(12) **PATENT**

(19) NO (11) **321858** (13) **B1**

NORGE

(51) Int Cl.
H04Q 11/04 (2006.01)
H04L 29/06 (2006.01)

Patentstyret

(21)	Søknadsnr	19975866	(86)	Int.inng.dag og søknadsnr	1996.06.08 PCT/DE96/01068
(22)	Inng.dag	1997.12.12	(85)	Videreføringsdag	1997.12.12
(24)	Løpedag	1996.06.08	(30)	Prioritet	1995.06.13, DE, 19521485
(41)	Alm.tilgj	1998.02.05			
(45)	Meddelt	2006.07.17			

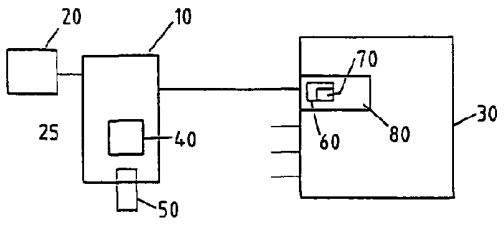
(73)	Innehaver	Deutsche Telekom AG , Friedrich-Ebert-Allee 140, 53113 BONN, DE
(72)	Oppfinner	Helmut Stolz, Sieben, DE
(74)	Fullmektig	Zacco Norway AS , Postboks 2003 Vika, 0125 OSLO, NO

(54) Benevnelse **Fremgangsmåte og innretning for overføring av fortrolige forbindelsesoppbygnings- og tjenesteinformasjon mellom abonnentterminaler og en eller flere digitale sentraler**

(56) Anførte publikasjoner US 5546463, WO 95/15634 A1

(57) Sammendrag

Fremgangsmåte og anordning for sending av konfidensiell og autentisk forbindelse og/eller tjenesteinformasjon mellom abonnenters dataterminaler og en eller flere sentraler til et digitalt kommunikasjonssystem. Når konfidensiell informasjon blir sendt mellom en abonnents terminal og en sentral i et ikke-kodet språk, er det en risiko for at inntrengere eller lyttere kan motta denne informasjonen. Det er derfor et formål for foreliggende oppfinnelse å gjøre et misbruk av sentralen så vel som en beskadigelse av abonnenttilslutningsinnehaveren ved en ikke-berettiget inntrengning svært vanskelig eller til og med umulig. For dette formål er det tilveiebragt en fremgangsmåte og anordning hvor det er i det minste en første sikkerhetsanordning ved den første abonnent, i det minste en andre sikkerhetsanordning ved sentralen, eller, alternativt, før hver sentral er en ytterligere anordning ved hvilken det er i det minste en andre sikkerhetsanordning. Den første og andre sikkerhetsanordningen kan kode og/eller dekode abonnentens forbindelse og/eller tjenesteinformasjon og utveksle den med hverandre.



Foreliggende oppfinnelse angår en fremgangsmåte for fortrolig og autentisk forbindelsesoppbygnings- og/eller tjenesteinformasjon mellom abonnentsidige terminaler og en eller flere sentraler til et digitalt kommunikasjonsnett, især et ISDN nettverk, av den art som angitt i innledningen til krav 1, så vel som en innretning for overføring av fortrolige forbindelsesoppbygnings- og/eller tjenesteinformasjon av den art som angitt i innledningen til henholdsvis krav 6 og 8.

Det er kjent digitale kommunikasjonsnett, som har til rådighet flere abonnenttilslutninger og digitale sentralsteder. Da en abonnenttilslutning sender all velger- og tjenesteinformasjon ukodet, dvs. i klartekst, til en digital sentral, kan inntrengere eller såkalte lyttere ganske enkelt høre disse fortrolige informasjonene på tilslutningsledningen, idet de kobler seg inn ved forskjellige punkter i en bestående forbindelsebane, henholdsvis kobler seg på en bestående forbindelse. Har en inntrenger på denne måten først tilveiebragt seg velger- og serviceinformasjon, kan han selv om han ikke er autorisert benytte sentralen på tilslutningsinnehaverens kostnader.

I artikkelen "INTEGRATING CRYPTOGRAPHY IN ISDN", publisert i "ADVANCES IN CRYPTOLOGY["], Santa Barbara, 16.-20. august 1987, konfr. nr. 7, 1. januar 1987, Pomerance C., side 9-18, XP000130200, beskriver K. Presttun et kryptografisk sikret ISDN kommunikasjonssystem med flere dataterminalinnretninger, som er tilsluttet til ISDN-nettet via en nettavslutningsinnretning, så vel som ved flere sentraler, som er tilordnet et autentifikasjonstjenesteinnretning. I dataterminalene eller nett-tilslutningsinnretningene er det anordnet respektive sikkerhetsmoduler, som tjener kun til koding og dekoding av nyttedata som overføres over B-kanalen til en ISDN-forbindelse. D-kanalen til ISDN-forbindelsen anvendes for fordeling av sikkerhetsnøkler mellom dataterminalene og til sikkerhetstjenesteadministrasjonen. Kodingen av forbindelsesoppbygnings- og tjenesteinformasjonen er ikke beskrevet der.

Foreliggende oppfinnelse har derfor til oppgave å vanskeliggjøre eller til og med fullstendig eliminere et misbruk av sentralen og en beskadigelse av autoriserte abonnenttilslutningsinnehavere ved en ikke-autorisert inntrengning.

Foreliggende oppfinnelse løser denne oppgaven ved hjelp av den innledningsvis nevnte fremgangsmåten hvis karaktertrekk fremgår av krav 1 så vel som ved hjelp av innretninger av den art hvis karaktertrekk fremgår av henholdsvis krav 6 og 8.

Oppfinnelsen er virkeliggjort i et digitalt kommunikasjonsnett, fortrinnsvis ISDN-nett. Et slikt digitalt kommunikasjonsnett innbefatter som kjent flere sentraler og minst en ved abonnenten installerte nett-tilslutningsinnretning, til hvilke det er tilkoblet minst en dataterminal, for eksempel telefonapparat, PC eller telefaksapparat. En ikke-ønsket bruk av sentralen av en inntrengning blir nå forhindret ved at det ved innehaveren til en abonnenttilslutning er anordnet i det minste en første sikkerhetsinnretning, at det videre er anordnet i det minste i en sentral minst en andre sikkerhetsinnretning, idet henholdsvis første og andre til en bestemt abonnent tilordnet sikkerhetsinnretning koder og/eller dekoder forbindelsesoppbygnings- og/eller tjenesteinformasjonen til denne abonnenten og hvilken informasjon kan utveksles med hverandre via en spesiell styrekanal til det digitale kommunikasjonsnettet. Sikkerhetsinnretningen har respektive sikkerhetsmoduler som på sin side kan oppta en identitetsbærer.

Ved hver sentral er det innbygd tilslutningsspesifikke komponenter, som hver inneholder en andre sikkerhetsinnretning. Denne utførelsesformen er imidlertid dyr og komplisert da selve sentralen må bli bygd om.

En billigere måte, som kan bli utført på enkel måte, består i installering av ytterligere enheter basert på eksisterende digitale sentraler mellom sentralen og respektive nett-tilslutningsinnretninger. I denne tilleggsinnretningen er for hver tilhørende abonnenttilslutning anordnet tilsvarende andre sikkerhetsinnretninger.

Den første sikkerhetsinnretningen til en bestemt tilslutningsinnehaver er fortrinnsvis anordnet i den til abonnenttilslutningen tilordnede nett-tilslutningsinnretning. I dette tilfelle er det tilstrekkelig med en eneste sikkerhetsinnretning også når innehaveren til en abonnenttilslutning kan tilsluttes via en S_0-buss opptil åtte dataterminaler til nett-tilslutningsinnretningen. Det er mulig å utruste hver dataterminal, som er tilordnet en nett-tilslutningsinnretning, med en egen sikkerhetsinnretning. Et ytterligere alternativ kan bestå deri at mellom hver dataterminal og tilhørende nett-tilslutningsinnretning tilsluttes en sikkerhetsinnretning. Det skal imidlertid bemerkes at de to sistnevnte utførelsesmulighetene er dyre og kompliserte, da det for hver dataterminal er nødvendig med en egen sikkerhetsinnretning. Tjenesteinformasjonen kan for eksempel innbefatte videreanropslednings- og konferansekoblingsfunksjoner. Er det digitale kommunikasjonsnettet et ISDN-nett, så foregår overføringen av den fortrolige informasjonen mellom den abonnentsidige første sikkerhetsinnretningen og sikkerhetsinnretningen tilordnet sentralen via D-kanalen til ISDN-nettet. Hver identifiseringsbærer kan lagre en individuell på innehaveren til abonnenttilslutningen

henført kryptografisk nøkkel. Identitetsbæreren kan være et chip-kort, som kan føres inn av innehaveren til en abonnenttilslutning i den første sikkerhetsmodulen av en betjeningsperson hos nettdriveren i den andre sikkerhetsmodulen. Et hensiktsmessig alternativ angår en programvaremodul som identitetsbærer, som kan settes inn utskiftbar i respektive sikkerhetsmoduler. Ved en ytterligere fordelaktig videreutførelse av første abonnentsidesikkerhetsinnretning og den andre sikkerhetsinnretningen tilordnet sentralen utføres en autentifisering av abonnenten i forhold til sentralen. Alternativt kan for denne oppgaven installeres separate autentifiseringsinnretninger.

Beskyttelse av sentralen og den berettigede tilslutningsinnehaveren kan forbedres ved at første og andre sikkerhetsanordninger, tildelt en gitt abonnent, for henholdsvis koding og dekoding, blir en bruker-til-brukerkommunikasjon sendt via styrekanalen til det digitale kommunikasjonsnettverket.

Den abonnentsidige sikkerhetsanordningen til en gitt abonnent og sikkerhetsanordningen til sentralen har fortrinnsvis samme abonnentspesifikke identitet. De koder og dekoder dessuten konfidensiell informasjon med samme abonnentspesifikke nøkkel.

I det påfølgende skal oppfinnelsen beskrives nærmere med henvisning til tegningene, hvor:

Fig. 1 skjematisk viser et snitt av et digitalt kommunikasjonsnettverk vist som en linje fra en telefonsett til en digital sentral hvor foreliggende oppfinnelse er utført.

Fig. 2 viser en utførelsesform hvor sikkerhetsanordningen ifølge oppfinnelsen er installert i en ytterligere anordning på sentralsiden.

Fig. 3 viser et detaljert blokkdiagram av nettverkavslutningen med sikkerhetsanordningen ifølge oppfinnelsen.

Fig. 4 viser et detaljert blokkdiagram av en forbindelsesspesifikk enhet i sentralen med en innebygd sikkerhetsmodul.

Fig. 5 viser rammeformatet til ISDN-bitstrømmen.

Fig. 1 viser en forenklet form av en del av et digitalt kommunikasjonsnettverk, som for den påfølgende eksempelbeskrivelsen skal være et ISDN-nett. Et telefonapparat 20 er vist som en dataterminal på abonnentsiden, som er forbundet med nettverkavslutning 10 via en S_0-buss 25. Nettverkavslutningen 10, også henvist til som "nettverksterminator" (NT), kan bli installert i bygningen eller rommet til en abonnenttilslutningsinnehaver. Opp til åtte dataterminaler, slik som andre telefonapparater 20, telefaksmaskiner eller PC'er, kan være forbundet med S_0-bussen 25. I det viste eksemplet er en abonnentside-sikkerhetsanordning 40, 50 ifølge oppfinnelsen bygd inn i nettverkavslutningen 10. Sikkerhetsanordningen innbefatter en abonnentspesifikk identifikasjonsbærer 50 og en sikkerhetsmodul 40, som kan være permanent installert i nettverkavslutning 10, hvor identifikasjonsbæreren 50 kan være satt inn. Identifikasjonsbæreren 50 kan være et smartkort eller en programvaremodul. Sikkerhetsanordningen 40 og identifikasjonsbæreren 50 er konstruert slik at de kan kode eller dekode konfidensielle forbindelsesetableringer eller tjenesteinformasjon med en abonnentspesifikk eller forbindelsesspesifikk nøkkel. Denne nøkkelen kan bli lagret i en lagringsmodul til smartkortet tilhørende forbindelsesinnehaveren. Utgangen til nettverkavslutningen 10 er forbundet med korresponderende ISDN-sentral 30 via en tvunnet totråds kabel på kjent måte. Et ISDN-nettverk kan naturligvis innbefatte flere nettverkavslutninger 10 og flere sentralsystemer 30, som kan være sammenkoblet via tvunne totrådskabler. I fremtiden kan konvensjonelle totråds kabler bli supplementert og erstattet av fiberoptiske kabler for eksempel. Sentralen 30 innbefatter flere enheter 80 (idet Fig. 1 kun viser en enkel forbindelsesspesifikk enhet 80), hver tildelt bestemte abonnentforbindelsesinnehavere. I den første utførelsesformen ifølge oppfinnelsen er en sikkerhetsanordning 60, 70 anordnet i hver forbindelsesspesifikke enhet 80. Som abonnentspesifikk sikkerhetsanordning 40, 50 innbefatter sikkerhetsanordningen 60, 70 i sentralen 30 en modul 60, som kan være permanent installert i enheten 80 og en identifikasjonsbærer 70, som kan bli satt inn i denne. Det antas at identifikasjonsbæreren 70 i sentralen 30 også inneholder den kryptografiske nøkkelen til abonnentsidesikkerhetsanordningen 40, 50.

Fig. viser en alternativ utførelsesform hvor en ytterligere anordning 100 er forbundet mellom nettverkavslutningen 10 og sentralen 30. For tydelighetens skyld viser Fig. 2 ytterligere anordning 100 kun med innebygd sikkerhetsanordning 60, 70. Normalt er alle sikkerhetsanordningene 60, 70 til abonnentene eller nettverkavslutningene sammen betjent av sentralen 30 installert i den ytterligere anordning 100. Korresponderende forbindelselinjer er indikert på Fig. 1 og 2. Igjen kan identifiseringsbærerne 70 bli satt inn som smartkort fra utsiden av en operatør eller utført som en programvaremodul og

installert i respektive sikkerhetsanordning 60. Bruk av ytterligere anordning 100 har den fordelen at eksisterende ISDN nettverksentraler kan fortsatt bli anvendt uten tidsforbrukende, dyre og komplekse modifikasjoner på sentralsystemet for å sende konfidensiell informasjon for eksempel til abonnenten av telefonapparatet 20 til sentralen 30.

Fig. 3 viser et forenklet blokkdiagram av den kjente nettverkavslutningen 10, hvor sikkerhetsanordningen 40 ifølge oppfinnelsen sammen med identifikasjonsbæreren 50 er installert. På abonnentsiden har nettverkavslutningen 10 en forbindelsesenhet for S_0-bussen 25, til hvilken opp til åtte dataterminaler 20 kan være forbundet. Siden strukturen og operasjonsmodusen til nettverkavslutningen 10 er generelt kjent, skal de vesentlige komponentene bare kort beskrives nedenfor. Nettverkavslutning 10 har en sendebane og en mottagerbane. Sendebanen innbefatter en kode 210, som blant annet tilfører konfidensiell informasjon som skal bli sendt i D-kanalen til ISDN nettverket til en koder i sikkerhetsanordning 40, 50 og en multiplekser 200, som kombinerer de to B-kanalene og D-kanalen til en kontinuerlig datastrøm i en tidsmultipleks operasjon. Et egnet rammeformat består av 48 biter per 250 ms, med kun fire D-kanalbiter tilveiebrakt per ramme. Med andre ord blir 16 kbiter/sek sendt over D-kanalen (jfr. Fig. 5). Sendebanen går så til en gaffelvender 170 via en sender 180, idet gaffelvenderen sender utgående datastrøm til en totråds kabel som forbinder sentralen 30 med nettverkavslutningen 10. Innkommende datastrøm går via gaffelvenderen 170, en mottager 160 og en anordning 150, som utjevner og forsterker datastrømmen mottatt og gjenvinner klokkesignalet fra den. Datastrømmen passerer så gjennom en demultiplekser 140, som dekomprimerer datastrømmen igjen i to B-kanaler og D-kanalen. Den demultiplekse datastrømmen passerer gjennom dekoderen 130 og blir så sendt, i samsvar med en bestemmelsesadresse, til telefonapparatet 20, for eksempel via S_0-bussen 25. En ekkokompensator 190, forbundet parallelt mellom senderen 180 og mottageren 160, anvendes blant annet for å kompensere utgående meldinger sendt til mottagerbanen via gaffelvenderen 170 og mottageren 160. Hjertedelen til nettverkavslutningen 10 er en styrer 220, som styrer administrasjon og felles styring av enkeltkomponentene. Sikkerhetsanordning 40 ifølge oppfinnelsen med innsatt identifikasjonsbærer 50 er for eksempel forbundet med styreren 220, koderen 210, multiplekseren 200, demultiplekseren 140 og dekoderen 130. Styreren 220 er også ansvarlig for aktivering eller desaktivering av sikkerhetsanordning 40, 50 som krevd av situasjonen.

Fig. 4 viser et eksempel på et blokkdiagram av en abonnentspesifikk enhet 80, installert i sentralen 30. Den forbindelsesspesifikke enheten 80 danner hovedsakelig motdelen av nettverkavslutningen 10. Innkommende datameldinger går via totrådslinjen til en gaffelvender 230 og passerer så gjennom en demultiplekser 240, en dekoder 250 og en D-kanalhåndterer 260. D-kanalhåndtereren 260 tilfører styreinformasjon til en sentral styrer til sentralen 30. I motsatt retning går utgående meldinger gjennom en koder 270, en multiplekser 290 og en gaffelvender 230 på totrådslinjen til nettverkavslutningen 10. Også ved den forbindelsesspesifikke enheten 80 er en styrer 280 ansvarlig for administrasjon av samvirket mellom de enkelte komponentene. Sikkerhetsanordning 60 er installert i den forbindelsesspesifikke enheten 80 ifølge oppfinnelsen med et smartkort som kan bli satt inn fra utsiden eller en installert programvaremodul 70. Sikkerhetsanordningen 60, 70, som innbefatter sikkerhetsmodulen 60 og identifikasjonsbæreren 70 er forbundet med koderen 270, dekoderen 250, D-kanalhåndtereren 260 og styreren 280. Som nevnt tidligere, kan autentifiseringsanordning 60, 70 også bli installert i ytterligere anordning 110, som vist på Fig. 2.

Det er hensiktsmessig å installere autentifiseringsanordning 40, 50 i nettverkavslutningen 10, siden det på denne måten kun er nødvendig med en autentifiseringsanordning 40, 50 uansett antall tilkoblede dataterminaler 20. Det er også hensiktsmessig å anordne abonnentsidig sikkerhetsanordning 40, 50 i hver dataterminal 20. Et annet alternativ består av å anordne en sikkerhetsanordning (ikke vist) mellom nettverkavslutningen 10 og hver forbundet dataterminal 20, idet sikkerhetsanordning 40, 50 da implementeres i sikkerhetsanordningen. Av økonomiske grunner er det hensiktsmessig å installere sikkerhetsanordningene 40, 50 i selve nettverkavslutningen 10, vist på Fig. 1. Identifikasjonsbæreren 50 kan bli installert i form av en programvaremodul av nettverkoperatøren når nettverkavslutningen 10 er installert ved abonnenten. Dersom identifikasjonsbæreren 50 er et smartkort, kan abonnenten kjøpe dette kortet, som inneholder abonnentens individuelle abonnentnøkkel, fra nettverkoperatøren.

Transmisjonen av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon mellom telefonapparatet 20 og sentralen 30 skal nå beskrives nærmere.

Det er antatt at en abonnentside sikkerhetsanordning 40, 50 er installert i nettverkavslutningen 10 og en andre sikkerhetsanordning 60, 70 er installert i enheten 80, tildelt abonnenten til telefonapparatet 20 i sentralen 30. Ifølge utførelsesformen vist

på Fig. 2 kan også sikkerhetsanordningen 60, 70 bli installert i en ytterligere anordning 100. Prosedyren beskrevet nedenfor forekommer hovedsakelig på samme måte i begge tilfeller.

Det skal nå antas at abonnentside identifikasjonsbæreren 50 og sentralside identifikasjonsbæreren 70 har samme ID, dvs. identiteten til abonnenten av telefonapparatet 20. Abonnentside sikkerhetsanordningen 40, 50 og sentralside sikkerhetsanordningen 60, 70 har dessuten samme kryptografiske nøkkel tilknyttet abonnenten til telefonapparatet 20. Begge identifikasjonsbærerne 50, 70 er smartkort.

Etter at sikkerhetsanordningen 40, 50 har autentifisert abonnenten til telefonapparatet 20 til sentralen 30 forbundet med sikkerhetsanordningen 60, 70 installert i den abonnentspesifikke enheten 80 - autentifiseringen kan bli utført av separate autentifiseringsanordninger - blir alle forbindelsesetableringer og tjenesteinformasjon kodet av abonnentside sikkerhetsanordningen 40, 50 med den abonnentspesifikke nøkkelen og sendt til sikkerhetsanordningen 60, 70 i den abonnentspesifikke enheten i D-kanalen via ISDN-nettverket. Sikkerhetsanordningen 60, 70 i sentralen 30 dekoder mottatt kodet forbindelsesetablering og/eller tjenesteinformasjon med den felles abonnentspesifikke nøkkelen og sender dekodet informasjon via D-kanalhåndtereren til en sentral enhet i sentralen 30. Som reaksjon på dekodet forbindelsesetablerings-informasjon blir den ønskede forbindelsen til anropte abonnent etablert og som reaksjon på dekodet tjenesteinformasjon blir den de anmodede tjenestene gjort tilgjengelig. Dette sikrer at en ikke-autorisert inntrenger ikke vil være i stand til å etablere en forbindelse på bekostning av eieren av forbindelsen til telefonapparatet 20. Forskjellige kjente kodeprosedyrer kan bli anvendt for kodingen og dekodingen, slik som for eksempel "Riwest-Shamir-Adlerman"-metoden eller "Data Encryption Standard"-metoden.

Det skal nå antas at istedenfor smartkortet er en spesiell kodings- og dekodingsmodul 70 installert i den abonnentspesifikke enheten 80. Før kodingen av konfidensiell forbindelsesetablering og tjenesteinformasjon og sending av den via ISDN-nettverket til sentralen 30 er dekodingsmodulen 70 forsynt med en nøkkel tildelt abonnenten av telefonapparatet 20 ved hjelp av en sentral eller desentralisert krypteringssenter. Nøkkelen kan bli sendt til sikkerhetsanordningen 60, 70 via et datamedium, slik som en diskett, eller ved en elektronisk dataoverføring. Viktige og kjente sikkerhetstrekk må bli tatt med i beregningen, spesielt ved konfidensiell og autentifisert informasjonstransmisjon, slik at den abonnentspesifikke nøkkelen ikke blir kjent for ikke-autoriserte tredjeparter. Etter at sikkerhetsanordningen 60, 70 til enheten 80 har

mottatt den abonnentspesifikke kryptografinøkkelen, blir konfidensiell forbindelsesetablering og tjenesteinformasjon sendt som beskrevet ovenfor.

En fordelaktig videreutførelse av oppfinnelsen sørger for at styrekanalen (D-kanalen) til det digitale kommunikasjonsnettverket tjener som en datatransmisjonslinje for bruker-til-bruker-transmisjon, spesielt mellom dataterminalen 20 og sentralen 30 i en kodet form. I dette tilfelle er abonnentside sikkerhetsanordningen 40, 50 i stand til å kode for eksempel data sendt av en PC og sende de til sikkerhetsanordningen 60, 70 til sentralen 30. Sikkerhetsanordningen 60, 70 kan bli installert i den abonnentspesifikke enheten 80 eller i en ytterligere anordning 100, kan dekode denne datainformasjonen og sende den i forbindelse med sentralen 30 for eksempel via Datex P nettverk til den anropte abonnenten.

P a t e n t k r a v

1.

Fremgangsmåte for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon mellom abonnentside terminaler (20) og en eller flere digitale sentraler (30) til et digitalt kommunikasjonsnettverk med i det minste en abonnentside nettverkavslutning (10), med hvilken i det minste en dataterminal (20) kan bli forbundet, med minst en sikkerhetsanordning (40, 50) anordnet ved en abonnent og i det minste en andre sikkerhetsanordning (60, 70) tildelt sentralen (30), k a r a k - t e r i s e r t v e d

koding og/eller dekoding av forbindelsesetableringen og/eller tjenesteinformasjon ved abonnentsidens første sikkerhetsanordning (40, 50),

transmisjon av kodet forbindelsesetablering og/eller tjenesteinformasjon mellom første (40, 50) og andre (60, 70) sikkerhetsanordning over en separat styrekanal til det digitale kommunikasjonsnettverket, og

koding og/eller dekoding av forbindelsesetableringen og/eller tjenesteinformasjon av den andre sikkerhetsanordningen (60, 70).

2.

Fremgangsmåte ifølge krav 1, k a r a k t e r i s e r t v e d at den konfidensielle forbindelseetableringen og/eller tjenesteinformasjonen dekodet av den andre sikkerhetsanordningen (60, 70) sendes til en sentral enhet til respektive sentral (30), som som reaksjon på forbindelsesetableringen og/eller tjenesteinformasjonen etablerer en forbindelse med anropt abonnent og/eller gjør den anmodede tjenesten tilgjengelig.

3.

Fremgangsmåte for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon ifølge krav 1 eller 2, k a r a k t e r i s e r t v e d at forbindelsesetableringen og/eller tjenesteinformasjonen kodes og/eller dekodes med samme abonnentspesifikke nøkkel av første (40, 50) og andre (60, 70) sikkerhetsanordning.

4.

Fremgangsmåte for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon ifølge et av kravene 1 til 3, k a r a k t e r i s e r t v e d at autentifiseringen mellom abonnenten til nettverkavslutning (10) og respektive sentral (30) utføres av første sikkerhetsanordning (40, 50) og en andre sikkerhetsanordning (60, 70) eller ved hjelp av separate autentifiseringsanordninger før transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon.

5.

Fremgangsmåte for konfidensiell forbindelsesetablering og/eller tjenesteinformasjon ifølge et av kravene 1 til 4, k a r a k t e r i s e r t v e d at forbindelsesetableringen og/eller tjenesteinformasjonen sendes via D-kanalen til et ISDN-nettverk.

6.

Anordning for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon mellom abonnentsidedataavslutninger (20) og en eller flere sentraler (30) til digitale kommunikasjonsnettverk med i det minste en abonnentside-nettverksavslutning (10), til hvilken minst en dataterminal (20) kan bli forbundet, k a r a k t e r i s e r t v e d at i det minste en første abonnentside sikkerhetsanordning (40, 50) er anordnet ved i det minste en abonnent, og at i det minste en andre sikkerhetsanordning (60, 70) er anordnet ved i det minste sentralen (30), med i det minste første (40, 50) og andre (60, 70) sikkerhetsanordning i stand til å kode og/eller dekode og utveksle, via en separat styrekanal til det digitale kommunikasjonsnettverket, forbindelsesetablering og/eller tjenesteinformasjon til abonnenten.

7.

Anordning for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon ifølge krav 6, k a r a k t e r i s e r t v e d at sentralen (30) har flere forbindelsesspesifikke enheter (80) tildelt til visse abonnenter, hvor en andre sikkerhetsanordning (60, 70) er anordnet.

8.

Anordning for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon mellom abonnentside dataterminaler (20) og en eller flere sentraler (30) til et digitalt kommunikasjonsnettverk med i det minste en første abonnentside-

nettverksavslutning (10), til hvilken i det minste en dataterminal (20) kan bli forbundet, k a r a k t e r i s e r t v e d at en første sikkerhetsanordning (40, 50) er anordnet ved i det minste en abonnent, at en ytterligere anordning (100) med en andre sikkerhetsanordning (60, 70) er forbundet oppstrøms fra (eller hver) sentral (30), med første (40, 50) og andre (60, 70) sikkerhetsanordning i stand til å kode og/eller dekode og utveksle forbindelsesetablering og/eller tjenesteinformasjon via en separat styrekanal til det digitale kommunikasjonsnettverket til abonnenten.

9.
Anordning for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon ifølge et av kravene 6 til 8, k a r a k t e r i s e r t v e d at hver sikkerhetsanordning har i det minste en sikkerhetsmodul (40, 60), som kan motta en identifikasjonsbærer (50, 70).

10.
Anordning for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon ifølge et av kravene 6 til 9, k a r a k t e r i s e r t v e d at første sikkerhetsanordning (40, 50) er anordnet i nettverkavslutningen (10).

11.
Anordning for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon ifølge et av kravene 6 til 9, k a r a k t e r i s e r t v e d at en første sikkerhetsanordning (40, 50) er anordnet i hver dataterminal (20) forbundet med nettverkavslutningen (10).

12.
Anordning for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon ifølge et av kravene 6 til 9, k a r a k t e r i s e r t v e d at første sikkerhetsanordning (40, 50) er anordnet mellom hver dataterminal og respektive nettverkavslutning (10).

13.
Anordning for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon ifølge et av kravene 6 til 12, k a r a k t e r i s e r t v e d at det digitale kommunikasjonsnettverket er et ISDN-nettverk og kodet

informasjon er utvekslet mellom første sikkerhetsanordning (40, 50) og andre sikkerhetsanordning (60, 70) via D-kanalen til ISDN-nettverket.

14.

Anordning for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon ifølge et av kravene 9 til 13, k a r a k t e r i s e r t v e d at identifikasjonsbæreren (50, 70) er et smartkort eller en programvaremodul som kan kode og/eller dekode konfidensiell informasjon.

15.

Anordning for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon ifølge et av kravene 6 til 14, k a r a k t e r i s e r t v e d at første (40, 50) og andre (60, 70) sikkerhetsanordning tildelt en gitt abonnent har samme ID og kan kode og/eller dekode konfidensiell informasjon med samme abonnentspesifikke nøkkel.

16.

Anordning for transmisjon av konfidensiell forbindelsesetablering og/eller tjenesteinformasjon ifølge et av kravene 6 til 15, k a r a k t e r i s e r t v e d at første (40, 50) og andre (60, 70) sikkerhetsanordning tildelt en gitt abonnent kan kode og/eller dekode alle data som skal bli sendt over styrekanalen til det digitale kommunikasjonsnettverket.

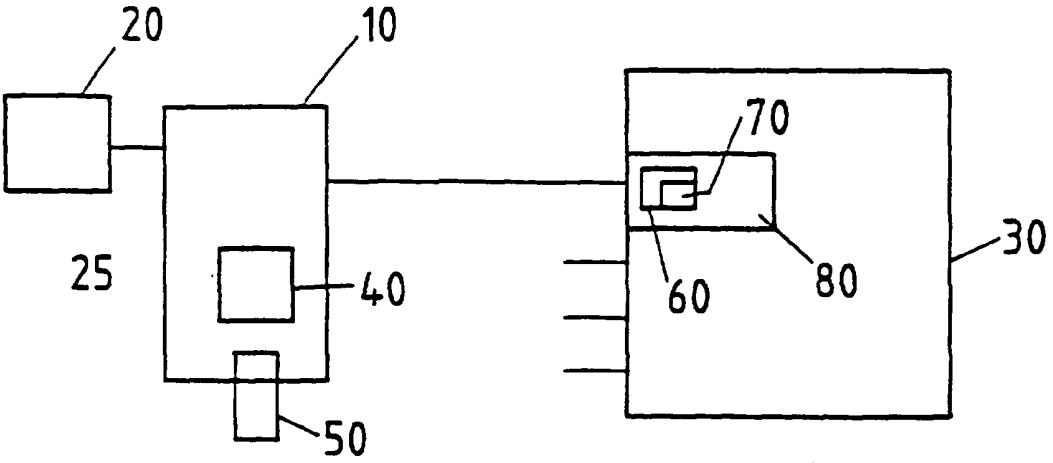


Fig. 1

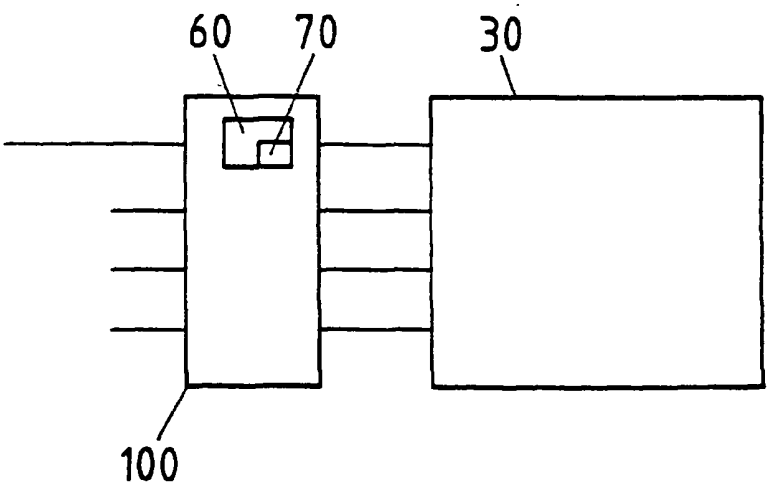


Fig. 2

1	1	8	1	1	1	1	1	8	1	1	1	8	1	1	1	8	1	1
F	L	B_1	E	D	A	F	F	B_2	E	D	S	B_1	E	D	S	B_2	E	D

Fig. 5

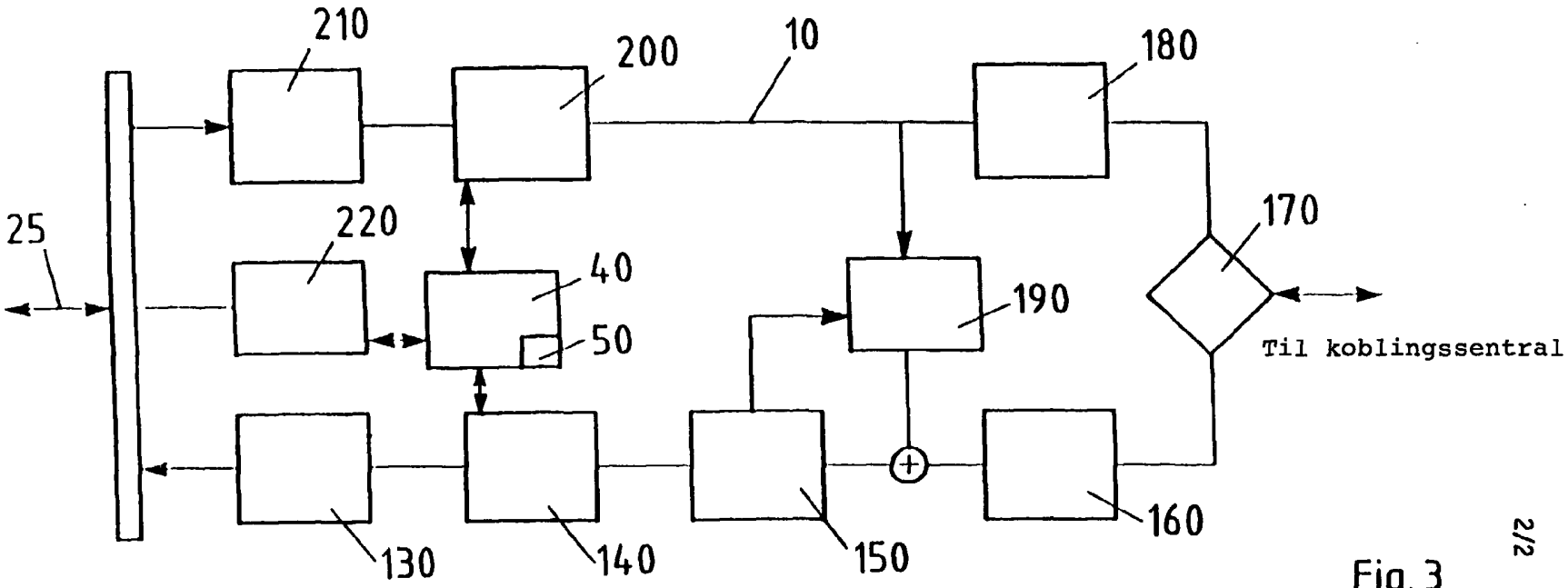

210
200
10
180
25
220
40
50
190
170
Til koblingssentral
130
140
150
160

Fig. 3

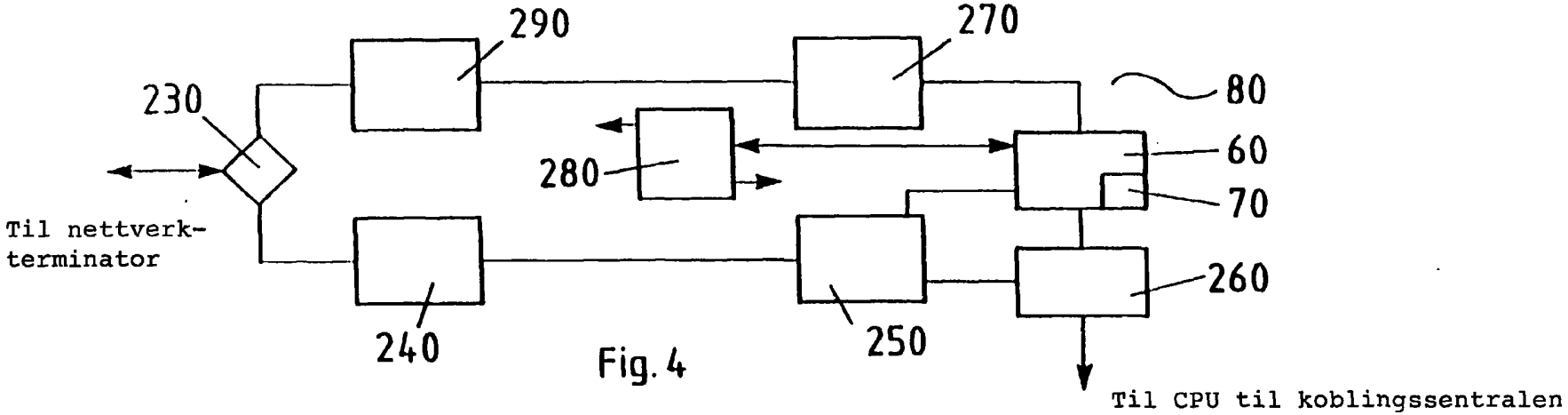

290
270
230
80
280
60
70
Til nettverk-
terminator
240
250
260
Til CPU til koblingssentralen

Fig. 4