Nærings- og fiskeridepartementet

Høringsnotat

Forslag til lov om gjennomføring av EUs forordning om elektronisk identifisering og tillitstjenester for elektroniske transaksjoner på det indre marked

Innhold

1 Hovedinnholdet i høringsnotatet 2

2 Bakgrunn 3

3 Gjeldende rett 4

3.1 Esignaturloven 4

3.2 Elektronisk identifisering (eID) – eForvaltningsforskriften og Kravspesifikasjon for PKI i offentlig sektor 6

3.3 Den nye ordningen med nasjonalt ID-kort 7

4 Arbeidet med regelverket i EU og Norge 7

5 Gjennomføring av regelverket 9

6 Formål og virkeområde 10

6.1 Innholdet i forordningen 10

6.2 Departementets vurdering og forslag 11

7 Elektronisk identifisering (kapittel II) 12

7.1 Innholdet i forordningen 12

7.2 Eksisterende norske sikkerhetsnivåer 14

7.3 Departementets vurdering og forslag 14

8 Tillitstjenester (kapittel III) 18

8.1 Begrepet «tillitstjeneste», krav til tilbyderne m.m. 18

8.1.1 Innholdet i forordningen 18

8.1.2 Departementets vurdering og forslag 23

8.2 Rettsvirkninger av elektroniske signaturer og krav til referanseformater m.m. 25
8.2.1 Innholdet i forordningen 25
8.2.2 Departementets vurdering og forslag 26
8.3 Tilsynsorganets oppgaver 27
8.3.1 Innholdet i forordningen 27
8.3.2 Departementets vurdering og forslag 28
8.4 Erstatningsansvar og bevisbyrde 30
8.4.1 Innholdet i forordningen 30
8.4.2 Departementets vurdering og forslag 30
8.5 Sanksjoner – straff og tvangsmulkt 31
8.5.1 Innholdet i forordningen 31
8.5.2 Departementets vurdering og forslag 31
8.6 Gebyr 32
9 Bør selvdeklarasjonsordningen beholdes? 32
10 Avsluttende bestemmelser, ikrafttredelse og overgangsperiode 33
10.1 Innholdet i forordningen 33
10.1.1 Overgangsordning for bestemmelsene om eID 33
10.1.2 Overgangsordning for kvalifiserte sertifikater og registrerte tjenestetilbydere 34
10.2 Departementets vurdering og forslag 34
11 Endringer i annet regelverk 34
12 Om lovens anvendelse på Svalbard 35
13 Økonomiske og administrative konsekvenser 35

1 Hovedinnholdet i høringsnotatet

Nærings- og fiskeridepartementet foreslår i dette høringsnotatet en ny lov som gjennomfører europaparlaments- og rådsforordning (EU) 910/2014 om elektronisk identifisering og tillitstjenester for elektroniske transaksjoner på det indre marked og om opphevelse av direktiv 1999/93/EF[1]. Endringene legger til rette for økt elektronisk samhandling mellom næringsdrivende, borgere og offentlige myndigheter på tvers av landegrensene i EU/EØS og dermed sterkere økonomisk vekst i

[1] Europaparlaments- og rådsdirektiv 1999/93/EF om en fellesskapsramme for elektroniske signaturer.

det indre marked. Formålet med høringen er å få høringsinstansenes syn på departementets forslag til gjennomføring av forordningen i norsk rett.

Høringsnotatet er utarbeidet sammen med Kommunal- og moderniseringsdepartementet (KMD), som er ansvarlig for oppfølgingen av forordningens bestemmelser om gjensidig anerkjennelse av eID i offentlig sektor (forordningens kapittel II).

I kapittel 2 redegjøres det for bakgrunnen for forordningen og for EØS-relevansen av bestemmelsene. Kapittel 3 gir en oversikt over gjeldende rett, mens kapittel 4 sier noe om arbeidet med regelverket i EU og i Norge. I kapittel 5-11 gjennomgås bestemmelsene i forordningen, med en vurdering av hvilke konsekvenser endringene vil få for norsk rett. I kapittel 12 redegjøres det for de økonomiske og administrative konsekvensene av forslaget. Kapittel 13 sier litt om lovens anvendelse på Svalbard. Departementets lovforslag er presenteres i kapittel 14.

Departementet har lagt ved den engelske oversettelsen av forordningen, i påvente av en norsk oversettelse.[2] I EU benyttes ofte forkortelsen «eIDAS-regulation» om forordningen, og denne benyttes enkelte steder i høringsnotatet.

2 Bakgrunn

Forordning 910/2014 ble vedtatt 23. juli 2014, basert på et forslag av Europakommi-sjonen av 4. juni 2012 (COM(2012) 238 final). I fortalen er det uttalt at å sikre tillit på internett er en nøkkel til økonomisk og sosial utvikling. Mangel på tillit gjør at forbrukere, næringslivet og offentlige myndigheter vegrer seg for å gjennomføre elektroniske transaksjoner og å utvikle nye tjenester. I fortalen uttales det også at direktivet om elektronisk signatur ikke har vært et hensiktsmessig verktøy for sikre grensekryssende elektroniske transaksjoner. Forordningen styrker og utvider reglene om elektronisk signatur, regulerer eID og omfatter også andre typer elektroniske tillitstjenester. Direktivet om elektronisk signatur oppheves.

I fortalen vises det videre til «A Digital Agenda for Europe» fra 2010, hvor Europakommisjonen uttaler at mangelen på interoperabilitet og økningen av kriminalitet på internett er to vesentlige hindre mot den «virtuelle syklus» i den digitale økonomien. I rapporten "Dismantling the obstacles to EU citizen's rights" (2010) peker Kommisjonen på behovet for å løse problemene som forhindrer EUs borgere fra å utnytte fordelene ved et digitalt indre marked og grensekryssende digitale tjenester.

Forordningen er todelt, og inneholder regler som skal legge til rette for:

1. *Gjensidig aksept av løsninger for elektronisk identifisering (eID) – kapittel II*
   Dette innebærer at privatpersoner og bedrifter skal kunne bruke sin eID, utstedt enten av offentlig sektor eller under ansvar av en offentlig myndighet, for å få tilgang til elektroniske tjenester fra offentlig sektor i andre land som tilbyr pålogging med eID. Dette gjelder eID-løsninger som har blitt notifisert til Europakommisjonen og er oppført på en liste publisert i Official Journal of the European Union. Anerkjennelsesplikten begrenses til eID til bruk for tjenester i offentlig sektor, og medlemsstaten må for slik bruk tilby gratis validering av notifiserte eID-er, jf. art. 7 bokstav f, annet ledd. Forordningen innebærer ingen plikt for

[2] Ulike språkversjoner av forordningen kan finnes på http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

landene til å etablere en nasjonal elektronisk ID-løsning, og endrer heller ikke offentlig tjenesteeiers rett til å velge sikkerhetsnivå, men for offentlige tjenesteeiere vil det bli en plikt til å likebehandle notifiserte utenlandske eID-er med de nasjonale. Det fremgår av fortalen pkt. 17 at medlemsstatene også oppfordres til å muliggjøre bruk av notifiserte eID-er også i privat sektor.

2. *Gjensidig aksept av elektronisk signatur og andre tillitstjenester – kapittel III og IV*

   Forordningen styrker dagens regler om elektronisk signatur (esignatur) og innfører regler om flere typer elektroniske tillitstjenester, deriblant om elektroniske segl, tidsstemplingstjenester, elektronisk registrerte leveringstjenester og sertifikattjenester for webside-autentisering. Tilbydere av elektroniske tillitstjenester får flere plikter å forholde seg til, deriblant mer detaljerte krav for identitetskontroll, sikkerhetskrav til virksomheten og opplysningsplikter overfor tilsynsmyndigheten. Det stilles også krav om at utstedere av kvalifiserte tillitstjenester skal revideres av et godkjent revisjonsfirma (samsvarsvurderingsorgan) hvert andre år. Tilbydere av ikke-kvalifiserte tjenester omfattes av deler av regelverket, og tilsynsorganet får nye og mer omfattende håndhevingsoppgaver.

Særskilt om EØS-relevans

Esignaturdirektivet er innlemmet i EØS-avtalen og gjennomført i norsk rett. Forordningen utvider området for reguleringen av elektroniske tillitstjenester sammenliknet med hva direktivet omfattet. Harmonisering av krav til flere typer tillitstjenester kan gjøre det enklere å tilby slike tjenester på tvers av landegrensene. Videre kan strengere krav øke tilliten blant brukerne. Forordningen legger også til rette for at eID-løsninger som oppfyller visse betingelser, skal kunne benyttes på tvers av landegrensene. Som det fremgår av forordningens fortale pkt. 12 er målet med dette «at sørge for, at der findes sikker elektronisk identifikation og autentifikation, der gør det muligt at få adgang til grænseoverskridende onlinetjenester, som medlemsstaterne udbyder.» Etter departementets syn kan reglene i forordningen bidra til flere elektroniske transaksjoner på tvers av landegrensene, slik at det indre marked kan fungere bedre, og etter departementets syn er forordningen både EØS-relevant og akseptabel.[3]

Dersom rettsakten innlemmes i EØS-avtalen, vil det innebære en plikt til å gjennomføre forordningen i norsk rett, jf. den nærmere omtalen av dette i kapittel 5.

3 Gjeldende rett

3.1 Esignaturloven

Lov 15. juni 2001 nr. 81 om elektronisk signatur (esignaturloven) gir rettslige rammebetingelser for bruk av elektronisk signatur og tilknyttede tjenester. Loven gjennomfører Europaparlaments- og rådsdirektiv 1999/33/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer. Tilsynsmyndighet etter loven er Nasjonal kommunikasjonsmyndighet (Nkom) (som frem til 1. januar 2015 het Post- og teletilsynet).

[3] Jf. departementets EØS-posisjonsnotat i EØS-notatbasen.

Esignaturloven § 3 nr. 1 definerer elektronisk signatur som «data i elektronisk form som er knyttet til andre elektroniske data og som brukes som autentiseringsmetode». Loven regulerer i hovedsak utstedere av «kvalifiserte sertifikater» som er etablert i Norge. Et sertifikat er en kopling mellom signaturverifikasjonsdata og undertegner som bekrefter undertegners identitet og er signert av sertifikatutsteder. Betegnelsen «kvalifisert sertifikat» brukes om sertifikater som oppfyller kravene i lovens § 4, mens det i §§ 10-16 stilles nærmere krav til utstedere av kvalifiserte sertifikater, som krav til forsvarlig virksomhet og tilstrekkelige økonomiske ressurser, krav om bruk av pålitelige produkter og systemer, krav om hurtig og sikker katalog- og tilbaketrekkingstjeneste og krav til lagring av opplysninger m.m.

Med hjemmel i lovens § 16 er det gitt utfyllende krav, jf. forskrift 15. juni 2001 nr. 611 om krav til utsteder av kvalifiserte sertifikater mv. I forskriftens § 7 stilles det blant annet krav om at identifisering av person som ønsker et kvalifisert sertifikat må skje ved personlig fremmøte hos sertifikatutsteder eller en representant for denne, med mindre vedkommende allerede er identifisert ved personlig fremmøte gjennom eksisterende kundeforhold. Det er derimot ikke nærmere angitt hvilke typer av dokumenter som må legges frem ved en slik identifisering.

Esignaturloven § 6 fastslår at dersom det i lov, forskrift eller på annen måte er oppstilt krav om underskrift for å få en bestemt rettsvirkning, og disposisjonen kan gjennomføres elektronisk (dvs. at det er rettslig adgang til dette), vil en kvalifisert elektronisk signatur alltid oppfylle et slikt krav. En elektronisk signatur som ikke er kvalifisert kan imidlertid også oppfylle et slikt krav. I Ot.prp. nr. 82 (1999-2000) Om lov om elektronisk signatur s. 51 er det vist til at en slik rettsvirkning vil bero på en konkret vurdering i det enkelte tilfellet, jf. prinsippet i norsk rett om fri bevisvurdering og fri bevisbedømmelse.

Loven inneholder også nærmere bestemmelser om innsamling av personopplysninger, jf. § 7. Disse kravene gjelder for alle utstedere av elektroniske signaturer uansett hvilken type elektronisk signatur som tilbys. Datatilsynet fører tilsyn med at bestemmelsen etterleves.

I esignaturloven §§ 8-9 gis det nærmere krav til sikre signaturfremstillingssystemer. Per i dag finnes det ikke slike sertifikater på det norske markedet, og det er ikke innført et system for godkjennelse av slike signaturfremstillingssystem i Norge. Godkjennelse som er foretatt av et organ i en annen EØS-stat skal imidlertid likestilles med norsk godkjennelse.

Esignaturloven § 16a gir departementet adgang til å innføre en frivillig sertifiserings-, godkjennings- eller selvdeklarasjonsordning for sertifikatutstedere. Formålet er å bidra til å øke tilliten til og derved øke bruken av elektroniske signaturer, jf. Ot.prp. nr. 74 (2004-2005). En selvdeklarasjonsordning er innført for sertifikatutstedere som ønsker å tilby sertifikater i henhold til den til enhver tid gjeldende «Kravspesifikasjon for PKI i offentlig sektor», jf. forskrift 21. november 2005 nr. 1296 om frivillige selvdeklarasjonsordninger for sertifikatutstedere. Gjennom denne ordningen kan en sertifikatutsteder erklære at en sertifikattype som utstederen tilbyr, oppfyller de nærmere angitte kravene. Se nærmere omtale under pkt. 3.2 nedenfor.

Lovens § 20 fastsetter at for å sikre at bestemmelser gitt i eller i medhold av loven, kan tilsynet bestemme at sertifikatutsteder skal betale tvangsmulkt. Lovens § 21 pålegger straffeansvar for en kvalifisert sertifikatutsteder som forsettlig eller grovt uaktsomt overtrer plikten til å sende registreringsmelding til tilsynet, unnlater å gi opplysninger eller gir uriktige eller villedende opplysninger til tilsynet, eller behandler personopplysninger i strid med reglene om innsamling, bruk og lagring av opplysninger etter §§ 7 og 14.

Etter esignaturloven § 22 første ledd vil en utsteder av kvalifiserte sertifikater være erstatningsansvarlig for tap hos en fysisk eller juridisk person når denne hadde rimelig grunn til å ha tillit til sertifikatet i henhold til nærmere angitte forhold. Dette gjelder med mindre utstederen godtgjør at han eller hun ikke har handlet uaktsomt (omvendt bevisbyrde).

Esignaturloven § 24 gir hjemmel for å fastsette at registreringspliktige utstedere skal betale gebyr til tilsynet. Gebyrene må ikke overstige kostnadene ved tilsynets virksomhet. Bestemmelser om gebyr er fastsatt i forskrift 21. februar 2005 nr. 168 om gebyr til Post- og teletilsynet § 5. Tilsynet gis adgang til ved enkeltvedtak å «fastsetje årleg gebyr for sertifikatutstedar som er registreringspliktig i samsvar med lov 15. juni 2001 nr. 81 om elektronisk signatur § 18, jf. § 3 og § 24, eller som kjem inn under frivillige sertifiseringsordningar, godkjenningsordningar eller sjølvdeklarasjonsordningar, jf. § 16a og forskrift om frivillige sjølvdeklarasjonsordningar for sertifikatutstedarar § 14.»

3.2 Elektronisk identifisering (eID) – eForvaltningsforskriften og Kravspesifikasjon for PKI i offentlig sektor

«Kravspesifikasjon for PKI i offentlig sektor» er en overordnet, funksjonell kravspesifikasjon for selvdeklarering og anskaffelse av PKI-baserte elektroniske identitetsbevis (eID) som skal benyttes ved elektronisk kommunikasjon med og i offentlig sektor. Kravspesifikasjonen er hjemlet i eForvaltningsforskriften § 36. Formålet med kravene er å bidra til enklere anskaffelser og felles krav til sikre og standardiserte PKI-tjenester i forvaltningen. Den definerer tre sertifikatklasser – «Person Høyt», «Person Standard» og «Virksomhet». Ansvaret for kravspesifikasjonen tilligger KMD, som har koordineringsansvaret for forvaltningens bruk av sikkerhetstjenester og -produkter etter eForvaltningsforskriften. Nkoms enkeltvedtak etter selvdeklarasjonsforskriften kan påklages til KMD.

Den enkelte virksomhet må gjøre selvstendige sikkerhets- og sårbarhetsvurderinger og avgjøre hvilke sikkerhetstjenester og hvilket sikkerhetsnivå den har behov for, i tråd med deres sikkerhetsmål og -strategi.

PKI-løsninger som benyttes i offentlig virksomhet skal oppfylle kravspesifikasjonen. Sertifikattilbydere kan gjennom selvdeklarasjonsordningen erklære at de oppfyller kravspesifikasjonen. En erklæring om oppfyllelse av nivå Person Høyt er også en forutsetning for å levere eID-tjenester på høyeste sikkerhetsnivå (nivå 4) i henhold til «Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor» (fastsatt av Fornyings- og administrasjonsdepartementet i 2008).

Forskrifter som viser til Kravspesifikasjon for PKI i offentlig sektor

Det finnes en rekke forskrifter som gjelder for privat sektor og som viser til kravspesifikasjonen for PKI. Et eksempel er forskrift om tiltak mot hvitvasking og terrorfinansiering mv. av 13. mars 2009 nr. 302 (hvitvaskingsforskriften). Den utfyller hvitvaskingslovens bestemmelse om likestilling mellom

elektronisk og fysisk legitimasjon for fysiske personer. I henhold til hvitvaskingsforskriften § 6 er *g*yldig elektronisk legitimasjon for fysiske personer, elektronisk signatur som oppfyller kravene i selvdeklarasjonsforskriften § 3 og som er oppført på publisert liste i henhold til § 11 første ledd i nevnte forskrift. Dette innebærer krav om en elektronisk signatur som er i tråd med kravene til «Person Høyt» i Kravspesifikasjonen for PKI i offentlig sektor.

Det er nedsatt et lovutvalg som skal vurdere endringer i hvitvaskingsregelverket. Kravene til legitimasjonskontroll, herunder hvilke krav som vil måtte stilles til en eID før den kan legges til grunn i kundekontrollen, vil vurderes som en del av utvalgets arbeid. Utvalget skal avgi sin rapport til Finansdepartementet i august 2016.

Et annet eksempel på henvisning til selvdeklarasjonsordningen er forskrift 25. juni 2010 nr. 977 om elektronisk kommunikasjon med namsmannen og Statens innkrevingssentral i saker etter tvangsfullbyrdelsesloven og i saker for forliksrådet. Se for øvrig opplisting i kapittel 12.

3.3 Den nye ordningen med nasjonalt ID-kort

Det tas sikte på å innføre en ny ordning med nasjonalt ID-kort i Norge i 2017. Ordningen vil gi borgerne tilbud om et offentlig utstedt identitetsbevis som vil være like pålitelig som passet, og mer praktisk å bruke som legitimasjon. Loven åpner for å utstede ID-kort til EØS-borgere, gitt at grunnlaget for identifisering er sikkert. De rettslige rammene for ordningen er vedtatt ved lov 5. juni 2015 nr. 39 om nasjonalt identitetskort (ID-kortloven). Loven legger også til rette for å inkludere et elektronisk identitetsbevis (NeID) i ordningen, og det pågår en nærmere kost-nyttevurdering av dette spørsmålet som ledd i politiets anskaffelse av de nye systemene for pass og ID-kort. Ettersom en eventuell NeID vil bli tildelt sammen med utstedelsen av nasjonalt ID-kort, vil kravene til identitetskontroll, herunder personlig oppmøte og avleggelse av biometriske personopplysninger, være de samme som for utstedelsen av det fysiske identitetsbeviset. NeID tilknyttet nasjonalt ID-kort vil være et supplement til løsninger fra markedet.

4 Arbeidet med regelverket i EU og Norge

Nærings- og handelsdepartementet (nå Nærings- og fiskeridepartementet) sendte Europakommisjonens forslag til forordning på høring høsten 2012.[4] Hovedinntrykket etter høringen var at høringsinstansene i utgangspunktet var positive til forslaget, samtidig som mange etterlyste viktige avklaringer. Dette gjaldt for eksempel behovet for en nærmere angivelse av sikkerhetsnivå for notifiserte eID-tjenester og harmoniserte krav til utstedelsesprosedyrer. Videre ble det anført at årlig revisjon av sertifikatutstedere var for ofte, og at det legges opp til for mange delegerte rettsakter og gjennomføringsrettsakter, noe som kan svekke forutberegnelighet og klarhet. I høringsrunden kom det også innspill om at forslaget kan få konsekvenser for reglene om ID-kontroll i hvitvaskingsforskriften, forskrift om frivillig selvdeklarasjonsordninger for sertifikatutstedere og Kravspesifikasjon for PKI i offentlig sektor.

[4] Høringsbrevet og høringsuttalelsene kan finnes her:

https://www.regjeringen.no/nb/dokumenter/europakommisjonens-forslag-til-forordnin/id699224/

I EFTA har forslaget vært fulgt opp av EFTA-arbeidsgruppen for elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunn (WG ECASIS). En felles uttalelse fra EØS/EFTA-landene[5] ble oversendt EU 19. mars 2013, hvor flere av innspillene fra høringsrunden ble tatt med.

En referansegruppe som har bestått av NFD, KMD, JD, Difi, Politidirektoratet, Nkom og Brønnøysundregistrene har fulgt arbeidet med utviklingen av rettsakten. I forbindelse med Kommisjonens arbeid med gjennomføringsrettsakter har også Skattedirektoratet og Nasjonal Sikkerhetsmyndighet deltatt. NFD har løpende orientert bransjen, blant annet på møter i Nkoms «Aktørforum esignatur», og med enkeltaktører som BankID, Finans Norge, Commfides og Buypass.

I forbindelse med behandlingen i Rådet og Europaparlamentet, ble Europakommisjonens forslag endret og utdypet på en rekke punkter. Blant annet ble det tatt inn en nærmere angivelse av innholdet i de ulike sikkerhetsnivåene for eID. Forordningen ble publisert i Den europeiske unions tidende 28. august 2014 og trådte i kraft 17. september 2014. Gjennomføringsfrister og overgangsperiode er omtalt i kapittel 11.

Gjennomføringsrettsakter og delegerte rettsakter

Europakommisjonen startet våren 2014 med å utarbeide gjennomføringsrettsakter som utfyller bestemmelsene i forordningen. Til å bistå, har Kommisjonen etablert «eIDAS Expert Group» der Norge deltar. Norge deltar også som observatør i «eIDAS Committee», som avgir en vurdering av forslaget etter det såkalte komitologisystemet. Frem til dags dato er følgende gjennomføringsrettsakter vedtatt:

- Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services
- Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[5] http://www.efta.int/media/documents/eea/eea-efta-comments/2013/2013-03-19-eea-efta-comment-proposal-regulation-e-id-and-trust-services-for-electronic-transactions.pdf

- Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

EØS-posisjonsnotater om disse rettsaktene er under utarbeidelse og vil bli publisert i EØS-notatbasen.

Forordningen inneholder også bestemmelser om gjennomføringsrettsakter og delegerte rettsakter som Kommisjonen «kan» gjennomføre. Dette gjelder blant annet følgende:

- Art. 9 nr. 5 om format og prosedyre for notifisering
- Art. 17 nr. 8 om format og prosedyre for tilsynsorganets rapportering til Kommisjonen
- Art. 19 nr. 4 om sikkerhetstiltak som pålegges virksomhetene
- Art. 20 nr. 4 om akkreditering og regler for revisjon
- Art. 21 nr. 4 prosedyrer ifm. oppstart av en tillitstjeneste
- Art. 24 nr. 5 om etablering av referanser til standarder for sikre («trustworthy») systemer og produkter
- Art. 27 nr. 4 om referanser til standarder for avanserte esignaturer
- Art. 28 nr. 6 om referanser til standarder for kvalifiserte sertifikater.

5 Gjennomføring av regelverket

I EU gjelder forordninger som overnasjonale lover i den enkelte medlemsstat i kraft av å være vedtatt av de kompetente EU-organene. Ettersom EØS-avtalen ikke innebærer overføring av lovgivningsmyndighet til fellesskapsorganene, må regelverket gjennomføres i nasjonal rett.

Det følger av artikkel 7 i EØS-avtalen at gjennomføringsplikten gjelder rettsakter som er «omhandlet i eller inntatt i vedlegg til denne avtale eller i EØS-komiteens vedtak». En forordning som er innlemmet i EØS-avtalen skal derfor gjøres til en del av den interne rettsorden.

Etter artikkel 7 bokstav a skal en forordning «som sådan» gjøres til en del av den interne rettsorden. Dette innebærer at forordningen skal gjennomføres ved inkorporasjon. Inkorporasjon innebærer at det vedtas en lov- eller forskriftsbestemmelse som fastsetter at forordningen i EØS-tilpasset form skal gjelde direkte i norsk rett. Dette ivaretar hensynet til rettsenhet.

Forordninger inneholder aldri egne sanksjonsbestemmelser. Det vil derfor være nødvendig å regulere dette særskilt. Det samme gjelder tilsynsorganets beføyelser (adgang til lokale mv.) Det vil også være nødvendig å vedta ulike forskriftshjemler og hjemmel til å oppnevne tilsynsmyndighet mv.

Departementet har vurdert å foreslå å endre esignaturloven, men har kommet til at det er mer naturlig å foreslå en ny lov. Begrunnelsen for dette er at forordningen regulerer mange flere typer tjenester enn elektronisk signatur og inneholder omfattende endringer i både kravene til tilbyderne og tilsynsmyndighetene. Dersom man skulle beholde gjeldende lov, ville de fleste av de materielle bestemmelsene i esignaturloven med forskrifter uansett måtte endres. En ny lov vil være ryddigere, samtidig som man unngår misforståelser med gamle henvisninger. Departementet viser også til at Kommisjonen har opphevet esignaturdirektivet. På denne bakgrunn mener departementet at det er mest hensiktsmessig å vedta en ny lov og å oppheve esignaturloven med forskrifter.

6 Formål og virkeområde

6.1 Innholdet i forordningen

Formålet med forordningen er, som nevnt i innledningen, å sikre et velfungerende indre marked, samtidig som man ivaretar et adekvat sikkerhetsnivå for elektronisk identifisering og tillitstjenester, jf. artikkel 1. Forordningen skal ivareta dette ved å:

- Fastsette på hvilke vilkår medlemsstatene skal anerkjenne elektroniske identifikasjonsmidler for fysiske og juridiske personer som omfattes av en notifisert eID-ordning i en annen medlemsstat,
- Fastsette regler for tillitstjenester, spesielt for elektroniske transaksjoner, og
- Etablere et rettslig rammeverk for elektroniske signaturer, elektroniske segl, elektronisk tidsstempler, elektroniske dokumenter, elektroniske registrerte leveringstjenester og sertifikattjenester for webside-autentisering.

I artikkel 2 defineres virkeområdet. Forordningen gjelder for elektroniske identifikasjonsordninger som har blitt meldt inn av en medlemsstat. Videre gjelder den for tilbydere av tillitstjenester som er etablert i unionen. Hva som anses som en tillitstjeneste omtales i kapittel 7 nedenfor.

Forordningen gjelder ikke for tillitstjenester som utelukkende er brukt innenfor lukkede systemer i henhold til nasjonal lovgivning eller avtale mellom en avgrenset krets av personer. Dette er utdypet i fortalen pkt. 21 på følgende måte:

«Denne forordning bør også fastlægge en generel lovramme for brug af tillidstjenester. Der bør dog ikke indføres en generel pligt til at bruge dem eller til at oprette et adgangspunkt for alle eksisterende tillidstjenester. Den bør navnlig ikke omfatte levering af tjenester, der udelukkende anvendes i lukkede systemer mellem et defineret sæt deltagere, der ikke har virkning over for tredjemand. For eksempel bør systemer, der er oprettet i virksomheder eller offentlige forvaltninger til styring af interne procedurer ved brug af tillidstjenester, ikke være omfattet af kravene i denne forordning. Kun tillidstjenester, der udbydes til offentligheden, og som har virkning over for tredjemand, bør opfylde kravene i denne forordning.»

Forordningen får heller ikke innvirkning på nasjonal rett eller EU-rettslige regler om inngåelse av kontrakter og kontrakters gyldighet, eller andre rettslige og prosessuelle forpliktelser som gjelder formkrav, jf. artikkel 2 nr. 3.

Indre marked-prinsippet (art. 4)

I artikkel 4 stadfestes «indre marked-prinsippet», som innebærer at tilbydere av tillitstjenester har rett til, uten restriksjoner, å tilby deres tjenester i en annen medlemsstat, når tjenestens formål omfattes av forordningen. Videre skal det være fri bevegelighet for produkter og tjenester som er i samsvar med forordningen i EØS-området.

Personvern (art. 5)

Artikkel 5 nr. 1 fastsetter at behandling av personopplysninger skal skje i samsvar med EUs personverndirektiv (direktiv 95/46/EF). I fortalen pkt. 11 utdypes dette ved å vise til at autentisering i forbindelse med en online-tjeneste kun skal omfatte behandling av de identifikasjonsdata som er tilstrekkelige, relevante og ikke omfatter mer enn hva som er nødvendig for å gi adgang til den aktuelle tjenesten. Videre er det uttalt at tillitstjenestetilbydere og tilsynsorganer bør oppfylle kravene i direktiv 95/46/EF om konfidensialitet og behandlingssikkerhet.

I artikkel 5 nr. 2 slås det fast at bruken av pseudonym ikke skal være forbudt.

6.2 Departementets vurdering og forslag

Indre marked-prinsippet og personvern

Prinsippet om fri bevegelighet av varer, tjenester, personer og kapital utgjør kjernen i det indre marked. Det er avtalen om Det europeiske økonomiske samarbeidsområdet (EØS-avtalen) som formelt sett knytter Norge til det indre marked.

EUs personverndirektiv er gjennomført i personopplysningsloven, jf. lov 14. april 2000 nr. 31 om behandling av personopplysninger. Datatilsynet håndhever disse bestemmelsene. Videre er overtredelse av loven straffesanksjonert i personvern-opplysningsloven § 48. Loven gjelder generelt, og det er etter departementets syn derfor ikke nødvendig med egne tilleggs-bestemmelser om personvern i lovforslaget.

Kommisjonen fremmet 21. januar 2012 et forslag til ny personvernforordning, jf. KOM (2012) 11. Det pågår nå trilogforhandlinger mellom Rådet, Europaparlamentet og Kommisjonen om forordningsutkastet.

Avgrensningen mot lukkede systemer mv.

Som det fremgår av pkt. 5.1 ovenfor er det kun tillitstjenester som tilbys til offentligheten, og som har virkning over for tredjemann, som omfattes av forordningen.

I forarbeidene til esignaturloven diskuterte departementet om lovens virkeområde burde avgrenses mot bruk av elektronisk signatur innenfor systemer som er basert på frivillige avtaler mellom et begrenset antall deltakere, omtalt som «lukkede nett», jf. Ot.prp. nr. 82 (1999-2000) s. 21 flg. Departementet antok at eksempler på slike «lukkede nett» kunne være signaturer som brukes mellom ansatte innad i en bedrift eller som brukes innenfor en begrenset medlemsmasse, men at den nærmere grensedragningen ville måtte finne sted gjennom praksis. Etter høringsrunden, konkluderte departementet med at sertifika-tutstedere som utsteder kvalifiserte sertifikater innenfor lukkede systemer og som registrerer seg hos tilsynet, skulle omfattes av loven. Det ble blant annet uttalt at for å sikre forutberegnelighet ved bruk av elektroniske signaturer, var det ønskelig at flest mulige signaturer oppfyller kravene til kvalifiserte signaturer og dermed omfattes av lovreguleringen. Videre ble det vist til at grensegangen mellom lukkede og åpne nett var uklar og at loven burde åpne opp for at alle sertifikat-utstedere som ønsker å falle inn under lovreguleringen omfattes. Statoil er et eksempel på et selskap som har valgt å registrere seg som sertifikatutsteder, til bruk for autentiserings- og signeringsløsninger internt blant de ansatte.

Dersom man ønsker å videreføre dagens reguleringsmulighet for lukkede systemer mv., er det et spørsmål om det kan gjøres ved å utvide virkeområdet for kvalifiserte tillitstjenester nasjonalt.

Departementet er skeptisk til en slik utvidelse av virkeområdet, ettersom forordningens regulering gir tilbydere av kvalifiserte tillitstjenester vesentlig mer omfattende forpliktelser enn dagens esignaturlov. Dessuten omfattes mange flere tjenester. Sikkerhetskrav til virksomheten og kravene om samsvarsvurdering annet hvert år påfører virksomhetene kostnader. Samtidig pålegges tilsynet mer omfattende tilsynsoppgaver. Etter departementets syn taler dette imot å la forordningens bestemmelser få en videre anvendelse enn det den er ment for. Det samme gjelder hensynet til like

regler mellom landene. Departementet foreslår derfor at reglene ikke får anvendelse på lukkede systemer i henhold til nasjonal lovgivning eller avtale mellom en avgrenset krets av personer, iht. artikkel 2 og som utdypet i fortalen pkt. 21. Vi ber likevel om høringsinstansenes syn på dette.

En annen reguleringsmåte er å videreføre en selvdeklarasjonsordning, som et supplement til forordningens regulering av kvalifiserte tillitstjenester. Vi viser til omtalen av dette i høringsnotatets kapittel 8.

Når det gjelder forholdet til kontraktsretten og prosessuelle krav, omtales dette i kapittel 7.

7 Elektronisk identifisering (kapittel II)

7.1 Innholdet i forordningen

Forordningens bestemmelser om elektronisk identifisering gjelder for notifiserte («notified») eID-løsninger («electronic identification scheme») og offentlige myndigheters plikt til å anerkjenne andre lands notifiserte elektroniske identitetsbevis («electronic identification means»).

Forordningen etablerer en mulighet for medlemsstatene til å notifisere sine eID-løsninger. Notifiserte eID-løsninger på sikkerhetsnivåene betydelig og høy skal gjensidig anerkjennes for tilgang til andre EØS-lands offentlige nett-tjenester. Anerkjennelsesplikten påvirker ikke medlemsstatens rett til å avgjøre hvilket sikkerhetsnivå som skal kreves for tilgang til offentlige tjenester. Det etableres heller ingen plikt til å notifisere egne eID-løsninger.

Gjensidig anerkjennelse av eID (artikkel 6)

Regler om gjensidig anerkjennelse av eID framgår av artikkel 6. Når forvaltningen krever bruk av elektroniske identitetsbevis for å få tilgang til forvaltningens nett-tjenester, så skal elektroniske identitetsbevis fra medlemslandenes notifiserte løsninger gjensidig anerkjennes for grenseoverskridende pålogging til tjenesten. Det utenlandske identitetsbeviset må være på sikkerhetsnivå betydelig eller høyt ihht. forordningen, og dette må tilsvare et sikkerhetsnivå som er like høyt eller høyere enn det nivået som kreves i den nasjonale tjenesten. Videre er anerkjennelsesplikten begrenset til offentlige tjenester som bruker elektronisk identitetsbevis på forordningens nivå betydelig eller høyt, jf. forordningens artikkel 6 nr. 1 bokstav c.

Innholdet i anerkjennelsesplikten er ikke nærmere regulert. Forordningens artikkel 6 bruker i engelsk språkdrakt begrepet "mutual recognition" (på dansk "gjensidig anerkendelse"), men rekkevidden av anerkjennelsesplikten kan imidlertid oppfattes på to ulike måter:

1. Norske myndigheter har bare plikt til å anerkjenne andre EØS- lands notifiserte eID-løsninger etter forordningen dersom også norske løsninger er notifiserte (gjensidig anerkjennelsesplikt utløst av gjensidig notifisering). Norske myndigheter kan likevel velge å anerkjenne andre EØS-lands notifiserte løsninger for tilgang til norske offentlige tjenester.
2. Norske myndigheter har plikt til å anerkjenne andre EØS-lands notifiserte eID-løsninger etter forordningen uavhengig av om norske

løsninger er notifisert (gjensidig anerkjennelsesplikt utløst av ensidig notifisering).

Rekkevidden av anerkjennelsesplikten omtales nærmere i punkt 7.3.

Notifisering av elektronisk identifiseringsløsning (artikkel 7 og 9)

Artikkel 7 og 9 gir bestemmelser om hvordan elektroniske identifiseringsløsninger skal notifiseres.

En løsning for elektronisk identifisering skal notifiseres etter en bestemt prosedyre. Kommisjonen offentliggjør og oppdaterer en liste over notifiserte systemer. Medlemsstaten kan også trekke tilbake en melding om notifisering, slik at den ikke lenger står på listen. Videre vil sikkerhetsbrudd i løsningen (teknisk, organisatorisk, rutinemessig) kunne føre til at den notifiserte løsningen fjernes fra listen og dermed ikke lenger vil kunne brukes mot tjenester i utlandet.

Ved notifisering av eID-løsning innestår medlemsstaten for at personer i løsningen er entydig identifiserte. Videre må medlemsstaten sørge for at det er mulig for andre medlemsstater gratis å få validert elektroniske identitetsbevis fra løsningen ved bruk mot andre medlemsstaters offentlige tjenester. For eventuell bruk av identitetsbevisene mot privat sektor, kan det stilles vilkår og betingelser for tilgang til valideringstjenesten jf. artikkel 7 bokstav f, annet ledd og fortalen pkt. 17, tredje punktum. Anerkjennelsesplikten gjelder kun for offentlig sektor.

Sikkerhetsnivåer (artikkel 8)

Forordningen definerer i artikkel 8 tre sikkerhetsnivåer for elektronisk identifisering: lavt, betydelig og høyt sikkerhetsnivå. Kommisjonen har i gjennomføringsrettsak 2015/1502 av 8. september 2015 fastsatt nærmere bestemmelser om sikkerhetsnivåene. Nivåene er beskrevet ved hjelp av skjønnspregede begreper, og åpner for at nivåene kan oppnås med ulike teknologier. Gjennom notifiseringsprosessen og interoperabilitetsrammeverket (artikkel 12) legges det opp til prosesser for å sikre en felleseuropeisk forståelse av nivåene.

På høyeste sikkerhetsnivå er det krav om identitetskontroll som baseres på fysisk fremmøte hvor foto eller biometriske egenskaper som fremgår av et identitetsbevis skal sammenlignes med den fremmøttes egenskaper, jf. gjennomføringsrettsaktens pkt 2.1.2 nr 1 for HIGH, ev. andre løsninger som gir samme sikkerhet (alternativene b og c samme sted). Identitetsbeviset som benyttes skal være anerkjent av medlemsstaten som utsteder eID-en.

Det er den notifiserende medlemsstat som angir hvilket sikkerhetsnivå eID-løsningen skal notifiseres på. Dersom det oppstår uenighet, som ikke løses gjennom notifiseringsprosessen, vil fastsettelse av sikkerhetsnivå i siste instans måtte avgjøres av EU-domstolen/EFTA-domstolen.

Sikkerhetshendelser (artikkel 10)

Hvis identifiseringsløsningen utsettes for sikkerhetsbrudd eller på annen måte kompromitteres slik at tilliten til den notifiserte løsningen svekkes, så har medlemsstaten plikt til å varsle Kommisjonen og medlemsstatene om dette. Løsningen skal også settes ut av drift så langt dette er nødvendig. Hvis manglene ikke utbedres, kan det føre til at den innmeldte ordningen trekkes fra listen.

Erstatningsansvar (Artikkel 11)

Medlemsstaten, eID-utstederen og valideringstjenestetilbyderen vil være erstatningsansvarlig i henhold til nasjonal rett for skader som oppstår på grunn av manglende oppfyllelse av sine plikter etter forordningen. Medlemsstaten har ansvaret for de unike identifiseringsopplysningene som representerer personen og at valideringstjenesten er tilgjengelig, jf. artikkel 7 bokstav d og f, mens eID-utstederen er ansvarlig for at det elektroniske identitetsbeviset tildeles den aktuelle personen som opplysningene viser til, jf. artikkel 7 bokstav e.

Samarbeid og interoperabilitet (artikkel 12)

Forordningen inneholder bestemmelser som skal bidra til teknisk samordning og tillitsbyggende prosesser i forbindelse med den gjensidige anerkjennelsen av elektroniske identitetsbevis. Kommisjonen har ved gjennomføringsrettsakt 2015/1501 etablert et interoperabilitetsrammeverk som skal tilrettelegge for samhandling mellom notifiserte eID-løsninger. I rammeverket er det blant annet fastsatt tekniske minimumskrav og krav til hvilke identifiserende personopplysninger som minimum skal formidles om personene som identifiseres i notifiserte eID-løsninger. Personer skal minimum identifiseres med nåværende navn, fødselsdato og en nasjonalt valgt, unik identifikator som er så varig («persistent») som mulig, samt ett tilleggsattributt. Videre er det fastsatt regler om samarbeid mellom medlemsstatene om en faglig vurdering («peer review») av notifiserte elektroniske identifiseringsløsninger, utveksling av informasjon, erfaringer og god praksis for notifiserte eID-løsninger.

Ved notifisering skal det etableres en knytning mellom sikkerhetsnivåene ihht. nasjonalt rammeverk for de notifiserte eID-løsninger og eIDAS' sikkerhetsnivåer, jf. artikkel 12 nr. 4 bokstav b.

7.2 Eksisterende norske sikkerhetsnivåer

ID-porten, som muliggjør innlogging til offentlige nett-tjenester, støtter i dag innlogging på de to høyeste nivåene i det norske rammeverket for autentisering og uavviselighet. MinID er på det nest høyeste nivå (nivå 3), mens eID-ene fra BankID, Buypass og Commfides er på det høyeste nivået (nivå 4). Den viktigste forskjellen mellom nivåene er at det kreves personlig oppmøte for første gangs utlevering av eID på nivå 4, mens for nivå 3 baseres utlevering av eID på koder sendt til adresse registrert i folkeregisteret.

Det var i 2014 ca. 52 millioner pålogginger via ID-porten til offentlige norske nett-tjenester. De aller fleste var til nivå 3-tjenester.

7.3 Departementets vurdering og forslag

Forordningen vil kunne gjøre det enklere for innehavere av eID fra andre EØS-land å bruke norske offentlige nett-tjenester som bruker det relevante eIDAS sikkerhetsnivået. Dette gjelder naturligvis uavhengig av hvor personen fysisk oppholder seg, m.a.o. også personer som fysisk befinner seg i Norge. Ved at de kan gjenbruke sin utenlandske eID, slipper de å skaffe seg et norsk elektronisk identitetsbevis for å benytte tjenestene. Tilsvarende vil norske nettbrukere kunne få mulighet til å

gjenbruke sin eID i andre EØS-land. I hvilken grad slike gevinster oppnås, vil bero på hvordan eIDAS-sikkerhetsnivåene fortolkes og tas i bruk, ikke minst sikkerheten i, og utbredelsen av notifiserte eID-løsninger.

Anerkjennelsesplikten kan som nevnt i punkt 7.1 forstår på to ulike måter (betydningen av begrepet "gjensidig"), med noe ulike virkninger for norske tjenesteeiere. Kommunal- og moderniseringsdepartementet vil arbeide videre for å avklare disse spørsmålene.

Artikkel 6 omhandler gjensidig anerkjennelse. Anerkjennelsesplikten gjelder kun for notifiserte eID-er som er på et eIDAS sikkerhetsnivå som er likt med eller høyere enn det nasjonale nivået som kreves i tjenesten, jf. artikkel 6 nr. 1 b. Dessuten må den anerkjennende medlemsstaten bruke et eIDAS sikkerhetsnivå, jf. artikkel 6 nr. 1 c. Hvordan anerkjennelsesplikten skal fungere i praksis, dersom medlemsstaten ikke har notifisert egne løsninger, og ikke derved bruker eIDAS sikkerhetsnivåer nasjonalt, er ikke nærmere regulert i forordningen.

Departementet har som utgangspunkt at de to høyeste norske sikkerhetsnivåene vil svare til forordningens to høyeste nivåer. Sikkerhetsnivåene er definert med mange skjønnsmessige begreper, og ingen eID-løsninger er per i dag notifisert. Foreløpig er det derfor vanskelig å si hvor stort spenn det vil være mellom eID-løsningene som ligger innenfor samme sikkerhetsnivå etter eIDAS- forordningen og tilhørende rettsakter.

Spesielle problemstillinger oppstår hvis det nasjonalt stilles strengere krav til eID enn eIDAS nivå høyt. Der er departementets vurdering at tjenester som krever denne sikrere eID ikke er pliktig til å anerkjenne notifiserte eID-er på eIDAS nivå høyt, jf. at vilkårene for anerkjennelsesplikt i artikkel 6 nr. 1 ikke vil være oppfylt.

Dersom en medlemsstat skulle velge å notifisere en slik eID-løsning, vil den imidlertid bare kunne notifiseres på eIDAS nivå høyt, jf. at dette er det høyeste nivået i henhold til forordningen. Prinsippet om gjensidig anerkjennelse og bestemmelsene i artikkel 6 innebærer da at de aktuelle tjenester vil måtte akseptere andre eID-er på dette eIDAS-nivået. Notifisering vil i en slik situasjon innebære at medlemsstaten senker kravene til eID-en i tjenesten. Konsekvensen av dette vil etter departementets vurdering kunne bli at medlemsstater velger å ikke notifisere løsninger som de anser som vesentlig sikrere enn det høyeste eIDAS-nivået løsningen kan notifiseres på.

Det er et behov for å sammenligne, eller "mappe", de nasjonale sikkerhetsnivåene med eIDAS-nivåene. For notifiserte eID-løsninger er dette et krav, jf. gjennomføringsrettsakt 2015/1502 av 8. september 2015. Gitt at gjensidig anerkjennelsesplikt bare utløses av ensidig notifisering vil en lignende vurdering også være nødvendig for ikke-notifiserte eID-løsninger. Dette fordi det må avklares om vilkårene i artikkel 6 nr. 1 bokstav b er oppfylt.

Departementet vil arbeide videre med å avklare disse spørsmålene ved gjennomføring av forordningen. Forordningen foranlediger i seg selv ikke noen endring i det norske rammeverket, men

det må vurderes nærmere om det er hensiktsmessig å justere rammeverket på bakgrunn av en sammenligning med forordningens sikkerhetsnivåer.

I dag benyttes ID-porten som nav for innlogging til norske offentlige tjenester. ID-porten arbeider med å implementere støtte for eIDAS-infrastrukturen, i første omgang i forbindelse med en pilotløsning høsten 2015 for pålogging med svensk eID. Ved en eventuell innlogging med utenlandske notifiserte eID-er, vil ID-porten validere eID-en mot medlemsstatens gratis valideringstjeneste. Dersom norske eID-er skal benyttes for innlogging i utenlandske tjenester, vil Norge måtte tilby en tilsvarende gratis valideringstjeneste i ID-porten.

Identifiseringsutfordringer ved bruk av utenlandske identitetsbevis

Anerkjennelsesplikten innebærer at identitetsbeviset skal anerkjennes som et bevis for identiteten til den innloggede, på samme måte som andre identitetsbevis innenfor samme sikkerhetsnivå. Det er imidlertid kun anerkjennelsen av autentiseringen som reguleres direkte av forordningen. Koblingen av identiteten mot nasjonale tjenester er ikke regulert eller løst gjennom forordningen. Dette må det etableres nasjonale løsninger for. Hvordan dette skal gjøres i praksis, må medlemsstatene utrede nærmere.

Hvorvidt det er behov for at en innlogget person identifiseres med et nasjonalt identitetsnummer, må tjenesteeierne vurdere. Det er i så fall en nasjonal oppgave å avklare om personen er registrert i Folkeregisteret med fødselsnummer eller d-nummer fra før, og – hvis personen ikke er registrert – om personen skal registreres. Det finnes i dag nasjonale regler om slik registrering i folkeregisterforskriften. Forordningen gir ikke utlendinger flere rettigheter overfor norsk forvaltning enn i dag, og departementet vurderer det slik at forordningen ikke krever endring av dagens regelverk for tildeling av identitetsnumre i Folkeregisteret.

Flere instanser (blant annet Nav, Brønnøysundregistrene, Skatteetaten og finansinstitusjoner) er gitt kompetanse til å rekvirere d-nummer fra folkeregistermyndigheten. De skal i den forbindelse blant annet se legitimasjon fra personen som skal registreres, og i mange tilfeller kreves personlig frammøte for legitimasjonskontroll. Bekreftet kopi av legitimasjonsdokument skal sendes til folkeregistermyndigheten som registrerer personer med d-nummer hvis vilkårene er til stede. Selve legitimasjonskontrollen foretas hos rekvirenten av d-nummer. Departementet antar det normalt vil være behov for supplerende dokumentasjon til det elektroniske identitetsbeviset, før personen kan tildeles et norsk identitetsnummer. Blant annet vil det være viktig at opplysningene er tilstrekkelige til å avklare om personen er registrert fra før.

Hvilke identifiseringsopplysninger som skal følge med elektroniske identitetsbevis i notifiserte løsninger, er fastsatt i gjennomføringsrettsakt til forordningen, jf. artikkel 12 nr. 4 d. Etter norsk rett skal legitimasjonsdokument som brukes ved rekvirering av d-nummer inneholde fotografi av personen og opplysninger om fullt navn, fødselsdato, statsborgerskap og kjønn, jf. folkeregisterforskriften § 2-7 annet og tredje ledd. Bestemmelsen omhandler ikke elektroniske

identitetsbevis. Statsborgerskapsopplysninger vil imidlertid ikke automatisk følge med ved innlogging med notifiserte løsninger, og opplysning om kjønn vil bare følge med i den grad den aktuelle medlemsstat har valgt å tilby dette som tilleggsattributt. Departementet vil se nærmere på behov for endringer i norsk regelverk som kan bli nødvendig, når utenlandske elektroniske identitetsbevis skal brukes i Norge.

I arbeidet med gjennomføring av forordningen må det ses nærmere på hvordan personer som har et norsk d-nummer eller fødselsnummer kan gjenkjennes når vedkommende identifiserer seg med en utenlandsk eID fra en notifisert løsning. Hvilke identifiseringsopplysninger som formidles fra valideringstjenestene vil trolig variere fra medlemsstat til medlemsstat. For valideringstjenester som formidler et nasjonalt identitetsnummer for personen, kan det ligge bedre til rette for automatisert gjenkjenning av personen (og knytning til vedkommendes norske identitetsnummer) enn for valideringstjenester som kun formidler et løpenummer. Utfordringene på dette området har fellestrekk med identifiseringsutfordringen når personer opptrer med fysiske identitetsbevis fra utlandet, som heller ikke har norsk identitetsnummer.

8 Tillitstjenester (kapittel III)

8.1 Begrepet «tillitstjeneste», krav til tilbyderne m.m.

8.1.1 Innholdet i forordningen

8.1.1.1 Tillitstjenester - generelt

Ved å regulere tillitstjenester legger forordningen til rette for å oppnå elektronisk samhandling mellom innbyggere i Europa. Tillitstjenestene er avgrenset til å omfatte de tjenestene som er tilgjengelige og omsettes på det åpne markedet.

I artikkel 3 nr. 16 er en tillitstjeneste definert som en elektronisk tjeneste som normalt utføres mot betaling og som består av generering, kontroll og validering av elektroniske signaturer, elektroniske segl eller elektroniske tidsstempler, elektronisk registrerte leveringstjenester og sertifikater relatert til disse tjenestene, eller generering, kontroll og validering av sertifikater for websideautentisering, eller lagring av elektroniske signaturer, segl eller sertifikater relatert til disse tjenestene. Departementet oppfatter listen som uttømmende.

De fleste kravene i forordningen gjelder for kvalifiserte tillitstjenester.

En kvalifisert tillitstjeneste er i henhold til artikkel 3. nr. 17 definert som en tillitstjeneste som oppfyller forordningens krav. Dette betyr at en kvalifisert tillitstjenestetilbyder må oppfylle alle de kravene for den spesifikke kvalifiserte tillitstjenesten som tilbys, og også alle kravene som stilles for kvalifiserte tillitstjenestetilbydere gjennom forordningen.

8.1.1.2 Elektronisk signatur og elektroniske segl

Forordningen har bestemmelser om elektronisk signatur for fysiske personer (art. 25–34), og elektroniske segl for juridiske personer (art. 35-40). Innholdet i bestemmelsene for disse tillitstjenestene er de samme, og behandles derfor under ett her.

Elektronisk segl er definert i artikkel 3 nr. 25 som data i elektronisk form som er knyttet til eller logisk forbundet med andre data i elektronisk form og som gir sikkerhet for disse tilknyttede dataenes ekthet og integritet.

I forordningen stilles det vilkår for hva som skal anses som en avansert elektronisk signatur eller et avansert elektronisk segl. Disse vilkårene er de samme som bestemmelsene om avansert elektronisk signatur i direktiv 1999/93/EF. Vilkårene i artikkel 26 og 36 sikrer at signaturen eller seglet entydig kan knyttes til og identifisere undertegneren eller skaperen av seglet, at signaturen/seglet er laget kun ved hjelp av midler som vedkommende har kontroll over og er knyttet til andre elektroniske data slik at det oppdages om disse har blitt endret etter signering. Det fremgår av fortalen avsnitt 58-59 at segl vil dannes av juridiske personer, mens fysiske personer signerer.

Et kvalifisert elektronisk sertifikat kan være en bestanddel for å lage en avansert elektronisk signatur eller et avansert elektronisk segl. Forordningen stiller krav gjennom artiklene 28 og 38 til kvalifiserte sertifikater som sikrer identifisering av innehaveren av sertifikatet, og på den måten gir sikkerhet for at signaturen eller seglet virkelig tilhører vedkommende.

En avansert elektronisk signatur basert på et kvalifisert sertifikat og som er fremstilt av et kvalifisert elektronisk signaturfremstillingssystem gir en kvalifisert elektronisk signatur. Tilsvarende vil et avansert elektronisk segl basert på et kvalifisert sertifikat og som er fremstilt av et kvalifisert elektronisk seglfremstillingssystem, gi et kvalifisert elektroniske segl.

Gjennom forordningens artikkel 29 og vedlegg II til forordningen, stilles det krav til det kvalifiserte elektroniske signaturfremstillingssystemet. Dette systemet skal blant annet sikre at de elektroniske signaturgenereringsdataene med rimelig sikkerhet er konfidensielle og at de elektroniske signaturgenereringsdataene kun kan forekomme én gang. Systemet skal også sikre at de elektroniske signaturgenereringsdataene som anvendes ikke kan utledes, og at den elektroniske signaturen er beskyttet mot forfalskning og andres bruk. Kommisjonen kan fastsette gjennomføringsrettsakter hvor det oppstilles referansenummer til standarder for kvalifiserte elektroniske signaturfremstillingssystemer.

Videre skal et kvalifisert elektronisk signaturfremstillingssystem sertifiseres i henhold til artikkel 30 i forordningen. Medlemslandene skal melde fra til Kommisjonen om hvilket organ som skal foreta en slik sertifisering og hvilke systemer som har blitt sertifisert. Kommisjonen skal lage en offentlig tilgjengelig oversikt over sertifiserte signaturfremstillingssystemer, jf. art. 31. Etter art. 39 gjelder art. 29-31 tilsvarende for kvalifiserte elektroniske segl-genereringssystemer.

Sertifiseringen av kvalifiserte elektroniske signaturfremstillingssystemer skal etter artikkel 30 punkt 3 basere seg på refererte standarder fastsatt ved gjennomføringsrettsakt fra Kommisjonen. Fortalens punkt 55 uttaler at IT-sikkerhetssertifiseringen bør baseres på internasjonale standarder, som for eksempel ISO 15408, og dertil tilknyttede evaluerings-metoder og gjensidige anerkjennelsesordninger. Alternative evalueringsprosesser skal kun benyttes for evaluering av teknologiske løsninger hvor det ennå ikke er utarbeidet eller fastsatt en standard som disse systemene kan evalueres etter. Alternative evalueringsprosesser skal så langt som mulig være sammenlignbare med allerede fastsatte standarder for IT-sikkerhets-sertifisering.

Forordningen stiller i artikkel 32 krav til valideringen av en kvalifisert elektronisk signatur for å kunne fastslå gyldigheten av signaturen på signeringstidspunktet. Blant annet skal valideringen fastslå at det kvalifiserte sertifikatet var gyldig og utstedt av en kvalifisert tillitstjenestetilbyder på signeringstidspunktet. I artikkel 33 stilles det også krav til den som tilbyr en kvalifisert valideringstjeneste for kvalifiserte elektroniske signaturer, som for eksempel at valideringen skal utføres i henhold til artikkel 32 punkt 1. Artikkel 32 og 33 gjelder også for validering av kvalifiserte elektroniske segl, jf. art. 40.

En kvalifisert tillitstjenestetilbyder som tilbyr lagringstjeneste for kvalifiserte elektroniske signaturer og segl må kunne sikre rettsvirkningene av den elektroniske signaturen eller seglet over et lengre tidsrom, og garantere at de kan valideres uavhengig av teknologisk utvikling, jf. artikkel 34 og 39.

For artiklene 28-34 og 37-38 kan Europakommisjonen blant annet fastsette gjennomføringsrettsakter som definerer referansestandarder for de ulike kravene til elektroniske signaturer og elektroniske segl. Etter artikkel 30 kan Europakommisjonen fastsette en delegert gjennomføringsrettsakt med kriterier til det organet som utpekes til sertifiseringsorgan for kvalifiserte elektroniske signaturfremstillingssystemer.

8.1.1.3 Elektronisk tidsstempling

Elektronisk tidsstempel er i artikkel 3 nr. 33 definert som data i elektronisk form som binder andre data i elektronisk form til et bestemt tidspunkt og dermed utgjør bevis for at disse andre data eksisterte på det gjeldende tidspunktet.

I artikkel 42 fastsettes kravene til et kvalifisert elektronisk tidsstempel slik at de skal kunne binde sammen dato og tidspunkt på en sånn måte at det med rimelighet utelukker muligheten for å endre dataen uten at dette oppdages. De kvalifiserte elektroniske tidsstemplene skal bygge på en presis tidskilde og være signert med den kvalifiserte tillitstjenestetilbyderens avanserte elektroniske signatur eller segl, eller med annen tilsvarende metode.

Europakommisjonen kan ved hjelp av gjennomføringsrettsakter fastsette referansenummer på standarder om forbindelsen mellom data og tidspunkt for data og for bruk av nøyaktige tidskilder.

8.1.1.4 Elektronisk registrert leveringstjeneste

Elektronisk registrert leveringstjeneste er definert i artikkel 3 nr. 36 som en tjeneste som gjør det mulig å sende data mellom tredjeparter elektronisk, og dokumenterer behandlingen av de sendte data, herunder kvittering for avsendelse og mottakelse av dataene, og som beskytter de sendte data mot tap, tyveri, skade og endring.

Den kvalifiserte elektronisk registrerte leveringstjenestetilbyderen skal blant annet oppfylle krav om at tjenesten tilbys av en kvalifisert tillitstjenestetilbyder, at tjenesten med høy grad av tillit sikrer avsenderens og mottakers identitet, og at forsendelsen eller mottakelsen av data er beskyttet av en kvalifisert tillitstjenestetilbyders avanserte elektroniske signatur eller segl på slik måte at det er umulig å endre dataene uten at dette oppdages, jf. artikkel 44.

Europakommisjonen kan fastsette referansenummer til standarder om forsendelse av data og prosesser for mottakelse av data.

8.1.1.5 Sertifikat for websideautentisering

I henhold til artikkel 3 nr. 38 er et sertifikat for websideautentisering en attestasjon som gjør det mulig å autentisere en webside og knytte denne til den fysiske eller juridiske personen som sertifikatet er utstedt til. Tilbyder av kvalifiserte sertifikater for websideautentisering skal oppfylle kravene som er å finne i vedlegg IV. For eksempel skal det angis at sertifikatet er utstedt som et kvalifisert sertifikat for websideautentisering, det skal inneholde et sett data som entydig

representerer den kvalifiserte tillitstjenestetilbyderen, herunder opplysninger om hvilken medlemsstat utstederen tilhører og den juridiske personens navn, og eventuelt organisasjonsnummer.

Europakommisjonen kan fastsette referanser til standarder for kvalifiserte sertifikater for websideautentisering, hvor en ved oppfyllelse av standarden antas å oppfylle vedlegg IV.

8.1.1.6 Krav til tilbyderne – samsvarsvurdering m.m.

For at tillitstjenestene skal tas i bruk, må brukerne ha tillit til at tjenesten er sikker og fungerer. I forordningen fremkommer ulike forpliktelser for tillitstjenestetilbyderne som er utformet slik at de skal gi sikre tillitstjenester. I forhold til dagens regulering gjennom esignaturloven vil tilbydere av tillitstjenester oppleve sterkere og mer omfattende krav.

En tjenestetilbyder som ønsker å tilby en kvalifisert tillitstjeneste må etter forordningens artikkel 21 underrette tilsynsmyndigheten om dette. Sammen med meldingen skal det foreligge en samsvarsrevisjonsrapport gjennomført av et godkjent samsvarsvurderings-organ for å sjekke om tillitstjenestetilbyderen oppfyller forordningens krav. Tilsynsmyndigheten skal gjennomgå rapporten og på bakgrunn av denne avgjøre om tilbyderen av en tillitstjeneste kan anses som en kvalifisert tillitstjenestetilbyder. Først etter innvilgelsen av slik status, som markeres i tillitslisten, kan tilbyderen tilby sin kvalifiserte tillitstjeneste i markedet.

Europakommisjonen kan fastsette gjennomføringsrettsakter om formater og prosedyrer for notifisering av ny tjeneste til tilsynsmyndigheten.

Et samsvarsvurderingsorgan er i forordningens artikkel 3 nr. 18 definert som et organ som er definert i artikkel 2 nr. 13 i forordning (EF) nr. 765/2008, og som er akkreditert i overensstemmelse med den samme forordningen med kompetanse til å utføre samsvarsrevisjoner av en kvalifisert tillitstjenestetilbyder og de kvalifiserte tillitstjenestene som tilbys. Art. 2 nr. 13 omfatter organ som utfører samsvarsvurderingsvirksomhet, herunder kalibrering, overprøving, sertifisering og inspeksjon.

I henhold til artikkel 20 nr. 4 kan Europakommisjonen fastsette gjennomføringsrettsakter med referanser til standarder for akkreditering av samsvarsvurderingsorganer og samsvarsvurderingsrapporten, og for gjennomføringen av samsvarsvurderingen.

Etter artikkel 19 er tilbydere av tillitstjenester, både kvalifiserte og ikke-kvalifiserte, pålagt å gjennomføre sikkerhetsarbeid i virksomheten. Dette uttrykkes blant annet ved at de skal iverksette tekniske og organisatoriske sikkerhetstiltak som er proporsjonale med risikoen knyttet til den tjenesten de tilbyr. For å sikre transparens og oppnå tillit, er tilbyderne også pålagt å melde fra til tilsynsmyndigheten, og eventuelt andre myndigheter, om uønskede sikkerhetshendelser.

Rapporteringen skal gjøres så snart som mulig og senest innen 24 timer etter at den uønskede hendelsen er oppdaget.

Europakommisjonen kan fastsette gjennomføringsrettsakter som utdyper det sikkerhetsarbeidet tillitstjenestetilbydere er pålagt å gjennomføre, og om plikten til å rapportere om uønskede sikkerhetshendelser.

I henhold til artikkel 20 nr. 2 kan tilsynsmyndigheten gjennomføre tilsyn ved virksomheten, eller pålegge ny samsvarsrevisjon utenom den allerede fastsatte revisjonssyklusen. Ved uoverensstemmelse med forordningen, og dersom den kvalifiserte tillitstjenestetilbyderen ikke iverksetter tiltak for å rette opp i dette, kan tilsynsmyndigheten vurdere å trekke tilbake kvalifisert status og markere dette i tillitslisten, jf. artikkel 22.

Etter artikkel 20 skal tilbydere av kvalifiserte tillitstjenester hvert andre år gjennomføre en samsvarsrevisjon for å sjekke at de krav som forordningen stiller, fortsatt oppfylles. Den kvalifiserte tillitstjenestetilbyderen skal selv dekke kostnadene forbundet med samsvarsrevisjonen, og sende rapporten for gjennomgang til tilsynsmyndigheten.

Se for øvrig pkt. 10.1 om overgangsregler for kvalifiserte sertifikater mv. som er utstedt i henhold til direktiv 1999/93/EF.

Artikkel 24 stiller krav til den kvalifiserte tillitstjenestetilbyderens identifikasjonskontroll, som skal gjennomføres ved hjelp av hensiktsmessige midler og i overensstemmelse med nasjonal rett, for å sikre riktig identitet til sertifikatinnehaveren. Det stilles krav om fysisk oppmøte, slik som det også kreves etter dagens regulering i esignaturloven § 13, jf. forskrift om krav til utstedere av kvalifiserte sertifikater § 7. I tillegg tillater forordningen blant annet bruk av elektroniske identitetsbevis, hvor personlig oppmøte har vært gjennomført og som oppfyller kravene i forordningens artikkel 8 i forhold til sikringsnivåene «betydelig» og «høy».

8.1.1.7 Tillitsliste

Artikkel 22 pålegger medlemsstatene å lage, vedlikeholde og offentliggjøre tillitslister. Listen skal som et minimum inneholde oversikt over de kvalifiserte tillitstjenestetilbyderne, de skal kunne leses elektronisk og de skal signeres elektronisk eller ved elektronisk segl. Informasjon om ansvarlig myndighet for listen skal sendes til Kommisjonen.

Europakommisjonen har i en gjennomføringsrettsakt av 8. september 2015 presisert de opplysninger som det vises til i artikkel 22 punkt 1, og fastlagt nærmere tekniske spesifikasjoner og formater for tillitslisten. (Se kapittel 4 for lenke til rettsakten.)

8.1.2 Departementets vurdering og forslag

8.1.2.1 Tillitstjenester

Etter dagens esignaturlov er det kun tilbydere av elektronisk signatur som er underlagt lovreguleringen. Med forordningen introduseres begrepet tillitstjenester og dermed utvides hvem som er å anse som tilbyder og omfattes av lovreguleringen. I motsetning til i esignaturloven, omfattes også ikke-kvalifiserte tillitstjenestetilbydere. I forordningens artikkel 19 pålegges disse for eksempel å gjennomføre sikkerhetsarbeid og iverksette tekniske og organisatoriske sikkerhetstiltak som står i forhold til den tjenesten som tilbys.

I forordningens fortale fremgår det at Kommisjonens gjennomgang av virkningene av esignaturdirektivet, viste at en ved bare å regulere elektronisk signatur, ikke klarte å legge til rette for en digital samhandling mellom borgerne internt i et land, eller på tvers av landegrensene. Dagens samfunn ønsker tilgjengelige digitale løsninger. Ved for eksempel inngåelse av en avtale vil partene i avtalen velge den metoden som oppleves sikrest og mest tilgjengelig. For å kunne sidestille tradisjonelle papirdisposisjoner med elektroniske disposisjoner er det etter departementets vurdering naturlig og viktig å utvide hvilke tjenester som omfattes av en lovregulering. Ved en slik utvidelse vil det bli stilt kvalitetskrav til tjenesten og til tilbydere av tjenesten, samt bli påsett at de lovbestemte kravene følges opp.

Som beskrevet ovenfor i punkt 8.1.1 stiller forordningen krav om sertifisering av kvalifiserte elektroniske signaturfremstillingssystemer i artikkel 30. Slik departementet tolker bestemmelsen, foreligger det ikke noen plikt for medlemslandene til å tilby et slik sertifiseringssystem. Den som skal tilby kvalifisert elektronisk signatur kan velge å benytte seg av et sertifisert signaturfremstillingssystem fra et annet medlemsland.

Europakommisjonen kan i henhold til artikkel 30 fastsette en delegert rettsakt med kriterier til det organet som utpekes som sertifiseringsorgan for kvalifiserte elektroniske signaturfremstillingssystemer. Innholdet i en slik rettsakt kan påvirke hvilken myndighet som anses best egnet til å foreta sertifiseringen.

I Norge er det Nasjonal Sikkerhetsmyndighet v/SERTIT som innehar rollen som norsk sertifiseringsmyndighet etter ISO/IEC 15408 (dvs. Common Criteria) og deltar under de internasjonale avtalene CCRA og SOGIS MRA (europeisk) som kvalifisert sertifiseringsmyndighet på dette området. Etter departementets syn vil det derfor være naturlig at det er SERTIT som utpekes som sertifiseringsorgan etter artikkel 30, jf. artikkel 39 punkt 2 i Norge, dersom man ser at det er behov for å ha et system for slik sertifisering i Norge.

Departementet har i lovforslagets § 1 annet ledd gitt Kongen forskriftsfullmakt til å fastsette nærmere regler om krav til, og sertifisering av, kvalifiserte elektroniske signaturfremstillingssystemer.

8.1.2.2 Krav til tilbyderne – samsvarsvurdering m.m.

Som tidligere beskrevet får tilbydere av tillitstjenester flere og sterkere forpliktelser etter forordningen enn i dagens lovregulering. De nye kravene skal gi et harmonisert europeisk marked med sikre og brukervennlige tillitstjenester.

Et samsvarsvurderingsorgan er som nevnt i 8.1.1 et organ som er akkreditert i overensstemmelse med forordning (EF) nr. 765/2008 med kompetanse til å utføre samsvarsvurderinger av en kvalifisert tillitstjenestetilbyder og de kvalifiserte tillitstjenestene som tilbys. EØS-vareloven § 3 utpeker Norsk akkreditering som akkrediteringsorgan etter den nevnte forordningen, og det vil derfor være Norsk akkreditering som vil akkreditere eventuelle samsvarsvurderingsorganer i Norge.

I henhold til EØS-vareloven, skal Norsk akkreditering føre tilsyn med de samsvarsvurderingsorganene som det har utstedt akkrediteringsbevis til, jf. lovens § 2 og forordning (EF) nr. 765/2008 art. 5 nr. 3. Betaling for akkrediteringstjenestene er fastsatt i forskrift 1. juli 2013 nr. 821 om gebyrer for Norsk akkrediterings tjenester. Dersom et akkreditert samsvarsvurderingsorgan ikke lenger er kompetent til å utøve samsvars-vurderingsvirksomheten, eller det på en alvorlig måte har unnlatt å oppfylle sine forpliktelser, skal akkrediteringsorganet treffe «alle egnede tiltak for å begrense, midlertidig oppheve eller trekke tilbake akkrediteringsbeviset», jf. samme forordning art. 5 nr. 4.

Det foreligger ingen forpliktelse for medlemslandene til å ha et nasjonalt samsvarsrevisjonsorgan. En tjenestetilbyder vil også kunne benytte et akkreditert samsvarsvurderingsorgan fra et annet medlemsland. Dersom det er få akkrediterte samsvarsrevisjonsorganer i Europa kan man imidlertid risikere at revisjonsselskapene ikke har kapasitet til å revidere alle virksomhetene som har behov for det. Departementet mener derfor at det vil være en fordel dersom det finnes revisjonsselskaper i Norge som blir akkreditert til å være et samsvarsvurderingsorgan i henhold til forordningen.

8.1.2.3 Tillitsliste

Artikkel 22 pålegger medlemslandene å lage, vedlikeholde og publisere en tillitsliste med informasjon om de kvalifiserte tillitstjenestetilbyderne og deres kvalifiserte tillitstjenester. Medlemslandene skal notifisere til Kommisjonen det myndighetsorganet som er ansvarlig for tillitslisten.

En tillitsliste er allerede etablert gjennom Europaparlaments- og rådsdirektiv 2006/123/EC om tjenester på det indre markedet (tjenestedirektivet) artikkel 8, gjennomført ved Kommisjonsbeslutning 2009/767/EF. Medlemslandene er i henhold til disse bestemmelsene pålagt å etablere, vedlikeholde og publisere en tillitsliste med oversikt over utstedere av kvalifiserte sertifikater underlagt tilsyn. Under dagens ordning er det Nasjonal kommunikasjonsmyndighet (Nkom) som er ansvarlig for tillitslisten.

For å kunne ha en oppdatert og riktig tillitsliste, kan det være nødvendig å pålegge tillitstjenestetilbyderne å bidra til å oppfylle dette. Av denne grunn foreslår departementet at Kongen kan fastsette forskrift for tillitslisten, jf. § 1, andre ledd i lovforslaget.

Departementet foreslår at tilsynsmyndigheten skal være ansvarlig myndighet for oppfyllelse av forpliktelsene etter artikkel 22 i forordningen. Tillitslisten skal benyttes aktivt til å markere status for utstederne av tillitstjenester, og det er tilsynsmyndigheten som vil være nærmest tillitstjenestetilbyderne til å gjøre dette. Det er også tilsynsmyndigheten som vil kunne trekke tilbake kvalifisert status hos en tilbyder dersom dette viser seg nødvendig. Det er derfor mest naturlig at det er tilsynsmyndigheten som er ansvarlig myndighet for tillitslisten.

8.2 Rettsvirkninger av elektroniske signaturer og krav til referanseformater m.m.

8.2.1 Innholdet i forordningen

Artikkel 25 regulerer rettsvirkninger av elektroniske signaturer. Liknende bestemmelser gis for elektroniske segl (art. 35), elektronisk tidsstempel (art. 41), elektronisk registrerte leveringstjenester (art. 43) og elektroniske dokumenter (art. 46).

Det følger av art. 25 nr. 1 at en elektronisk signatur ikke må nektes rettsvirkning og anerkjennelse som bevis under rettssaker, alene på grunn av at den er i elektronisk form, eller at den ikke oppfyller kravene til kvalifiserte elektroniske signaturer. Tilsvarende regler finnes om elektroniske segl (35.1), elektronisk tidsstempling (41.1) og elektroniske leveringstjenester i henhold til art. 43 pkt. 1.

Etter art. 25 nr. 2 skal en kvalifisert elektronisk signatur ha samme rettsvirkning som en håndskreven underskrift.

I forordningen art. 35 nr. 2 fastsettes det at for et kvalifisert elektronisk segl, gjelder det en presumpsjon for integriteten (uforandrethet) av de data, og nøyaktigheten av opprinnelsen av de data, som det kvalifiserte elektroniske seglet er knyttet til. Tilsvarende presumpsjonsbestemmelser finnes i art. 41 nr. 2 og 43 nr. 2 om hhv. kvalifisert elektronisk tidsstempel og kvalifisert elektronisk registrert leveringstjeneste.

Etter art. 25. nr. 3 skal en kvalifisert elektronisk signatur, som er basert på et kvalifisert sertifikat og utstedt i en medlemsstat, anerkjennes som en kvalifisert elektronisk signatur i alle andre medlemsstater.

Artikkel 27 regulerer bruk av avanserte signaturer i offentlige tjenester. Dersom en medlemsstat krever bruk av avansert elektronisk signatur, herunder avansert elektronisk signatur basert på et kvalifisert sertifikat, for bruk av elektroniske tjenester hos et offentlig organ, så skal medlemsstaten også anerkjenne tilsvarende signaturer i nærmere angitte referanseformater og referansemetoder. Kommisjonen har i gjennomføringsrettsakt 2015/2016 fastsatt at tre signaturformater må anerkjennes (XAdES, CAdES, PAdES). Videre skal andre formater anerkjennes forutsatt at

tillitstjenestetilbyderens hjemland tilbyr en gratis valideringstjeneste som oppfyller nærmere angitte krav, jf. gjennomføringsrettsaktens artikkel 2. Medlemsstatene kan ikke kreve bruk av elektronisk signatur på et høyere sikkerhetsnivå enn kvalifisert elektronisk signatur, for grenseoverskridende bruk av elektroniske tjenester som tilbys av et offentlig organ, jf. forordningens artikkel 27 nr. 3.

Tilsvarende bestemmelser gjelder for elektroniske segl, jf. artikkel 37.

8.2.2 Departementets vurdering og forslag

8.2.2.1 Rettsvirkning av kvalifisert elektronisk signatur

Avtalefrihet, herunder formfrihet, er et sentralt prinsipp i norsk rett. Som utgangspunkt velger partene selv i hvilken form de ønsker å inngå en bindende avtale, for eksempel muntlig, skriftlig på papir eller elektronisk. I forbindelse med vedtakelsen av esignaturloven, valgte man å ta inn en presisering om at en kvalifisert elektronisk signatur alltid vil oppfylle et krav om underskrift, forutsatt at disposisjonen kan gjennomføres elektronisk, jf. Ot.prp. nr. 82 (1999-2000) s. 36 flg.

Etter departementets syn er derfor regelen i art. 25 nr. 1 og 2 om rettsvirkninger i tråd med norsk rett. Departementet legger til grunn at det fortsatt gjelder en forutsetning om at disposisjonen kan gjennomføres elektronisk, og viser til avgrensningen i artikkel 2 nr. 3 mot rettslige og prosessuelle forpliktelser som gjelder formkrav.

8.2.2.2 Bruk av tillitstjenester som bevis

Norsk sivilprosess bygger på prinsippet om fri bevisføring og fri bevisvurdering, jf. lov 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvisteloven) §§ 21-2 og 21-3. Dette innebærer at partene i utgangspunktet kan føre ethvert bevis de finner hensiktsmessig, og at dommeren etter en samvittighetsfull prøvelse av hele saken avgjør hvilket faktum som ut fra en sannsynlighetsvurdering skal legges til grunn. Det er således ikke noe rettslig i veien for at elektroniske dokumenter legges frem som bevis for en norsk domstol, jf. forordningens art. 25 nr. 1 og de tilsvarende bestemmelsene om elektronisk segl, tidsstempling og elektroniske leveringstjenester.

Bestemmelsene om presumpsjon for integritet og om korrekt opphav, jf. art. 35 nr. 2, 41 nr. 2 og 43.2, kan sies å gripe inn i dommerens vekting av bevisene i en rettssak. Etter departementets syn går disse bestemmelsene likevel ikke lenger enn hvordan man må anta at slike data uansett hadde blitt vurdert. De tekniske metodene som bestemmelsene gjelder, må i utgangspunktet antas å ha høy bevisverdi. Bestemmelsene er heller ikke til hinder for at motbevis føres.

8.2.2.3 Krav til signaturformater ved bruk i offentlig sektor

Forordningens krav til anerkjennelse av signaturer i referanseformater mv. vil bidra til at private kan gjenbruke sin signeringsløsning mot offentlige tjenester i ulike medlemsstater, og kan således bidra til å stimulere tilbudet av slike løsninger.

For forvaltningen innebærer forordningen at det i forbindelse med etablering av krav om bruk av elektronisk signering må tas høyde for at signaturen kan komme inn i andre formater enn det formatet forvaltningen foretrekker, jf. gjennomføringsrettsaktens bestemmelser.

Departementet legger til grunn at forordningen bare gjelder anerkjennelsen av signaturens evne til å oppfylle eventuelle formkrav om bruk av signatur, men at det ikke innebærer at ethvert signert dokument vil oppfylle alle formkrav på det aktuelle rettsområdet. Formkrav om bruk av signatur kan eksempelvis være begrunnet i at signaturen skal sannsynliggjøre at dokumentet har et bestemt opphav og et bestemt innhold. I den grad det er stilt andre krav til dokumentet eller innsendingsmåten, som at data skal sendes i et elektronisk og strukturert format, vil dette måtte vurderes for seg. Slike krav kan de facto få betydning for hvilke signaturformater som i praksis kan benyttes, ettersom signaturformatene kan ha ulik evne til å understøtte slike krav.

Norsk forvaltning stiller i dag i liten grad krav til bruk av avanserte elektroniske signaturer eller segl. I stor grad benyttes elektroniske nettløsninger som baserer seg på autentisering av aktørene, uten digital signering av dokumenter. For de løsninger som krever bruk av avanserte signaturer, vil forordningen kunne innebære behov for noen tilpasninger for å etterleve anerkjennelsesplikten. Hvor store tilpasninger som kreves, vil blant annet bero på i hvor stor grad andre signaturformater enn referanseformatene vil bli brukt og hvordan de tilhørende valideringstjenester i så fall vil utformes.

I forbindelse med videreutvikling av ID-porten arbeides det med etablering av felles signeringsløsninger. I dette arbeidet vil Difi også vurdere om det er behov for fellesløsninger for validering av signaturer og segl for at forvaltningen enklere skal kunne etterleve anerkjennelsesplikten etter forordningen.

8.2.2.4 Er det behov for å videreføre særhjemmel om esignatur i offentlig sektor?

Esignaturloven § 5 inneholder hjemmel til å fastsette nærmere regler om hvilke krav som skal stilles til kvalifiserte elektroniske signaturer som skal brukes ved kommunikasjon med og i offentlig sektor. Eforvaltningsforskriften er i dag hjemlet i både forvaltningsloven § 15a og i esignaturloven § 5. Departementet er i tvil om det er behov for å videreføre bestemmelsen. Etter departementets vurdering er forskriftskompetansen som gis i esignaturloven i all hovedsak dekket av forvaltningsloven § 15a, slik at det sannsynligvis ikke er behov for annet enn mindre justeringer av ordlyden i forvaltningsloven § 15a, når esignaturloven oppheves. Vi ber om høringsinstansenes syn på dette.

8.3 Tilsynsorganets oppgaver

8.3.1 Innholdet i forordningen

For å påse at forordningens krav til kvalifiserte tilbydere av tillitstjenester oppfylles, styrkes også forpliktelsene for tilsynsmyndighetene.

Alle medlemsland er gjennom artikkel 17 pålagt å ha en tilsynsmyndighet, enten i eget land eller etter avtale med et annet medlemsland. Tilsynsmyndigheten skal gis nødvendige fullmakter og tilstrekkelige ressurser for å kunne utøve de oppgavene som er pålagt gjennom forordningen. Tilsynsmyndighetene skal blant annet utføre tilsynsaktiviteter i forkant (ex ante) av utstedelse av en kvalifisert tillitstjeneste og ved etterfølgende (ex post) tilsynsaktiviteter overfor kvalifiserte tillitstjenestetilbydere, og også foreta handlinger overfor ikke-kvalifiserte tillitstjenestetilbydere når dette viser seg nødvendig. Tilsynsmyndigheten skal blant annet samarbeide med andre tilsynsmyndigheter, analysere samsvarsrevisjonsrapporter, informere om uønskede sikkerhetshendelser, rapportere til Kommisjonen om utført tilsynsaktivitet, innvilge og trekke tilbake kvalifisert status på tillitstjenester og informere ansvarlig myndighet for tillitslisten slik at denne kan oppdateres.

Europakommisjonen kan fastsette gjennomføringsrettsakter som definerer formatet og prosedyrene for tilsynsmyndighetens rapport om utført tilsynsaktivitet til Kommisjonen og om rapportering av uønskede sikkerhetshendelser iht. art. 19.

Gjennom artikkel 18 legges det til rette for tilsynsorganenes samarbeid over landegrenser. Tilsynsmyndighetene i de ulike medlemslandene skal samarbeide for å dele vellykket praksis, og det legges også til rette for å be tilsynsmyndighetene i et annet medlemsland om hjelp. Det forespurte tilsynsorganet kan avslå henvendelsen under nærmere bestemte vilkår som fremkommer i artikkel 18.

Dersom en tillitstjenestetilbyder melder fra til tilsynsmyndigheten om en uønsket sikkerhetshendelse i medhold av artikkel 19 skal tilsynsmyndigheten melde fra til ENISA (European Union Agency for Network and Information Security) dersom dette involverer andre medlemsland. Tilsynsmyndigheten skal utarbeide en årlig rapport til ENISA med oversikt over sikkerhetshendelser. ENISA har etablert en ekspertgruppe med deltakere fra Kommisjonen og ulike myndighetsorganer for å bli enige om implementeringen av artikkel 19, med hovedfokus på rapporteringen av uønskede sikkerhetshendelser. Norge deltar i denne ekspertgruppen.

I henhold til artikkel 20 kan også tilsynsmyndigheten gjennomføre tilsyn eller pålegge samsvarsrevisjon hos kvalifiserte tillitstjenestetilbydere. Dersom den kvalifiserte tillitstjenestetilbyderen ikke oppfyller forordningen, og heller ikke foretar handlinger for å oppfylle forordningen etter pålegg fra tilsynsmyndigheten, kan den kvalifiserte status trekkes tilbake etter en konkret helhetsvurdering av situasjonen.

8.3.2 Departementets vurdering og forslag

Tilsynsmyndighetene skal gjennomføre tilsynsaktiviteter i forkant av utstedelse av en kvalifisert tillitstjeneste og ved kontroller i ettertid, for å påse at forordningen oppfylles. Tydeliggjøringen av tilsynets oppgaver og roller slik de fremkommer i artikkel 17 bidrar til at alle tilsynsmyndigheter, uavhengig av land de er etablert i, skal gjennomføre de samme oppgavene.

For å kunne foreta et godt og grundig tilsyn med en velbegrunnet konklusjon er tilsynsmyndigheten avhengig av å kunne få tilgang til de nødvendige dokumenter om tjenestetilbyderens virksomhet. Det kan også være nødvendig å foreta kontroller i virksomhetens lokaler i forbindelse med tilsynet. Esignaturloven § 17 gir tilsynsmyndigheten tilgang til dokumenter og rett til å kreve adgang til virksomhetens lokaler. Departementet mener at det er viktig å videreføre disse beføyelsene i den nye loven slik at tilsynet skal kunne gjennomføres i samsvar med forordningens formål. Bestemmelser om dette fremkommer i lovforslagets § 4.

Departementet foreslår videre at tilsynsmyndigheten skal kunne gi påbud om at forhold som er i strid med bestemmelser etter loven skal opphøre og stille vilkår for oppfyllelse, jf. lovforslagets § 3. Om tvangsmulkt og straff, se kap. 8.5 nedenfor. Som etter gjeldende rett foreslår departementet at tilsynets enkeltvedtak skal kunne påklages, jf. lovforslagets § 6.

Som omtalt i pkt. 8.1.2 foreslår departementet også at tilsynsmyndigheten skal være ansvarlig myndighet til å føre en tillitsliste med informasjon om de kvalifiserte tillitstjenestetilbyderne og deres kvalifiserte tillitstjenester, jf. artikkel 22 i forordningen.

Som nevnt i pkt. 3.1 er Nkom utpekt som tilsynsmyndighet etter gjeldende rett. Med den nye forordningen, er det flere typer tillitstjenester som reguleres og flere forpliktelser som påhviler både tjenestetilbyderne og tilsynsorganene. Det er derfor naturlig å vurdere om Nkom fortsatt skal være tilsynsorgan med denne typen tjenester eller om det er andre myndigheter som bør ha oppgaven.

Nkom driver tilsyn med dem som tilbyr posttjenester og tilbydere av elektronisk kommunikasjonsnett og -tjeneste etter lov om formidling av landsdekkende postsendinger (postloven) og lov om elektronisk kommunikasjon (ekomloven). Nkom har som oppgave å sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester og posttjenester. Nkom har vært tilsynsmyndighet etter esignaturloven siden loven ble innført i 2001. Av forarbeidene fremgår det at Nkom ble valgt som tilsynsmyndighet blant annet fordi etaten allerede hadde ansvar for å føre tilsyn med aktørene på post- og teleområdet, og på grunn av sin kompetanse på det tekniske, økonomiske og juridiske området, jf. Ot.prp. nr. 82 (1999-2000) pkt. 8.7.3 flg. I ettertid har Nkom også fått i oppgave å føre en liste over tjenestetilbydere med hjemmel i tjenesteloven, jf. pkt. 8.1.2, som nå skal utvides gjennom forordningen.

Departementet har vurdert om det er andre myndigheter som kan være aktuell som tilsynsmyndighet, for eksempel Direktoratet for IKT og forvaltning (Difi). Som forvalter av ID-porten og Kravspesifikasjonen for PKI i offentlig sektor, har Difi god faglig kompetanse på området. Difi har imidlertid ikke erfaring med tilsynsvirksomhet, som er en kompetanse det vil ta tid å bygge opp. Det kan også oppstå en uheldig dobbeltrolle som følge av oppgavene knyttet til regelverksforvaltning og forhandlingen med eID-leverandørene i ID-porten

Etter departementets vurdering taler den erfaringen og ekspertise som Nkom har på teleområdet generelt, og som tilsynsmyndighet etter gjeldende esignaturlov spesielt, for å utpeke Nkom som tilsynsmyndighet også etter den nye loven. Nkom har også etablert et godt samarbeid med aktørene i bransjen, som det vil være nyttig å bygge videre på når det utvidete tilsynet skal etableres.

Departementet foreslår på denne bakgrunn at Nkom oppnevnes som tilsynsorgan etter den nye loven. Departementet ber imidlertid også høringsinstansene om innspill på om det er andre myndigheter enn Nkom som bør ha tilsynsoppgavene etter loven.

8.4 Erstatningsansvar og bevisbyrde

8.4.1 Innholdet i forordningen

I artikkel 13 i forordningen gis det bestemmelser om erstatning. En tillitstjenestetilbyder er erstatningsansvarlig for skade som forsettlig eller uaktsomt påføres en fysisk eller juridisk personer som følge av manglende oppfyllelse av forordningens forpliktelser.

Regelen bevisbyrde er forskjellig for den kvalifiserte tillitstjenestetilbyderen og den ikke-kvalifiserte tillitstjenestetilbyderen. For den ikke-kvalifiserte tillitstjenestetilbyderen er det den skadelidte som må bevise at tillitstjenestetilbyderen har handlet forsettlig eller uaktsomt. Den kvalifiserte tillitstjenestetilbyderen presumeres å ha handlet forsettlig eller uaktsomt med mindre den kvalifiserte tillitstjenestetilbyderen beviser at skaden oppstod uten forsett eller uaktsomhet fra tillitstjenestetilbyderens side.

I artikkel 13 punkt 2 innskrenkes erstatningsansvaret for tillitstjenestetilbydere. Dersom tillitstjenestetilbyderen gir grundig informasjon til deres kunder om begrensningene i bruken av tjenestene og disse begrensningene er identifiserbare for kundene, faller erstatningsansvaret bort for skader som påføres ved at bruken av tjenesten går utover de begrensninger som ligger i den.

8.4.2 Departementets vurdering og forslag

Artikkel 13 skal anvendes i overensstemmelse med nasjonale regler om erstatningsansvar. Dette utdypes i fortalens punkt 37 hvor det fremkommer at forordningen ikke skal påvirke nasjonale bestemmelser om definisjonen av skade, forsett, uaktsomhet eller relevante prosedyreregler. Det foreligger derfor ikke behov for egne nasjonale regler som behandler erstatning i forhold til forordningen. Også etter gjeldende lov er det omvendt bevisbyrde for utstedere av kvalifiserte sertifikater, jf. esignaturloven § 22, andre ledd.

8.5 Sanksjoner – straff og tvangsmulkt

8.5.1 Innholdet i forordningen

Etter forordningen art. 16 er det medlemsstatene som fastsetter sanksjoner for overtredelse av forordningen. Sanksjonene skal være effektive, stå i rimelig forhold til overtredelsen og ha avskrekkende virkning.

8.5.2 Departementets vurdering og forslag

Som det fremgår av pkt. 2.1 inneholder esignaturloven bestemmelser om både tvangsmulkt og straffansvar for en sertifikatutsteder. Etter det departementet er kjent med, har bestemmelsene hittil ikke vært brukt og aktørene i bransjen har vært opptatt av gode skussmål. Spørsmålet er om bestemmelsene bør videreføres. Loven vil omfatte en rekke nye typer tillitstjenester som hittil ikke har vært særskilt regulert, der en tjenestetilbyder pålegges flere plikter.

Tilsynsmyndigheten har imidlertid allerede en rekke beføyelser som kan iverksettes ved brudd på pliktene, jf. pkt. 8.1.1. Når det gjelder brudd på bestemmelsene om personopplysninger, dekkes disse av den generelle straffebestemmelsen i personopplysningsloven § 48. Departementet antar også at enkelte tilfeller vil omfattes av markedsføringslovens sanksjonsbestemmelser, for eksempel utstedelse av kvalifiserte tillitstjenester som i virkeligheten ikke er kvalifiserte.

Etter departementets syn taler likevel preventive hensyn og hensynet til en effektiv håndheving, at dagens straffebestemmelse og adgangen til å ilegge tvangsmulkt videreføres. De forpliktelsene som forordningen pålegger utstederne av tillitstjenester, er med på å ivareta viktige offentlige eller private interesser, og brudd på pliktene kan få alvorlige konsekvenser for dem som rammes. Ved at forordningen innfører regler om flere typer tillitstjenester, er det sannsynlig at det vil oppstå et nytt marked. En straffebestemmelse kan virke preventivt mot useriøse aktører. Det kan likevel være grunn til at bestemmelsene begrenses til å gjelde utstedere av *kvalifiserte* tillitstjenester. Deres tjenester benyttes normalt til transaksjoner av stor betydning for brukerne og der bevaring av tillit er ekstra viktig.

Som etter gjeldende rett, foreslår departementet at tvangsmulkt skal kunne anvendes for å sikre at bestemmelser som er gitt i eller i medhold av loven overholdes. Mulkten skal ikke løpe før klagefristen er ute, og ved klage, løper ingen tvangsmulkt før klagesaken er avgjort, med mindre klageorganet bestemmer noe annet. Som etter gjeldende rett, må mulktens størrelse fastsettes i lys av alminnelige forvaltningsrettslige prinsipper, herunder hensynet til rimelig forholdsmessighet mellom det målet som søkes oppnådd og de virkemidlene som benyttes, jf. Ot.prp. nr. 82 (1999-2000) s. 55.

Når det gjelder straff, må loven presisere nærmere hvilke bestemmelser som kan håndheves med dette, jf. Grunnloven § 96 om at straff krever hjemmel i formell lov. De forpliktelser som følger av forordningen er av ulik karakter og har ulik presisjonsgrad, jf. for eksempel sikkerhetskravene i art. 19 nr. 1. Departementet har vektlagt at det må fremgå klart og tydelig hvilke handlinger som kan

medføre straff. Departementet foreslår på denne bakgrunn at straff kan idømmes den som forsettlig eller grovt uaktsomt

a. opptrer som utsteder av kvalifisert tillitstjeneste uten å være registrert som dette etter loven
b. unnlater å gi opplysninger etter § 3
c. gir uriktige eller villedende opplysninger til tilsynet.

8.6 Gebyr

Som nevnt i pkt. 3.1 gir esignaturloven § 24 gir hjemmel for å fastsette at registreringspliktige utstedere skal betale gebyr til tilsynet og at gebyrene ikke må overstige kostnadene ved tilsynets virksomhet.

I forordningen utvides tilsynets oppgaver, både med hensyn til tilsynsobjekter og tilsynsoppgaver. Departementet foreslår at tilsynet fortsatt skal finansiere sin tilsynsvirksomhet gjennom gebyrer fra dem som omfattes av regelverket og at nærmere retningslinjer fastsettes i forskrift. Det vil i den forbindelse være naturlig å gjennomgå gebyrpraksis slik den har vært frem til nå. Departementet forutsetter videre at gebyrene fastsettes slik at de dekker kostnadene ved tilsynets virksomhet, samtidig som de heller ikke overstiger disse, jf. Finansdepartementets retningslinjer for gebyr- og avgiftsfinansiering av statlige myndighetshandlinger (R-112/2006 og R-4/2006).

Samferdselsdepartementet er ansvarlig for gebyrforskriften til Nkom. Forutsatt at Nkom blir tilsynsmyndighet etter den nye loven, vil det være naturlig at kompetansen til å fastsette forskrifter etter lovforslagets § 7 delegeres til Samferdselsdepartementet.

9 Bør selvdeklarasjonsordningen beholdes?

Som omtalt i pkt. 3.1 gir esignaturloven § 16 a hjemmel til å etablere frivillige sertifiserings-, godkjennings- eller selvdeklarasjonsordninger for sertifikatutstedere. Formålet er å øke tilliten til og derved bruken av elektroniske signaturer. Gjennom slike ordninger er det etter dagens regler mulig å stille tilleggskrav utover de krav som allerede gjelder i esignaturloven for kvalifiserte sertifikater og utstedere av slike. Ordningene vil også kunne stille krav på andre sikkerhetsnivåer.

En selvdeklarasjonsordning er innført for sertifikatutstedere som ønsker å tilby sertifikater i offentlig sektor i henhold til «Kravspesifikasjon for PKI i offentlig sektor». Videre inneholder enkelte lover, deriblant hvitvaskingsloven med forskrift, en henvisning til samme regelsett. I kravspesifikasjonen fremgår det under pkt. 1.3 at selvdeklarerte sertifikatutstedere skal levere *basis sertifikattjenester* for bruksområdene autentisering og signering med tilhørende statustjenester og oppslagstjenester. Sertifikatutstederne kan velge hvorvidt de vil levere sertifikater for bruksområdet kryptering og hvilke underliggende tjenester de vil levere.

Når det gjelder tillitstjenester som er omfattet av forordningen, vil en ordning med *selvdeklarasjon* ikke oppfylle forordningens krav. Som det fremgår av pkt. 8.1.1 stiller forordningen krav om at det skal foreligge en samsvarsvurdering og en kontroll av denne og registrering hos tilsynsmyndigheten, før tilbyderen kan tilby tillitstjenester. Dette innebærer med andre ord en godkjenningsordning.

Utenfor forordningens virkeområde kan det imidlertid være behov for å beholde en selvdeklarasjonsordning mv., for eksempel for rene autentiseringstjenester og krypteringstjenester. Her vil en selvdeklarasjonsordning kunne være med på å øke tilliten til slike tjenester. Videre vil det, etter departementets syn, være mulig rettslig sett å beholde en selvdeklarasjonsordning for tillitstjenester på et lavere nivå enn kvalifisert. Her er det ikke krav om forhåndsgodkjenning i forordningen. I en slik ordning vil det uansett være nødvendig å tilpasse kravene til forordningen. Det samme gjelder ved eventuelt ønske om å innføre frivillige sertifiseringstjenester.

Kommunal- og moderniseringsdepartementet vil vurdere behovet for å opprettholde en særskilt kravspesifikasjon for PKI offentlig sektor og eventuelt tilpasse kravene i denne til forordningen. Situasjonen er forandret fra det tidspunktet da spesifikasjonen første gang ble etablert (2005), da man ikke hadde fellesløsninger for eID i offentlig sektor. I dag har vi en velfungerende ID-port med eID på høyeste nivå, forvaltet av én aktør (Difi). Samordningsbehovet, som kravspesifikasjonen dels skal ivareta, er således ivaretatt på andre måter. Samtidig må man også vurdere hvilke implikasjoner eventuelle endringer vil få for de eID- og esignaturløsninger som er hjemlet i andre lover og som henviser til selvdeklarasjonsordningen som gjelder for offentlig sektor.

Departementet foreslår på denne bakgrunn at hjemmelen til å etablere frivillige sertifiserings-, godkjennings- eller selvdeklarasjonsordninger for sertifikatutstedere beholdes inntil vurderingen av behovet for å beholde Kravspesifikasjon for PKI i offentlig sektor er gjennomført. Vi ber samtidig om høringsinstansenes syn på reguleringsbehovet.

10 Avsluttende bestemmelser, ikrafttredelse og overgangsperiode

10.1 Innholdet i forordningen

Forordningen trådte i kraft 17. september 2014 og gjelder direkte i EUs medlemsstater. Fristen for å gjennomføre forordningen i nasjonal rett er 1. juli 2016, jf. artikkel 52, med noen unntak.

10.1.1 Overgangsordning for bestemmelsene om eID

Artikkel 6 om gjensidig anerkjennelse av eID får anvendelse fra tre år etter gjennomføringsrettsaktene i medhold av art. 8, nr. 3 og art. 12, nr. 8 (bestemmelser om minimumsstandarder for sikkerhetsnivå, og interoperabilitet m.m.) er på plass. Fristen for å vedta disse gjennomføringsrettsaktene er 18. september 2015. En ordning med gjensidig anerkjennelse av eID må dermed være på plass fra 18. september 2018.

Artikkel 52 nr. 4 gir medlemslandene mulighet til å anerkjenne et annet medlemslands notifiserte eID på frivillig basis, når gjennomføringsrettsaktene er på plass 18. september 2015. Etter art. 52 nr. 2 b) får art. 7 (vilkår for notifisering), art. 8, nr. 1 og 2 (angivelse av sikkerhetsnivå), art. 9 (notifisering), 10 (sikkerhetsbrudd), 11 (erstatningsansvar) og art. 12 nr. 1 (interoperabilitet), anvendelse når gjennomføringsrettsaktene i medhold av art. 8 nr. 3 og 12 nr. 8 er på plass 18 september 2015.

10.1.2 Overgangsordning for kvalifiserte sertifikater og registrerte tjenestetilbydere

Etter art. 51 nr. 2 skal kvalifiserte sertifikater som er utstedt til fysiske personer i henhold til esignaturdirektivet (1999/93/EF), anses som kvalifiserte sertifikater for elektroniske signaturer i henhold til forordningen, inntil de utløper.

Etter art. 51 nr. 3 har en som har utstedt kvalifiserte sertifikater i henhold til direktiv 1999/93/EF mulighet til å beholde sin status som kvalifisert tjenestetilbyder dersom vedkommende forelegger en samsvarsvurderingsrapport for tilsynsorganet så snart som mulig, og senest 1. juli 2017.

10.2 Departementets vurdering og forslag

For at regelverket skal gjelde i Norge, må forordningen tas inn i EØS-avtalen og gjennomføres i norsk rett. Forutsatt at lovforslaget fremmes og vedtas i løpet av høstsesjonen 2016, legger departementet opp til at loven trer i kraft 1. januar 2017 og at de samme regler som skal gjennomføres i EU innen denne dato, gjennomføres i norsk rett samtidig.

Dette innebærer at forskrifter som gjennomfører rettsakter med hjemmel i kapittel II om eID, først vil være på plass høsten 2018, jf. omtalen i pkt. 9.1 over.

Etter departementets syn er det ikke nødvendig å vedta egne overgangsbestemmelser som gjelder status for et kvalifisert sertifikat som er utstedt med hjemmel i esignaturloven, eller som gjelder statusen til en utsteder av kvalifiserte sertifikater. Dette er regulert i forordningen, jf. pkt. 9.1. Når det gjelder forskrifter med hjemmel i esignaturloven foreslår departementet at disse skal gjelde inntil de blir opphevet. Det samme skal gjelde for eventuelle erstatningskrav som er idømt etter loven.

11 Endringer i annet regelverk

Departementet har ikke identifisert lover som inneholder henvisninger til lov om elektronisk signatur. En rekke forskrifter inneholder derimot henvisninger til esignaturloven med forskrifter:

- Forskrift 29. desember 2007 nr. 1610 om behandling av helseopplysninger i nasjonal database for elektroniske resepter (reseptformidlerforskriften) § 2-4
- Forskrift 4. oktober 2013 nr.1185 om forsvars- og sikkerhetsanskaffelser §§7-3 og 11-2
- Forskrift 21. februar 2005 nr. 168 om gebyr til Post- og teletilsynet § 5
- Forskrift 13. mars 2009 nr. 302 om tiltak mot hvitvasking og terrorfinansiering mv. § 6

- Forskrift 7. april 2006 nr. 402 om offentlige anskaffelser § 7-3
- Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) §§ 2, 3, 4 og 18
- Forskrift 25. juni 2010 nr. 977 om elektronisk kommunikasjon med namsmannen og Statens innkrevingssentral i saker etter tvangsfullbyrdelsesloven og i saker for forliksrådet § 8
- Forskrift 20. september 2013 nr. 1097 om behandling av opplysninger i po1itietog påtalemyndigheten (politiregisterforskriften) § 36-4
- Forskrift 3. mai 2007 nr. 476 om prøveprosjekt for e-kommunikasjon § 4.

Departementet vil utarbeide et eget høringsnotat med forslag til nødvendige forskrifts-endringer. Noen av vurderingene i det høringsnotatet vil avhenge av hvilke endringer som vil bli foretatt i Kravspesifikasjon for PKI i offentlig sektor, jf. kapittel 8 ovenfor.

12 Om lovens anvendelse på Svalbard

Esignaturloven som gjelder i dag, er ikke gjort gjeldende for Svalbard. Som ikke-medlem av EØS, er Svalbard utenfor det indre marked, og faller dermed utenfor hovedformålet med den nye loven. Det å sikre tillit ved samhandling på internett og felles løsninger på tvers av landegrensene vil imidlertid også være interessant for Svalbard. På samme måte som i gjeldende lov, foreslår departementet derfor en forskriftshjemmel i den nye loven som gir Kongen myndighet til å gi loven anvendelse for Svalbard og Jan Mayen. Det vil være behov for en egen vurdering og gjennomgang dersom loven skal gjøres gjeldende for Svalbard.

13 Økonomiske og administrative konsekvenser

Gjensidig anerkjennelse av eID og esignatur i offentlig sektor (kap. II, art. 27 og 37)
Rettsakten vil få administrative og økonomiske konsekvenser i forbindelse med nettjenester som omfattes av anerkjennelsesplikten og eventuell notifisering av norske eID-løsninger. Det må tilrettelegges for innlogging med utenlandsk eID og for at notifiserte norske eID-er kan benyttes i nett-tjenester i utlandet/EØS. Offentlige myndigheter som krever bruk av elektroniske signaturer eller segl vil iht. forordningen (art. 27 og 37) måtte anerkjenne tilsvarende signaturer eller segl fra utlandet i nærmere bestemte formater. Enklere gjenbruk av eID-er forventes imidlertid å føre til økt anvendelse av digitale selvbetjenings-løsninger både nasjonalt og på tvers i EU/EØS og følgelig medføre samfunnsøkonomiske gevinster og kostnadsbesparelser.

Etter departementets vurdering er det ønskelig at offentlige myndigheter som tilbyr elektroniske tjenester i større grad kan tilby slike tjenester til brukere som har utenlandske eID-er. Elektroniske tjenester og fagsystemer er som oftest avhengig av at utenlandske brukere kan identifiseres gjennom fødselsnummer/d-nummer eller organisasjonsnummer. Rettsakten kan få administrative og økonomiske konsekvenser i forbindelse med utstedelse av egne identifikasjonsnumre til slike brukere. Spesielt vil dette gjelde for Folkeregisteret.

Elektroniske tillitstjenester (kap. III)

Et mer omfattende tilsynsregime og en rapporteringsplikt for tilsynsmyndigheten til Kommisjonen og ENISA vil videre få økonomiske og administrative konsekvenser for Nasjonal kommunikasjonsmyndighet (Nkom) som er foreslått som tilsynsmyndighet. Ettersom tilsynets virksomhet er gebyrfinansiert, legges det opp til at tilsynets økte kostnader finansieres ved høyere gebyrer. Omfanget av tilsynsoppgavene vil være avhengig av antall markedsaktører og antall tillitstjenester de tilbyr. På bakgrunn av innspill fra Nkom anslås de økte tilsynsoppgavene å ville medføre ytterligere 1 årsverk i tillegg til eksisterende 2,5 årsverk som dekker dagens tilsynsoppgaver på området. Viser tilsynsoppgavene seg mer omfattende enn forutsatt eller en får en økning i antall nye tillitstjenester vil antall årsverk måtte oppjusteres. Dette vil få økonomiske konsekvenser for sertifikatutstedere. Sertifikatutstederne vil også få økte administrative og økonomiske kostnader som følge av de strengere kravene til virksomhetene og kravet om hyppigere revisjoner. I siste instans vil sluttbrukerne måtte betale mer for sertifikattjenestene.

Videre kan kravene til elektronisk registrert leveringstjeneste tenkes å få økonomiske og administrative konsekvenser for Altinn og Digital postkasse samt private leverandører av elektroniske postkasser. Dette avhenger av det nærmere innholdet i Europakommisjonens gjennomføringsrettsakter, når disse er på plass.

Norsk akkreditering er nasjonalt akkrediteringsorgan. Et samsvarsvurderingsorgan som vil bli akkreditert i Norge, må søke om dette til Norsk akkreditering, som vurderer om organet oppfyller de krav som følger av EØS-vareloven, bestemmelsene som foreslår i det foreliggende lovforslaget, og eventuelt nærmere forskrifter. Akkrediteringsvirksomheten finansieres gjennom gebyrer, jf. forskrift 1. juli 2013 nr. 821 om gebyrer for Norsk akkrediterings tjenester, som skal dekke samtlige kostnader for akkrediteringen.

Forslag
til lov om gjennomføring av EUs forordning om elektronisk identifisering og tillitstjenester for elektroniske transaksjoner på det indre marked (lov om elektroniske tillitstjenester)

§ 1 *eID og elektroniske tillitstjenester i EØS*

EØS-avtalen vedlegg XI nr. … (forordning (EU) nr. 910/2014) om elektronisk identifisering og tillitstjenester for elektroniske transaksjoner på det indre marked gjelder som lov med de tilpasninger som følger av vedlegg XI, protokoll 1 til avtalen og avtalen for øvrig.

Kongen kan gi forskrift om myndighetssamarbeid, etablering av et felles tillitsmerke, fastsettelse av sikkerhetsnivåer, etablering av rammeverk for sikring av notifiserte nasjonale eID-løsningers interoperabilitet, tillitslister, om akkreditering av samsvarsvurderingsorganer, utforming av samsvarsrevisjonsrapport og regler for gjennomføring av samsvarsrevisjoner, om krav til, og sertifisering av, kvalifiserte elektroniske signatur- og seglfremstillingssystemer, om kvalifiserte valideringstjenester for elektronisk signatur og elektronisk segl, og om referanseformater m.m. for avansert elektronisk signatur og avansert elektronisk segl i offentlig sektor.

Kongen fastsetter hvilket organ som skal være notifiseringsmyndighet overfor Kommisjonen.

Kongen fastsetter hvilket organ som skal opprette, ajourføre og offentliggjøre en tillitsliste.

Kongen fastsetter hvilket organ som skal godkjenne kvalifiserte elektroniske signaturfremstillingssystemer.

§ 2 *Etablering av frivillige sertifiseringsordninger, godkjenningsordninger eller selvdeklarasjonsordninger*

I de tilfellene der det ikke allerede er et krav om det etter § 1, kan departementet for å høyne nivået for, og øke tilliten til, bruk av elektroniske tillitstjenester gi forskrift om frivillige sertifiserings-, godkjennings- eller selvdeklarasjonsordninger, herunder hvilke krav som stilles for slike frivillige ordninger.

Departementet fastsetter hvilket organ som skal godkjenne og føre tilsyn med de frivillige ordningene.

§ 3 *Tilsyn*

Kongen fastsetter hvilket organ som skal føre tilsyn med at bestemmelsene gitt i eller i medhold av loven, blir oppfylt.

Som ledd i tilsynet, kan tilsynsorganet gjennomføre kontroll hos virksomhetene, kreve de opplysninger og dokumenter som er nødvendige for å utføre tilsynet, og fastsette en tidsfrist for å sende dem inn.

Den som blir kontrollert, plikter å gi tilsynsorganet uhindret adgang til virksomheten, lokaler, utstyr og dokumentasjon og til å gi opplysninger og ellers medvirke til gjennomføringen av kontrollen.

Tilsynsorganet kan gi påbud om at forhold som er i strid med bestemmelser gitt i eller i medhold av denne loven, skal opphøre og kan stille vilkår som må oppfylles for at virksomheten skal være i samsvar med loven.

Kongen kan gi forskrift om tilsynets virksomhet.

Kongen kan i forskrift bestemme at tjenestetilbydere som er registreringspliktige etter § 1 skal betale gebyr. Gebyrene må ikke overstige kostnadene ved tilsynets virksomhet.

§ 4 *Tvangsmulkt*

For å sikre at bestemmelser gitt i eller i medhold av denne loven overholdes, kan tilsynsorganet bestemme at en kvalifisert tjenestetilbyder skal betale en daglig løpende mulkt til staten inntil lovstridig virksomhet er opphørt eller pålegg og vilkår gitt med hjemmel i loven er etterkommet. Adgangen til å ilegge tvangsmulkt gjelder tilsvarende for tilsynsmyndigheten for frivillige ordninger regulert i forskrift gitt med hjemmel i § 2.

Mulkten løper ikke før klagefristen er ute. Påklages vedtaket om tvangsmulkt, løper ingen tvangsmulkt før klagesaken er avgjort med mindre klageorganet bestemmer annerledes.

Tilsynet kan frafalle påløpt tvangsmulkt.

§ 5 *Straff*

Med bøter straffes den som forsettlig eller grovt uaktsomt

a) opptrer som utsteder av kvalifisert tillitstjeneste uten å være registrert som dette etter loven
b) unnlater å gi opplysninger etter § 3,
c) gir uriktige eller villedende opplysninger til tilsynet.

§ 6 *Klageadgang*

Tilsynets avgjørelser etter bestemmelser gitt i eller i medhold av denne loven, kan påklages til det organ Kongen utpeker.

§ 7 *Gebyr*

Kongen kan gi forskrift om at tjenestetilbydere som er registreringspliktig etter loven eller etter forskrift gitt med hjemmel i § 2, skal betale gebyr. Gebyrene må ikke overstige kostnadene ved tilsynets virksomhet.

§ 8 *Anvendelse på Svalbard og Jan Mayen*

Kongen kan gi forskrift om lovens anvendelse på Svalbard og Jan Mayen og fastsette særlige regler under hensyn til de stedlige forhold.

§ 9 *Ikrafttredelse*

Loven gjelder fra den tid Kongen bestemmer. Fra samme tidspunkt oppheves lov 15. juni 2001 nr. 81 om elektronisk signatur.

§ 10 *Overgangsregler*

Forskrifter og enkeltvedtak gitt i medhold av lov 15. juni 2001 nr. 81 om elektronisk signatur, gjelder inntil de blir opphevet. Det samme gjelder utpeking av tilsynsmyndighet og klageorgan, samt eventuelle idømte erstatningskrav med hjemmel i samme lov.