(12) **PATENT**

(19) NO (11) **326037** (13) **B1**

NORGE (51) Int Cl.
G06F 1/00 (2006.01)

Patentstyret

(21)	Søknadsnr	20033407	(86)	Int.inng.dag og søknadsnr	2002.08.12 PCT/GB02/03707
(22)	Inng.dag	2003.07.30	(85)	Videreføringsdag	2003.07.30
(24)	Løpedag	2002.08.12	(30)	Prioritet	2001.08.10, GB, 0119629
(41)	Alm.tilgj	2003.11.12			
(45)	Meddelt	2008.09.01			

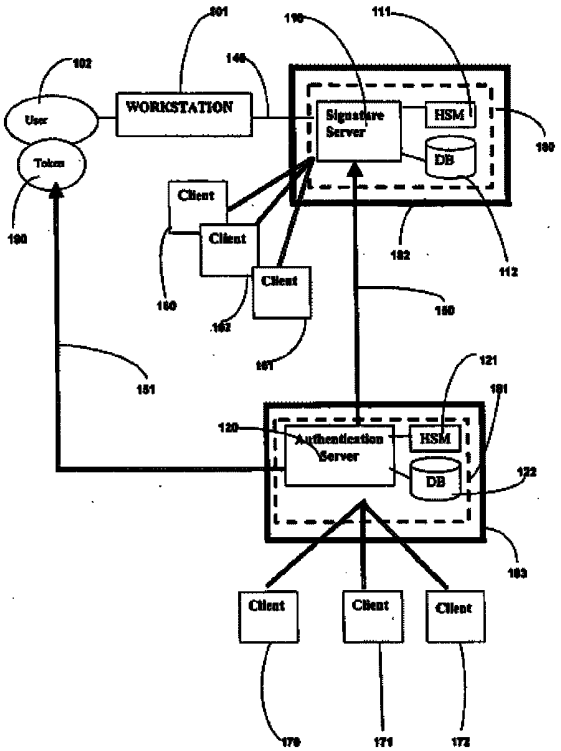
(73) Innehaver Cryptomathic A/S, Jægergaardsgade 118, 8000 ÅRHUS C, DK
(72) Oppfinner Peter Landrock, 52 Storey's Way, CB30DX CAMBRIDGE, CAMBRIDGESHIRE, GB
Jonathan Roshan Tuliani, 206 The Rowans, Milton, CB46ZL CAMBRIDGE, CAMBRIDGESHIRE, GB
(74) Fullmektig Zacco Norway AS, Postboks 2003 Vika, 0125 OSLO

(54) Benevnelse **Databekreftelsesmetode og apparat**

(56) Anførte publikasjoner D1 EP 1102157 A1

(57) Sammendrag

Et apparat og fremgangsmåte for å signere elektroniske data med en digital signatur i hvilket en sentral server omfatter en signaturserver (110) og en autentiseringsserver (120). Signaturserveren (110) sikkerhetslagrer de private kryptografiske nøkler av et antall brukere (102). Brukeren (102) kontakter den sentrale server ved bruk av en arbeidsstasjon (101) gjennom en sikker tunnel som er satt opp for dette formål. Brukeren (102) leverer et password eller annet symbol (190) basert på informasjon tidligere levert til brukeren ved autentiseringsserveren (120) gjennom en separat autentiseringskanal. Autentiseringsserveren forsyner signaturserveren med en utledet versjon av den sanne informasjon gjennom en permanent sikret tunnel mellom serverne, som blir sammenlignet med den som er levert av brukeren (102). Hvis de passer sammen, blir data mottatt fra brukeren (102) signert med brukerens private nøkkel.



Den foreliggende oppfinnelse angår bekreftelse av data sendt over et nettverk, mer spesielt over et usikkert nettverk så som internett, ved kryptografiske midler, som fremsatt i de vedlagte uavhengige krav 1, 10 og 33.

Når informasjon blir overført over et usikkert nettverk, er det mulighet for at det kan bli avbrudd og forstyrret på en eller annen måte. Derfor, mange aktiviteter som utføres ved bruk av et slikt nettverk for å forbinde partene involvert i aktiviteten, krever at hver part bekrefter identiteten av den andre part. Dette er spesielt tilfellet med aktiviteter utført over internett.

En måte å møte de ovenfor nevnte kravene er å bruke en digital signatur.
Opprinnelsen av data sendt over et usikkert nettverk kan bli godgjort ved bruk av en digital signatur.

En slik signatur oppfyller rollene av den tradisjonelle signatur: å frembringe autentisering av opprinnelsen, og kan også ha en legal betydning. Det er derfor viktig å sikre at det er vanskelig, om ikke umulig, å signere et elektronisk dokument falskt, for å foreslå et ukorrekt opprinnelsespunkt.

En generelt akseptert - og den eneste kjente - måte å oppnå dette på, er å bruke kryptografi. Spesielt, en form av asymmetrisk kryptografi kalt en offentlig nøkkelplan er brukt. En offentlig nøkkelplan benytter to forskjellige men matematisk relaterte "nøkler". Slike asymmetriske nøkler virker ved å bruke en såkalt "enveis" algoritme. En slik algoritme kan brukes til å produsere en såkalt digital signatur med en nøkkel og å verifisere denne med den andre nøkkelen, men det er meget tidkrevende og faktisk i praksis uoppnåelig, med det rette valg av nøkkelstørrelse, å bruke verifiseringsnøkkelen til å generere signaturen. For tiden er det en meget enkel sak å bruke verifiseringsnøkkelen til å verifisere signaturen og dermed integriteten av opprinnelsen av meldingen, og dette er hvordan hvert nøkkelpar blir normalt brukt. Disse offentlige nøkkelplanene kan enten være basert på en såkalt enveisfunksjon, hvor verifiseringsprosessen involverer sjekking av en matematisk ligning (f.eks. ElGamal, elliptisk kurve, osv. se Menezes, A., Oorschot, P.van, og Vanstone, S., Handbook of Applied Cryptography, CRC, 1996, hvis innhold er tatt inn her ved referanse), eller på krypterings/dekrypteringsfunksjoner (f.eks. RSA, se Rivest, R.L., Shamir, A. og Adleman, L, A method for Obtaining Digital Signatures of Public Key Cryptosystems, Communications of the ACM, 21 (2), 1978: 120-126, hvilket innhold er tatt inn her ved referanse). Det sistnevnte er forskjellig fra symmetrisk kryptering, hvor den samme nøkkel ble brukt til både kryptering og dekryptering av en melding. En av fordelene med en slik asymmetrisk metode, er at selv om en tredje part er i besittelse av nøkkelen som er brukt til å verifisere meldingen, kan det ikke produsere signaturen uten den andre nøkkelen. Hvis en kryptering/dekrypteringsplan er

brukt, er krypteringsnøkkelen verifiseringsnøkkelen, og dekrypteringsnøkkelen er signeringsnøkkelen.

Den mest brukt offentlige plan, RSA, gjør bruk av to meget store hovedtall, det faktum at, på den tiden det skrives, tar det meget lang tid å fakturere produktet av disse to hovedtallene tilbake til de to opprinnelige tall. Ved tilstrekkelig store tall, kan RSA derfor være meget bestandig mot signaturforfalskning. Generelt, en av nøklene er produktet n av de to hovedfaktorene pa og q og en såkalt offentlig eksponent e, og den andre er et tall utledet fra paret av hovedtall og e som bruker modulær aritmetikk. Den offentlige eksponent e må være valgt som en gjensidig begynnelse til p-1 og q-1, og en hemmelig eksponent d kan så være utledet f.eks. som det minste positive hele tall som tilfredsstiller ed-x(p-1)(q-1)=1 for en x som bruker Euclids algoritmer gjentatt. Videre informasjon av dette kan bli funnet i Menezes m.fl., som nevnt ovenfor.

Fordi kunnskap om nøkkelen brukt for verifisering ikke muliggjør signering, er det mulig å kringkaste denne nøkkel (den såkalte "offentlige nøkkel") så bredt som mulig, til så mange som mulig, typisk ved å frembringe den såkalte Public Key Infrastructure (PKI, se CCITT. (Consultative Comm. on Intern. Telegraphy and Telephony), Recommendation X.509: The Directory---Authentication Framework, 1994 og Public Key Infrastructure: The PKIX Reference Implementation, Internet Task Engineering Force, som begge er tatt inn her ved referanse), slik at hvem som helst kan gjøre bruk av dem.

Hvis en spesiell offentlig nøkkel kan brukes til å verifisere en melding, viser dette at opphavsmannen til meldingen må ha vært brukeren som holder den private nøkkel. Det er derfor mulig å indikere opprinnelsen av en spesiell melding ved å gjøre bruk av offentlig nøkkelplaner.

Dette krever imidlertid at det er en plan på plass for å binde identiteten av brukeren til et spesielt offentlig nøkkelpar.

F.eks., holderen kunne ganske enkelt annonsere for verden at han eier det offentlige/private nøkkelpar. Mottakeren av det signerte dokument vil imidlertid da bare ha holderens ord for hans identitet og at holderen er eieren, og at nøkkelen ikke har vært kompromittert. I dette tilfellet, kan ikke mottakere av meldingen verifisere at senderen av meldingen sier sannheten om identiteten eller eierskapsstatusen, bare at meldingen har kommet fra noen som krever en spesiell identitet og krever å være eieren av nøkkelparet.

På grunn av de ovennevnte problemer med verifisering av identitet og status for en PKI nøkkeleier, har det oppstått tredje parter kalt sertifiseringsautoriteter (CA) for å sertifisere at

en spesiell bruker er den han sier han er. Brukeren må vise visse kreditiver til CA og hans offentlige nøkkel, og CA vil i retur utstede et såkalt sertifikat, som bare er en signatur generert av CA på en melding i et valgt format, så som en X.509v3, bestående av brukerens kreditiver og hans offentlige nøkkel. I tillegg, må CA gjøre tilgjengelig en veiledning, fra hvilken status av hvilken som helst brukernøkkel kan bli kommunisert til hvilken som helst annen bruker på hvilket som helst tidspunkt, enten ved bruk av såkalte revokasjonslister, eller ved undersøkelser på linjen. Videre, CA utsteder en sertifikatpolitikkmelding, som sier at reglene for brukere av systemet, omfattende den fremgangsmåte ved hvilken brukerne har vært identifisert. For detaljer, se CCITT, og Public Key Infrastructure: The PKIX Reference Implementation, nevnt ovenfor.

Et digitalt sertifikat, omfattende en offentlig nøkkel/privat nøkkelpar har ytterligere fordeler over en tradisjonell signaturløsning uten sertifikater, idet den kan ha en begrenset operasjonsperiode og kan også bli suspendert eller oppsagt, om den private nøkkel av brukeren blir kompromittert, f.eks. ved å bli gjort tilgjengelig til en tredje part. For at signaturen skal være av noen nytte, må den fortrinnsvis være representert i et standardisert format, så som Public Key Crypto Standard (PKCS#1) signaturer, formatert i henhold til CMS (the Cryptographic Message Syntax) (PKCS#7), for videre informasjon om hvilket PKCS#1, 7, RSA Cryptography Standard, RSA Laboratories, 2001, innhold av hvilket er tatt inn her ved referanse).

Som man kan se fra det ovenstående, er det meget viktig at den private signaturnøkkel blir holdt hemmelig til alle tider, ellers er dens verdi fjernet, siden verdien ligger i det faktum at den bekrefter identiteten av forfatteren av en melding ved å vise at meldingen oppstod fra eieren av et spesielt nøkkelpar. Dette er bare tilfellet hvor den private nøkkel ikke er kompromittert. Derfor må skritt tas for å opprettholde sikkerheten av den private nøkkel.

En etablert tilnærming til beskyttelsen av den private nøkkel av et nøkkelpar som brukes for digitale signaturer er å bruke programvareløsninger og så å lagre den på eierens arbeidsstasjon eller en floppydisk beskyttet av en pinkode eller passfrase styrt av eieren. Det er imidlertid en generell oppfatning av en slik løsning med bare programvare ikke er tilstrekkelig sikker for høyverditransaksjoner, hvis ikke arbeidsstasjonen er ekstraordinært vel beskyttet. Dette er fordi det vil typisk være mulig å få den private nøkkel ved bruk av en utvidet søkning for passordet på arbeidsstasjonen, og i alle tilfelle, er det vanskelig å beskytte den private nøkkel fra den såkalte "Trojanske hest" angrep. Her blir et ondsinnet program, en type virus, installert av en innbryter, f.eks. via en e-mail som inneholder en eksekuterbar fil, og dette programmet kopierer hemmelig den private nøkkel av brukeren når den blir brukt i en signaturprosess, eller den kopierer hemmelig passfrasen som brukes til å beskytte den private nøkkel. Det kan innføres midler som gjør slike angrep mer vanskelig, men selv da er de

fremdeles ikke lette å hindre. For sikkerhet og anvendbarhets grunner er den fysiske beskyttelse som tilbys av smartkort, som i tillegg gir en mobil løsning, attraktive. Ulempen med denne metoden er at det krever smartkortlesere, som fremdeles ikke er bredt tilgjengelig.

Et alternativ, som lenge var ansett meget attraktivt, er isteden å lagre den private nøkkel på et smartkort (chipkort). Men dette krever at arbeidsstasjonen som brukes for denne applikasjonen må ha en smartkortleser tilkoplet. Siden arbeidsstasjoner meget sjelden har en slik leser innbygd som standard, og siden det ikke er noen enkelt dominerende standard for kommunisering med chipkortet, er den eneste mulighet å tilkople en ekstern enhet og installere en driver på arbeidsstasjonen, som er både tidskrevende og kostbar.

Identifikasjon og sikkerhet er hovedsaker for løsninger som tillater brukeren å generere en digital signatur. Det er derfor et mål for denne oppfinnelsen å fjerne eller redusere i det minste et av problemene forbundet med tidligere teknikk. Spesielt, et mål er å nå et høyt sikkerhetsnivå, som samtidig gir en fleksibel løsning av problemet.

I tillegg, private nøkler lagret på en arbeidsstasjon kan oppstå "i klar tekst", dvs. i ikke-kryptert form, i brukerens datamaskinoppbevaringssted eller printeroppbevaringssted eller spoler, eller ellers på en internettserviceprovider (ISP) oppbevaring, selv om de er slettet fra brukerens datamaskin. Selv slettede enheter kan faktisk bli fjernet fra en datamaskin ved bruk av spesialiserte teknikker for å gjenvinne data fra harddiskdrivere osv. Hvor den private nøkkel blir brukt for å generere signatur, må den faktisk frembringes i ubeskyttet form.

Andre løsninger på sikkerhetsproblemet tillater brukeren å nedlaste sine private nøkler fra en sentral server og å generere signaturen på arbeidsstasjonen i programvaren. Dette gir mobilitet, men er fremdeles sårbart for angrep hvis arbeidsstasjonen er usikret, hvilket er typisk hvis det ikke er restriksjoner på hvilke arbeidsstasjoner kan brukes til å nedlaste den private nøkkel.

EP 1 102 157 A1 beskriver en fremgangsmåte for å sikre innlogging i et kommunikasjonssystem som inkluderer en mobil enhet, et mobilt kommunikasjonsnettverk, et autentiseringssenter, en applikasjonsserver, en datamaskin og et ikke-sikret nettverk, hvor brukeren setter opp en applikasjonssesjon via en datakommunikasjon fra sin personlige datamaskin til en applikasjonsserver og sender en identitet. Deretter vil serveren forespørre autentisering fra et autentiseringssenter. Når så autentiseringssenteret sender et enkelt merke (token) til serveren som sender dette merket til brukeren over dataforbindelsen. Til slutt vil brukeren lese merket på skjermen i sin personlige datamaskin og sender merket som en tekstmelding fra den mobile enheten til autentiseringssenteret, som også finner mobiltelefonnummeret og celleidentifikasjonen til brukeren.

I en utførelse av den foreliggende oppfinnelse, er brukerens private nøkkel lagret sentralt på et sikringsapparat bestående av en eller flere servere, ikke nødvendigvis alle på det samme fysiske sted. Serverne er finklebestandige, og benytter typisk en maskinvare sikkerhetsmodul (HFM) så som en IBM 4758 med et begrenset kommandosett tilgjengelig. En av disse serverne, kalt signaturserveren, inneholder de private nøkler for forskjellige brukere, initiert på en slik måte at bare den rette eier kan initiere signaturgenerering med sin egen private nøkkel.

Ifølge oppfinnelsen er det frembrakt en fremgangsmåte for å sikre data levert av en bruker ved å generere en digital signatur eller lignende på disse data ved hans kontroll ved hjelp av hans private nøkkel, hvor fremgangsmåten omfatter mottakelse av data som skal bekreftes ved et apparat fra en kildeanordning, bekrefting av data ved bekreftelsesapparatet med et eller flere elementer av informasjon sikret til bekreftingsapparatet, hvor elementene er unike for brukeren, og utsending av dataene som bekreftet fra bekreftingsapparatet, for å passeres til en mottakeranordning, hvor elementene for sikker informasjon bekrefter at leverandøren av dataene er brukeren.

Den ovenstående fremgangsmåte gir fordeler med reduserte kostnader av administrasjon av bekreftelsesapparatet, lettere bruk for brukeren, og øket sikkerhet, siden informasjon som er unik for brukeren aldri forlater signaturserveren av bekreftelsesapparatet, enten i kodet form eller ikke. Dette tillater brukeren å bruke flere arbeidsstasjoner uten å bære deres private nøkkel til hver arbeidsstasjon. Derfor, kan bare et brudd på signaturserveren resultere i at private nøkler blir gjort tilgjengelige utenfor signaturserveren, hvilket følgelig måtte bli hindret ved bruk av finklebestandige maskinvare designet for dette formål, så som IBM 4758.

I mer avanserte scenarier, kunne den private nøkkel bli fordelt mellom hvilket som helst antall N av servere som bruker hva som er kjent som "hemmelig deling" i en slik måte at hver har en komponent av nøkkelen ved hvilken de kan beregne en inngang for generering av signaturen, hvilken blir levert tilbake til kildeanordningen, hvor den fulle digitale signatur så blir beregnet fra K innganger hvor K er et tall mellom 2 og N. Fordelen med dette er at minst K servere måtte bli kompromittert før en angriper kunne beregne den private nøkkel.

Det bekreftende apparat kan omfatte hvilket som helst som er sentralt basert, og tilgjengelig fra en eller flere kildeanordninger. Fortrinnsvis omfatter det bekreftende apparat en signaturserver. Fortrinnsvis, omfatter det bekreftende apparat også en autentiseringsserver. Fortrinnsvis er det bekreftende apparat tilgjengelig fra mange kildeanordninger.

Kildeanordningen kan typisk være en arbeidsstasjon, men kan også være en interaktiv televisjon, eller en automatisk tellemaskin for å levere kontanter eller annen informasjon fra et

sentralt bekreftende apparat. Kildeanordningen vil ha all programvare som er nødvendig for å kommunisere effektivt med det bekreftende apparat, men dette kunne bli levert eller nedlastet til kildeanordningen for den nødvendige varighet av interaksjon. Kildeanordningen tillater kommunikasjon med det bekreftende apparat.

Det unike element eller elementer omfatter fortrinnsvis den private nøkkel av en offentlig nøkkel/privat nøkkelpar som er spesifikt for brukeren. Det unike element eller elementer kan generere en digital signatur spesifikk for brukeren, på data levert av brukeren. En slik PKI nøkkel og digital signatur gir høy sikkerhet for grunner som er gitt ovenfor, idet de er meget vanskelige å dekode falskt.

Mottakeranordningen kan være den samme som kildeanordningen, eller alternativt, den kan være en tredjeparts anordning. Sistnevnte tillater at hele meldinger eller bare en utledet del, (fortrinnsvis en hashverdi) av en melding som skal bekreftes for å bli overført til den ønskede part uten nødvendigvis å returnere den bekreftede melding til kildeanordningen etter bekreftelse.

Tredjepartanordningen kan være en passende anordning for å motta de bekreftede data, andre enn kildeanordningen, så som en separat arbeidsstasjon, eller et nettverk av datamaskiner. F.eks., den tredje part kunne være en portvei for et lokalområdenettverk (LAN). Alternativt, kunne det bekreftende apparat og en tredjepartanordning være innenfor en enkelt LAN, eller omfatte et vidt område nettverk (WAN).

I et videre aspekt ved oppfinnelsen, er det frembrakt en fremgangsmåte for å bekrefte elektroniske data levert av en bruker som er original fra den brukeren, hvor fremgangsmåten omfatter å etablere en sikker forbindelse mellom en kildeanordning og et bekreftende apparat, sending av dataene fra kildeanordningen som skal mottas av det bekreftende apparat, og mottaking av en versjon av dataene fra det bekreftende apparat bekreftet som å ha oppstått fra brukeren som bruker informasjon unikt til brukeren ved kryptografiske teknikker.

Det trinn med å inkludere den bekreftede versjon av dataene til ytterligere data som skal sendes til en tredje part anordning er fortrinnsvis inkludert.

Fortrinnsvis holder det bekreftende apparat informasjon som er unik for brukeren til å utføre bekreftelsen.

Den unike informasjon er fortrinnsvis det private nøkkel av en offentlig nøkkel/privatnøkkel par som er spesifikk for brukeren. Fortrinnsvis er også den unike informasjon en digital signatur som er spesifikk for brukeren. Fortrinnsvis er dataene som skal bekreftes en

spredningsverdi av en melding. Dette gir den fordel at hele meldingen ikke trenger å bli sendt til signaturserveren for å bli signert, og reduserer således nettverktrafikken mellom kildeanordningen og signaturserveren.

Kildeanordningen og det bekreftende apparat etablerer fortrinnsvis en autentisert forbindelse mellom dem før og under overføring av dataene som skal bekreftes. I tillegg, kan forbindelsen være kodet. Dette resulterer muligheten for at forbindelsen vil bli avbrutt eller forstyrret.

Kildeanordningen kan levere en eller flere symboler til det bekreftende apparat for autentisering. Fortrinnsvis blir ett av symbolene levert til brukeren eller kildeanordningen ved det bekreftende apparat via en alternativ kanal til den autentiserte forbindelsen. Dette øker også sikkerheten betydelig, ved å kreve at to kanaler blir innfanget for å få aksess til dataene.

Den alternative kanal kunne være en mobil telefonnettverkkanal. Det er spesielt foretrukket å bruke kortmeldingsservicemeldinger for å overføre symbolet.

Symbolet kan være et fast passord i den enkleste løsning. I en foretrukket løsning, er symbolet et engangs passord, som har vært kommunisert gjennom en autentisert kanal så som en mobil telefon, eller er beregnet dynamisk ved hjelp av et fysisk symbol som deler en nøkkel med det bekreftende apparat. Slike løsninger er generelt tilgjengelige på markedet, og eksempler er gitt nedenfor.

Symbolet er fortrinnsvis unikt for hver transaksjon, hvor en transaksjon er en prosess av signering av data, levert av kildeanordningen, ved den bekreftende anordning og å levere de signerte data til en mottakeranordning. Symbolet kan være lagret på en transportabel anordning.

Fortrinnsvis, kan mer enn en type symbol autentisere bruker- eller kildeanordningen. F.eks., et fast passord kan være brukt i tillegg til et engangspassord generert ved et fysisk symbol eller sendt til brukerens mobiltelefon. Uavhengigheten av disse symbolene gjør det meget vanskelig for en angriper å kompromittere begge samtidig. Slike planer sies således å gi sterk autentisering av brukeren, og kan benyttes til å oppnå et høyere nivå av sikkerhet enn det som oppnås ved bruk av enkelt autoriseringssymbol alene.

Et ytterligere foretrukket trekk er at fremgangsmåten virker med et nivå av sikkerhet nådd ved autentisering av brukeren uansett kildeanordningen, og et annet, høyere nivå av sikkerhet nådd ved autentisering av brukeren og kildeanordningen. Fortrinnsvis, vil det bekreftende apparat bekrefte dataene med forskjellige unike elementer, avhengig av typen av symbol som er brukt til å autentisere brukeren eller kildeanordningen for sikkerhet så vel som data. Slike

flere nivåer av autentisering tillater forskjellige nivåer av sikkerhet, og pålitelighet, for å bli plassert på forbindelser som benytter forskjellige typer av symbol, og forskjellige nivåer av signatur som skal brukes avhengig av symbolet som brukes.

Hvor mer enn en type symbol er brukt, kanskje samtidig, for å autentisere brukeren, kan det være ønskelig å sikre at administrasjonen av disse symbolene blir håndtert ved separate uavhengige grupper av administratorer. For dette formål, er det mulig å konfigurere det bekreftende apparat som en gruppe av mer enn en separat server, og å ha hver server styre et eller flere uavhengige autentiseringssymboler.

Et eksempel på dette er det tilfellet hvor brukerens private nøkkel blir fordelt ved bruk av hemmelig delingsplan mellom flere servere. Et alternativ er for brukerens nøkkel å bo i en enkelt server, kjent som signaturserveren, og for dette å operere i samband med en eller flere andre servere forbundet med brukerens autentisering, kjent som autentiseringsservere.

Brukeren kan etablere separate forbindelser til hver server. Det er også mulig for brukeren å autentisere seg selv ved bruk av symboler styrt ved separate servere uten å måtte etablere separate forbindelser for hver server. Et eksempel på en slik plan er gitt i beskrivelsen av en utførelse av oppfinnelsen nedenfor.

Valideringsdata for validering av brukeren og/eller dataene som skal bekreftes må fortrinnsvis være mottatt av det bekreftende apparat før dataene kan bli bekreftet.

Fortrinnsvis, sender det bekreftende apparat et ønske til en fjern innretning for å forsyne brukeren med identifiseringsdata. Videre, kan det bekreftende apparat motta en versjon av identifiseringsdataene (f.eks. et engangspassord) for fjernanordningen, og denne versjonen kan sammenlignes med ytterligere brukerdata levert av brukeren (f.eks. en utledet versjon av engangspassordet). Hvis sammenligningen er vellykket, er således dataene som skal bekreftes bekreftet som å oppstå fra brukeren.

En forbindelse kan bli etablert mellom arbeidsstasjonen for brukeren og den fjerne anordning. Denne forbindelsen kan bli verifisert og autentisert uavhengig av forbindelsen mellom arbeidsstasjonen og den bekreftende anordning/signaturserver.

Ifølge et ytterligere aspekt ved oppfinnelsen, er det frembrakt en fremgangsmåte for bruk i bekreftelse av data omfattende mottakning av et ønske fra en fjernanordning om å forsyne en bruker med identifiseringsdata, levering av de nevnte identifiseringsdata til en bruker, og forsyning av en utledet versjon av identifiseringsdata for den fjerne anordning. Denne fremgangsmåten gir en ytterligere kanal for å sende identifikasjonsdata så som et

engangspassord til brukeren. Metoden for å overføre identifiseringsdata kan være forskjellig fra metoden som brukes for å overføre ønsket fra en fjern anordning, og fremgangsmåten for å sende den utledede versjon av identifiseringsdata.

Ifølge et ytterligere aspekt ved oppfinnelsen, er et datamaskinapparat frembrakt ifølge kravene 43 til 45. Ifølge ytterligere aspekter ved oppfinnelsen, er et bærermedium frembrakt ifølge kravene 44 eller 46.

Ifølge et ytterligere aspekt ved den foreliggende oppfinnelse, er det frembrakt et databekreftelsesapparat, omfattende en signeringsanordning tilpasset til å bekrefte data mottatt fra en fjern kildeanordning som opprinnelig fra en bruker, hvor det bekreftende apparat er anordnet til å motta data fra kildeanordningen, bekrefte dataene som å tilhøre brukeren, ved bruk av informasjon lagret i det bekreftende apparat, hvor den nevnte informasjon er unik for brukeren, og å sende de bekreftede data til en mottakeranordning.

Mottakeranordningen er fortrinnsvis kildeanordningen. Alternativt, kan mottakeranordningen være en tredjepartsanordning.

Kildeanordningen og det bekreftende apparat er fortrinnsvis anordnet til å etablere en autentisert forbindelse mellom dem før og under overføring av data som skal bekreftes. Et ytterligere foretrukket trekk er at forbindelsen er kodet.

Kildeanordningen kan være anordnet til å levere et symbol til det bekreftende apparat for autentisering. Dette symbolet er fortrinnsvis levert til brukeren eller kilden ved autentiseringsanordningen via en alternativ kanal til den autentiserte forbindelsen. Symbolet kan være et fast passord. Alternativt, kan passordet være et engangspassord. Igjen kan symbolet være unikt til transaksjonen.

Fortrinnsvis, i apparatet ifølge den foreliggende oppfinnelse kan mer enn en type symbol autentisere brukeren og kildeanordningen.

Som et ytterligere foretrukket trekk, kan databekreftelsesapparatet være anordnet til å operere ved et nivå av sikkerhet nådd ved en autentisering av brukeren uansett kildeanordningen, og et annet, høyere sikkerhetsnivå nådd ved autentisering av brukeren og kildeanordningen, hvis en spesiell kildeanordning, f.eks. en pålitelig arbeidsstasjon er brukt. I tillegg, kan det bekreftende apparat være anordnet til å bekrefte dataene med forskjellige unike elementer, avhengig av typen av symbol som brukes til å autentisere brukeren eller kildeanordningen for sikkerhet, så vel som dataene.

Det bekreftende apparat kan også omfatte instruksjonsanordning for å sende et ønske til en fjern anordning for å instruere den fjerne anordning til å sende identifikasjonsdata, (f.eks. et engangspassord) til brukeren. Det bekreftende apparat kan også omfatte mottakeranordning for å motta data utledet fra identifiseringsdataene fra den fjerne anordning.

De utledede data fra den fjerne anordning kan sammenlignes med en sammenligningsanordning for ytterligere data mottatt fra mottakeranordningen, og bekreftende anordning som bekrefter dataene som skal bekreftes hvis dataene sammenlignet ved sammenligningsanordningen passer sammen.

Ifølge et videre aspekt ved oppfinnelsen, er det frembrakt et apparat for bruk til databekreftelse, omfattende mottakeranordning for å motta et ønske fra en fjern anordning om å forsyne en bruker med identifiseringsdata leveringsanordning for å levere identifikasjonsdata til en bruker, og videre en leveringsanordning for å levere en utledet versjon av identifiseringsdataene til den fjerne anordning.

En passordgenereringsanordning er fortrinnsvis også frembrakt, som genererer et passord, f.eks. et engangspassord, skjønt andre identifikasjonsdata også kan genereres. Mottakeranordningen og videre leveringsanordningen er fortrinnsvis anordnet til å operere via en annen kommunikasjonsmetode enn leveringsanordningen.

De utførelser og aspekter ved oppfinnelsen som er beskrevet ovenfor skal ikke bare bli tolket individuelt eller bare i kombinasjon, men kan bli kombinert på hvilken som helst måte for å frembringe ytterligere utførelser av oppfinnelsen. I tillegg, kan individuelle trekk fra en utførelse bli kombinert med andre trekk fra en annen utførelse slik at forskjellige kombinasjoner av individuelle trekk fra forskjellige utførelser og aspekter også gir ytterligere utførelser av oppfinnelsen.

Spesifikke utførelser av den foreliggende oppfinnelse skal nå beskrives, bare gjennom eksempler, med henvisning til tegningene, hvor: Figur 1 viser arkitekturen av forbindelser mellom forskjellige komponenter i henhold til en første utførelse av den foreliggende oppfinnelse; figur 2 viser trinnene som er involvert i å gi en bruker eksklusiv tilgang til signaturnøkkel i henhold til den første utførelse av oppfinnelsen; figur 3 viser et flytdiagram av en metode ifølge en første utførelse av oppfinnelsen; figur 4 viser et flytdiagram av en fremgangsmåte ifølge en ytterligere utførelse av oppfinnelsen; og figur 5 viser et flytdiagram ifølge en ytterligere utførelse av den foreliggende oppfinnelse.

Figur 1 viser skjematisk et system ifølge en utførelse av den foreliggende oppfinnelse. Det viser en bruker 102 som opererer en kildeanordning, som i den foreliggende utførelse er en

arbeidsstasjon 101, som er forbundet med en bekreftende anordning, som i den foreliggende utførelse er en signaturserver 110, via en kommunikasjonslinje 140. Kommunikasjonslinjen 140 er ikke i seg selv sikker. Arbeidsstasjonen 101 kan være hvilken som helst terminal ved hvilken kommunikasjon kan bli etablert med signaturserveren 110. F.eks., kan arbeidsstasjonen 101 være et interaktivt televisjonsapparat. Kravet er at arbeidsstasjonen 101 kan kommunisere med signaturserveren 110. Ingen spesiell programvare er nødvendig ved arbeidsstasjonens 101 side av forbindelsen. Signaturserveren 110 lagrer sikkert den private nøkkel for hver bruker og kan i tillegg logge noe eller all relevant informasjon angående brukerne og deres aktiviteter. Signaturserveren 110 håndterer ønsker fra brukere via arbeidsstasjonen 101 og kan utstede ønsket til en CA server. Signaturserveren 110 er ideelt sertifisert til en internasjonal standard, så som FIPS 140-1, nivå 3 eller 4 (se FIPS publikasjon 140-1, 1994, National Institute of Standards & Technology, USA, innholdet av hvilken er tatt inn her ved referanse), som er en generell akseptert standard for å indikere kvaliteten av de fingerbestandige trekkene ved maskinvarebeskyttelsen av serveren.

Signaturserveren 110 mottar data, som skal verifiseres som opprinnelig fra brukeren, fra arbeidsstasjonen 101. Verifiseringen er oppnådd ved bruk av privatnøkkelen for brukeren, som er lagret på signaturserveren 110, for å kryptere data mottatt fra arbeidsstasjonen 101, og å returnere data til en mottaker, som kan være brukeren eller en tredje part. Prosesser ifølge utførelsen av den foreliggende oppfinnelse vil bli beskrevet i mer detalj med henvisning til figurene 3, 4 og 5 nedenfor.

Detaljene av maskinvaren som brukes i utførelsen av oppfinnelsen skal nå beskrives. I tillegg til signaturserveren 110, i utførelsen av den foreliggende utførelse har det bekreftende apparat også en separat autentiseringsserver 120, som er forbedret ved fingerbestandig maskinvare på samme måte som signaturserveren 110. Alternativt, kan autentiseringsserveren 120 være fjernt fra signaturserveren 110. Signaturserveren 110 er forbundet med autentiseringsserveren 120 via et sterkt kryptografisk ledd 150 (f.eks. kryptert og autentisert) f.eks. ved en delt masternøkkel, eller basert på en offentlig nøkkelkoding-dekoding, bruk av standardløsninger, og noen ganger kjent som en VPN (virtuelt privat nettverk). Dette brukes til å etablere en sesjonsnøkkel og sikre en kodet kanal mellom servere som bruker standard kryptografiske teknikker som er vel kjent i teknikken. Nøkkelen som brukes kan avhenge av brukerpassordet brukt for aksess. Den sikre tunnel 150 fra autentiseringsserver 120 til signaturserver 110 fortsetter inn i maskinvaredelen av signaturserveren 110, i den forstand at nøkler som brukes for denne tunnelen blir styrt ved fingerbestandig maskinvare og aldri oppstår klart utenfor det bekreftende apparat. Integriteten av systemet trenger da ikke å avhenge så meget av det sikre området som serveren er plassert i. Det samme gjelder for all kommunikasjon til og fra både signaturserveren 110 og autentiseringsserveren 120.

Autentiseringsserveren 120 fordeler engangspassord og/eller utfordringer til kunder gjennom en alternativ kanal 151. I den foreliggende utførelse, benytter den alternative kanal 151 SMS (kortmeldingsservice) meldinger sendt via et cellenettverk for mobile telefoner for å kommunisere engangspassordene. Alternativt, kan brukeren benytte en håndholdt såkalt sikkert symbol 190, en liten innretning som deler en individuell nøkkel med autentiseringsserveren 120. Så snart utfordringen er mottatt via arbeidsstasjonen 101, blir denne nøklet inn ved brukeren på symbolet 190, og responsen som fundamentalt er en kodning av utfordringen med nøkkel holdt på symbolet 190, blir nøklet inn i arbeidsstasjonen 101 som engangspassordet. Signaturserveren 110 kan verifisere at responsen er faktisk en kodning av fordringen når den mottar en utledet versjon av engangspassordet fra autentiseringsserveren 120. Imidlertid, mange alternativer er tilgjengelige, så som Wireless Application Protocol (WAP) over et cellenettverk (som er en spesialisert versjon av internett, og som kan aksesseres av WAP styrte mobiltelefoner), eller ordinær papirpost. Alternativt, kan passord bli fordelt via internett, via en applet, som kommuniserer så direkte som mulig med en printer tilkoplet arbeidsstasjonen 101 (siden dette begrenser risikoen for at kopier av passordet forblir i printer/spoler buffere, eller arbeidsstasjonen 101 ved hjelp av Trojanske hester som "lukter" passordene). Eksempler på typer av passord som kan brukes i den foreliggende oppfinnelse er diskutert nedenfor. I alle tilfeller, er ikke den eksakte natur av denne autentiseringsprosessen begrenset til det som er beskrevet, og mange variasjoner er mulige innenfor oppfinnelsens kontekst.

Ved registrering, blir et fast passord sendt på en sikker måte til brukeren 102 - som på hvilket som helst tidspunkt kan endre - slik at hver bruker 102 kan bli autentisert i forbindelse med en arbeidsstasjon 101 og signaturserver 110 som en del av brukerautentiseringsprosessen. I den foreliggende utførelse, i tillegg til en på linje, engangspassord blir distribuert via SMS melding fra autentiseringsserveren 120 til brukerens mobiltelefon (ikke vist). Et slikt på linje engangspassord kan ha en meget kort gyldighetsperiode, som sammen med autentiseringen antydet ved det faktum at serveren kjenner hvordan man lokaliserer kunden, gir høy sikkerhet til passordet. Mobiltelefonnummeret for brukeren bestemmer unikt brukeren, slik at den mobile telefon må være stjålet, lånt eller klonet for at identifiseringen skal feile, hvis ikke SMS meldingen blir oppfanget av noen som samtidig kan gjøre bruk av informasjonen, hvilket er forholdsvis vanskelig siden autentiseringskanalen er uavhengig av kommunikasjonskanalen.

Denne utførelsen tillater brukeren 102 å gjøre bruk av den digitale signatur, som sikrer at den digitale signatur selv aldri forlater det sikre sentrale bekreftende apparat, enten den er kodet eller ikke.

Fordelingen av passordsymboler ifølge en utførelse av den foreliggende oppfinnelse skal nå beskrives ved bruk av de elementer som er vist på figur 1. Først, kontakter brukeren 102 signaturserveren 110 fra arbeidsstasjonen 101 via kanal 152. Signaturserveren 110, via den sikre link 150 etablert mellom signaturserveren 110 og autentiseringsserveren 120, instruerer så autentiseringsserveren 120 til å sende ut et engangspassord til brukeren 102. Autentiseringsserveren 120 gjør dette ved bruk av SMS meldinger, som beskrevet ovenfor, på kanal 151. Autentiseringsserveren 120 utstyrer også signaturserveren 110 med en utledet versjon av engangspassordet, via kanalen 150. Denne utledede versjon er, i denne utførelsen, en nøkkelverdi av engangspassordet. Nøkkelverdien er utledet ved bruk av en standard enveis algoritme, så som SHA-1 (se Secure Hash Standard; FIPS Pub 180-1, 1995, National Institute of Standards & Technology, USA, innholdet av hvilken er tatt inn her ved referanse). En nøkkelverdi er typisk meget mindre enn den melding fra hvilket den er utledet, og så snart nøkkelverdien er beregnet, kan ikke den opprinnelige meldingen bli funnet fra den. Det er også meget usannsynlig at to meldinger vil ha den samme nøkkelverdi. Nøkkelverdien av engangspassordet blir så sammenlignet med den nøkkelverdien levert av arbeidsstasjonen 101. Siden den samme standardalgoritmen er brukt både ved autentiseringsserveren 120 og arbeidsstasjonen 101, hvis de to passer sammen, blir brukeren akseptert som å være autentisert ved signaturserveren 110. Alternativt, en annen type utledet versjon av passordet kan bli sendt til signaturserveren 110. Det kravet at bare den prosessen blir brukt til å utlede versjonen av passordet eller symbolrespons er den samme i autentiseringsserveren 120 og arbeidsstasjonen 101, slik at et passord vil bli gitt den samme utledede versjon som autentiseringsserveren 120 og arbeidsstasjonen 101, men to forskjellige passord vil ikke gi det samme resultat.

Sammenligning av nøkkelverdier tillater brukeren å bli verifisert mens signaturserveren 110 aldri mottar det aktuell engangspassord.

En variasjon av fordelingen av passordsymboler beskrevet ovenfor skal nå beskrives. Brukeren etablerer uavhengige forbindelser til både signaturserveren 110 og autentiseringsserveren 120, i stedet for bare til signaturserveren 110. I dette tilfellet blir dataene som skal bekreftes sendt til autentiseringsserveren 120 gjennom et grensesnitt og en nøkkelverdi av dataene til signaturserveren 110 gjennom et annet grensesnitt. Alternativt, kunne nøkkelverdien bli erstattet med, eller tillagt, andre relaterte data. Typisk blir dataene som skal bekreftes generert ved kildeanordningen på basis av tredjepart applikasjoner (f.eks. en bank) gjennom f.eks. en applet eller appleter, som så viderefører dataene og en spredning på dataene til autentiseringsserveren 120 og signaturserveren 110. Hver forbindelse kan bli autentisert ved bruk av et separat symbol, f.eks. et fast passord for signaturserverforbindelsen og et engangspassord for autentiseringsserverforbindelsen. Autentiseringsserveren 120 viderefører dataene som skal bekreftes til signaturserveren 110, som kan beregne en spredning

av dataene og sammenligne denne med den spredningen som er mottatt direkte fra brukeren 102. Denne planen frembringer også en sterk sikring ved signaturserveren 110 at brukeren 102 er blitt autentisert ved autentiseringsserveren 120, men har den fordelen at ingen informasjon angående autentiseringsserveren brukerautentisering er mottatt eller tilgjengelig til signaturserveren 110.

Signaturserveren 110 er understøttet av en fiklebestandig maskinvare sikkerhetsmodul (HSM) som har et beskyttet kryptografisk system så som IBM 4758, hvor nøklene og signaturene blir generert, og hvis nøklene ikke er bruk, blir de lagret eksternt, kryptert under en masternøkkel. Som vist på figur 2, i en utførelse av oppfinnelsen, blir første data frembrakt av arbeidsstasjonen 110 til det bekreftende apparat, overført til HSM 111 via en kanal 141 satt opp ved bruk av passordet for brukeren 120 og standard krypteringsteknikker. Et annet lag av koding 140 strekker seg fra arbeidsstasjonen til det bekreftende apparat, men strekker seg ikke inn i HSM 111. Dette er en sterk kodet link med autentisering av serveren, og kanalen bærer ytterligere informasjon angående detaljer av brukeren 102 og spesifiserer autentiseringsmetoden som skal brukes for den alternative kanal 151. Hovedpoenget er at ingen følsom nøkkel noensinne oppstår åpent utenfor sikkerhetsboksen. Slike løsninger er meget brukt av f.eks. bankmiljøet, f.eks. i forbindelse med pinkodebeskyttelse. Databasen 112 registrerer all informasjon angående administratorer. HSM 111 håndterer lagring av nøkler og kryptografisk funksjonalitet. Signaturserveren 110 er beskyttet både av en brannvegg 180 og ved fysisk sikkerhet 182 for å hindre, redusere eller motvirke uautorisert aksess.

I en utførelse av oppfinnelsen, er signaturserver 110 understøttet av klienter 160, 161, 162 operert av pålitelig personell f.eks. under dobbelt kontroll, forbundet ved en autentisert og kryptert link til signaturserveren 110. Under en sesjon mellom signaturserveren 110 og klient, vil administratoren først logge på, og på dette trinn sesjonere nøkler til å autentisere og kryptere all kommunikasjon mellom klient 160, 161, 162 og signaturserveren 110 er enig i bruk av masternøkkel, igjen ved bruk av standardprosedyrer for å sette opp en VPN mellom klient 160, 161, 162 og serveren. De nødvendige transportnøkler (masternøkler for utveksling av sesjonsnøkler) er lagret på smartkort, er operert ved administratorer og er brukt til å administrere (dvs. skape/klargjøre/avslutte) sikkerhetsoffiser og kontorist konti for signaturserver 110, for å lese inn data i signaturserverens 110 database og å registrere kunder (de som har signatur på serveren) på signaturserveren 110.

I høy sikkerhetstransaksjoner, tilbyr en utførelse av oppfinnelsen videre forbedring, for å stoppe angrep startet gjennom den grafiske brukers grensesnitt for å oppnå hva som er kjent som WYSIWYS (What You See Is What You Sign): En enkelt mulighet er å la det bekreftende apparat bekrefte essensielle deler av data levert av brukeren for bekreftelse via

den andre kanal brukt for autentiseringsformål før bekreftelse er utført. I dette tilfellet, må hele meldingen som skal bekreftes bli sendt over til det bekreftende apparat for inspeksjon.

Sikkerhetsoffiserer og kontorfolk er to nivåer av administrator av signaturserveren 110: sikkerhetsoffiseren er ansvarlig for alle sikkerhetsrelaterte aspekter av operering av signaturserveren 110, deriblant tilsetning av nye administratorer, eksportering av revisjonslogg, og suspendering eller avslutting av administratorkonti. Kontorpersonen er ansvarlig for brukerrelaterte aktiviteter så som registrering av nye kunder med systemet, suspendering, avslutning av kunder, uttrekning av rapporter om kundens aktiviteter og lignende. De to nivåer gir øket sikkerhet til systemet ved å begrense aksess til noen systemer mer enn andre.

Med to nivåer av signaturserver 110 som administratorer er gitt, er det mulig å dividere autoriserte aktiviteter mellom hvilket som helst antall av forskjellige strukturer som nødvendig. F.eks., er det mulig å tillate kunden å utføre enkle administrative oppgaver så som utsteding av nye passord, å be om rapporter om deres aktivitet eller å suspendere hans egen konto hvis det er mistanke om falsk bruk. Imidlertid, i den foreliggende utførelse kan konti bare bli gjenopprettet av en kontorperson, og vil resultere i at et nytt passord blir sendt fra autentiseringsserveren 120 til kunden via brukerens mobiltelefon.

Autentiseringsserveren 120 er også forbedret ved en maskinvaresikkerhetsmodul 121, og har en database 122, på samme måte som signaturserveren 110, og beskyttet ved en brannvegg 181 og fysisk sikkerhet 183. Autentiseringsserveren 120 er også forbundet med klienter 170, 171, 172 som bruker autentiserte krypterte kanaler som beskrevet ovenfor i forhold til signaturserveren 110 klientledd. For sikkerhet, er disse klientene 170, 171, 172 separat fra klienter 160, 161, 162 som administrerer signaturserveren 110.

Signaturserveren 110 og autentiseringsserveren 120 er fortrinnsvis huset geografisk atskilt, og blir hver operert av et uavhengig legeme med atskilte klienter 160, 161, 162 og 170, 171, 172 som administrerer hver. Dette reduserer muligheten for at det vil være uautorisert aksess til begge serverne, hvilket vil være nødvendig hvis private nøkler av brukeren skulle være misbrukt.

Alternativt, kan autentiseringsserveren 120 og signaturserveren 110 være huset i det samme bekreftende apparat. I et slikt tilfelle skulle administrasjonsklienter 160, 161, 162, og 170, 171, 172 for hver server (f.eks. grensesnittet gjennom hvilket serveren blir operert) fortrinnsvis forbli separate, slik at øket sikkerhet er frembrakt, ved å sikre at aksess til begge serverne ikke kan oppnås gjennom samme klient, skjønt det kunne være det samme. Fordelen med denne enkeltservertilnærming er at denne tilnærmingen er enklere, siden bare en server

blir operert istedenfor to, men ulempen er at større forsiktighet er nødvendig for å sikre at pålitelig personell ikke kan blokkere systemet på noen måte.

Så vel som det på linje engangspassord gitt hittil i den foreliggende utførelse, kan et antall andre typer av passord og leveringsmetoder bli benyttet i tillegg til SMS meldinger som fordeler på linje engangspassord. Autentisering kan oppnås ved hjelp av symboler 190, f.eks. passord, engangspassord, lagrede hemmeligheter osv. De forskjellige typer av symboler har forskjellige egenskaper angående deres mobilitet og sikkerhet. For alle typer passord blir en nøkkel generert for å autentisere ønsket ved signaturserveren 110. Signaturserveren 110 vil generere nøkkelen på lignende måte og verifiserer ønsket.

Faste passord er passord som ikke endrer seg, og kan brukes mange ganger, ved forskjellige anledninger, til å autentisere en bruker. Slike faste passord er mobile, men mindre sikre enn engangspassord fordi de er lette å overhøre, enten ved fysisk å observere kunden når passordet blir endret, eller ved å lure kunden til å entre passordet i en falsk passordpåminnelse. Det er ikke mulig å bestemme hvorvidt et fast passord er kompromittert eller ikke, men i tilfellet av mistanke om kompromittering (f.eks. basert på revisjonsprøver), kan passordet bli avsluttet.

Faste passord må opprinnelig være frembrakt av autentiseringsserveren 120, til brukeren, via en sikker kanal (f.eks. i en forseglet konvolutt) fordi fra begynnelsen har ikke brukeren noen måte for å autentisere seg selv på nettverket. Etter det første passord er mottatt, kan brukeren endre passordet på linjen hvis tilstrekkelig autentisering og konfidensialitet er frembrakt.

Faste passord kan bli kategorisert ved hvor utsatt de er for å bli kompromittert, slik at man kan ha et passord for kontrollerte eller sikre miljøer og et annet for mindre kontrollerte eller sikre miljøer.

Alternativt, lagrede engangspassord kan benyttes, som er mobile og sikrere enn faste passord, men kan bli kompromittert ved fysisk tyveri eller ved kopiering. Tyveri er lett detektert når passordet er lagret på print eller i en mobil innretning. Kopiering er imidlertid ikke detekterbar.

Lagrede engangspassord har lang gyldighetsperiode, og må sendes sikkert fra autentiseringsserveren 120 til brukeren. Kopiering av engangspassord må hindres, og dette kan være meget vanskelig å gjøre hvis passordet blir sendt på linje over internett fordi de kan ligge i forskjellige filer, printer, buffere osv. i lang tid etter at brukeren tror at de er slettet. Kryptografisk sikret kommunikasjon reduserer problemet med å oppnå passord under transmisjon til brukeren, men garanterer ikke noe om klar tekst kopier lagret på arbeidsstasjonen.

På linje engangspassordene ifølge den foreliggende utførelse er sikrere enn lagrede engangspassord på grunn av den korte gyldighetsperiode som gjør tyveri og senere bruk virtuelt umulig. Oppfanging av den alternative kanal er imidlertid fremdeles mulig, skjønt det er høyst usannsynlig at begge kanaler kan angripes av samme angriper på samme tid, hvilket er en styrke av tilnærmingen.

Et ytterligere alternativ er et terminalfingeravtrykk, som kan brukes til å identifisere en spesiell brukers arbeidsstasjon 101. Det er en verdi som unikt identifiserer arbeidsstasjonen 101. Et slikt fingeravtrykk kan beregnes basert på hemmeligheter lagret i arbeidsstasjonen 101, hvor maskinvare konfigurasjonen av arbeidsstasjonen 101 og alle serienumre av maskinvareinnretninger i arbeidsstasjonen 101. Imidlertid, siden et fingeravtrykk kan forfalskes ved å kopiere all denne informasjon, er fingeravtrykk bare relevante for terminaler i styrte miljøer, dvs. de som har fysisk og programvarebeskyttelse. Terminalfingeravtrykk er ikke egnede symboler i en situasjon hvor kunden bruker mange forskjellige terminaler, men heller for den situasjon hvor pålitelig informasjon er nødvendig for en enkelt terminal. Stjeling av et fingeravtrykk krever innbrudd eller hackerangrep, men kan ikke anses detekterbart.

Det ville forbedre sikkerheten hvis det er en sikker pålitelig arbeidsstasjon 101 tilgjengelig til brukeren med en sikker tunnelforbindelse til signaturserveren 110 så vel som autentiseringsserveren 120, idet dette ville gjøre det mulig for brukeren f.eks. å endre sitt memoriserte passord på en sikker måte på hvilket som helst tidspunkt fra denne spesielle arbeidsstasjon.

I et ytterligere alternativ, et høyt nivå av sikkerhet oppstår når sesjoner med signaturserveren 110 er kjedet. Dette betyr at serveren returnerer et symbol 190, som er lagret på arbeidsstasjonen 101 og returnert til serveren ved begynnelsen av neste sesjon. Symbolet 190 returner kan være eller ikke være fordelt og holdt sikkert, men vil alltid tillate kunden å detektere misbruk av signatur, siden den neste sesjon vil peile autentisering fordi symbolet ville ha vært returnert til en falsk bruker, istedenfor en legitim en. Denne løsningen krever forsiktig synkronisering mellom kunde og server for å sikre at symboler ikke blir tapt i tilfellet forbindelser feiler. Det er mange kjente og vel forståtte metoder for å håndtere dette.

Videre, sikrere symbol 190 er et kryptografisk tillegg for en datamaskin, som tillater komplett identifisering av en arbeidsstasjon 101 ved bruk av en utfordringsresponsprotokoll. Skjønt slike tillegg kan være fysisk små og fleksible, er de ikke egnet til bruk med flere arbeidsstasjoner 101 siden deres komplette identifikasjon for en enkelt arbeidsstasjon 101 er nødvendig. Et eksempel på disse ville være en liten enhet ("dongel") forbundet med en

serieport av arbeidsstasjonen 101, så som anordninger tilgjengelig på markedet for programvare og informasjonsbeskyttelse.

Håndholdte innretninger så som passordgeneratorer og smartkortfrontende tillater meget pålitelig identifikasjon ved vedkommende anordning, selv om anordningen kan være stjålet, som hvilken som helst annen anordning. Sammenlignet med terminal engangspassord via SMS til en annen telefon, er fordelen med håndholdte kryptografiske innretninger at SMS meldinger kan bli avlyttet eller innfanget, mens den kryptografiske innretning ikke kan bli det.

Det sikreste middel for identifisering kan være bruk av en fysisk egenskap av brukeren, så som en retina eller fingeravtrykksskann. For tiden, er imidlertid slike skannere ikke lett tilgjengelige på noen arbeidsstasjon 101 gjennom hvilke sesjoner kan ønskes utført.

Når kommunikasjon med mobilenheter blir mer avansert, vil det bli mulig å tilpasse flere og flere avanserte autentiseringskanaler, og disse ville likeledes bli brukt, så lenge de fyller kravene for brukerautorisering og/eller autentisering.

Det er klart at forskjellige planer diskutert ovenfor vil ha forskjellige nivåer av sikkerhet. Det laveste nivå (nivå 1) er hvor brukeren bare memoriserer et passord som han deler med signaturserveren, som han inkluderer hver gang en signatur må genereres.

Mer avansert er den løsning (nivå 2) hvor i tillegg han inkluderer en engangspassord som han har mottatt tidligere via en uavhengig autorisert kanal fra autentiseringsserveren, f.eks. en SMS melding, en papirbasert liste ved ordinær post, eller kommunisert til en sikker arbeidsstasjon gjennom en kryptert tunnel og så printet ut. Ved hver ny transaksjon, blir et nytt passord brukt i tillegg til et unikt passord memorisert av brukeren.

Enda mer avansert og fleksibel (nivå 3) er den situasjon hvor brukeren er i besittelse av et håndholdt symbol, så som et VASCO Digipass, eller RSA SecureID Key Fob, som deler f.eks. konvensjonell nøkkel med signaturserveren. Når brukeren logger på, vil han enten motta en såkalt utfordring fra den bekreftende anordning som han taster inn på symbolet. Symbolet beholder så utfordringen og returnerer en såkalt respons på displayet, som blir tastet inn på arbeidsstasjonen av brukeren som et engangspassord, og verifisert til å være korrekt ved bekreftelsesanordningen. Andre symboler, generelt tilgjengelige på markedet, vil automatisk beregne en ny respons ved regulære intervaller ved bruk av en nøkkel delt med bekreftelsesanordningen, som kan variere uten bruk av en utfordring, siden utfordringen er implisitt til systemet.

For nivå 3, hvilken som helst tilstrekkelig sikker personlig identifikasjonsplan basert på symboler tilgjengelige på markedet kan i prinsippet bli inkludert i oppfinnelsen for å skape den nødvendige autentisering av brukeren. Dette symbolet kan også være en mobil anordning, som kan kommunisere sikkert med bekreftelsesanordningen f.eks. ved bruk av en WAP-sikkerhet for mottak av engangspassord fra autentiseringsserveren, eller hvilken kommunikasjonssikkerhet er tilgjengelig for denne anordningen, så som en Bluetooth eller infrarød båret kommunikasjon til en terminal forbundet med autentiseringsserveren gjennom et fysisk nettverk. Igjen, det fysiske nettverk trenger ikke å være sikkert, siden kommunikasjonen blir sikret ved hjelp av en sikker tunnel mellom autentiseringsserveren og den mobile innretning.

Et ytterligere nivå av sikkerhet, f.eks. for en fast permanent pålitelig arbeidsstasjon 101 kan bli nådd hvis en maskinvare kryptografisk innretning brukes til å frembringe komplett identifisering av arbeidsstasjonen 101. For dette nivå kunne arbeidsstasjonen 101 bli bundet til en IP-adresse eller et telefonnummer.

Det er klart, at mange nivåer av aksess og sikkerhet kan bli introdusert som nødvendig med forskjellige egenskaper og krav. Fordeler med de ovennevnte utførelser at signaturserveren 110 blir brukt på en slik måte at den private nøkkel for en bruker aldri blir sendt utenfor den sikre signaturserver 110, enten den er kryptert eller ikke. Dette betyr at den vesentlig økede sikkerhet er tilgjengelig og beskytter brukerens private nøkler.

Fordi det er mulig å operere med forskjellige pålitelighetsnivåer, avhengig av autentiseringssymbolet 190 eller symboler levert til signaturserveren 110, kan dårlig identifiserte sesjoner (dvs. de som er autentisert i henhold til nivå 2) bli brukt for bare signaturer for transaksjoner med små potensielle tap som en følge av et falskneri (f.eks. små banktransaksjoner) mens en sikrere sesjon (dvs. de som er autentisert i henhold til nivåene 3 eller 4) så som brukerens hjemme PC, kan brukes for transaksjoner med større potensielle tap som følge av falskneri, tillater utførelsen av den foreliggende oppfinnelse kombinasjonen av bruk av et sikkert fast terminalsystem sammen med mobilitet gitt ved å være i stand til å bruke arbeidsstasjonene 101. Derfor er fordelene for hver gitt.

Når en kunde ønsker å bli registrert ved signaturserveren 110, vil han eller hun kontakte en kontorperson, som tar vare på registreringen. Hvis kunden ønsker å bli registrert med sertifikat, fins det to valg, avhengig av hvorvidt CA og signaturserveren 110 blir operert av den samme organisasjon eller ikke.

1. Hvis begge serverne blir operert av samme organisasjon, kan klienten bli registrert ved CA og signaturserveren 110 samtidig, og et nøkkelpar og sertifikat kan bli generert umiddelbart.

2. Hvis serveren blir operert ved forskjellige organisasjoner, trenger kunden først å bli registrert ved CA og kanskje motta en senders nøkkel ID og en IAK (Initial Authentication Key) og kunden kan bare bli registrert ved signaturserveren 110. Hvis kunden er villig til å bekjentgjøre sender ID og IAK til kontorpersonen, kan nøkkelparet bli generert umiddelbart som i tilfellet 1, ellers må nøkkelgenereringen bli startet via internett.

Registreringsprosedyren kan oppnås ved bruk av vel kjente og forståtte metoder, så som den internasjonale standard PKIX, og ville typisk være ansvarlig for den valgte CA. Sertifikater ville bare være nødvendige når det bekreftende apparat mottar data som skal bekreftes fra flere kildeanordninger. Hvis kildeanordningen er kjent, ville ingen ekstern CA være nødvendig.

Figur 3 viser et flytdiagram av de trinn som er involvert når den melding er signert med brukerens private nøkkel holdt i signaturserveren 110.

Ved S300 er meldingen entret inn i en arbeidsstasjon 101. Meldingen kan bli entret manuelt ved arbeidsstasjonen 101. Alternativt, kan meldingen bli skrevet på et tidligere trinn og lagret på annet sted før den blir lastet inn i arbeidsstasjonen 101. Når meldingen er klar til å bli sendt, i denne utførelsen blir arbeidsstasjonen 101 forbundet med internett. Imidlertid, direkte (punkt til punkt) forbindelse mellom arbeidsstasjonen og signaturserver 110 kan alternativt bli brukt. Internett blir brukt til å kontakte signaturserveren 110 over en sikret kanal. Ved dette trinn, ville ikke signaturserveren 110 og arbeidsstasjonen 101 vite hvem de er forbundet med. For å bestemme dette, er verifisering av kommunikasjoner nødvendig ved S302. Verifisering av signaturserveren 110 kan oppnås ved bruk av en offentlig nøkkel / privat nøkkel par. Signaturserverens 110 offentlige nøkkel er publisert og tilgjengelig til arbeidsstasjonen 101, f.eks. fra en CA. Forskjellige metoder for å etablere identiteten av serveren som da er tilgjengelig i det hele tatt involverer bruken av serverens private nøkkel til å kryptere eller dekryptere en melding. Siden den private nøkkel av signaturserveren 110 er kjent bare for signaturserveren 110, er arbeidsstasjonen 101 i stand til å identifisere meldinger som kommer fra signaturserveren 110. Også, ved bruk av signaturserverens 110 private nøkkel /offentlige nøkkel par, er det mulig å sette opp en sikker tunnel fra arbeidsstasjonen 101 til signaturserveren 110 ved at arbeidsstasjonen 110 krypterer med serverens offentlige nøkkel og bare serveren er i stand til å dekryptere med den private nøkkel. En bred variasjon av autentisering og krypteringsprosesser, som er vel kjent i teknikken, kan benyttes i oppfinnelsen. I den foreliggende utførelse, blir brukeren identifisert ved bruk av et fast passord som blir gjenkjent av signaturserveren under autentiseringsprosessen.

Imidlertid, ved dette trinn, har ikke signaturserveren 110 autentisert arbeidsstasjonen 101 som brukt av en spesiell bruker av bekreftelsessystemet. Signaturserveren 110 trenger å motta en hemmelighet fra arbeidsstasjonen 101, som bare er kjent av brukeren, for å utføre autentiseringen. Dette blir gjort ved at signaturserveren 110 ber om at autentiseringsserveren 120 sender en på linje engangspassord til brukeren over en separat kanal til linken mellom signaturserveren 110 og arbeidsstasjonen 110 ved S304. I denne utførelsen, er dette gjort ved en SMS melding. Brukeren entrer senere inn i arbeidsstasjonen 101 ved S308, så snart den er mottatt. Fordi forbindelsen fra arbeidsstasjonen 101 til signaturserveren 110 er sikker i retning fra arbeidsstasjonen 101 til signaturserveren 110, vil avlytting ikke identifisere det passord som blir entret og sendt til signaturserveren 110. I tillegg, som nevnt ovenfor, vil arbeidsstasjonen 101 utlede en spredningsverdi fra passordet, istedenfor å sende passordet over forbindelsen ved S310. Autentiseringsserveren 120 sender sin egen versjon av det utledede resultat til signaturserveren 110 ved S312, og signaturserveren 110 sammenligner begge verdier. Hvis de er de samme, er det meget usannsynlig at et ukorrekt passord var entret, og passordet blir verifisert ved S314.

Så snart passordet er verifisert, blir en toveis sikker kanal etablert ved S316. Denne kan settes opp ved bruk av hemmeligheten (dvs. passordet) som blir sendt til signaturserveren 110 med signaturserverens 110 offentlige nøkkel for å generere en sesjonsnøkkel. Denne sikre kanal er basert på de vanlige prinsipper av en VPN.

Alternativt, kan en av de andre former av passord eller symbol 109 som diskutert ovenfor bli brukt til å autentisere brukeren avhengig av hvorvidt brukeren er en sikker arbeidsstasjonen 101 eller en ikke sikker arbeidsstasjon 101.

Som nevnt, er ikke oppfinnelsen begrenset til noen spesifikk algoritme og metode for å sette opp sikkerhetskanalen. Kravet er simpelthen at en sikker kanal blir etablert. I tilfellet av den foreliggende utførelse, er den sikre kanal toretnings. Imidlertid, dette trenger ikke å være tilfellet i sin alminnelighet.

Så snart den sikre toretningskanal er etablert, beregner arbeidsstasjonen 101 en spredningsverdi av den melding som brukeren ønsker bekreftet ved S318. Denne spredningsverdi blir sendt over den sikre kanal, til signaturserveren 110. Så snart signaturserveren 110 mottar spredningsverdien, henter den ut den private nøkkel for brukeren fra HSM og koder spredningsverdien med brukerens private nøkkel ved S320 (det er klart at brukerens private nøkkel kan hentes ut når som helst etter at brukerens identitet er etablert).

Den signerte spredning blir så returnert til arbeidsstasjonen 101. Spredningen har nå blitt kryptert ved bruk av den private nøkkel av brukeren, og er bekreftet som opprinnelig fra

denne brukeren. Dette er oppnådd uten at den private nøkkel har forlatt et fysisk og programvarebeskyttet miljø av signaturserveren 110. Denne utførelsen av oppfinnelsen overvinner derfor sikkerhetsulempene ved å sikre at den private nøkkel aldri er tilgjengelig utenfor signaturserveren 110. Denne økning i sikkerhet av den private nøkkel resulterer i en øket verdi av sertifikatet, siden meldingen mer sannsynlig er autentisk.

Den signerte spredningsverdi blir så lagt inn i den fulle opprinnelige melding ved S322 og kan så bli sendt over en usikret kanal, så som internett, til en mottaker S324. Meldingen blir bekreftet som å være fra eieren av den digitale signatur.

I tillegg, på grunn av i en utførelse av oppfinnelsen, er signaturserveren 110 og autentiseringsserveren 120 begge brukt, og er fortrinnsvis separert geografisk, og fordi alle tre av arbeidsstasjonen 101, signaturserveren 110 og autentiseringsserveren 120 må være involvert i bekreftingen av dataene fra arbeidsstasjonen 110, må både signaturserveren og autentiseringsserveren være kompromittert for å forfalske en bekreftelse. Sannsynligheten for dette er redusert ved atskillelse av serverne, og ved uavhengig administrering av hver server.

En usikret kanal kan brukes til å distribuere den signerte melding, siden den signerte spredningsverdi virker både til å identifisere og autentisere meldingens innhold. Ved S326 på figur 3, sjekker mottakeren med den bekreftelsesautoritet som er brukt til å utstede brukerens offentlige nøkkel / privat nøkkel par, og mottar brukerens offentlige nøkkel. Denne blir brukt til å dekryptere spredningsverdien av meldingen og å bekrefte at opphavsmannen for meldingen er brukeren. I tillegg, kan mottakeren beregne spredningsverdien av selve meldingen og sjekke at denne spredningsverdi passer sammen med den krypterte spredningsverdi. Hvis dette ikke er tilfellet, har meldingen vært fingret med og kan kasseres.

Hvis meldingen er sendt over en usikret kanal, skjønt det ikke vil være mulig å fingre med meldingen uten deteksjon, er det fremdeles mulig å oppfange og lese meldingen før den blir mottatt av mottakeren. For å unngå dette, kan en sikret kanal mellom brukeren og mottakeren bli etablert ved bruk av en fremgangsmåte som beskrevet ovenfor, eller hvilken som helst annen egnet metode. Den sikrede kanal trenger bare å være fra brukeren til mottakerne. Mottakerne trenger ikke å etablere en sikret kanal for informasjon som går tilbake til brukeren, hvis ikke følsom eller hemmelig informasjon skal returneres til brukeren fra mottakeren.

Alternativt, for å unngå problemet av tredje parter oppfanger og leser meldingen mellom bruker og mottaker, kan en fremgangsmåte som vist på figur 4 benyttes.

Denne fremgangsmåten er lik den som er vist på figur 3. Ved S400 blir meldingen entret i arbeidsstasjonen 101. S402 til S406 er beskrevet ovenfor med henvisning til figur 3, for å etablere en sikret kanal mellom arbeidsstasjonen 101 og signaturserveren 110. Imidlertid, en enveis sikret kanal trenger å bli etablert fordi, i denne utførelsen, trinnene som følger etableringen av den sikrede kanal er forskjellige fra utførelsen vist ovenfor på figur 3. Denne utførelsen er forskjellig idet hele meldingen blir sendt fra arbeidsstasjonen 101 til signaturserveren 110 ved S418.

Ingen informasjon som krever kryptering trenger derfor å bli returnert til arbeidsstasjonen 101 fra signaturserveren 110. I praksis, blir imidlertid en toretnings sikret kanal fortrinnsvis satt opp, for å unngå at feilinformasjon fra en tredje part angående signaturserveren 110 og dens status, blir sendt til arbeidsstasjonen 101.

I denne utførelse, bruker signaturserveren 110 brukerens private nøkkel til å kryptere hele meldingen som sendt av brukeren. I tillegg, leverer brukeren også leveringsdetaljer for meldingen til en mottaker. Ved dette trinn, annet enn en notis om mottakelse av meldingen, trenger ikke signaturserveren 110 å svare til arbeidsstasjonen 101.

Så snart meldingen er kryptert med brukerens private nøkkel, vil signaturserveren 110 også legge til signaturserveren 110 signatur, ved å kryptere med signaturserverens private nøkkel, og å sende denne krypterte melding til den nye mottaker direkte. Mottakeren kan verifisere meldingen på samme måte som diskutert i forbindelse med figur 3, unntatt at signaturserverens 110 private nøkkel blir brukt, så vel som brukerens offentlige nøkkel. Igjen, standard metoder for kryptering og signering blir brukt her. Noen, eller alle signaturønsker kan ha et oppsummeringsfelt som er logget inn i revisjonsloggen. Hensikten med denne oppsummering er å gjøre det mulig å trekke ut meningsfulle rapporter over kundens aktiviteter og tillate sporfølging hvis det er spørsmål om en transaksjon.

I tillegg, kan flere ønsketransaksjoner bli understøttet, hvor brukeren leverer flere ønsker for flere signaturer, hvor hvert ønske må være separat autentisert. Dette tillater kunden å forberede et antall ønsker og å ha dem alle utført med en enkelt logging. Om nødvendig, kan spesielle nettverksapplikasjoner lagre passord for å danne et mer brukervennlig grensesnitt.

Brukeren kan også be om at en melding eller meldingsspredning skal være tidsstemplet og har en begrenset levetid. Dette blir gjort ved bruk av et flagg i signaturønsket som bestemmer hvorvidt et tidsstempel skal leveres eller ikke. Tidsstemplingen kunne f.eks. bli understøttet ved å kontakte en tidsstempelserver via PKIX TSP-protokollen, hvor en mottatt signatur på en eller annen melding, eller sammenkjedning av et antall signaturer blir sendt til en uavhengig

tredje part, og tilbyr uavhengig tidsstempling. Et tidsstempel blir så lagt til, og en signatur generert på meldingen bestående av de mottatte signaturer og tidsstempelet.

En alternativ fremgangsmåte til den som er beskrevet med henvisning til figur 3 og 4 ovenfor vil bli beskrevet med henvisning til figur 5.

Systemet og fremgangsmåten er spesielt nyttig når signaturen og autentiseringsserveren 110, 120 er geografisk atskilt og administrert av uavhengige organisasjoner. Alle andre trekk kan være som beskrevet med henvisning til en av figurene 3 og 4.

Dataene som skal signeres blir entret på arbeidsstasjonen ved S500. En applikasjon eller annet program nedlastet fra en tredje part til arbeidsstasjonen 101. I denne utførelsen, kjører arbeidsstasjonen en applet eller program, som forbinder begge signaturserverne 110 og autentiseringsserveren 120. Signaturserveren 110 ber om og mottar et fast passord fra brukeren 102 (som beskrevet i forbindelse med registrering ovenfor) ved S502. En autorisert forbindelse med signaturserveren 110 blir så etablert ved S504 som beskrevet ovenfor med henvisning til S302 som beskrevet ovenfor. Signaturserveren 110 ber så som at autoriseringsserveren 120 sender et engangspassord til brukeren via en annen kanal ved S506, som ved S304 beskrevet ovenfor.

Engangspassordet blir sendt til brukeren ved S508 som entrer det over forbindelsen etablert mellom arbeidsstasjonen 101 og autoriseringsserveren 120 ved S510. En verifisert forbindelse blir derfor satt opp mellom både arbeidsstasjonen 101 og signaturserveren 110, og arbeidsstasjonen 101 og autentiseringsserveren 120, ved S512.

Dataene som skal bekreftes blir sendt til autentiseringsserveren 120 gjennom en forbindelse ved S514, og en utledet verdi (i denne utførelsen en spredningsverdi av dataene som beskrevet ovenfor) av dataene som skal bekreftes blir sendt til signaturserveren 110 ved S516.

Autentiseringsserveren 120 sender dataene som skal bekreftes til signaturserveren, som beregner spredningen av dataene for å produsere en utledet verdi for sammenligning med den utledede verdi sendt direkte fra arbeidsstasjonen.

De to utledede verdier blir så sammenlignet av signaturserveren 110 ved S518, som sikrer at de serverne er forbundet med samme bruker.

Signaturserveren 110 kan så signere dataene mottatt fra autentiseringsserveren 120 og returnere dem til arbeidsstasjonen 101, eller videre til en tredje part mottaker.

Det er også mulig at den utledede versjon av dataene blir sendt til autentiseringsserveren 120 og de virkelige data sendt til signaturserveren 110. Dette er imidlertid ikke å foretrekke siden signaturserveren 110 da er i besittelse av dataene som skal signeres før autentiseringsserveren 120 autentiserer det og systemet kunne derfor bli misbrukt hvis ulovlig kontroll av signaturserveren 110 ble oppnådd.

Så vel som bruk av et engangspassord utstedt av autentiseringsserveren 120 for å autentisere forbindelsen mellom arbeidsstasjonen 101 og signaturserveren 110, som beskrevet ovenfor, er det også mulig å bruke et symbol til å validere forbindelsen mellom arbeidsstasjonen 101 og signaturserveren 110, i tilfellet med figur 4, og separate symboler for å validere forbindelsen mellom arbeidsstasjonen 101 og hver server i tilfellet med figur 5. I denne alternative valideringsprosedyren, blir de to kanaler etablert fullstendig uavhengig, hvilket er spesielt nyttig når signatur og autentiseringsserveren 110, 120 er geografsk atskilt og administrert separat.

Utførelsene frembringer en bekreftelsesmetode som møter behovene for tilstrekkelig beskyttelse av den private nøkkel, f.eks. for å møte behovene i direktivet av den europeiske union på kvalifiserte sertifikater; å tillate den riktige eier å initiere genereringen av en digital signatur fra hvilken som helst egnet arbeidsstasjon 101 forbundet med passende nettverk, så som internett, uten å kompromittere signaturnøkkelen, og samtidig hindre at noen med total kontroll over en arbeidsstasjon 101 som har vært brukt som beskrevet ovenfor, til senere å ha en ny signatur generert ved hjelp av nøkkelen til denne eier.

Skjønt de ovenstående utførelser er beskrevet i forbindelse med en arbeidsstasjon og server, vil også hvilken som helst situasjon hvor en melding trenger å bli signert med en digital signatur uten at den private nøkkel av brukeren forlater en sikker server, også falle innenfor denne oppfinnelsen. Også uttrykkene server, klient og arbeidsstasjon som brukt her er ikke begrenset til den smale mening av termene. En server kan være en hvilken som helst datamaskin eller lignende, som kan være forbundet ved en sentral enhet ved et antall arbeidsstasjoner. En arbeidsstasjon er i grensesnitt mellom brukeren og serveren, som sender de elektroniske data og passord, om nødvendig, til serveren. Klienter er ganske enkelt grensesnitt, som tillater administrasjon av en server.

Den foreliggende oppfinnelse er beskrevet ovenfor bare gjennom eksempler, og modifikasjoner kan gjøres innenfor oppfinnelsens ånd. Oppfinnelsen omfatter også hvilken som helst individuelt trekk beskrevet eller antydet her eller vist eller implisitt i tegningene eller hvilken som helst kombinasjon av slike trekk eller en generalisering av slike trekk eller kombinasjoner, som strekker seg til ekvivalenter av disse.

Hvis ikke innholdet klart krever annerledes, gjennom beskrivelse og krav, skal ordene "omfatte", "bestå", og lignende, anses i en inklusiv i motsetning til eksklusiv eller utstrakt forstand, dvs. i betydningen "omfattende, men ikke begrenset til".

P a t e n t k r a v

1.

Fremgangsmåte for å sertifisere elektronisk data levert av en bruker, k a r a k - t e r i s e r t v e d at fremgangsmåten innbefatter trinnene:

å ta imot data levert av brukeren som blir sertifisert i et sertifiseringsapparat (110) fra en kildeinnretning (101),

å sende en forespørsel til en fjern innretning (120) som instruerer den fjerne innretningen om å sende et passord til brukeren,

å ta imot en hashverdi utledet fra passordet fra den fjerne innretningen,

å ta imot en videre hashverdi fra brukeren,

å sammenligne den videre hashverdien fra brukeren med hashverdien fra den fjerne innretningen for derved å validere brukeren,

å sertifisere dataene i sertifiseringsapparatet (110) med ett eller flere elementer med informasjon som er sikker i sertifiseringsapparatet, der elementene er unike for brukeren, dersom den videre hashverdien samsvarer med hashverdien utledet fra den fjerne innretningen, og

å sende ut dataene som er sertifisert fra sertifiseringsapparatet (110), for å gi disse videre til en mottagende innretning,

hvor elementene, med sikker informasjon, sertifiserer at leverandøren av dataene er brukeren.

2.

Fremgangsmåte i henhold til krav 1, videre k a r a k t e r i s e r t v e d å innbefatte autentisering av en forbindelse mellom kildeinnretningen og sertifiseringsapparatet ved å bruke et fast passord gjenkjent av sertifiseringsapparatet, og

å etablere en sikker kanal mellom kildeinnretningen og sertifiseringsapparatet ved å bruke hashverdien mottatt fra sertifiseringsapparatet sammen med en offentlig nøkkel for sertifiseringsapparatet for å generere en sesjonsnøkkel for den sikre kanalen.

3.

Fremgangsmåte i henhold til krav 1 eller 2, videre k a r a k t e r i s e r t v e d å innbefatte og etablere en kryptert kanal mellom den fjerne innretningen og sertifiseringsapparatet, hvor sertifiseringsapparatet og den fjerne innretningen inkluderer fiklemotstandsdyktig hardware (111, 121), og hvor den krypterte kanalen innbefatter en sikker tunnel (150) mellom den fjerne innretningen og sertifiseringsapparatet slik at nøklene som er brukt for tunnelen blir kontrollert av den fiklemotstandsdyktige hardware og ikke opptrer klart på utsiden av sertifiseringsapparatet.

4.
Fremgangsmåte i henhold til krav 1, 2 eller 3, k a r a k t e r i s e r t v e d at den private nøkkelen til et offentlig nøkkel-/privat nøkkelpar spesifikt for brukeren definerer elementet som er unikt for brukeren.

5.
Fremgangsmåte i henhold til ett av de foregående krav hvor en digital signatur spesifikt for brukeren definerer elementet som er unikt for brukeren.

6.
Fremgangsmåte i henhold til ett av de foregående krav, hvor den mottagende innretningen er den sikre kilden.

7.
Fremgangsmåte i henhold til ett av kravene 1 til 6, k a r a k t e r i s e r t v e d at den mottagende innretning er en tredje parts innretning.

8.
Fremgangsmåte i henhold til ett av de foregående krav, k a r a k t e r i - s e r t v e d at en hashverdi til en melding som blir sertifisert blir generert i kildeinnretningen, hashverdien er dataene som blir sertifisert av sertifiseringsapparatet.

9.
Fremgangsmåte i henhold til ett av de foregående krav, k a r a k t e r i - s e r t v e d at sertifiseringsapparatet er tilpasset til å ta imot data fra et flertall av forskjellige kildeinnretninger.

10.
Fremgangsmåte for å sertifisere elektroniske data levert av en bruker, k a r a k - t e r i s e r t v e d at fremgangsmåten innbefatter trinnene:
å etablere en sikker forbindelse mellom en kildeinnretning (101) styrt av brukeren og et sertifiseringsapparat (110),
å sende data levert av brukeren fra kildeinnretningen (101) som blir mottatt av sertifiseringsapparatet (110),
å ta imot et passord fra en fjern innretning,
å sende en hashverdi med passordet til sertifiseringsapparatet, og
å ta imot i kildeinnretningen en versjon av dataene fra sertifiseringsapparatet (110) sertifisert som å stamme fra brukeren, ved å bruke informasjonen som er unik for brukeren.

11.
Fremgangsmåte i henhold til krav 10, videre k a r a k t e r i s e r t v e d å innbefatte autentisering av en forbindelse mellom kildeinnretningen og sertifiseringsapparatet ved å bruke et fast passord gjenkjent av sertifiseringsapparatet, og å etablere en sikker kanal mellom kildeinnretningen og sertifiseringsapparatet ved å bruke hashverdien sammen med en offentlig nøkkel for sertifiseringsapparatet for å generere en sesjonsnøkkel for den sikre kanalen.

12.
Fremgangsmåte i henhold til krav 10 eller 11, videre k a r a k t e r i s e r t v e d å innbefatte trinnet med å innarbeide en sertifisert versjon av dataene i videre data som blir sendt til en tredje parts innretning.

13.
Fremgangsmåte i henhold til krav 10, 11 eller 12, k a r a k t e r i s e r t v e d at sertifiseringsapparatet holder informasjon som er unik for brukeren for å utføre sertifiseringen.

14.
Fremgangsmåte i henhold til krav 13, k a r a k t e r i s e r t v e d at den unike informasjonen er i den private nøkkelen til et offentlig nøkkel/privat nøkkelpar spesifikt for brukeren.

15.
Fremgangsmåte i henhold til krav 13 eller 14, k a r a k t e r i s e r t v e d at den unike informasjonen er en digital signatur spesifikt for brukeren.

16.
Fremgangsmåte i henhold til ett av kravene 10 til 15, k a r a k t e r i s e r t v e d at dataene som blir sertifisert er en hashverdi til en melding.

17.
Fremgangsmåte i henhold til ett av de foregående krav, k a r a k t e r i - s e r t v e d at sertifiseringsapparatet innbefatter en signaturserver (110).

18.
Fremgangsmåte i henhold til ett av de foregående krav, k a r a k t e r i - s e r t v e d at sertifiseringsapparatet innbefatter et flertall av signaturservere som bruker hemmelig deling for å lagre individuelle deler av privat nøkkel til en bruker, og hvor

signaturen blir generert basert på individuelle deler av en privat nøkkel til en bruker lagret på noen eller alle av signaturserverne.

19.

Fremgangsmåte i henhold til krav 17 eller 18, k a r a k t e r i s e r t v e d at sertifiseringsapparatet videre innbefatter en eller flere autentiseringsservere (120).

20.

Fremgangsmåte i henhold til ett av de foregående krav, k a r a k t e r i s e r t v e d at kildeinnretningen (101) innbefatter en arbeidsstasjon.

21.

Fremgangsmåte i henhold til krav 20, videre k a r a k t e r i s e r t v e d å innbefatte og etablere en uavhengig verifisert og autentisert kommunikasjonskanal mellom arbeidsstasjonen og den fjerne innretningen.

22.

Fremgangsmåte i henhold til ett av kravene 1 til 19, k a r a k t e r i s e r t v e d at kildeinnretningen innbefatter et interaktivt televisjonsapparat.

23.

Fremgangsmåte i henhold til ett av de foregående krav, k a r a k t e r i s e r t v e d at kildeinnretningen og sertifiseringsapparatet etablerer autentiserte individuelle forbindelser mellom kildeinnretningen og en eller flere servere til sertifiseringsapparatet før og under overføring av dataene som blir sertifisert.

24.

Fremgangsmåte i henhold til krav 23, k a r a k t e r i s e r t v e d at fremgangsmåten virker ved å autentisere brukeren uansett kilden for å gi et første nivå av sikkerhet, og virker ved å autentisere brukeren og kildeinnretningen for å gi et andre nivå av sikkerhet høyere enn det første nivået av sikkerhet.

25.

Fremgangsmåte i henhold til krav 1 eller 10, k a r a k t e r i s e r t v e d at kildeinnretningen leverer et merke (token) (190) til sertifiseringsapparatet for autentisering, og hvor sertifiseringsapparatet sertifiserer dataene med forskjellige unike elementer avhengig av typen av merke brukt for å autentisere brukeren eller kildeinnretningen.

26.
Fremgangsmåte i henhold til ett av de foregående krav, k a r a k t e r i s e r t v e d at valideringsdata for å validere dataene som blir sertifisert blir mottatt fra en fjern innretning før dataene blir sertifisert.

27.
Fremgangsmåte i henhold til ett av de foregående krav, videre k a r a k t e r i s e r t v e d å innbefatte at sertifiseringsapparatet sender forespørselen til den fjerne innretningen etter mottak av en forespørsel om å sertifisere data.

28.
Fremgangsmåte i henhold til ett av kravene 1 til 27, videre k a r a k t e r i s e r t v e d å innbefatte:
å ta imot en forespørsel fra sertifiseringsapparatet i den fjerne innretningen for å levere brukeren passordet,
å levere passordet til brukeren, og
å levere hashverdien utledet fra passordet til sertifiseringsapparatet.

29.
Fremgangsmåte i henhold til ett av de foregående krav hvor passordet er et engangspassord.

30.
Fremgangsmåte i henhold til krav 28 eller 29, k a r a k t e r i s e r t v e d at forespørselen og hashverdien utledet fra passordet blir overført via en forskjellig kommunikasjonsfremgangsmåte til passordet.

31.
Datamaskinlesbart medium som lagrer instruksjoner, k a r a k t e r i s e r t v e d at når disse blir eksekvert i en datamaskin forårsaker det datamaskinen å utføre hver av fremgangsmåtetrinnene i ett av kravene 1 til 9.

32.
Datamaskinlesbart medium som lagrer instruksjoner, k a r a k t e r i s e r t v e d at når de blir eksekvert i en datamaskin forårsaker det datamaskinen i å utføre hver av fremgangsmåtetrinnene i henhold til ett av kravene 10 til 30.

33.
Datasertifiseringsapparat (110, 120), k a r a k t e r i s e r t v e d å innbefatte:

en signeringsinnretning (110, 111) tilpasset til å sertifisere elektroniske data mottatt fra en fjern kildeinnretning (101) som stammer fra en bruker, hvor sertifiseringsapparatet er anordnet til å ta imot data fra kildeinnretningen, sertifisere dataene som hører til brukeren, å bruke informasjon lagret i sertifiseringsapparatet og kryptografiske teknikker, der informasjonen er unik for brukeren, og å sende de sertifiserte data til en mottagende innretning, og videre innbefattende instruksjonsinnretning for å sende en forespørsel til en videre fjern innretning som instruerer den videre fjerne innretningen å sende passord til brukeren, mottagende innretning for å ta imot en hashverdi utledet fra passordet fra den videre fjerne innretningen og for å ta imot en videre hashverdi fra brukeren, sammenligningsinnretning for å sammenligne den videre hashverdien fra brukeren med hashverdien fra den videre fjerne innretningen, og sertifiseringsinnretning (110, 111) for å sertifisere dataene som blir sertifisert dersom videre hashverdien fra brukerdataene samsvarer med hashverdien fra den videre fjerne innretningen.

34.
Datasertifiseringsapparat i henhold til krav 33, k a r a k t e r i s e r t v e d å innbefatte innretning for å autentisere en forbindelse mellom kildeinnretningen og sertifiseringsapparatet ved å bruke et fast passord gjenkjent av sertifiseringsapparatet, og innretning for å etablere en sikker kanal mellom kildeinnretningen og sertifiseringsapparatet ved å bruke hashverdien mottatt av sertifiseringsapparatet sammen med en offentlig nøkkel for sertifiseringsapparatet for å generere en sesjonsnøkkel for den sikre kanalen.

35.
Datasertifiseringsapparat i henhold til krav 33 eller 34, k a r a k t e r i - s e r t v e d videre å innbefatte innretning for å etablere en kryptert kanal mellom den fjerne innretningen og sertifiseringsapparatet, hvor sertifiseringsapparatet og den fjerne innretningen inkluderer fiklemotstandsdyktig hardware (111, 121), og hvor den krypterte kanalen innbefatter en sikker tunnel (150) mellom den fjerne innretningen og sertifiseringsapparatet slik at nøklene som er brukt for tunnelen blir kontrollert av den fiklemotstandsdyktige hardware og ikke opptrer klart på utsiden av sertifiseringsapparatet.

36.
Datasertifiseringsapparat i henhold til krav 33, k a r a k t e r i s e r t v e d at sertifiseringsapparatet innbefatter innretning for å etablere en autentisert forbindelse med kildeinnretningen før og underoverføring av data som blir sertifisert.

37.
Datasertifiseringsapparat i henhold til krav 36, k a r a k t e r i s e r t v e d at den autentiserte forbindelsen blir kryptert.

38.
Datasertifiseringsapparat i henhold til krav 36 eller 37, k a r a k t e r i s e r t v e d at sertifiseringsapparatet innbefatter innretning for å akseptere et merke (token) fra kildeinnretningen for autentisering, og hvor sertifiseringsapparatet innbefatter innretning for å bruke mer enn en type av merke for å autentisere brukeren eller kildeinnretningen.

39.
Datasertifiseringsapparat i henhold til krav 38, k a r a k t e r i s e r t v e d at datasertifiseringsapparatet er anordnet til å virke ved å autentisere brukeren uansatt kildeinnretningen som blir gitt et første nivå av sikkerhet, og som virker ved å autentisere brukeren og kildeinnretningen for å gi et andre nivå av sikkerhet høyere enn det første nivået av sikkerhet.

40.
Datasertifiseringsapparat i henhold til krav 36 eller 37, k a r a k t e r i s e r t v e d at kildeinnretningen innbefatter innretning for å levere et merke (token) (190) til sertifiseringsapparatet for autentisering, og hvor sertifiseringsapparatet innbefatter innretning for å sertifisere dataene med forskjellige unike elementer, avhengig av typen av merke som er brukt for å autentisere brukeren eller kildeinnretningen.

41.
Datasertifiseringsapparat i henhold til ett av kravene 33 til 40, k a r a k t e r i s e r t v e d at sertifiseringsapparatet innbefatter en signaturserver (110).

42.
Datasertifiseringsapparat i henhold til krav 41, k a r a k t e r i s e r t v e d at sertifiseringsapparatet innbefatter et flertall av signaturservere, hver signaturserver er anordnet til å bruke hemmelig deling for å lagre individuelle andeler av en privat nøkkel til en bruker, hvor signaturen blir generert.

43.
Datasertifiseringsapparat i henhold til krav 41 eller 42, k a r a k t e r i s e r t v e d at sertifiseringsapparatet videre innbefatter en autentiseringsserver (120).

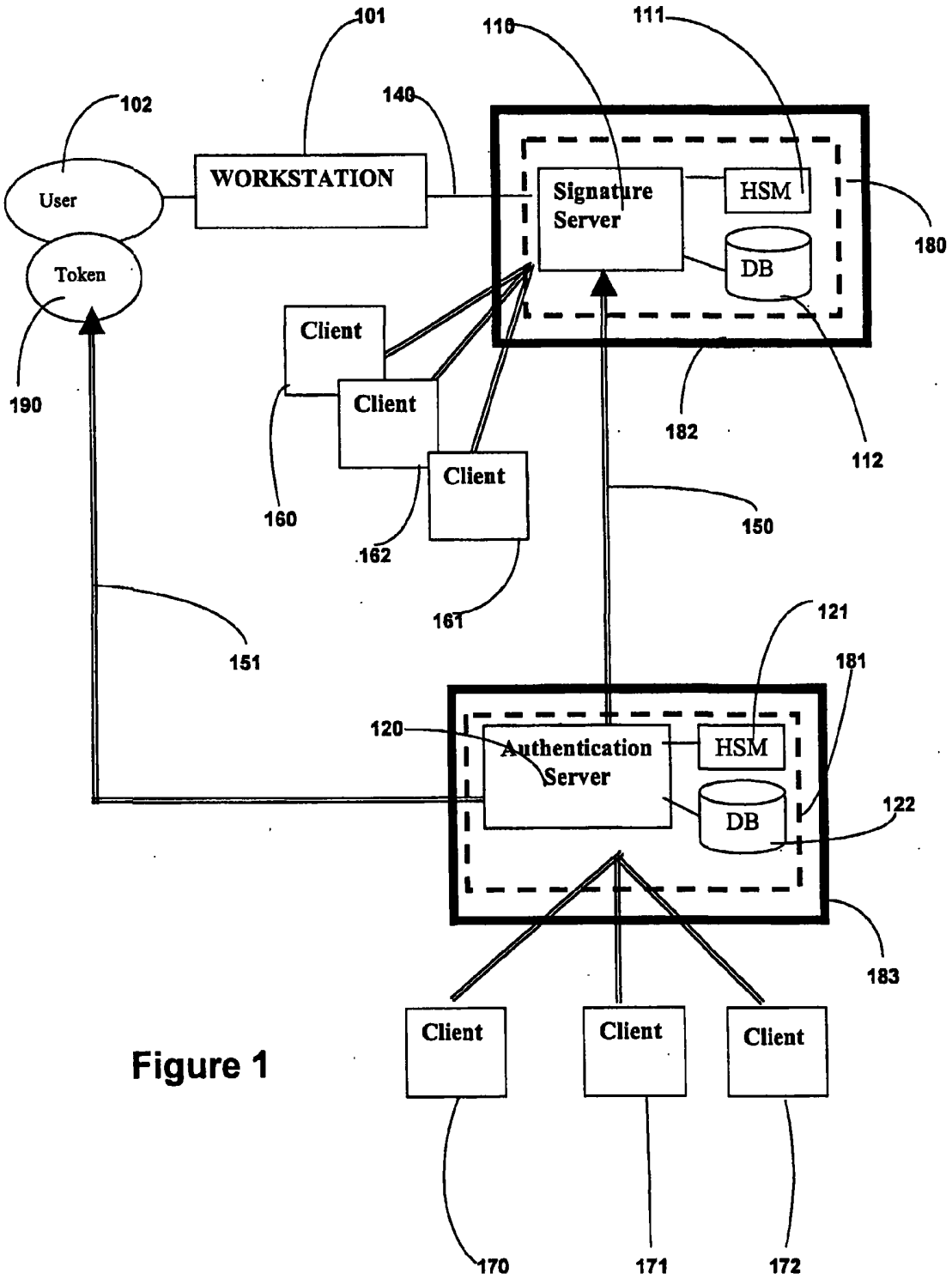

101
110
111
102
140
WORKSTATION
User
Token
Signature Server
HSM
DB
180
190
Client
Client
Client
160
162
161
182
112
150
151
121
181
120
Authentication Server
HSM
DB
122
183
Client
Client
Client
170
171
172

Figure 1

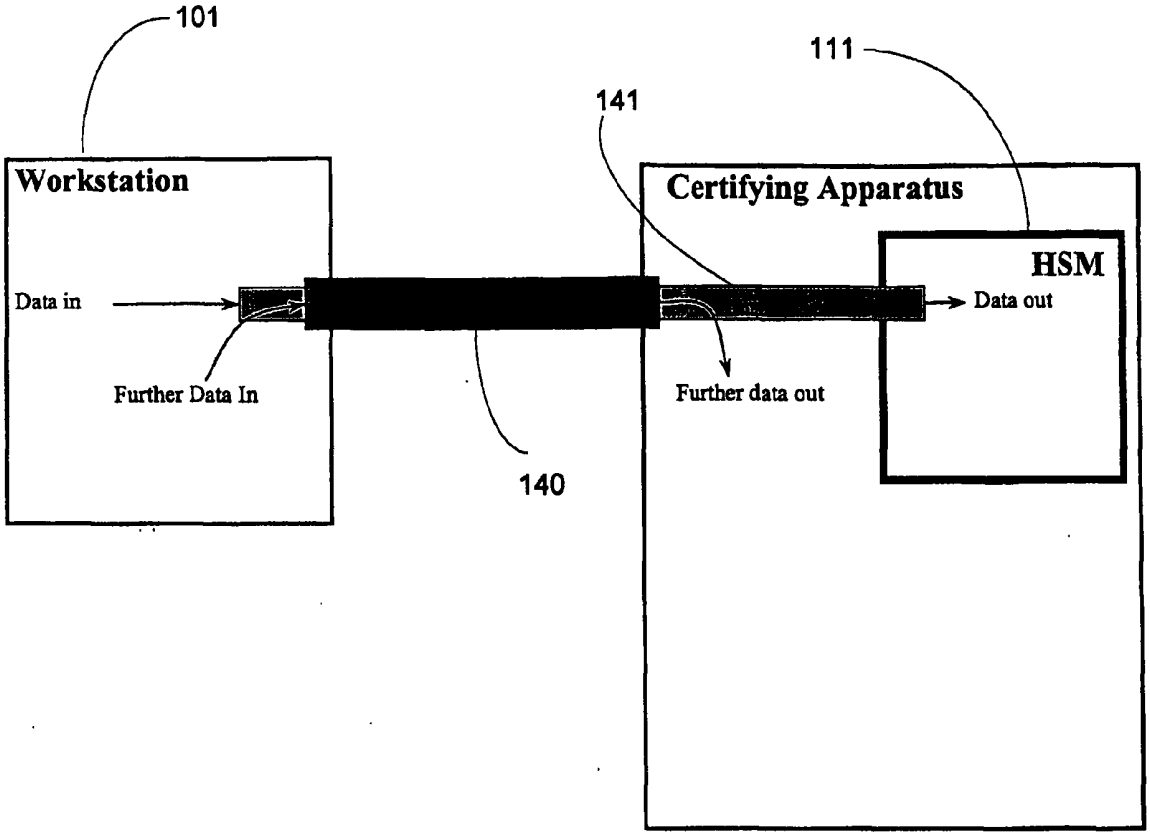

101
111
141
Workstation
Certifying Apparatus
HSM
Data in
Data out
Further Data In
Further data out
140

Figure 2

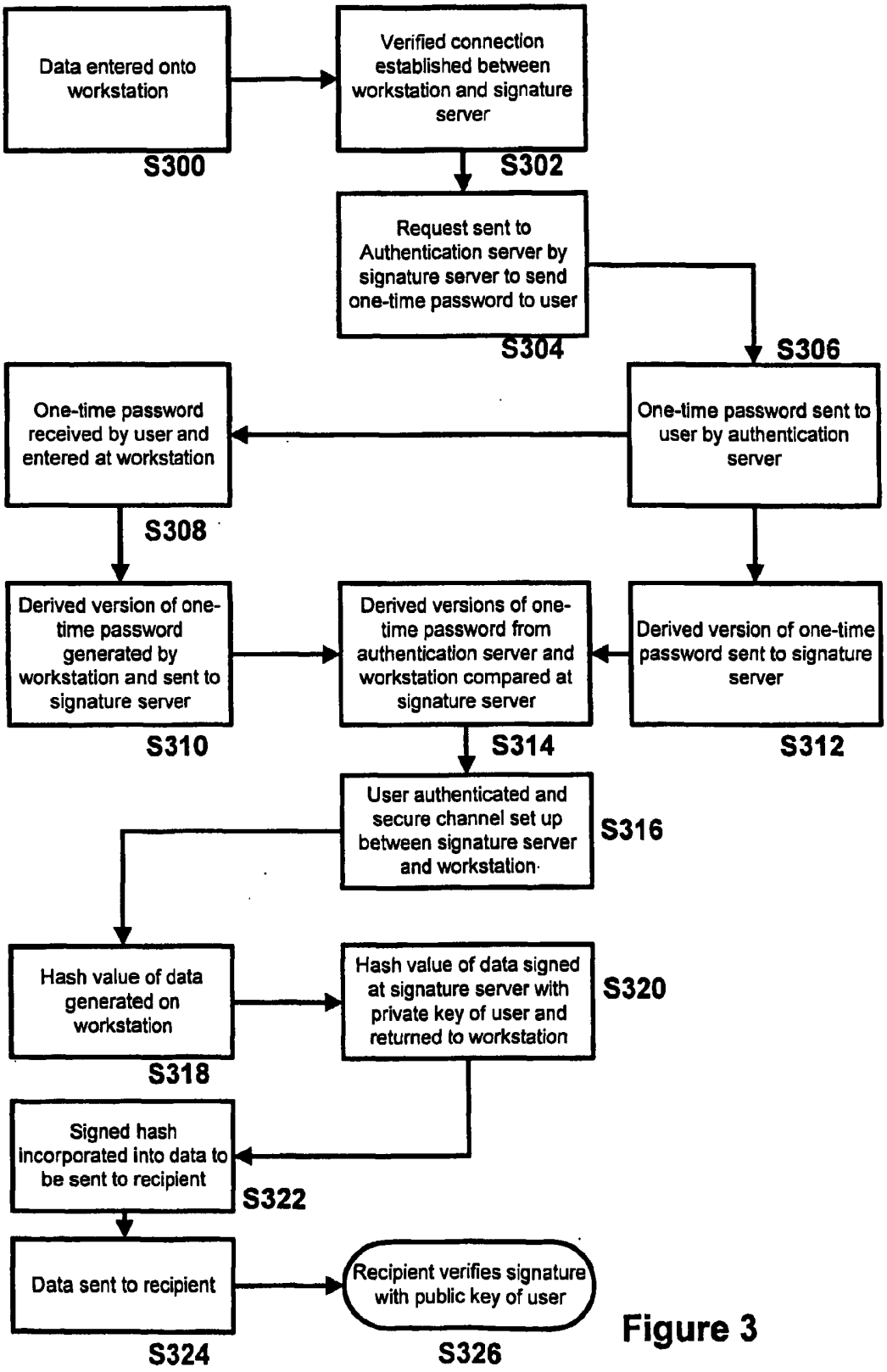

Data entered onto workstation
S300
Verified connection established between workstation and signature server
S302
Request sent to Authentication server by signature server to send one-time password to user
S304
S306
One-time password sent to user by authentication server
One-time password received by user and entered at workstation
S308
Derived version of one-time password generated by workstation and sent to signature server
S310
Derived versions of one-time password from authentication server and workstation compared at signature server
S314
Derived version of one-time password sent to signature server
S312
User authenticated and secure channel set up between signature server and workstation
S316
Hash value of data generated on workstation
S318
Hash value of data signed at signature server with private key of user and returned to workstation
S320
Signed hash incorporated into data to be sent to recipient
S322
Data sent to recipient
S324
Recipient verifies signature with public key of user
S326

Figure 3

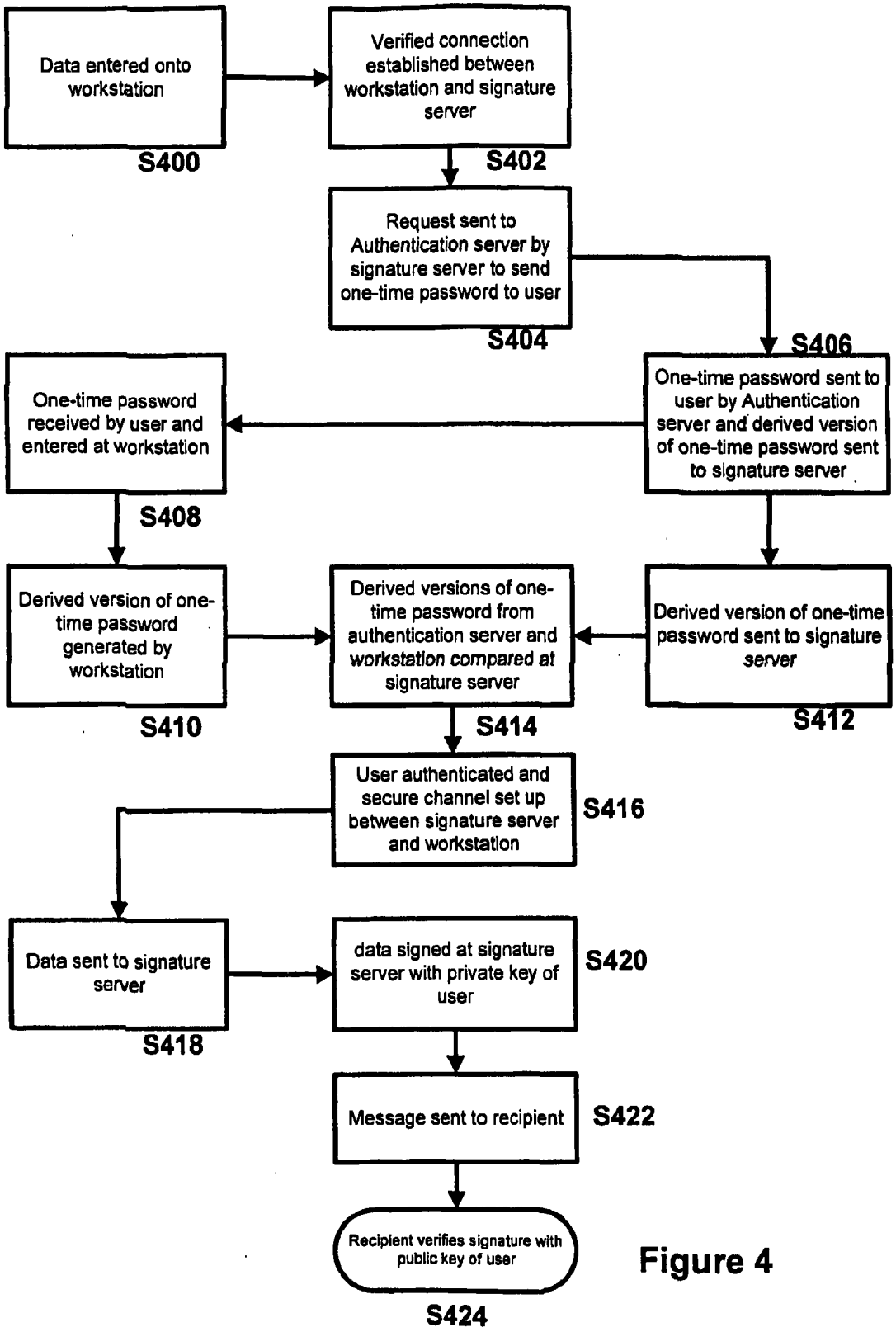

Data entered onto workstation
S400
Verified connection established between workstation and signature server
S402
Request sent to Authentication server by signature server to send one-time password to user
S404
S406
One-time password sent to user by Authentication server and derived version of one-time password sent to signature server
One-time password received by user and entered at workstation
S408
Derived version of one-time password generated by workstation
S410
Derived versions of one-time password from authentication server and workstation compared at signature server
S414
Derived version of one-time password sent to signature server
S412
User authenticated and secure channel set up between signature server and workstation
S416
Data sent to signature server
S418
data signed at signature server with private key of user
S420
Message sent to recipient
S422
Recipient verifies signature with public key of user
S424

Figure 4

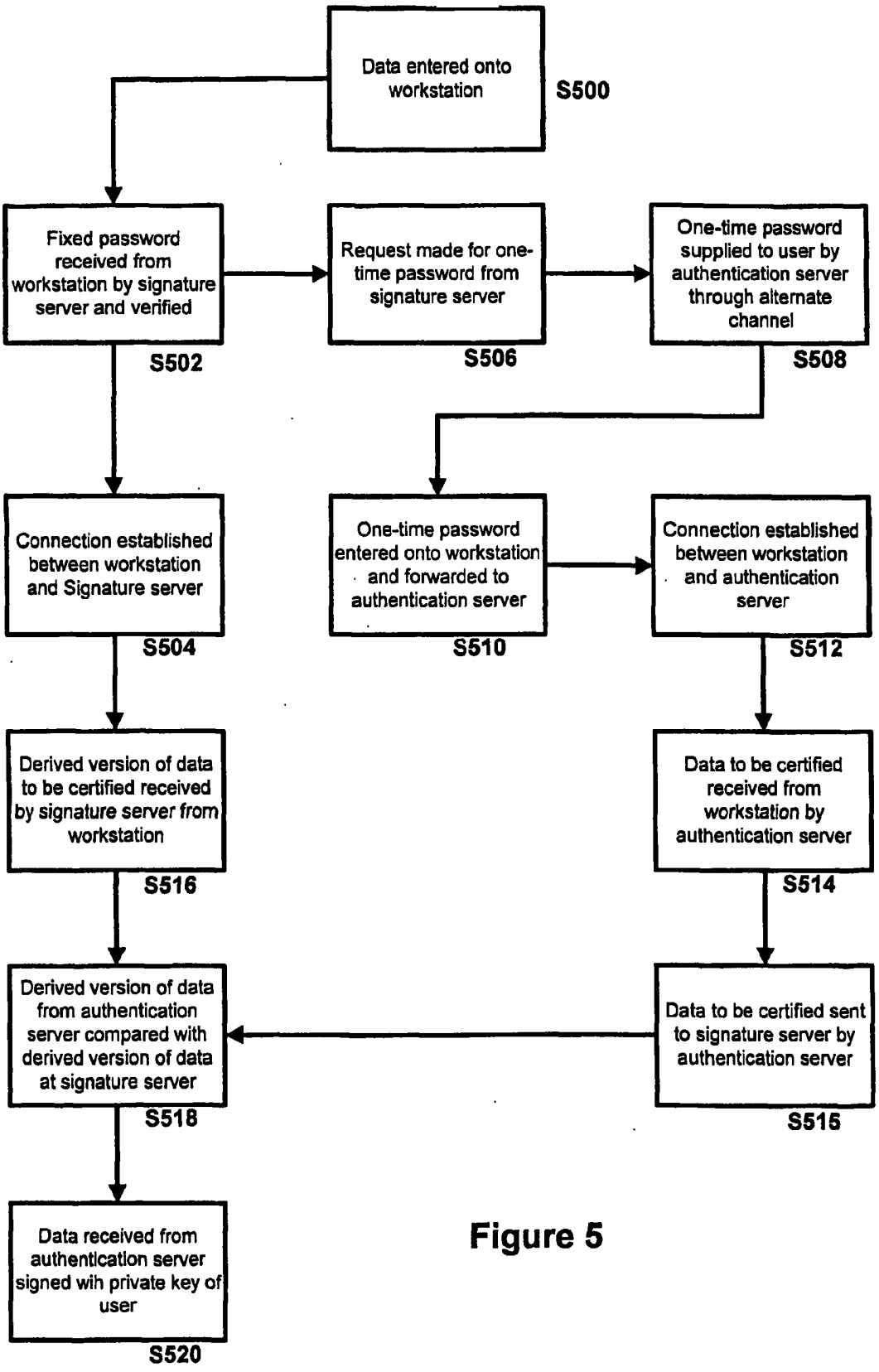

Data entered onto workstation
S500
Fixed password received from workstation by signature server and verified
S502
Request made for one-time password from signature server
S506
One-time password supplied to user by authentication server through alternate channel
S508
Connection established between workstation and Signature server
S504
One-time password entered onto workstation and forwarded to authentication server
S510
Connection established between workstation and authentication server
S512
Derived version of data to be certified received by signature server from workstation
S516
Data to be certified received from workstation by authentication server
S514
Derived version of data from authentication server compared with derived version of data at signature server
S518
Data to be certified sent to signature server by authentication server
S515
Data received from authentication server signed wih private key of user
S520

Figure 5