(12) **PATENT**

(19) NO (11) **335397** (13) **B1**

NORGE

(51) Int Cl.
G06F 21/30 (2013.01)
G06F 21/64 (2013.01)
H04L 9/32 (2006.01)

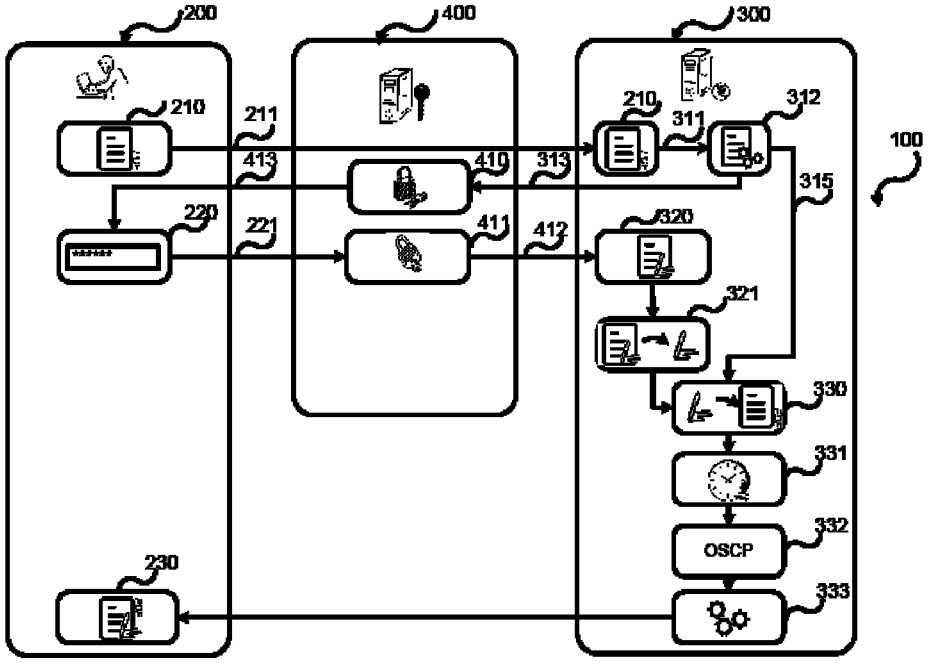
Patentstyret

(21)	Søknadsnr	20121349	(86)	Int.inng.dag og søknadsnr	
(22)	Inng.dag	2012.11.15	(85)	Videreføringsdag	
(24)	Løpedag	2012.11.15	(30)	Prioritet	
(41)	Alm.tilgj	2014.05.16			
(45)	Meddelt	2014.12.08			

(73)	Innehaver	Maestro Soft AS, Postboks 403 Skøyen, 0213 OSLO, Norge
(72)	Oppfinner	Liana Gyulzadyan Svendsen, c/o Maestro Soft AS, Karenslyst allé 8 B, 0213 OSLO, Norge
(74)	Fullmektig	Acapo AS, Postboks 1880 Nordnes, 5817 BERGEN, Norge

(54)	Benevnelse	**Signaturportering**
(56)	Anførte publikasjoner	Masterthesis med tittel Advanced Electronis Signature av Azizi, Fazel Ahmad publisert Juni 2011, Norwegian University of Science and Technology Department of Telematics lastet ned fra Internett 2013.04.24
(57)	Sammendrag	

En fremgangsmåte for digital signering av dokumenter er tilveiebrakt. Dette tilveiebringes ved et signaturporteringssystem som ekstraherer signatur 5 fra et signert dokument og porterer den ekstraherte signatur til et forhåndsbehandlet dokument. Dette muliggjør multisignering av et dokument.



Oppfinnelsens bakgrunn

Teknisk område

Oppfinnelsen angår digital signering generelt og nærmere bestemt et system for og en fremgangsmåte for digital signering av dokumenter med elektroniske identifiseringssystemer.

Bakgrunnsteknikk

Følgende forkortelser fra faget vil bli benyttet:

PKI	Private Key Infrastructure
PKCS	Public Key Cryptography Standards
CMS	Cryptographic Message Syntax
ETSI	European Telecommunications Standards institute
CAdES-BES	CMS Advanced Electronic Signatures - Basic Electronic Signature
SEID	Samarbeidsprosjekt om eID og eSignatur.
SDO	Signed Data object
XML	Extensible Markup Language
PDF	Portable Data Format
PAdES	PDF Advanced Electronic Signature
LTV	Long term validation
OCSP	Online Certificate Status Protocol
CRL	Certificate Revocation List
TSA	Time Stamping Authority
CSP	Cryptographic Service Provider
TTP	Trusted Third Party
e-ID	Elektronisk Identitet.

Eksisterende PKI-leverandører har sine egne PKI løsninger hvor en digital signatur kan returneres på ulike signaturinnpakkingsformater. For eksempel kan det være CMS signatur basert på PKCS#7 , CMS signatur basert på ETSI CAdES-BES, XML basert signatur formatert i SEID SDO (http://www.npt.no/ikbViewer/Content/44963/SEID_Leveranse_3_v1.0.pdf) eller Adobe PDF signatur. For å kunne lese informasjon om signatar og kunne se selve dokumentet som er signert, krever noen av disse formatene et eget proprietært

leseverktøy. Det er derfor ønskelig å støtte signering i Adobe PDF formatet som er et allment tilgjengelig format i dag hvor både signatur og dokument kan vises i Adobe PDF Reader som er svært allment utbredt også på verdensbasis. I 2009 utarbeidet ETSI profiler for PAdES dokumenter som imøtekommer kravene til det Europeisk Direktivet 1999/93/EC (European Directive on A Community Framework for Digital Signatures).

Den fysiske plasseringen av selve privat-nøkkelen og sertifikatet kan også inngå som en del av kravene, eksempelvis som at sertifikatet og privat-nøkkelen må være fysisk hos brukeren. I så måte må det vises til BankID der sertifikatet og privat-nøkkelen faktisk ikke er hos brukeren, men i stedet er hos banken. Andre løsninger som Buypass tilveiebringer sertifikatet i brikken som brukeren innehar.

Fra den kjente teknikk skal det vises til følgende teknologier.

Digital signering av dokumenter med smartkort (Cryptographic Service Providers)
`http://msdn.microsoft.com/en-us/library/aa380245.aspx`
Ved å bruke denne teknologien, kan man delvis oppnå ønsket funksjonalitet, men svakheten er at den krever installasjon av tredjeparts programvare hos brukeren eller konfigurasjon av eksisterende rammeverk. Dette er lite levedyktig fordi blant annet det ikke er garantert at løsningen vil ha nok rettigheter til å endre konfigurasjon lokalt hos brukeren. Samtidig kan det være en del begrensninger forbundet med at ikke alle implementeringer av klientprogramvare støtter oppslag i online registre for verifisering av brukersertifikater.

Digital Signering av ved hjelp av PKI
Løsningen tilveiebringer muligheten for digital signering med PKI, imidlertid er dette beheftet med flere utfordringer, blant annet fordi PKI tjeneste leverandørene har forskjellige implementeringer av infrastrukturen. Resultatet er at det er vanskelig å få ønsket sluttresultat i den format som man ønsker pluss er det begrensninger når det kommer til multisignering av samme dokument med forskjellige elektroniske identiteter (e-ID).

Fra den kjente teknikk skal det også vises til Masterthesis med tittel «Advanced Electronis Signature» av Azizi, Fazel Ahmad, publisert juni 2011, Norwegian University of Science and Technology, Department of Telematics. Denne omhandler elektroniske signaturer med proxy-signaturer. En fremgangsmåte omtales der man

signerer på vegne av en bruker med andre nøkler som er kalkulert ut i fra brukerens nøkler. I og med at løsningen beskriver et signaturfremstillingssystem som signerer med en tiltrodd kopi eller utledet nøkkel av brukerens private nøkkel, opptrer løsningen som en tiltrodd tredjepart og forvalter av nøkler (keyring). Dokumentet omtaler ulike måter å overføre private eller beregnede nøkler til nøkkelbeholder (key ring), men beskriver imidlertid ikke en portering av signaturen etter denne er påført i signaturfremstillingssystemet

Det er derfor et behov for en løsning som løser overnevnte problemer.

Kort gjennomgåelse av oppfinnelsen

Et hovedmål med den foreliggende oppfinnelse er å tilveiebringe en løsning der man kommer frem til system for og en fremgangsmåte for digital signering av dokumenter med elektroniske identifiseringssystemer. Det er også et mål å komme frem til system og fremgangsmåte for å ta frem en PAdES-signatur med utgangspunkt i en CMS, SDO, XML basert signatur. Videre er det et mål å muliggjøre flere signatarer med ulike PKI løsninger ved signering av samme dokument.

Problemer som måtte løses med oppfinnelsen

Av denne grunn er det et hovedmål med den foreliggende oppfinnelse å tilveiebringe en fremgangsmåte for å lage et system hvor man kan signere et PDF-dokument i et proprietært signaturformat som støttes av en gitt PKI leverandør, men likevel klare å ekstrahere signaturen i senere tid og lage en gyldig PAdES kompatibel signatur. Original signatur kan være CMS, SDO, eller XML-basert og for å kunne se både data som er signert og informasjon om hvem som har signert og andre detaljer om signatar kreves i noen tilfeller enten en online tjeneste eller en ikke utbredt ekstern visningsapplikasjon. Av denne grunn har det vært et ønske om å kunne generere et PAdES dokument for å kunne fremvise det signerte dokumentet og detaljer om signatarer i Adobe Reader. Problemet var at PKI-leverandørene enten ikke støttet signaturer i PDF-fil eller de støttet bare en begrenset profil av PDF signatur som gjorde det umulig å bruke deres PDF-signeringstjeneste. Det har også vært et ønske om å kunne ha mulighet til å multi-signere en PDF-fil med flere signatarer hvor de kan bruke flere forskjellige PKI løsninger. Dette var umulig siden de forskjellige PKI løsningene returnerte signaturer i forskjellige filformater.

I noen av PKI-løsningene besitter brukeren sin private nøkkel og sertifikat, mens i de andre PKI løsningene ligger både privat nøkkel og sertifikat lagret hos godkjent tiltrodd tredjepart (TTP). Dette har skapt utfordringer siden vanlig prosess for laging av digital signatur forutsetter at signatar har tilgang til sin private nøkkel og sertifikat. Derfor er det umulig for brukeren å bruke CSP (Cryptographic Service Provider) for å signere dokumentet i det formatet han ønsker. I stedet sendes dokumentet eller en hash av innholdet i dokumentet til PKI leverandøren som ved hjelp av flere sikkerhetsfaktorer henter privat nøkkel til brukeren og lager signatur over innholdet (samt signaturer over en del andre parametere). Når signaturen over dokumentet lages er den basert på HASH av innholdet i PDF-filen. Dette innebærer at inkludering av signaturfelter i den originale PDF-filen i ettertid vil endre på hash av filen og gjøre signaturen ugyldig.

De midler som trengs for å løse problemene

Den foreliggende oppfinnelse når det mål som er satt opp ovenfor ved en fremgangsmåte for digital signering av dokumenter som definert i innledningen til krav 1, med trekkene i karakteristikken til krav 1.

Den foreliggende oppfinnelse når det mål som er satt opp ovenfor ved en fremgangsmåte for digital multisignering av dokumenter som definert i innledningen til krav 3, med trekkene i karakteristikken til krav 3.

Den foreliggende oppfinnelse når det mål som er satt opp ovenfor ved et signaturporteringssystem som ekstraherer signatur fra et signert dokument og porterer den ekstraherte signatur til et forhåndsbehandlet dokument.

Virkningene av oppfinnelsen

Den tekniske forskjell fra eksisterende PKI-løsninger er at foreliggende oppfinnelse tilveiebringer signering av dokumenter så som PDF-dokumenter ved bruk av ekstraksjon av mottatt signatur fra signering fra PKI og portering av denne signaturen for å signere dokumentet i ønsket format.

Disse effektene tilveiebringer i sin tur ytterligere gunstige effekter:

det gjør det mulig å signere et PDF-dokument i ønsket PAdES eller annet PDF signaturformat, selv om PKI leverandøren ikke direkte støtter dette, og

multisignering av et PDF-dokument med av signatarer som hver kan anvende ulike PKI løsninger.

Oppfinnelsen tilveiebringer en fremgangsmåte der man har funnet en metode hvor man ved å sende ekstra data sammen med PDF-dokumentet klarer å få tilbake signatur som er basert på en hash av PDF-dokumentet med signeringsfelter som signeres senere.

Hvis hovedsertifikat-kjeden er tilgjengelig enten via OCSP oppslag eller via fysisk tilgjengelige rot-sertifikater, kan man også konstruere en gyldig LTV signatur. Samtidig tilføyes tidsstempel fra Time Stamping Authority.
Metoden løser også problemet med multisignaturer fordi ved å sekvensielt sende PDF-dokumentet til de forskjellige PKI løsningene, tilveiebringes et PDF-dokument med flere signaturer.

Kort gjennomgåelse av tegningene

Oppfinnelsen skal i det følgende beskrives nærmere under henvisning til tegningsfigurene som viser flere utførelseseksempler, og der

fig. 1 skjematisk viser informasjonsflyten i et signatursystem som er basert på løsningen.

fig. 2 skjematisk viser et eksempel på multippel signering av et dokument av 2 brukere med 2 forskjellige PKI løsninger.

fig. 3 skjematisk viser strukturen av et signert PDF-dokument.

Gjennomgåelse av henvisningstallene som viser til tegningene

100	Signatursystem
200	Bruker
210	Original PDF-dokument
211	Opplasting av original PDF-dokument til Signatur porteringssystem
220	Smartkort, OTP generator, pinkoder eller passord.
221	Brukeren autentiserer seg med passord, pinkoder, osv.
230	Digitalt signert PAdES PDF-dokument
300	Signatur porteringssystem
311	Forhåndsbehandle PDF-dokument og klargjøre den til PKI signering
312	Forhåndsbehandlet dokument.
313	Send forespørsel om signering til PKI.

315	Send forhåndsbehandlet dokument for sluttføring av signatur.
320	Digital signatur i for eksempel SDO, CMS, PKS#7, XML eller andre formater
321	Ekstraher signatur fra mottatt signert dokument.
330	Porter signaturen til PDF-dokument
331	Koble til TSA for tidsstempling
332	Lag OCSP oppslag
333	Sluttfør signering og lag PAdES dokument med LTV
400	Private Key Infrastructure
410	PKI-løsningens lager av sertifikater og eventuelt nøkler.
411	PKI-løsningen signerer dokument med privat nøkkel og sertifikat
412	Levering av signatur basert på Bruker sine privatnøkler til Signaturporteringssystem.
413	Forespørsel fra PKI om autentisering.
101	MultiSignatursystem
1200	Bruker_1
2200	Bruker_2
1300	Multisignatur porteringssystem.
1400	Private Key Infrastructure som Bruker_1 skal bruke for signering (PKI_1)
2400	Private Key Infrastructure som Bruker_2 skal bruke for signering (PKI_2)
1212	Bruker_1 interaksjon med systemer (f.eks. klargjøring av maskinvare for autentisering, inntasting av passord, pinkoder)
1213	Bruker_1 autentiserer seg med passord, pinkoder.
1401	PKI_1 sender forespørsel til Bruker_1 om autentisering
1402	Levering av signatur basert på Bruker_1 private nøkler til Signaturporteringssystem.
1340	Behandling av signaturer og dokumenter fra Bruker_1 og PKI_1
1342	Signaturporteringssystem sender forespørsel til PKI_1 om signatur
1343	Sluttføring og laging av PDF-dokument med signatur fra Bruker_1
1230	PDF-dokument signert av Bruker_1
2212	Bruker_2 interaksjon med systemer (f.eks. klargjøring av maskinvare for autentisering, inntasting av passord, pinkoder)
2213	Bruker_2 autentiserer seg med passord, pinkoder.
2340	Behandling av dokumenter og signaturer fra Bruker_2 og PKI_2
2342	Signaturportseringssystem sender forespørsel til PKI_2 om signatur
2401	PKI_1 sender forespørsel til Bruker_1 om autentisering

2402	Levering av signatur basert på Bruker_2 private nøkler til Signaturporteringssystem.
2343	Sluttføring og laging av PDF-dokument med signatur fra Bruker1 og Bruker_2
12230	PDF-dokument signert av Bruker_1 og Bruker_2
1344	Nedlasting av PDF-dokument med to signaturer til Bruker_1
2344	Nedlasting av PDF-dokument med to signaturer til Bruker_2
102	Detaljer om signert PDF-dokument
500	Struktur i signer PDF-dokument
510	Innhold
511	Sertifikat
512	Signert melding digest
513	Tidsstempel

Nærmere beskrivelse av oppfinnelsen

Oppfinnelsen skal i det følgende beskrives nærmere under henvisning til tegningsfigurene som viser flere utførelseseksempler, og der

Fig. 1 viser skjematisk et signatursystem med en interaksjon mellom en bruker, et signaturporteringssystem og en PKI, og

Fig. 2 viser skjematisk oppbyggingen av et signert PDF-dokument signert ifølge oppfinnelsen

Prinsipper som ligger til grunn for oppfinnelsen

Dersom et dataobjekt, eller fil, er signert med kvalifisert elektronisk signatur, vil også samtlige kopier være valide signerte utgaver. En kvalifisert elektronisk signatur er knyttet til dataobjektet gjennom en kryptografisk algoritme slik at signaturen ikke validerer dersom dataobjektet endres. Ideen bak oppfinnelsen ligger imidlertid i at en kvalifisert elektronisk signatur kan løses fra sitt signaturobjekt og benyttes til å påføre en valid signatur på en kopi av signaturobjektet i et annet signaturinnpakkingsformat. Denne signaturporteringen kan utføres uten å involvere signatarer, sertifikatautoriteter. Avhengig av hvilke formater som konverteres fra og til vil det være behov å spesifisere noen basiskrav som originalsignaturen må støtte. For eksempel algoritme over beregning av hash, osv.

Beste måter å utføre oppfinnelsen på

Utførelseseksempelet av oppfinnelsen vist i Fig. 1 og 2 omfatter system med en signatur og system med flere signaturer på samme dokument, også kalt multisignatursystem.

Det er ønskelig å benytte BankID PKI og Buypass PKI til å signere PDF i PAdES format. I utgangspunktet vil vi støtte PAdES, part 4 LTV profile (Long term validation), men andre formater kan også implementeres.

På nåværende tidspunkt støtter imidlertid ikke BankID signering av PDF i Adobe PDF format, men kan returnere en SEID SDO fil (innpakkingsformat). Foreliggende oppfinnelse for signaturportering løser problemet ved å portere signaturene fra SDO til PAdES-formatet.

Buypass PKI leverandør har begrenset støtte for PDF signering, med begrensning i filstørrelse, samt manglende støtte for fullt PAdES LTV format. Buypass PKI leverandøren støtter imidlertid CMS CADES-BES formatet, og foreliggende oppfinnelse muliggjør derfor PAdES-signatur av PDF-dokumenter ved å portere signaturen fra CMS CADES-BES formatet til PAdES-formatet for PDF-dokumenter av vilkårlig størrelse.

Generelt i denne løsningen er at vi skal kunne portere en slik signatur hvis

1. PKI leverandør kan returnere en PKCS#7-kompatibel signatur blob (CMS eller CADES-BES) over data eller hash av data.
2. PKI leverandør kan prosessere data eller hash uten å anvende noen koding eller dekoding eller noe annet endring av data.
3. Det er ønskelig at PKI leverandør inkluderer all validerings informasjon (sertifikater, CRL og OCSP respons) som er nødvendig for å kunne lage langtids validering av alle involverte sertifikatkjeder. Dette inkluderer hovedsertifikatkjede fra sertifikatet som er brukt til signering til root sertifikatet. I tillegg er det ønskelig kjede av sertifikater for leverandører av valideringsinformasjon (OSCP tjenester, CRL utstedere og TSA) er inkludert.
4. Hvis PKI leverandør ikke inkluderer all nødvendig informasjon for validering, skal denne informasjonen kunne hentes på andre måter (for eksempel via online tjenester). All manglende valideringsinformasjon må være tilgjengelig enten som i form av sertifikater offline eller via online tjenester (CRL).

Fig. 1 viser informasjonsflyten i et signatursystem 100 med bare en enkelt bruker med tilhørende utstyr, fortrinnsvis samlokalisert, 200 som signerer et dokument 210. Brukeren begynner prosessen ved opplasting 211 av dokumentet 210 til signaturporteringssystemet 300.

Signaturporteringssystemet 300 omfatter en rekke komponenter som kan være samlokaliserte, og som i en typisk utførelse ikke ligger hos brukeren. I signaturporteringssystemet blir det mottatte opplastede dokument 210 forhåndsbehandlet og klargjort for signering 311 og lagres eller mellomlagres som et forhåndsbehandlet dokument 312 og som sendes til to forskjellige ruter i systemet.

I en første rute sendes 313 dokumentet som forespørsel om signering til PKI, og sendes da til Private Key Infrastructure, ofte forkortet som PKI 400 og omfatter en rekke delsystemer. Blant disse er PKI-løsningens lager av sertifikater og eventuelt nøkler 410. Denne krever autentisering, så en forespørsel om autentisering 411 overføres til brukeren 200, som bruker Smartkort, OTP generator, pinkoder eller passord 220 for dette. Responsen er at brukeren autentiserer seg 221 med passord, pinkoder, osv. til PKI 400 slik at PKI-løsningen signerer dokument med privat nøkkel og sertifikat 411. Deretter skjer levering 412 av signatur basert på bruker sine privatnøkler til Signaturporteringssystemet 300 som da skaper en digital signatur 320 i for eksempel SDO, CMS, PKS#7, XML eller andre formater. Deretter ekstraheres 321 signatur fra mottatt fil og overføres til en enhet for portering 330 av signaturen til PDF-dokumentet.

I en andre rute sendes 315 det forhåndsbehandlede dokument for sluttføring av signatur til enheten for portering 330 av signaturen til PDF-dokumentet. I denne prosessen tas signert melding digest ut fra det signerte dokumentet som er mottatt fra PKI og legges til forbehandlet PDF-dokumentet for sluttføring av signatur. I denne fasen mangler man tidstempel fra TSA og OSCP-oppslag.
Fra enheten for portering går prosessen til en enhet 331 for kobling til Time Stamping Authority, ofte forkortet TSA, for tidsstempling, og deretter en enhet 332 for å lage Online Certificate Status Protocol, ofte kalt OCSP, oppslag. TSA gir tid fra uavhengig tiltrodd tredjepart fra for eksempel atom-klokke. Tidsstempelet kan verifiseres og gir nødvendig bevis om signeringstidspunktet. OSCP-oppslag gjøres for å kunne verifisere gyldighet til brukersertifikat på signeringstidspunktet. Hvis for eksempel sertifikatet er utgått eller sperret må signeringsprosessen avbrytes. I tillegg lages LTV signatur hvor valideringsdata (CA-sertifikater, OSCP-oppslag eller CRL)

lagres sammen med dokumentet for å kunne brukes senere ved validering av digital signatur.

Til slutt i signaturporteringssystemet går dette til en enhet 333 for sluttføring av signering og lag PAdES dokument med LTV, og som returnerer til brukeren et digitalt signert PAdES PDF-dokument 230.

Fig. 2 viser skjematisk et eksempel 101 på multippel signering av et dokument av 2 brukere omfattende en første bruker 1200 og en andre bruker 2200 med 2 forskjellige PKI løsninger. Hver bruker omfatter tilhørende utstyr som fortrinnsvis er samlokalisert hos hver enkelt bruker, mens hver bruker kan være lokalisert separat.

I dette eksempelet signeres PDF-dokumentet fortrinnsvis først av Bruker_1 1200, deretter av Bruker_2 2200.
Bruker_1 1200 laster opp PDF-dokumentet 210 til Multi-signaturporteringssystemet 1300. Deretter behandles dokumentet i 1340 og lages dokument som sendes 1342 til signering til PKI system 1400. PKI systemet krever autentisering 1401 fra Bruker_1. Bruker_1 klargjør maskinvare nødvendig til autentisering (brikker, smartkort) 1212 og autentiserer seg 1213 med OTP, pinkoder, passord. På bakgrunn av det, lages signatur og sendes tilbake 1402 til Multi-signaturporteringssystemet 1300.
Signeringsprosessen sluttføres i 1343 med å kontakte OSCP og TSA servere og lagres som PAdES PDF-dokument med LTV 1230. Deretter forbehandles dette dokumentet i 2340 for klargjøring til signering av Bruker_2 2200. Bruker_2 kan ha tilgang ti en annen PKI løsning 2400. Dokumentet som er forbehandlet i 2340 sendes 2342 til PKI system 2400 til signering. Bruker_2 får forespørsel 2401 om autentisering, klargjør smartkort, brikker 2212 og autentiserer seg 2213 med pinkoder, OTP eller passord. PKI 2400 lager digital signatur.
Når signaturen overføres tilbake 2402 til Multi-siganturporteringssystemet 1300, sluttføres signeringsprosessen i 2343 ved å portere signatur, samt gjøre oppslag til OSCP og TSA server og tidsstempling for laging av PAdES LTV signatur.
Det signerte dokumentet 12230 lagres klar til nedlasting. Til slutt kan dokumentet 12230 som har nå signaturer fra begge brukere lastes ned 1344 av Bruker_1 for lagring lokalt 1344 og lastes ned 2344 av Bruker_2 for lagring lokalt.
Bruker_1 har signert det originale dokumentet, mens Bruker2 har signert original dokumentet med signatur fra Bruker1.

Merk at multisignering skjer ved å kjede sammen en prosess. I eksempelet over er det overføringen 1343 som knytter signeringsprosessen fra bruker_1 sammen med signeringsprosessen for bruker_2. Det er derfor mulig å utvide prosessen til fler enn 2 brukere ved å fortsette kjedingen. En slik kjede omfatter typisk

en oppstart der en første bruker laster opp et dokument som skal signeres,
en signering for hver enkelt bruker, og
en avslutning, der dokumentet sammenstilles og overføres til hver enkelt som skal motta dokumentet.

Typisk er mottakerne de samme som signerte dokumentet.

Fig. 3 viser skjematisk en struktur 500 av et signert PDF-dokument, omfattende innhold 510, et sertifikat 511, en signert melding digest 512, og et tidsstempel 513.

Ytterligere utførelsesformer

En kan se for seg en rekke variasjoner over overstående, men som ikke er en del av kravomfanget. Eksempelvis muliggjør signaturportering så lenge noen det finnes algoritmisk kompatibilitet mellom formatene.

Man kan også tenke seg å kunne lage en del av signaturen offline, for eksempel så lenge man sitter med private nøkler for deretter å legge til annet informasjon tilgjengelig online for å imøtekomme standardene.

Industriell anvendbarhet

Oppfinnelsen finner sin nytte ved bruk i av digital signering av dokumenter.

Patentkrav

1. Fremgangsmåte for digital signering av dokumenter (210) av en bruker (200) omfattende trinnene:

mottak (211) av et dokument (210),

klargjøring for signering (311) og lagring eller mellomlagring som et forhåndsbehandlet dokument (312),

overføring (313) av det forhåndsbehandlede dokument som forespørsel om signering til PKI,

mottak (412) av signatur fra PKI,

skape en digital signatur (320),

ekstrahering (321) av signatur fra mottatt signatur fra PKI og overføring til en enhet for portering (330) av signaturen,

overføring (315) av det forhåndsbehandlede dokumentet for sluttføring av signatur til enheten for portering (330) av signaturen til dokumentet,

tidsstempling (331),

oppslag for å lage OCSP (332),

sluttføring av signering (333), og

returnering av signert dokument (230),

karakterisert ved at brukeren (200) signerer med sin egen private nøkkel.

2. Fremgangsmåte ifølge krav 1, karakterisert ved at sluttføring av signering lager et PAdES-dokument med LTV.

3. Fremgangsmåte for digital multisignering av dokumenter (210) omfattende trinnene:

mottak (211) av et dokument (210),

signering av minst en bruker (200, 1200, 2200) omfattende

klargjøring for signering (311) og lagring eller mellomlagring som et forhåndsbehandlet dokument (312),

overføring (313) av det forhåndsbehandlede dokument som forespørsel om signering til PKI,

mottak (412) av signatur fra PKI,

skape en digital signatur (320),

ekstrahering (321) av signatur fra mottatt signatur fra PKI og overføring til en enhet for portering (330) av signaturen,

overføring (315) av det forhåndsbehandlede dokumentet for sluttføring av signatur til enheten for portering (330) av signaturen til dokumentet,

tidsstempling (331),

oppslag for å lage OCSP (332),

sluttføring av signering (333), og

overføring (2340) til en påfølgende bruker (2200) for signering,

returnering (1344, 2344) av signert dokument (230, 12230),

karakterisert ved at brukerne (200, 1200, 2200) signerer med egen private nøkkel.

4. Fremgangsmåte ifølge krav 3, karakterisert ved at sluttføring av signering lager et PAdES-dokument med LTV.

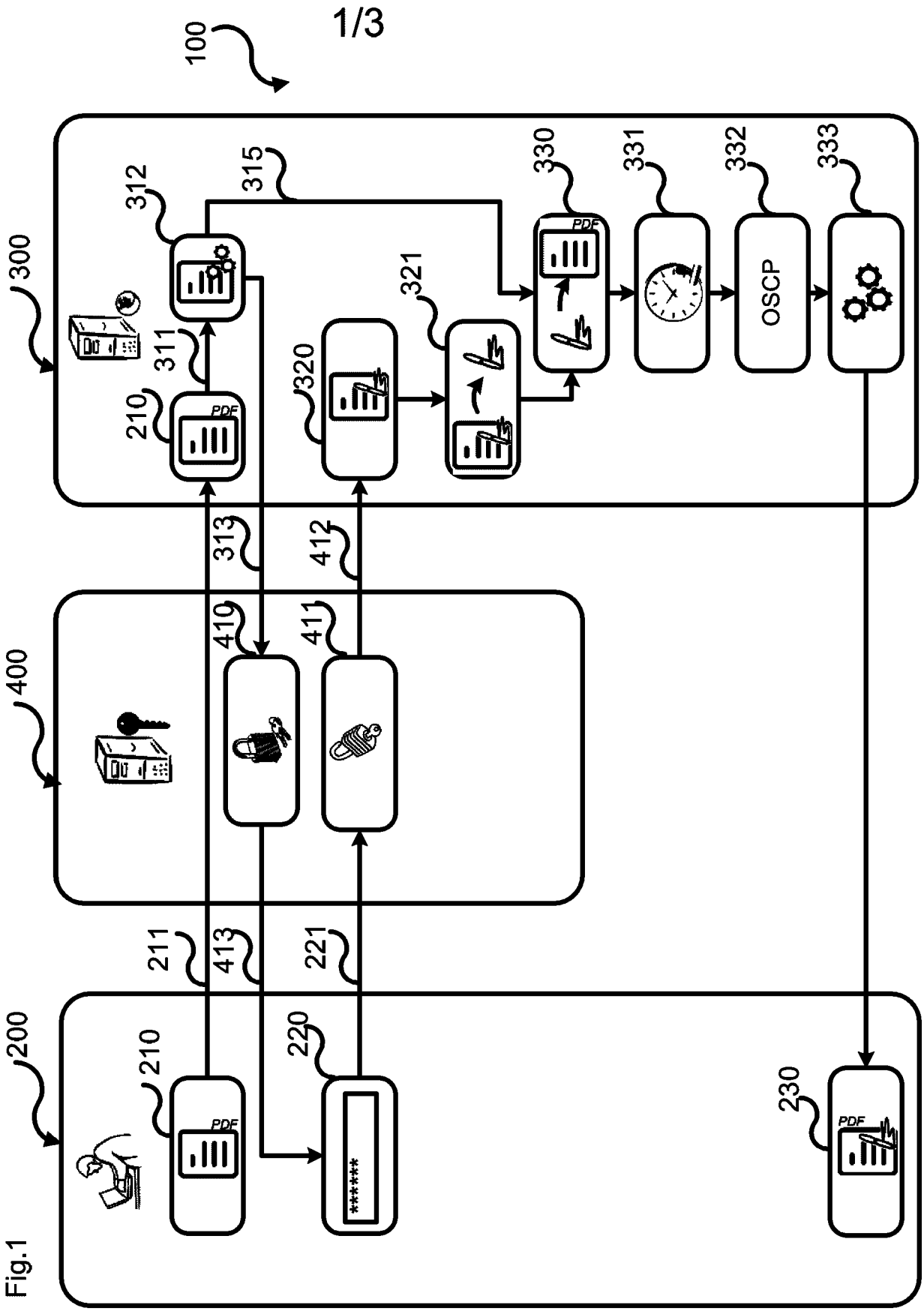

100
200
210
PDF
211
220
****
221
230
PDF
300
310
311
PDF
312
313
315
320
321
330
PDF
331
332
OSCP
333
400
410
411
412
413

Fig.1

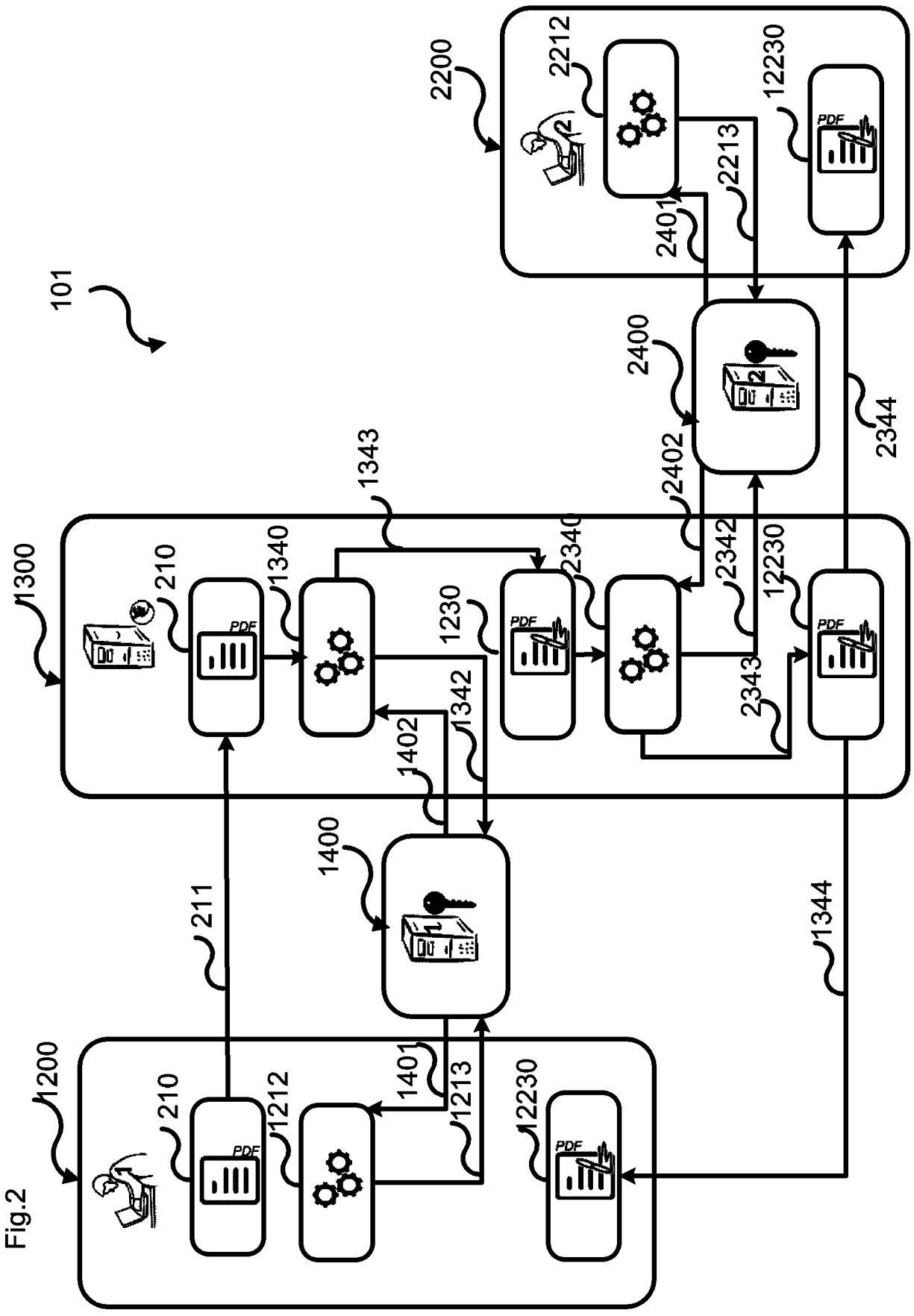

101
1200
210
1212
1401
1213
12230
1400
211
1344
1300
210
1340
1343
1230
2340
1342
1402
2342
12230
2343
2344
2400
2402
2200
2212
2213
12230
2401
PDF

Fig.2

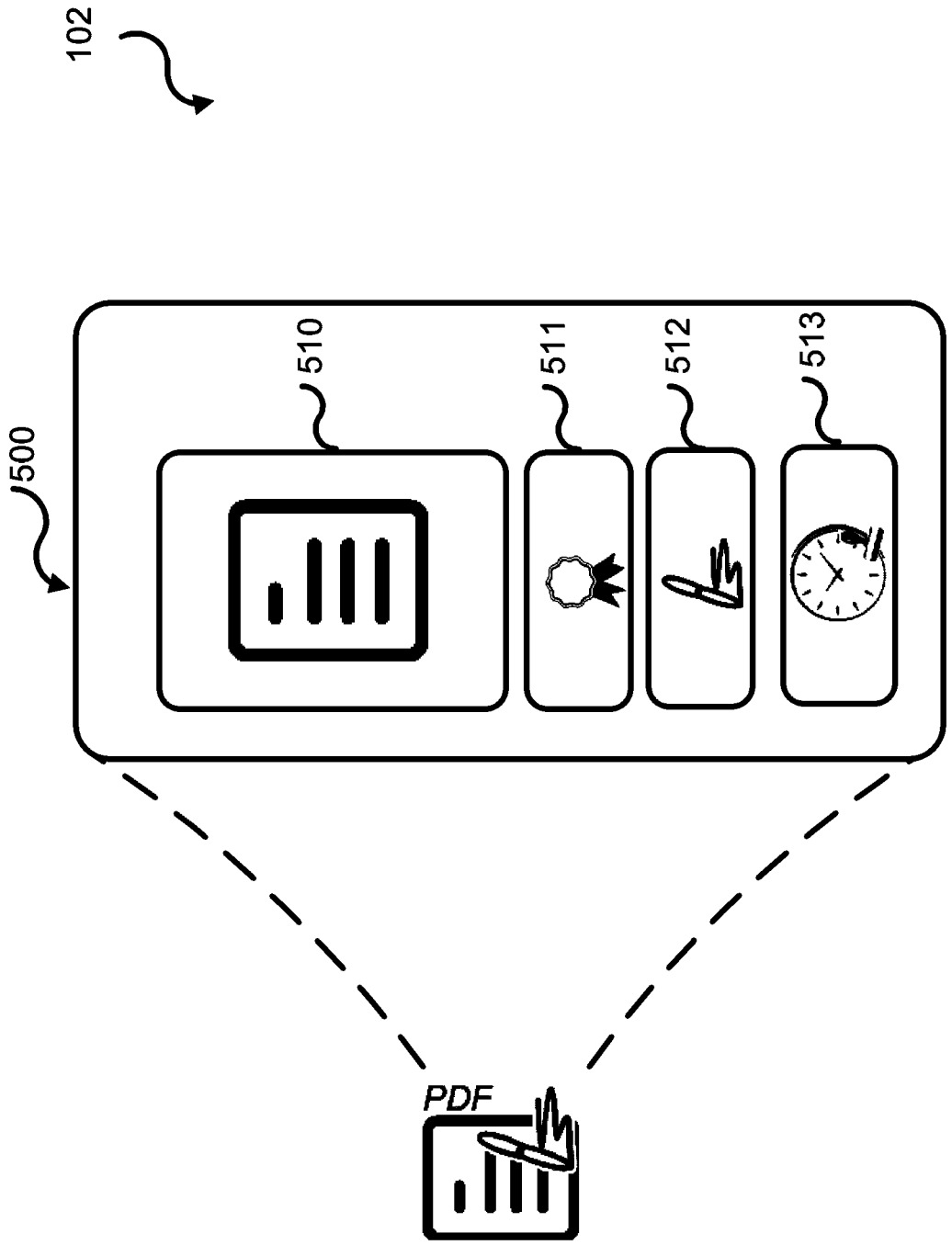


Fig.3