NORGE

(12) **PATENT**

(19) NO (11) **314372** (13) B1

(51) Int Cl[7] G 09 C 5/00

Patentstyret

(21) Søknadsnr	20013078	(86) Int. inng. dag og søknadsnummer	
(22) Inng. dag	2001.06.20		
(24) Løpedag	2001.06.20	(85) Videreføringsdag	
(41) Alm. tilgj.	2002.12.23	(30) Prioritet	Ingen
(45) Meddelt dato	2003.03.10		

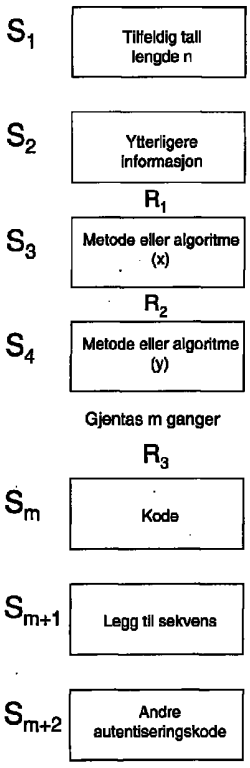
(71) Patenthaver Kezzler AS, Postboks 2311 Solli, 0201 Oslo, NO
(72) Oppfinner Magnar Løken d y, 0956 Oslo, NO
(74) Fullmektig Ingen

(54) Benevnelse **Fremgangsmåte for frembringelse og senere benyttelse av autentiseringsinformasjon**

(56) Anførte publikasjoner EP A2 278740, DE A1 3915262, DE A1 3631797, DE A1 4107266, CN 1266325, CN 1239256, US 6069955, US 4972475, US 4463250, EP B1 6498

(57) Sammendrag

Foreliggende oppfinnelse vedrører en fremgangsmåte for frembringelse av autentiseringsinformasjon for anvendelse i en eller flere påfølgende autentiseringsoperasjoner. Slike autentiseringsoperasjoner kan f eks være å identifisere personer, varer eller andre objekter og har i hovedsak til hensikt å avgjøre hvorvidt en vare, person eller annet objekt er autentisk i forhold til oppgitt bestemt informasjon. Autentiseringsinformasjonene som genereres med fremgangsmåten ifølge foreliggende oppfinnelse er bestående av minst en første autentiseringskode og minst en andre autentiseringskode. Den første koden kan tilfeldig velges eller på annet vis frembringes og den andre genereres på bakgrunn av den første autentiseringskode.



Foreliggende oppfinnelse vedrører en fremgangsmåte for frembringelse av autentiseringsinformasjon for anvendelse i en eller flere påfølgende autentiseringsoperasjoner. Slike autentiseringsoperasjoner kan f eks være å identifisere personer, varer eller andre objekter og har i hovedsak til hensikt å avgjøre hvorvidt en vare, person eller annet objekt er autentisk i forhold til oppgitt bestemt informasjon. Autentiseringsinformasjonene som genereres med fremgangsmåten ifølge foreliggende oppfinnelse er bestående av minst en første autentiseringskode og minst en andre autentiseringskode. Den første koden kan tilfeldig velges eller på annet vis frembringes og den andre genereres på bakgrunn av den første autentiseringskode.

I mange applikasjoner hvor autentisering foregår benyttes enkle koder eller kodepar i en identifiserings- eller bekreftelsesprosess. Dette kan eksemplevis være ved pålogging til bestemte sider på et datanettverk som internett eller lignende, eller ved anvendelse av f eks identitetskort, bankkort eller lignende. I slike tilfeller genereres enkle koder som er kjent for en bruker eller kodepar hvor begge kodene er kjent for en bruker og hvor et oppslag i en database med en kode fremskaffer den andre kode. Brukeren kan derved selv undersøke hvorvidt kodeparet er korrekt. I slike tilfeller genereres kodene i par som på forhånd er definert og lagret f eks i en database.

Objekter som kan autentiseres kan være nærmest alt tenkelig av varer og produkter med et "genuint" opphav som merkevarer i form av klær, klokker, smykker og andre forbrukerartikler. Videre kan legemidler og medisinsk utstyr kunne autentiseres. Deler til f eks fly og andre kritiske kjøretøyer eller kritiske komponenter i industri kan også være ønskelig å autentisere. I tillegg kan det være ønskelig å autentisere tjenester som er unike som f eks tegninger, dokumenter etc. Verdiobjekter som pass, verdipapirer etc kan også autentiseres med foreliggende oppfinnelse.

Kodepar genereres som oftest ved anvendelse av såkalte "generatorer for tilfeldige tall" som genererer en rekke tilfeldige tall. Disse tallene kan igjen uttrykkes på mange ulike måter slik at de utrykkes som koder av ønsket form med ønskede karakterer etc. Således kan ingen gjette eller resonere seg frem til relasjonen mellom kodene i et kodepar bestående av to eller flere koder.

Ulempen med slike lagrede kodepar oppstår særlig når antall kodepar f eks blir svært høyt eller antallet oppslag blir svært høyt i databasen. I slike tilfeller blir adkomsttiden ved tilgangen til kodeparene redusert. Videre blir databasen svært stor når et høyt antall kodepar er generert. Dette er kostbart i form av lagringsplass og prosessorkapasitet ved uthenting og øvrig håndtering.

Det finnes mange teknikker for autentisering av varer, og en retning innenfor dette tekniske området er merking av produkter med diverse tallsystemer eller serienummer, samt ulike krypteringsteknikker, hvor nøkler eller krypterte meldinger festes til varen som skal autentiseres, og at denne informasjonen benyttes i en påfølgende autentiseringsprosess.

Av kjent nærliggende teknikk som vedrører autentisering av varer, skal det spesielt nevnes patentskrift CN 1266325 som omhandler to autentiseringskoder hvor den andre koden beregnes med utgangspunkt i den første med en kjent algoritme. Ved autentisering oppgis den første koden, hvorved en algoritme beregner den andre koden, og som må sammenfalle med den andre koden for det kodeparet som ønskes kontrollert, for at kodene skal ansees være autentiske.

Av ytterligere kjent nærliggende teknikk skal det spesielt nevnes patentskrift CN 1239256 som omhandler en autentiseringskode som ved autentisering behandles av en algoritme, hvilken autentiseringskode etter dekoding må samsvare med en tidligere dekodet autentiseringskode lagret i en database, for at den autentiseringskoden som kontrolleres skal ansees være autentisk.

Det som spesielt oppnås i forhold til kjent teknikk med foreliggende oppfinnelse, er at kodene ikke trenger lagres i noen database, eller å benytte noen form for avansert kryptering, noe som gjør at lengden på kodene kan reduseres til en praktisk anvendbar lengde. Dette oppnås ved, som angitt i krav 1-6, at i det minste den andre koden inneholder henvisning(er) til de metoder og den informasjonen som ble benyttet i frembringelsen av autentiseringsinformasjonen, slik at kodene kan rekonstrueres kun med utgangspunkt i kodene selv, samt de metodene og informasjonen de henviser til. Videre oppnås det, som angitt i krav 7-8, at en vare eller produkt kan merkes med autentiseringsinformasjonen for etterfølgende autentisering.

Ytterligere en hensikt med foreliggende oppfinnelse er å betydelig redusere eller på det nærmeste eliminere behovet for database kapasitet samtidig som et høyt, og fortrinnsvis svært høyt antall kodepar kan håndteres.

Ytterligere en hensikt oppnås i hovedsak ved at kodeparene ikke lenger genereres på forhånd og deretter lagres, men at det genereres en første tilfeldig kode som ved hjelp av ytterligere informasjon og prosesser benyttes til å generere den andre koden i et kodepar. Den ytterligere informasjon som benyttes ved å generere den andre koden i kodeparet kan videre være tilveiebrakt som tilfeldig valgt, kjent informasjon og/eller kombinert med en eller flere tilfeldig valgte, kjente metoder eller algoritmer.

For å møte de ovenfor angitte hensikter er det ifølge foreliggende oppfinnelse frembrakt en fremgangsmåte for frembringelse av autentiseringsinformasjon for anvendelse i en eller flere påfølgende autentiseringsoperasjoner, hvilken autentiseringsinformasjon er bestående av minst en første autentiseringskode og minst en andre autentiseringskode. Fremgangsmåten er kjennetegnet ved at den andre autentiseringskode er frembrakt på bakgrunn av den første autentiseringskode med en eller flere på forhånd kjente metoder, hvor den første autentiseringskode opprinnelig er tilfeldig valgt eller tilfeldig frembrakt, og at den andre autentiseringskode uttrykker henvisning til de metoder og den informasjon som er benyttet i frembringelsen av den andre autentiseringskode.

I den foretrukne utførelsesform benytter den på forhånd kjente metode et eller flere tilfeldig valgte sett av kjent informasjon i kombinasjon med den første autentiseringskode for frembringelse av den andre autentiseringskode. Dette er foretrukket ettersom det er denne informasjonen og kombinasjonen av denne informasjonen sammen med den eller de metoder som benyttes som definerer sikkerhetsmarginen i forhold til muligheten for å kompromittere kodeparet.

Den tilfeldig valgte informasjon som benyttes under dannelsen av den andre autentiseringskode kan være et eller flere elementer fra en gruppe bestående av referanseverdier som dato eller lignende, referanse til tekst eller tallstrenger, referanse til koordinater eller annen grafisk informasjon, eller referanser til multidimensjonale matriser.

Videre knyttes autentiseringsinformasjonen til objektet som senere skal autentiseres. Autentiseringsinformasjonen overføres etter frembringelse til et egnet medium som papir, plast eller direkte på produktet eller varen dersom dette er hensiktmessig slik at kodene tilgjengeliggjøres. Hvordan selve mediet med kodene festes til varen er kjent teknikk og innenfor hva en fagmann på området vil kunne forventes å beherske.

Det er dog et viktig aspekt ved denne oppfinnelsen at koden i gitte tilfeller kan tilknyttes produktet på en slik måte at autentiseringsinformasjonen er skjult inntil en forsegling er brutt. Et slik tilfelle er bokser, plasker, beholdere og lignende hvor eksempelvis kodene festes på innsiden av lokket på en medisinpakke eller boks.

Et annet relevant eksempel er at kodene for autentisering av produkter som eksempelvis klær, hvor kodene vises på vaskemerkingen, er sydd eller vevd i selve tekstilet.

I en ytterligere utførelsesform vil det kunne være aktuelt å benytte "objekt spesifikk" informasjon som en del av den kjente informasjon som benyttes i frembringelsen av den andre autentiseringskode. Dette kan eksempelvis være

pakkedato, serienummer, produsent informasjon, produktinformasjon eller annen egnet informasjon som er helt eller delvis unik for produktet eller objektet. Slik objekt spesifikk informasjon kan ved generering av autentiseringskoder og/eller ved autentisering f eks måtte innhentes fra produktet og/eller produsenten av produktet eller objektet.

Hovedprinsippet i foreliggende fremgangsmåte er at den andre autentiseringskoden dannes med grunnlag av den første autentiseringskoden, ved at en rekke forskjellige metoder og algoritmer benyttes på en tilfeldig men rekonstruerbar måte. Hvor mange forsøk, metoder eller algoritmer som skal benyttes er et valg som gjøres i forhold til statistiske beregninger hvor formålet er å optimalisere mellom sikkerhet og den beregningskraft og kompleksitet som da trengs for å utføre fremgangsmåten. Et annet viktig aspekt ved oppfinnelsen er at prosessen, metodene og den informasjonen som benyttes ikke er kjent for andre enn den part som skal produsere autentiseringskodene. Således vil denne informasjonen være den eneste som nødvendigvis må lagres og sparepotensialet i oppfinnelsen ligger bl.a. i forskjellen i nødvendig lagringskapasitet på denne bakgrunn.

Den første eller andre koden inneholder referanseinformasjon eller også kalt sekvensrekke som benyttes ved rekonstruksjon slik at autentisering kan utføres.

Frembringelsen av et kodepar bestående av to eller flere autentiseringskoder kan skje på forhånd, før merking av et objekt, eller ved produksjon så kan merkingen genereres i virkelig tid mens produksjonen og merkingen foregår. F eks kan det opprettes en sikker forbindelse mellom en frembringer av autentiseringsinformasjon ifølge foreliggende oppfinnelse og en produsent. Den første autentiseringskode kan genereres hos produsenten av produktet eller objektet, eller hos den som generer autentiseringskoder. Videre kan f eks produkt- eller produsentspesifikk informasjon oversendes til den som genererer den andre autentiseringskode som "del-informasjon" ved frembringelse av den andre autentiseringskoden, ifølge foreliggende oppfinnelse. Den andre autentiseringskoden genereres og overbringes tilbake til produsenten som igjen merker produktet eller objektet med den første og andre autentiseringskode, eventuelt flere autentiseringskoder dersom det er ønskelig sammen med eventuell produktspesifikk informasjon.

I et eksempel på en utførelsesform av fremgangsmåten ifølge foreliggende oppfinnelse frembringes det først et tilfeldig tall eller kode av valgt lengde. Koden kan bestå av en hvilket som helst kombinasjon av alfanumeriske siffer og bokstaver eller tegn. Dette tallet skal senere danne grunnlaget for den andre autentiseringskoden. Deretter tilføres som tidligere forklart ytterligere informasjon eller data inn som skal benyttes i fremgangsmåten på et senere trinn. Denne type informasjon kan typisk være dato, klokkeslett og lignende.

Igjen genereres det et tilfeldig tall i en på forhånd valgt og definert tallrekke. Tallrekken går dermed fra 1 til n, hvor er en definert øvre eller nedre verdi. Eksempelvis fremkommer tallet 5. Tallet 5 vil ifølge fremgangsmåten nå bestemme hvilken metode eller algoritme som skal brukes videre under generering av den andre autentiseringskoden.

Den første koden og relevant informasjon "blandes" eller benyttes nå ved den utkomne valgte metode.

Så genereres igjen et eller flere tilfeldig tall hvor det metoden denne gangen kan være å trekke ut noen digitale filer. Innholdet i disse er helt irrelevant men de bør alle være svært forskjellige i natur og heller ikke for store med hensyn til ytelse og skalerbarhet. Digitale filer har et utall formater og det er hensiktmessig å benytte en optimal miks av disse, bildefiler, tegninger og lignende.

Når dette er gjentatt og utført ønsket antall ganger er den andre autentiseringskoden nesten ferdig fremskaffet. Den siste operasjon, som også kan velges å være tilfeldig er å tillegge og tilføre referanseinformasjonen som beskriver den faktisk utførte sekvensen.

Den tilfeldige men rekonstruerbare prosessen kan best illustreres ved å forklare en tenkt ferdig fremstilt autentiseringskode. I fremstillingen ble den tilfeldige sekvensen 3, 4 og 56. I dette eksemplet består prosessen av tre trinn.

Det første tilfeldige tallet var 34554 og det andre tallet før tilføring av sekvensinformasjonen var 676. For å kunne autentisere legges sekvensen inn i denne koden. Dette kan også gjøres på mange forskjellige måter. I et tenkt tilfelle kan sekvensen settes bak den andre koden. Dermed blir koden 6763456.

I selve autentiseringsprosessen vil en applikasjon eller et system av en eller annen utførelse trekke denne referanseinformasjonen ut, skille den fra resten av koden, og utføre sekvensen som ble benyttet for å fremskaffe kodene første gang. Ved autentiseringen er selvsagt ikke prosessen tilfeldig, den er derimot rekonstruert.

Rekkefølgen og kombinasjonen av metoder og algoritmer vil settes sammen i hvilken som helst kombinasjon og antall.

Det er videre en betydelig fordel ved foreliggende oppfinnelse at de autentiseringskoder som genereres og anbringes på et objekt som skal autentiseres vil kunne være synlige i "klartekst" for brukeren av autentiseringskodene.

Ved autentisering benyttes typisk internett eller annet telekommunikasjonsmedie mellom den som frembringer autentiseringsinformasjon og den som autentiserer et objekt.

Videre vedrører foreliggende oppfinnelse en fremgangsmåte for autentisering av produkt eller objekt merket med autentiseringsinformasjon fortrinnsvis, men ikke utelukkende frembrakt ifølge foreliggende oppfinnelse. Fremgangsmåten er kjennetegnet ved at minst den andre autentiseringskode overbringes til prosess som kan rekonstruere den kodeoppbygning som ligger til grunn for frembringelsen av den første kode, og som returnerer minst den første autentiseringskode. En prosess kan i dette tilfellet eksempelvis være en datamaskin som kan gjennomføre den nødvendige rekonstruksjon av den første autentiseringskoden. Overføringen kan skje må mange ulike vis men fortrinnsvis via telekommunikasjonsmidler som telefon, internett, annet datanett el.l.

Som en alternativ utførelsesform kan prosessen som returner den første autentiseringskode også tilføres produktspesifikk informasjon som kan bidra til autentisering av produktet eller objektet.

Foreliggende oppfinnelse er videre eksemplifisert og illustrert i den vedlagte figuren hvor:

figur 1 viser en sekvens for utarbeidelse av autentiseringsinformasjon ifølge en utførelsesform av foreliggende oppfinnelse;

Det er i figur 1 beskrevet en sekvens for utarbeidelse av autentiseringsinformasjon i form av et kodepar med utgangspunkt i en første autentiseringskode representert ved et tilfeldig tall av lengde n i sekvenstrinnet S_1. Dette kombineres med ytterligere kjent informasjon (sekvenstrinn S_2) i en kjent metode eller algoritme (sekvenstrinn S_3), hvor metoden eller algoritmen velges blant et antall på bakgrunn av et tilfeldig valgt tall R_1. Dette gjentas et ønsket antall ganger slik at en del av den andre autentiseringskode frembringes i sekvenstrinn S_m. Deretter kombineres denne "delkoden" med henvisning til den gjennomførte sekvens (sekvenstrinn S_{m+1}) slik at prosessen blir rekonstruerbar og dette uttrykkes i den andre autentiseringskode (sekvenstrinn (S_{m+2}).

Et eksempel på en frembringelse av autentiseringsinformasjon bestående av et kodepar ifølge foreliggende oppfinnelse vil nå bli beskrevet. Den første autentiseringskode er tilfeldig valgt som 3640 (sekvenstrinn S_1 i figur 1). Etter gjennomgang ifølge en første del av fremgangsmåten ifølge foreliggende oppfinnelse, som angitt med sekvenstrinn S_m i figur 1 fremkommer med den anvendte metoden tallet 5641. Sekvensen som er benyttet er metode 1 med informasjon 12 og 20. Denne informasjonen legges til (sekvenstrinn S_{m+1} i figur 1) og den andre autentiseringskode blir : 564111220 (sekvenstrinn S_{m+2} i figur 1).

Kodeparet blir som følger : Autentiseringskode 1 : 3640 og autentiseringskode 2 : 564111220.

Det er åpenbart at den første og andre kode ikke nødvendigvis skal ha samme lengde eller oppbygning. I tillegg kan kodene representeres på ulike vis og kan i tillegg kamufleres blant øvrig informasjon slik at kodene fremstår i en annen form.

PATENTKRAV

1. Fremgangsmåte for frembringelse av autentiseringsinformasjon for anvendelse i en eller flere påfølgende autentiseringsoperasjoner, hvilken autentiseringsinformasjon er bestående av minst en første autentiseringskode og minst en andre autentiseringskode, hvor den første autentiseringskode opprinnelig er tilfeldig valgt eller tilfeldig frembrakt,
k a r a k t e r i s e r t v e d at den andre autentiseringskode uttrykker henvisning(er) til de metoder og den informasjon som er benyttet i frembringelsen av den andre autentiseringskode, at den andre autentiseringskode er frembrakt på bakgrunn av den første autentiseringskode med de metoder og den informasjonen det er henvist til i den andre autentiseringskode.

2. Fremgangsmåte ifølge krav 1,
k a r a k t e r i s e r t v e d at de metoder og den informasjonen som er benyttet i frembringelsen av den andre koden består av et eller flere tilfeldig valgte sett av informasjon og metoder i kombinasjon med den første autentiseringskode for frembringelse av den andre autentiseringskode.

3. Fremgangsmåte ifølge krav 2,
k a r a k t e r i s e r t v e d at den tilfeldig valgte informasjon er valgt fra en gruppe bestående av bl.a.: referanseverdier som dato eller lignende, referanse til tekst eller tallstrenger, referanse til koordinater eller annen grafisk informasjon, eller referanser til multidimensjonale matriser.

4. Fremgangsmåte ifølge krav 1-3,
k a r a k t e r i s e r t v e d at autentiseringsinformasjonen tilknyttes et produkt eller vare slik at denne kan autentiseres.

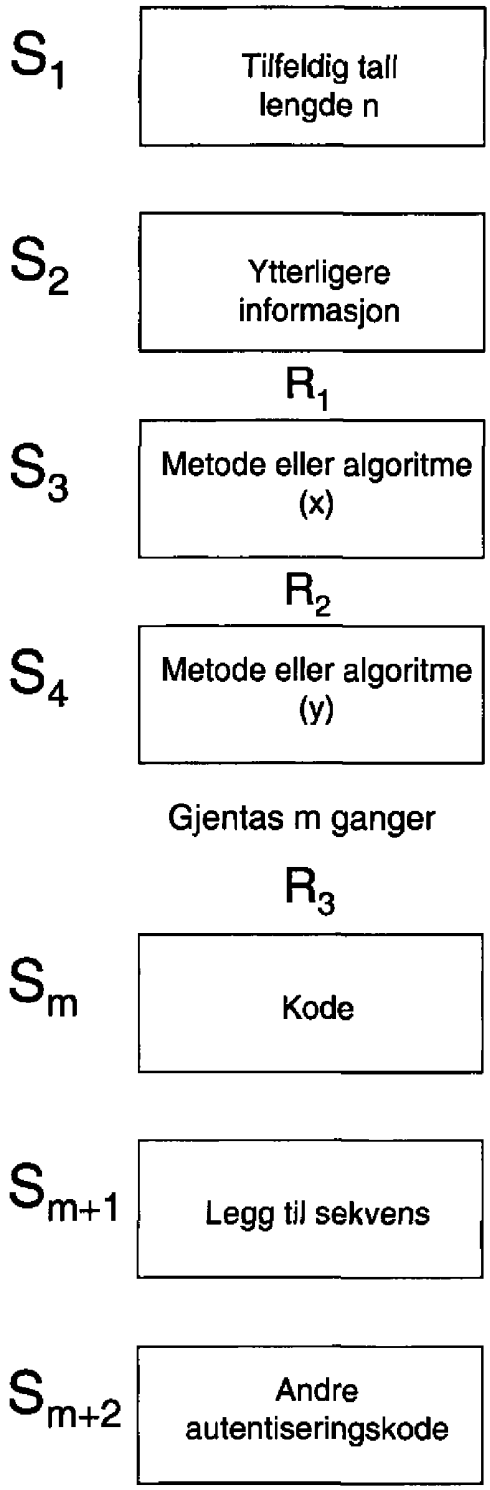
5. Fremgangsmåte ifølge krav 4,
k a r a k t e r i s e r t v e d at de metoder og den informasjonen som er benyttet i frembringelsen av kodene benytter et eller flere valgte sett av kjent produktspesifikk informasjon i kombinasjon med den første autentiseringskode for frembringelse av den andre autentiseringskode.

6. Fremgangsmåte ifølge krav 5,
k a r a k t e r i s e r t v e d at den produktspesifikke informasjon velges blant en gruppe bestående av: serienummer, produksjons eller pakkedato, produktbetegnelse, produsent betegnelse e.l.

7. Fremgangsmåte for autentisering av produkt eller objekt merket med autentiseringsinformasjon frembrakt ifølge fremgangsmåten ifølge krav 1-6,
k a r a k t e r i s e r t v e d at minst den andre autentiseringskode overbringes til prosess som kan rekonstruere den kodeoppbygning som ligger til grunn for frembringelsen av den første kode, og som returnerer i det minste den første autentiseringskode.

8. Fremgangsmåte ifølge krav 7,
k a r a k t e r i s e r t v e d prosessen som returner i det minste den første autentiseringskode også returnerer produktspesifikk informasjon som kan bidra til autentisering av produktet eller objektet

Figur 1


S1
Tilfeldig tall lengde n
S2
Ytterligere informasjon
R1
S3
Metode eller algoritme (x)
R2
S4
Metode eller algoritme (y)
Gjentas m ganger
R3
Sm
Kode
Sm+1
Legg til sekvens
Sm+2
Andre autentiseringskode