RIKSARKIVAREN

Fornyings- og administrasjonsdepartementet
v/ Eivind Jahren
Postboks 8004 Dep.
0030 Oslo

Deres ref	Vår ref.	Dato
200700605-KDB	2007/5866 ANNDOR	14.05.2007

Høring - Forslag til strategi for bruk av eID og e-signatur i offentlig sektor

Vi viser til høringsbrev fra Fornyingsdepartementet datert 12.03.2007 med forslag til strategi for bruk av eID og e-signatur i offentlig sektor.

I høringsbrevet er det satt opp en del punkter som høringsinstansene blir bedt om å svare på. De fleste av disse punktene er av en slik type at det ikke berører Riksarkivarens virksomhet, og Riksarkivaren har derfor ingen synspunkter på dem. Riksarkivaren har heller ingen planer om snarlig realisering av elektroniske tjenester med behov for elD, og har derfor ingen synspunkter på tidsløpet eller forretningsmodellen.

Derimot ønsker Riksarkivaren å komme med sine synspunkter i forhold til innsynsarkiv og autentiserende metadata.

Innsynsarkiv

Et arkiv i arkivlovens forstand er dokumenter som blir til som ledd i den virksomheten et forvaltningsorgan, en organisasjon, et selskap, en person el. bedriver. Et dokument er å forstå som en logisk avgrenset informasjonsmengde, som er lagret på et medium for senere lesing, lytting, visning eller overføring.

Mer spesifikt kan man si at et arkiv består av dokumenter som mottas eller produseres som ledd i den virksomhet man utøver, med tilhørende spor etter aktiviteter, transaksjoner, beslutninger ol. Verken i arkivloven eller i forskriftene er det foretatt begrensninger i forhold til bestemte typer dokumenter, transaksjoner, framstillingsverktøy, system e.l., rent bortsett fra at dokument som verken er gjenstand for saksbehandling eller har verdi som dokumentasjon, skal holdes utenfor eller fjernes fra arkivet. De vanligste arkivene består av saksdokumenter – men også elektroniske registre, databaser og fagsystem er arkiv i arkivlovens forstand.

Postadresse:	Kontoradresse:	Organisasjonsnr.	Telefon : 22 02 26 00	Telefaks: 22 23 74 89
Pb. 4013 Ullevål Stadion	Folke Bernadottes vei 21	961 181 399	www.arkivverket.no/riksarkivet	
0806 OSLO			riksarkivet@arkivverket.no	

I Strategi for eID og e-signatur i offentlig sektor omtales ”innsynsarkiv” flere steder, men slik vi leser det defineres begrepet på ulike måter:

- På s. 8 defineres innsynsarkiv som ”Et arkiv som tjenesteyter gjør tilgjengelig for sluttbruker…”.
- På s. 17 forklares begrepet slik: ”Digitalt arkiv (innsynsarkiv) for signerte dokumenter/hash-verdier, som et tilbud til de virksomheter som selv ikke vil ha tekniske forutsetninger til å lagre digitalt signerte dokumenter over lengre tid”.
- På s. 51 står det ”Tiltrodd digitalt arkiv over signerte dokumenter eller signerte hash-verdier (dokument-fineravtrykk), s.k. innsynsarkiv
- På s. 52 står det: ”Digitalt arkiv er en tjeneste som henger tett sammen med tjeneste for signering. Det vil teknisk sett kunne være vanskelig å introdusere en tjeneste for digitalt arkiv etter at tjeneste for signering er etablert. Behovet for slikt arkiv oppstår i hovedsak av to årsaker (som også kan være komplementære):
    1. vanskeligheter med å håndtere digitalt signerte dokumenter hos mindre aktører
    2. behov for kopilager av elektroniske dokumenter som er digitalt signert og som skal gis tilgang til for privatpersoner som dokumentene berører (innsynsarkiv)”

Ut fra sitatene ovenfor ser det ut til at strategidokumentet omtaler to typer tredjepartsarkiv, uten å skille tydelig mellom dem. Sett fra Riksarkivarens ståsted kan det skilles mellom to former for tredjepartsarkiv:

A. Arkiv i arkivlovens forstand som settes bort for drift hos en tredjepart. Dette ser ut til å være tilfelle for digitalt arkiv slik det er beskrevet på s. 17 og i pkt 1 på s. 52

B. ”Kopiarkiv” over elektronisk signerte dokumenter. Dette kan realiseres enten ved at både dokumenter og signaturer med alle komponenter lagres, eller at bare hash-verdier av dokumenter med signaturer lagres. Dette ser ut til å være tilfelle for innsynsarkiv/digitalt arkiv slik det er beskrevet på s. 8, s. 17 og i pkt 2 på s. 52

Pkt A: Arkiv i arkivlovens forstand

I pkt A ovenfor er tredjepartsarkivet helt klart arkiv i arkivlovens forstand. Hvis arkivet tilhører et kommunalt eller statlig forvaltningsorgan, skal det håndteres i tråd med arkivloven med forskrifter, og det skal være klart definert at forvaltnings-organet er ansvarlig for all bruk og håndtering av arkivet.

For elektroniske tredjepartsarkiv gjelder følgende arkivmessige krav:

- Arkiveringen skal følge arkivforskriften og bestemmelsene om elektronisk arkivering av saksdokumenter[1].

[1] Forskrift om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver. Kapittel IX: Elektronisk arkivering av saksdokumenter

- Elektronisk signerte dokumenter kan ikke trekkes ut av sin opprinnelige sammenheng (kontekst). Saken kan m.a.o. ikke deles mellom forvaltningsorganets eget arkiv og tredjepartsarkivet.
- Verifiseringsdata skal inngå i organets journal-/arkivsystem, for å sikre autentisitet over tid og hindre at dokumentet kan byttes ut med et annet senere. Kravet til sikker autentisering av et elektronisk dokument øker etter hvert som tiden går. Ved å bevare verifiseringsdataene vil bevisverdien til dokumentet tas vare på ettersom manipulering i ettertid vanskeliggjøres.
- Lesbarheten skal kunne opprettholdes over tid. For bevaringsverdige elektroniske arkiv skal det etableres faste rutiner for konvertering til godkjent arkivformat og lagringsmedium og faste rutiner for reautentisering for å opprettholde autentisitet (ekthet).
- Et arkiv skal avleveres samlet, uansett hvem som faktisk har lagret arkivet eller utfører avleveringen.
- Verifiseringsdata skal følge det elektronisk signerte dokumentet ved avlevering. Selv om det etter eForvaltningsforskriften ikke er et absolutt krav at selve dokumentet og verifiseringsdata skal arkiveres fysisk samlet – det viktigste er et de er tilgjengelig når dokumentet skal presenteres og signatur verifiseres – hjemler arkivloven at verifiseringsdataene skal følge det elektronisk signerte dokumentet ved avlevering.

Avvik fra disse kravene må vurderes fra sak til sak og individuell godkjenning fra Riksarkivaren må innhentes.

Pkt B:"Kopiarkiv" over elektronisk signerte dokumenter
Riksarkivaren har ingen innvendinger mot at en tredjepart har et kopiarkiv for bare elektronisk signerte dokumenter i form av et "innsynsarkiv". Forutsetningen er at dette reelt er et kopiarkiv, dvs at forvaltningsorganet selv har dokumentene i sitt arkiv, som "originaler". Hvis verifiseringsdataene bare er hos tredjepart, må de være direkte lenket sammen med det offentlige arkivet hos forvaltningsorganet. Skal forvaltningsorganets arkiv avleveres, skal verifiseringsdataene følge dokumentene ved avlevering.

Hvis opplysninger og dokumenter i tredjepartsarkivet bare er kopier av ditto i forvaltningsorganets arkiv, vil ikke Riksarkivaren stille krav til håndteringen av dette kopiarkivet ut over at det skal slettes når det ikke lenger er behov for opplysningene og dokumentene ut fra administrative eller rettslige formål.

Autentiserende metadata

Ved elektronisk kommunikasjon er det de elektroniske signaturene og verifiseringen av disse som viser at kommunikasjonen har funnet sted, hvem som har sendt dokumentet, hvem som er mottaker, om dokumentet virkelig har kommet fram mv. Det er mange utfordringer knyttet til bruk av elektroniske signaturer. En av dem er å oppbevare det signerte materialet på en slik måte at det også i ettertid er mulig å foreta en tilfredsstillende verifisering av e-signaturen og eID-en og av at opplysningene ikke er endret.

I e-forvaltningsforskriften § 26 står det at meldinger som er signert med en avansert elektronisk signatur, og som blir arkivert, skal arkiveres sammen med de opplysninger som er nødvendige for å bekrefte signaturen. For meldinger som skal konverteres til annet format, skal arkivet ved mottak verifisere signaturen, og deretter på hensiktsmessig måte bekrefte tilknytningen mellom meldingen, meldingens signatur og relevante opplysninger fra sertifikatet sammen med opplysning om tidspunktet for bekreftelsen. Arkivet skal sikre at ikke meldingene, eller dataene som bekrefter de nevnte forholdene, utilsiktet eller urettmessig endres i oppbevaringsperioden. Tilsvarende gjelder meldinger der tilhørende sertifikaters gyldighetsperiode er kortere enn den tiden det kan være behov for å bekrefte meldingens innhold, med mindre det benyttes tidsstempel eller annen tjeneste som sikrer at signaturen ikke endres og at den også i ettertid kan verifiseres.

Ut fra dette kan det se ut til at både signaturopplysninger, sertifikatopplysninger og verifikasjonsopplysninger er å anse som autentiserende metadata for forvaltningsorganet.

I strategidokumentet berøres ikke problemstillingene knyttet til hva som vil være autentiserende metadata i et lengre perspektiv. For dokumenter som skal oppbevares lenge, og kanskje avleveres til arkivdepot, er det en utfordring å definere hva som er tilstrekkelige autentiserende metadata i et lengre perspektiv. Vil det være nødvendig å bevare både signaturopplysninger, sertifikatopplysninger og verifikasjons-opplysninger? På hvilket detaljeringsnivå skal opplysningene oppbevares? Vil det være ulike behov for ulike saksforhold eller sikkerhetsnivå? Vil det være ulike behov på kort og lang sikt?

Konklusjon

Riksarkivaren ser det som nødvendig at det i det videre strategiarbeidet skilles klart mellom tredjepartsarkiv som er å betrakte som kopiarkiv, og tredjepartsarkiv som er å betrakte som arkiv i arkivlovens forstand. Det er helt sentrale forskjeller mellom disse to typene.

Riksarkivaren ser det også som nødvendig at det videre strategiarbeidet berører problemstillingene knyttet til autentiserende metadata for e-signatur, eID og verifikasjon både i et kort og langt perspektiv.

Med hilsen

Ivar Fonnes
riksarkivar

Anne Mette Dørum
seniorrådgiver