14) til brug ved begrænsning af den datamængde, der skal udledes fra filerne. Kryptografinøglen er kryptograferet for kommunikation til kundeterminalerne i unikke enhedsnøgler (42), der er lagret (ved 24) i de respektive kundeterminaler. Kundeterminalen begrænser (ved 22) datamængden udledt fra filerne i overensstemmelse med kreditsignalet, registrerer (ved 23) mængden af data udledt fra filerne og tilfører til autorisationsterminalen en legaliseret rapport (62) af den registrerede datamængde udledt fra filerne. Hukommelsen (37) indeholder datafiler af forskellige datakøbere, og kundeterminalen registrerer separat (ved 23) udledningen af data fra filerne af de forskellige købere.

fortsættes

FIG. 2


37
FIL A
FIL B
BLK 1
BLK 2
BLK 3
BLK 4
BLK 5
44
46
AFKRYPTOGRAFERET DATA
BLOK ID
16
AFKRYPTOGRAFERING AF DATA
58
47
34
TASTATUR
35
ANMODNING OM ANGIVELSE AF FIL
TILLADELSE TIL ANVENDELSE AF FIL
33
12
39
48
49
17
FIL NØGLE
ENHEDSIDENTIFIKATION KRYPTOGRAFERET FILNØGLE
RAM
AFKRYPTOGRAFERING AF FILNØGLE
13
25
13
50
42
24
ENHEDSNØGLE HUKOMMELSE
19
KREDITDATA
LEGALISERING AF KREDITDATA
14
41
42
18
LEGALISERING AF OMKOSTNINGER
OMKOSTN. DATA
22
ENHED TIL STYRING AF UDLEDNING
ENHEDSIDENTIFIKATION
39
20
66
27
54
30
31
KREDIT
KOMPERATOR
LOGIK
AKTIVERING
64
GENERERING AF AUTORISERET KREDIT- OG DEBET STATUSRAPPORT
29
AKKUMULER
56
68
28
52
53
56
DEBET
AKTIVERING
67
42
ENHEDSNØGLE
OMKOSTNINGSDATA
ENHEDSIDENTIFIKATION
AKTIVERING 51
39
21
23
62
GENERERING AF AUTORISERET BRUGERRAPPORT
LAGER FOR BRUGERHISTORIE
BLOK ID
63
60
47
42
ENHEDSNØGLE
FORESPØRGSEL
61

Opfindelsen angår en brugerterminal for udtag af data, omfattende en hukommelse der kan indeholde krypterede datafiler, og hvorfra udtag af data må autoriseres, og en enhed til at regulere og holde regnskab med udtag af data fra datafilerne, idet terminalen er indrettet til at kunne kommunikere med en fjerntliggende central terminal og omfatter en autoriseringsenhed for at tillade udtag af data ved at frembringe en krypteringsnøgle, som muliggør udtag af data fra nævnte datafiler og dekryptering af disse.

Fra GB-2-136175 kendes en fremgangsmåde til at styre udledningen af data fra et lager, hvorved der frembringes et lager indeholdende en krypteret datafil, hvorfra udledning af data skal autoriseres ved at tilvejebringe en krypteringsnøgle, der åbner for udledningen af de pågældende data. Midler til begrænsning af den udtagne datamængde er imidlertid ikke angivet.

Fra EP-0-135422 er det endvidere kendt at regulere mængden af udledte data fra en datafil i en hukommelse, hvor udledningen autoriseres ved at frembringe et kreditsignal, der anvendes til at begrænse den mængde data, som kan udtages fra datafilen. Der er ikke angivet midler til beskyttelse af de udledte data eksempelvis ved anvendelse af kryptering.

Formålet med opfindelsen er at anvise, hvorledes udledning af data kan gøres mere sikker og lettere at kontrollere end hidtil kendt.

En brugerterminal af den indledningsvis nævnte art er ifølge opfindelsen ejendommelig ved, at autoriseringsenheden er indrettet til at frembringe et kreditsignal til at begrænse den datamængde, som kan udtages fra datafiler, idet brugerterminalen desuden omfatter

- en reguleringsenhed for i afhængighed af kreditsignalet at begrænse den mængde data, som kan udtages fra datafilerne,
- en registreringsenhed til at holde regnskab med den nævnte dataenhed ved at registrere den mængde data, som er udtaget fra datafilerne,
- en rapporteringsenhed til at oprette en autentisk brugsrapport med hensyn til den registrerede datamængde, som er udtaget fra datafilerne, og

- en enhed til at sende den autentiske brugsrapport til den fjerntliggende centrale terminal med henblik på fakturering.

Derved opnås midler til at regulere, begrænse og kontrollere den datamængde, som indehaveren af en given krypteringsnøgle er i stand til at udlede fra en given datafil, idet organerne til at autorisere udledningen af data ved hjælp af en krypteringsnøgle giver en vis sikkerhed, mens kreditsignalet til begrænsning af udledningen af data giver en yderligere sikkerhed.

Underkravene angår særlig hensigtsmæssige udførelsesformer for opfindelsen.

Opfindelsen skal nærmere forklares i det følgende under henvisning til tegningen, hvor

fig. 1 viser et blokdiagram, der illustrerer signaludvekslingen imellem en autorisations- og en nøglefordelingsterminal og en brugerterminal i en foretrukken udførelsesform for opfindelsen,

fig. 2 et diagram over brugerterminalen i fig. 1,

fig. 3 et rutediagram til illustration af rutinerne i en alternativ udførelsesform for opfindelsen,

fig. 4 et rutediagram til illustration af rutinerne i en anden udførelsesform for opfindelsen,

fig. 5 et rutediagram til illustration af visse aspekter ved rutinerne i en anden udførelsesform for opfindelsen,

fig. 6 et blokdiagram til illustration af brugen af en brugerterminal i en persondatamat til udledning af data fra en CD-ROM og

fig. 7 et skema til rækkeanbringelse af forskellige typer af datafelter i en hukommelse i en foretrukken udførelsesform for opfindelsen.

Det i fig. 1 viste system omfatter en autorisations- og nøglefordelingsterminal 10 og en brugerterminal 11 ifølge opfindelsen. Det er underforstået, at der i praksis er et antal brugerterminaler 11, der kommunikerer med en enkelt central autorisations- og nøglefordelingsterminal 10. En hukommelse indeholdende en krypteret datafil, fra hvilken udledning må være autoriseret, fyldes i brugerterminalen 11. Forskellige datafiler i hukommelsen kan være associeret med forskellige datakøbere. Kommunikationer mellem autorisations- og nøglefordelingsterminalen 10 og bruger-terminalen 11 transmitteres typisk over telefonlinier.

Til opnåelse af autorisation til udledning af krypterede data fra en given fil lagret i hukommelsen i brugerterminalen 11 foranlediger kunden, at et filanmodningssignal 12 kommunikeres til autorisations- og nøglefordelingsterminalen 10. Filanmodningssignalet identificerer filen, for hvilken der anmodes om autorisation, og indeholder også et ID- nummer, der identificerer brugerterminalen 11, hvorfra anmodningssignalet 12 sendes.

Autorisations- og nøglefordelingsterminalen 10 signalbehandler anmodningssignalet for at fastslå, om brugerterminalen identificeret ved hjælp af ID-nummeret i filanmodningssignalet 12 er autoriseret til at udlede data fra filen identificeret i filanmodningssignalet 12. En sådan fastslåelse indbefatter en kontrol af status af en kundekonto i forbindelse med brugerterminalen 11, hvorfra anmodningssignalet 12 udledes, og kan desuden indbefatte en fastslåelse af lovligheden af, at kunden udleder data fra en sådan fil, uanset resultatet af kreditkontrollen.

Ved bestemmelse af status af kundens konto i forbindelse med brugerterminalen 11, ved bemyndigelser til autorisation af udledning af data fra filen identificeret i fileanmodningssignalet 12, autoriserer terminalen 10 brugerterminalen 11 til at udlede data fra

filen ved at tilføre både en filkrypteringsnøgle 13 og et autoriseret kreditdatasignal 14 til brugerterminalen 11. Kreditdatasignalet 14 indikerer en kreditforøgelse til brugerterminalen 11 for udledning af data fra filen identificeret i filanmodningssignalet 12.

Filnøglen 13 er krypteret i en enhedsnøgle, der er unik for brugerterminalen 11, hvortil den krypterede filnøgle og den krypterede kreditnøgle er kommunikeret. Enhedsnøglerne for hver af brugerterminalerne 11 i forbindelse med en given autorisations- og nøglefordelingsterminal 10 er lagret i autorisations- og nøglefordelingsterminalen 10 og er individuelt udtaget i overensstemmelse med brugerterminalens identifikationsnummer, der er indeholdt i filanmodningssignalet 12. Hver brugerterminal lagrer også permanent sin egen unikke enhedsnøgle. Det autoriserede kreditdatasignal 14 er genereret ved at indeholde både ikke-krypterede og krypterede kreditdata, der dannes ved kryptering af ikke-krypterede kreditdata med enhedsnøglen af den brugerterminal, der autoriseres.

Driften af brugerterminalen 11 under udledning af krypterede data fra den deri indlagte hukommelse er beskrevet i forbindelse med fig. 2. Visse funktionsenheder af brugerterminalen 11 er implementeret i en mikrocomputer. Disse funktionsenheder indeholder en data-dekrypteringsenhed 16, en filnøgle-dekrypteringsenhed 17, en omkostningsdata-autorisationsenhed 18, en kreditdata-autorisationsenhed 19, en autoriseret kredit- og debetstatusrapportgenereringsenhed 17, en autoriseret brugsrapport-genereringsenhed 21, en udlednings-reguleringsenhed 22 i forbindelse med hver datakøber, en brugerhistorie-registreringsenhed 23 i forbindelse med hver datakøber, en enhedsnøglehukommelse 24 og en RAM 25. Reguleringsenheden 22 indeholder et kreditregister 27, et debetregister 28, en akkumulator 29, en komparator 30 og en logisk enhed 31. Brugerterminalen 11 indeholder desuden et tastatur 33 for generering af en filbrugeranmodning 34 og en filtilgangsordre 35.

En ROM 37 indeholdende de krypterede datafiler er indført i brugerterminalen 11. ROM 37 indeholder et antal krypterede datafiler, fil A, fil B. Hver datafil indeholder krypterede datablokke, blok 1, blok 2, ..., blok 5. Hver datafil indeholder datablokke af en given

associationstype. De forskellige datafiler kan være associeret med forskellige datakøbere, og der kan være et antal datafiler i forbindelse med hver af de forskellige købere. Hver blok af data indeholder krypterede data, et blokidentifikationssignal og autoriserede omkostningsdata. De autoriserede omkostningsdata indikerer omkostningerne i forbindelse med udledning af den givne krypterede datablok.

For at gøre det muligt for brugerterminalen 11 at udlede data fra en given fil i den nævnte ROM 37, er filanmodningen 34, der identificerer en given fil, genereret ved hjælp af tastaturet 33 og kombineret med et enhedsidentifikationsnummer 39 for brugerterminalen 11 til tilvejebringelse af filanmodningssignalet 12, der kommunikeres til autorisations- og nøglefordelingsterminalen 10. Som før nævnt reagerer autorisations- og nøglefordelingsterminalen 10 på filanmodningssignalet 12 ved at tilvejebringe den krypterede filnøgle 13 og det autoriserede kreditdatasignal 14 til brugerterminalen 11, når autorisations- og nøglefordelingsterminalen 10 fastslår, at brugerterminalen 11 er autoriseret til at udlede dataene identificeret i filanmodningssignalet 12.

Den krypterede filnøgle 13 lagres i en RAM 25.

Det modtagne kreditdatasignal 14 indeholdende kreditdataene i både krypteret og ikke-krypteret form er legaliseret ved hjælp af kreditdata-legaliseringsenheden 19, der nøgles ved hjælp af en enhedsnøgle 42 lagret i enhedsnøglehukommelsen 24 til dekryptering af de krypterede kreditdata, og derved tilvejebringe et dekrypteret kreditdatasignal, der sammenlignes med det ikke-krypterede kreditdatasignal i det legaliserede kreditdatasignal 14 for derved at legalisere det modtagne kreditdatasignal 14. Et autoriseret kreditdatasignal 41 er lagret i kreditregisteret 27 af reguleringsenheden 22 i forbindelse med samme køber som filen, fra hvilken dataudledning er autoriseret. Hvis kreditregisteret 27 allerede har en kreditbalance, bliver en sådan balance forøget med beløbet indikeret ved hjælp af det autoriserede kreditsignal 41.

En meddelelse (ikke vist), der indikerer at autorisationen er blevet givet for brugerterminalen 11 til at udlede data fra den forespurgte fil, er også kommunikeret ved hjælp af autorisations- og nøglefordelingscenteret 10 til brugerterminalen 11 og vist på en monitor (ikke vist) ved brugerterminalen 11.

Til udledning af en given datablok fra en autoriseret datafil i ROM 37 er tastaturet 33 drevet til at tilvejebringe en filtilgangsordre 35 indeholdende et adressesignal 44, der føres til ROM 37 for tilgang til den givne datablok. I eksemplet i fig. 1 er den datablok, hvortil der er opnået adgang, blokken 5 af fil B. Ved tilgang til datablokken er de krypterede data 46, blokidentifikationssignalet 47 og autoriserede omkostningsdata 48 læst derfra. De autoriserede omkostningsdata indeholder både ikke-krypterede og krypterede omkostningsdata dannet ved kryptering af de ikke-krypterede omkostningsdata med den anvendelige filnøgle for filen indeholdende den datablok, der udledes.

Den anvendte krypterede filnøgle 13 udledes fra RAM 25 i afhængighed af en filadresse 49 i filtilgangsordren 35, og som er dekrypteret ved hjælp af filnøgle-dekrypteringsenheden 17, nøglet ved hjælp af enhedsnøglen 42 i enhedsnøglehukommelsen 24. Filnøgle-dekrypteringsenheden 17 tilvejebringer en dekrypteret filnøgle 50 til datadekrypteringsenheden 16 og omkostningsdataautorisationsenheden 18.

Det udledte omkostnings-datasignal 48 indeholdende omkostningsdata i både krypteret og ikke-krypteret form legaliseres ved hjælp af omkostningsdata-autorisationsenheden 18, der nøgles ved hjælp af filnøglen 50 og initieres ved hjælp af blokidentifikationssignalet 47 (anvendt som en begyndelsesvektor) til dekryptering af de krypterede kreditdata, og tilvejebringelse af et dekrypteret omkostnings-datasignal, der sammenlignes med det ikke-krypterede omkosntings-datasignal i det udledte omkostnings-datasignal 48 til legalisering af omkostnings-datasignalet.

Et legaliseret omkostnings-datasignal 51 tilføres til debetregisteret 28 og akkumulatoren 29. Debetregisteret 28 er ikke umiddelbart inkrementeret ved hjælp af omkost-

nings-datasignalet 51. Akkumulatoren 29 adderer først omkostnings-datasignalet 51 til debetsignalet 52. Debetsignalet 52 indikerer summen af tidligere dataudledningsomkostninger akkumuleret i debetregisteret 28. Summen 53 er omkostningsdataene og de tidligere akkumulerede data-udledningsomkostninger indikeret i akkumulatoren 29 er derefter ved hjælp af komparatoren 31 sammenlignet med et akkumuleret kreditsignal 54 fra kreditregisteret 27 til at bestemme om brugerterminalen 11 er blevet krediteret med en tilstrækkelig værdi til at man kan legalisere en udledning af data fra den ønskede fil. Når sammenligningen indikerer, at der er en tilstrækkelig akkumuleret kredit til at legalisere et sådant udtag, tilfører logikenheden 31 et aktiveringssignal 56 til data-dekrypteringsenheden 16, debetregisteret 28 og brugerhistorielagerenheden 23. Aktiveringssignalet 56 muliggør en inkrementering af omkostningsdataene 51 til debetregisteret 28. Som før nævnt indeholder brugerterminalen 11 et antal udledningsstyreenheder 22 svarende til et antal forskellige købere for at føre regnskab med udledningen af data fra filerne i forbindelse med hver af køberne.

Aktiveringssignalet 56 aktiverer endvidere driften af datadekrypteringsenheden 16. Datadekrypteringsenheden 16 nøgles ved hjælp af enhedsnøglen 42 i enhedsnøglehukommelsen 24 for dekryptering af krypterede data 46 og tilvejebringelse af udledte data 58. Blokidentifikationssignalet 47 anvendes som en begyndelsesvektor af datadekrypteringsenheden 16 i kombination med en dekrypteret filnøgle 50 for dekryptering af de dekrypterede data 46.

Efter aktiveringen ved hjælp af aktiveringssignalet 56 vil brugerhistorie-lagerenheden 23 lagre blokidentifikationssignalet 47 til registrering af identiteten af blokkene af data udledt fra den nævnte ROM 37. Blokidentifikationssignalet identificerer filen, hvorfra dataene blev udledt, og inkluderer en adresse, der identificerer køberen i forbindelse med den udledte fil for addressering af brugerhistorie-lagerenheden 23 i forbindelse med køberen af dataene i den udledte fil. Som før nævnt indeholder brugerterminalen 11 et antal brugerhistorie-lagerenheder 23 svarende til et antal forskellige købere for separat

registrering af datamængden udledt fra filerne i forbindelse med hver af de forskellige købere.

En brugerrapport 60, der indikerer brugerhistorien registreret i brugerhistorie-lagerenheden 23, er genereret for kommunikation til autorisations- og nøglefordelingsterminalen 10 i afhængighed af en betjening af tastaturet 33 eller et forespørgselssignal 61 udledt fra autorisations- og nøglefordelingsterminalen 10.Blokidentifikationsnummeret identificerer desuden de udledte data efter type, hvorpå typen af de udledte data registreres i historielagerenheden 23 og inkluderes i brugerrapporten 60.

En autoriseret brugerrapport 62 genereres ved hjælp af den autoriserede brugerrapport-frembringerenhed 21, der nøgles ved hjælp af enheden 42 lagret i enhedsnøglehukommelsen 24 til kryptering af brugerrapporten. Den autoriserede brugerrapport-frembringerenhed 21 tilvejebringer den autoriserede brugerrapport 62, der indeholder brugerrapporten i både krypteret og dekrypteret form, og som kombineres med enheds- identifikationsnummeret 39 for kommunikation til autorisations- og nøglefordelingsterminalen 10 som en autoriseret brugerrapport og identifikationssignal 63.

Sammen med den autoriserede brugerrapport og identifikationssignalet 63 er der desuden til autorisations- og nøglefordelingsterminalen 10 kommunikeret en autoriseret kredit- og debetstatusrapport og et identifikationssignal 64. Signalet 64 tilføres i afhængighed af driften af tastaturet 33 eller forespørgselsignalet 61 til udledningsstyreenheden 22. Signalerne 66 og 67, der indikerer status af henholdsvis kredit- og debetregistrene 27 og 28, krypteres ved hjælp af den autoriserede kredit- og debet-statusrapportgenereringsenhed 20, der nøgles ved hjælp af enhedsnøglen 42 i nøglehukommelsen 24. Den autoriserede kredit- og debetstatusrapportgenerator 20 tilfører et autoriseret kredit- og debetstatusrapportsignal 68, der indeholder en sådan statusrapport i både krypteret og dekrypteret form, og som kombineres med identifikationsnummeret 39 til tilvejebringelse af den autoriserede kredit- og debetstatusrapport og identifikationssignalet 64.

Kreditregisteret 27, debetregisteret 28 og brugerhistorie-registreringsenheden 23 for enhver given køber kan nulstilles efter ønske i afhængighed af en registerfornyelseskommando 70 (fig. 1) kommunikeret fra autorisations- og nøglefordelingsterminalen 10. En sådan kommando 70 kommunikeres f.eks., når en given brugerterminalkonto i forbindelse med en given køber er lukket ude.

I en alternativ foretrukken udførelsesform som vist i fig. 3 er en separat anmodning om anvendelsen af en fil kommunikeret fra en brugerterminal 72 til en autorisations- og nøglefordelingsterminal 73 for hver datafil, der skal udledes. Driftsrutinerne illustreret i fig. 3 er implementeret ved hjælp af en mikrocomputer.

Til at begynde med udføres en rutine 75 i brugerterminalen 72 for generering af en autoriseret anmodning om anvendelse af en fil indeholdende et identifikationsnummer 76 for brugerterminalen 72 og filnummeret 77 for den ønskede fil. Den genererede anmodning om anvendelse af en fil krypteres i krypteringsnøglen 78, der er unik for brugerterminalen 72, og kommunikeres til autorisations- og nøglefordelingsterminalen 73 i en autoriseret filanmodningsmeddelelse 79, der også indeholder det ikke-krypterede enhedsidentifikationsnummer 76.

Ved modtagelse af meddelelsen 79 udfører autorisations- og nøglefordelingsterminalen 73 en opslagsrutine 80 for opslag af nøglen for brugerterminalen 72 identificeret ved hjælp af det modtagne ikke-krypterede identifikationsnummer.

Under anvendelse af den nøgle 81, der er slået op, udfører autorisations- og nøglefordelingsterminalen 73 en dekrypteringsrutine 82 for dekryptering af enhedsidentifikationsnummeret og det ønskede filidentifikationsnummer fra den modtagne meddelelse 79.

Terminalen udfører derefter en anden opslagsrutine 83, i hvilken det dekrypterede filidentifikationsnummer 84 anvendes til opslag af den filnøgle 85, der blev anvendt til kryptering af filen identificeret ved hjælp af det dekrypterede filnummer 84.

Terminalen 73 foretager også en autorisationsrutine 86 til at bestemme, om den modtagne meddelelse 79 er autentisk, i hvilken rutine det dekrypterede identifikationsnummer 87 sammenlignes med identifikationsnummeret i den modtagne meddelelse 79. Hvis det ud fra en sådan sammenligning 86 fastslås, at meddelelsen 79 ikke er autentisk, genererer terminalen 73 en fejlmeddelelse 88, der indikerer, at den modtagne meddelelse 89 ikke er autentisk. Fejlmeddelelsen er derefter kommunikeret til og vist (ved 89) ved brugerterminalen 72.

Hvis det ud fra sammenligningen 86 fastslås, at meddelelsen 79 er autentisk, udfører terminalen 73 en kreditkontrolrutine 90 for brugerterminalen 72 identificeret ved hjælp af identifikationsnummeret. Hvis det ud fra en sådan kreditkontrol 90 fastslås, at kreditten skal udvides med henblik på udledning af data fra den ønskede fil ved den identificerede brugerterminal 72, genererer autorisations- og nøglefordelingsterminalen 73 en fejlmeddelelse 88, der indikerer, at kreditten ikke er autoriseret, og kommunikerer fejlmeddelelsen til brugerterminalen for visning 89 ved brugerterminalen 72.

Hvis det ud fra kreditkontrollen 90 fastslås, at kreditten skal udvides for udtagning af data fra den ønskede fil ved den identificerede brugerterminal 72, bliver filnøglen 85 krypteret i enhedsnøglen 81 for den identificerede kunderterminal 72 ved hjælp af en krypteringsrutine 91, og den krypterede filnøgle 92 kommunikeres til brugerterminalen 72.

Brugerterminalen udfører derefter en dekrypteringsrutine 93, i hvilken enhedsnøglen 78 anvendes til dekryptering af den krypterede filnøgle 92.

Brugerterminalen udfører derefter en dekrypteringsrutine 94, i hvilken den dekrypterede filnøgle 95 anvendes til dekryptering af filhovedet for den krypterede datafil 96 identificeret ved hjælp af det ønskede filnummer 77. Det dekrypterede filhoved 97 kommunikeres til autorisations- og nøglefordelingsterminalen 73, der på sin side udfører en sammenligningsrutine 98 for at fastslå, om det dekrypterede hoved er det korrekte hoved for filen identificeret ved hjælp af det dekrypterede filnummer 84. Denne rutine 98

verificerer dekrypteringen af den krypterede filnøgle, kommunikeret til brugerterminalen 72 inden debitering af kontoen for brugerterminalen 72. Hvis det fastslås, at det korrekte hoved ikke er blevet dekrypteret, udfører terminalen 73 en fejlmeddelelsesrutine, i hvilken en fejlmeddelelse, der indikerer fejlen, er genereret og kommunikeret til brugerterminalen 72 for visning 89.Hvis det fastslås, at det korrekte hoved er blevet dekrypteret, kommunikeres et aktiveringssignal til brugerterminalen 72 til igangsætning af en datafil-dekrypteringsrutine 100. Aktiveringssignalet 79 igangsætter også en rutine 101 i autorisations- og nøglefordelingsterminalen 73, i hvilken en transaktionsrapport, der identificerer brugerterminalen 72 og datafilen er genereret og kommunikeret til en notaudskrivningserminal 102 for debitering af kunden i forbindelse med brugerterminalen 72 for udledningen af data fra den ønskede fil.

I en alternativ udførelsesform vist i fig. 1 udfører en autorisationsterminal 105 og en brugerterminal 106 flere autorisations- og rapporteringsrutiner. Driftsrutinerne i fig. 4 implementeres ved hjælp af en mikrocomputer.

Brugerterminalen 106 foretager til at begynde med en rutine 107, i hvilken en autorisationsanmodning 108 indeholdende brugerterminalens identifikationsnummer 109, genereres og kommunikeres til autorisationsterminalen 105. Autorisationsterminalen 105 udfører en opslagsrutine 109 for opslag af nøglen 110 for brugerterminalen 106 identificeret ved hjælp af enhedsidentifikaitonsnummeret indeholdt i anmodningen 108.

Autorisationsterminalen udfører derefter en rutine 111, til generering af et autorisationssignal, i hvilken rutinenøglen 110 anvendes til kryptering af en forespørgselskommando. Den krypterede forespørgselskommando 112 kombineres med den ikke-krypterede forespørgselskommando til tilvejebringelse af en autoriseret forespørgselskommando, der kommunikeres til brugerterminalen 106, hvor den legaliseres ved hjælp af den deri lagrede nøgle 113.

Rutinerne til generering af autoriserede givne data, der er beskrevet heri, inkluderer trinnene til kryptering af de givne data og generering af et signal, der indeholder de givne data i både krypteret og ikke-krypteret form.

Rutinerne til legalisering af givne data beskrevet heri, inkluderer en dekryptering af de givne data, der er blevet krypteret, og en sammenligning af de dekrypterede data med de givne data i ikke-krypteret form.

Det er underforstået, at andre teknikker til generering af autoriserede data og til legalisering af givne data, vil kunne anvendes i andre udførelsesformer for opfindelsen.

Brugerterminalen 106 reagerer på forespørgselskommandoen 112 ved at udlede en brugerhistorierapport 114 for brugerterminalen 106 fra en brugerhistorie-lagerenhed 115 og en debet- og kreditrapport 116 for brugerterminalen 106 fra debet- og kreditregistre 117. Brugerterminalen udfører derefter en autorisationsrutine 118, i hvilken enhedsnøglen 113 anvendes til at kryptere brugerhistorierapporten 114 og debet- og kreditrapporten 116. En autoriseret rapport 119 indeholdende rapporterne 114 og 116 i både krypteret og ikke-krypteret form er kommunikeret til autorisationsterminalen 105.

Autorisationsterminalen udfører en rutine 121 under anvendelse af enhedsnøglen 110 til at legalisere rapporten 119. Brugerhistorien og debet- og kreditrapporterne er også signalbehandlet i relation til hinanden i overensstemmelse med visse kriterier til fastslåelse af deres ægthed. Hvis det fastslås, at rapporten 119 ikke er autentisk, er en rapport 123 genereret i autorisationsterminalen 105, og en fejlmeddelelse kommunikeres til og vises (ved 124) ved brugerterminalen 106.

Hvis det fastslås, at rapporterne 119 er autentiske, er brugerhistorien lagret (ved 125) for en rapport 125a til en notaudskrivningsterminal 126, og autorisationsterminalen 105 udfører en kreditkontrolrutine 127 i lyset af status af kontiene for brugerterminalen 106 opdateret ved hjælp af den autoriserede rapport 119 til at fastslå, om brugerterminalen

106 skal autoriseres til at udlede data fra krypterede datafiler lagret deri. Under udførelse af en sådan kreditkontrol opnår kreditkontrolrutinen 127 også adgang til en kreditopslagstabel 128, der indeholder en liste 129 over dårlige betalere modtaget fra notaudskrivningsterminalen 126.

Hvis kreditkontrolrutinen 127 fastslår, at brugerterminalen 106 ikke skal autoriseres til at udlede data fra de deri indførte krypterede datafiler, genereres en fejlrapport 130 i autorisationsterminalen 105, og en fejlmeddelelse kommunikeres til og vises (ved 124) i brugerterminalen 106.

Hvis kreditkontrolrutinen 127 fastslår, at brugerterminalen 106 skal autoriseres til at udlede data fra deri indførte krypterede datafiler, udfører autorisationsterminalen 105 en rutine 132, i hvilken enhedsnøglen 110 anvendes til at generere et autoriseret kreditdatasignal 133, der kommunikeres til brugerterminalen 106. Kreditdatasignalet indikerer et forudbestemt antal udledningsenheder i overensstemmelse med kredit- retten for den pågældende brugerterminal 106.

Brugerterminalen udfører en autorisationsrutine 134 på kreditdatasignalet 133 under anvendelse af enhedsnøglen 113 lagret i brugerterminalen 106. Hvis det efter en autorisationsrutine 134 fastslås, at kreditdatasignalet 133 ikke er autentisk, er en fejlmeddelelse vist (ved 124) i brugerterminalen 106 og rapporteret i autorisationsterminalen 105.

Hvis autorisationsrutinen 134 fastslår, at det krypterede kreditsignal er autentisk, bliver kreditregisteret i brugerterminalen 106 opdateret (ved 136) og dekrypteringen af dataene i datafilen i brugerterminalen igangsættes (ved 137) i overensstemmelse med størrelsen af den opdaterede kredit.

Tilvejebringelsen af en krypteret filnøgle fra autorisationscenteret 105 til brugerterminalen 106 er ikke nødvendigvis inkluderet i kombination med operationer beskrevet i relation til udførelsesformen i fig. 4, selv om det måtte være ønsket. Alternativt kan filnøglen

for hver køber være permanent lagret i brugerterminalen 106 til brug ved dekryptering af data krypteret i filnøglen for den respektive køber, eller filnøglen for hver køber kan være indeholdt i et kort, der uafhængigt indføres i brugerterminalen 106, og som kan ændres fra tid til anden eller i overensstemmelse med den særlige køber, fra hvis datafil dataene skal udledes.

Fig. 5 illustrerer et eksempel på en serie af rutiner, der kan anvendes i forbindelse med udførelsesformen i fig. 4 til styring af udledningen af data fra forskellige krypterede datafiler i forbindelse med hver køber og for registrering af udledningen af data fra sådanne filer. Operationerne beskrevet i forbindelse med fig. 5 udføres ved hjælp af en mikrocomputer i brugerterminalen. I dette eksempel indeholder hver datafil et antal datablokke og datablokke af forskellige typer. Hver type datablok har sine egne unikke omkostningsdata manifesteret i en specificeret mængde af udledningsenheder R i forbindelse hermed.

Efter et antal udledningsrutiner 140 er et kvantum på N blokke af en type, der har en udledningsomkostning på R, udledt fra datafilerne i forbindelse med køberen Y, hvorpå brugerhistorielageret for køberen Y er opdateret (ved 141), og debetregisteret for køberen Y er inkrementeret med N x R udledningsenheder 142. En sammenligningsrutine 143 udføres hver gang debetregisteret inkrementeres for at fastslå, om beløbet i debetregisteret for køberen Y er lig med eller overstiger beløbet i kreditregisteret for køberen Y. Hvis dette ikke er tilfældet, kan yderligere dataudledninger fra datafilerne i forbindelse med køberen Y fortsætte. Når beløbet i debetregisteret er lig med eller overstiger beløbet i kreditregisteret, standses dekrypteringen (ved 144), og en meddelelse om, at udledning ikke er autoriseret, vises (ved 145) ved brugerterminalen.

Kunden ved da, at han skal have brugerterminalen til at generere en anden autorisationsanmodning 108, som i udførelsesformen i fig. 4 til modtagelse af et yderligere kreditsignal fra autorisationsterminalen og derved inkrementere kreditregisteret inden yderligere udtag fra datafilerne vil kunne autoriseres.

I lyset af lagerkapaciteten og den lethed, hvormed data vil kunne udtages, er en CD-ROM foretrukket som lagermedium for de datafiler, der skal udledes i overensstemmelse med opfindelsen. I fig. 6 er en CD-ROM 148 indført i et CD-ROM drev 149, der er forbundet til en brugerterminal 150, der f.eks. svarer til den terminal, der er omtalt i forbindelse med fig. 2. Brugerterminalen 150 er indeholdt i en mikrocomputer i en personlig datamat 151 og anvender en mikrocomputerbus 152 til at kommunikere med en autorisations- og nøglefordelingsterminal (ikke vist) via et telefonmodem 153 og en telefonlinie 154.

Data Encryption Standard (DES) algoritme er at foretrække for de heri beskrevne krypterings- og dekrypteringstrin. Enhedsnøglehukommelsen i brugerterminalerne er en sikker hukommelse, der er indeholdt i en integreret kredsløbchip med en arkitektur, der hindrer adgang til hukommelsen fra chippen. Der kan kun opnås adgang til den sikre hukommelse ved hjælp af processoren i mikrocomputeren, der udfører DES-algoritmen.

Udledningen af forskellige typer af data fra hukommelsen i brugerterminalen kan autoriseres i forudbestemte rækker svarende til de forskellige typer af data som vist i et eksempel illustreret i fig. 7. I dette eksempel indeholder datafilen J datablokke 1, 2, 3, der hver især indeholder et antal tilsvarende forskellige datafelter a, b, c, d, e. Hver af de almindeligt designerede datafelter er relateret til en fælles datatype. I eksemplet i fig. 7 har hver datablok a, b, c, d, e, relation til et specielt firma; feltet "a" indeholder firmanavnet, feltet "b" indeholder zip-koden; feltet "c" indeholder antallet af medarbejdere; feltet "d" indeholder grundarealet, og feltet "e" indeholder årlige indtægter. Hver datablok indeholder desuden et blokidentifikationsnummer.

For at begrænse udledningsautorisationen for forskellige brugerterminaler til forskellige datatyper er filnøglen underopdelt i et antal feltnøgler svarende til de forskellige datafelter. Filnøglen for datafeltet J indeholder feltnøgler aj, bj, cj, dj, ej. Forskellige autorisationsrækker A, B, C er tildelt forskellige brugerterminaler i overensstemmelse med de forskellige kombinationer af de forskellige typer af datafelter, de er autoriseret til at udlede. I eksemplet i fig. 7 er rækken A tilordnet brugerterminaler, der er autoriseret til

at udlede data fra alle datafelterne i datafilen; rækken B er tilordnet brugerterminaler autoriseret til kun at udlede data fra felterne b og d, og rækken C er tilordnet til brugerterminaler, der er autoriseret til kun at udlede data fra felterne b, c og e.

PATENTKRAV

1. Brugerterminal (11) for udtag af data, omfattende en hukommelse (37), der kan indeholde krypterede datafiler, og hvorfra udtag af data må autoriseres, og en enhed til at regulere og holde regnskab med udtag af data (58) fra datafilerne, idet terminalen (11) er indrettet til at kunne kommunikere med en fjerntliggende central terminal (10) og omfatter en autoriseringsenhed (17, 19) for at tillade udtag af data ved at frembringe en krypteringsnøgle (50), som muliggør udtag af data (58) fra nævnte datafiler og dekryptering af disse, **kendetegnet ved**, at autoriseringsenheden (17, 19) er indrettet til at frembringe et kreditsignal (41) til at begrænse den datamængde, som kan udtages fra datafilerne, idet brugerterminalen desuden omfatter

- en reguleringsenhed (22) for i afhængighed af kreditsignalet at begrænse den mængde data, som kan udtages fra datafilerne,
- en registreringsenhed (23) for at holde regnskab med nævnte dataenhed ved at registrere den mængde data (58), som er udtaget fra datafilerne,
- en rapporteringsenhed (21) til at oprette en autentisk brugsrapport (62) med hensyn til den registrerede datamængde, som er udtaget fra datafilerne, og
- en enhed til at sende den autentiske brugsrapport (62) til den fjerntliggende centrale terminal (10) med henblik på fakturering.

2. Terminal ifølge krav 1, **kendetegnet ved**, at autoriseringsenheden (17, 19) omfatter en enhed (91) til at kryptere den nævnte krypteringsnøgle.

3. Terminal ifølge krav 1, **kendetegnet ved**, at autoriseringsenheden (17, 19) omfatter en enhed (91) til at autorisere kreditsignalet (41).

4. Terminal ifølge krav 1, **kendetegnet ved**, at reguleringsenheden (22) omfatter en enhed til at afgøre, om kreditten skal udvides som en reaktion på en udtagsanmodning, og hvis dette er tilfældet, angive kreditbeløbet ved kreditsignalet (41).

5. Terminal ifølge krav 1, **kendetegnet ved**, at

- hukommelsen (37) indeholder krypterede datafiler for hver af et antal forskellige dataleverandører, idet en speciel krypteringsnøgle (13) er nødvendig for at udtage en eller flere datafiler hørende til den enkelte leverandør,
- nævnte autoriseringsenhed omfatter en enhed (25) for at frembringe et separat sæt for hver leverandør bestående af en krypteringsnøgle (50) og et kreditsignal (41, 41) hørende til udtagsautorisationen,
- reguleringsenheden (22) omfatter en enhed til at begrænse udtag af datafiler hørende til forskellige leverandører hver for sig i afhængighed af den krypteringsnøgle og det kreditsignal, som er frembragt for vedkommende leverandør, og
- registreringsenheden (23) omfatter en enhed for separat registrering af den udtagne datamængde med hensyn til hver leverandør.

6. Terminal ifølge krav 1 eller 5, **kendetegnet ved**, at hukommelsen (37) indeholder flere krypterede datafiler fra en givet dataleverandør, og at registreringsenheden (23) omfatter en enhed for separat registrering af den udtagne datamængde (60) med hensyn til hver datafil fra den respektive leverandør.

7. Terminal ifølge krav 1, **kendetegnet ved**, at hukommelsen (37) indeholder ukrypterede initialiseringsvektordata (47) hørende til den enkelte krypterede datafil (46), og at terminalen desuden omfatter en dekrypteringsenhed (16) til at udnytte initialiseringsvektordataene (47) i kombination med krypteringsnøglen (50) for udtag af data (58) fra datafilerne (46).

8. Terminal ifølge krav 1, **kendetegnet ved**, at hukommelsen (37) indeholder ukrypterede initialiseringsvektordata (47) hørende til hver af datablokkene i den enkelte krypterede datafil (46), og at terminalen desuden omfatter en dekrypteringsenhed (16) for at udnytte initialiseringsvektordataene (47) i kombination med krypteringsnøglen (50) for udtag af data (58) fra datafilerne (46), idet registreringsenheden (23) udnytter initiali-

seringsvektordataene (47) for efter dataudtaget at registrere identiteten af den datablok (58), som er udtaget fra datafilen (46).

9. Terminal ifølge krav 1, **kendetegnet ved**, at hukommelsen (37) indeholder ukrypterede identifikationsdata (47) hørende til hver sin datablok (58) i den enkelte krypterede datafil (46), idet dekrypteringsenheden (16) udnytter de særegne identifikationsdata (47) til efter dataudtaget at identificere den datablok (58), som er udtaget fra datafilen (46).

10. Terminal ifølge krav 1, **kendetegnet ved**, at hukommelsen (37) indeholder omkostningsdata (51) hørende til forskellige datablokke (46), som kan udtages fra hukommelsen, idet reguleringsenheden (22) er indrettet til i afhængighed af en anmodning om udtag af en givet datablok at behandle omkostningsdataene (51) sammen med kreditsignalet (41) og derved afgøre, om udtag af den ønskede datablok (46) er autoriseret.

11. Terminal ifølge krav 10, **kendetegnet ved**, at den desuden omfatter en enhed (18) til at vurdere ægtheden af nævnte omkostningsdata (51) inden behandlingen af disse.

12. Terminal ifølge krav 1, **kendetegnet ved**, at hukommelsen er en lagerplade (141) af typen CD, som kun kan læses (CD-ROM).

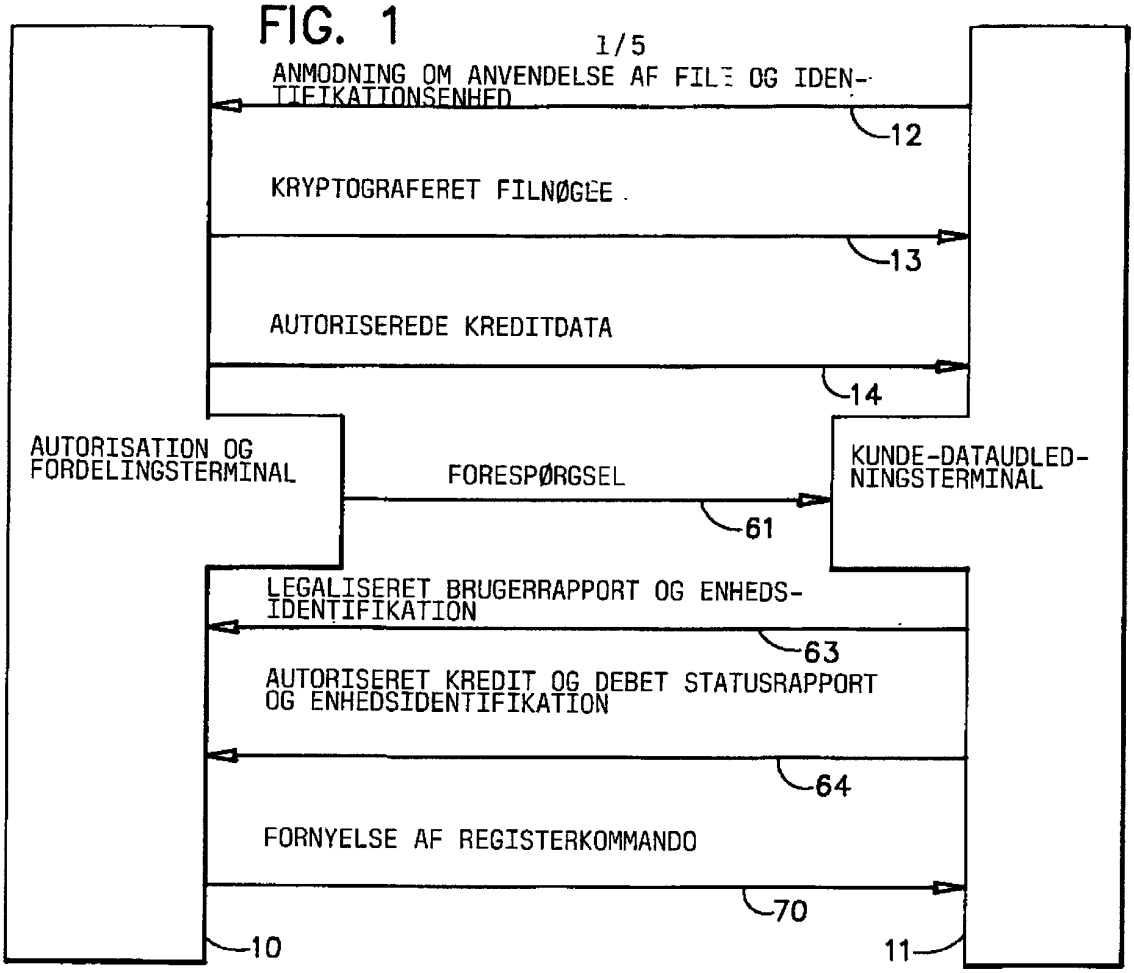
13. Anordning til at regulere udtag af data omfattende en brugerterminal ifølge krav 1 samt en fjerntliggende terminal (10, 73, 105), **kendetegnet ved**, at den fjerntliggende terminal omfatter en enhed (90, 127, 83, 132) til at afgøre, om status for en konto hørende til nævnte brugerterminal berettiger til autorisering af nævnte dataudtag, og hvis dette er tilfældet at frembringe nævnte krypteringsnøgle (50, 95) og nævnte kreditsignal (14, 133) i brugerterminalen (11, 72, 106).

14. Anordning ifølge krav 13, **kendetegnet ved**, at hukommelsen (37) indeholder omkostningsdata (48) hørende til forskellige datablokke, som kan udtages fra hukommelsen, idet anordningen desuden omfatter en behandlingsenhed (20) for at registrere omkost-

ningsdata (51) i brugerterminalen (11) for de datablokke (46), som er udtaget i forbindelse med det kreditsignal (41), som er frembragt i terminalen, og for at rapportere til den fjerntliggende terminal (10) de omkostningsdata (51), som er registreret i forbindelse med kreditsignalet (41).

15. Anordning ifølge krav 14, **kendetegnet ved**, at behandlingsenheden (20) er indrettet til at vurdere ægtheden af rapporten over registreringer af omkostningsdata i forbindelse med kreditsignalet.

FIG. 1


ANMODNING OM ANVENDELSE AF FILE OG IDEN-TIFIKATIONSENHED
12
KRYPTOGRAFERET FILNØGLE
13
AUTORISEREDE KREDITDATA
14
AUTORISATION OG FORDELINGSTERMINAL
FORESPØRGSEL
61
KUNDE-DATAUDLED-NINGSTERMINAL
LEGALISERET BRUGERRAPPORT OG ENHEDS-IDENTIFIKATION
63
AUTORISERET KREDIT OG DEBET STATUSRAPPORT OG ENHEDSIDENTIFIKATION
64
FORNYELSE AF REGISTERKOMMANDO
70
10
11

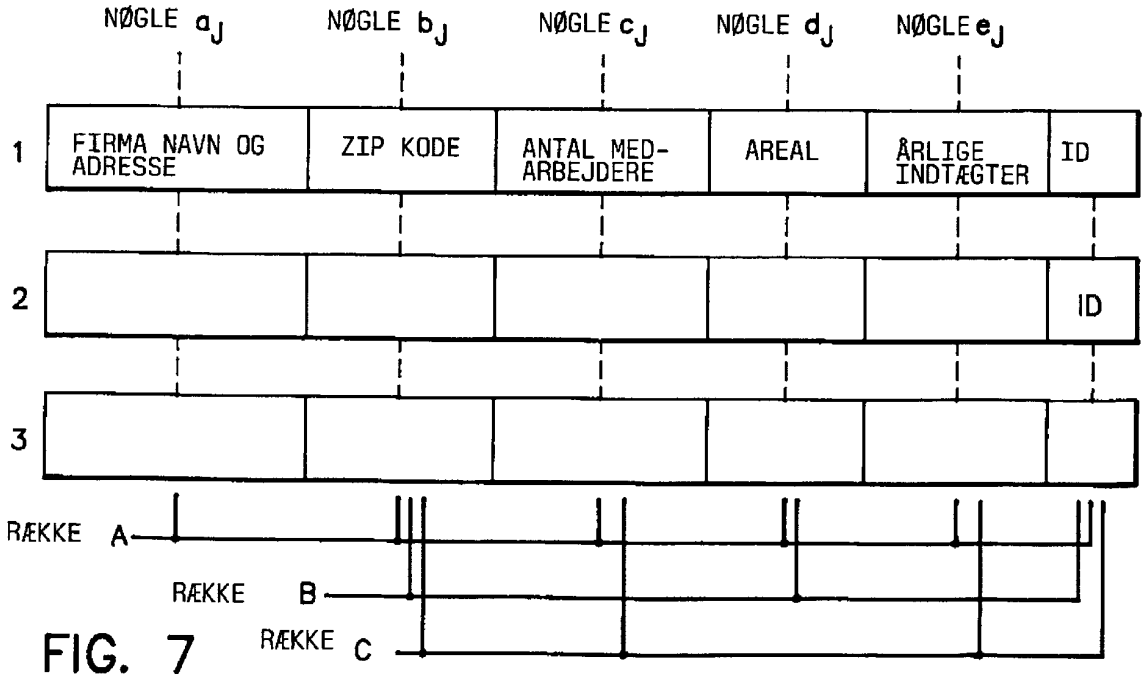
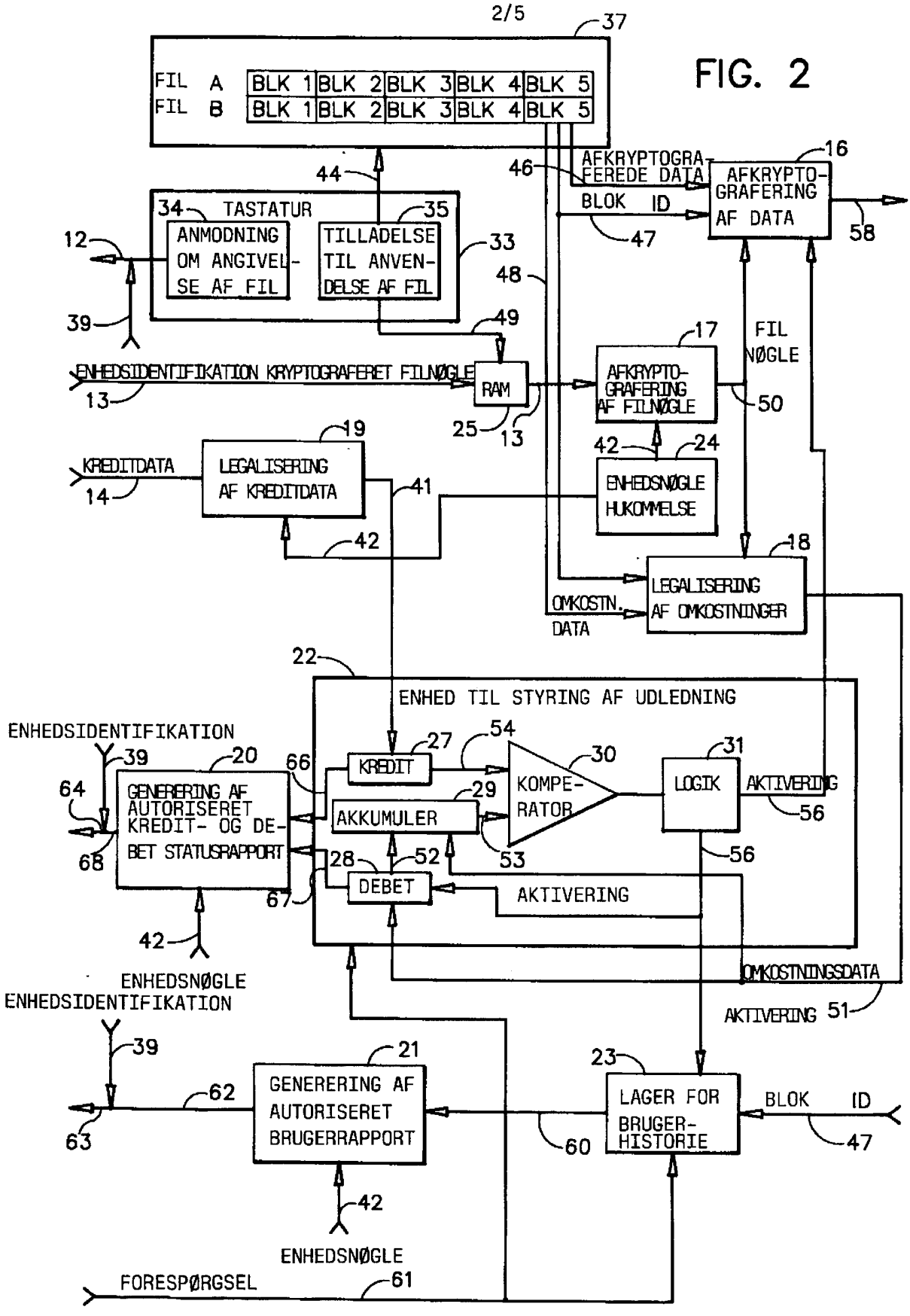

NØGLE a_J
NØGLE b_J
NØGLE c_J
NØGLE d_J
NØGLE e_J
1
FIRMA NAVN OG ADRESSE
ZIP KODE
ANTAL MED-ARBEJDERE
AREAL
ÅRLIGE INDTÆGTER
ID
2
ID
3
RÆKKE A
RÆKKE B
RÆKKE C

FIG. 7

FIG. 2


37
FIL A BLK 1 BLK 2 BLK 3 BLK 4 BLK 5
FIL B BLK 1 BLK 2 BLK 3 BLK 4 BLK 5
44
46
AFKRYPTOGRAFERET DATA
16
AFKRYPTOGRAFERING AF DATA
58
BLOK ID
47
34 TASTATUR
35
12
ANMODNING OM ANGIVELSE AF FIL
TILLADELSE TIL ANVENDELSE AF FIL
33
48
39
49
17
FIL NØGLE
ENHEDSIDENTIFIKATION KRYPTOGRAFERET FILNØGLE
RAM
AFKRYPTOGRAFERING AF FILNØGLE
13
25
13
50
42
24
19
KREDITDATA
LEGALISERING AF KREDITDATA
14
41
ENHEDSNØGLE HUKOMMELSE
42
18
LEGALISERING AF OMKOSTNINGER
OMKOSTN. DATA
22
ENHED TIL STYRING AF UDLEDNING
ENHEDSIDENTIFIKATION
39
20
66
27
54
30
31
64
GENERERING AF AUTORISERET KREDIT- OG DEBET STATUSRAPPORT
KREDIT
KOMPERATOR
LOGIK
AKTIVERING
29
AKKUMULER
56
68
28
52
53
56
DEBET
AKTIVERING
67
42
ENHEDSNØGLE
OMKOSTNINGSDATA
ENHEDSIDENTIFIKATION
AKTIVERING 51
39
21
23
62
GENERERING AF AUTORISERET BRUGERRAPPORT
LAGER FOR BRUGERHISTORIE
BLOK ID
63
60
47
42
ENHEDSNØGLE
FORESPØRGSEL
61

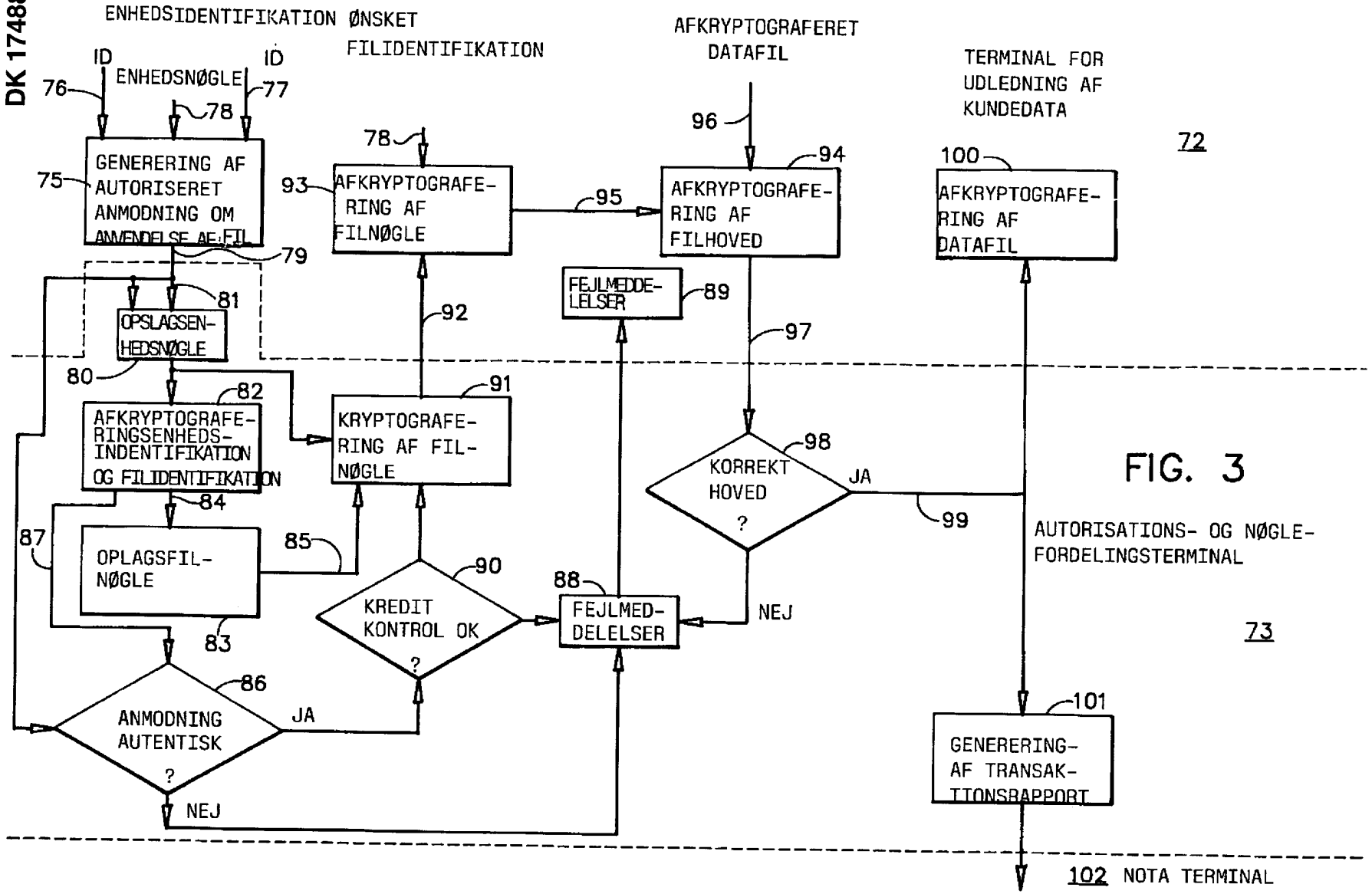
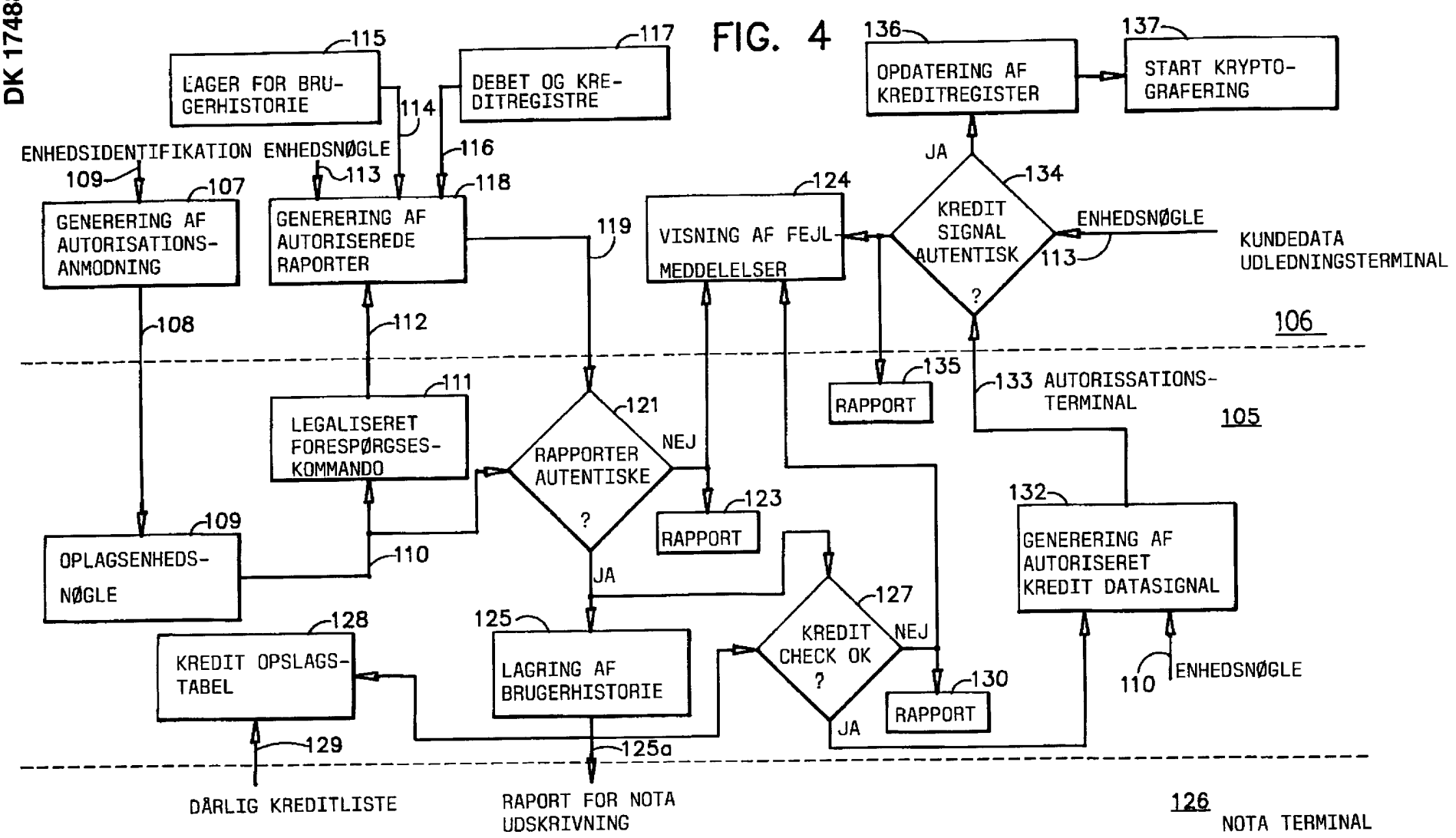

ENHEDSIDENTIFIKATION ØNSKET
FILIDENTIFIKATION
AFKRYPTOGRAFERET DATAFIL
TERMINAL FOR UDLEDNING AF KUNDEDATA
72
ID
ENHEDSNØGLE
ID
76
78
77
GENERERING AF AUTORISERET ANMODNING OM ANVENDELSE AF FIL
75
79
OPSLAGSENHEDSNØGLE
81
80
AFKRYPTOGRAFERINGSENHEDS-INDENTIFIKATION OG FILIDENTIFIKATION
82
84
OPLAGSFILNØGLE
87
83
85
ANMODNING AUTENTISK ?
86
JA
NEJ
78
AFKRYPTOGRAFERING AF FILNØGLE
93
92
KRYPTOGRAFERING AF FILNØGLE
91
KREDIT KONTROL OK ?
90
95
AFKRYPTOGRAFERING AF FILHOVED
96
94
FEJLMEDDELELSER
89
88
97
KORREKT HOVED ?
98
JA
99
NEJ
FEJLMEDDELELSER
AFKRYPTOGRAFERING AF DATAFIL
100
AUTORISATIONS- OG NØGLEFORDELINGSTERMINAL
73
GENERERING-AF TRANSAKTIONSRAPPORT
101
102 NOTA TERMINAL

FIG. 3

FIG. 4


LAGER FOR BRUGERHISTORIE
115
DEBET OG KREDITREGISTRE
117
114
116
ENHEDSIDENTIFIKATION
ENHEDSNØGLE
109
113
107
118
GENERERING AF AUTORISATIONS-ANMODNING
GENERERING AF AUTORISEREDE RAPORTER
119
108
112
111
LEGALISERET FORESPØRGSES-KOMMANDO
121
RAPPORTER AUTENTISKE ?
NEJ
JA
109
OPLAGSENHEDS-NØGLE
110
123
RAPPORT
128
KREDIT OPSLAGS-TABEL
125
LAGRING AF BRUGERHISTORIE
127
KREDIT CHECK OK ?
NEJ
JA
130
RAPPORT
129
125a
DÅRLIG KREDITLISTE
RAPPORT FOR NOTA UDSKRIVNING
126
NOTA TERMINAL
136
OPDATERING AF KREDITREGISTER
137
START KRYPTO-GRAFERING
JA
134
KREDIT SIGNAL AUTENTISK ?
ENHEDSNØGLE
113
KUNDEDATA UDLEDNINGSTERMINAL
124
VISNING AF FEJL MEDDELELSER
106
135
RAPPORT
133 AUTORISSATIONS-TERMINAL
105
132
GENERERING AF AUTORISERET KREDIT DATASIGNAL
110
ENHEDSNØGLE

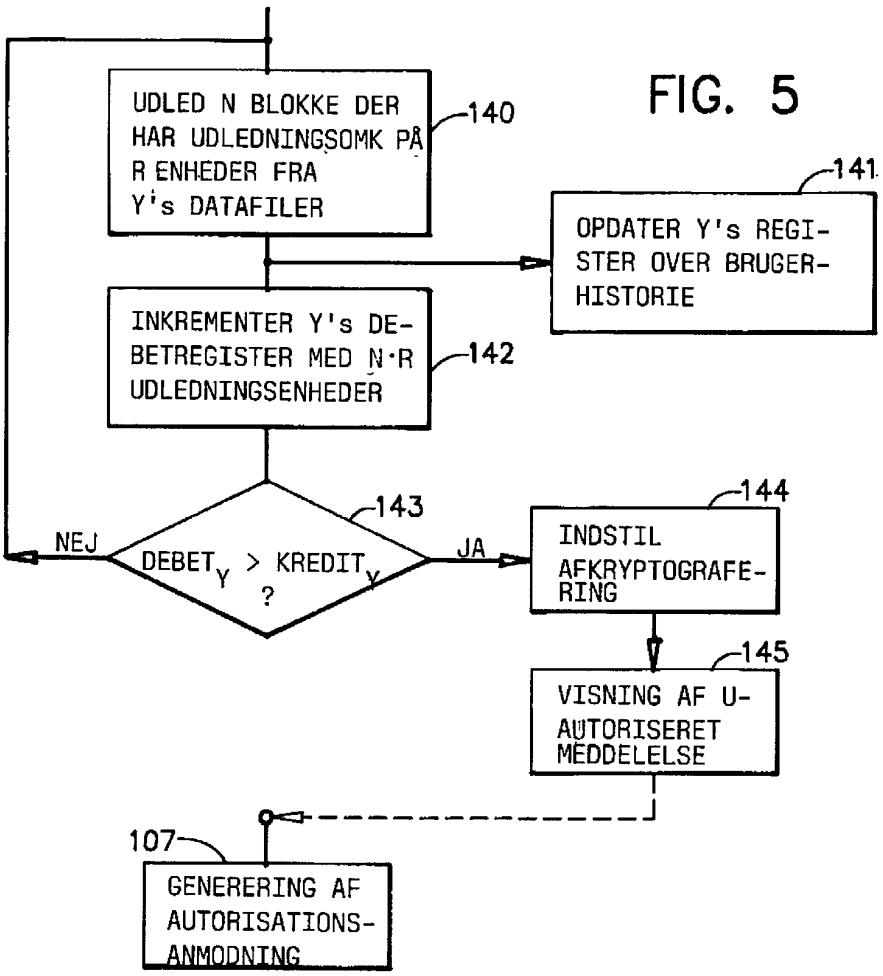

UDLED N BLOKKE DER HAR UDLEDNINGSOMK PÅ R ENHEDER FRA Y's DATAFILER
140
OPDATER Y's REGISTER OVER BRUGERHISTORIE
141
INKREMENTER Y's DEBETREGISTER MED N·R UDLEDNINGSENHEDER
142
DEBET$_Y$ > KREDIT$_Y$?
143
NEJ
JA
INDSTIL AFKRYPTOGRAFERING
144
VISNING AF UAUTORISERET MEDDELELSE
145
GENERERING AF AUTORISATIONSANMODNING
107

FIG. 5

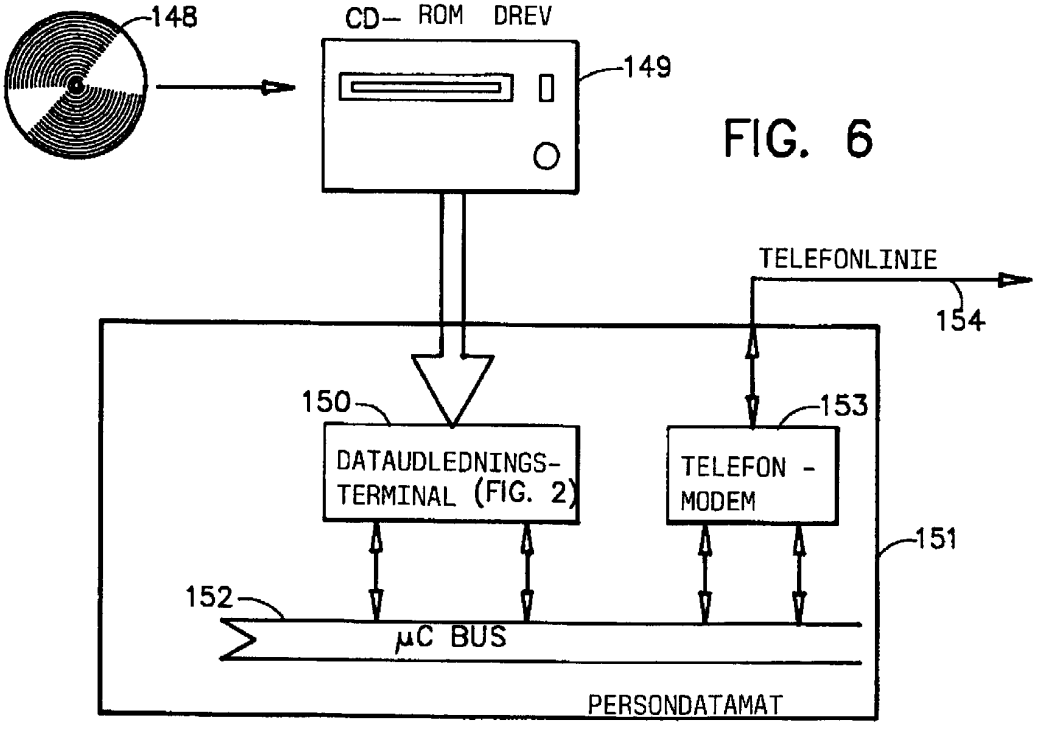

148
CD– ROM DREV
149
TELEFONLINIE
154
150
DATAUDLEDNINGSTERMINAL (FIG. 2)
153
TELEFON - MODEM
151
152
µC BUS
PERSONDATAMAT

FIG. 6