NORGE

(12) **PATENT**

(19) NO (11) **307120** (13) B1

(51) Int Cl[7] H 04 L 9/00

Patentstyret

(21) Søknadsnr	19914815	(86) Int. inng. dag og søknadsnummer	1990.06.07, PCT/DK90/00141
(22) Inng. dag	1991.12.06	(85) Videreføringsdag	1991.12.06
(24) Løpedag	1990.06.07	(30) Prioritet	1989.06.07, DK, 2790/89
(41) Alm. tilgj.	1991.12.06		
(45) Meddelt dato	2000.02.07		

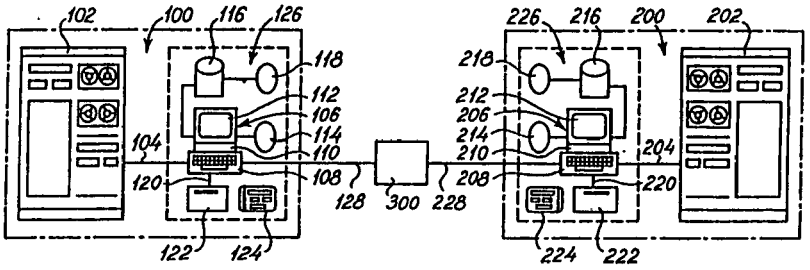
(71) Patenthaver Kommunedata I/S, Vester Søgade 10, DK-1601 København V, DK
(72) Oppfinner Jørgen Bjerrum, Oure, DK
Steen Ottosen, Odense, DK
Sven Nielsen, Albertslund, DK
(74) Fullmektig Bryns Patentkontor AS, 0106 Oslo

(54) Benevnelse **Fremgangsmåte til overføring av data, og et system for overføring av data**

(56) Anførte publikasjoner Ingen

(57) Sammendrag

Når data, et elektronisk dokument eller lignende overføres fra et første datasystem (100) til et andre datasystem (200) via en dataoverføringslinje (300), f.eks. en offentlig dataoverføringslinje, benyttes det en første utgangs- og inngangsstasjon (122) omfattende et første elektronisk kort (124) og en andre utgangs- og inngangsstasjon (222) som omfatter et andre elektronisk kort (224). Data overføres til det første elektroniske kort (124) fra det første datasystem (100) via den første stasjon (122) og krypteres i det første elektroniske kort (124) hvoretter data føres som utgang fra det første elektroniske kort (124) i kryptert form og overføres via den første stasjon (122) til det første datasystem (100) og derfra til dataoverføringslinjen (300). Data mottas av det annet datasystem (200) i kryptert form og overføres til det annet elektroniske kort (224) via den annen stasjon (222) hvoretter data dekrypteres i det annet elektroniske kort (224) og føres som utgang fra det annet elektroniske kort via den annen stasjon (222) til det annet datasystem (200). Da dataoverføring mellom det første og andre datasystem foregår mellom det første og det andre elektroniske kort vil ingen tredje part hverken autorisert eller uautorisert ha muligheter for å forstyrre dataoverføringen og eventuelt forandre data eller det elektroniske dokument. Det første og det andre elektroniske kort (124, 224) danner et sammenhørende sett kort omfattende sammenhørende krypterings-/dekrypteringsnøkler som er innført i de interne lagere i kortene.


102
100
116
126
118
112
106
114
110
104
120
108
128
300
228
122
124
226
216
200
202
218
212
206
214
210
204
208
220
224
222

Foreliggende oppfinnelse angår en fremgangsmåte til overføring av data fra et første datasystem til et andre datasystem via en dataoverføringslinje, f.eks. en offentlig dataoverføringslinje som angitt i innledning til krav 1, samt system for overføring av data som angitt i innledningen til krav 23.

Det er tidligere kjent flere teknikker og standarder for overføring av data, elektroniske dokumenter eller lignende fra et første datasystem til et andre datasystem via forskjellige dataoverføringslinjer så som hurtigkommunikasjonslinjer, private eller offentlige dataoverføringslinjer etc. Hvis dataoverføringslinjen i seg selv ikke er sikret mot at tredjemann med eller uten autorisasjon vil være i stand til å tappe data som overføres over dataoverføringslinjen eller det elektroniske dokument som overføres via dataoverføringslinjen er det en vanlig teknikk å sørge for kryptering av data eller det elektroniske dokument i overensstemmelse med kryptering/dekrypteringsteknikker som er velkjent, og disse teknikker kan omfatte enten symmetriske eller asymmetriske krypteringsalgoritmer, eller hemmelige eller offentlige nøkler. Ved denne tekst skal det bare henvises til den velkjente DES-algoritme (Data Encryption Standard), som er utviklet av IBM i samarbeid med National Bureau of Standards (NBS), USA. Som et eksempel på en data/dokumentutvekslingsprotokoll skal her nevnes den data/dokumentutvekslingsprotokoll -LECAM- som er utviklet av FRANCE TELECOM i forbindelse med Minitel datamaskiner som benyttes i stor utstrekning i Frankrike, og i henhold til hvilket data/-dokumentoverføring kan finne sted i kryptert eller ikke-kryptert form (ytterligere spesifikasjoner av protokollen finnes i S.T.U.C.A.M. - Spécification Techniques d'Utilisation du LECAM, desember 1987, FRANCE TELECOM, Télétel). En slik kryptert dataoverføring forutsetter imidlertid at senderen og mottakeren kan bli enige om å sette opp et innbyrdes sett av krypterings/dekrypteringsnøkler da de parter som tar del, nemlig sender og mottaker, nødvendigvis

må røpe noen detaljer ved sikkerhetsnivåer etc. Slike avtaler krever imidlertid at både sender og mottaker må stole helt ut på hverandre. Selv om de to parter som skal foreta en overføring av data eller en overføring av et elektronisk dokument fra et første datasystem til et andre datasystem kan bli enige om en slik utveksling av krypterings/dekrypteringsnøkler for bruk i forbindelse med en krypterings/-dekrypteringsalgoritme det er enighet om vil selv ikke en slik kryptert dataoverføring sikre at data som blir sendt fra det første datasystem eller det elektroniske dokument som sendes fra det første datasystem mottas korrekt av det andre datasystem, idet det vil være mulig å manipulere data eller det elektroniske dokument i forbindelse med utførelse av krypteringsalgoritmen i det første datasystem på samme måte som mottakeren etter dekrypteringen kan manipulere data eller det elektroniske dokument. En slik kryptert dataoverføring vil i seg selv ikke sikre at den overføring som finner sted er den tilsiktede eller ønskede overføring av data eller det elektroniske dokument eller at de data som mottas av det andre datasystem eller det elektroniske dokument som mottas av det andre datasystem i den form dataene eller det elektroniske dokument hadde i det andre datasystem etter overføringen er identiske med de data som ble sendt fra det første datasystem eller det elektroniske dokument som ble sendt fra det første datasystem. En slik kryptert dataoverføring via offentlige eller private dataoverføringslinjer vil i seg selv heller ikke sikre at de to datasystemer som står i forbindelse med hverandre er de rette tilsiktede parter i forbindelsen.

DE-A 3631797 beskriver en fremgangsmåte og en innretning for kryptering/dekryptering av sendt/mottatt data, idet innretningen består av en kommunikasjonsenhet med en permanent isolert krypteringsinnretning såvel som operasjonsinnretning som er isolert for datatransmisjonslinjen. For å kryptere/dekryptere sendte/mottatte data må en hemmelig nøkkel bli ført inn i den permanent isolerte krypteringsinnretningen,

dvs. kopiering av nøkler fra et lagringsmedium, slik som et brikke-(chip)kort. Fremgangsmåten til systemet ved foreliggende oppfinnelse adskiller seg fra det kjente systemet ved at kryptering/dekrypteringsinnretningen såvel som den hemmelige nøkkelen (nøklene) er lokalisert utelukkende på et fjernbart elektronisk kort.

Formålet med foreliggende oppfinnelse er å komme frem til en fremgangsmåte av den type som er omhandlet ovenfor, ifølge hvilken det blir mulig å etablere øyeblikkelig en sikker data- eller dokumentoverføring mellom to datasystemer uten å behøve å utveksle krypterings/dekrypteringsnøkler mellom datasystemene, oppgi detaljer som gjelder sikkerhetsnivåene etc. og i henhold til hvilken fremgangsmåte det sikres at den ønskede data- eller dokumentoverføring virkelig finner sted, idet man har sikkerhet for at det ikke vil være mulig for noen av partene eller for en tredjemann å forstyrre data- eller dokumentoverføringen. Formålene med foreliggende oppfinnelse er dermed mer i detalj å komme frem til teknikker som sikrer at ved overføring av data eller et elektronisk dokument fra et første datasystem til et andre datasystem via en dataoverføringslinje, f.eks. en offentlig dataoverføringslinje, garanteres det at de data som mottas av det andre datasystem eller det elektroniske dokument som mottas av det andre datasystem er identisk med de data som ble sendt fra det første datasystem eller det elektroniske dokument som ble sendt fra det første datasystem og omvendt.

Dette formål tilveiebringes ved hjelp av en fremgangsmåte av den innledningsvis nevnte art og hvis karakteristiske trekk fremgår av vedlagte patentkrav 1. Ytterligere trekk ved fremgangsmåten fremgår av de øvrige uselvstendige kravene. Videre tilveiebringes ovenfornevnte ved et system av den innledningsvis nevnte art hvis karakteristiske trekk fremgår av vedlagte patentkrav 23. Ytterligere trekk ved systemet fremgår av de påfølgende uselvstendige krav.

I henhold til det første aspekt ved oppfinnelsen foregår overføring av data eller dokumentet fra det første datasystem til det andre datasystem ved hjelp av to sammenhørende elektroniske kort som selv sørger for den nødvendige sikring av dataoverføringen når denne foregår i kryptert form, idet bruken av to sammenhørende elektroniske kort samtidig i forhold til både sender og mottaker, garanterer at data-utmatningen fra det andre elektroniske kort eller det elektroniske dokument som er utmatningen fra dette andre kort er identisk med datainnmatningen til det første kort eller det elektroniske dokument som er innmatning til det første elektroniske kort.

Da dataoverføringen mellom det første og andre datasystem foregår mellom de første og andre elektroniske kort, vil ingen tredjepart med eller uten autorisasjon være i stand til å innvirke på dataoverføringen og forandre data eller det elektroniske dokument. Det vil være klart at overføringen av data eller dokumentet i henhold til den lære som ligger til grunn for oppfinnelsen er mulig uten å behøve å foreta noen annen forandring i forbindelsen mellom det første og det andre datasystem enn utbyggingen (som er karakteristisk for oppfinnelsen) av både det første og det andre datasystem med tilhørende inngangs- og utgangsstasjoner som benyttes til innmatning og utmatning av data i de respektive elektroniske kort som tilhører det sammenhørende sett kort. Slike sammenhørende sett av kort kan utstedes øyeblikkelig, leies ut eller selges av en nøytral og utenforstående kortutsteder som på denne måte uten hverken sender eller mottaker for å skaffe informasjoner om hemmeligheter ved dataoverføringen som f.eks. krypteringsalgoritmer, sikkerhetsnivåer etc. kan sette sender og mottaker i stand til å overføre data eller elektroniske dokumenter mellom de tilhørende datasystemer uten noen risiko for at de data som mottas hos mottakeren eller det elektroniske dokument som mottas av mottakeren ikke skulle være identisk med de data som ble sendt av senderen eller det elektroniske dokument som senderen har sendt.

Ifølge foreliggende oppfinnelse er det videre mulig å sikre at overføringen finner sted mellom datamaskiner, hvis pålitelighet er kontrollert i forhold til hverandre, idet en pålitelighetskontroll av det første elektroniske kort i forhold til det andre elektroniske kort og omvendt fortrinnsvis utføres før overføringen av data eller det elektroniske dokument fra det første datasystem til det andre datasystem.

Ved fremgangsmåten ifølge oppfinnelsen er det videre mulig å kontrollere at data- eller dokumentoverføringen er korrekt, dvs. å kontrollere at de data som mottas av mottakeren eller det andre datasystem eller det elektroniske dokument som mottas av mottakeren eller det andre datasystem er identisk med de data som ble sendt fra det første datasystem eller det elektroniske dokument som ble sendt fra det første datasystem, idet ifølge oppfinnelsen en pålitelighetskontroll av data- eller dokumentoverføringen fortrinnsvis utføres ved overføringen av data eller det elektroniske dokument fra det første datasystem til det andre datasystem.

Bruken av et sammenhørende sett av elektroniske kort som er kjennetegnende for oppfinnelsen, ved hjelp av hvilket data- og dokumentoverføring finner sted, gjør det mulig å foreta dataoverføringen fullstendig anonymt uten noen mulighet for forstyrrelse eller inngrep hverken fra datasystemene som anvendes, personer, innbefattende operatører som med eller uten autorisasjon forsøker å forandre data eller det elektroniske dokument som overføres, siden ifølge oppfinnelsen innmatning til og utmatning fra krypteringen og dekrypteringen og eventuelt pålitelighets- og integritetskontrollen fortrinnsvis styres anonymt av den sentrale databehandlingsenhet i de enkelte kort.

I henhold til et spesielt trekk ved foreliggende oppfinnelse foregår den egentlige overføring av data eller det elektroniske dokument mellom det første og det andre datasystem

fortrinnsvis i overensstemmelse med den tidligere nevnte LECAM-protokoll enten i kryptert eller dekryptert form.

Ved pålitelighetskontroll tjener de første, andre og tredje data på en egenartet og logisk måte, når det gjelder det første og andre elektroniske kort til å bekrefte at overføringen av data eller det elektroniske dokument har funnet sted riktig og dermed at de data eller det elektroniske dokument som ble mottatt av det andre elektroniske kort er identisk med data som ble sendt av det første elektroniske kort, eller det elektroniske dokument som ble sendt av det første elektroniske kort, og videre til å sikre at sender og mottaker er autorisert sender og mottaker, og også at sender og mottaker er hva de utgir seg for å være.

Ifølge den foreliggende foretrukne utførelse blir imidlertid integritetsverifiseringen utført ved overføring av en komprimert data- eller dokumentversjon fra det første elektroniske kort til det andre elektroniske kort såvel som fra det andre elektroniske kort til det første elektroniske kort og sammenligning av både overførte, komprimerte data- eller dokumentversjoner til lagrede, komprimerte data- eller dokumentversjoner i de to elektroniske kort.

I henhold til alternative utførelsesformer for fremgangsmåten ifølge oppfinnelsen, der de alternative utførelsesformer utgjør kombinasjoner av pålitelighetskontrollen og integritetsverifiseringen foregår overføringen av de komprimerte data- eller dokumentversjoner som frembringes i det første datasystem eller det første elektroniske kort fra det første elektroniske kort til det andre elektroniske kort samtidig med overføringen av selve de nevnte data eller det elektroniske dokument, hvilke data eller hvilket elektroniske dokument og de komprimerte data- eller dokumentversjoner er satt sammen og kryptert som en enhet før overføringen eller som et alternativ kan overføringen av de komprimerte data- eller dokumentversjoner som frembringes i det andre data-

system eller i det andre elektroniske kort fra det andre elektroniske kort til det første elektroniske kort foregå samtidig med en ny overføring av de nevnte data eller det nevnte elektroniske dokument som er mottatt fra det første elektroniske kort fra det andre elektroniske kort til det første elektroniske kort, hvilke data eller hvilket elektroniske dokument som skal overføres pånytt og hvilke komprimerte data- eller dokumentversjoner blir satt sammen og kryptert som et hele før den nevnte overføring.

I henhold til en kombinasjon av disse alternative integritets- og autentisitets-(pålitelighet)verifiseringer foregår en samtidig ny overføring av den komprimerte data- eller dokumentversjon som mottas av det andre elektroniske kort og som frembringes i det første datasystem eller i det første elektroniske kort, ved overføringen av den komprimerte data- eller dokumentversjon som frembringes i det andre datasystem eller i det andre elektroniske kort og den nevnte nye overføring av data eller det elektroniske dokument fra det andre elektroniske kort, blir både de komprimerte data- eller dokumentversjoner og de nevnte data eller det elektroniske dokument som skal føres tilbake kombinert og kryptert som et hele før overføringen.

Ifølge foreliggende oppfinnelse kan det i det nevnte system inngå som nevnte første og andre elektroniske kort et sammenhørende sett av kort som omfatter de sammenhørende krypterings-/dekrypteringsnøkler som er innført i kortenes interne lagre. Det sammenhørende sett kort som benyttes i dette system ifølge oppfinnelsen omfatter fortrinnsvis kort av typen DES smartkort (Philips), Super smartkort (Bull) eller CP8 smartkort (Bull) eller i det minste et kort som er bygget opp på et trykt kretskort, et tykk-filmsubstrat, en tynn-filmmodul, etc.

Oppfinnelsen vil nå bli videre beskrevet under henvisning til tegningen, der

fig. 1 viser et system ifølge oppfinnelsen omfattende et første datasystem og et andre datasystem som kommuniserer med hverandre via en dataoverførings-
5 linje til utførelse av fremgangsmåten ifølge oppfinnelsen,

fig. 2 viser skjematisk oppbygningen av programvaren i det system som er vist på fig. 1,

10

fig. 3 viser skjematisk et system ifølge oppfinnelsen omfattende to datasystemer som kommuniserer med hverandre via en dataoverføringslinje og videre en minidatamaskin,

15

fig. 4 viser skjematisk et utvidet system omfattende tre datasystemer som ifølge læren ved oppfinnelsen kommuniserer med hverandre via en dataoverførings-
linje, og der et av systemene videre kommuniserer med
20 to terminaler eller Minitel-enheter via passende grensesnitt og dataoverføringslinjen,

fig. 5 viser et blokkdiagram for pålitelighetskontroll, og

25 fig. 6 viser et blokkdiagram for integritetsverifisering.

På fig. 1 er det skjematisk vist et system ifølge oppfinnelsen til utøvelse av fremgangsmåten ifølge oppfinnelsen, der systemet omfatter to selvstendige datasystemer med et
30 første datasystem vist på den venstre del av fig. 1 og betegnet med henvisningstallet 100 i sin helhet, og et andre datasystem vist på høyre del av fig. 1 og betegnet med henvisningstallet 200 i sin helhet. De to datasystemer 100 og 200 er skjematisk vist omfattende de samme typer komponenter
35 som for de to datasystemer er angitt med de samme to siste tall i henvisningstallene, idet henvisningstallene for komponenter som tilhører det første datasystem 100 begynner

med tallet 1 og henvisningstallene for komponenter som tilhører det andre datasystem 200 begynner med tallet 2. De to datasystemer 100 og 200 omfatter således hver en "i huset" hoveddatamaskin 102 resp. 202. Disse hoveddatamaskiner 102 og 202 kommuniserer via datalinjer 104, 204 med terminaler eller personlige datamaskiner (PC'er) 106, 206, og hver av disse omfatter et tastatur 108, 208, en databehandlingsseksjon 110, 210 og en dataskjerm 112, 212. Terminalene eller PC'ene 106, 206 står videre i forbindelse med tilhørende diskettstasjoner eller optiske platelagere 114, 214 såvel som hardplater 116, 216 med tilhørende reservediskettstasjoner eller optiske platelagere 118, 218. Terminalene eller PC'ene 106, 206 er videre via respektive dataoverføringslinjer 120, 220 forbundet med stasjoner 122 resp. 222 for innføring og utføring av data i de respektive elektroniske kort eller brikkekort, såkalte smartkort, som er angitt med henvisningstallene 124, 224.

Sammen med tilhørende periferiutstyr som omfatter diskettstasjonene eller optiske platelagere 114, 214, hardplatene 116, 216, reservediskettstasjonene eller optiske platelagere 118, 218 er de tilhørende stasjoner 122, 222 såvel som tilhørende elektroniske kort 124, 224, terminalene eller PC'ene 106, 206 innenfor blokkene 126, 226 som er angitt med stiplede linjer.

Formålet eller hensikten med oppfinnelsen er å skape en mulighet til overføring av data fra det første datasystem til det andre datasystem der dataoverføringen sikrer at de data som blir sendt er identiske med de data som menes å bli sendt, at data som mottas er identiske med de sendte data og fortrinnsvis videre at overføringen bare finner sted mellom parter som er spesielt uttatt for å sende og motta data, at mottak av data bekreftes av mottakeren og videre at mottak av mottakerens bekreftelse bekreftes av senderen i forhold til mottakeren. I den følgende beskrivelse tenkes dataoverføringen å finne sted fra det første datasystem 100 til det

andre datasystem 200, men det er naturligvis klart at dataoverføringen også kan finne sted i den motsatte retning. I henhold til oppfinnelsen kan dataoverføringen videre bestå i en utveksling av data mellom de to datasystemer, dvs. omfatte en overføring av data fra det første datasystem 100 til det andre datasystem 200 og overføring av data fra det andre datasystem 200 til det første datasystem 100. Ingen av de respektive sider av de to datasystemer 100 og 200 har noe kjennskap til sikkerhetsnivåer, overføringsprotokoller, krypterings-/dekrypteringsalgoritmer etc. for det andre datasystem. Via grensesnitt som inneholdes i de tilhørende terminaler eller PC'er 106, 206 og tilhørende dataoverføringslinjer 128, 228 er de to datasystemer 100 og 200 forbundet med et offentlig dataoverføringsnett som samlet er angitt med henvisningstallet 300. Istedenfor et offentlig dataoverføringsnett, f.eks. et X25 datanett, kan dataoverføringsnettet 300 være et privatnett eller omfatte kombinasjoner av offentlige og private datanett og videre ved tilhørende modemer (modulatorer/demodulatorer) være forbundet med f.eks. telefonlinjer eller andre signal- eller overføringslinjer.

For å sikre at de ovennevnte krav til dataoverføringen tilfredsstilles, kan dataoverføringen foretas ved at data som skal overføres fra datasystemet 100 til datasystemet 200 først føres som utmatning fra hoveddatamaskinen 102 i datasystemet 100 til terminalen eller PC'en 106 og overføres til stasjonen 122. Fra stasjonen 122 blir data videreført til det elektroniske kortet 124 via inngangs-/utgangsporten i dette kort, hvoretter data blir behandlet utelukkende av det elektroniske kort 124. På samme måte som kortet 224 har kortet 124 i tillegg til den ovennevnte inngangs-/utgangsport en sentral prosessorenhet eller CPU, et internt lager, en krypterings-/dekrypteringsblokk som styrt av den interne, sentrale prosessorenhet i kortet er i stand til å kryptere og dekryptere data ved å føre data som utmatning fra kortet eller ved å føre data som innmatning til kortet, ved bruk av

en eller flere krypterings-/dekrypteringsnøkler som innmatning til kortet på forhånd, slik det vil bli beskrevet mer i detalj i det følgende i en detaljert beskrivelse av system/programvare. For overføring av data mellom kortene utgjør kortene 124, 224, etter at de er utstedt sammen, et sammenhørende sett kort som er forprogrammert når det gjelder krypterings-/dekrypteringsalgoritmer og nøkler på en slik måte at kortene er i stand til å kommunisere med hverandre og dekryptere data som overføres fra det første kort til det andre kort og omvendt.

I det elektroniske kort 124 blir det foretatt en kryptering av datainnmatningen, og de krypterte data overføres via stasjonen 122, dataoverføringslinjen 120, terminalen eller PC'en 106, de tilhørende grensesnitt og dataoverføringslinjen 128 til dataoverføringsnettet 300 hvorfra data via dataoverføringslinjen 228, grensesnittet for terminalen eller PC'en 206, terminalen eller PC'en 206, dataoverføringslinjen 220 og stasjonen 222 overføres til det elektroniske kort 224 hvori data blir dekryptert ved hjelp av krypterings-/dekrypteringsnøkkelen (nøklene) som er lagret i kortet svarende til krypterings-/dekrypteringsnøklene i kortet 124. Etter dekryptering av data i kortet 224 kan dataene føres som utmatning i klar tekst fra det elektroniske kort 224 til stasjonen 222 og bli overført via dataoverføringslinjen 220, terminalen eller PC'en 206 og dataoverføringslinjen 204 til hoveddatamaskinen 202. Når dataoverføringen fra det første datasystem 100 til det andre datasystem 200 bare finner sted mellom to elektroniske kort 124 og 224, sikres det at dataversjonsutmatningen fra det elektroniske kort 224 er identisk med dataversjonsinnmatningen til det elektroniske kort 124. Med dette oppnås sikkerhet for at data som overføres til det andre datasystem 200 er identisk med de tilsiktede data som ble sendt fra det første datasystem 100 og sett fra den første datamaskins 100 side blir det også sikret at dataversjonen som datasystemet 200 har mottatt er

identisk med de data som opprinnelig ble sendt fra det første datasystem 100.

I den følgende systembeskrivelse vil det videre bli forklart hvorledes pålitelighetskontroll mellom de to elektroniske kort 124, 224 utføres før den egentlige overføring og videre hvorledes bekreftelser inneholdende komprimerte dataversjoner blir signert for pålitelighetskontroll, hvilke bekreftelser overføres mellom mottaker og sender, dvs. mellom kortet 224 og kortet 124.

På fig. 2 er programvareoppbygningen i hoveddatamaskinene 102, 202 i datasystemene 100 og 200 og terminalene eller PC'ene 106, 206 vist skjematisk. Det skal påpekes at programvareoppbygningen bare skal være illustrerende og bakgrunn for forklaringen og ikke på noen måte oppfattes som begrensning av det beskyttelsesomfang som er angitt i kravene. Hver hovedprogramvare omfatter en "i huset" programvare 130, 230, en kommunikasjonsprotokoll 132, 232 for overføring av data til den tilhørende terminal eller PC 106, 206 via dataoverføringslinjene 104, 204 (f.eks. en asynkron RS 232 kommunikasjonsprotokoll), to programvareomformere eller kompilatorblokker 134, 234 og 136, 236 for omforming eller kompilering fra "i huset" -format til den overførings-protokoll som bestemmes av blokken 132, 232 resp. fra overføringsprotokollen som bestemmes av blokken 132, 232 til "i huset" -format. Programvaren 102, 202 for hoveddata-maskinen kan videre omfatte en ytterligere blokk 138, 238, et såkalt Edifact-program som vil bli beskrevet i det følgende.

Terminalene eller PC'ene 106, 206 inneholder de følgende programvareblokker: En kommunikasjonsprotokoll 140, 240 for kommunikasjon med hoveddatamaskinen 102, 202 via dataover-føringslinjen 104, 204, et internt sentralt program 142, 242 for styring av funksjonene i terminalen eller PC'en det gjelder, en omformer- eller kompilatorprogramvare 144, 244 svarende til programvareblokken 138, 238 i hoveddatamaskinen

102, 202, en kommunikasjonsprotokoll 146, 246, f.eks. en X25 protokoll, hvilke protokoller danner grensesnittet mellom terminalen eller PC'en og de tilhørende dataoverføringslinjer 128, 228, en programvareblokk 148, 248 for kommunikasjon med tilhørende periferiutstyr for terminalene eller PC'en såsom diskettstasjonene og hardplatene 114, 214 og 116, 216 som vist på fig. 1, en programvareblokk 150, 250 inneholdende informasjon vedrørende f.eks. "sorte lister" etc. og sluttelig en programvareblokk 152, 252 for kommunikasjon med den tilhørende stasjon 122, 222. PC-programmet kan videre omfatte en blokk svarende til blokkene 138 og 238 som er omhandlet ovenfor og som omfatter Edifact-programmet.

Det skal påpekes at dataoverføringen som omfatter pålitelighetskontroll/integritetsverifisering etc., som er kjennetegnende for oppfinnelsen kan utføres med et integrert kretskort som er en kombinasjon av en stasjon og et elektronisk kort såsom en kombinasjon av stasjonen 122 og kortet 124 eller av stasjonen 222 og kortet 224. Slike trykte kretskort er vist i den nedre del av fig. 2 og betegnet med henvisningstallene 160 og 260. De trykte kretskort 160, 260 utgjør dermed et kort som er komplementært i forhold til det andre trykte kretskort eller i forhold til et elektronisk kort til bruk sammen med en tilhørende stasjon. Dermed kan det trykte kretskort 160 være et kretskort som er komplementært til det trykte kretskort 260 eller et kort som er komplementært til det elektroniske kort 224. Tilsvarende kan det trykte kretskort 260 være komplementært til det elektroniske kort 124 eller et kort som er komplementært til det trykte kretskort 160.

I en ytterligere alternativ utførelse av oppfinnelsen kan den ovenfor beskrevne dataoverføring fra det elektroniske kort 124 til det elektroniske kort 224 foregå mellom samsvarende sikkerhetsmoduler 170, 270 som er vist på den nedre del av fig. 2. Disse sikkerhetsmoduler eller sikkerhetsterminaler utgjør såkalte "fuskesikre" stasjoner, dvs. stasjoner som på

grunn av denne spesielle fysiske oppbygning gjør det umulig å åpne systemet og derved avdekke materiell såvel som programvare. På samme måte som de elektroniske kort 124, 224 inneholder disse sikkerhetsmoduler en inngangs-/utgangsport, en sentral prosessorenhet, interne lagre og krypterings-/dekrypteringsblokker. I motsetning til de elektroniske kort 124, 224 og de trykte kretskort 160, 260 som integrerer stasjoner og kort kan de interne lagre i sikkerhetsmodulene inneholde flere krypterings-/dekrypteringsnøkler som blir adressert til en gitt dataoverføring ved hjelp av et kort, f.eks. et elektronisk kort eller et magnetisk kort som på samme måte som de elektroniske kort 124, 224 og trykte kretskort 160, 260 som integrerer stasjoner og elektroniske kort blir utstedt av en kortutsteder som på samme måte som når det gjelder det elektroniske kort eller magnetiske kort utsteder et tilsvarende magnetisk kort eller et elektronisk kort eller et trykt kretskort til bruk ved dataoverføring fra en sikkerhetsmodul som blir adressert med det magnetiske kort det gjelder til en sikkerhetsmodul som blir adressert med et tilhørende elektronisk kort og sluttelig til et trykt kretskort eller omvendt.

På fig. 3 er det skjematisk vist et system som er utbygget sammenlignet med det system som er vist på fig. 1 og som i tillegg til de to datasystemer 100 og 200 omfatter en minidatamaskin som er betegnet med henvisningstallet 306 som et hele og har et tastatur 308, en sentral prosessorenhet 310 og en dataskjerm 312. Minidatasystemet 306 kan videre omfatte periferiutstyr så som en diskettstasjon eller en båndstasjon, en skriver etc. Dette periferiutstyr er ikke vist på fig. 3. For overføring av data til et av datasystemene 100 eller 200 eller for mottak av data fra et av disse datasystemer i henhold til den lære som ligger til grunn for oppfinnelsen er minidatasystemet 306 forbundet med en stasjon 322 svarende til stasjonene 122, 222 som er vist på figurene 1, 2 og 3 via en dataoverføringslinje 320 svarende til dataoverføringslinjene 120 og 220 som er vist på fig. 1. Via dataover-

føringslinjen 328 som svarer til dataoverføringslinjene 128, 228 via et grensesnitt som ligger i den sentrale dataprosessorenhet 310 i minidatasystemet og videre eventuelt via et modem som ikke er vist på fig. 3 er minidatasystemet 306 forbundet med et offentlig telefonnett 330. Det offentlige telefonnett 330 er via et modem som heller ikke er vist på fig. 3 og en dataoverføringslinje 332 forbundet med en omformer 346 inneholdende omformer- eller kompilatorunderblokker 334, 336 svarende til programvareblokkene 134, 234 og 136, 236 som er vist på fig. 2 og som via dataoverføringslinjen 338 er forbundet med nettet 300.

Ved hjelp av to sammenhørende kort hvorav det ene er innført i stasjonen 322 og det andre er innført i stasjonen 122 eller 222 i henholdsvis datamaskinen 100 og 200, er det mulig ifølge oppfinnelsen å overføre data til og fra minidatasystemet 306 fra og til det datasystem det gjelder som har fått innført et elektronisk kort, ikke vist, svarende til det elektroniske kort som er innført i kortstasjonen 322 på samme måte som minidatasystemet 306 kan det datasystem som minidatamaskinen kommuniserer med ha sitt elektroniske kort integrert med den tilhørende stasjon i et trykt kretskort på samme måte som det trykte kretskort som er vist på fig. 2 og betegnet med henvisningstallene 160, 260 tilhørende datasystemene 100, 200 eller ha en sikkerhetsmodul eller en sikkerhetsterminal som kan adresseres ved hjelp av et elektronisk kort eller et magnetkort som forklart ovenfor.

På fig. 4 er det vist et alternativt datasystem som i tillegg til det ovenfor beskrevne datasystem omfatter det første datasystem 100 og det andre datasystem 200 som er forbundet med hverandre med et nett 300 som innbefatter et antall minidatasystemer, i det foreliggende eksempel to minidatasystemer 406 som fortrinnsvis er såkalte Minitel-maskiner i forbindelse med en tilsluttet vertsmaskin som er vist i det øvre midtparti på fig. 4 og betegnet med henvisningstallet 400 som en helhet og som utgjør et datasystem. Minidatasystemet 406

og vertsmaskinen 400 danner et såkalt videotex-system som vil bli forklart mer i detalj i det følgende i beskrivelsen av system/programvare. Kommunikasjonen mellom Minitel-maskinene 406 og vertsmaskinen 400 opprettes fortrinnsvis i henhold til den LECAM-protokoll som er utviklet av FRANCE TELECOM. Datasystemet 400 utgjør et datasystem svarende til et av datasystemene 100, 200 og mellom datasystemet 400 og et av datasystemene 100, 200 kan data overføres begge veier på den ovenfor beskrevne måte ved hjelp av to sammenhørende kort, særlig to sammenhørende elektroniske kort. Datasystemet 400 er således hovedsakelig en oppbygning som tilsvarer oppbygningen av datasystemene 100, 200 og omfatter en sentral prosessorenhet 402 som er forbundet med en kommunikasjonsblokk 426 svarende til blokkene 126, 226 via en dataoverføringslinje 404, hvilken blokk 426 er forbundet med nettet 300 via en dataoverføringslinje 428 svarende til dataoverføringslinjene 128, 228. Datasystemet 400 omfatter videre en hardplate 460 eller platelager, en dataskjerm 462 og en kortleser 464. Kortleseren 464 er innrettet til å motta et elektronisk kort av den type som er beskrevet ovenfor, særlig et såkalt smartkort, ved overføring av data til og fra Minitel-datamaskinen 406 slik det vil bli forklart mer i detalj i det følgende i beskrivelsen av system/programvare. Kortleseren eller stasjonen 464 har på den annen side ingen forbindelse med de utenforliggende datasystemer 100, 200, idet dataoverføring mellom datasystemet 400 og et av datasystemene 100, 200 styres av kommunikasjonsblokken 426 på den måte som er beskrevet ovenfor. De selvstendige Minitel-maskiner 406 har et tastatur 408, en dataskjerm 412 og en kortleser 422 som på samme måte som kortleseren 464 er innrettet til å motta et elektronisk kort som gjør det mulig å overføre data til og fra Minitel-maskinen 406 henholdsvis fra og til datasystemet 400. Forbindelsen fra den selvstendige minitelmaskinen 406 til datasystemet 400 opprettes via en dataoverføringslinje 428 som forbinder den selvstendige Minitel-maskinen 406 med et offentlig telefonnett 430 ved hjelp av passende modemenheter, en forbindelse fra

det offentlige telefonnett 430 til datasystemet 400 via en første dataoverføringslinje 432, en omformer eller kompilator 446 og en andre dataoverføringslinje 438.

Minitel-maskinene som er vist på fig. 4 tjener for det første til å fordele elektronisk dokument "post" internt idet Minitel-system som tilhører datasystemet 400, idet data eller dokumentoverføring foregår fra den selvstendige Minitel-maskinen 406 via det offentlige telefonnett 430 og nettet 300 ved hjelp av et elektronisk kort utstedt av den organisasjon som driver datasystemet 400 til stasjonen 464 i datasystemet 400.Datasystemet som er vist på fig. 4 har dessuten muligheter til overføring av data eller dokumenter fra den selvstendige Minitel-maskin 406 til datasystemet 400, hvorfra data eller dokumenter kan overføres videre til et andre datasystem, f.eks. datasystemet 100 eller datasystemet 200 via dataoverføringsblokken 426 med tilhørende elektroniske kort ifølge den overføring som er beskrevet tidligere.

Eksempel

Et datasystem av den type som er vist på fig. 1 og 2 ble bygget om med:

Personlig datamaskin:

AT 10 MHz med lager på 640 kbytes,
40 Mbyte hardplate, 2 serie RS232 porter, dansk tastatur, svart/hvit skjerm innbefattende adapter.
Type: Philips P3204.

Den følgende programvare ble benyttet:
MS-DOS operativsystem versjon 3.3.
Type: Microsoft

RTOS sanntids operativsystem versjon 4.00.
Type: Dansk informasjonsteknologi

X.25 kommunikasjonskort - 16 porter:
Type: Stollmann SICC-PC-X25.

Smartkortleser med strømtilførsel og RS232 grensesnittkabel:
Type: Philips/Control Data Laserdrive 510 DT

For denne systemoppbygning ble det benyttet programvare som var utviklet av Netplus (©1989). Programvaren er utviklet i C, Pascal og Assembler.

I datasystemet ble data og dokumenter i kryptert og ikke-kryptert form videre utvekslet mellom en Minitel-terminal av den type som er vist på fig. 4 med henvisningstallet 406 og et datasystem av den ovenfor beskrevne type i overens-stemmelse med oppfinnelsens prinsipper ved hjelp av LECAM-protokollen som er utviklet av FRANCE TELECOM (©desember 1987 - FRANCE TELECOM - TELETEL).

Et detaljert system og en programvarespesifikasjon vil bli beskrevet i det følgende både når det gjelder dataoverføring fra det første datasystem til det andre datasystem, f.eks. fra datasystemet 100 til datasystemet 200 og dataoverføring til og fra en Minitel-maskin 406 henholdsvis til og fra datasystemet 400.

System- og programvarebeskrivelse:

Systemet har et grensesnitt mot en stor omgivende verden som ikke er under kontroll under alle omstendigheter. Dette innebærer at man må sikre seg mot at uautoriserte personer får uautorisert adgang til eller innsikt i systemet. I det følgende er systemets sikkerhet beskrevet sammen med de krav som dessuten stilles til systemet slik at dette kan være av nytte i praksis.

Det finnes sikkerhetssystemer som er umulige å bryte, men som er ubrukbare i praksis, men også sikkerhetssystemer som er

kommersielt tilgjengelige og synes å være brukbare i praksis, men som dessverre også er enkle å bryte.

Et antall sikkerhetskrav som systemet oppfyller vil nå bli beskrevet:

1. Stort nøkkelrom
2. Ingen reell eller statistisk mulighet til å finne en nøkkel på grunnlag av klar tekst og kryptotekst
3. Ingen klar tekst i kryptotekst
4. Lagdelt struktur i overføringsnettet

Vedr. 1. Antall nøkler må være så stort at det ikke er praktisk gjennomførlig å finne den rette nøkkel ved omfattende søking. Det må være et krav at to forskjellige nøkler krypterer samme klartekst til forskjellige kryptotekster. Nøyaktig hvor stort nøkkelrommet må være avhenger naturligvis også av de ressurser som er tilgjengelige for en potensiell "fiende". For de transaksjoner som er nevnt i dette system er 56 biter som i DES tilstrekkelig, idet det gjennomsnittlig vil ta minst 4 måneder å desifrere en kryptotekst med den hurtigste tilgjengelige datakraft. Da en ny nøkkel benyttes for hver overføring vil det være praktisk umulig å oppnå full innsikt.

Vedr. 2. Selv om mange sammenhørende klartekstmeldinger og tilhørende kryptotekstmeldinger er kjent skal det ikke være mulig å bestemme den anvendte nøkkel på grunnlag av dette.

Vedr. 3. I kryptoteksten må det ikke finnes noe statistisk fremtredende spor av klarteksten. Hvis det ikke finnes noe slikt spor vil "fiendens" eneste våpen være omfattende søking hvis bare kryptoteksten er tilgjengelig.

Vedr. 4. Grensesnittspesifikasjonene for overføringsnettet over hvilket de krypterte data eller tekst sendes vil

normalt også foreskrive overføring av kontrollinformasjon vedrørende operasjonen, noe som naturligvis ikke må være kryptert svarende til adressefelter og lignende for de nevnte data. Problemer kan oppstå hvis grensesnittet ikke har en lagdelt struktur eller hvis det ikke er helt klart på hvilket nivå krypteringen skal finne sted.

Bruk av brikkekort og DES-algoritmene utgjør en løsning der

1. størrelsen på nøkkelrommet er tilstrekkelig, særlig siden forskjellige nøkler benyttes for forskjellige overføringer og nøklene for utveksling av krypteringsnøkkelen er trygt skjult i brikkekortet,

2. det har ingen praktisk verdi å finne nøkkelen på grunnlag av både klartekst og kryptotekst da denne nøkkel bare benyttes for en overføring, og

3. DES-krypteringen av dokumentene sikrer at det ikke finnes noen klartekst i kryptoteksten.

Ved bruk av brikkekort og DES-algoritme på denne måte blir både det offentlige X.25 nett såvel som et teletel videotex-nett benyttet. Begge disse nett forenkler en transparent overføring av kryptert tekst. Det finnes forskjellige protokoller for overføring, som følges i forbindelse med dokumentoverføringen. For videotex-nettet benyttes LECAM-protokollen.

Symmetriske/asymmetriske systemer

Når det er mulig benyttes enkle metoder for å sikre data, men uten å redusere sikkerheten. Av den grunn foretrekkes et symmetrisk system (f.eks. DES) fremfor et asymmetrisk system (f.eks. RSA) siden asymmetrisk system såsom RSA krever langt større datakraft enn et symmetrisk system, såsom DES. Et symmetrisk system som f.eks. DES krever på den annen side større sikkerhet når det gjelder nøklene.
(Se ovenfor når det gjelder DES og RSA).

1. Symmetriske kryptosystemer
2. Asymmetriske kryptosystemer
3. Hastigheter

Vedr. 1. Et symmetrisk kryptosystem er kjennetegnet ved at samme nøkkel benyttes både til kryptering og dekryptering. En meget benyttet og sikker algoritme for denne bruk er DES-algoritmen.

DES-algoritmen (Data Encryption Standard) ble utviklet av IBM i samarbeid med National Bureau of Standards NBS) og publisert i 1977. DES er bare benyttet for sivil kryptering og er i dag det mest utbredte kryptosystem. Særlig er DES meget benyttet i bankverdenen og også i "DANKORT"-systemet.

I DES algoritmen blir kryptering utført i blokker på 64 biter ved hjelp av en nøkkel på 56 biter. Først blir de 64 biter som skal krypteres underkastet en permutasjon som tjener til å blande bitene da inngangen i den typiske anvendelse består av 8 byter. Ifølge dette blir 16 gjentatte krypteringer utført ved hjelp av forskjellige nøkler utledet fra den valgte nøkkel og klarteksten da de 64 biter før hver gjentakelse er blitt delt opp i en venstre side Li og en høyre side Ri hver bestående av 32 biter. I den i+1ste gjentakelse blir Ri overført som den neste venstre side Li+1 og den nye høyre side Ri+1 frembringes som XOR av Li og 32 andre biter som opptrer som en kompleks men fullstendig beskrevet funksjon av Ri og Ki+1 der Ki+1 er en nøkkel på 48 biter som er avledet fra den valgte nøkkel på 56 biter.

Selve funksjonen kan beskrives slik: De 32 biter i Ri endres til 48 biter ved bitskifting og blir deretter permutert. XOR for Ki+1 frembringes. De resulterende 48 biter telles 6 om gangen i 8 familier, som ved hjelp av S-boksene blir omdannet til 8 familier med bare 4 biter i hver, slik at 32 biter blir

avgitt. Etter en fast permutasjon av disse finnes de ovennevnte 32 biter.

Etter 16 iterasjoner blir de 64 biter permutert med den inverse permutasjon av den opprinnelige. Dette er nødvendig for å sikre at den påfølgende dekryptering av kryptoteksten kan foretas ved ganske enkelt å utføre DES-algoritmen igjen, men med de 16 avledede nøkler i omvendt orden.

Vedr. 2. Forskjellen mellom et symmetrisk kryptosystem og et asymmetrisk kryptosystem er at det ikke er mulig i et asymmetrisk system ved beregning å finne dekrypteringsnøkkelen selv om krypteringsnøkkelen er kjent, og omvendt.

Istedenfor "kryptering" og "dekryptering" er det derfor riktigere å snakke om en hemmelig omformingsnøkkel SK (Secret Key) og en offentlig omformingsnøkkel PK (Public Key). Særlig er det nødvendig for alle meldingen X at

$$PK(SK(X)) \rightarrow X \quad \text{og} \quad SK(PK(X)) \rightarrow X$$

Et asymmetrisk kryptosystem kan benyttes både til å skjule og til pålitelighet og til og med til frembringelse av digitale signaturer. Det skal imidlertid påpekes at for hver selvstendige bruker A som velger en nøkkel eller heller et par nøkler (PA, SA), kan A benytte SA til mottakning av hemmelige meldinger såvel som for sin egen digitale signatur og andre personers offentlige nøkler for å sende skjulte meldinger. På sin side kan andre personer benytte den offentlige nøkkel til A for å sende skjulte meldinger til A.

Et av de best kjente asymmetriske kryptosystemer er RSA kryptosystemet (oppkalt etter systemets fedre: Rivest, Shamir og Adelman). Det er basert på erfaringer som matematikere har gjort i løpet av flere tusen år når det gjelder primtall. Det er forholdsvis enkelt å bestemme om et bestemt valgt tall n er et primtall eller ikke. Men hvis det viser

seg at det ikke er et primtall vil vanskeligheten med å finne primtalldivisorene øke eksponensielt med størrelsen på tallet. Selv ved bruk av alle de midler matematikere har utviklet i tidens løp har det ikke vist seg mulig å finne en enkel måte til utledning av primtalldivisorene. Det er ekstremt mange tall med hundre sifre eller mindre (grensen i dag er omtrent 90) som det er praktisk talt umulig å oppløse i primfaktorer.

I RSA kryptosystemet er opprinnelsen to tilfeldig valgte primtall p og q på omtrent 100 sifre hver. Disse primtall må være sterke primtall som har den virkning at ved hjelp av kjente metoder vil det ta milliarder av år å finne divisorene i n på grunnlag av n = pq (p og q holdes hemmelig). Det er nødvendig at disse egenskaper finnes på grunn av sikkerheten i systemet. Deretter velges et tall e som må være primtall med (p-1)(q-1). Hvis man kjenner p og q er det mulig å finne et annet tall d med følgende egenskaper:

Hvis det er gitt et tilfeldig tall m mindre enn n, vil resten av m^de (dvs. m multiplisert med seg selv (d multiplisert med e) ganger) etter påfølgende divisjon av hele tall med n igjen gi tallet m.

Det er mulig på mange måter å dele meldinger i blokker som kan representeres entydig med tall mellom 1 og n, f.eks. ved hjelp av ASCII-koder. En klartekst m, som er representert på denne måte, blir deretter kryptert som

$$c=m^e \text{ modul } n,$$

dvs. at resten av m blir multiplisert med seg selv e ganger ved påfølgende deling av sifrene med n.

Dekryptering av c utføres ved beregning av

$$c^d \text{ modul } n$$

som i henhold til det ovenstående er lik m.

Paret av tall (e, n) kan naturligvis benyttes til å spesifisere en offentlig nøkkel, f.eks. nøkkelen

$$P(m)=m^e \text{ modul } n,$$

mens paret av tall (d, n) spesifiserer den hemmelige nøkkel

$$S(x)=x^d \text{ modul } n,$$

(det er bare d som må holdes hemmelig sammen med p og q).

Resultatet av dette er er offentlig nøkkelsystem.

Vedr. 3. Et viktig trekk for kryptosystemer er ofte at en viss hastighet blir garantert. Maskinvareutstyr der algoritmen er lagret i spesielt utformede brikker arbeider med langt større hastighet enn programvareutstyr. Det kan være spørsmål om en faktor på hundre eller mer avhengig av utstyret.

Som et eksempel skal nevnes at DES i programvare i f.eks. utstyr med en INTEL 8086 prosessor og en klokkefrekvens på 4,7 MHz krypterer med en hastighet på omtrent noen få tusen biter pr. sekund (det er muligheter for betydelige variasjoner avhengig av implementeringen).

Når det gjelder programvareimplementeringen for RSA vil de hurtigste 32 bitbrikker i dag, f.eks. MOTOROLA 68030, med en klokkefrekvens på 20 MHz frembringer en RSA blokkryptering med 512 biter på omtrent 4 sekunder og en dekryptering på omtrent 1 sekund (ved hjelp av et mindre matematisk kunstgrep). Ved hjelp av såkalte "digitale signalbehandlings"-brikker kan dette reduseres ytterligere, sannsynligvis til 1 sekund eller mindre for en kryptering.

På markedet i dag er det tilgjengelig "sorte bokser" inneholdende krypteringsbrikker som kan foreta kryptering med et høyt sikkerhetsnivå. En av disse såkalte SCP-bokser som i tillegg til å være en brikkekortleser med tastaturform PIN-kodekontroll også omfatter en skjerm, en forholdsvis hurtig CPU, 128 Kb direktelager og DES-enheten såvel som RSA-algoritmer. Boksen er utført slik at den tilintetgjør seg selv når det gjøres forsøk på å få fysisk adgang til elektronikken, dvs. at den er en såkalt "fuskesikker" boks. Den har en krypteringskapasitet på rundt 40 000 byter pr. minutt med DES-algoritme. Ved å benytte denne boks blir brikkekortets evne til å lagre nøkler benyttet for å sikre påliteligheten og ved hjelp av en tabell i leselageret i kombinasjon med brikkekortet kan nøkler utarbeides som er spesielle for den individuelle kryptering og overføring av informasjon.

Brikkekort

Fra et kryptologisk synspunkt har den eksplosive utvikling av meget små brikker ført til en meget interessant utvikling, dvs. brikkekortet. Dette kort har samme form og størrelse som et magnetisk kort, men inneholder videre, som nevnt ovenfor, en liten prosessor og et lite lager (i typiske tilfeller på 1-2 kbyter), som f.eks. kan være av typen EEPROM (Electrically Eraseable Programmable Read Only Memory), slik at adgang både til inngang og utgang kan oppnås via en kortleder.

Et kort av denne art er særlig egnet for lagring av f.eks. en hemmelig nøkkel. Det er videre mulig å beskytte denne nøkkel på en effektiv måte med en kryptering som er styrt av en PIN-kode, og ved å sikre nøkkelen slik at den ikke kan leses fra kortet, men bare kan benyttes for kryptering og dekryptering. Det er også mulig å la kartet ødelegge seg selv (logisk) hvis en gal PIN-kode benyttes mer enn f.eks. tre ganger, og ved å gi kortet en bestemt levetid (et bestemt antall anvendelser).

Detaljert beskrivelse av brikkekort

Brikkekortet inneholder en mikroprosessor, data- og programlager og en I/O port, med hemmelig informasjon og beskyttet informasjon skjult eller lagret i et datalager. Da I/O porten styres av mikroprosessoren, blir all lesing av informasjon styrt av denne mikro-prosessor. Lesing av hemmelige data er ikke mulig og lesing av beskyttet data er bare mulig etter positiv vurdering av PIN koden for kortet. Med riktig PIN kode er det mulig å kryptere og dekryptere data og frembringe midlertidige nøkler. For kryptering og dekryptering benyttes Data Encryption Standard (DES). I tillegg til operativsystemet for mikroprosessoren inneholder også programlageret krypteringsalgoritmen DES. Dette har som resultat at kortet i virkeligheten kan benyttes til å kryptere og dekryptere data selv om dette er en ganske langsom prosess (omtrent 128 byter pr. sekund).

Brikkekortene i sine nåværende versjoner (DES smartkort (Philips) og CP8 smartkort (Bull)) kan inneholde opptil 1024 byters informasjon innbefattende forskjellige "topptekster". Dette svarer til 500-800 byter av brukerinformasjon avhengig av oppbygningen av informasjonen i kortet.

Fire forskjellige korttyper finnes:

Satskort: Dette kort mottas sammen med de nye kort og blir benyttet når disse personaliseres.

Rotkort: Dette kort benyttes under personaliseringen for å dekryptere anvendelsesnøkler og personlige nøkler før de skrives inn i brikkekortet. Dette har den virkning at de personlige nøkler kan lagres i en fil i kryptert form og vil bare være kjent i lagre for personaliseringssystemet under utførelse av personaliseringen. Rotkortet inneholder for hver type av personlig nøkkel en tilsvarende rot-nøkkel.

Rehabiliteringskort: Benyttes ved rehabilitering av et transaksjonskort.

Transaksjonskort. Dette er det kort som deles ut til brukerene. Det benyttes til å lagre og beskytte personlige nøkler og til frembringelse av midlertidige nøkler for adgangsstyring og kryptering og dekryptering.

Levetiden for brikkekortet blir delt i forskjellige faser:

1. For-personalisering
2. Personalisering
3. Aktiv fase
4. Avsluttet levetid
5. Rehabilitering

Vedrørende 1. For-personalisering

I denne fase er kortet tomt bortsett fra fremstillingsinformasjon. Den eneste informasjon som finnes i kortet på dette tidspunkt er en produksjonsnøkkel og informasjon og hvilken "sats" kortet tilhører. For å få adgang til lageret i kortet er det nødvendig å kjenne til eller få adgang til produksjonsnøkkelen som bare kan fåes ved at man er i besittelse av det såkalte satskort som tilhører denne bestemte "sats".

Dette sikrer at bare innehaveren av satskortet kan personalisere kort og at innehaveren av satskortet bare kan personalisere kort som tilhører den "sats" det gjelder.

Vedrørende 2. Personalisering

Når produksjonsnøkkelen finnes i brikkekortet, er det mulig å innføre informasjon i lageret. Informasjonen kan for eksempel være hemmelige nøkler, DES identifikasjon, navnene på innehaveren av kortet og kortets utsteder etc. Når denne fase er over, går kortet over i sin aktive fase.

Vedrørende 3. Aktiv fase

I denne fase blir kortet benyttet av en bruker for kryptering og dekryptering og til frembringelse av midlertidige nøkler. Kortet kan benyttes inntil en av tre situasjoner oppstår:

a) Kortet blir gjort ugyldig med en instruksjon om avsluttet levetid.

b) Kontrollsonen i kortet er full. Kortet inneholder tre spesielle soner: styresone for produksjonsnøkkelen, styresone for anvendelsesnøkkelen og styresone for PIN. I de første to soner innføres en bit når det er gjort en feil ved presentering av nøkkelen. I den siste sone innføres det en bit hver gang det foretas en kontroll for PIN koden. Hvis den siste sone blir full, går kortet over i fasen for avslutning av levetiden. Dette vil skje etter et maksimum på 6000 presentasjoner av PIN koden. Innholdet i denne sone reduseres når brukerinformasjon og tjenestenøkler innføres i kortet.

c) Tre på hverandre følgende uriktige innføringer av PIN koden fører til at kortet blir sperret. Kortet kan åpnes igjen ved rehabilitering.

Vedrørende 4. Avsluttet levetid

I denne fase kan kortet ikke benyttes. Kortet kan rehabiliteres hvis det er blitt benyttet en uriktig PIN kode.

Vedrørende 5. Rehabilitering

Kortet kan rehabiliteres hvis kortets innehaver fremdeles husker den riktige PIN kode, men ellers ikke. Rehabilitering bør utføres av kortutstederen og innehaveren av kortet sammen. For å rehabilitere et brikkekort benyttes det et kort som er spesielt laget for dette formål, dvs. rehabiliteringskortet.

Utførelsen av brikkekortet gir en mulighet til lagring av nøkler som er beskyttet av PIN koden, eventuelt kryptert og dedikert til bruk av nøkler (for eksempel bare dekryptering). Samtidig vil innføringen av informasjon og nøkler i et brikkekort avhenge av om man har adgang både til rotkortet og satskortet, dvs. at bare bestemte personer har adgang til inngangsnøkler/informasjon.

Administrasjon av nøkler

Et av de største problemer i forbindelse med kryptosystemer i praktisk bruk er den egentlige håndtering av nøklene, da nøklene er systemets "grensesnitt" mot brukerene og utgjør det svakeste ledd i systemet.

Når en bruker får en nøkkel utlevert eller registrert, må det være mulig å identifisere ham på en tilfredsstillende måte. Nøkkelen holdes i et brikkekort som kan være tildelt en bestemt levetid og som, som nevnt ovenfor, også ødelegger seg selv når en gal PIN kode er blitt benyttet tre ganger.

Jo mer en nøkkel benyttes, jo større er risikoen for at nøkkelen blir kjent. Det er derfor nødvendig å forandre nøkkelen med jevne mellomrom. Når antall brukere blir stort og vilkårlige brukere må kommunisere med hverandre i kryptert form, er brukerene utstyrt med nøkler som ikke benyttes for datakryptering og filkryptering, men bare til utveksling av virkelige krypteringsnøkler.

En administrasjon blir skapt rundt sikkerhetssystemet og håndteringen av nøklene som

a) sikrer at brukte nøkler holdes hemmelige,

b) sikrer en mulighet til å gjenskape brukte hemmelige nøkler og en mulighet til å verifisere at en bestemt nøkkel er blitt benyttet for et spesielt formål,

c) gir en enkel og trygg tildeling av nøkler, og

d) hindrer bedrageri ved tildeling av brikkekort med en stabil og hermetisk prosedyre.

Prosedyren ved omsetning av nøkler i forbindelse med et brikkekort omfatter:

1. Frembringelse av nøkler
2. Innføring av nøkler og ønsket informasjon i brikkekortene
3. Fordeling av kortene
4. Fornyelse/tilbaketrekning av kort

Vedrørende 1. Frembringelse av kort

Nøklene for innføring av informasjon i brikkekortet frembringes på en slik måte at de både er forskjellige fra og frembringes med tilfeldige tall. Det er derfor ikke mulig å forutse eller gjette verdien av nøkkelen. For å starte programmet til frembringelse av nøkler må et brikkekort presenteres (sikret med en PIN kode). Nøklene som blir frembragt lagres i kryptert form i en fil ved hjelp av dette kort.

Vedrørende 2. Innføring av nøkler og ønsket informasjon i brikkekortet

Data (nøkler og eventuell informasjon) skal innføres i kortene frembringes ved bruk av filen der de tidligere ble innført. Denne bruk sørger for at disse data bare kan overføres fra den krypterte fil til et brikkekort av to forskjellige personer med to forskjellige brikkekort som har hver sin PIN kode. Det første kort er et kort som er tildelt kortutstederen og innholdet av dette er utelukkende kjent av produsenten som fremstiller de "tomme" brikkekort. Det andre datakort er et kort som følger den sats av kort som klargjøres. Av den grunn har den eller de personer som frembringer nøklene og informasjonen ingen mulighet til å innføre nøkler og informasjon i brikkekortene. På den annen

side har den eller de personer som innfører data i brikke-kortene ingen mulighet til å få kjennskap til det som innføres i kortene. Når kortene klargjøres, vil det bli foretatt en logging til en kryptert fil. Denne fil vil ha toleranse overfor feil og vil gjenspeile en alternativ fysisk posisjon. Filen vil bli sikret ved hjelp av en passende sikkerhetsrutine.

Vedrørende 3. Fordeling av kortene

Tradisjonelt blir kortene utstedt til brukere i satser. Kortet sendes for seg og PIN koden sendes separat. PIN koden blir sendt eller utlevert etter at kvittering for kortet er mottatt.

Vedrørende 4. Fornyelse/tilbaketrekning av kort

Når et kort er utløpt av en eller av grunn, må det returneres til kortutstederen så sant dette er mulig. Kortutstederen tilintetgjør kortet og utsteder eventuelt et nytt kort som erstatning for det gamle. Av sikkerhetsgrunner er det å foretrekke at når kort byttes ut, lages det et nytt kort som er forskjellig når det gjelder de innførte nøkler fra det kort som er løpt ut. Hvis en bruker slutter å benytte brikkekortet, må dette returneres til kortutstederen. Under alle omstendigheter blir kortet sperret elektronisk. En mulighet til sperring av kortet ved første presentasjon etter sperringen kan være en inngang i kortet.

Følges disse foranstaltninger, sikres det

at bare én person alene ikke kan frembringe et brikkekort,
at bare kortutstederen kan innføre informasjon og nøkler,
at nøklene kan frembringes når som helst for verifisering av bruken av et kort som er utløpt og at den rette bruker kommer i besittelse av kortene uten noen risiko for at kortet benyttes av uautoriserte personer.

Pålitelighet

Påliteligheten, dvs. den sikkerhet at de parter som er i bildet, sender/mottager er den de skal være, kan sikres på forskjellige måter avhengig av om systemet er

1. et symmetrisk system eller
2. et asymmetrisk system.

Vedrørende 1. Symmetrisk kryptosystem

For å sikre at en sender (A) og en mottager (B) er den de forutsettes å være, sender A et tall i kryptert form til B, og B verifiserer at tallet kommer fra A. Deretter sender B en kombinasjon av en del av tallet som B mottok fra A sammen med et tall frembragt av B i kryptert form til A. A kan deretter verifisere at kombinasjonen har kommet fra B og på samme tid kan A kontrollere den del av tallet som ble frembragt av A. A vil nå kryptere tallet som A mottok fra B og sende dette tilbake til B som etter verifisering kan se at B har mottatt den samme kombinasjon som B sendte til A. I det følgende blir det forklart hvordan et brikkekort kan benyttes for å sikre pålitelighet. Ved anvendelse av et symmetrisk kryptosystem må man vente en svak risiko for at en nøkkel brytes og at data leses av utenforstående. Denne risiko oppstår hvis en tidligere deltager i systemet med et godt kjennskap til typen av begynnelsesutveksling av meldinger er i besittelse av et gyldig brikkekort og hvis denne deltager tapper forbindelsen mellom sender og mottager og er i besittelse av det kryptoprogram som benyttes.

En slik person vil være i stand til å dekryptere dokumentene som utveksles, kryptert med den beskrevne nøkkel i den overføring det gjelder. Det vil imidlertid ikke være mulig å forandre innholdet av dokumentet og en fornyet desifrering vil også måtte gjøres ved tapping av den neste dokumentoverføring, siden en ny nøkkel benyttes for denne overføring.

I systemet ifølge oppfinnelsen er en brikkekortleser 122, 222 og 426 forbundet med hvert datasystem eller hver vert henholdsvis i datasystemene 100, 200 og 400.

De to datasystemer som utgjør sender og mottager med datasystemene 100 og 200 som er vist på fig. 1-4, er utstyrt med autoriserte brikkekort og er autorisert til å benytte disse.

Hvert kort 122 og 222 har to tjenestesoner for dette formål:

En tjenestesone med en "verifiseringsnøkkel" (Vk) som benyttes til å verifisere at krypteringen som motparten har benyttet er riktig.

En tjenestesone med en "signaturnøkkel" (Sk) som benyttes for kryptering av kommunikasjonen.

Vk kan bare benyttes til dekryptering og Sk kan bare benyttes for kryptering.

I den prosedyre som er vist på fig. 5, er de følgende forkortelser benyttet:

VkA:	Verifiseringsnøkkel for A eller datasystemet 100
SkA:	Signaturnøkkel for A eller datasystemet 100
VkB:	Verifiseringsnøkkel for B eller datasystemet 200
SkB:	Signaturnøkkel for A eller datasystemet 200
E:	Kryptering
D:	Dekryptering
R1, R2, R3:	Tilfeldige tall
M1, M2, M:	Overførte meldinger
IdA:	Offentlig kjent identifikasjon for A eller datasystemet 100
IdB:	Offentlig kjent identifikasjon for B eller datasystemet 200

Prosedyren fremgår av fig. 5.

Vedrørende 2. Asymmetrisk kryptosystem

Pålitelighetskontrollen som er beskrevet ovenfor under henvisning til fig. 5 er bare basert på anvendelse av et krypteringssystem som bygger på DES, men for fullstendighetens skyld er det asymmetriske system kort beskrevet nedenfor.

Hvis A eller datasystemet 100 skal sende en klartekst M som skal holdes hemmelig når den sendes, til B eller datasystemet 200, benytter A den offentlige nøkkel PB som tilhører B og som har B har offentliggjort for hvem som helst, og sender

$$PB(M) \rightarrow C$$

Bare B kan dekryptere, siden B kjenner hans private nøkkel og $SB(C) \rightarrow M$.

Hvis A skal sende en klartekst X til B i kryptert form på en slik måte at B kan kontrollere om meldingen kommer fra A, sender A

$$SA(X) \rightarrow Y$$

B prøver da med den offentlige nøkkel PA for A og finner

$$PA(Y) \rightarrow X$$

Hvis X er meningsfull, må SA være blitt benyttet, da bare A kan kryptere på en slik måte at PA kan dekryptere meldingen til noe med mening i. Det skal påpekes at påliteligheten bare sikres første gang meldingen X blir signert. I praksis må derfor en slik melding være egenartet, for eksempel ved å angi tiden på dagen.

Begge egenskaper kan oppnås på den følgende måte:

Hvis A ønsker å sende M til B, slik at B er sikker på at meldingen kommer fra A samtidig med at man sikrer at bare B av alle parter kan dekrypter meldingen, sender A

$$PB(SA(M))\rightarrow C.$$

Den eneste måte man kan avlede M er slik:

$$PA(SB(C))\rightarrow M$$

Integritet

Integriteten sikrer at data ikke blir endret under eller etter en fullført overføring. Dette sikres ved å beregne senderens (A) signatur og mottagerens (B) signatur, hvoretter disse føyes sammen med dokumentet og både A og B verifiserer disse signaturene. Med DES algoritme frembringes det signaturer som kan krypteres og verifiseres ved hjelp av brikkekort:

I systemet ifølge oppfinnelsen er det tilsluttet en brikkekortleser til hvert datasystem eller hver vert. De to datasystemer som utgjør sender og mottager 100 og 200, som vist på fig. 1-4, er utstyrt med autoriserte brikkekort og er autorisert til å benytte disse.

For dette formål har hvert kort tre tjenestesoner:

- En tjenestesone med en såkalt "verifiseringsnøkkel" (Vk) som benyttes til verifisering av signaturen som motparten har føyet til dokumentet.
- En tjenestesone med en "signaturnøkkel" (Sk) som benyttes til kryptering av signaturen.
- En tjenestesone med en "komprimeringsnøkkel" (Ck) som benyttes til frembringelse av signaturen (MAC).

Vk kan bare benyttes til dekryptering og Sk kan bare benyttes

til kryptering. Ck er identisk i alle brikkekort og kan benyttes for komprimering av dokumentet til signaturen.

I prosedyren som er vist på fig. 6 er de følgende forkortelser benyttet:

VkA:	Verifiseringsnøkkel for A eller datasystemet 100
SkA:	Signaturnøkkel for A eller datasystemet 100
MacA:	Det komprimerte dokument sett fra A's side
EmacA:	Kryptert MacA
VkB:	Verifiseringsnøkkel for B eller datasystemet 200
SkB:	Signaturnøkkel for B eller datasystemet 200
MacB:	Det komprimerte dokument sett fra B's side
EmacB:	Kryptert MacB
Ck:	Komprimeringsnøkkel
E:	Kryptering
D:	Dekryptering
C:	Komprimering
R1:	Tilfeldige tall som er utvekslet tidligere
M1, M2, M3:	Overførte meldinger
IdA:	Offentlig kjent identifikasjon for A
IdB:	Offentlig kjent identifikasjon for B

Prosedyren fremgår av fig. 6.

Integriteten sikres siden både sender og mottager er sikker på (med mulighet for kontroll) at dokumentet ikke er blitt endret før eller etter sendingen uten mulige forandringer som utvetydig kan bringes på det rene. Funksjonen *A2 er bygget opp på en slik måte at brikkekortet kan frembringe en nøkkel ved hjelp av en offentlig kjent identifikasjon som kan dekryptere den krypterte B/Mac og dermed danne grunnlag for en kontroll om at Mac som er føyet til dokumentet er gyldig, beregnet på grunnlag av det dokument som er mottatt av den ventede sender. Det samme gjelder i motsatt retning for funksjonen *B2.

Det er viktig at Mac'ene som frembringes er skjult i dokumentet, da de er egne signaturer for partene.

Sikkerheten ved adgangen til videotex systemet er vist på fig. 4.

Denne sikkerhet oppnås ved bruk av brikkekort for automatisk logging til videotex systemet:

1. Automatisk presentasjon av identifikasjon og passord.

2. Kryptering av kommunikasjon mellom terminal og videotex tjener.

3. Sikkerheten i videotex tjeneren når det gjelder den individuelle brukers adgang til de individuelle postbokser og anvendelser av systemet.

Vedrørende 1. Automatisk presentasjon av identifikasjon og passord

En brikkekortleser 422 av typen LECAM forbundet med en Minitel 409 har en intelligens som fører til at den leser i en bestemt posisjon på kortet med leting etter data for automatisert oppringing. Når oppringingen har funnet sted, vil anvendelsen som løper i videotex systemet overføre et program til RAM lageret i brikkekortleseren. Dette program vil da finne identifikasjonen og passordet i kortet og be om at PIN koden blir innført og kommuniserer med anvendelsen i videotex tjeneren. Hvis PIN koden oppgis uriktig, har programmet ingen mulighet til å samle informasjon i brikkekortet.

Vedrørende 2. Kryptering av kommunikasjon mellom terminal og videotex tjener

Det program som overføres til brikkekortleseren finner den nøkkel som skal benyttes for krypteringen ved å avlese

brikkekortet. Videotex anvendelsen leser en tabell i verten eller datasystemet 400 og finner en tilsvarende nøkkel. Kryptering foretas på grunnlag av denne nøkkel for hele kommunikasjonen mellom Minitel 400 og vert 400. Det er hensiktsmessig å benytte denne krypteringsnøkkel for å kryptere utvekslingen av den tilfeldig valgte nøkkel som benyttes til kryptering av resten av kommunikasjonen, da dette har som resultat at en forskjellig krypteringsnøkkel benyttes for hver enkelt kommunikasjon.

Vedrørende 3. Sikkerheten i videotex tjeneren når det gjelder den enkelte brukers adgang til de individuelle postbokser og anvendelsene av systemet.

Adgangen til postboksene, data og brukene i videotex tjeneren sikres ved "logg-inn" som gjøres på grunnlag av informasjonen som finnes i brikkekortet. Da utvekslingen av identifikasjon og passord finner sted i kryptert form, vil det ikke være mulig ved tapping av linjen og terminalen å rekonstruere disse. Med andre ord, vil det ikke være mulig å komme i kontakt med postboksen uten å være i besittelse av et brikkekort med en hemmelig PIN kode (som bare finnes i kortet).

Etter at det er oppnådd adgang til videotex systemet blir det sikret at adgang ikke kan oppnås til datamaskinen som er hovedvert. Dette gjøres for å unngå at datatyver ved en feil i videotex systemet kan få adgang til operativsystemet i datamaskinen som er vert.

Sikkerhet ved utveksling av dokumenter

Sikkerhetssystemet passer på at dokumenter som er bygget opp i henhold til EDIFACT standard kan overføres trygt mellom sammenkoblede verter.

Det blir sikret

1. at dokumentene kan forsynes med signatur,
2. at dokumentene ikke kan forfalskes,
3. at dokumentene bare kan leses av/overføres til den person som er autorisert, og
4. at det er mulig å skaffe utvetydig bevis i forbindelse med en mulig meningsutveksling.

Vedrørende 1. Dokumentene kan forsynes med en signatur

Senderen går gjennom dokumentet eller deler av dette for å frembringe et forkortet uttrykk av dokumentet (for eksempel en 64 biters nøkkel). Dette uttrykk inneholder minst et serienummer, dato, tidspunkt og alle de følsomme data. Uttrykket blir kryptert av et brikkekort med en nøkkel som finnes i kortet og som ikke kan leses, men bare benyttes for kryptering og dekryptering i kortet. Det krypterte resultat (MAC = Message Authentification Code) er spesielt for dette dokument og denne sender, og MAC blir tilføyet dokumentet hvoretter det er klart for "sending".

Vedrørende 2. Dokumentene kan ikke forfalskes

Hvis forandringer gjøres i dokumentet etter overføring betraktes som utført, vil det være mulig å forsikre seg om dette, da MAC'ene som er inkludert i dokumentet kan bli vurdert, hvoretter dokumentet godkjennes eller betraktes som ugyldig.

Vedrørende 3. Dokumentene kan bare leses av/overføres til den autoriserte person

Både sender og mottager forsikrer seg om at de er i kontakt med den rette person hvoretter dokumentet blir kryptert ved hjelp av en nøkkel som bare er kjent av sender og mottager og som er vilkårlig og bare gjelder denne ene overføring.

Vedrørende 4. Mulighet til frembringelse av utvetydig bevis i forbindelse med en eventuell meningsutveksling (MAC)

Dette sikres ved at kortutstederen holder de utstedte nøkler på en tilfredsstillende måte slik at det et hvilket som helst

tidspunkt kan bestemmes om det er identitet mellom et dokument og de tilknyttede MAC'er.

EDIFACT definisjon

EDIFACT (Electronic Data Interchange For Administration, Commerce and Transport) er en standardisert metode til elektronisk overføring av alle forretningsdokumenter som har en organisert struktur. Standarden - som er godkjent av ISO (International Standard Organization) - er beregnet for utveksling av dokumenter mellom datasystemer på både hjemlig og utenlandsk nivå. Standarden er derfor ikke avhengig av språk. Standarden foreskriver ikke hvorledes den egentlige nettverk kommunikasjon skal utføres. Den er en teknisk uavhengig standard.

Et EDIFACT dokument kan deles i bestemte deler eller moduler som kalles segmenter. Hvert segment har et bestemt formål for det dokument det gjelder og posisjonen av segmentet i meldingen er foreskrevet av standarden for den type det er tale om. Alle segmenter identifiseres med en kode med tre bokstaver som foreskrevet av standarden. En melding består av mange forskjellige segmenter som sammen inneholder all den informasjon som er nødvendig for å skape dokumentet.

Et segment kan for eksempel se slik ut:

CUM+DEM:IN'

CUX er en topptekst for segmentet, CUX betyr type av mynt
+ er et dataelement skilletegn
DEM betyr tyske mark - verdien kan være hva som helst annet som kan defineres vilkårlig så lenge både sender og mottager er enige om betydningen av kodene,
: er et datakomponent skilletegn
IN er en betegnelse for nota - men kan også defineres vilkårlig
' betegner slutt på et segment.

Innholdet i et segment kan deles i dataelementer. Et dataelement blir delt opp i en eller flere datakomponenter. I det eksempel som er gjengitt ovenfor med segmentet CUX, finnes det bare et dataelement. Dette dataelement består av to datakomponenter, nemlig DEM og IN.
: er det skilletegn som skiller sammenhørende datakomponenter, mens + er skilleanordningen for de enkelte dataelementer i et segment. Denne teknikk til beskrivelse av informasjonen i et dokument er generell og benyttes i alle EDIFAC segmenter.

De data som følger toppteksten for et gitt segment, er definert i standarden og kan derfor ikke forandres. Det er imidlertid ikke alle data som er nødvendige, da en god del kan utelates avhengig av behovet.

I meget stor utstrekning benyttes det koder i de enkelte segmenter. Med dette menes at for eksempel DEM i eksempelet ovenfor betyr tyske mark.

Begge parter i kommunikasjonen (sender og mottager) må være enige om bruken av disse, da de ikke er dekket av standarden.

P a t e n t k r a v

1.

Fremgangsmåte til overføring av data fra et første datasystem (100) til et andre datasystem (200) via en dataoverføringslinje (128, 228), hvor

en første stasjon (122) anvendes for utmating av data fra et første elektronisk kort (124), idet første stasjon (122) er forbundet med og kommuniserer med det første datasystemet (100) og dessuten er forbundet med dataoverføringslinjen (128, 228) via det første datasystemet (100) og et grensesnitt,

en andre stasjon (222) anvendes for utmating av data fra et andre elektronisk kort (224), idet den andre stasjonen (222) er forbundet med og kommuniserer med det andre datamaskinsystemet (200) og dessuten er forbundet med datatransmisjonslinjen (128, 228) via det andre datasystemet (200) og grensesnittet,

idet data overføres i kryptert form via nevnte første stasjon (122) til det første datasystem (100) og overføres derfra via grensesnittet for det første datasystemet (100) til dataoverføringslinjen (128, 228), og

hvor data mottas av det andre datasystemet (200) i kryptert form via grensesnittet for det andre datasystemet (200),

k a r a k t e r i s e r t v e d :

at det første og andre elektroniske kort (124, 224) er midlertidig forbundet med eller fjernbare fra hhv. første og andre stasjon (122, 222),

at nevnte første og andre elektroniske kort (122, 124) hver innbefatter en sentral databehandlingsenhet, en inngangs-/utgangsport for å kommunisere med korresponderende stasjon (122, 222), en krypterings-/dekrypteringsinnretning såvel som et indre lager og sammen utgjør et samhørende sett med elektroniske kort omfattende samhørende nøkkel eller nøkler tidligere lagret i det indre lageret for de elektroniske kortene (124, 224), idet nøkkelen eller nøklene anvendes som krypterings-/dekrypteringsnøkler eller anvendes

for å generere samhørende krypterings-/dekrypteringsnøkler, idet krypterings-/dekrypteringsnøklene mates inn i det indre lageret til de elektroniske kortene (124, 224), idet nøkkelen (nøklene) og de koherente krypterings-/dekrypteringsnøklene generert ved bruk av hemmelig nøkkel eller nøkler bare håndteres i de elektroniske kortene (124, 224),

at data overføres til det første elektroniske kortet (124) fra det første datasystemet (100) via første stasjon (122) og inngangs-/utgangsporten til det første elektroniske kortet (124), idet nevnte data innmates og lagres midlertidig i det interne lageret til det elektroniske kortet (124),

at data utmates fra det indre lageret til det første elektroniske kortet (124) og krypteres i det første elektroniske kortet (124) ved hjelp av krypterings-/dekrypteringsinnretningen til det første elektroniske kortet (124) og krypteringsnøkkelen eller -nøklene lagret i det indre lageret til det første elektroniske kortet (124), hvor data mates ut fra det første elektroniske kortet (124) i kryptert form via inngangs-/utgangsporten til det første elektroniske kortet (124) før overføring av kryptert data fra første datasystem (100) til det andre datasystem (200),

at overførte krypterte data overføres fra det andre datasystemet (200) til det andre elektroniske kortet (224) via den andre stasjonen (222) og via inngangs-/utgangsporten til det andre elektroniske kort (224) og mates inn og lagres midlertidig i det indre lageret til det andre elektroniske kortet (224),

at data mates ut fra det indre lageret til det andre elektroniske kort (224) i kryptert form og dekrypteres i det andre elektroniske kort (224) ved hjelp av krypterings-/dekrypteringsinnretningen til det andre elektroniske kort (224) og dekrypteringsnøkkelen eller -nøklene lagret i det indre lageret til det andre elekroniske kortet (224),

at data etter dekryptering i det andre elektroniske kortet (224) mates ut fra det andre elektroniske kortet (224) og tilføres det andre datasystemet via inngangs- eller utgangs-

porten til det andre elektroniske kortet (224) og via den andre stasjonen (222),

at data overføres fra første datasystem (100) til det andre datasystem (200) uten utveksling av hemmelige nøkler mellom datasystemene (100, 200), og

at dataoverføringen innbefatter en autentisitets-/integritetsverifikasjon.

2.

Fremgangsmåte som angitt i krav 1, k a r a k t e r i s e r t v e d at verifikasjonen av autentisiteten til det første elektroniske kort (124) i forhold til det andre elektroniske kort (224) og omvendt foretas før overføringen av data fra det første datasystem (100) til det andre datasystem (200).

3.

Fremgangsmåte som angitt i et hvilket som helst av de foregående krav, k a r a k t e r i s e r t v e d at innmatningen til og utmatningen fra krypteringen og dekrypteringen og eventuelt autentisitets- og integritetsverifiseringen styres selvstendig av den sentrale databehandlingsenhet i det individuelle kort (124, 224).

4.

Fremgangsmåte som angitt i et hvilket som helst av de foregående krav, k a r a k t e r i s e r t v e d at overføringen av data utføres i overensstemmelse med LECAM-protokollen.

5.

Fremgangsmåte som angitt i krav 1 eller 2, k a r a k t e r i s e r t v e d at pålitelighetskontrollen utføres ved :

at et første sett av data (R1) frembringes i det første elektroniske kort (124), hvilket sett av data innmates til og lagres i det interne lager i det første elektroniske kort

(124) og krypteres i det første elektroniske kort (124) ved hjelp av krypterings-/dekrypteringsanordningen i det første elektroniske kort (124) og krypteringsnøkkelen eller -nøklene som er lagret i det interne lager i det første elektroniske kort (124),

hvilket første sett av data (R1) utmates fra det første elektroniske kort (124) i kryptert form via inngangs-/utgangsporten i det første elektroniske kort (124) samt overføres via den første stasjon (122) til det første datasystem (100) og overføres derfra via grensesnittet for det første datasystem (100) til dataoverføringslinjen(128, 228),

hvilket første settav data (R1) mottas av det andre datasystem (200) i kryptert form via grensesnittet for det andre datasystem (200) samt overføres til det andre elektroniske kort (224) via den andre stasjon (222) og via inngangs-/utgangsporten for det andre elektroniske kort (224) og innmates inn i og lagres midlertidig i det interne lager i det andre elektroniske kort (224),

hvilket første sett av data (R1) som er mottatt av det andre datasystem (200) i kryptert form utmates fra det interne lager i det andre elektroniske kort (224) og dekrypteres i det andre elektroniske kort (224) ved hjelp av krypterings-/dekrypteringsanordningen i det andre elektroniske kort (224) og dekrypteringsnøkkelen eller -nøklene som er lagret i det interne lager i det andre elektroniske kort (224), og

hvilket første sett av data (R1) som mottas av det andre datasystem (200) i kryptert form og som er dekryptert i det andre elektroniske kort (224) innmates til og lagres i det interne lager i det andre elektroniske kort (224),

at et andre sett av data (R2) frembringes i det andre elektroniske kort (224), hvilket andre sett av data innmates til og lagres i det interne lager i det andre elektroniske kort (224),

at en første kombinasjon (R1, R2) av det første sett av data (R1) som mottas av det andre datasystem (200) i

kryptert form blir dekryptert og lagret i det interne lager i det andre elektroniske kort (224), mens det andre sett av data (R2) som er lagret i det interne lager i det andre elektroniske kort (224) frembringes i det andre elektroniske kort (224), hvilken første kombinasjon (R1, R2) innmates til og lagres i det interne lager i det andre elektroniske kort (224),

hvilken første kombinasjon (R1, R2) krypteres i det andre elektroniske kort (224) ved hjelp av krypterings-/dekrypteringsanordningen i det andre elektroniske kort (224) og krypteringsnøkkelen eller -nøklene som er lagret i det interne lager i det andre elektroniske kort (224),

hvilken første kombinasjon (R1, R2) utmates fra det andre elektroniske kort (224) i kryptert form via inngangs-/utgangsporten for det andre elektroniske kort (224) og overføres via den andre stasjonen (222) til det andre datasystem (200) og føres videre derfra via grensesnittet for det andre datasystem (200) til dataoverføringslinjen (128, 228),

hvilken første kombinasjon (R1, R2) mottas av det første datasystem (100) i kryptert form via grensesnittet for det første datasystem (100) samt overføres til det første elektroniske kort (124) via den første stasjon (122) og via inngangs-/utgangsporten for det første elektroniske kort (124) som innmatning til og for midlertidig lagring i det interne lager i det første elektroniske kort (124),

hvilken første kombinasjon (R1, R2) som mottas av det første datasystem (100) i kryptert form utmates fra det interne lager i det første elektroniske kort (124) og blir dekryptert i det første elektroniske kort ved hjelp av krypterings-/dekrypteringsanordningen i det første elektroniske kort (124) og dekrypteringsnøkkelen eller -nøklene som er lagret i det interne lager i det første elektroniske kort (124),

hvilken første kombinasjon (R1, R2) som mottas av det første datasystem (100) i kryptert form og blir dekryptert i det første elektroniske kort (124) innmates til og blir

lagret i det interne lager i det første elektroniske kort (124),

hvilken første kombinasjon (R1, R2) som er lagret i det interne lager i det første elektroniske kort (124) blir oppløst for å danne et første sett av data (R1) som overføres på nytt til det første elektroniske kort (124) og et andre sett av data (R2) som overføres til det første elektroniske kort (124),

hvilket første sett av data (R1) som overføres på nytt til det første elektroniske kort (124) og det andre sett av data (R2) som overføres til det første elektroniske kort (124) innmates til og lagres i det interne lager i det første elektroniske kort (124), og

hvilket første sett av data (R1) som er lagret i det interne lager i det første elektroniske kort (124) blir sammenlignet med det første sett av data (R1) som overføres på nytt til det første elektroniske kort (124) og lagres i det interne lager i det første elektroniske kort (124) for verifisering av identiteten mellom disse sett av data for verifisering av autentisiteten av det andre elektroniske kort (224) i forhold til det første elektroniske kort (124),

at et tredje sett av data (R3) frembringes i det første elektroniske kort (124), hvilket tredje sett av data (R3) innmates til og lagres i det interne lager i det første elektroniske kort (124),

at en andre kombinasjon (R2, R3) av det andre sett av data (R2) som mottas i kryptert form av det første datasystem (100) og som blir dekryptert og lagret i det interne lager i det første elektroniske kort (124), og det tredje sett av data (R3) som er lagret i det interne lager i det første elektroniske kort (124) frembringes i det første elektroniske kort (124), og hvilken andre kombinasjon (R2, R3) innmates til og lagres i det interne lager i det første elektroniske kort (124),

hvilken andre kombinasjon (R2, R3) blir kryptert i det første elektroniske kort (124) ved hjelp av krypterings-/dekrypteringsanordningen i det første elektroniske kort

(124) og krypteringsnøkkelen eller -nøklene som er lagret i det interne lager i det første elektroniske kort (124),

hvilken annen kombinasjon (R2, R3) utmates fra det første kort (124) i kryptert form via inngangs-/utgangsporten for det første elektroniske kort (124) og overføres via den første stasjon (122) til det første datasystem (100) og videreføres derfra via grensesnittet i det første datasystem (100) til dataoverføringslinjen (128, 228),

hvilken andre kombinasjon (R1, R2) som mottas av det andre datasystem (200) i kryptert form via grensesnittet for det andre datasystem (200), og overføres til det andre elektroniske kort (224) via den andre stasjon (222) og via inngangs-/utgangsporten for det andre elektroniske kort (224) innmates til og lagres midlertidig i det interne lager i det andre elektroniske kort (224),

hvilken andre kombinasjon (R1, R2) som mottas av det andre datasystem (200) i kryptert form utmates fra det interne lager i det andre elektroniske kort (224) og blir dekryptert i det andre elektroniske kort (224) ved hjelp av krypterings-/dekrypteringsanordningen for det andre elektroniske kort (224) og dekrypteringsnøkkelen -nøklene som er lagret i det interne lager i det andre elektroniske kort (224),

hvilken andre kombinasjon (R1, R2) som mottas av det andre datasystem (200) i kryptert form og blir dekryptert innmates til og lagres i det interne lager i det andre elektroniske kort (224),

hvilken andre kombinasjon (R1, R2) som er lagret i det interne lager i det andre elektroniske kort (224) blir oppløst for å frembringe et andre sett av data (R2) som overføres på nytt til det andre elektroniske kort (224) og det tredje sett av data (R3) som overføres til det andre elektroniske kort (224),

hvilket andre sett avdata (R2) som overføres på nytt til det andre elektroniske kort (224) og tredje sett av data (R3) som overføres til det andre elektroniske kort (224)

innmates til og lagres i det interne lager i det andre elektroniske kort (224), og

hvilket andre sett av data (R2) som er lagret i det interne lager i det andre elektroniske kort (224) blir sammenlignet med det andre sett av data (R2) som er overført på nytt til det andre elektroniske kort (224) og lagret i det interne lager i det andre elektroniske kort (224) til bekreftelse av identiteten mellom disse sett av data for autentisitets-verifisering av det første elektroniske kort (124) i forhold til det andre elektroniske kort (224).

6.

Fremgangsmåte som angitt i krav 1, k a r a k t e r i s e r t v e d at integritetsverifiseringen foretas ved

å frembringe en komprimert versjon av data i det første datasystem (100) eller i det første elektroniske kort (124), hvilken komprimerte versjon innmates til og lagres i det interne lager i det første elektroniske kort (124),

å frembringe en komprimert versjon av data som er overført til det andre datasystem (200) som er frembragt i det andre datasystem (200) eller i det andre elektroniske kort (224), hvilken komprimerte versjon innmates til og lagres i det interne lager i det andre elektroniske kort (224),

å utmate av den komprimerte versjon som er lagret i det interne lager i det første elektroniske kort (124) fra det interne lager i det første elektroniske kort (124) med kryptering i det første elektroniske kort (124) ved hjelp av krypterings-/dekrypteringsanordningen i det første elektroniske kort (124) og krypteringsnøkkelen eller -nøklene som er lagret i det interne lager i det første elektroniske kort (124),

å utmate den komprimerte dataversjon som er kryptert med krypterings-/dekrypteringsanordningen i det første elektroniske kort (124) fra det første elektroniske kort (124) via inngangs-/utgangsporten for det første elektroniske kort (124) med overføring via den første stasjon (122) til

det første datasystem (100) og overføring derfra via grensesnittet for det første datasystem (200) til overføringslinjen (128, 228),

å motta den krypterte og komprimerte dataversjoner som overføres fra det første datasystem (100) ved det andre datasystem (200) via grensesnittet for det andre datasystem (200) med overføring til det andre elektroniske kort (224) via den andre stasjon (222) og via inngangs-/utgangsporten for det andre elektroniske kort (224), for innføring i og midlertidig lagring i det interne lager i det andre elektroniske kort (224),

å utmate den komprimerte dataversjon som mottas av det andre datasystem (200) i kryptert form fra det interne lager i det andre elektroniske kort (224) med dekryptering i det andre elektroniske kort (224) ved hjelp av krypterings-/dekrypteringsanordningen i det andre elektroniske kort (224) og dekrypteringsnøkkelen eller -nøklene som er lagret i det interne lager i det andre elektroniske kort (224),

å innmate den dekrypterte, komprimerte dataversjon som mottas av det andre datasystem (200) i kryptert form og dekryptert av det andre elektroniske kort (224) for innføring og lagring i det interne lager i det andre elektroniske kort (224), og

å sammenligne de komprimerte dataversjoner som er lagret i det andre elektroniske kort (224) med de dekrypterte, komprimerte dataversjoner som ble mottatt av det andre datasystem (200) i kryptert form og etter dekryptering er utført i det andre elektroniske kort (224) for verifisering av integriteten eller identiteten mellom data som overføres fra det første datasystem (100) og data som mottas av det andre datasystem (200).

7.

Fremgangsmåte som angitt i krav 1, k a r a k t e r i s e r t v e d at integritetsverifiseringen foretas ved

å frembringe en komprimert versjon av data i det første datasystem (100) eller i det første elektroniske kort

(124), hvilken komprimerte versjon innmates til og lagres i det interne lager i det første elektroniske kort (124),

å frembringe en komprimert versjon av data som er overført til det andre datasystem (200) som er frembrakt i det andre datasystem (200) eller i det andre elektroniske kort (224), hvilken komprimerte versjon innmates til og lagres i det interne lager i det andre elektroniske kort (224),

å utmate den komprimerte versjon som er lagret i det interne lager i det andre elektroniske kort (224) fra det interne lager i det andre elektroniske kort (224) med kryptering i det andre elektroniske kort (224) ved hjelp av krypterings-/dekrypteringsanordningen for det andre elektroniske kort (224) og krypteringsnøkkelen eller -nøklene som er lagret i det interne lager i det andre elektroniske kort (224),

å utmate de komprimerte dataversjoner som er kryptert med krypterings-/dekrypteringsanordningen i det andre elektroniske kort (224) fra det andre elektroniske kort (224) via inngangs-/utgangsporten for det andre elektroniske kort (224) med overføring via den annen stasjon (222) til det andre datasystem (200) og overføring derfra via grensesnittet for det andre datasystem (200) til dataoverføringslinjen (128, 228),

å motta krypterte og komprimerte dataversjoner som overføres fra det andre datasystem (200) ved det første datasystem (100) via grensesnittet for det første datasystem (100) med overføring til det første elektroniske kort (224) via den første stasjon (122) og via inngangs-/utgangsporten for det første elektroniske kort (124), for innmatning til og midlertidig lagring i det interne lager i det første elektroniske kort (124),

å utmate de komprimerte dataversjoner som mottas av det første datasystem (100) i kryptert form fra det interne lager i det første elektroniske kort (124) med dekryptering i det første elektroniske kort (124) ved hjelp av krypterings-/dekrypteringsanordningen i det første elektroniske kort

(124) og dekrypteringsnøkkelen (nøklene) som er lagret i det interne lager i det første elektroniske kort (124),

å innmate de dekrypterte, komprimerte dataversjoner som mottas av det første datasystem (100) i kryptert form og dekryptert i det første elektroniske kort (124), til og for til og for lagring i det interne lager i det første elektroniske kort (124), og

å sammenligne de komprimerte dataversjoner som er lagret i det første elektroniske kort (124) med de dekrypterte, komprimerte dataversjoner som ble mottatt av det første datasystem (100) i kryptert form og etter dekryptering er utført i det første elektroniske kort (124) for verifisering av integriteten eller identiteten mellom de data som overføres fra det første datasystem (100) og de data som mottas av det andre datasystem (200).

8.

Fremgangsmåte som angitt i kravene 6 og 7, k a r a k t e r i s e r t v e d at en overføring av en komprimert dataversjon fra det første elektroniske kort (124) til det andre elektroniske kort (224) såvel som fra det andre elektroniske kort (224) til det første elektroniske kort (124) og en sammenligning av begge de overførte, komprimerte dataversjoner med de lagrede, komprimerte dataversjoner i de nevnte to elektroniske kort (124, 224) utføres for integritetsverifiseringen.

9.

Fremgangsmåte som angitt i krav 6 eller 8, k a r a k t e r i s e r t v e d at overføringen av den komprimerte dataversjon som frembringes i det første datasystem (100) eller i det første elektroniske kort (124) fra det første elektroniske kort (124) til det andre elektroniske kort (124) utføres samtidig med overføringen av selve dataene, hvilke data og komprimerte dataversjoner settes sammen og krypteres som et hele før overføringen.

10.
Fremgangsmåte som angitt i krav 7 eller 8, k a r a k t e r i s e r t v e d at overføringen av de komprimerte dataversjoner som frembringes i det andre datasystem (200) eller i det andre elektroniske kort (224) fra det andre elektroniske kort (224) til det første elektroniske kort (124) foregår samtidig med en ny overføring av data som mottas fra det første elektroniske kort (124) fra det andre elektroniske kort (224) til det første elektroniske kort (124), hvilke data som skal sendes på nytt og de komprimerte dataversjoner settes sammen og krypteres som et hele før overføringen.

11.
Fremgangsmåte ifølge krav 8, k a r a k t e r i s e r t v e d at overføringen fra det andre elektroniske kortet (224) til det første elektroniske kortet (124) av den komprimerte dataversjonen generert i det andre datasystemet (200) eller i det andre elektroniske kortet (224) utføres samtidig med en sending på nytt fra det andre elektroniske kortet (224) til det første elektroniske kortet (124) med den komprimerte dataversjonen mottatt av det andre elektroniske kortet (224), hvor overføringen og sendingen pånytt av komprimerte dataversjoner også gjøres samtidig med en ny sending fra det andre elektroniske kortet (224) til det første elektroniske kortet (124) med data mottatt av det andre elektroniske kortet (224), hvor data som skal sendes på nytt og komprimerte dataversjoner kombineres og krypteres som et hele før overføringen.

12.
Fremgangsmåte ifølge krav 5, k a r a k t e r i s e r t v e d at krypteringsnøkkelen anvendt for kryptering av det første datasett (R1) og den andre kombinasjonen (R2, R3) utføres ved bruk av en første signaturnøkkel (SkA) lagret i det første elektroniske kortet (124),

at dekrypteringsnøkkelen anvendt for dekryptering av den krypterte formen av første datasett (R1) og den krypterte

formen av den andre kombinasjonen (R2, R3) utføres ved bruk av en andre verifikasjonsnøkkel (VkB) lagret i det andre elektroniske kortet (224) og en offentlig kjent identifikasjon (IdA) til det første elektroniske kortet (124),

at krypteringsnøkkelen anvendt for kryptering av den første kombinasjonen (R1, R2) utføres ved bruk av en andre signaturnøkkel (SkB) lagret i det andre elektroniske kortet (224), og

at dekrypteringsnøkkelen anvendt for dekryptering av den krypterte formen av den første kombinasjonen (R1, R2) utføres ved bruk av en første verifikasjonsnøkkel (VkA) lagret i det første elektroniske kortet (124) og en offentlig nøkkelidentifikasjon (IdB) til det andre elektroniske kortet (224).

13.

Fremgangsmåte ifølge krav 5 eller 12, k a r a k t e r i s e r t v e d at krypterings- og dekrypteringsnøkkelen anvendt for kryptering og dekryptering av overført data utføres ved bruk av et første datasett (R1) generert i autentisitetsverifisering som utføres før overføring av data.

14.

Fremgangsmåte ifølge krav 9, k a r a k t e r i s e r t v e d at den komprimerte dataversjonen krypteres ved bruk av en første signaturnøkkel (SkA), som er lagret i det første elektroniske kortet (124) før kombinering med data og ytterligere kryptering som et hele, og

at den krypterte komprimerte dataversjonen dekrypteres ved bruk av en andre verifikasjonsnøkkel (VkB) lagret i det andre elektroniske kortet (224) og en offentlig kjent identifikasjon (IdA) til det første elektroniske kortet (124) ette atr kombinasjonen av dataene og den komprimerte dataversjonen er blitt overført og dekryptert som et hele.

15.

Fremgangsmåte ifølge krav 5 og 9, eller 5 og 12, k a r a k t e r i s e r t v e d at krypterings- og dekrypterings-

nøkkelen anvendt for kryptering og dekryptering av kombinasjonen av data og av komprimert dataversjon utføres ved bruk av et første sett av data (R1) generert ved autentisitets-verifiseringen som er gjort før overføring av dataene.

16.

Fremgangsmåte ifølge krav 10, k a r a k t e r i s e r t v e d

at den komprimerte dataversjonen krypteres ved bruk av en andre signaturnøkkel (SkB), som er lagret i det andre elektroniske kortet (224) før kombineringen med data som skal bli sendt på nytt og ytterligere kryptering som et hele, og

at krypterte, komprimerte data dekrypteres ved bruk av en verifikasjonsnøkkel (VkA) lagret i det første elektroniske kortet (124) og en offentlig kjent identifikasjon (IdB) til det andre elektroniske kortet (224) etter kombinasjon av data som skal bli sendt på nytt, og den komprimerte dataversjonen har blitt overført og dekryptert som et hele.

17.

Fremgangsmåte ifølge krav 5 og 10, eller 5 og 12, k a r a k t e r i s e r t v e d at krypterings- og dekrypteringsnøkler anvendt for kryptering og dekryptering av kombinasjonen med data som skal bli sendt på nytt og komprimert dataversjon utføres ved bruk av et første datasett (R1) generert i autentiserings-verifisseringen som er utført før overføringen av data.

18.

Fremgangsmåte ifølge krav 8, k a r a k t e r i s e r t v e d

at overføring fra det første elektroniske kortet (124) til det andre elektroniske kortet (224) av den komprimerte dataversjonen generert ved det første datasystemet (100) eller i det første elektroniske kortet (124) utføres samtidig med overføringen av selve dataene, idet data og den komprimerte dataversjon kombineres og krypteres som et hele før overføringen,

at overføringen fra det andre elektroniske kortet (224) til det første elektroniske kortet (124) av den komprimerte dataversjonen generert til det andre datasystemet (200) eller i det andre elektroniske kortet (124) utføres samtidig med sending på nytt fra det andre elektroniske kortet (224) til det første elektroniske kortet (124) av den komprimerte dataversjonen mottatt av det andre elektroniske kortet (224), idet overføringen og sendingen på nytt av den komprimerte dataversjonen også utføres samtidig med en sending på nytt fra det andre elektroniske kortet (224) til det første elektroniske kortet (124) av data mottatt av det andre elektroniske kortet (224), idet data som skal bli sendt på nytt og de komprimerte dataversjoner kombineres og krypteres som et hele før overføringen.

19.

Fremgangsmåte ifølge et hvilket som helst av kravene 6, 7, 9, 10 eller 18, k a r a k t e r i s e r t v e d at komprimerte data genereres ved bruk av en felles kompresjonsnøkkel (Ck) forhåndslagret i de elektroniske kortene (124, 224).

20.

Fremgangsmåte ifølge krav 1 eller 2, k a r a k t e r i s e r t v e d

at krypteringsnøkkelen (nøklene) lagret i det indre lageret til det første elektroniske kortet (124) innbefatter en første krypteringsnøkkel dannet ved bruk av en første signaturnøkkel (SkA) lagret i det første elektroniske kortet (124),

at dekrypteringsnøkkel eller -nøkler lagret i det indre lageret i det andre elektroniske kortet (224) innbefatter en andre dekrypteringsnøkkel dannet ved bruk av en andre verifikasjonsnøkkel (VkB) lagret i det andre elektroniske kortet (224) og en offentlig kjent identifikasjon (IdA) for det første elektroniske kortet (124),

at krypteringsnøkkel eller -nøkler lagret i det indre lageret i det andre elektroniske kortet (224) innbefatter en andre krypteringsnøkkel dannet ved bruk av en andre signaturnøkkel (SkB) lagret i det andre elektroniske kortet (224),

at dekrypteringsnøkkel eller -nøkler lagret i det indre lageret til det første elekroniske kortet (124) innbefatter en første dekrypteringsnøkkel dannet ved bruk av en første verifikasjonsnøkkel (VkA) lagret i det første elektroniske kortet (124) og en offentlig kjent identifikasjon (IdB) til det andre elektroniske kortet (224), og idet autentisitetsverifiseringen omfatter trinnene:

a) å generere første tilfeldige tall (R1) i senderen,

b) å kryptere det første tilfeldige tall (R1) ved bruk av denførste krypteringsnøkkel for å tilveiebringe en første autentisitetsmelding i det første elektroniske kortet (124)

c) å sende den første autentisitetsmeldingen til det andre elektroniske kortet (224),

d) å dekryptere den første autentisitetsmeldingen i det andre elektroniske kortet (224) ved bruk av den andre dekrypteringsnøkkelen for å tilveiebringe det første tilfeldige tall (R1) i det andre elektroniske kortet (224),

e) å generere det andre tilfeldige tall (R2) i mottakeren,

f) å kombinere det første tilfeldige tallet (R1) med det andre tilfeldige tallet (R2) for å tilveiebringe den første kombinasjonen (R1, R2) i det andre elektroniske kortet (224),

g) å kryptere den første kombinasjonen (R1, R2) ved bruk av den andre krypteringsnøkkelen for å tilveiebringe en andre autentisitetsmelding med det andre elektroniske kortet (224),

h) å sende den andre autentisitetsmeldingen til det første elektroniske kortet (124),

i) å dekryptere av den andre autentisitetsmeldingen i det elektroniske kortet (124) ved bruk av den første dekryp-

teringsnøkkel som tilveiebringer den første kombinasjonen (R1, R2) i det første elektroniske kortet (R1, R2),

j) å separere mottatte første kombinasjon (R1, R2) i det første elektroniske kortet (124),

k) å sammenligne verdien til det første tilfeldige tallet (R1) generert i senderen med verdien av det første tilfeldige tallet (R1) mottatt fra det andre elektroniske kortet (224) og lagret i det første elektroniske kortet (124) og i tilfelle at de to verdier er like, verifisering av autentisiteten til identiteten for det andre elektroniske kortet (224),

l) å generere et tredje tilfeldig tall (R3) i senderen,

m) å kombinere det mottatte andre tilfeldige tallet (R2) med det tredje tilfeldige tallet (R3) for å tilveiebringe en andre kombinasjon (R2, R3) i det første elektroniske kortet (124),

n) å kryptere den andre kombinasjonen (R2, R3) ved bruk av den første krypteringsnøkkelen for å tilveiebringe en tredje autentisitetsmelding i det første elektroniske kortet (124),

o) å sende den tredje autentisitetsmeldingen til det andre elektroniske kortet (224),

p) å dekryptere den tredje autentisitetsmeldingen i det andre elekroniske kortet (224) ved bruk av den andre dekrypteringsnøkkelen for å tilveiebringe en andre kombinasjon (R2, R3) i det andre elektroniske kortet (224),

q) å separere den mottatte andre kombnasjonen (R2, R3) i det andre elektroniske kortet (224), og

r) å sammenligne verdien av det andre tilfeldige tallet (R2) generert i mottakeren ved verdien av det andre tilfeldige tallet (R2) mottatt fra det første elektroniske kortet (124) og lagret i det andre elektroniske kortet (224) og i tilfelle av at de to verdiene er like, verifisering av autentisiteten til identiteten for det første elektroniske kortet (124).

21.

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

at krypteringsnøkkelen (nøklene) lagret i det indre lageret i det første elektroniske kortet innbefatter en første krypteringsnøkkel dannet ved bruk av en første signaturnøkkel (SkA) lagret i det første elekroniske kortet (124),

at dekrypteringsnøkkel eller -nøkler lagret i det indre lageret i det andre elektroniske kortet (224) innbefatter en andre dekrypteringsnøkkel dannet ved bruk av den andre verifiseringsnøkkel (VkB) lagret i det andre elektroniske kortet (224) og en offentlig kjent identifikasjon (IdA) for det første elektroniske kortet (124),

at krypteringsnøkkel eller -nøkler lagret i det indre lageret i det andre elektroniske kortet (224) innbefatter en andre krypteringsnøkkel dannet ved bruk av en andre signaturnøkkel (SkB) lagret i det andre elektroniske kortet (224),

at dekrypteringsnøkkel eller -nøkler lagret i det indre lageret i det første elektroniske kortet (124) innbefatter en første dekrypteringsnøkkel dannet ved bruk av en første verifikasjonsnøkkel (VkA) lagret i det første elektroniske kortet (124) og en offentlig kjent identifikasjon (IdB) for det andre elektroniske kortet (224),

at en felles komprimeringsnøkkel (Ck) lagres i det indre lageret i det første elektroniske kortet (124) og i det indre lageret til det andre elektroniske kortet (224),

at krypteringsnøkkel eller -nøkler lagret i det indre lageret i det første elektroniske kortet (124) og i det indre lageret til det andre elektroniske kortet (224) innbefatter en tilfeldig krypteringsnøkkel dannet ved bruk av et tidligere utvekslet tilfeldig tall (R1),

at dekrypteringsnøkkel eller -nøkler lagret i det indre lageret i det første elektroniske kortet (124) og i det indre lageret i det andre elektroniske kortet (224) innbefatter en tilfeldig dekrypteringsnøkkel dannet ved bruk av et tidligere utvekslet tilfeldig tall (R1), og

at integritetsverifiseringen omfatter trinnene:

a) å generere et første komprimert dokument (MacA) med data i senderen ved bruk av felles kompresjonsnøkkel (Ck),

b) å kryptere første komprimerte dokument (MacA) ved bruk av en første krypteringsnøkkel for å tilveiebringe et kryptert første komprimerte dokument (EmacA) i det første elektroniske kortet (124),

c) å kombinere data og det krypterte første komprimerte dokumentet (EmacA) til en første kombinasjon og kryptering av en første kombinasjon ved å bruke den tilfeldige krypteringsnøkkel for å tilveiebringe en første integritetsmelding i det elektroniske kortet (124),

d) å sende den første integritetsmeldingen til det andre elektroniske kortet (224),

e) å dekryptere den første integritetsmelding i det andre elektroniske kortet ved bruk av den tilfeldige dekrypteringsnøkkel for å tilveiebringe den første kombinasjonen i det andre elektroniske kortet (224),

f) å separere den første kombinasjon i det andre elektroniske kortet (224),

g) å generere i mottageren den andre versjonen av det første komprimerte dokumentet (MacA) av mottatt data ved bruk av den felles komprimeringsnøkkelen (Ck),

h) å dekryptere det mottatte, krypterte første komprimerte dokument (EmacA) i det andre elektroniske kortet (224) ved bruk av den andre dekrypteringsnøkkelen for å tilveiebringe en første versjon av det første komprimerte dokumetet (MacA),

i) å sammenligne tilveiebragte resultater av første og andre versjon av første komprimerte dokument (MacA), og i tilfelle at de to versjonene er like å redusere i mottageren integriteten til sendingen av data fra første elektroniske kort (124) til andre elektroniske kort (224),

j) å generere i mottageren et andre komprimerte dokument (MacB) av den første kombinasjonen ved bruk av den felles komprimeringsnøkkel (Ck),

k) å kryptere det andre komprimerte dokument (MacB) ved bruk av den andre krypteringsnøkkel for å tilveiebringe et

kryptert andre komprimert dokument (EmacB) i det andre elektroniske kort (224),

l) å kombinere den første kombinasjonen og det kryptert andre komprimerte dokument (EmacB) til en andre kombinasjon og kryptere den andre kombinasjonen ved bruk av den tilfeldige krypteringsnøkkelen for å tilveiebringe en andre integritetsmelding i det andre elektroniske kort (224),

m) å sende den andre integritetsmeldingen til det første elektronisk kort (124),

n) å dekryptere den andre integritetsmeldingen i det første elektroniske kortet (124) ved bruk av den tilfeldige dekrypteringsnøkkelen for å tilveiebringe en andre kombinasjon i det første elektroniske kortet (124),

o) å separere den andre kombinasjonen i det første elektroniske kortet (124),

p) å generere i senderen en andre versjon av det andre komprimerte dokumentet (MacB) av den mottatte første kombinasjon ved bruk av den felles komprimeringsnøkkelen (Ck),

q) å dekryptere det mottatte, krypterte andre komprimerte dokument (EmacB) i det første elektroniske kort (124) ved bruk av den første dekrypteringsnøkkelen for å tilveiebringe en første versjon av det andre komprimerte dokumentet (MacB), og

r) å sammenligne tilveiebragte resultater av første og andre versjon av det andre komprimerte dokumentet (MacB), og i tilfelle de to versjoner er like å verifisere i senderen integriteten til sendingen av data fra første elektroniske kort (124) til andre elektroniske kort (224).

22.

Fremgangsmåte ifølge krav 20 og 21, k a r a k t e r i s e r t v e d at de tidligere utvekslede tilfeldige tall (R1) er blitt utvekslet i autentisitesverifiseringen.

23.

System for overføring av data fra et første datasystem (100) til et andre datasystem (220), hvilket andre datasystem (200) er autonomt i forhold til det første datasystem (100) via en datatransmisjonslinje (128, 228), ifølge fremgangsmåten ifølge et hvilket som helst av kravene 1-11, idet systemet innbefatter en første stasjon (122) og en andre stasjon (222), som er sammenkoblet til å kommunisere med henholdsvis det første og det andre datasystem (100, 200), og som dessuten er koblet via henholdsvis første og andre datasystem (100, 200) og korresponderende grensesnitt til dataoverføringslinjen (128, 228), så vel som første og andre elektroniske kort (124, 224), k a r a k t e r i s e r t v e d at

det første og andre elektroniske kort (124, 224) er midlertidig forbundet med eller fjernbart fra henholdsvis første og andre stasjon (122, 222),

at det første og det andre elektroniske kort (124, 224) hver innbefatter en sentral databehandlingsenhet, en inngangs-/utgangsport for kommunikasjon med korresponderende stasjon (122, 222), en krypterings-/dekrypteringsinnretning så vel som et indre lager og sammen utgjør et samsvarende sett med elektroniske kort (124, 224) innbefattende samsvarende hemmelig nøkkel eller nøkler som er tidligere lagret i det indre lageret i de elektroniske kortene (124, 224), idet de hemmelige nøklene anvendes som krypterings-/dekrypteringsnøkler eller anvendes for generering av samhørende krypterings-/dekrypteringsnøkler, idet krypterings-/dekrypteringsnøklene er matet inn i det indre lageret til de elektroniske kortene (124, 224), og hvor den hemmelige nøkkelen (nøklene) og nevnte samhørende krypterings-/dekrypteringsnøkler generert ved bruk av den hemmelige nøkkel (nøklene) kun håndteres i de elektroniske kortene (124, 224).

24.

System ifølge krav 23, k a r a k t e r i s e r t v e d at det første og andre elektroniske kort (124, 224) er av typen DES Smart Kort fra firma Philips, Super Smart Kort fra firma Bull eller CP8 Smart Kort fra firma Bull.

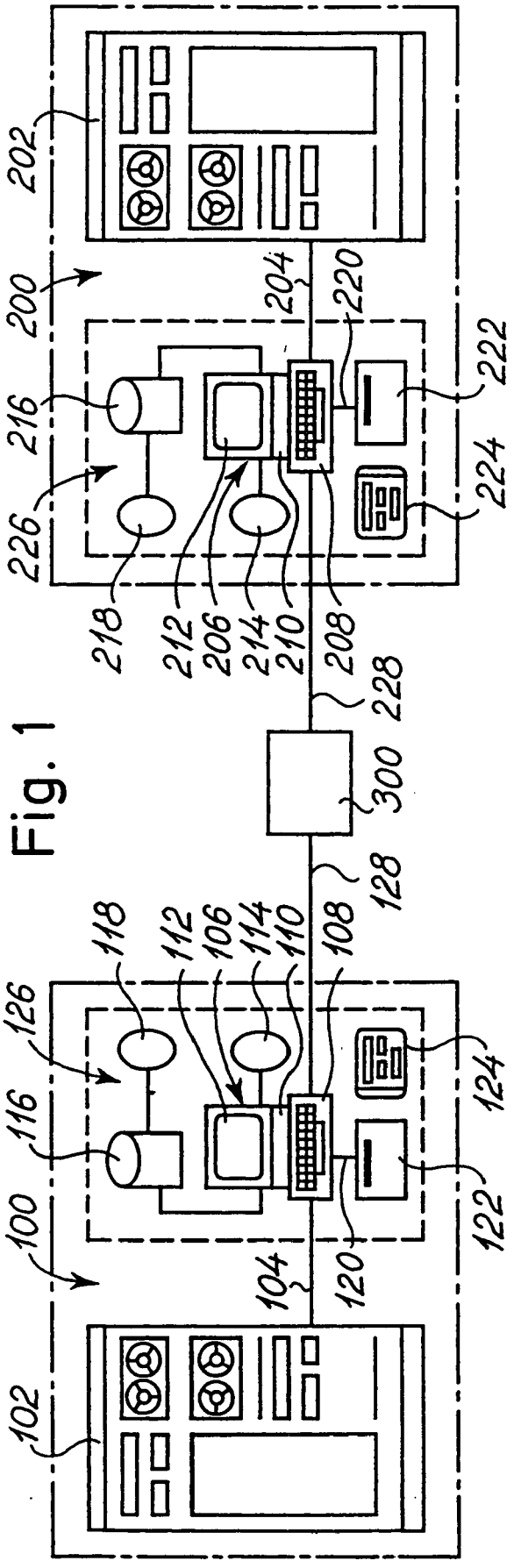

202
200
204
220
222
216
226
224
218
212
206
214
210
208
228
300
128
118
112
106
114
110
108
126
116
124
100
122
104
120
102

Fig. 1

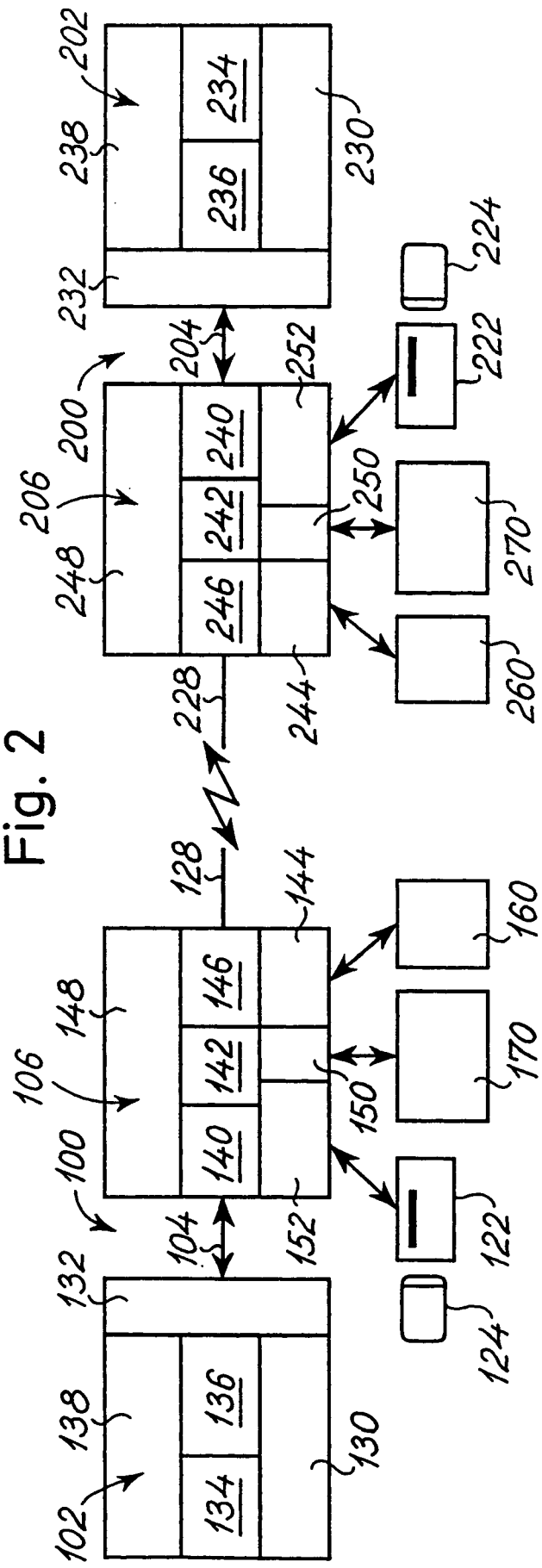

202
238
234
236
230
232
224
204
222
252
200
206
240
242
250
248
246
270
260
228
244
128
144
160
148
146
106
142
170
150
100
140
104
152
122
132
124
138
136
130
134
102

Fig. 2

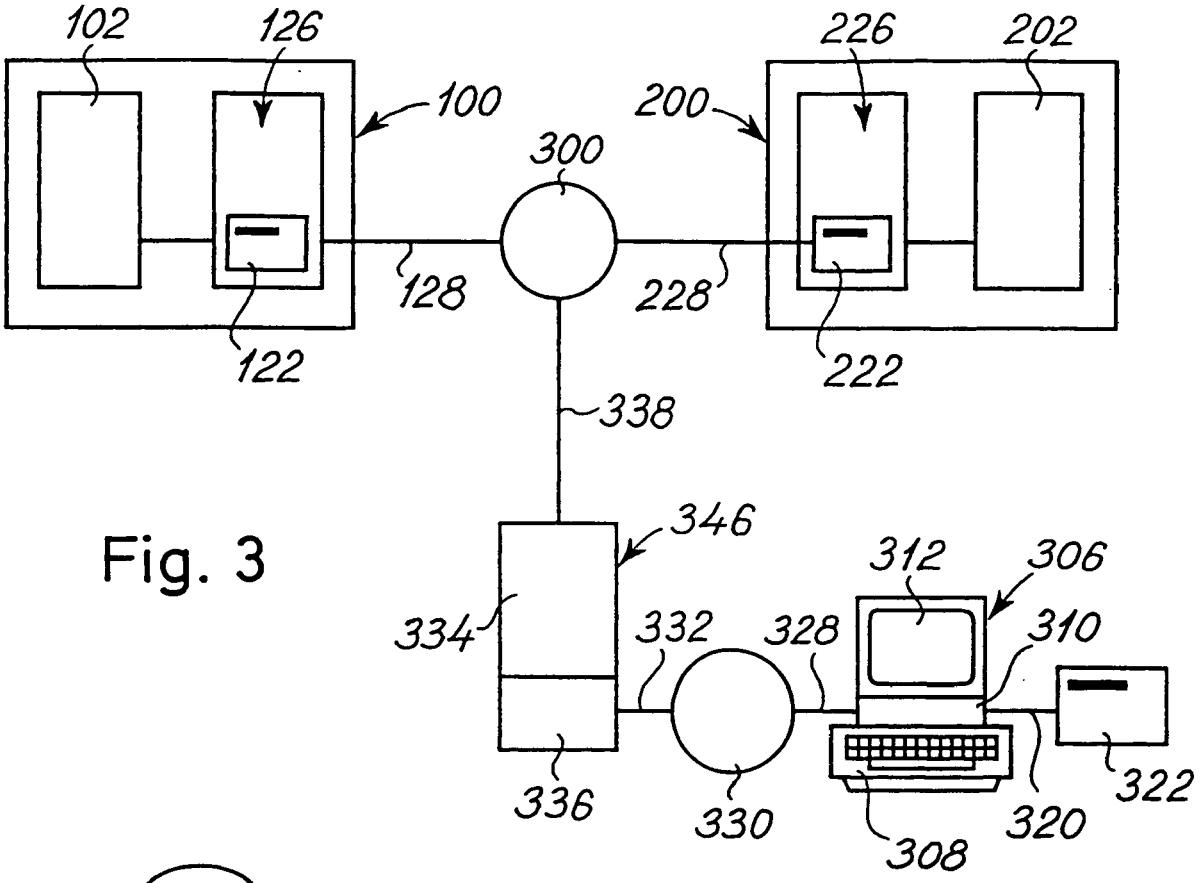

102
126
100
200
226
202
300
128
228
122
222
338
346
334
312
306
332
328
310
336
330
308
320
322

Fig. 3

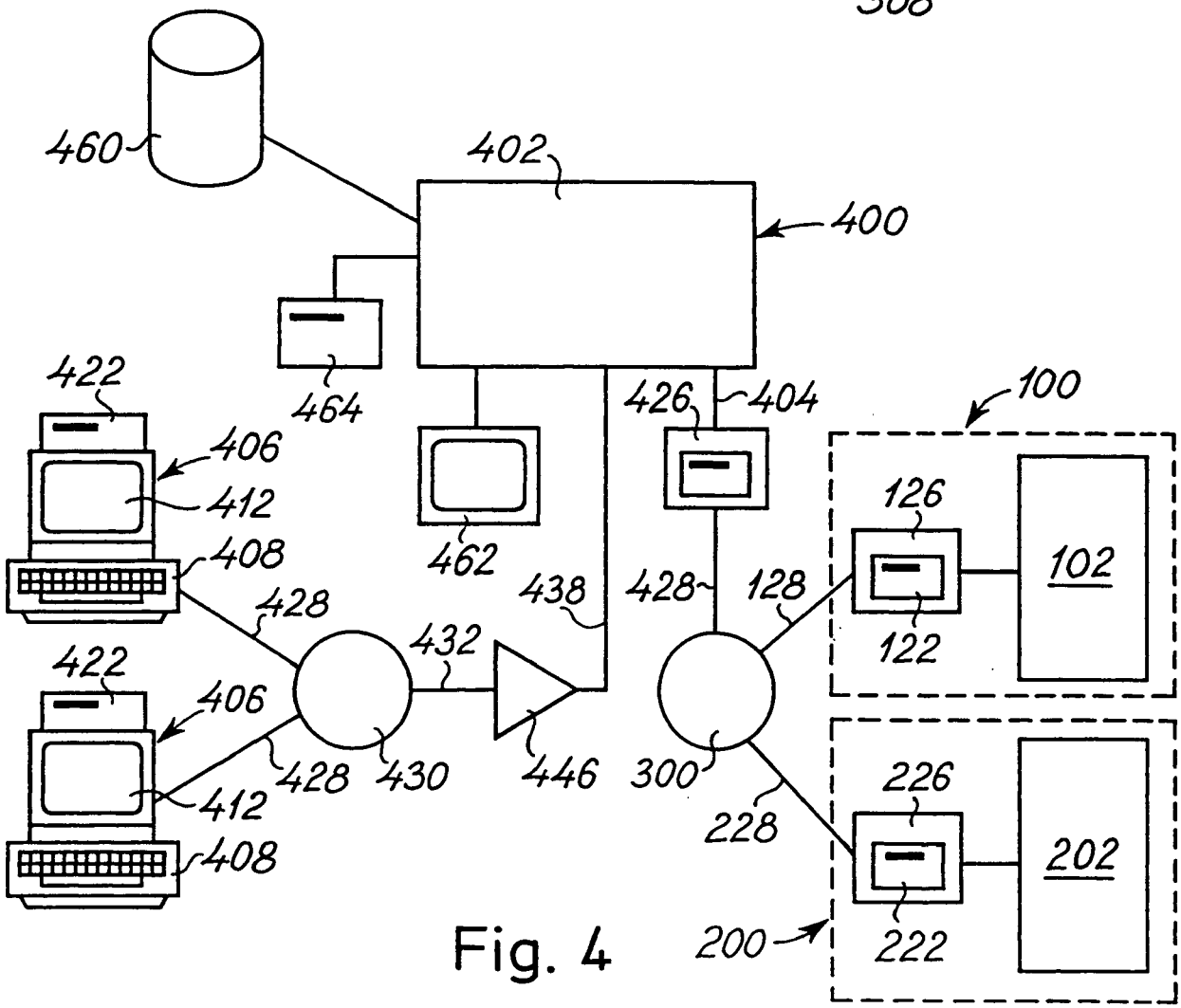

460
402
400
464
422
406
412
408
462
426
404
100
126
102
438
428
128
122
432
422
406
428
430
446
300
228
412
408
226
202
222
200

Fig. 4

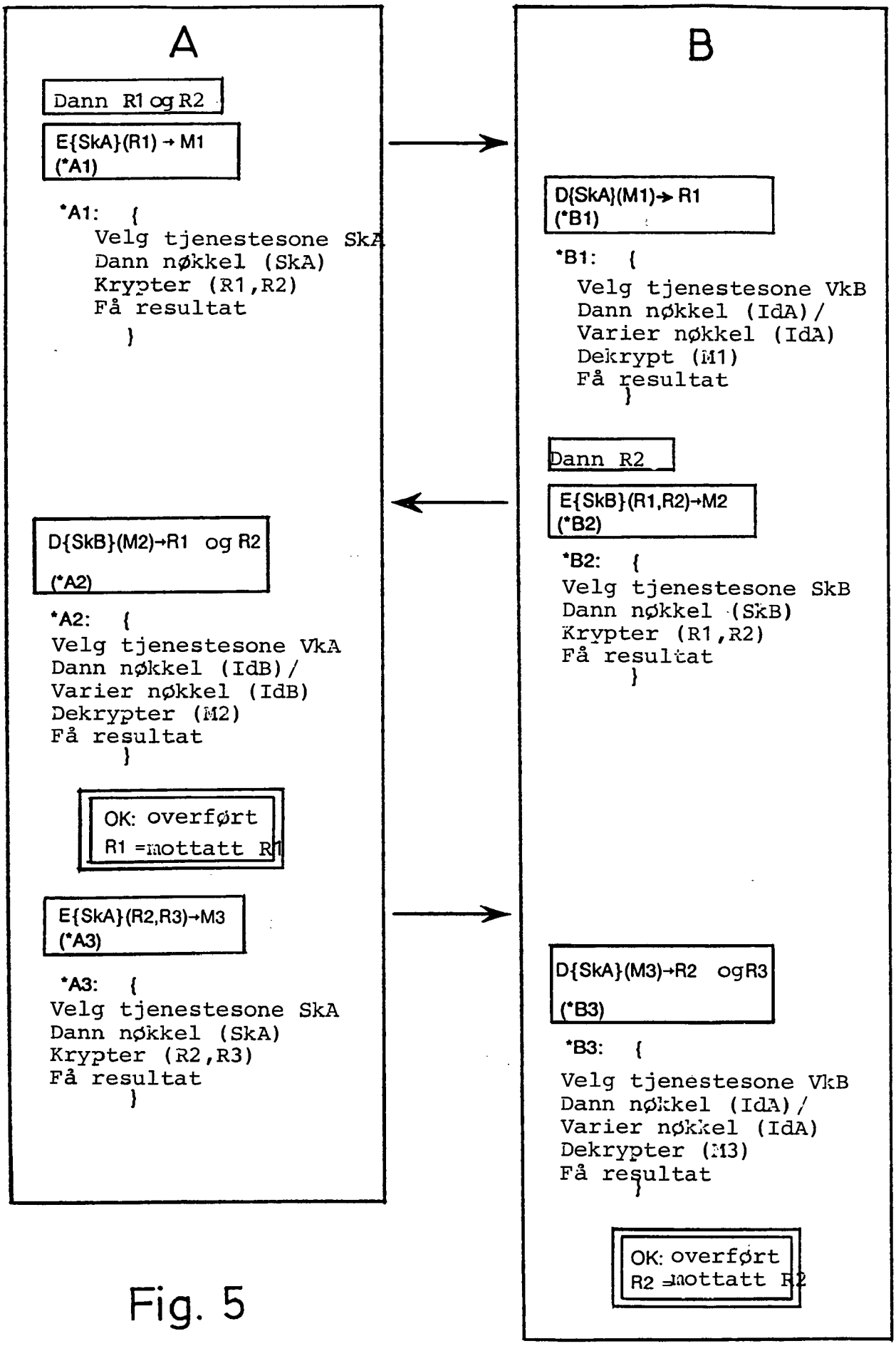

A
Dann R1 og R2
E{SkA}(R1) → M1
(*A1)
*A1: {
Velg tjenestesone SkA
Dann nøkkel (SkA)
Krypter (R1,R2)
Få resultat
}
D{SkB}(M2)→R1 og R2
(*A2)
*A2: {
Velg tjenestesone VkA
Dann nøkkel (IdB)/
Varier nøkkel (IdB)
Dekrypter (M2)
Få resultat
}
OK: overført
R1 =mottatt R1
E{SkA}(R2,R3)→M3
(*A3)
*A3: {
Velg tjenestesone SkA
Dann nøkkel (SkA)
Krypter (R2,R3)
Få resultat
}
B
D{SkA}(M1)→ R1
(*B1)
*B1: {
Velg tjenestesone VkB
Dann nøkkel (IdA)/
Varier nøkkel (IdA)
Dekrypt (M1)
Få resultat
}
Dann R2
E{SkB}(R1,R2)→M2
(*B2)
*B2: {
Velg tjenestesone SkB
Dann nøkkel (SkB)
Krypter (R1,R2)
Få resultat
}
D{SkA}(M3)→R2 ogR3
(*B3)
*B3: {
Velg tjenestesone VkB
Dann nøkkel (IdA)/
Varier nøkkel (IdA)
Dekrypter (M3)
Få resultat
}
OK: overført
R2 =mottatt R2

Fig. 5

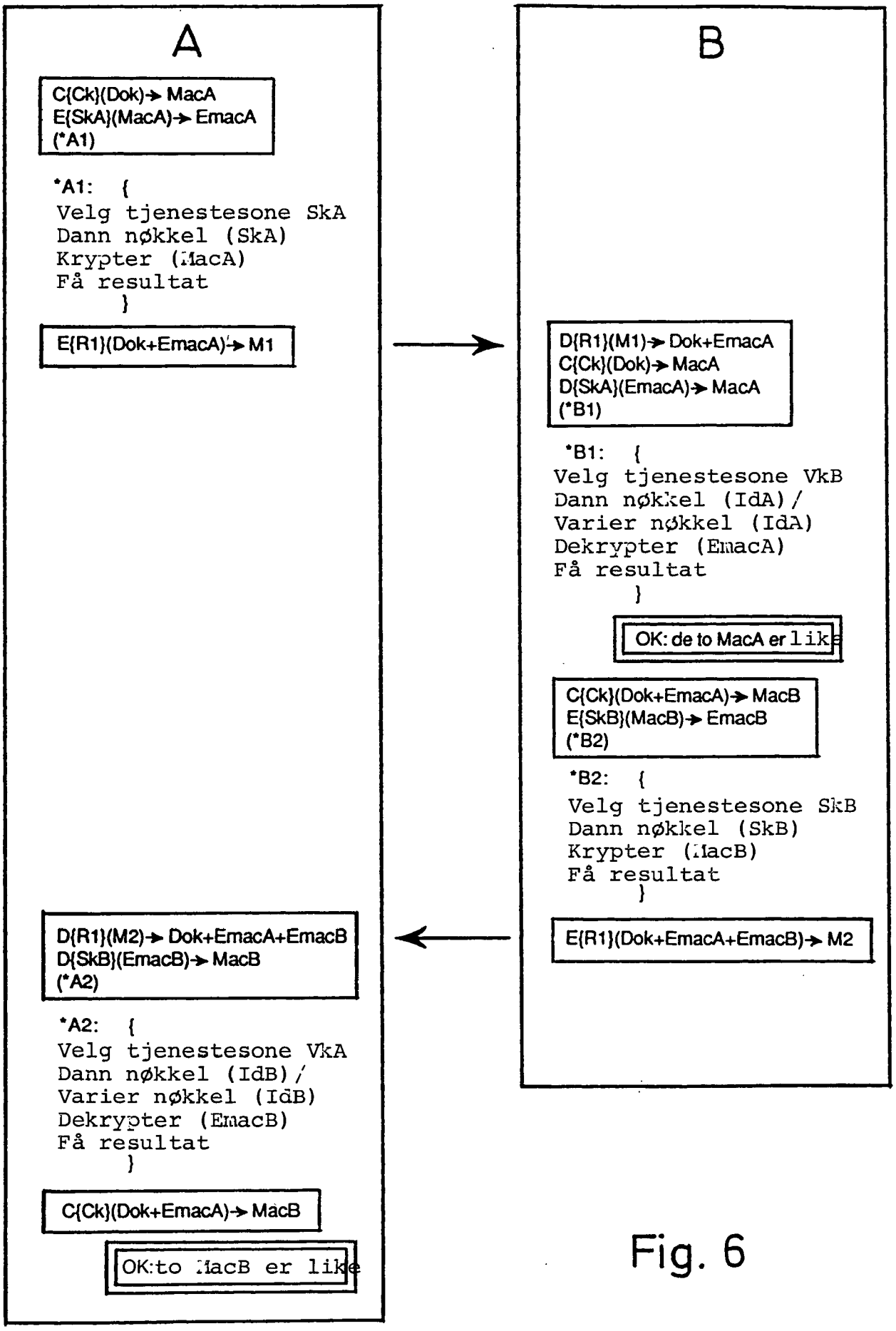

A
C{Ck}(Dok)→ MacA
E{SkA}(MacA)→ EmacA
(*A1)
*A1: {
Velg tjenestesone SkA
Dann nøkkel (SkA)
Krypter (MacA)
Få resultat
}
E{R1}(Dok+EmacA)→ M1
D{R1}(M2)→ Dok+EmacA+EmacB
D{SkB}(EmacB)→ MacB
(*A2)
*A2: {
Velg tjenestesone VkA
Dann nøkkel (IdB)/
Varier nøkkel (IdB)
Dekrypter (EmacB)
Få resultat
}
C{Ck}(Dok+EmacA)→ MacB
OK:to MacB er like
B
D{R1}(M1)→ Dok+EmacA
C{Ck}(Dok)→ MacA
D{SkA}(EmacA)→ MacA
(*B1)
*B1: {
Velg tjenestesone VkB
Dann nøkkel (IdA)/
Varier nøkkel (IdA)
Dekrypter (EmacA)
Få resultat
}
OK: de to MacA er like
C{Ck}(Dok+EmacA)→ MacB
E{SkB}(MacB)→ EmacB
(*B2)
*B2: {
Velg tjenestesone SkB
Dann nøkkel (SkB)
Krypter (MacB)
Få resultat
}
E{R1}(Dok+EmacA+EmacB)→ M2

Fig. 6