(12) **PATENT**

(19) NO (11) **326836** (13) **B1**

NORGE (51) Int Cl.
H04Q 7/00 (2006.01)

Patentstyret

(21)	Søknadsnr	20023738	(86)	Int.inng.dag og søknadsnr	2001.02.10 PCT/EP01/01469
(22)	Inng.dag	2002.08.07	(85)	Videreføringsdag	2002.08.07
(24)	Løpedag	2001.02.10	(30)	Prioritet	2000.02.21, DE, 10007807
(41)	Alm.tilgj	2002.08.07			
(45)	Meddelt	2009.02.23			

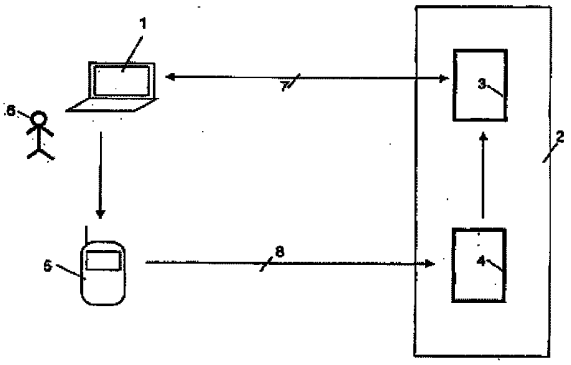
(73) Innehaver E-Plus Mobilfunk GmbH & Co KG, E-Plus-Platz 1, 40468 DÜSSELDORF, DE
(72) Oppfinner Siegfried Ergezinger, Nietzschestrasse 38, D-40822 Mettmann, DE
Christian Müller, Nettelbeckstrasse 4, D-40477 Düsseldorf, DE
Alexis Trolin, Ludwigkirchstrasse 13, D-10719 Berlin, DE
Anita Döhler, Eindamshauser Strasse 42, D-40822 Mettmann, DE
(74) Fullmektig Zacco Norway AS, Postboks 2003 Vika, 0125 OSLO

(54) Benevnelse **Fremgangsmåte til å fastslå autentsiteten ved identiteten til en tjenestebruker og innretning til utførelse av fremgangsmåte**

(56) Anførte publikasjoner DE 197 22 424 C1, US 5 875 394 A

(57) Sammendrag

Oppfinnelsen angår en fremgangsmåte og en anordning til å fastslå autentisiteten for identiteten til en tjenestebruker overfor en tjenesteyter for å frigi en adgangsrett (passord) for en tjeneste under anvendelse av to forskjellige datainngangsterminaler, en registreringsserver og en informasjonsomformer.



BESKRIVELSE

Område

Oppfinnelsen angår en fremgangsmåte til å fastslå autentisiteten ved identiteten til en tjenestebruker overfor en tjenesteyter til å frigi en adgangsrett (passord) for en tjeneste.

Videre angår oppfinnelsen en innretning til utførelse av den nevnte fremgangsmåte.

Teknikkens stand

Fra DE 197 18 103 A1 er det kjent en fremgangsmåte og en innretning til autorisering i et dataoverføringssystem ved anvendelse av et transaksjonsnummer (TAN) eller et sammenlignbart passord. Den kjente fremgangsmåte foreslår at

- brukeren i et første trinn over en datainngangsenhet sender sin identifisering og/eller et identifiseringsanrop for datainngangsenheten sammen med anmodning om frembringelse eller utvalg av et TAN eller et sammenlignbart passord fra en datafil til en autoriseringsinnretning;

- i et andre trinn genererer autoriseringsinnretningen TAN eller det sammenlignbare passord eller velger dette fra en datafil;

- i et tredje trinn sender autoriseringsinnretningen TAN eller det sammenlignbare passord over en annen overføringsbane enn i trinn 1 til en mottaker;

- i et fjerde trinn overtar brukeren dette TAN eller det sammenlignbare passord fra mottakere og innfører dette i datainngangsenheten;

- i et femte trinn blir dette TAN eller det sammenlignbare passord igjen overført til autoriseringsinnretningen;

- i et sjette trinn kontrollerer autoriseringsinnretningen gyldigheten for TAN eller det sammenlignbare passord for så

- i et syvende trinn å sette opp eller frikople en forbindelse mellom datainngangsenheten og en mottakerenhet.

Videre blir det i den kjente publikasjon foreslått at det skal dreie seg om et engangsbenyttet TAN eller et sammenlignbart passord. Gyldigheten for TAN eller det sammenlignbare passord kan være en på forhånd bestemt brukstid. Videre kan gyldigheten for TAN eller det sammenlignbare passord være avhengig av et påforhånd angitt antall av overførte datafiler. Gyldigheten for TAN eller det sammenlignbare passord er avhengig av en på forhånd bestemt størrelse for de overførte data. Tilgangen til datainngangsenheten og/eller mottaker og/eller mottakerenheten er beskyttet med passordet. De datafiler som overføres fra datainngangsenheten til mottakerenheten eller omvendt er kodet. De data som overføres fra datainngangsenheten til autoriserings-innretningen eller omvendt er likeledes kodet. Mottakeren kan være en personsøker. Det er også mulig at mottakeren er en mobiltelefon. Videre blir det foreslått å utføre mottakeren som telefaks. Mottakeren kan imidlertid også være en e-mail- eller nettadresse. Videre er det mulig at mottakeren er en datautgangsenhet. Til slutt blir det foreslått at taleutgangsenheten anvendes som høyttaler eller som taleenhet i en telefon. Det blir også beskrevet at mottakeren er en radiomottaker som er innbygget i datainngangsenheten og som frembringer TAN eller det sammenlignbare passord som vises på visningsanordningen eller monitoren i datainngangsenheten. Radioapparatet kan ha et element for brukeridentifisering og det er da mulig at identifiseringselementet for brukere er et magnetkort eller en kortbrikke. Til slutt er det tenkelig å utforme brukeridentifiseringselementet ved grafiske innretninger til kontroll av fingeravtrykk eller til bildeidentifisering av brukere. I autoriseringsinnretningen og i mottakeren er det lagt inn overensstemmende kodemoduler. Mottakerenheten kan imidlertid også være utført som en dørlåsemekanisme.

Dessuten blir det foreslått at autoriseringsinnretningen og mottakerenheten er integrert i et apparat. Datainngangsenheten, autoriseringsinnretningen og mottakerenheten kan integreres i et samlet apparat.

Ved den beskrevne fremgangsmåte skal de i DE 197 18 103 A1 beskrevne ytterligere tidligere kjente fremgangsmåter som "telebankvirksomhet" og det såkalte "tilbakeringesystem" gjøres funksjonssikrere.

Når brukeren ved det første trinn over en datainngangsenhet sender sin identifisering og/eller et identifiseringsanrop fra datainngangsenheten sammen med anmodning om

frembringelse eller utvalg av et TAN eller et sammenlignbart passord fra en datafil til en autoriseringsinnretning følger det tredje trinn som nemlig består i at autoriserings-innretningen sender TAN eller det sammenlignbare passord til mottakeren over en annen overføringsvei, mens brukeren i et fjerde trinn overtar dette TAN eller det sammenlignbare passord fra denne mottaker og igjen innfører dette i sin datainngangsenhet. Dermed blir to forskjellige overføringsveier tatt i bruk. Brukerens autentisitet som for tjenesteyteren er av meget høy betydning blir ikke kontrollert i den fremgangsmåte som er beskrevet i DE 197 18 103 A1.

Den fremgangsmåte som er beskrevet i DE 197 28 103 A1 åpner muligheten for at en bruker legger frem falsk identitet for å kunne foreta misbruk. De følgende misbrukmuligheter består her av:

1. En bruker melder seg under falsk identitet og får tilsendt passordet på mottakeren.

2. En bruker melder seg på forskriftsmessig måte. På grunn av tekniske problemer forsinkes utstedelsen av passordet til mottakeren. Mottakeren kan i mellomtiden komme i uriktige hender.

Fremgangsmåten bygger på at et gyldig passord blir sendt til mottakeren, noe som med en gang gjør det mulig med falsk bruk av tjeneste til skade for tjenesteyteren eller tredjemann.

Ved DE 197 22 424 C1 er det kjent en fremgangsmåte til sikret tilgang for en bruker til et adskilt system med data som er lagret i et datalager, med de følgende trinn:

Opprettelse av en første forbindelse mellom en første kommunikasjonsinnretning og en tilgangsanordning og overføring av et første kodeord fra den første kommunikasjonsinnretning til tilgangsanordningen;

Sammenligning av det første kodeord med første autentiseringsdata som er lagret i tilgangsinnretningen;

Oppstilling av en andre forbindelse mellom en andre kommunikasjonsinnretning og tilgangsanordningen og overføring av et andre kodeord fra den andre kommunikasjons-innretning til tilgangsanordningen;

Sammenligning av det andre kodeord med andre autentiseringsdata som er lagret i tilgangsanordningen; og

Frigivningen av et tilgang til systemet med en eller begge kommunikasjonsinnretninger når det foreligger en på forhånd angitt betingelse mellom det første og det andre kodeord med de andre autentiseringsdata som er lagret i tilgangsanordningen.

I denne forbindelse blir det også foreslått følgende trinn:

overføring av det andre eller et tredje kodeord fra tilgangsanordningen til den første kommunikasjonsinnretning;

overføring av det andre eller tredje kodeord fra den første kommunikasjonsinnretning til den andre kommunikasjonsinnretning; og

overføring av det andre eller det tredje kodeord fra den andre kommunikasjons-innretning til tilgangsanordningen som foretar en tilsvarende kontroll av kodeordet før tilgang til dataene blir frigitt.

Videre blir det foreslått opprettelse av en forbindelse mellom en første kommunikasjonsinnretning og en tilgangsanordning og overføring av et første kodeord fra den første kommunikasjonsinnretning til tilgangsanordningen hvorved det foregår en sammenligning av det første kodeord med de første autentiseringsdata som er lagret i tilgangsanordningen.

Når det finnes en på forhånd angitt betingelse mellom det første kodeord og autentiseringsdataene som er lagret i tilgangsanordningen kan det opprettes en andre forbindelse mellom tilgangsanordningen og en andre kommunikasjonsinnretning og overføring av et andre kodeord fra tilgangsanordningen til den andre kommunikasjons-innretning:

overføring av det andre kodeord fra den andre kommunikasjonsinnretning til den første kommunikasjonsinnretning:

overføring av det andre kodeord fra den første kommunikasjonsinnretning til tilgangsanordningen;

sammenligning av det andre kodeord med de andre autentiseringsdata som er lagret i tilgangsanordningen; og

frigivning av en tilgang til systemet med en eller begge kommunikasjonsinnretninger når det finnes et på forhånd angitt forhold mellom det andre kodeord og de andre autentiseringsdata som er lagret i tilgangsanordningen.

Videre blir det foreslått en fremgangsmåte som er kjennetegnet ved opprettelse av den første og andre forbindelse over kommunikasjonsbaner som er uavhengig av hverandre der det som første eller andre kommunikasjonsinnretning benyttes en databehandlings-anordning og forbindelsen mellom databehandlingsanordningen og tilgangsanordningen opprettes over et databehandlingsnett. Som forbindelsen mellom tilgangsanordningen og databehandlingsanordningen kan det anvendes et Internett. Som første eller andre kommunikasjonsinnretning kan det anvendes en telefon idet forbindelse mellom telefonen og tilgangsanordningen er dannet av et telefonnett. Som kommunikasjons-innretning kan det anvendes en mobiltelefon. Det første eller andre kodeord kan overføres ved betjening av en telefonanropstast eller i det minste en annen tast på telefonen. Systemet kan være et GSM-nett og lageranordningen kan være et Home Location Register der data som er knyttet til deltakere er lagret. Minst ett av kodeordene kan frembringes i tilgangsanordningen eller på et annet sted og bare være gyldig for engangs bruk. Videre blir det foreslått at minst ett av kodeordene frembringes under anvendelse av en deltakeridentifikasjon og under aktuelt klokkeslett og dato. Ett av kodeordene kan anvendes for en datakoding og for en dataoverføring mellom den første eller den andre kommunikasjonsinnretning og tilgangsanordningen. Etter frigivning av tilgang til data kan det fra en av kommunikasjonsinnretningene overføres minst ett ytterligere kodeord til tilgangsanordningen for å frigi en utvidet tilgang til systemet eller til ytterligere data som er lagret i lageranordningen. Som anordning kan det anvendes et system med sammenkoplede tilgangsanordninger, med en databehandlingsanordning, eller over et databehandlingsnett, som kan tilkoples tilgangsanordningen under anvendelse av en fast tilkoplet telefon, en mobiltelefon, som over et fast nett resp. et mobilnett kan tilknyttes tilgangsanordningen.

Denne anordning frembringer på en meget komplisert måte forskjellige kodeord som sendes over adskilte kommunikasjonsinnretninger.

Fra WO 95/19593 er det kjent et datasikkerhetssystem der systemet frembringer en tilfeldig kode A som blir omtransformert og frembringer en kode B og til og med

frembringer en tredje kode som skal sammenlignes med den andre kode og først ved overensstemmelse mellom den andre og den tredje kode frigis tilgang.

Formål

Formålet med foreliggende oppfinnelse er å utforme en fremgangsmåte til frigivning av en tilgangsrett på basis av kontroll av autentisiteten for identiteten til en tjenestebruker på det området det her gjelder. Fremgangsmåten som skal gi tjenesteyteren sikkerhet for at tilgangsrett bare blir frigitt til tjenestebrukeren når dennes autentisitet er kontrollert.

Videre er formålet med oppfinnelsen å frembringe en fordelaktig anordning til utførelse av fremgangsmåten ifølge oppfinnelsen.

Løsning av oppgaven vedrørende fremgangsmåten

Denne oppgave blir løst med de trekk som er gjengitt i patentkrav 1.

Noen fordeler

Ved oppfinnelsen blir det i motsetning til DE 197 18 103 A1 bare over en f.eks. en sikret forbindelse oversendt identifiseringen til tjenesteyteren, mens denne over den samme forbindelse sender tilbake det ennu ugyldige passord eller lignende til brukeren.

Fremgangsmåten kan anvendes når en adgangsrett til bruk av en tjeneste bare skal frigis av tjenesteyteren når på forhånd autentisiteten for identiteten til tjenestebrukeren ble kontrollert med høy sikkerhet. Ved denne kontroll av autentisiteten for identiteten til tjenestebrukeren og tilknytningen mellom frigivningen av tilgangsanropet til denne kontroll blir muligheten for misbruk ved fremleggelse av en falsk identititet i høy grad redusert.

Utnyttelse ved misbruk er bare mulig når sluttutstyret på tidspunktet for registreringen allerede er i gale hender.

Videre utførelsesformer ifølge oppfinnelsen

Ytterligere utførelsesformer ifølge oppfinnelsen er beskrevet i **patentkravene 2 til 8.**

Begrensningen med tidsrommet i løpet av hvilket det fremdeles ugyldige passord kan benyttes for å autentisere tjenestebrukeren forbedrer også sikkerheten siden tjenestebrukeren er tvunget til å autentiseres seg i det nevnte tidsintervall. En autentisering etter utløp av tidsintervallet er ikke mulig og i dette tilfellet må tjenestebrukeren registrere seg på nytt og får da et nytt ugyldig passord - **patentkrav 2.**

Etterat tjenestebrukeren ble riktig autentisert og passordet ble frigitt ham av tjenesteyteren skal det for tjenestebrukeren være mulig å endre passordet etter eget ønske - **patentkrav 3.**

For å øke sikkerheten er det en mulighet å begrense bruken av det gyldige passord på en slik måte at passordet bare forblir gyldig ved et på forhånd bestemt antall bruk. Når dette antall er nådd blir passordet automatisk gjort ugyldig. Gyldigheten blir først gjenopprettet ved at tjenestebrukeren på nytt autentiserer seg med den fremgangsmåte som er beskrevet i patentkrav 1 - **patentkrav 4.**

Kodingen byr tjenestebrukeren på den fordel at hans personlige data som f.eks. bankforbindelse, kredittkortnummer og annet ikke blir opplyst til tredjemann - **patentkrav 5.**

Kodingen byr for tjenesteyteren på den fordel at det ugyldige passord og ytterligere informasjoner til registreringsserveren ikke kan misbrukes av tredjemann - **patentkav 6.**

GSM-standarden har til rådighet høysikre fremgangsmåter til sikringen av autentisiteten til en mobilradiobruker. Der er overføringen av data fra sluttanordningen til informasjonsomformeren velegnet - **patentkrav 7.**

For å fastslå identiteten i ISDN kan den såkalte "Calling Line Identification" benyttes som, ifølge teknikken stand også anordnes for andre formål som f.eks. identisitetstrekk - **patentkrav 8.**

Løsning av oppgaven vedrørende anordningen

Denne oppgave blir løst med de trekk som er beskrevet i **patentkrav 9**.

Noen fordeler

Når fremgangsåten som er angitt i **patentkrav 9** benyttes i et mobilradionett fremkommer det for tjenestebrukeren og den som driver nettet de følgende fordeler:

En mobilradiokunde (tjenestebruker) har en avtale med den som driver mobilradionettet (tjenesteyteren) som tillater at de påløpende gebyrer kan belastes bankkonto av den som driver mobilradionettet. Når mobilradiokunden beslutter seg for å benytte en Internettjeneste som også tilbys av den som driver mobilfunknettet må kunden registrere seg for denne tjeneste. Etter registreringen skal kunden kunne benytte tjenesten under anvendelse av adgangsretten. Denne bruk av tjenesten blir likeledes avregnet ved trekk i bankinnskudd. I forbindelse med den bestående rett til belastning av bankinnskudd er det for å beskytte mobilradiokunden og den som driver mobilradionettet viktig å sikre autentiseteten for identiteten til en tjenestebruker som registrerer seg for å utelukke misbruk. Anvendelsen av et ISDN-nett i stedet for et mobilradionett byr på den samme fordel.

På tegningen er oppfinnelsen, delvis skjematisk, vist i form av et utførelseseksempel.

Med henvisningstallet 1 er det vist til en datainngangsterminal som første endeanordning og som i dette tilfellet er utført som en PC, mens det med henvisningstallet 2 er angitt en tjenesteyter som omfatter en registreringsserver 3 og et Short-Message-Service-Center som informasjonsomformer 4.

Henvisningstallet 5 angir en andre sluttanordning som i dette tilfellet er utført som en mobilradioanordning.

Datainngangsterminalen 1 som første sluttanordning og den andre sluttanordning 5 er begge registrert for en tjenestebruker 6 av tjenesteyteren 2. Dette betyr altså at tjenesteyteren 2 kjenner de personlige data til tjenestebrukeren 6. Som regel befinner sluttanordningen 1 og sluttanordningen 5 seg hos den samme tjenestebruker 6.

Datainngangsterminalen 1 kan over en sikret forbindelse 7, som for eksempel Secure Socket Layer settes i forbindelse med registreringsserveren 3 hos tjenesteyteren, mens den andre endeanordning 5 kan komme i forbindelse med informasjonsomformeren 4 over en forbindelse 8 for eksempel over et GSM-mobilradionett eller over ISDN eller SUS.

Fremgangsmåten er som følger:

Trinn 1:

Tjenestebrukeren 6 setter seg med den første sluttanordning 1, altså med datainngangsterminalen 1 over den sikrede forbindelse 7 i forbindelse med registreringsserveren 3 som kjenner tjenestebrukerens 6 personlige data.

Trinn 2:

Registreringsserveren 3 sender til tjenestebrukeren 6 på vedkommendes datainngangsterminal 1 og over den samme forbindelse 7 et fremdeles ugyldig passord (kodenummer. TAN eller lignende).

Trinn 3:

Tjenestebrukeren 6 leser passordet, kodenummeret. TAN eller lignende på sin sluttanordning 1.

Trinn 4:

Tjenestebrukeren 6 det ifølge trinn 3 avleste passord, kodenummer eller lignende over sin andre endeanordning 5 over forbindelsen 8, for eksempel over et GSM-mobilradionett til informasjonsomformeren 4.

Trinn 5:

Tjenesteyteren 2 kontrollerer, over forbindelsen 7 passordet, kallesignalet eller lignende som er sendt til datainngangsterminalen 1 med det passord eller lignende som er mottatt over forbindelsen 8 fra tjenestebrukeren 6. Ved likhet blir passordet, kallesignalet eller lignende gjort gyldig og tjenestebrukeren 6 kan benytte tjenesteyterens 2 tjeneste, for eksempel i Internett.

Registreringsserveren 3 og informasjonsomformeren 4 kan være bygget sammen.

Videre er det mulig at datainngangsterminalen 1 kan videreføre det passord, kallesignal eller lignende som er mottatt over ledningen 7 fra registreringsserveren 3 automatisk over en andre sluttanordning 5 og dermed over forbindelsen 8 til informasjons-omformeren 4.

De trekk som er beskrevet i sammendraget, i patentkravene og i beskrivelsen såvel som vist på tegningen kan både enkeltvis og i forskjellige kombinasjoner være vesentlige for virkeliggjørelse av oppfinnelsen.

Liste over henvisningstall

1	Datainngangsterminal, sluttanordning 1, PC
2	Tjenesteyter
3	Registreringsserver
4	Short-Message-Service-Center, informasjonsomformer
5	Andre sluttanordning, mobilradioanordning, datainngangsterminal
6	Tjenestebruker
7	Sikret forbindelse
8	GSM-mobilradionett, ISDN; SUS-forbindelse
TAN	Transaksjonsnummer

Litteraturfortegnelse

DE 197 18 103 A1

DE 197 22 424 C1

WO 95/19593 A1

Nye patentkrav

1.

Fremgangsmåte til å fastslå autentisiteten ved identiteten til en tjenestebruker (6) overfor en tjenesteyter (2) med en registreringsserver (3) og en informasjonsomformer (4) for klarering av en adgangstilgang for en tjeneste, ved å bruke to forskjellige datainngangsterminaler (1,5) registrert for den samme tjenestebrukeren (6) med en registreringsserver (3), karakterisert ved at fremgangsmåten innbefatter trinnene:

a) tjenestebrukeren (6) etablerer via den første datainngangsterminalen (1) via en forbindelse (7) sikret ved, for eksempel, secure socket layer kontakt, med registreringsserveren (3) som kjenner de personlige data for tjenestebrukeren (6),

b) registreringsserveren (3) sender til tjenestebrukeren (6) via den samme sikrede forbindelsen (7) til sin første datainngangsterminal (1) en ugyldig adgangskode ved hjelp av hvilket adgang til tjenesten fremdeles er mulig,

c) tjenestebrukeren (6) identifisert via den sikrede forbindelsen (7) i henhold til egenskapen a), legger merke til på sin første datainngangsterminal (1) på den ugyldige adgangskoden som er sendt til ham,

d) den ugyldige adgangskoden sendt via den første datainngangsterminalen (1) blir sendt til den samme informasjonsomformeren (4) via en andre datainngangsterminal (5) via en videre sikret forbindelse (8), for eksempel, via et GSM/SMS mobilt telefonnettverk eller via en ISDN forbindelse,

e) tjenesteyteren (2) kontrollerer den ugyldige adgangskoden sendt via den videre sikrede forbindelsen (8) i henhold til egenskap d) og sammenlikner den med den ugyldige adgangskoden sendt til den første datainngangsterminalen (1) via den første sikrede forbindelsen (7) og, dersom de er like, tillates adgang til tjenesten fra tjenestebrukeren (6).

2.

Fremgangsmåte i henhold til krav 1, karakterisert ved at den initielt bygger via adgangskoden sendt til den første datainngangsterminalen (1) til tjenestebrukeren (6) via den sikrede linjen (7) kan bli brukt av tjenestebruekren (6) for bare en begernset tidsperiode.

3.

Fremgangsmåte i henhold til krav 1 eller 2, k a r a k t e r i s e r t v e d at adgangskoden for tjenestebrukeren (6) kan bli forandret av tjenestebrukeren (6) etter hans ønske etter klarering fra tjenesteyteren (2).

4.

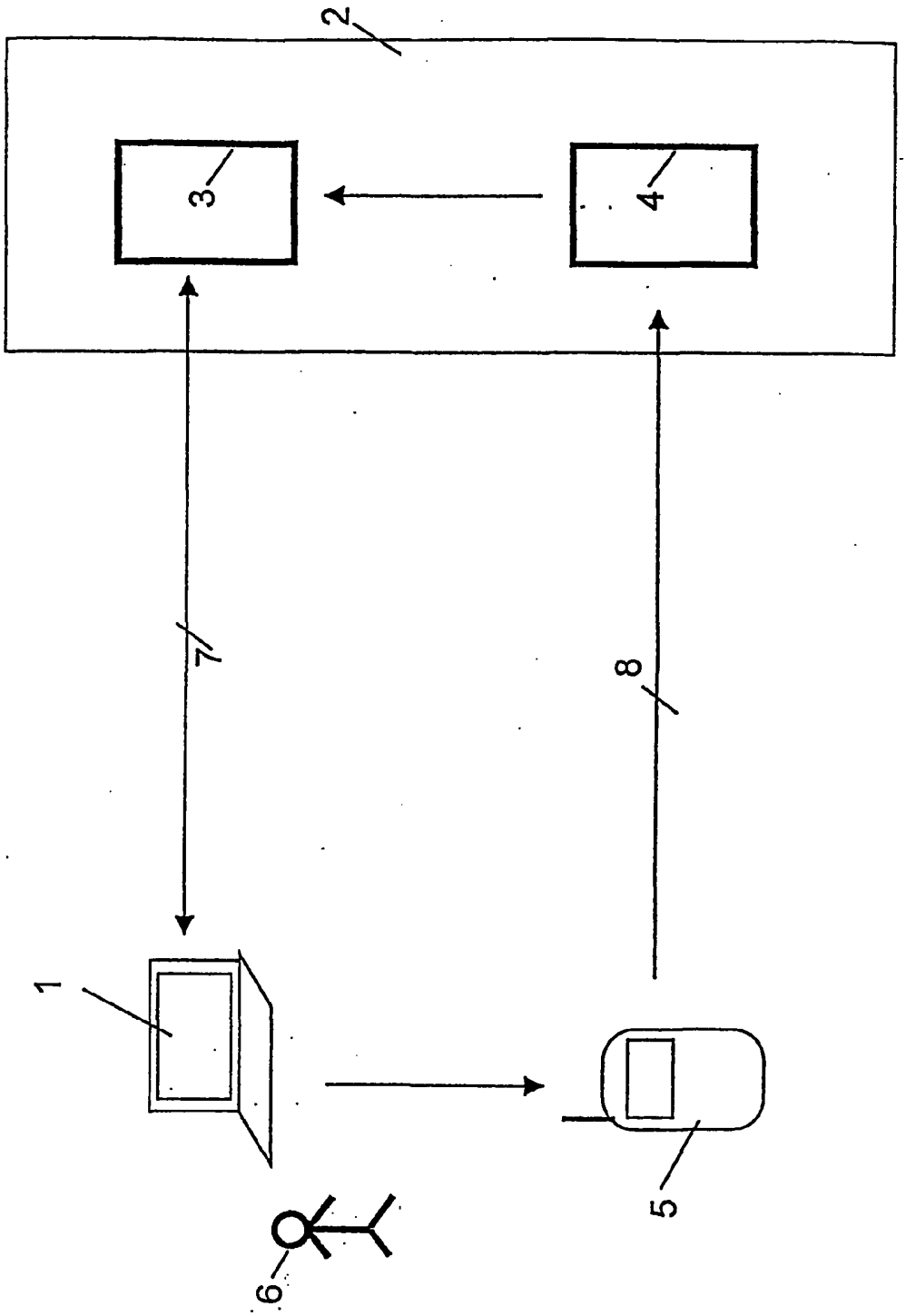
Fremgangsmåte i henhold til krav 1 eller ett av kravene 2 til 3, k a r a k - t e r i s e r t v e d at den gyldige adgangskoden er begrenset til et spesifikt antall av bruk.

5.

Fremgangsmåte i henhold til krav 1 eller ett av kravene 2 til 4, k a r a k - t e r i s e r t v e d at data sendt fra den første datainngangsterminalen (1) til registreringsserveren (3) er kodet.

6.

Fremgangsmåte i henhold til krav 1 eller ett av kravene 2 til 5, k a r a k - t e r i s e r t v e d at den initielt fremdeles ugyldige adgangskoden sendt tilbake fra registreringsserveren (3) til den første datainngangsterminalen (1) er kodet.


2
3
4
7
8
1
5
6