(12) **PATENT**

(19) NO (11) **337079** (13) **B1**

NORGE (51) Int Cl.

G06K 19/00 (2006.01)
G06K 19/10 (2006.01)
G06Q 20/00 (2012.01)
G07F 7/08 (2006.01)
G07F 7/10 (2006.01)
G09C 1/00 (2006.01)

Patentstyret

(21)	Søknadsnr	19995529	(86)	Int.inng.dag og søknadsnr	1998.05.14 PCT/SE1998/00897
(22)	Inng.dag	1999.11.12	(85)	Videreføringsdag	1999.11.12
(24)	Løpedag	1998.05.14	(30)	Prioritet	1997.05.15, SE, 9701814
(41)	Alm.tilgj	2000.01.10			
(45)	Meddelt	2016.01.18			

(73) Innehaver Comex Electronics AB, Tumstocksvägen 11 B, S-187 66 Täby, SE-, Sverige
(72) Oppfinner Hans Sjöblom, Grindögatan 138, SE-25732 RYDEBÄCK, Sverige
(74) Fullmektig Tandbergs Patentkontor AS, Postboks 1570 Vika, 0118 OSLO, Norge

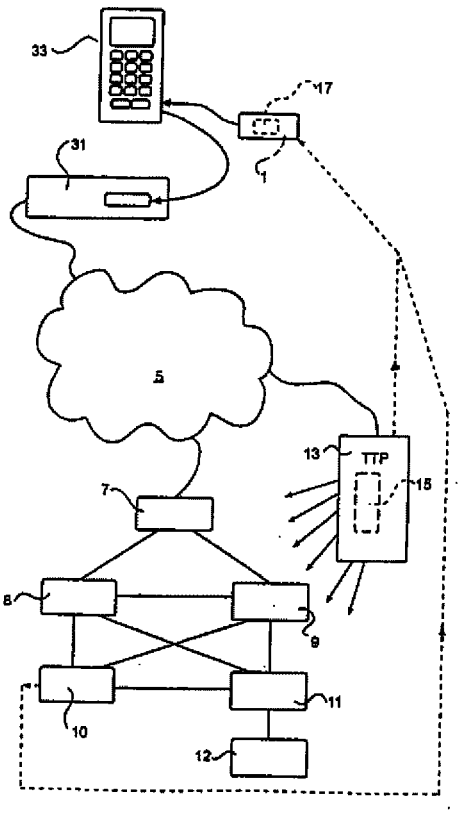
(54) Benevnelse **Elektronisk transaksjon**

(56) Anførte publikasjoner

WO 96/32700 A1
Handbuch der Chipkarten, 2. Auflage 1996, Rankl/Effing
EP 567610 B1
GB 2261538 A
EP 386867 B1
US 4926480 A
US 4868376 A
WO 86/03040 A1
US 5130519 A
WO 97/16779 A2
EP 214609 A2
US 5280527 A

(57) Sammendrag

Fremgangsmåte og apparatur for å utføre elektroniske transaksjoner. En sender fremstiller under full egenkontroll en transaksjonsmelding i et smartkort (1) og forsyner meldingen med sin digitale signatur i kortet for etterfølgende overføring.



Fagfelt

Oppfinnelsen gjelder elektroniske transaksjoner, det vil si hovedsakelig betalinger som utføres elektronisk. Nærmere bestemt gjelder oppfinnelsen elektroniske belastningskort eller liknende, idet slike kort gjerne kalles smartkort, magnetkort eller elektroniske kort.

Bakgrunn

I senere år har interessen for elektroniske transaksjoner økt i stor grad, særlig sammen med anvendelsen av globale kommunikasjonsnett (Internett). Det har vært fokusert på sikring, og forskjellige systemer og standarder har vært foreslått for å garantere sikkerheten i forbindelse med elektronisk overføring av transaksjons-meldinger. Et område som har fått stor interesse er hvordan man for eksempel skal benytte overføring av kredittkortnumre via Internett i forbindelse med netthandel. Det de forskjellige systemer og standarder har i fellesskap som forslag, er at de enten baseres på den betingelse at følsom informasjon som kan bli misbrukt, for eksempel kredittkortnummer, ikke skal overføres via kommunikasjonsnettet, eller på den betingelse at slik følsom informasjon bare skal overføres i kodet eller kryptert form. I begge alternativer er det fokusert på den relativt kompliserte administrasjonsrutine og de nødvendige systemkonfigurasjoner som trengs, hvilket fører til restriksjoner og hindringer for en mer generell bruk, hvilket lett innses.

Følgende dokumenter angir beslektet teknikk på dette område:

WO9632700A1 beskriver en elektronisk transaksjonsterminal, til bruk i gjennomføringen av elektroniske finansielle transaksjoner, som omfatter, i kombinasjon, et smartkort og en kommunikasjonsmodul. Smartkortet har kreditt lagret på det. Kommunikasjonsmodulen benyttes til å overføre elektronisk kreditt fra smartkortet til en betalingsmottaker. Smartkortet omfatter lagringsmidler for å lagre elektronisk kreditt og overføringsmidler for tilføying, eller fjerning av elektronisk kreditt. Kommunikasjonsmodulen omfatter drivmidler for å generere et signal for overføringen av elektronisk kreditt, rutingsmidler for å generere en adresse til hvilke dette elektroniske signalet skal sendes, en visningsanordning for å vise data angående en kredittoverføring, og en tastatur for å legge inn detaljer om en elektronisk overføring. Den elektroniske transaksjonsterminalen er innrettet slik at betaleren beholder fysisk styring av smartkortet alltid under gjennomføringen av en transaksjon.

'Handbuch der Chipkarten', 2. utgave 1996, Rankl/Effing beskriver et smartkort for utførelse av elektroniske transaksjoner.

EP567610B1 fremlegger et verdioverføringssystem som muliggjør verdier overført mellom elektroniske lommebøker og har en meldingsoverføringsprotokoll som omfatter en akseptmelding for å utgjøre et bevis for overføring, i en

regnskapstjeneste. Dette tillater avbrudd av en transaksjon før verdimeldingen i seg selv sendes.

GB 2261538 A Et transaksjonsautentiseringssystem omfatter et mikrobrikkekort og en terminal. Kortet har et minne for å lagre PIN-data og transaksjonssekvensdata. En prosessor inkrementerer transaksjonssekvensdata hver gang kortet benyttes i en transaksjon, og kombinerer og krypterer de inkrementerte transaksjonssekvensdata og en gitt PIN-datakomponent for å tilveiebringe en unik transaksjonssignatur. Den gitte PIN-datakomponenten og krypteringsnøkkelen som brukes under generering av transaksjonssignaturen omfatter en hemmelig komponent personlig for brukeren men skjult for brukeren og kun kjent for autorisatøren.

US4926480A og US4868376A viser bruk av digital signatur og såkalt avansert smartkort.

EP214609A2 fremlegger en elektronisk transaksjon hvor en for å forbedre en pålitelighet av meldingssertifisering ved digital signatur og muliggjør anvendelsen av den digitale signaturen i en formell transaksjon i stedet for tradisjonell signatur eller segle er følgende prosedyrer implementert ved å utnytte det faktum at, i e kryptografisk system med offentlig nøkkel representert gjennom et RSA-system, en første kodede melding avledet ved koding av en første dekodete melding ved å bruke en offentlig nøkkel av en første transaksjonsdetaker er lik en andre kodet melding utledet ved koding av en andre dekodet melding ved å bruke en offentlig nøkkel av en andre transaksjonsdeltaker.

Oppsummering

Et hovedmål med denne oppfinnelse er å lette elektroniske transaksjoner på en forenklet måte, selv om man opprettholder full sikkerhet. Nok et mål er å kunne utføre forskjellige typer elektroniske transaksjoner innenfor rammen om samme grunnkonsept.

Et annet mål er å lette slik elektronisk transaksjon uavhengig av valget av informasjonsoverføringskanal for den brukte transaksjonsmelding, og endelig er det et mål med oppfinnelsen å lette elektronisk transaksjon hvor det i prinsippet ikke trengs overføring av den brukte transaksjonsmelding via en pålitelig informasjonsoverføringskanal.

De mål som er nevnt ovenfor, nås med de trekk som antas å være oppfinneriske og som er satt opp i patentkravene.

Oppfinnelsen bygger således på innsikten om fordelaktig bruk av spesielle overføringsmeldinger som uavhengig av hverandre og under full brukerkontroll etableres av brukeren, og som har en slik natur at de bare kan være blitt etablert av brukeren. De kan derved ikke være blitt endret under overføringen til en mottaker eller

adressat uten at slik endring lett blir oppdaget (autentisering), og disse meldinger kan lett undersøkes med hensyn til gyldighet etter overføringen, i den hensikt å avslutte den ønskede transaksjon på foreskrevet måte. I samsvar med oppfinnelsen bruker senderen et unikt smartkort som er tilordnet vedkommende og som har liggende lagret en privat nøkkel (hvis offentlige ekvivalent i et asymmetrisk krypteringssystem generelt vil være tilgjengelig), slik at brukeren kan sende ut en transaksjonsmelding fra sin senderside og med en digital signatur som vil være unik for senderen, hvorved denne signerte transaksjonsmelding kan overføres på vilkårlig måte.

Bare en lovlydig bruker av smartkortet kan aktivere dette for signatur, og på denne måte tilfredsstilles et grunnidentitetskrav. Den digitale signatur inneholder videre en "datalås" som hindrer at meldingen kan endres uten at dette gjenkjennes i en etterfølgende autentisering, ved bruk av den generelt tilgjengelige offentlige nøkkel som hører til brukeren. Brukerens uavhengige etablering av ransaksjonsmeldingen betyr full kontroll over innholdet i meldingen. I og med oppfinnelsen kreves således at følsom informasjon, så som et kortnummer i den overførte transaksjonsmelding blir koplet til en digital signatur slik at informasjonen først da gjøres tilgjengelig ved utstedelsen. Uten kopling til en slik digital signatur vil informasjonen derved i prinsippet ikke ha noen verdi og følgelig ikke kunne misbrukes for falske nett-transaksjoner, selv om informasjonen skulle bli fanget opp av en person som ikke skal være involvert i overføringen av transaksjonsmeldingen. I grunnprinsippet vil det være irrelevant hvordan overføringen finner sted, og dette betyr en løsning som er i full motsetning til dagens streben etter etablering av spesielle pålitelige, det vil si krypterte kommunikasjonssystemer for overføring av transaksjonsmeldinger via for eksempel Internett.

Det foretrekkes at en transaksjonsmelding ifølge oppfinnelsen inneholder informasjon om senderen transaksjonsmengden og mottakeren, og fortrinnsvis et variabelt informasjonsledd, så som et serienummer.

Ifølge oppfinnelsen kan brukeren følgelig etablere det som kan kalles en signert "elektronisk sjekk" som kan overføres på vilkårlig måte og ved et vilkårlig tidspunkt til en adressat eller en mottaker.

Ved mottakingen kan en transaksjonsmelding ifølge oppfinnelsen kontrolleres med hensyn på om den er autentisk eller ikke, ved å kontrollere den digitale signatur, hvoretter en validering og en belastning eller kreditering av mottakeren kan finne sted for det aktuelle overføringsbeløp, på vilkårlig og hensiktsmessig måte, fortrinnsvis i henhold til de samme prinsipper som gjelder vanlig belastning av sjekker eller belastning når man betaler med et generelt elektronisk kort.

I henhold til oppfinnelsen kan den overførte signerte transaksjonsmelding inneholde den nødvendige transaksjonsinformasjon som klartekst, i hvilket tilfelle den

digitale signatur på i og for seg kjent måte kan være tilveiebrakt på basis av et konsentrat av den aktuelle meldingsinformasjon. Dette betyr at den etterfølgende autentisering, validering og kreditering på mottakersiden blir lettere, siden den nødvendige informasjon umiddelbart vil være tilgjengelig, så som informasjon om senderen, hvilket gjør det mulig å hente inn den korrekte offentlige nøkkel for autentisering av den digitale signatur.

Dersom denne digitale signatur utføres for hele transaksjonsmeldingen, slik at denne overføres i kryptert form, vil meldingen kunne utrustes med spesiell sender-informasjon som muliggjør på mottakersiden at man kan hente inn den riktige offentlige nøkkel for autentisering og omvandling av transaksjonsmeldingen til klartekst.

I henhold til oppfinnelsen kan transaksjonsmeldingen inneholde sender-informasjon av vilkårlig, hensiktsmessig form, så som i det minste ett av følgende informasjonselementer: et kortnummer, et kontantkortnummer, et belastningskort-nummer, et kredittkortnummer, et kontonummer, et fakturanummer og et identifikasjonsnummer. Hvis smartkortet brukes i henhold til oppfinnelsen og er et kort som er koplet til en konto, så som et kredittkort, kan man foretrekke å bruke det tilhørende kortnummer som senderinformasjon. For fagfolk er det imidlertid åpenbart at man kan bruke en hvilken som helst annen form for informasjon som på mottakersiden lett kan koples til en brukeridentitet og som følgelig kan koples til en tilhørende konto som skal belastes.

For mottakerinformasjonen gjelder hovedsakelig det samme. I det minste ett av følgende informasjonselementer kan for eksempel der være involvert i et kortnummer, et betalingskortnummer, et belastningskortnummer, et kredittkortnummer, et kontonummer, et fakturanummer og et identifikasjonsnummer. Også i dette tilfelle vil det være tilstrekkelig at informasjonen på mottakersiden utvetydig kan relateres til en mottaker av en betaling. Det skal bemerkes at overføring av et transaksjonsbeløp til en mottaker ikke behøver innebære kreditering av mottakerens konto, men det kan også innebære at for eksempel en administrativ enhet mottar transaksjonsmeldingen etter autentisering og validering, hvoretter en senderkonto belastes, slik at mottakeren får tilsendt informasjon om dette og et beløp som kan være i form av en sjekk eller en postanvisning.

Som beskrevet ovenfor er det et hovedtrekk med den foreliggende oppfinnelse at senderen, det vil si brukeren av smartkortet, etablerer og signerer transaksjons-meldingen under egen styring, det vil si at i alt vesentlig uavhengig av forbindelse med noe kommunikasjonsnett og en datamaskindialog med en mottaker, selv om en slik dialog naturligvis kan finne sted i forbindelse med selve overføringen av den signerte transaksjonsmelding. Følgelig etableres transaksjonsmeldingen fortrinnsvis uten

kopling til noe kommunikasjonsnett, det vil si uten direktekopling. Dette betyr at senderen har full kontroll over hvilke data som legges inn for etablering av transaksjonsmeldingen. Det er innlysende at signeringen kan utføres bare av senderen, siden vedkommende i det normale tilfelle vil være den eneste som kan aktivere sitt eget smartkort og derved frigi signaturmekanismen. Når det gjelder overføringen eller formidlingen av den signerte transmisjonsmelding, er det imidlertid ingen restriksjoner, hvilket vil forstås av beskrivelsen nedenfor. Brukeren eller en person som hejlper vedkommende, kan for eksempel ta smartkortet med den signerte transaksjonsmelding for å sende meldingen senere, for å sende meldingen fra et annet sted, etc., slik at man har en stor grad av frihet når det gjelder valg. Den signerte transaksjonsmelding kan også overføres til spesielle mellomliggende elementer eller via et transportmedium som formidler overføringen til mottakeren og/eller adressaten.

Ifølge oppfinnelsen er det fordelaktig at overføringsmeldingen etableres i smartkortet. Meldingen kan passende etableres ved hjelp av den programvare som er lagt in i dette på forhånd, og den senderinformasjon som fortrinnsvis legges inn i kortet, også på forhånd, det vil si et kortnummer. Passende kan et nytt serienummer automatisk etableres for hver transaksjonsmelding som skal utføres. Innføringen av den nødvendige meldingsinformasjon i kortet kan utføres på forskjellig måte, for eksempel ved hjelp av inngangskretser anordnet i selve kortet, idet kortet fortrinnsvis er bygget opp som et såkalt avansert smartkort. Informasjon som trengs for transaksjonsmeldingen kan også føres inn ved hjelp av en beskyttet kortterminal som fortrinnsvis kan bestå av brukerens egen terminal eller datamaskin, og utrustet med en kortleser. Informasjonen som trengs for transaksjonsmeldingen kan også leges inn ved hjelp av en separat korkommunikasjonsenhet, idet en slik enhet fortrinnsvis senere også kan tjene som en kortaktivator. En slik enhet kan fordelaktig konstrueres som en mindre bærbar enhet som brukeren kan ta med seg og som kan brukes av vedkommende når han/hun ønsker å aktivere sitt kort og/eller inngangsinformasjonen i kortet i omgivelser hvor ingen beskyttet kortterminal er tilgjengelig.

Informasjon som trengs for transaksjonsmeldingen kan også legges inn ved hjelpe av telekommunikasjonsenheter eller liknende og som er under kommando av smartkortet, for eksempel en mobil enhet, gjerne en mobiltelefon. I denne sammenheng kan enheten også brukes for å overføre de signerte transaksjonsmeldinger, for eksempel ved å bruke en såkalt SMS-tjeneste (tjeneste for korte meldinger).

Det er åpenbart at det også er mulig å etablere den aktuelle transaksjonsmelding utenfor smartkortet ved for eksempel å bruke en av de midler som er nevnt ovenfor. Den etablerte transaksjonsmelding legges deretter inn i smartkortet for signatur.

I henhold til et første aspekt av den foreliggende oppfinnelse er det på denne basis skaffet til veie en fremgangsmåte for å utføre elektroniske transaksjoner, hvor en sender for transaksjonsmeldinger er tildelt et smartkort med en tilhørende unik identitet og en privat nøkkel lagret i kortet på beskyttet måte, og hvor en tilordnet offentlig nøkkel er holdt generelt tilgjengelig, kjennetegnet ved at senderen i forbindelse med en elektronisk transaksjon under senderens egen kontroll og fortrinnsvis ved senderens egen innlegging av meldingsinformasjon, etablerer en transaksjonsmelding som inneholder informasjon som er nødvendig for transaksjonen og i smartkortet, forsyner den etablerte transaksjonsmelding med sin digitale signatur ved å bruke sin egen private nøkkel for deretter utføring og overføring av transaksjonsmeldingen.

I henhold til et andre aspekt av oppfinnelsen er det skaffet til veie et smartkort for å utføre elektroniske transaksjoner og med midler for lagring av kortidentifikasjonsinformasjon, midler for beskyttet lagring av en privat nøkkel, midler for lagring av en asymmetrisk algoritme, midler for innlegging av transaksjonsinformasjon i kortet, prosessormidler for etablering i kortet av en transaksjonsmelding og basert på den innlagte transaksjonsinformasjon, så som informasjon om beløp og mottaker og eventuelt informasjon som er lagret i kortet, så som informasjon om senderen og fortrinnsvis et serienummer og i tillegg for å forsyne transaksjonsmeldingen med en digital signatur på basis av den private nøkkel og den asymmetriske algoritme, og midler for å føre ut den signerte transaksjonsmelding.

I henhold til et tredje aspekt av oppfinnelsen er det videre skaffet til veie en kombinasjon av et smartkort og en brukerkontrollert kommunikasjonsenhet som er anordnet for kommunikasjon med smartkortet og hvor kortet er innrettet for å kombineres med hensyn til å frembringe en elektronisk transaksjonsmelding, idet kortet omfatter midler for beskyttet lagring av en privat nøkkel, midler for lagring av en asymmetrisk algoritme, og prosessormidler for å forsyne en etablert transaksjonsmelding med en digital signatur basert på den private nøkkel og algoritmen, idet kommunikasjonsenheten omfatter midler for å legge inn transaksjonsinformasjon, og at det er anordnet midler i denne kommunikasjonsenhet og/eller i kortet for generering av transaksjonsmeldingen.

Et fjerde aspekt ved oppfinnelsen involverer bruken av et smartkort med en privat nøkkel som ligger lagret i det og en asymmetrisk kryptografisk algoritme for å etablere i kortet, uavhengig av kommunikasjonsnettet, en elektronisk transaksjonsmelding som forsynes med en digital signatur basert på den private nøkkel.

Kort beskrivelse av tegningen

Ytterligere aspekter for særmerkede trekk ved oppfinnelsen vil fremgå av den detaljbeskrivelse som er satt opp nedenfor og som gjelder forskjellig utførelser, idet det vises til de tilhørende tegninger, hvor

fig. 1 skjematisk viser et eksempel på hvordan elektronisk transaksjon kan utføres ved hjelp av et åpent nett, så som Internett, det hele i samsvar med en utførelse av oppfinnelsen,

fig 2 viser skjematisk det samme opplegg med alternative måter å utføre transaksjonen på,

fig. 3 viser skjematisk hvordan elektroniske transaksjoner kan utføres ved hjelp av en butikkortterminal, det hele ifølge en annen utførelse av oppfinnelsen,

fig. 4 viser skjematisk det samme i et annet eksempel,

fig. 5 viser skjematisk hvordan elektroniske transaksjoner kan utføres via et mobiltelefonnett,

fig. 6 viser hvordan elektroniske transaksjoner kan utføres via et åpent nett for direktekontakt med en bank, og

fig. 7 viser skjematisk hvordan et avansert smartkort kan brukes for å utføre elektroniske transaksjoner i en annen versjon av oppfinnelsen.

Detaljert beskrivelse av foretrukne utførelsesformer

Fig. 1 viser således skjematisk en første utførelse av oppfinnelsen, som kan brukes for kredittkortbetaling via et åpent nett, så som Internett, mellom en sender og en mottaker som er inkludert i et nett. Senderen har aksess til et smartkort 1 og en datamaskin 3 som er utrustet med en passende kortleser (angitt ved 2) og som typisk kan være en hjemmedatamaskin (pc) og er koplet til Internett 5. En nettserver 7 (også benevnt "tjener") er koplet til nettet 5 og til forskjellige kredittkortstasjoner (administrasjonsenheter) 8 og 9 som er inkludert i nettet. Stasjonene er på konvensjonell måte koplet til hverandre og til forskjellige institusjoner som holder regnskap, så som banker 10, 11. I det foreliggende eksempel antas at senderen har en konto i banken 10 og et kredittkort som administreres av stasjonen 8, mens mottakeren 12 har sin konto i banken 11 og et kredittkort som administreres av stasjonen 9.

En betrodd tredje part (TTP) 13 er nettadministrator og ansvarlig for den nødvendige håndtering av nøkler. TTP 13 tildeler således hver bruker (senderen og mottakeren) sin private nøkkel som lagres på beskyttet måte i brukerens kort1 og holder en katalog 15 tilgjengelig fra hvilken den offentlige nøkkel for hver bruker kan tas ut.

Brukerens smartkort 1, som også har en konvensjonell kredittkortfunksjon, inneholder på kjent måte et lager og en prosessor i form av en eller flere integrerte

kretser (angitt ved 17) så vel som konvensjonelle midler for å etablere kommunikasjon mellom kortet og en kortleser når kortet er lagt in i en slik.

I tillegg til den allerede nevnte private nøkkel inneholder lageret og prosessoren en kryptografisk algoritme av asymmetrisk type og som kan være en DES-algoritme, samt programvare for å utføre signering av en transaksjonsmelding ut fra den private nøkkel og den kryptografiske algoritme. Smartkortet aktiveres på vilkårlig hensiktsmessig måte, for eksempel ved en PIN-inngang i kortet eller biometrisk.

Når det utføres en transaksjon, legges kortet 1 inn i datamaskinenes 3 kortleser (også angitt med henvisningstallet 17) slik at kortet aktiveres dersom dette ikke allerede er gjort. En transaksjonsmelding kan nå etableres i smartkortet 1 og/eller i maskinen 3. Hvis etableringen finner sted utelukkende i kortet, hvilket kan være å foretrekke sett fra et sikkrehetshensynspunkt, vil kortet også inneholde programvare som er egnet for dette formål. I dette tilfelle føres den nødvendige informasjon for transaksjonsmeldingen (spesielt når det gjelder beløp og mottaker) inn via tastaturet på maskinen 3, til kortet.

Dersom den aktuelle transaksjonsmelding etableres i maskinen i stedet for i kortet har denne programvare som trengs for formålet, og programvaren vil stå til rådighet for brukeren i forbindelse med utstedelsen av smartkortet. Også i dette tilfelle vil meldingsinformasjon legges inn via tastaturet.

Det er fordelaktig å bruke som senderinformasjon en kortidentifikasjon, så som nummeret på smartkortet, idet dette automatisk følger med kortet når transaksjonsmeldingen etableres. Som mottakerinformasjon brukes fortrinnsvis kortnummeret på mottakersiden.

Etter etablering av transaksjonsmelding bør det utrustes med serienummer og signeres, hvilket utføres i kortet, slik det er nevnt ovenfor. Dersom den aktuelle melding er etablert i kortet, kan det være ønskelig når det gjelder å begrense programvaren som må være tilgjengelig i kortet, å utføre den digitale signatur for den aktuelle melding, hvorved denne får formen av en kryptert tekst. Den signerte melding som deretter overføres må kunne formidle informasjon om senderen, slik at det blir mulig å ta ut den offentlige nøkkel som trengs for autentiseringen, hvilket vil beskrives nedenfor. Dersom særlig transaksjonsmeldingen etableres i senderens beskyttende datamaskin, kan det være hensiktsmessig å generere den digitale signatur i et sammendrag av den aktuelle melding, idet et slikt sammendrag vil være tilgjengelig som klartekst og også kan overføres som en slik.

Den signerte transaksjonsmelding kan nå med fordel gis formen av en E-post-melding og deretter sendes via nettet 5 til nettserveren 7.

Er transaksjonsmeldingen tilgjengelig som klartekst, kan serveren 7 ut fra den informasjon som ligger i meldingen direkte sende den signerte melding enten til

senderens eller mottakeres kortstasjon 8, 9 for administrasjon, i den hensikt å kunne autentisere og eventuelt, dersom autentiseringen er etablert, utføre en etterfølgende validering, belastning av senderen og kreditering av samme med transaksjonsbeløpet innlagt, under anvendelse av en hensiktsmessig klareringsprosedyre.

Autentiseringsmidlene som for eksempel gjør at senderens kortadministrator kan hente inn den aktuelle offentlige nøkkel fra en nøkkelkatalog som administratoren selv har eller katalogen 15 som hører til TTP 13, hvoretter den kryptografiske algoritme inngår, for kontroll av den digitale signatur i meldingen.

Dersom meldingen som mottas av serveren ikke er tilgjengelig som klartekst, kan den offentlige nøkkel hentes ut fra katalogen 15, idet denne nøkkel hører til senderen som derved blir identifisert ut fra den mottatte, signerte transaksjonsmelding, det vil si på basis av spesiell senderinformasjon så som en nettidentitet eller en Internettidentitet. Etter konvensjonell dekryptering av meldingen ved å bruke den innhentede offentlige nøkkel, får serveren 7 adgang til informasjonen i meldingen som klartekst og kan sende denne melding for autentisering etc., som nevnt ovenfor.

Et annet alternativ er å legge inn en bestemt adresse som hører til den autoriserte kortadministrator, for eksempel stasjonen 8 i meldingen som sendes via nettet 5, slik at serveren kan direkte får meldingen inn til seg for fortsatt prosessering som beskrevet ovenfor. Dersom den signerte melding ikke er tilgjengelig som klartekst, vil den også i dette tilfelle kunne inneholde slik informasjon som gjør at den riktige offentlige nøkkel kan hentes for autentisering og dekryptering av den aktuelle melding.

Fig. 2 illustrerer skjematisk en andre utførelse av oppfinnelsen og som hovedsakelig bruker samme konfigurasjon som på fig. 1, selv om transaksjons-meldingen fra senderen sendes direkte til mottakerens datamaskin 21 via nettet 5. Mottakeren sender meldingen slik det er indikert med pilen 23 via nettet til serveren 7 eller via en eller annen alternativ rute som indikert med pilen 25.

I denne utførelse kan det være hensiktsmessig at den aktuelle melding er tilgjengelig som klartekst, slik at mottakeren kan lese ut informasjonen fra den selv om han/hun ikke har umiddelbar tilgang til senderens offentlige nøkkel for autentisering eller dekryptering av den digitale signatur. Hvis det er behov for det, kan imidlertid den signerte melding krypteres av senderen med en offentlig nøkkel som hører til mottakeren, i hvilket tilfelle mottakeren ved mottakingen dekrypterer meldingen ved å bruke sin private nøkkel og den tilhørende kryptografiske algoritme, hvoretter den dekrypterte, men fremdeles signerte melding videreformidles.

I tilfelle man velger en overføringsrute 25 som er utenom nettet 5, kan det være fordelaktig å bruke mellommateriell, for eksempel en plate (angitt ved 26) som i enkelte tilfeller og på pålitelig måte kan formidle overføring fra mottakeren til

kortadministratoren eller banken for fortsatt prosessering i samsvar med det som er beskrevet ovenfor. Det er klart at mottakeren kan hente inn flere mottatte transaksjonsmeldinger via en slik mellomstasjon eller liknende før vedkommende tar skritt for fortsatt prosessering.

Fig. 3 illustrerer skjematisk en utførelse av oppfinnelsen og som er egnet for transaksjoner via en fremmed "terminal" 31 og som bruker en brukerkontrollert bærbar enhet 33 for etablering av en transaksjonsmelding.

Enheten 33 består av en kombinert aktivator og midler for å legge inn informasjon i smartkortet, og den er på hensiktsmessig måte anordnet for kommunikasjon med kortet 1, for eksempel ved å inneholde en integrert kortleser som kortet kan føres inn i. enheten 33 har videre et tastatur og en skjerm eller et vindu.

Når man ønsker å betale i en butikk eller et annet sted, føres kortet inn i enheten 33 og aktiveres, for eksempel ved å taste inn en PIN-kode ved hjelp av enhetens tastatur. Med dette tastatur legges også den nødvendige informasjon om betalingen inn, så som beløp og mottaker. Dersom transaksjonsmeldingen både etableres og signeres i det aktuelle kort, vil den aktuelle informasjon overføres til dette kort. Hvis den aktuelle melding og eventuelt et sammendrag av den skal etableres i enheten 33 for å kunne overføre informasjonen til kortet 1 med signatur, har enheten en prosessor og den programvare som trengs for formålet.

Kortet med den signerte transaksjonsmelding tas deretter ut fra enheten 33 og føres inn i butikkens leser/terminal 31 fra hvilken meldingen overføres for fortsatt prosessering på samme måte som beskrevet ovenfor. Akseptert autentisering og validering kan deretter føre til en kvittering som sendes tilbake til terminalern.

Det er klart at terminalen 31 naturligvis kan kommunisere direkte med serveren 7 på en eller annen måte enn via nettet 5, for eksempel via en beskyttet forbindelse.

Fig. 4 illustrerer en variant av utførelsen vist på fig. 3. Enheten 33 på fig. 3 er her erstattet av en beskyttet, fortrinnsvis utenomkoplet datamaskin eller terminal 43 som kan anordnes i for eksempel en butikk og som tillater separat og sikker etablering av en transaksjonsmelding utenom direktelinjeforbindelse, på en måte som tilsvarer den som er beskrevet i forbindelse med fig. 3, og hvis hensikt er inngang i en butikkkortterminal 31.

Fig. 5 illustrerer en utførelse av oppfinnelsen og som involverer bruken av en mobiltelefoninnretning 51 og et tilhørende mobiltelefonnet 55. Enheten omfatter i tillegg til mobiltelefonfunksjonene også en aktiverings- og inngangsfunksjon som beskrevet i forbindelse med enheten 33 på fig. 3. Mobiltelefonfunksjonen er fortrinnsvis også styrt av smartkortet.

Ved hjelp av telefonfunksjonen kan en signert transaksjonsmelding overføres til en enhet eller sentral 57 som utfører fortsatt prosessering av transaksjonsmeldingen, for eksempel i samsvar med den måte som er beskrevet tidligere.

Overføringen av transaksjonsmeldingen kan fortrinnsvis finne sted under bruk av en såkalt SMS-tjeneste eller liknende tilhørende mobiltelefonnettet.

Sentralen 57 kan også være en spesialenhet som etter autentisering etc. utfører betalinger basert på de mottatte transaksjonsmeldinger.

Fig. 6 illustrerer en utførelse av oppfinnelsen og som på en fordelaktig måte kan brukes for å effektuere betalingsordre. På senderens, det vil si betalerens plass, etableres signerte transaksjonsmeldinger som beskrevet, i dette tilfelle eksemplifisert ved samme måte som på fig. 1. Transaksjonsmeldingen sendes til senderens bank 10 som holder kontoen, og banken har adgang til senderens offentlige nøkkel via en katalog 60. Banken kan også være kortutsteder og nøkkeladministrator, og sender-informasjonen i transaksjonsmeldingen kan passende bestå av senderens bankkonto-nummer.

Ved mottakingen av en transaksjonsmelding og autentiseringen av denne, kommer senderens bank 10 opp med en klareringsprosedyre for den det skal betales til og som identifiseres i transaksjonsmeldingen, passende med det aktuelle bankkonto-nummer, og vedkommende krediteres med det aktuelle beløp, det vil si mottakerens kontor i mottakerens bank 11 blir kreditert med det aktuelle beløp.

Et annet alternativ er mulig ved at senderens bank 10 sender en overførings-ordre direkte til mottakeren 12, basert på for eksempel mottakerinformasjon i transaksjonsmeldingen. Dette alternativ er indikert med stiplet linje 62 på fig. 6.

I den utførelse som er vist på fig. 6 kan det være hensiktsmessig å kryptere den sendte signerte transaksjonsmelding for å øke sikkerheten. Senderen bruker i så fall den offentlige nøkkel tilhørende banken 10 og fortrinnsvis samme kryptografiske algoritme som ble brukt for signeringen. Det er klart at banken 10 umiddelbart kan utføre dekryptering ved å bruke dens private nøkkel.

Dersom banken 10 er administrator for senderens par nøkler, det vil si har tilgang til både den offentlige og den private nøkkel for senderen, kan senderen alternativt utføre krypteringen av den signerte melding ved hjelp av sin offentlige nøkkel. Banken 10 kan deretter dekryptere den sendte melding ved å bruke senderens private nøkkel som i dette tilfelle kan tas ut fra en katalog, før autentistering utføres ved å bruke senderens offentlige nøkkel.

Endelig viser fig. 7 skjematisk bruken av et såkalt avansert smartkort i forbindelse med oppfinnelsen og som også har et tastatur og et vindu eller en skjerm. Dette avanserte smartkort 71 muliggjør at en signert transaksjonsmelding kan etableres i kortet, fullstendig og uten ytre hjelpemidler. Deretter kan kortet settes inn i for

eksempel en datamaskin eller en terminal for å kunne formidle meldingen og for fortsatt og kontinuerlig prosessering i samsvar med det som er beskrevet ovenfor.

Selv om oppfinnelsen her er illustrert i flere utførelser, er den naturligvis ikke begrenset til disse, og endringer og modifikasjoner vil kunne tenkes innenfor rammen av de patentkrav som er satt opp nedenfor. Følgelig vil de enkelte trekk som hører til de forskjellige utførelser kunne kombineres på andre måter innenfor oppfinnelsens konsept.

Patentkrav

1. Fremgangsmåte for å utføre finansielle elektroniske transaksjoner, hvor en sender for transaksjonsmeldinger er tildelt et smartkort (1,71) med en tilhørende unik identitet og en privat nøkkel lagret i kortet på beskyttet måte, og hvor en tilordnet offentlig nøkkel er holdt generelt tilgjengelig,
karakterisert ved at senderen i forbindelse med en elektronisk transaksjon under senderens egen kontroll og fortrinnsvis ved senderens egen innlegging av meldings-informasjon, etablerer uavhengig av noe forbindelse til et kommunikasjonsnettverk (5) og uten datamaskin-dialog med en mottaker på basis av den innlagde transaksjons-informasjon en transaksjonsmelding som inneholder informasjon som er nødvendig for transaksjonen i smartkortet (1,71) ved hjelp av programvare som tidligere ble lagret i smartkortet og ved hjelp av sender-informasjon som på forhånd ble lagt inn i kortet, hvor sender-informasjonen på mottaker-siden lett kan knyttes til en brukeridentitet og i hans smartkort forsyner den etablerte transaksjonsmelding med sin digitale signatur ved å bruke sin egen private nøkkel for deretter utføring og overføring av transaksjonsmeldingen.

2 Fremgangsmåte ifølge krav 1,
karakterisert ved at transaksjonsmeldingen inneholder informasjon om senderen, mottakeren, beløpet og fortrinnsvis et transaksjonsserienummer.

3 Fremgangsmåte ifølge krav 1,
karakterisert ved at transaksjonsmeldingen etableres utenfor noen direktelinje, det vil si ikke koplet til noe kommunikasjonsnett som brukes for den etterfølgende overføring av meldingen.

4 Fremgangsmåte ifølge ett av de forutgående krav,
karakterisert ved at smartkortet aktiveres biometrisk.

5 Fremgangsmåte ifølge ett av kravene 3,
karakterisert ved at den informasjon som trengs for transaksjonsmeldingen føres inn ved hjelp av innføringsmidler anordnet i smartkortet, idet dette fortrinnsvis er et såkalt avansert smartkort (71).

6 Fremgangsmåte ifølge ett av kravene 1-4,
karakterisert ved at den informasjon som trengs for transaksjonsmeldingen føres inn ved hjelp av en beskyttet kortterminal.

7 Fremgangsmåte ifølge ett av kravene 1-4,
karakterisert ved at den informasjon som trengs for transaksjonsmeldingen føres inn ved hjelp av en separat kortkommunikasjonsenhet som fortrinnsvis også er en kort-aktivator.

8 Fremgangsmåte ifølge ett av kravene 1-4,
karakterisert ved at den informasjon som trengs for transaksjonsmeldingen føres inn ved hjelp av en telekommunikasjonsenhet som styres av smartkortet, særlig en mobil telekommunikasjonsenhet (51) så som en mobiltelefon.

9 Fremgangsmåte ifølge ett av de foregående krav,
karakterisert ved at transaksjonsmeldingen inneholder senderinformasjon i form av minst ett av følgende informasjonselementer: et kortnummer, et betalingskortnummer, et kredittkortnummer, et belastningskortnummer, et kontonummer, et faktureringsnummer og et ID-nummer.

10 Fremgangsmåte ifølge ett av de foregående krav,
karakterisert ved at transaksjonsmeldingen inneholder mottakerinformasjon i form av minst ett av følgende informasjonselementer: et kortnummer, et betalingskortnummer, et kredittkortnummer, et belastningskortnummer, et kontonummer, et faktureringsnummer og et ID-nummer.

11 Fremgangsmåte ifølge ett av de foregående krav,
karakterisert ved at den signerte transaksjonsmelding sendes til en kort- eller konto-administrator (8,9) som er knyttet til senderen eller mottakeren, at den digitale signatur for transaksjonsmeldingen autentiseres ved bruk av den offentlige nøkkel som tildeles den som identifiseres som sender i den overførte transaksjonsmelding, og ved vellykket autentisering blir mottakeren kreditert med det overførte beløp i en klareringsprosess.

12 Fremgangsmåte ifølge krav 11,
karakterisert ved at den signerte transaksjonsmelding først sendes til mottakeren som eventuelt etter egen kontroll av den digitale signatur for meldingen videreformidler den signerte transaksjonsmelding til kort- eller kontoadministratoren.

13 Fremgangsmåte ifølge ett av kravene 1-10,
karakterisert ved at den signerte transaksjonsmelding krypteres ved bruk av en offentlig nøkkel som hører til adressaten som transaksjonsmeldingen sendes til, at den krypterte signerte transaksjonsmelding sendes til adressaten, at adressaten ved bruk av sin private nøkkel dekrypterer den signerte transaksjonsmelding, at den digitale signatur for transaksjonsmeldingen autentiseres ved bruk av den offentlige nøkkel som er tildelt den som identifiseres som sender i meldingen, og at mottakeren når autentiseringen er gyldig blir kreditert med transaksjonsbeløpet i en klareringsprosess.

14 Fremgangsmåte ifølge krav 13,
karakterisert ved at adressaten er mottaker, at mottakeren etter dekryptering sender den signerte transaksjonsmelding til en kort- eller kontoadministrator, hvoretter autentiseringen finner sted.

15 Fremgangsmåte ifølge ett av kravene 1-10,
karakterisert ved at den signerte transaksjonsmelding krypteres ved å bruke senderens offentlige nøkkel og tillegges en senderinformasjon hvoretter den sendes til en kort- eller kontoadministrator som har senderens private nøkkel og som fortrinnsvis har sendt ut brukerens smartkort, at administratoren dekrypterer den mottatte krypterte melding ved bruk av den private nøkkel, at autentiseringen av den digitale signatur for den dekrypterte transaksjonsmelding finner sted ved å bruke den offentlige nøkkel som er tildelt den som er identifisert som sender av meldingen, og at mottakeren, dersom autentiseringen er gyldig blir kreditert med transaksjonsbeløpet i en klareringsprosess.

16 Fremgangsmåte ifølge ett av kravene 1-12,
karakterisert ved at den signerte transaksjonsmelding sendes ukryptert, særlig via et offentlig kommunikasjonsnett så som Internett eller et telekommunikasjonsnett.

17 Fremgangsmåte ifølge krav 1,
karakterisert ved at den signerte transaksjonsmelding sendes via E-post.

18 Fremgangsmåte ifølge ett av kravene 1-16,
karakterisert ved at den signerte transaksjonsmelding sendes via et mobiltelefonnett, særlig via såkalt SMS-tjeneste for korte meldinger.

19 Smartkort for å utføre elektroniske transaksjoner og med
- midler for lagring av kortidenttfikasjonsinformasjon,
- midler for beskyttet lagring av en privat nøkkel,

- midler for lagring av en asymmetrisk algoritme,
- midler for innlegging av transaksjonsinformasjon i kortet,
- prosessormidler for etablering i kortet av en transaksjonsmelding og basert på den innlagte transaksjonsinformasjon, så som informasjon om beløp og mottaker og eventuelt informasjon som er lagret i kortet så som informasjon om senderen og fortrinnsvis et serienummer og i tillegg for å forsyne transaksjonsmeldingen med en digital signatur på basis av den private nøkkel og den asymmetriske algoritme, hvor transaksjonsmeldingen inneholder den informasjonen som er nødvendig for transaksjonen og blir opprettet i smartkortet ved hjelp av programvare som tidligere ble lagt inn i smartkortet og ved hjelp av sender-informasjon lagt inn i smartkortet på forhånd hvor sender-informasjonen på mottakersiden lett kan knyttes til en brukeridentitet og
- midler for å føre ut den signerte transaksjonsmelding, hvor transaksjonsmeldingen er opprettet av en sender under hans egen kontroll i forbindelse med en elektronisk transaksjon.

20 Kort ifølge krav 19,
karakterisert ved at det er av såkalt avansert type.

21 Kort ifølge krav 19 eller 20,
karakterisert ved midler for biometrisk aktivering av kortet.

22 Kombinasjon av et smartkort og en brukerkontrollert kommunikasjonsenhet som er anordnet for kommunikasjon med smartkortet og hvor kortet er innrettet for å kombineres med hensyn til å frembringe en elektronisk transaksjonsmelding, idet kortet omfatter:

- midler for å lagre unik kortidentifikasjonsdata,
- midler for beskyttet lagring av en privat nøkkel,
- midler for lagring av en asymmetrisk algoritme, og
- prosessormidler for å forsyne en etablert transaksjonsmelding med en digital signatur basert på den private nøkkel og algoritmen, idet kommunikasjonsenheten omfatter midler for å legge inn transaksjonsinformasjon,

karakterisert ved at prosessormidlene er innrettet for generering av transaksjonsmeldingen i kortet basert på innmatet transaksjonsinformasjon, hvor transaksjonsmeldingen inneholder data som er nødvendig for transaksjonen og er opprettet i smartkortet ved hjelp av programvare som tidligere ble lagret i smartkortet ved hjelp av sendeinformasjon innsatt i kortet på forhånd, hvor senderinformasjonen på mottaker-

siden lett kan knyttes til en brukeridentitet, hvor transaksjonsmeldingen er opprettet av en sender under dens egen kontroll i forbindelse med en elektronisk transaksjon.

23 Kombinasjon ifølge krav 22,
karakterisert ved at kommunikasjonsenheten er en mobil telekommunikasjonsenhet.

24 Kombinasjon ifølge krav 22,
karakterisert ved at kommunikasjonsenheten er en kombinert kortaktivator og en informasjonsinnføringsenhet/en prosessor.

25 Kombinasjon ifølge ett av kravene 21-23,
karakterisert ved at kortet inneholder midler for biometrisk aktivering av kortet.

26 Anvendelse av et smartkort ifølge til ett av kravene 19-21, med en privat nøkkel beskyttet lagret deri, for å etablere, uavhengig av kommunikasjon, en elektronisk transaksjonsmelding basert på innlagt transaksjonsinformasjon som forsynes med en digital signatur basert på den private nøkkel, hvor transaksjonsmeldingen opprettes i smartkortet ved hjelp av programvare tidligere lagret i smartkortet.

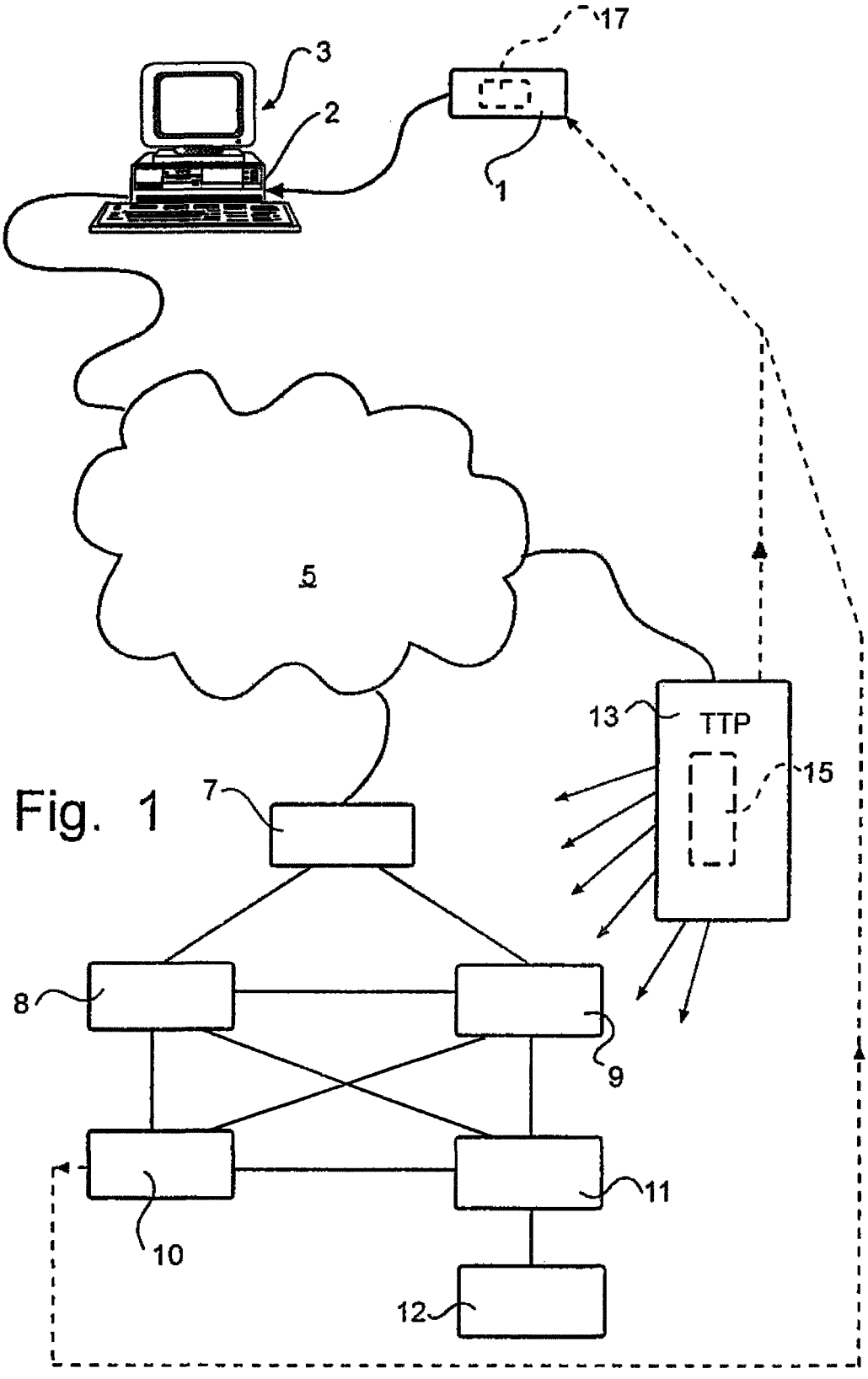


Fig. 1

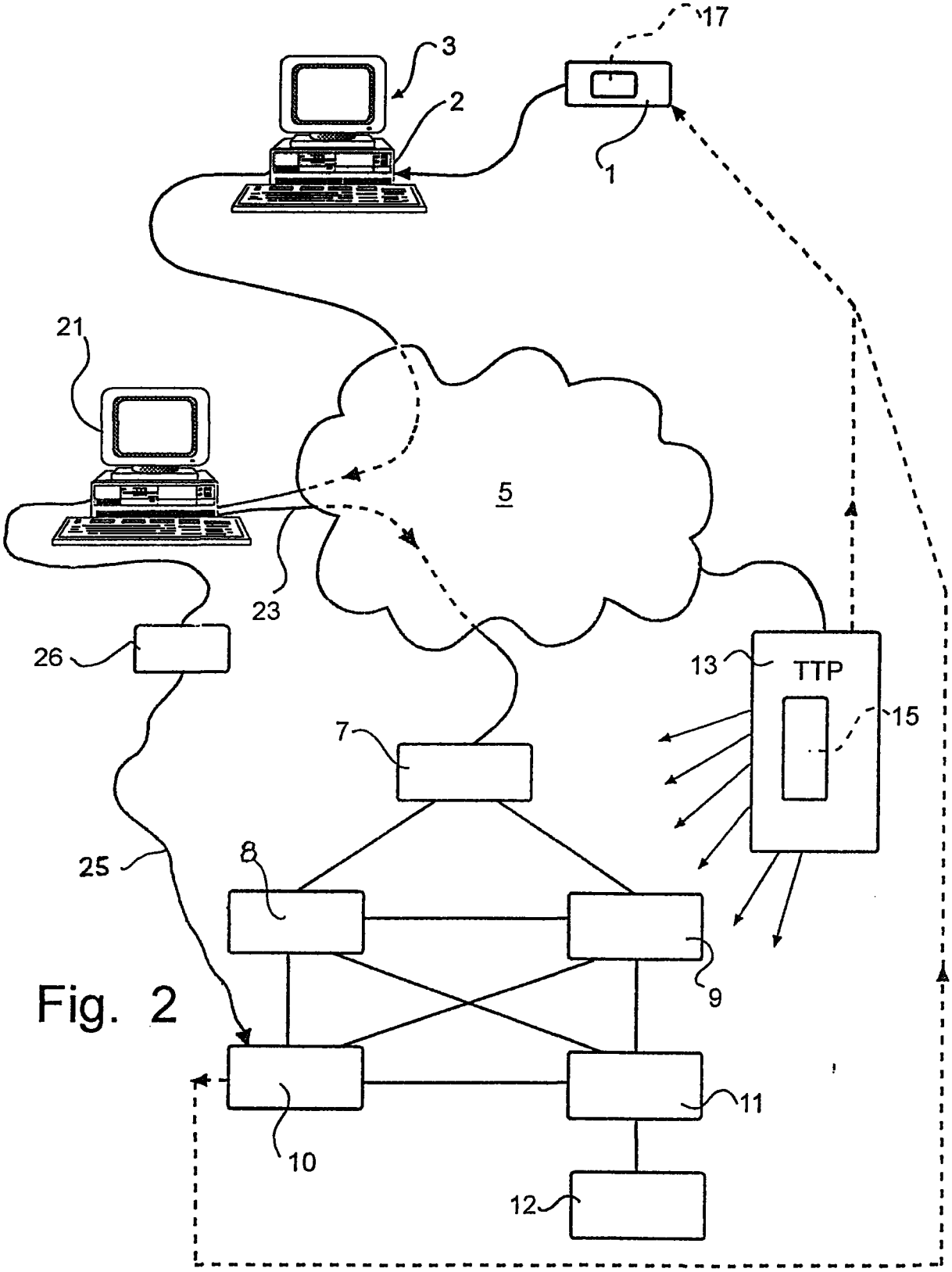


Fig. 2

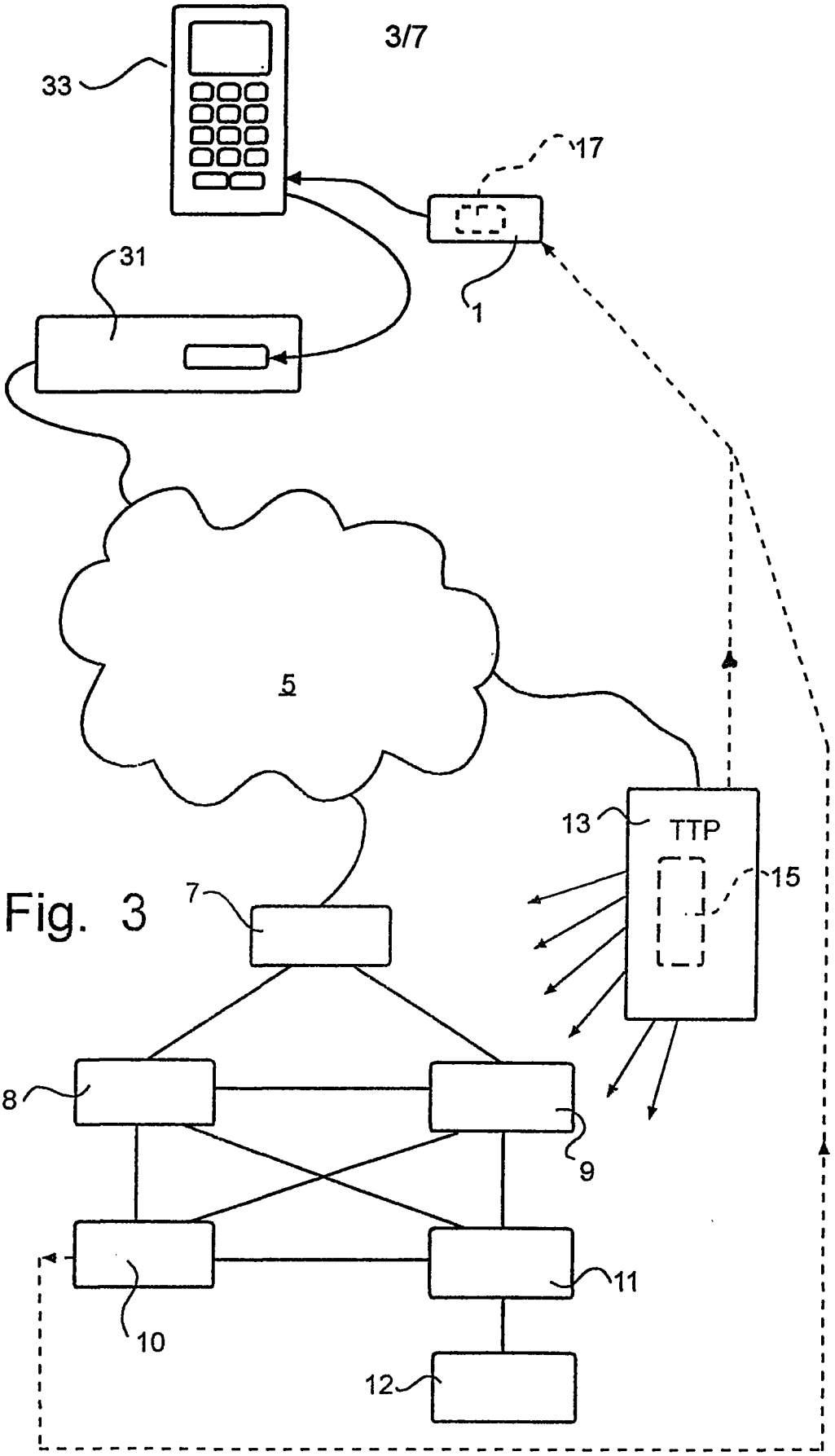


Fig. 3

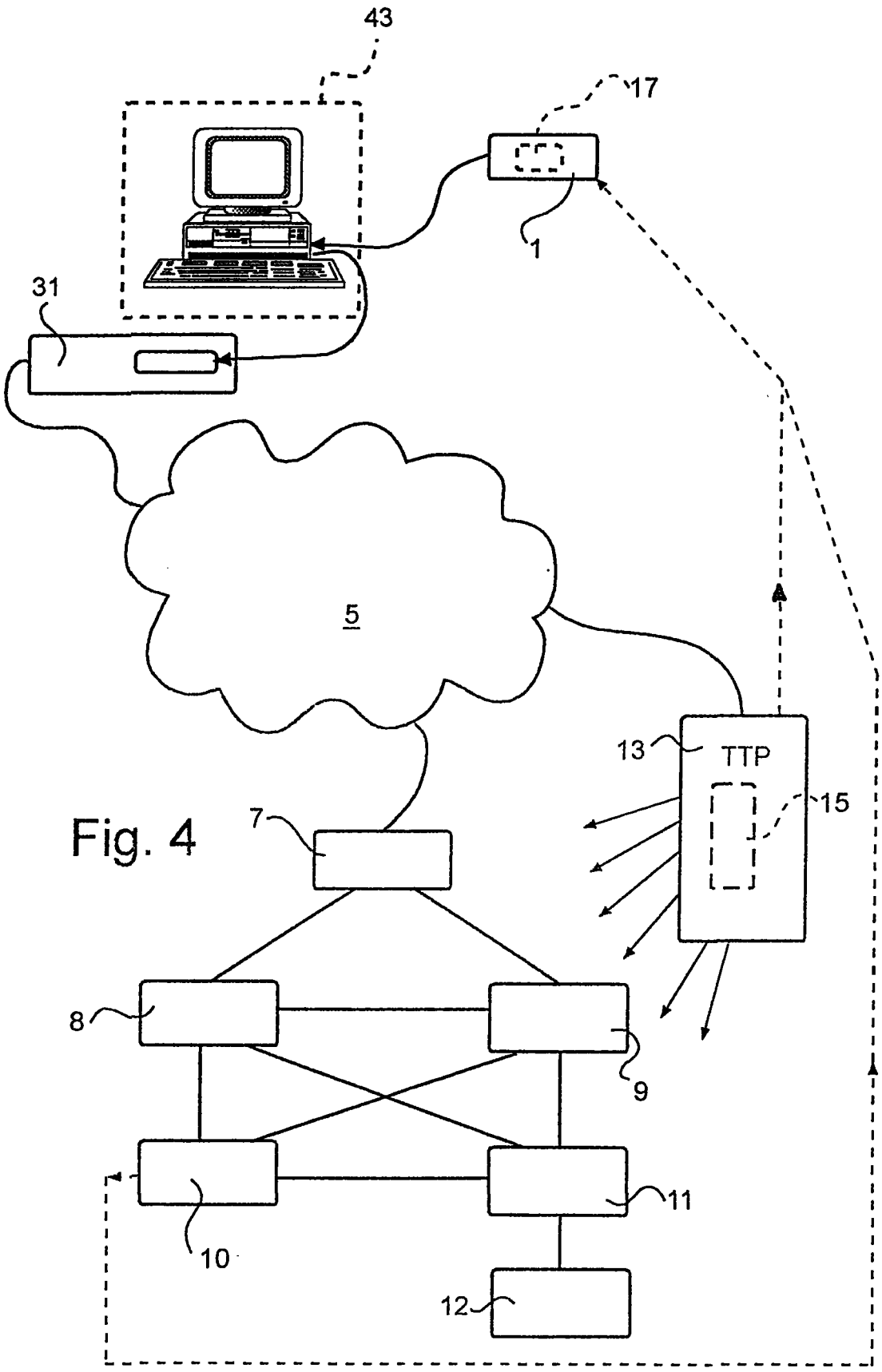


Fig. 4

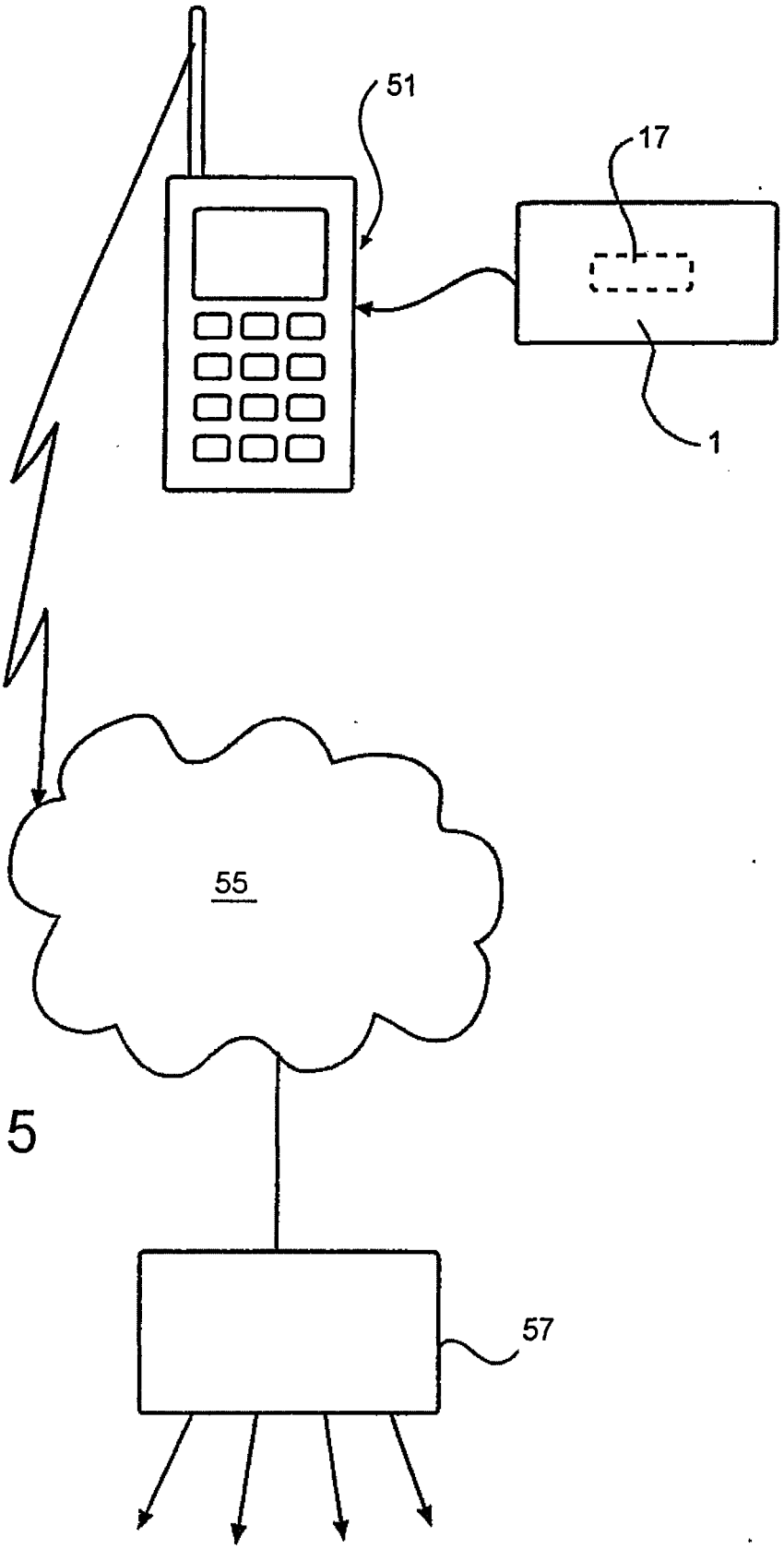


Fig. 5

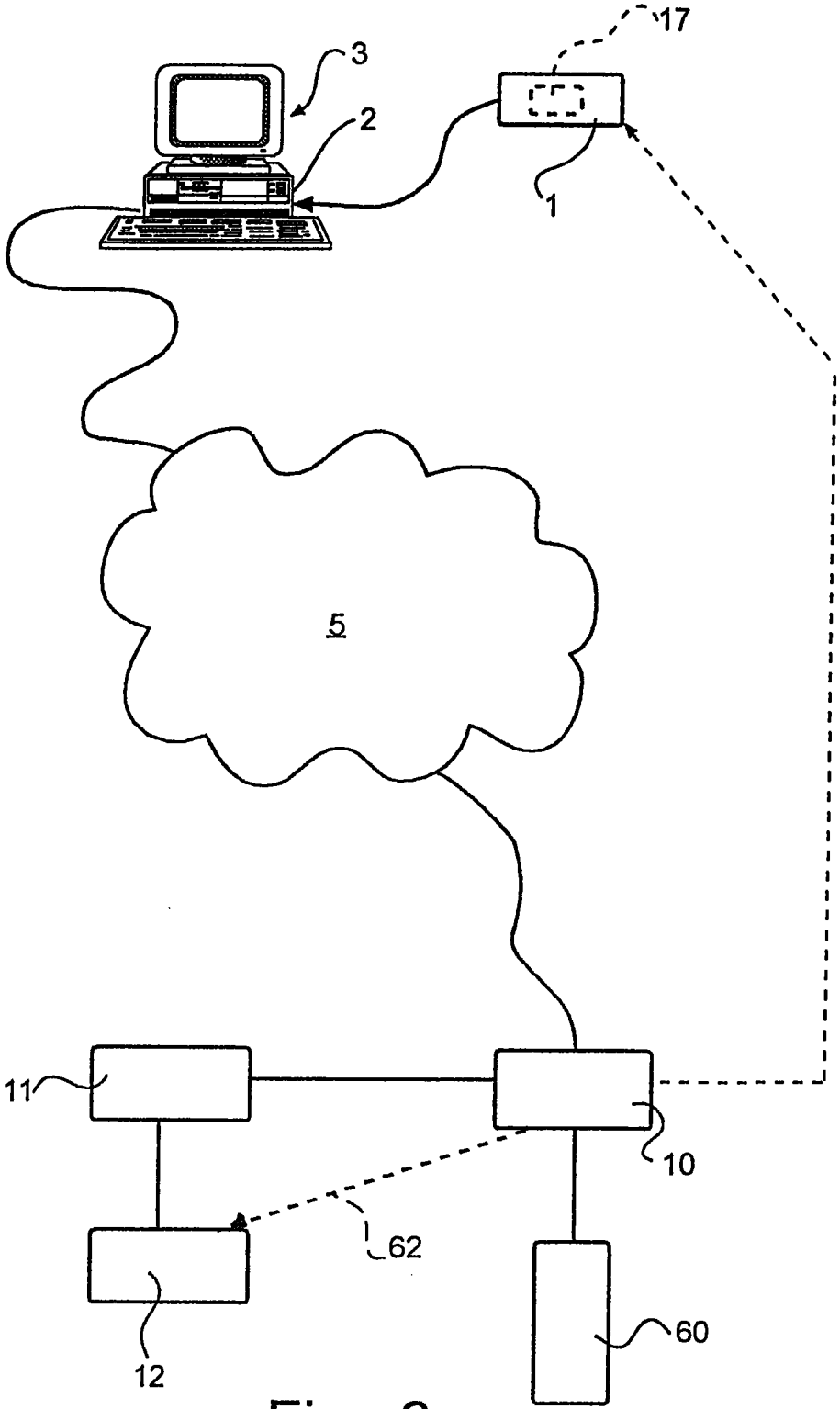


Fig. 6

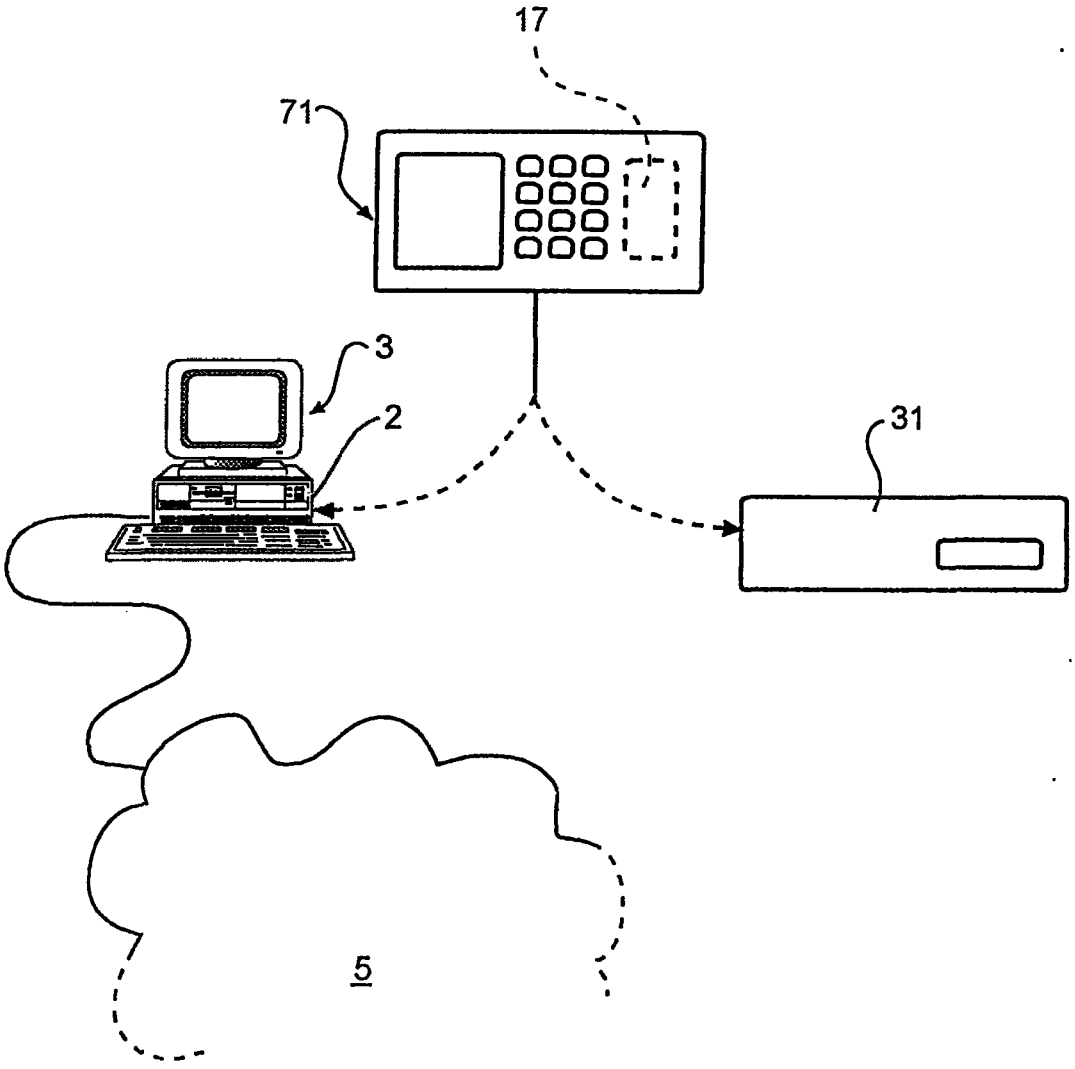


Fig. 7