

Spårbarhet (i rettsinformationsforsörjningen) – presentasjon for Föreningen Rättsinformation, Stockholm 29. november 2007

*Rolf Riisnæs, advokat dr. juris, advokatfirmaet Wikborg Rein (Oslo)*¹

1. Definisjon og problemstilling

Jeg er invitert til å si noen ord om sporbarhet. Med sporbarhet mener jeg i denne sammenheng muligheten for å fastlegge for eksempel:

- *hvem* som har opprettet en tekst eller utstedt et dokument, eller
- på hvilket *tidspunkt* eller
- i hvilken *sammenheng* et dokument er opprettet.

Spørsmålet er:

- *hvilke* krav som stilles til sporbarhet for normerende rettslige tekster,
- *hvor* eller hvordan slike krav er *forankret* og
- *hvordan* de eventuelt kan oppfylles.

Eksemplene jeg benytter er hentet fra norsk rett, men prinsippene er nok allmenne.

2. Om normerende tekster

De normerende tekster kan grovt sett deles i to: generelle og individuelle. Vi kjenner skillet typisk i forholdet mellom lov/forskrift på den ene siden og enkeltvedtak/dom på den annen side.

Det som preger begge grupper, er at de er underlagt *særlige form- og kompetanseregler*, både når det gjelder:

- deres *tilblivelse*, og når det gjelder
- *hvordan resultatet skal formidles* til, eller gjøres tilgjengelig for, de det angår.

¹ Wikborg Rein er blant Norges største advokatfirmaer og sysselsetter i dag ca 170 advokater. Rolf Riisnæs arbeider særlig med spørsmål knyttet til elektronisk forvaltning, informasjonssikkerhet, personvern og IKT-kontrakter. Han ble dr. juris i 2006 på sin avhandling *Digitale sertifikater og sertifikattjenester – roller, oppgaver og ansvar*, Fagbokforlaget 2007, ISBN 978-82-450-0589-9. E-post: rri@wr.no. (Referanser til flere publikasjoner på siste side.)

Dette er typisk regler om *hvem* som kan treffe vedtak eller fastlegge generelle regler av en spesiell type og *hvordan* man skal gå frem i forbindelse med at vedtak skal treffes eller regler skal fastsettes. I tillegg vil det gjerne finnes krav til *distribusjon* av vedtaket eller til *publisering* og tilgjengeliggjøring av reglene.

Vi har for eksempel Grunnlovens bestemmelser om hvordan det norske Storting går frem når de gir lover, og om Kongens sanksjon. Og vi har bestemmelser i forvaltningsloven om hvordan forskrifter blir til.

2.1 Generelle regler

Generelle regler publiseres typisk i en dertil egnet offentlig trykksak. I Norge i Norsk Lovtidend. Dette er bestemt ved egen lov. Det samme er for forskrifter bestemt i forvaltningsloven. Og forskriftene kan ikke påberopes overfor dem den før den er publisert.

Lovtidend trykkes på grunnlag av den elektroniske databasen hos stiftelsen Lovdata. Slik har man nå sikret at det som er fritt tilgjengelig elektronisk er identisk med det som er trykket i den offisielle publikasjonen.

Disse rammer omkring tilblivelse og tilgjengeliggjøring av normerende tekster skaper tradisjonelt forholdsvis stor grad av både forutberegnelighet og sporbarhet knyttet til tekstens grunnlag og innhold.

2.2 Individuelle vedtak

Individuelle vedtak følger naturligvis en annen rute. Individuelle vedtak formidles tradisjonelt til den det gjelder i form av *papirdokument* som etter sitt eget innhold, for eksempel fordi det er benyttet et lett gjenkjennelig brevark, tydelig stammer fra vedkommende offentlige myndighet. Og det fremsendes til den det gjelder ved hjelp av postvesenet som kan bidra til å skape sannsynlighet for den tidsmessige sammenhengen mellom tidspunktet da vedtaket ble truffet, eller i alle fall formidlet, og det tidspunkt da det ble mottatt.

Vanligvis vil det derfor være mulig, uten for store problemer, å fastlegge entydig hvilke normerende tekster som er vedtatt, av hvem de er vedtatt og på hvilket tidspunkt de kan gjøres gjeldende.

3. Publisering i elektronisk form

Utfordringene blir større når tekstene gjøres tilgjengelige i elektronisk form og spres ved hjelp av elektronisk kommunikasjon. Jeg vil belyse noen av de utfordringer dette reiser med noen eksempler på hvordan vi har håndtert dette i Norge.

Utfordringene gjelder, slik jeg ser det, særlig for individuelt normerende tekster, eller enkeltvedtak som det kalles i Norge. Det vil si avgjørelser som er bestemmende for enkeltpersoners rettigheter eller plikter. Jeg kommer straks tilbake til det.

Men også for generelle vedtak, reiser kommunikasjonsformen visse nye utfordringer.

For eksempel vil muligheten for publisering på de enkelte forvaltningsorganers egne nettsteder skape et press mot troverdigheten til materialet, i forhold til om de enkelte kopier er oppdaterte. Har man funnet siste versjon av den aktuelle teksten? Er det kommet endringer eller relevante tillegg som ikke fremgår her?

Et praktisk og meget uheldig eksempel er den norske eForvaltningsforskriften. Forskrift om elektronisk kommunikasjon med og i offentlig forvaltning. Forskriften nedfeller rammebetingelsene for *forvaltningens bruk av elektronisk kommunikasjon med borgerne og med hverandre*, også i forbindelse med prosesser som ender i normerende vedtak.

Forskriften forvaltes av Fornyings- og administrasjonsdepartementet, tidligere Moderniseringsdepartementet. Forskriften var tilgjengelig i fulltekst på departementets nettsider.

Forskriften, som først ble vedtatt i 2002, hadde en såkalt solnedgangsbestemmelse, som innebar at den ville opphøre å gjelde etter to år dersom den ikke ble fornyet. Som følge av dette ble forskriften grundig evaluert i god tid før den utløp. Det ble konstatert at forskriften var lite kjent og at den var til dels vanskelig å forstå, men at den innholdsmessig måtte videreføres. En revidert forskrift

ble derfor utarbeidet og den trådte i kraft 1. juli 2004, den dagen den opprinnelige forskriften etter sin ordlyd opphørte.

I oktober 2004, fire måneder etter at den nye forskriften ble vedtatt, var det fortsatt den gamle forskriften som lå ute på det ansvarlige departementets hjemmesider. Jeg oppdaget det ved en tilfeldighet, fordi jeg fant en utskrift av den gamle forskriften i skriveren på universitetet. Jeg gjorde vedkommende som hadde skrevet den ut oppmerksom på at det var kommet en ny forskrift, og han uttrykte bestyrtet at: ”Jammen, jeg har jo skrevet den ut fra departementets hjemmeside!” Dette er nok et tegn på at forskriften på det aktuelle tidspunkt var lite kjent. Men at departementet med ansvar for it-politikken ikke var i stand til å holde oppdatert sine egne regler om bruk av elektronisk kommunikasjon er et grelt eksempel.

Eksempelet synliggjør utfordringen med oppdatering av distribuerte tekster. I dette tilfellet var problemet forsterket ved at det var regelverksforvalter selv som ikke var oppdatert. Hadde det vært et underordnet organ, eller en annen nettside, ville en bruker hatt større foranledning til å kontrollere om det var skjedd endringer siden dokumentet ble publisert. Men når *kilden* var selve dokumentets utsteder, eier, forvalter, er det mindre nærliggende å utføre videre kontroller.

I dag lenker de fleste offentlige nettsted, i alle fall de statlige organer, direkte til forskriftsdata-basen i Lovdata, som inneholder de til enhver tid gjeldende tekster. Alle norske bestemmelser på lov og forskriftsnivå skal nå via Lovdata for publisering.

Det innebærer at hvis en forskrift er opphevet uten at lenken til Lovdata er oppdatert vil brukeren bli oppmerksom på det. Det er også mulig å knytte lenken til hjemmelsbestemmelsen, slik at eventuelle nye forskrifter med hjemmel i samme lov fanges opp automatisk.

Når det gjelder individuelle vedtak er utfordringene større.

De alminnelige regler vi har om formidling av individuelle avgjørelser, enkeltvedtak, bygger på en del ikke uttalte forutsetninger om hvordan formidling skjer.

Forvaltningsloven stiller krav om at underretning om enkeltvedtak skal skje skriftlig til den vedtaket gjelder. Skriftlighetskravet i

forvaltningsloven fra 1967 ble nok opprinnelig oppfattet som *motsetningen til muntlighet*. Og det *praktiske* alternativet for et skriftlig vedtak var i form av et papirdokument.

Når kravet var begrenset til skriftlighet bygde det ganske sikkert også på noen andre forutsetninger – som ikke var uttalt i loven. Blant annet en forutsetning om at vi har et rimelig velfungerende postvesen, som faktisk bringer de fleste brev frem til adressaten innen rimelig tid. Og en forutsetning om at *i alle fall de fleste* personer faktisk sjekker postkassen sin jevnlig, og at de stort sett leser brev de mottar fra det offentlige. Slike forutsetninger kan vi ikke uten videre operere med, i alle fall ikke foreløpig, når det benyttes elektronisk kommunikasjon.

Dette kan utløse krav til sporbarhet, bl.a. i forhold til om en handling (vedtak) har kommet frem til rette vedkommende, og i forhold til hvordan en handling kan dokumenteres over tid, eller overfor tredjepart.

I det følgende vil jeg knytte enkelte merknader til noen av de utfordringer og løsninger vi har knyttet til:

- Formidling av vedtak
- Herunder bruk av virksomhetssertifikater
- Oppbevaring av elektronisk signert materiale
- Innsyn i og utlevering av elektronisk signert materiale

Alle disse forhold er behandlet i den norske eForvaltningsforskriften.²

4. Formidling av vedtak

For formidling av vedtak gjelder som nevnt et skriftlighetskrav. Skriftlighetskravet i forvaltningsloven er nå definert slik at det også omfatter bruk av ”elektronisk melding når informasjonen i denne er tilgjengelig også for ettertiden”. Det er også åpnet for at formidling av vedtak kan skje i elektronisk form dersom den vedtaket retter seg mot *uttrykkelig har godtatt dette* og oppgitt den elektroniske adressen som varsel om vedtak skal sendes til (forvaltningsloven § 27).³

² Se <http://www.lovdata.no/for/sf/fa/fa-20040625-0988.html>

³ Se <http://www.lovdata.no/all/tl-19670210-000-005.html#27>

eForvaltningsforskriften (§ 8) inneholder mer detaljerte regler om hvordan formidling av vedtak skal foregå. Stikkordsmessig er det særlig tre forhold forskriften dekker. Det er krav til:

- 1) at bare rette vedkommende får tilgang til vedtaket,
- 2) at rette vedkommende har reelle muligheter til å gjøre seg kjent med vedtaket, og
- 3) at vedkommende har mulighet for å sikre seg at det faktisk er forvaltningsorganet som står bak vedtaket.

Bakgrunnen er at forvaltningens vedtak forutsetningsvis har betydning for våre rettigheter og plikter, og at det derfor ikke er likegyldig om vi blir kjent med dem eller ikke. Forskriften har derfor bygget inn mekanismer, bl.a. krav til sporbarhet, som skal sikre at ingen lider rettstap som følge av at vedtak ikke kommer frem, eller at den det gjelder av en eller annen grunn ikke blir oppmerksom på vedtaket eller ikke er i stand til å få tak i det.

4.1 Mulighet til å skaffe seg tilgang

Den første hovedtypen av utfordringer er altså knyttet til at rette vedkommende faktisk har *reell mulighet* til å skaffe seg kunnskap om vedtaket, og at det finnes reserveløsninger som sikrer at ikke vedkommende lider rettstap som følge av at han ikke blir kjent med det, som følge av omstendigheter han ikke selv rår over.

Den norske ordningen er derfor at underretning om vedtak kan skje i elektronisk form hvis den vedtaket retter seg mot uttrykkelig har godtatt det og oppgitt den elektroniske adressen som varsel om vedtaket skal sendes til. Dette kan være en e-postadresse, et mobiltelefonnummer for mottak av SMS, eller i prinsippet en nettbankkonto eller en personlig hjemmeside på en offentlig portal, det som i Norge går under navnet Min Side.

Poenget er at vedkommende varsles om at vedtak er fattet på en måte han selv har valgt, på en adresse vedkommende vanligvis benytter. Varsel skal inneholde opplysninger om hvordan mottakeren kan skaffe seg tilgang til vedtaket. Vanligvis i form av en lenke til en offentlig portal der vedtaket er lagt ut, og gjøres tilgjengelig for mottakeren når mottakeren autentiserer seg overfor portalen.

På denne måten sikres at bare rette vedkommende får tilgang til vedtaket.

4.2 Taushetsplikt

Forvaltningens vedtak vil i mange tilfeller være underlagt taushetsplikt, eller være knyttet til behandling av personopplysninger. Forskriften stiller derfor krav om at forvaltningsorganet skal sikre at bare rette vedkommende kan skaffe seg tilgang til vedtaket, og lagre data som dokumenterer at det var rette vedkommende som skaffet seg tilgang til vedtaket.

4.3 Reserveløsning

Men ordningen har også en annen hovedfunksjon. Forvaltningsorganet skal nemlig innrette seg slik at de kan kontrollere og dokumentere at mottakeren har skaffet seg tilgang til vedtaket, og om så ikke har skjedd innen en frist på syv dager, sende ut vedtaket på tradisjonell måte som om det ikke var gitt samtykke til bruk av elektronisk kommunikasjon.

På denne måten, ved å registrere opplysninger om tilgang (sporing), forsøker man å ivareta interessene til den som *har* samtykket i underretning i elektronisk form, men som av en eller annen grunn ikke kan eller vil benytte de aktuelle tjenestene.

4.4 Autentisering av forvaltningsorganet

Det andre spørsmålet er hvorledes den vedtaket retter seg mot skal kunne vite at det er forvaltningsorganet som er avsender eller som står bak vedtaket.

Det er tradisjon for å sende ut vedtak skriftlig, på forvaltningsorganets brevark, i konvolutter som identifiserer forvaltningsorganet. Og en bemyndiget person vil gjerne ha underskrevet vedtaket. Mottakeren vil imidlertid sjelden kunne verifisere underskriften, eller at det er rette person som har underskrevet. I praksis må mottakeren stole på at når vedtaket ser ut til å komme fra forvaltningsorganet, så gjør det det, og stole på at

forvaltningsorganet har rutiner som sikrer at rette vedkommende har undertegnet og ekspedert vedtaket.

Det mottakeren i praksis har behov for å få bekreftet er at forvaltningsorganet står bak vedtaket, ikke den enkelte saksbehandler. Etersom det siste er noe mottakeren uansett ikke kan få verifisert, må han sette sin lit til at de interne rutineene sikrer at prosedyrene er fulgt.

Derfor stiller eForvaltningsforskriften ingen krav om at saksbehandler eller bemyndiget skal signere vedtak elektronisk. Derimot forutsetter forskriften at det benyttes virksomhetssertifikater i forbindelse med underretning om vedtak i elektronisk form (eForvaltningsforskriften § 14).

4.5 Virksomhetssertifikater

Et virksomhetssertifikat er et sertifikat som identifiserer en virksomhet, i dette tilfellet et forvaltningsorgan, som inneholder av sertifikatet, i stedet for en fysisk person. Personen ville i så fall vært kalt undertegner i esignaturdirektivets terminologi.

Virksomhetssertifikater kan benyttes enten for signering av vedtak på vegne av forvaltningsorganet. Eller om man vil, påføring av et digitalt stempel på vegne av organet. Jeg mener terminologien er underordnet her. Poenget er at det benyttes prosesser som etablerer en kopling mellom den *tekst* som representerer vedtaket og det *forvaltningsorgan* som står bak vedtaket. Alternativt kan virksomhetssertifikatet benyttes for å autentisere forvaltningsorganet som kilde i forbindelse med at den vedtaket retter seg mot laster det ned, eller på annen måte skaffer seg tilgang til det fra forvaltningsorganets nettsted. Typisk i form av et serversertifikat som autentiserer forvaltningsorganet som inneholder at det nettstedet vedtaket gjøres tilgjengelig fra. Dette kan gjøres uten at man benytter signeringsteknologi knyttet til selve vedtaket.

5. Oppbevaring og utlevering av vedtak

I forlengelsen av elektronisk formidling av vedtak får forvaltningen også en annen oppgave. Nemlig å holde relevante opplysninger og dokumenter tilgjengelig også for partene over tid (eForvaltningsforskriften §§ 10 og 26).

Vi har tradisjon for både alminnelig innsynsrett og partsinnsyn, men perspektivet er i eforvaltningsforskriften utvidet til at forvaltningsorganet skal oppbevare materiale også på vegne av den vedtaket gjelder. På en måte kan vi snakke om at forvaltningsorganet også skal tilby å forvalte partenes private arkiv.

Dette skyldes bl.a. at det er de færreste av oss som er i stand til, på en forsvarlig måte, å forvalte elektroniske dokumenter over lang tid. Hvor mange av oss har for eksempel full oversikt over egen e-post og elektroniske dokumenter mer enn et par år tilbake.

Og det er ikke alle elektroniske dokumenter som lar seg skrive ut hvis de på en troverdig måte skal kunne formidles videre.

Dette siste har foranlediget et krav om at forvaltningsorganet, på begjæring, skal kunne utlevere signerte dokumenter sammen med de sertifikater og andre opplysninger som er nødvendige for å verifisere dem, eller på annen måte kunne tilby en bekreftet kopi av det aktuelle dokumentet.

Dette kan være aktuelt dersom den dokumentet direkte gjelder har behov for å påberope det overfor en tredjepart, for eksempel en domstol, eller overfor en nabo eller et annet forvaltningsorgan.

I denne sammenheng sikres sporbarhet ved at dokumentene hele tiden gjøres tilgjengelig fra forvaltningens eget system, og ved at forvaltningen må vedlikeholde verifiserbarheten av elektroniske signaturer, eller på annen måte tilby en bekreftet kopi av dokumentet.

6. Arkiv

Kravene henger sammen med krav til forvaltningens egen oppbevaring av dokumenter som er signert med elektronisk signatur.

Det er betydelige utfordringer knyttet til oppbevaring av elektronisk signert materiale over tid.

eForvaltningsforskriften (§ 26) stiller derfor krav om at dokumentet skal lagres sammen med signaturen og de øvrige opplysninger som er nødvendig for senere å kunne verifisere signaturen, typisk relevante sertifikater og opplysninger om sertifikatets status på signerings eller verifiseringstidspunktet.

I mange tilfeller vil det imidlertid være behov for å konvertere dokumentet til et annet format i forbindelse med lagring. Da kan den elektroniske signaturen ikke lenger verifiseres. I disse tilfellene må arkivet i henhold til forskriften overta ansvaret for sporbarheten ved å verifisere signaturen i forbindelse med arkivering, og lagre den sammen med relevante opplysninger fra sertifikatet på en måte som sikrer meldingens integritet over tid.

Og det er naturligvis en sammenheng med reglene om utlevering av dokumenter som jeg nettopp snakket om. Arkivet må innrettes slik at forvaltningsorganet er i stand til å oppfylle sine plikter til utlevering av verifiserbare signaturer eller på annen måte bekrefte kopier som er egnet som dokumentasjon overfor tredjepart.

7. Rekonstruksjon av hendelsesforløp – hva som ligger bak et signert dokument når det er resultatet av en prosess

En av de store utfordringer vi står overfor når det gjelder elektronisk samhandling, er at den dokumentasjon vi ender opp med, og som arkiveres, ofte er resultatet av en prosess, der en person gjennom dialog med et informasjonssystem har tilegnet seg informasjon, bearbeidet informasjon og avgitt informasjon, vanligvis i form av svar på spørsmål systemet har stilt i løpet av prosessen. Typisk at brukeren ledes gjennom et antall sider som dels orienterer, dels samler inn opplysninger. Arbeidsflytverktøy styrer denne prosessen, og kan tilrettelegge den for den enkelte bruker. Dette kan for

eksempel føre til at ulike brukere får ulik informasjon og valg fordi de har svart ulikt på innledende spørsmål.

Vi opplever i mange sammenhenger at det er veldig fokus på det signerte dokumentet som arkiveres som resultat av en slik prosess, og verdien av signaturen som dokumentasjon for de faktiske forhold. Men like viktig som signaturen og innholdet i det signerte dokumentet, er å kunne dokumentere den *prosessen* brukeren gikk igjennom, og som ledet frem til det signerte dokumentet som kanskje skal legges til grunn for et normerende vedtak.

I tradisjonell, papirbasert samhandling, vil de rettslige virkningene av den disposisjon personen har foretatt i mange tilfelle kunne knyttes direkte til innholdet i et dokument, typisk en papirblankett (eller et skjema). Ved gå gjennom det utfylte skjemaet får man et inntrykk av hva parten har svart på og hvordan det er svart.

I systemer for elektronisk samhandling vil det i mange tilfeller ikke være noen slik kopling mellom det brukeren opplevde i systemdialogen, og den måte resultatet av arbeidsprosessen er oppsummert i et signert dokument. Det signerte materiale vil typisk representere et uttrekk av de data som har vært involvert. (Det er altså ikke skjemapresentasjonen/skjermbildene slik brukeren opplevde det som er signert.)

Det skal i denne sammenheng legges til at signeringsoperasjonen ofte styres av saksbehandlingssystemet og er i realiteten utenfor brukerens kontroll. I interaktive systemer er det ikke slik at brukeren på sin lokale maskin fremstiller et dokument som han så signerer og sender.

Det vil nok snarere være slik at saksbehandlingssystemet, som en del av prosessen, tilrettelegger de data som skal signeres og oversender hashverdien av disse til brukerens klient for signering.

Brukeren er i disse tilfellene helt ute av stand til å kontrollere hva som faktisk går til signering, og tilliten til sporbarheten i systemløsningen blir derfor avgjørende for troverdigheten til det signerte materialet.

Av det signerte materiale kan man for eksempel konstatere om vedkommende svarte ja eller nei på et spørsmål, hvilke tall vedkommende oppga i et felt for inntekt mv. Men for å kunne gjøre

seg opp en mening om hva personen faktisk forstod, eller burde forstå, må vi også vurdere de spørsmålene eller ledetekstene som svarene relaterer seg til. Og vi må kanskje ta stilling til hele den prosessen brukeren ble ledet gjennom, og vurdere hvorledes det inntrykk prosessen var egnet til å etterlate hos brukeren kunne påvirke vedkommendes oppfatning av spørsmålene underveis.

Vi har eksempler på moderne saksbehandlingssystemer som signerer felter som brukeren aldri har blitt konfrontert med pga sporvalg, datoer som forekommer (skjult) flere steder mv. Dette er opplysninger som, når de settes inn i rette sammenheng, selvfølgelig ikke er til skade for brukeren, men bare tanken på at det faktisk signeres uttrekk av felter som brukeren aldri har sett kan innebære et press mot troverdigheten til systemløsningen.

Dette innebærer at verdien av det signerte materiale ikke kan måles uavhengig av de tiltak som er etablert med hensyn til sporbarhet mellom det signerte materialet som er resultatet av en arbeidsprosess, og dokumentasjonen for hvorledes selve prosessen forløp.

Det betyr at bl.a. opplysninger om gjeldende versjon av skjemadefinisjoner, arbeidsflyt og regelhåndteringsverktøy må kunne identifiseres med referanse fra det signerte materialet eller med kopling til det tidspunkt prosessen ble registrert gjennomført.

Dette kan antakelig håndteres enten ved hjelp av signerte attributter, definert innenfor rammen av en veldefinert signaturpolicy eller som lagrede revisjonsspor i tilknytning til den signerte melding, i begge tilfeller med referanse til systematisk og dokumentert lagring av alle relevante versjoner av skjemaer, arbeidsflyt og regelhåndteringsverktøy med angivelse av tidsmessig tilknytning.

Vi har ikke eksplisitte rettslige krav om lagring av slik sporingsinformasjon Norge, men det er antakelig helt nødvendig for å kunne føre fyllestgjørende og troverdig bevis for et hendelsesforløp.

Følgelig bør det antakelig anses som et grunnleggende krav til forsvarlig innretning av denne type systemer, selv om det ikke har kommet til uttrykk i noen skrevet regel.

Rolf Riisnæs har innenfor emnet publisert blant annet:

- *Digitale sertifikater og sertifikattjenester - roller, oppgaver og ansvar*, Fagbokforlaget (2007)
- *Regelverksutvikling og brukerdeltakelse i eForvaltningen*, i Dag Wiese Schartum (red.), Elektronisk forvaltning i Norden, Fagbokforlaget (2007)
- *Sikker elektronisk samhandling med og i forvaltningen (eForvaltningsforskriften)*, i Arild Jansen og Dag Wiese Schartum (red.), Informasjonssikkerhet - Rettslige krav til sikker bruk av IKT, Fagbokforlaget (2005)
- *Digital Certificates and Certification Services*, i Peter Wahlgren (ed), IT Law, Scandinavian Studies in Law Volume 47, Stockholm Institute for Scandinavian Law (2004)