VOLUM 5 2014
http://dx.doi.org/10.7577/ta.1186

Tidsskriftet Arkiv

FAGARTIKKEL

Herbjørn Andresen

Ny EU-forordning om digitale signaturer

SAMMENDRAG
EU har vedtatt en ny forordning, nr. 910/2014, om digitale signaturer. En grunn til at den nye forordningen bør være av særlig interesse for arkivarer, er artikkel 34 om langtidsbevaring av kvalifiserte elektroniske signaturer.
Her følger en kort presentasjon av hovedinnholdet, og noen betraktninger om hva man kan utlede av regler om en tillitstjeneste for langtidsbevaring av kvalifiserte, digitale signaturer i den nye forordningen. Det som i første omgang er viktigst å merke seg, er at kravene til tjenester for langtidsbevaring av signaturer ikke er komplette, de vil bli nærmere utdypet i en kommende sekundærlovgivning til forordningen.

Om vedtaket og ikrafttredelsen

Beslutningen er datert 23. juli 2014, med kunngjøring i Den Europæiske Unions Tidende 28. august 2014. I dansk språkversjon er den fulle tittelen *Europa-parlamentets og Rådets forordning (EU) Nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.*

Den nye EU-lovgivningen om digitale signaturer er en rettsakt av typen forordning, til forskjell fra det tidligere direktivet fra 1999. En forordning er en lovtekst som er direkte bindene for medlemslandene. For ordinære medlemsland gjelder forordningen direkte som lov fra og med ikrafttredelsen. I Norge, som ikke er EU-medlem, men som er forpliktet til deler av EU-lovgivningen gjennom EØS-avtalen, blir EØS-relevante forordninger innlemmet i nasjonal lovgivning ved eget vedtak i lov eller forskrift. Direktiver er en annen type rettsakt, der EU vedtar målsetninger på et område, og mer eller mindre åpne føringer for hvordan målene skal nås. Det enkelte medlemsland har da en viss grad av frihet til å bestemme hvordan landet best kan innpasse direktivets føringer i egen lovgivning. Rent

generelt kan man si at forordninger er en type rettsakt som er egnet når EU ønsker å oppnå en høy grad av harmonisert lovgivning på tvers av landegrensene, mens direktiver ofte sikter mot en mer moderat balanse mellom harmonisert lovgivning og nasjonalt handlingsrom.

Den nye forordningen har, ikke uvanlig for EUs forordninger, en to-leddet bestemmelse om ikrafttredelse. Forordningen trådte som sedvanlig i kraft «på tyvendedagen efter offentliggørelsen», altså 17. september 2014. Den skal imidlertid *anvendes* fra 1. juli 2016, som også er datoen det gamle direktivet om digitale signaturer oppheves.

Den praktiske konsekvensen av at forordningen allerede har trådt i kraft er at EU-kommisjonen kan begynne å utrede og vedta utfyllende sekundærlovgivning tilknyttet ulike artikler i forordningen. Sekundærlovgivningen til forordninger besluttes av EU-kommisjonen, etter egne utrednings- og beslutningsprosedyrer. Det er to hovedformer av sekundærlovgivning til forordninger, henholdsvis *delegerte rettsakter* og *gjennomføringsrettsakter*. Den nye forordningen har i alt 29 bestemmelser som åpner for sekundærlovgivning. Artikkel 34, om langtidsbevaring av signaturer, utgjør én av de mange bestemmelsene i forordningen der nærmere regler kan besluttes innenfor visse rammer ved en *gjennomføringsrettsakt*. EU har, ifølge underhåndenopplysninger, en intern tidsplan for de syv første og mest presserende gjennomføringsrettsaktene. De skal være klare senest et år etter forordningens ikrafttredelse, altså innen 16. september 2015. Gjennomføringsrettsakt for bestemmelser om langtidsbevaring av signaturer synes ikke å befinne seg i den første puljen av sekundærlovgivning, men vil formodentlig bli vedtatt på et senere tidspunkt.

Gjeldende norsk rett

I Norge trådte esignaturloven i kraft 1. juli 2001. Esignaturloven er den norske tilpasningen til det direktiv 1999/93/EF, som vil bli opphevet 1. juli 2016. Hovedinnholdet i esignaturloven er krav til elektroniske sertifikater, krav til virksomheter som utsteder slike sertifikater, og til systemene som fremstiller elektroniske signaturer. Loven skiller mellom elektroniske signaturer generelt, og kvalifiserte elektroniske signaturer. Rettsvirkningen av en kvalifisert elektronisk signatur er at den oppfyller kravet til underskrift, dersom handlingen i utgangspunktet kan gjennomføres elektronisk. I tråd med direktivets målsetning er altså kvalifisert elektronisk signatur sidestilt med håndskrevet underskrift i norsk rett.

Norge har i dag en forholdsvis stor utbredelse av sertifikat- og signaturtjenester, som mange enkeltpersoner kjenner fra nettbanker eller fra elektronisk samhandling med ulike deler av offentlig forvaltning. Det er også utbredt i samhandling mellom virksomheter, blant annet i helsesektoren, forvaltningen og næringslivet. Utbredelsen av elektroniske signaturer hviler riktignok ikke bare på esignaturloven, det har også vært behov for flere runder med tilpasninger i forvaltningsloven med forskrifter, for å tilrettelegge for samhandling med og i offentlig sektor.

Den gjeldende esignaturloven bekrefter i og for seg de behovene EU har anført for å velge å erstatte direktivet med en ny forordning: Infrastrukturen åpner ikke generelt for bindende elektronisk samhandling over landegrensene, hverken i form av gjensidige godkjenningsordninger for utstedere og teknologier, eller i form av sikker entydig identifisering av personer og virksomheter fra andre land.

Esignaturloven har heller ikke bestemmelser som ivaretar eventuelle behov for å kunne etterprøve signaturer langt frem i tid. Det problemet har jeg beskrevet i større bredde i et kapittel i «Arkivakademiboken» (Andresen 2014), som det vil være å håpe at den nye forordningen kan bidra til at raskt blir avleggs. Det er imidlertid neppe tilfelle før både ny lovgivning og nye løsninger har fått noe tid til å feste seg.

Hovedtrekkene i den nye forordningen

Et bærende prinsipp i den nye forordningen er gjensidig anerkjennelse av personers elektroniske identifikasjon («eID»), på tvers av landegrenser. En utsteder av elektronisk identifikasjon kan, av et lands myndigheter, meldes inn til EU-kommisjonens publiserte liste over notifiserte tilbydere. Ved bruk av offentlige elektroniske tjenester må en etat akseptere eID fra andre EU-lands notifiserte tilbydere som bevis for at vedkommende er den han gir seg ut for å være. En person som henvender seg til en norsk offentlig etat fra et annet EU-land trenger derfor ikke nødvendigvis norsk fødselsnummer, eller D-nummer utstedt i Norge. Hans eID utstedt av notifisert tilbyder i et annet EU-land godtgjør at han er entydig identifiserbar i det aktuelle landet. At et annet land må akseptere en persons eID betyr imidlertid bare at identiteten anses godtgjort, det betyr ikke nødvendigvis at vedkommende har rettigheter knyttet til en hvilken som helst tjeneste i det land han henvender seg til.

Forordningen innfører videre begrepet elektronisk segl, som et uttrykk for at det er en juridisk person, altså en virksomhet, som er identifisert elektronisk. Det tilsvarende begrepet som hittil har vært brukt i Norge er virksomhetssertifikater. Den nye bruken av begrepet elektronisk segl kan muligens komme til å skape noe forvirring, ettersom det tidligere også har vært vanlig å betegne integritetssikrende elektroniske signaturelementer, når de er påført dokumenter eller transaksjoner, som elektroniske «segl» i metaforisk forstand (Boudrez 2007).

Prinsippet om gjensidig aksept fører med seg en rekke andre bestemmelser som også må harmoniseres, blant annet om gjensidig aksept av andre lands utstedere av eID og signaturtjenester. Videre er det lagt opp til harmoniserte ordninger for tilsyn, ansvarsforhold, sanksjoner og tilbaketrekking av godkjenninger med mer.

Utover reglene som skal sikre gjensidig aksept av elektronisk identifikasjon, dreier forordningen seg om krav til tilbydere av tjenester for å generere, kontrollere, tidsstemple og oppbevare etc. digitale signaturer. Forordningen bruker samlebetegnelsen

tillitstjenester om slike funksjoner, som gjerne skal kunne utføres av konkurrerende private tilbydere mot betaling. Mange av tillitstjenestene er sammenlignbare med krav som ble innført med direktivet fra 1999, men definisjonen omfatter også et par nye tjenester i tillegg. Den ene av de disse er «generering, kontrol og validering af certifikater for webstedsautentifikation» (art. 3(16)(b)), den andre er «bevaring af elektroniske signaturer, segl eller certifikater relateret til disse tjenester» (art. 3(16)(c)). Definisjonen av bevaring som tillitstjeneste («preservation» i den engelske språkversjonen av forordningen) er grunnlaget for kravet i artikkel 34 om en tillitstjeneste for bevaring av kvalifiserte elektroniske signaturer.

Tillitstjenestene er også gjenstand for en målsetning om høy grad av harmonisering på tvers av landegrensene. Det er likevel visse begrensninger i harmoniseringstiltakene: «Retsvirkningerne af tillidstjenester i medlemsstaterne defineres i national ret, medmindre andet er fastsat i denne forordning» (fortalens avsnitt 22, annet punktum). De rettsvirkningene som forordningen stiller krav til er at elektroniske signaturer ikke må nektes rettsvirkning eller anerkjennelse som bevis i rettsaker alene fordi den er elektronisk, eller bare fordi den ikke oppfyller kravene til kvalifisert elektronisk signatur (art. 25). Det betyr at man i et medlemsland kan avvise en ikke-kvalifisert elektronisk signatur, dersom avvisningen bygger på andre konkrete innvendinger enn bare at den er elektronisk. Tilsvarende prinsipp om rettsvirkning gjelder for elektronisk segl (art. 35), elektronisk tidsstempel (art. 41), leveringstjenester (art. 43) og elektroniske dokumenter (art. 46). Andre regler om rettsvirkninger av *kvalifiserte* signaturer er at de skal ha samme rettsvirkning som håndskrevne signaturer har i medlemslandet, og at «kvalificeret elektronisk signatur, som er baseret på et kvalificeret certifikat, der er udstedt i en medlemsstat, anerkendes som en kvalificeret elektronisk signatur i alle andre medlemsstater».

Det er altså en forholdsvis høy grad av harmoniserte minimumskrav til rettsvirkningene av de mest sentrale kvalifiserte tillitstjenestene. Det er imidlertid også noen av tillitstjenestene som ikke har egne bestemmelser om rettsvirkninger i forordningen. I slike tilfeller vil rettsvirkningene formodentlig, basert på avsnitt 22 annet punktum i fortalen, i all hovedsak følge av nasjonal rett.

Noen betraktninger om artikkel 34 og langtidsbevaring

Artikkel 34 har to avsnitt. Ordlyden, i dansk språkversjon, er:

> Kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer
>
> 1. En kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer må kun stilles til rådighed af en kvalificeret tillidstjenesteudbyder, der anvender procedurer og teknologier, der gør det muligt at forlænge pålideligheden af den kvalificerede elektroniske signatur ud over den teknologiske gyldighedsperiode.

> 2. Kommissionen kan ved hjælp af gennemførelsesretsakter opstille referencenumre på standarder for kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer. En kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer, der opfylder disse standarder, formodes at overholde kravene i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 48, stk. 2.

Dette kravet til tillitstjenester for bevaring kommer, i hvert fall et stykke på vei, en av de mest problematiske sidene ved digitale signaturer i møte. Digitale signaturer, og sertifikater som bekrefter identitet, er i praksis bare etterprøvbare med opprettholdt bevisstyrke i relativt kort tid. Hverken direktiv 1999/93/EF eller den norske esignaturloven fastlegger krav som bøter på det. Løsningen i norsk forvaltning har vært at det er valgfritt hvorvidt man skal bevare faktiske signaturdata for senere validering, eller bare bevare metadata som i klartekst bekrefter at et dokument eller en transaksjon har vært signert elektronisk, og av hvem. Denne valgfriheten kommer til uttrykk i eForvaltningsforskriften § 28. Noark 5 åpner også for tilsvarende valgfrihet. Dersom det reises tvil om en elektronisk signatur på et eldre dokument, vil bevisspørsmålet i praksis dreie seg om arkivets pålitelighet.

Første avsnitt i artikkel 34 åpner for at langtidsbevaring av kvalifiserte signaturer kan inngå som en av de tillitstjenestene som en kvalifisert tilbyder velger å levere. Det er imidlertid ikke angitt som en plikt at enhver kvalifisert tilbyder må tilby langtidslagring. De som tilbyr langtidslagring av signaturer vil selvfølgelig ha et konkurransefortrinn når de skal selge tillitstjenester til virksomheter som kan ha behov for å få validert en signatur på nytt mange år etter at den ble påført. Artikkel 34 tar altså opp erkjente problemer, men med mange åpne spørsmål som neppe kan besvares før den tilhørende sekundærlovgivningen kommer på plass.

Det første åpne spørsmålet er hvilken tidshorisont som egentlig er ment med formuleringen «ud over den teknologiske gyldighedsperiode». Ambisjonsnivået synes noe forsiktig, sammenlignet med avsnitt 61 i fortalen: «Denne forordning bør sikre langtidsopbevaring af information, for at sikre at elektroniske signaturer og elektroniske segl har retsgyldighed over et længere tidsrum, og garantere, at de kan valideres uanset fremtidige teknologiske ændringer». Det er altså klart at man tar sikte på å opprettholde etterprøvbarheten lenge, men hverken artikkel 34 eller fortalen presiserer hvor lenge.

Varigheten av et digitalt sertifikat som sådan er oftest tre år eller kortere, og noen av problemene med å gjenta valideringen begynner allerede da. Den teknologiske gyldighetsperiode sikter helt klart et stykke lenger ut i tid enn dette. Det tar gjerne noen få år til før IT-systemer er utrangerte, og i beste fall ytterligere et par tiår før formater og presentasjonsmuligheter er vaklevorne. Selv med et ganske beskjedent ambisjonsnivå for lagringstid må det vel kunne forutsettes at artikkel 34 dreier seg om å bevare beviskraft for signaturer også etter at et arkivdokument både er overført til nye arkivsystemer og

konvertert til nye lagringsformater. Det konkrete arbeidet med å bevare etterprøvbare signaturer vil dermed støte på mange av de samme problemstillingene som man møter i langtidsbevaring av digitale arkiver generelt. Det er et eget fagområde med sine teorier, standarder og faglige normer, men som foreløpig i liten grad er rettslig regulert. Det er dessverre vanskelig å finne noen spor av koblinger til generelle standarder for digital langtidsbevaring i den nye forordningen.

I artikkel 34 brukes betegnelsen «kvalificeret tjeneste til bevaring». Hva begrepet tjeneste i denne sammenheng kan eller skal innebære fører til et annet åpent spørsmål: Hvem skal besitte de eldre, signerte dokumentene? Vil de forbli hos arkivskaperen, eller vil en slik tillitstjeneste forutsette at de bevares hos tjenestetilbyderen? Vil en tjeneste for bevaring av signaturer være innrettet slik at den opprettholder signaturens gyldighet også når et arkiv med signete dokumenter deponeres hos eller avleveres til et digitalt depot? Hverken arkivansvaret etter arkivloven § 6 eller avleveringsplikten etter arkivloven § 10 byr egentlig på noen tvilsspørsmål: Tillitstjenestene er kun oppdrag som kan utføres på vegne av den arkivansvarlige. Tjenestetilbyderen er ikke en aktør med noen selvstendig råderett hverken over signaturer eller andre deler av arkivdokumentene. Det som foreløpig er vanskelig å få tak i, ut fra forordningens artikkel 34, er om koblingene mellom et arkiv som inneholder signerte dokumenter og tjenester for å bevare etterprøvbare signaturer kan være så uavhengige av hverandre at arkivskaper og depotvirksomhet får gjennomført sine egne aktiviteter for å sikre og langtidsbevare arkiverer uten å miste forbindelsen til signaturene på veien. Et nært beslektet spørsmål er om bevarte signaturer vil være portable, altså mulige å overføre fra én tillitstjenestetilbyder til en annen på et vilkårlig tidspunkt.

Disse spørsmålene som står åpne etter første avsnitt, kan man håpe blir nærmere belyst i de utredninger og beslutninger om gjennomføringsrettsakter som avsnitt 2 i artikkel 34 åpner for.

Innholdet i den eller de gjennomføringsrettsakter EU-kommisjonen etter hvert kommer til å vedta er «referencenumre på standarder for kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer». Her er det foreløpig svært få kandidater å velge mellom. Et referansenummer som det ofte henvises til for slike spørsmål er RFC 4998 (2007), som har tittelen *Evidence Record Syntax (ERS)*. Strategien går ut på å fornye digitale tidsstempler, og bevare tidsstemplene i en struktur, et «hash-tre», der en nyere signatur også omfatter den integritetssikringen som ligger i de tidligere tidsstemplingene. En «evidence record» vil i prinsippet være adskilt fra selve arkivdokumentet, og gi et regelmessig fornyet bevis for at det er intakt. En strategi for langtidsvalidering av signaturer, som er basert på samme grunnleggende strategi, finnes også som en påbygningsmulighet i standarden ETSI TS 101 733, som i stor grad har vært premissgivende for bruken av digitale signaturer i norsk forvaltning. Strategien for langtidsbevaring i disse standardene bekrefter i hovedsak at en signatur har vært gyldig på et tidligere bekreftet tidspunkt, som man igjen kan bruke som utgangspunkt for en kjede av nye bekreftelser. De tar imidlertid ikke opp spørsmålet om hvordan man håndterer behovet for å migrere arkivdokumenter til nye formater eller systemmiljøer.

Rettsvirkninger av artikkel 34 er ikke omfattet av den harmoniseringen av minimumskrav som gjelder for enkelte av de andre tillitstjenestene. Dermed er utgangspunktet, jf. fortalens avsnitt 22, at rettsvirkningene defineres i nasjonal rett. Annet avsnitt av artikkel 34 gir likevel en viss føring for hvordan en tillitstjeneste for langtidsbevaring skal vurderes i en bevissituasjon: «En kvalificeret tjeneste til bevaring af kvalificerede elektroniske signaturer, der opfylder disse standarder, formodes at overholde kravene i stk. 1». «Formodes» bør vel forstås slik at dersom en tilbyder av langtidsbevaring av signaturer følger de prosedyrer og teknologiske krav som er angitt i standarder med de referansenumre som blir vedtatt som sekundærlovgivning, skal man som utgangspunkt anta at signaturen er ekte. Det vil imidlertid være mulig å bestride en signatur, enten ved å bevise konkret at den er falsk, eller ved å påvise at tjenestetilbyderen ikke etterlever standardene i tilstrekkelig grad til at man kan ha tillit til det arbeidet de har utført.

Oppsummering

Ny forordning (EU) nr. 910/2014 er vedtatt, og vil overta for den nåværende esignaturloven. Hovedformålet med den nye forordningen er å muliggjøre digital signering over landegrensene. En bestemmelse av særskilt interesse for arkivmiljøet er artikkel 34, om langtidsbevaring av digitale signaturer. Foreløpig er det vanskelig å ha veldig bestemte oppfatninger om hva dette kommer til å innebære, det vil antakelig bli klarere etter hvert som tilhørende sekundærlovgivning kommer på plass.

Litteratur

Andresen, H. (2014). Digital signering for samtid og ettertid. I Neergaard A. (red.). *Dokumentasjonsforvaltning og arkiv i det 21. århundre.* s. 199-218. Bergen: Fagbokforlaget.

Boudrez, F. (2007). Digital signatures and electronic records. *Archival Science 7(2)*, 179-193.

Direktiv 1999/93/EF. *Europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer.*

eForvaltningsforskriften. *Forskrift om elektronisk kommunikasjon med og i forvaltningen, 25. juni 2004 nr. 988.*

Esignaturloven. *Lov om elektronisk signatur, 15. juni 2001 nr. 81.*

ETSI TS 101 733 (2013). *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)*. v.2.2.1. Technical Specification. European Telecommunications Standards Institute.

Forordning (EU) nr. 910/2014. *Europa-parlamentets og Rådets forordning (EU) Nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.*

Forvaltningsloven. *Lov om behandlingsmåten i forvaltningssaker, 10. februar 1967.*

Noark 5 (2013). *Noark 5. Standard for elektronisk arkiv.* v.3.11. Riksarkivet, 2013.

RFC 4998 (2007) *Evidence Record Syntax (ERS)*. Proposed standard. Internet Engineering Task Force, IETF Trust.