ERHVERVS- OG VÆKSTMINISTERIET

SUPPLERENDE GRUND- OG NÆRHEDSNOTAT TIL FOLKETINGETS EUROPAUDVALG

Forslag til forordning e-signatur og elektronisk identifikation

Ændringer er markeret med streg i marginen.

1. Resumé

Kommissionen har den 4. juni 2012 stillet forslag om en forordning om identifikation og tillidstjenester. Forslaget er fremsat med henblik på at fremme borgere og virksomheders muligheder for at anvende elektroniske tjenester på tværs af EU's indre grænser.

Forslaget skal erstatte det eksisterende direktiv om elektroniske signaturer, 1999/93/EF, men har et bredere anvendelsesområde, idet forordningen i tillæg til regulering af elektroniske signaturer også regulerer en bredere gruppe af elektroniske tillidstjenester samt elektroniske identiteter og dokumenter.

2. Baggrund

Kommissionen har den 4. juni 2012 fremsat forslag til forordning om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (KOM(2012) 238).

Forslaget til forordningen er baseret på TEUF artikel 114 om harmonisering af medlemsstaternes lovgivninger vedrørende det indre markeds funktion og den frie bevægelighed for tjenesteydelser.

Forslaget skal vedtages af Rådet og Europa-Parlamentet efter den almindelige lovgivningsprocedure, jf. traktatens artikel 294. Rådet træffer afgørelse med kvalificeret flertal.

Baggrunden for forslaget er, at lovgivning om elektroniske signaturer samt gensidig anerkendelse af elektronisk identifikation og autentifikation er nøgletiltag i Den digitale dagsorden for Europa (KOM(2010)245). Lovgivning om gensidig anerkendelse af elektronisk identifikation og autentifikation på EU-plan og revision af direktivet om digitale signaturer er også blandt nøgletiltagene i akten for det indre marked (KOM(2011)206). Endelig understreger køreplanen for stabilitet og vækst (KOM(2011)669)

vigtigheden af at udvikle den digitale økonomi ved hjælp af den fremtidige lovramme, der skal sikre gensidig anerkendelse og accept af elektronisk identifikation og autentifikation på tværs af grænserne.

Den eksisterende EU-lovgivning dækker udelukkende elektroniske signaturer og udgør ikke en omfattende sektor- og grænseoverskridende EU-ramme for sikre, pålidelige og brugervenlige elektroniske transaktioner, der omfatter elektronisk identifikation, autentifikation og signaturer.

I forbindelse med fremsættelse af det foreliggende forordningsforslag afgav Kommissionen en konsekvensanalyse (KOM (2012) 238 endelig). I analysen beskrives de overvejelser, der ligger til grund for Kommissionens forslag.

Det anføres bl.a., at der er identificeret en opsplitning af markedet, idet der gælder forskellige regler for tjenesteydere afhængig af, i hvilken medlemsstat de leverer ydelsen. Disse forskellige nationale lovgivninger gør det svært for brugerne at føle sig sikre, når de interagerer på internettet.

De fire vigtigste årsager til disse problemer er ifølge Kommissionen:

A. Utilstrækkeligt anvendelsesområde for det nuværende lovgrundlag
B. Utilstrækkelig koordination mellem udvikling af elektroniske signaturer og elektronisk identifikation
C. Utilstrækkelig gennemsigtighed i sikkerhedsgarantier
D. Manglende bevidsthed/brugeranvendelse

Det er Kommissionens vurdering, at disse problemer alene vil blive løst, hvis der introduceres ny lovgivning med en udvidelse af anvendelsesområdet. For at sikre umiddelbar anvendelighed uden fortolkning og dermed større harmonisering har Kommissionen besluttet at benytte forordningsmodellen som retligt instrument.

Ligesom det er tilfældet med direktiv 99/93/EF, er retsgrundlaget for lovforslaget artikel 114 i TEUF om det indre marked, fordi den har til formål at fjerne eksisterende hindringer for det indre markeds funktion ved at fremme gensidig anerkendelse og accept af elektronisk identifikation, elektroniske signaturer og supplerende tillidstjenester på tværs af grænserne, når det er nødvendigt i forbindelse med elektroniske transaktioner.

Kommissionen anfører, at en indsats på EU-plan er tilstrækkelig og forholdsmæssig til at gennemføre det digitale indre marked på grund af de elektroniske tjenesters iboende ikke-territoriale karakter. Lovgivningsmæssige foranstaltninger truffet på nationalt plan kan som følge heraf ikke forventes at give det samme udfald. Det er derfor Kommissionens vurdering, at EU-intervention er påkrævet, hensigtsmæssig og berettiget.

3. Formål og indhold

3.1 Indledning

Forslaget til forordning har til formål at erstatte direktiv 1999/93/EF om en fællesskabsramme for elektroniske signaturer. Dette direktiv vil blive ophævet ved forordningens ikrafttrædelse. Den danske implementering af direktiv 1999/93/EF er sket ved lov nr. 417 af 31. maj 2000 om elektroniske signaturer. Denne lov regulerer ikke forhold ud over direktivet, hvorfor den ligeledes ved forordningens ikrafttrædelse skal ophæves.

En ophævelse af lov om elektroniske signaturer forventes i sig selv ikke at have praktisk betydning for Danmark, idet der ikke i øjeblikket udstedes elektroniske signaturer på baggrund heraf. Forslaget til forordning regulerer imidlertid et bredere område, end hvad der følger af den eksisterende regulering. Vedtagelse af forslaget vil derfor formentlig betyde, at den danske standard for Offentlige Certifikater til Elektronisk Service (OCES) og signaturer udstedt i medfør heraf vil blive omfattet af forordningen.

En række væsentlige tekniske forhold, herunder særligt vedrørende anvendelse af standarder og sikring af interoperabilitet mellem medlemsstaterne er endnu ikke fastlagt. Dette betyder, at det på nuværende tidspunkt ikke er muligt præcist at fastslå, hvorledes forslaget til forordning vil blive udmøntet i praksis. Kommissionen er som beskrevet nedenfor bemyndiget til at vedtage nærmere om disse forhold efter forordningens ikrafttræden.

Det bemærkes, at forslaget som beskrevet ovenfor i en række henseender tager udgangspunkt i den regulering, der følger af det gældende direktiv om en fællesskabsramme for elektroniske signaturer, der er gennemført i dansk ret ved lov om elektroniske signaturer. På denne baggrund vil der i det følgende hovedsageligt blive fokuseret på de nyskabelser og ændringer, som forslaget vil indebære.

I det følgende (afsnit 3.2 til afsnit 3.7) gennemgås de enkelte kapitler i forslaget til forordning.

3.2 Generelle bestemmelser (kapitel I)

I kapitel 1 fastsættes regler om forordningens genstand og formål og dens materielle og territorielle anvendelsesområder. Endvidere defineres en række udvalgte begreber.

Forslaget til forordningen har til formål at sikre fri bevægelighed inden for det indre marked for tillidstjenester og produkter, der overholder forordningens bestemmelser.

Forslagets overordnede formål er at fastlægge regler for:
1) Elektronisk identifikation i form af elektroniske identifikationsordninger
2) Elektroniske tillidstjenester til brug for elektroniske transaktioner
med det formål at sikre, at det indre marked kan fungere efter hensigten.

Ad.1) Elektronisk identifikation
Elektroniske identifikationsordninger har i praksis karakter af nationale elektroniske ID ordninger og har til formål at autentificere en borger over for en onlinetjeneste.

Forslaget til forordning fastlægger betingelser, under hvilke medlemsstaterne skal anerkende og acceptere fysiske og juridiske personers elektroniske identifikationsmidler, der er omfattet af en elektronisk identifikationsordning, som er anmeldt af en anden medlemsstat.

Ad. 2) Elektroniske tillidstjenester
Elektroniske tillidstjenester til brug for elektroniske transaktioner adresserer det område, der er omfattet af den eksisterende regulering. Med forslaget til forordning suppleres den eksisterende regulering af elektroniske signaturer med en række yderligere tillidstjenester.

Forslaget opstiller således en retlig ramme for følgende tillidstjenester:

- Elektroniske signaturer
- Elektroniske segl
- Elektroniske tidsstempler
- Elektroniske dokumenter
- Elektroniske leveringstjenester
- Webstedsautentifikation

Til forskel for i dag indebærer forsalget, at alle tillidstjenester er omfattet, uanset om de har status som kvalificeret eller ej.

Det fremgår af forslaget til forordning, at den ikke finder anvendelse på levering af elektroniske tillidstjenester på grundlag af privatretlige frivillige aftaler.

Endelig omfatter forslaget til forordningen ikke aspekter i forbindelse med kontrakters indgåelse og gyldighed eller andre retlige forpligtelser, som ifølge national ret eller EU-ret er undergivet formkrav.

Forordningens anvendelsesområde er afgrænset til ikke at omfatte elektroniske tillidstjenester på grundlag af privatretlige frivillige aftaler. Det eksisterende direktiv undtager ligeledes udstedelse baseret på frivillige privatretlige aftaler, men kvalificerer dette som systemer med et begrænset antal deltagere. Det er

uklart om det er hensigten, at forordningens anvendelsesområde skal kvalificeres tilsvarende.

3.3 Elektronisk identifikation (kapitel II)
I forordningsforslagets kapitel II fastlægges reglerne for elektroniske identifikationsordninger.

Forslaget har til hensigt at sikre gensidig anerkendelse og accept af elektroniske identifikationsordninger, således at disse kan anvendes på tværs af medlemsstaterne.

Forslaget forpligter således medlemsstaterne til gensidigt at anerkende og acceptere elektroniske identifikationsmidler, der er anmeldt til Kommissionen.

Forordningen forpligter ikke medlemsstaterne til at indføre eller anmelde elektroniske identifikationsordninger, men de skal anerkende og acceptere anmeldte elektroniske identifikationsmidler fra andre medlemslande for de onlinetjenester, hvor elektronisk identifikation er nødvendig for at få adgang på nationalt plan.

Efter forslaget kan identifikationsordninger anmeldes til Kommissionen af medlemsstaterne og de herunder udstedte identifikationsmidler skal enten være udstedt af, udstedt på vegne af eller under ansvar af den medlemsstat, der anmelder.

Medlemsstaterne skal påtage sig ansvaret for, at anmeldte identifikationsmidler er korrekt udstedt (der er entydig tilknytning mellem juridisk eller fysisk person og identifikationsdata) og skal til enhver tid stille en gratis autentifikationsmulighed til rådighed online, så personidentifikationsdata kan valideres.

For at sikre at der etableres interoperabilitet mellem elektroniske identifikationsmidler og for at øge sikkerheden i disse identifikationsmidler fastlægges en samarbejdsforpligtelse mellem medlemsstaterne.

Det samlede regime knyttet til elektroniske identifikationsordninger er en væsentlig nyskabelse i forhold til den eksisterende regulering, herunder særligt det forhold at medlemsstaterne er ansvarlige for identifikationsordningen og de heri indeholdte identifikationsmidler.

Det ansvar, der er forbundet med medlemsstaternes identifikationsordning og konsekvenserne heraf skal afklares i forbindelse med de kommende forhandlinger.

3.4 Tillidstjenester (kapitel III)

3.4.1 Indledning

Forordningsforslagets kapitel III regulerer tillidstjenester. Kapitlet adresserer således det domæne, der kendes fra den eksisterende regulering (elektroniske signaturer), men tilføjer som noget nyt regulering af en række yderligere tillidstjenester, som skal bidrage til at understøtte den praktiske og juridiske ramme for elektroniske transaktioner.

Kapitlet er opdelt i otte afdelinger, der hver regulerer et specifikt område.
I afdeling 1 fastlægges en række generelle bestemmelser, i afdeling 2 beskrives den nationale tilsynsforpligtelse, i afdeling 3 fastlæggelses den juridiske ramme for elektroniske signaturer og i afdeling 4 til 8 etableres en juridisk ramme for de nye tillidstjenester, der introduceres med forslaget.

Forslaget fastholder terminologien fra den eksisterende regulering, hvor der skelnes mellem kvalificerede og ikke kvalificerede ydelser (i forslaget benævnt *tillidstjenester*).

For at opnå ret til at udbyde tillidstjenester med betegnelsen kvalificerede skal tjenesteyderen underlægge sig en række specifikke krav til sikkerhed og tilsyn.

3.4.2 Generelle bestemmelser (Kapitel III, Afdeling 1)

Forslaget fastlægger ansvaret for tillidstjenesteydere (tjenesteyder, der udsteder en elektronisk tjeneste omfattet af forordningen).

Som en nyskabelse medfører forslaget en udvidelse af hvilke tillidstjenesteydere, der er omfattet af det regulerede ansvar, således at dette ikke blot retter sig mod kvalificerede tillidstjenesteydere (der udbyder kvalificerede tillidstjenester) men også til tillidstjenesteydere generelt.

Der fastlægges et skærpet ansvarsgrundlag i form af et præsumptionsansvar, således at tjenesteyderen i forbindelse med en hændelse er pålagt bevisbyrden for, at der ikke er udvist forsømmelighed.

Enhver tillidstjenesteyder er ansvarlig for enhver form for direkte skade, der forårsages for en fysisk eller juridisk person som følge af manglende overholdelse af forordningsforslagets bestemmelser om god sikkerhedspraksis.

For kvalificerede tjenesteydere omfatter det skærpede ansvar alle forordningens bestemmelser, herunder de særlige krav til kvalificerede tillidstjenesteydere. I forhold til i dag er dette en væsentlig udvidelse af tjenesteydernes ansvar for udførelse af deres opgaver.

I forslaget fastslås, at kvalificerede tillidstjenester, hvor udbyderen er etableret i et tredjeland skal accepteres på linje med kvalificerede tillidstjenester, der leveres af en udbyder i Unionen. En forudsætning for accept er dog, at der foreligger en aftale om anerkendelse mellem EU og tredjelande eller internationale organisationer.

I forslaget foretages en henvisning til persondatadirektivet. På denne baggrund pålægges tillidstjenesteudbydere og tilsynsorganer at sikre en rimelig og lovlig behandling af personoplysninger.

Tillidstjenesteyderens ansvar understreges ved at de ifølge forordningsforslaget skal garantere fortroligheden og integriteten af oplysningerne vedrørende de personer, der leveres tillidstjenester til.

På baggrund af FN-konventionen om handicappedes rettigheder, der er trådt i kraft i EU, introducerer forordningsforslaget som noget nyt et krav om, at tillidstjenester og slutbrugerprodukter, der bruges til levering af disse tjenester, skal være tilgængelige for handicappede, hvor det er muligt.

3.4.3 Tilsyn (Kapitel III – afdeling 2)

Kapitel III, afdeling 2 indeholder regler om de sikkerhedsmæssige krav, som tillidstjenesteydere skal opfylde samt en nærmere beskrivelse af det tilsyn, der skal udføres af et tilsynsorgan for sikre, at kravene opfyldes. Endelig indeholder afdeling 2 en kort beskrivelse af krav til iværksættelse af kvalificerede tillidstjenester.

Sikkerhedskrav

Forslaget opstiller en række krav, som tillidstjenesteyderne skal opfylde, således at der under hensyn til den teknologiske udvikling til stadighed kan garanteres et tilfredsstillende sikkerhedsniveau. Tillidstjenesteudbyderne pålægges ligeledes en pligt til at informere tilsynsorganet om eventuelle brud på sikkerheden.

Kvalificerede tillidstjenesteydere er efter forslaget underlagt en række specifikke sikkerhedskrav, herunder særligt i forhold til kontrol af identiteten på de fysiske eller juridiske personer, der skal have udstedt et kvalificeret certifikat.

Som noget nyt stilles der eksplicit krav om, at identiteten skal være kontrolleret ved fysisk fremmøde i forbindelse med udstedelse af et kvalificeret certifikat. Udstedelse på baggrund af online ansøgning kan kun ske med anvendelse af et anmeldt identifikationsmiddel, som er udstedt på baggrund af fysisk fremmøde.

Kravet om fysisk fremmøde svarer grundlæggende til den eksisterende danske regulering, hvor det fysiske fremmøde dog kan udelades, hvis tillidstjenesteyderen på forhånd har kendskab til den person, som certifikatet udstedes til.

Det er en nyskabelse, at der ligeledes kan udstedes certifikater til juridiske personer. Det skal bemærkes, at juridiske personer skal gennemføre den samme identifikationsproces, som fysiske personer.

Forslagets krav til sikring af identitet på den person, som et certifikat udstedes til, suppleres af en række yderligere krav til den kvalificerede tillidstjenesteyder, herunder anvendelse af pålidelige systemer og processer.

Tilsyn
I overensstemmelse med den eksisterende regulering forpligtes medlemsstaterne til at nedsætte nationale tilsynsorganer, der kan foretage overvågning af tillidstjenesteudbydere og føre tilsyn med kvalificerede tillidstjenesteudbydere. Forslaget til forordning indfører både udvidede forpligtelser og udvidede beføjelser for de nationale tilsynsorganer.

Kvalificerede tillidstjenesteydere er underlagt et tilsyn, der bl.a. omfatter at et anerkendt uafhængigt kontrolorgan en gang om året foretager en kontrol af tillidstjenesteyderne og dennes kvalificerede tjenester. Dette kontrolorgan anvendes til at dokumentere, at den kvalificerede tillidstjenesteydere lever op til kravene i forordningen. Resultaterne af kontrollen skal forelægges for tilsynsorganet i en sikkerhedskontrolrapport.

Tilsynsorganet gives efter forslaget ret til at foretage kontrolbesøg hos kvalificerede tillidstjenesteydere både på eget initiativ og på anmodning fra Kommissionen, hvilket er en skærpelse i forhold til eksisterende lovgivning.

I hvilket omfang, Kommissionen kan forpligte et nationalt tilsyn til at foretage kontrolbesøg, er ikke tydeligt.

Forslaget giver tilsynsorganer ret til at udstede bindende instrukser til tillidstjenesteydere vedr. sikkerhedsmæssige forhold. Udstrækningen af bestemmelsen er uklar og bør søges klarlagt i det videre lovgivningsarbejde.

Som noget helt nyt indføres en eksplicit forpligtelse til gensidig bistand mellem tilsynsorganerne i medlemsstaterne med det formål at muliggøre grænseoverskridende tilsyn. Forslaget indfører regler om fælles foranstaltninger samt tilsynsorganernes ret til at deltage i sådanne foranstaltninger hos de andre medlemsstater.

Idet alene kvalificerede tillidstjenesteudbydere er underlagt en anmeldelsesforpligtelse, er det ikke beskrevet hvorledes tilsynsorganerne i praksis skal

overvåge (ikke kvalificerede) tillidstjenesteudbydere. Dette forhold skal afklares i forbindelse med de kommende forhandlinger.

Tilsynsorganerne bliver pålagt en række udvidede forpligtelser i forhold til afrapportering til Kommissionen, Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) og de øvrige medlemsstater.

Iværksættelse af en kvalificeret tillidstjeneste
Ifølge forslaget til forordning skal en tillidstjenesteyder, der ønsker at iværksætte en kvalificeret tillidstjeneste foretage anmeldelse til tilsynsorganet. Herefter kan tillidstjenesteyderen udbyde kvalificerede tillidstjenester. Den eksisterende regulering, hvorefter der ikke stilles krav om forudgående godkendelse af en kvalificeret tillidstjenesteyder bibeholdes således i forslaget til forordning.

Efter anmeldelse af en kvalificeret tillidstjeneste til et tilsynsorgan optages den ansøgende tjenesteyder på en positivliste, der opretholdes af medlemsstaten. Parallelt hermed foretager tilsynsorganet en nærmere kontrol af, om vedkommende udbyder, opfylder kravene i denne forordning. I perioden indtil godkendelse må et offentligt organ ikke afvise at bruge den anmeldte tillidstjeneste til at gennemføre en administrativ procedure eller formalitet.

Forslaget til forordning er uklar i forhold til de nærmere procedurer for afslag på godkendelse af kvalificerede tillidstjenester og skal afklares i forbindelse med de kommende forhandlinger.

Som en nyskabelse fastlægges det eksplicit, at kvalificerede tillidstjenesteydere gratis skal stille oplysninger om gyldigheden på udstedte certifikater til rådighed. En anden nyskabelse er forslag til eksplicitte krav til den hastighed, hvormed kvalificerede tillidstjenesteydere skal registrere og offentliggøre tilbagekaldelse af et certifikat.

3.4.4 Elektronisk signatur (Kapitel III – afdeling 3)
I forordningsforslagets kapitel III, afdeling 3 om elektronisk signatur fastlægges de juridiske rammer for anerkendelse af elektroniske signaturer samt specifikke tekniske krav til elektroniske signaturer og tilhørende certifikater.

Retsvirkninger og accept af elektroniske signaturer
For at sikre ensartede retsvirkninger i medlemsstaterne af fysiske personers anvendelse af elektroniskes signaturer indføres i forslaget en eksplicit forpligtelse om at tillægge kvalificerede elektroniske signaturer samme retsvirkning som håndskrevne signaturer.

Bestemmelsen svarer til den eksisterende regulering i Danmark men sikrer, at der på fællesskabsplan etableres en mere tydelig og eksplicit regulering af de juridiske retsvirkninger.

Forslaget forbyder medlemsstaterne at kræve en elektronisk signatur med et højere sikkerhedsniveau til anvendelse hos offentlige onlinetjenester end det, der er forbundet med en kvalificeret signatur.

Forordningsforslaget indeholder en udvidelse i forhold til den eksisterende regulering, idet den forpligter medlemsstater til at acceptere elektroniske signaturer på et lavere sikkerhedsniveau end det niveau, der er forbundet med en kvalificeret elektronisk signatur i det omfang sådanne signaturer anvendes i medlemsstaten som forudsætning for adgang til en offentlig onlinetjeneste.

Beskrivelsen er uklar, idet den forudsætter en sammenkobling af eID (autentifikation) og elektronisk signatur, der i øvrigt er tilsigtet adskilt i reguleringen.

Tekniske krav til kvalificerede elektroniske signaturer og tilhørende certifikater
I forslaget fastlægges specifikke krav til kvalificerede certifikater for elektroniske signaturer, herunder krav til indholdet af certifikatet. Desuden stilles der krav til at kvalificerede tillidstjenesteydere skal stille valideringstjenester til rådighed. Kravene svarer i hovedtræk til, hvad der følger af eksisterende lovgivning, dog således at der er foretaget enkelte justeringer med henblik på at gøre anvendelsen af elektroniske signaturer mere operationel. De eksisterende muligheder for at anføre anvendelsesbegrænsninger i certifikatet (f.eks. i form af en beløbsgrænse) er på denne baggrund fjernet.

Forslaget opstiller krav til de systemer, der anvendes til generering af kvalificerede elektroniske signaturer (kvalificerede systemer til generering af elektroniske signaturer) og fastlægger, at certificering heraf skal ske ved passende offentlige eller private organer.

Et certificeret system skal anerkendes af de øvrige medlemsstater. Medlemsstaterne skal informere Kommissionen om hvilke systemer, der er certificeret, hvorefter Kommissionen offentliggør en liste herom.

Forordningsforslaget opstiller en række krav til validering af kvalificerede elektroniske signaturer, herunder hvilke forhold, der skal være gældende for at en elektronisk signatur anses for gyldig.

Med forslaget introduceres en forpligtelse til at kvalificerede tillidstjenesteydere skal stille en tjeneste til rådighed til bevaring af kvalificerede elektroniske signaturer ud over den tekniske gyldighedsperiode, således at muligheden for validering af kvalificerede elektroniske signaturer forlænges. Det fremgår ikke

tydeligt af forslaget, hvilken præcis karakter tjenesten har, herunder om den skal være gratis at anvende.

3.4.5 Elektroniske segl (Kapitel III – afdeling 4)

I forslagets kapitel II, afdeling 4 introduceres en nyskabelse i form af elektroniske segl til juridiske personer.

Et elektronisk segl er en elektronisk pendant til et virksomheds segl eller stempel, der anvendes på et dokument eller andre elektroniske aktiver til at sikre oprindelse og integritet. Alene juridiske personer kan anvende elektroniske segl.

Elektroniske segl tillægges retsvirkninger, der er parallelle til elektroniske signaturer, herunder at elektroniske segl ikke må nægtes retlig gyldighed og anerkendelse som bevis under retssager alene af den grund, at det er i elektronisk form. Tilsvarende skal et kvalificeret elektronisk segl anerkendes og accepteres i alle medlemsstater.

Desuden bestemmes i overensstemmelse med reguleringen af elektroniske signaturer, at hvis en medlemsstat accepterer elektroniske segl med et sikkerhedsniveau, som ligger under det niveau, der er forbundet med et kvalificeret elektronisk segl, skal elektroniske segl, der har mindst samme sikkerhedsniveau, accepteres.

Krav til generering, validering og opbevaring af elektroniske segl svarer til, hvad der i øvrigt gælder for elektroniske signaturer.

3.4.6 Elektronisk tidsstempel (Kapitel III – afdeling 5)

I forslagets kapitel II, afdeling 5 reguleres som noget nyt elektroniske tidsstempler.

Et elektronisk tidsstempel sætter dato og tid på et sæt af elektroniske data (f.eks. i form af et elektronisk dokument) og har til formål at bevise, at data eksisterede på det pågældende tidspunkt, og at data ikke har ændret sig siden da.

Tidsstempler sikres retsvirkninger, der er parallelle til elektroniske signaturer og elektroniske segl, herunder at et elektronisk tidsstempel ikke må nægtes retlig gyldighed og anerkendelse som bevis under retssager alene af den grund, at det er i elektronisk form. Tilsvarende skal et kvalificeret elektronisk tidsstempel anerkendes og accepteres i alle medlemsstater.

3.4.7 Elektroniske dokumenter (Kapitel III – afdeling 6)

I forslagets kapitel III, afdeling 6 introduceres en nyskabelse i form af en specifik regulering af retsvirkningerne af elektroniske dokumenter (dokumenter i en hvilken som helst elektronisk form).

Ifølge forslaget skal elektroniske dokumenter betragtes som ligestillet med papirdokumenter og kan godtages som bevismateriale under retssager under hensyntagen til graden af sikkerhed for dokumentets ægthed og integritet.

Hvis et elektronisk dokument er underskrevet med en kvalificeret elektronisk signatur eller bærer et kvalificeret elektronisk segl gælder en specifik formodning om integritet og autenticitet.

Forslaget fastsætter, at hvis der som forudsætning for at yde en offentlig tjeneste skal forelægges et originaldokument eller en bekræftet genpart skal elektroniske dokumenter, der er udstedt af personer med kompetence hertil, og som anses for originaler eller bekræftede genparter i henhold til national ret i oprindelsesmedlemsstaten, accepteres i andre medlemsstater, uden at der stilles yderligere krav.

3.4.8 Kvalificeret elektronisk leveringstjeneste (Kapitel III – afdeling 7)

Kapitel III, afdeling 7 introducerer en nyskabelse i form af en kvalificeret elektronisk leveringstjeneste.

En elektronisk leveringstjeneste er en tjeneste, der gør det muligt at sende data ad elektronisk vej samtidig med, at behandlingen af de sendte data dokumenteres.

Forslaget sikrer, at data der sendes eller modtages via en elektronisk leveringstjeneste kan godtages som bevismateriale under retssager. Data der sendes eller modtages via en kvalificeret elektronisk leveringstjeneste opnår en særstatus, idet der herefter gælder en formodning om data's integritet og nøjagtigheden af den dato og det tidspunkt for afsendelse eller modtagelse af data, som den kvalificerede elektroniske leveringstjeneste angiver.

Der opstilles i forslaget en række tekniske krav til kvalificerede elektroniske leveringstjenester, der bl.a. sikrer bevis for afsendelse og modtagelse af data og giver beskyttelse mod tyveri, beskadigelse og uautoriseret ændring.

3.4.9 Webstedsautentifikation (Kapitel III – afdeling 8)

Kapitel III, afdeling 9 introducerer en nyskabelse i form af et kvalificeret certifikat til webstedsautentifikation.

Et kvalificeret certifikat for webstedsautentifikation er en attestering, som gør det muligt at autentificere et websted og knytter webstedet til den person, som certifikatet er udstedt til

Forslaget fastsætter en række tekniske krav til det kvalificerede certifikat, der i vidt omfang er parallelle til de øvrige certifikater og fastslår, at certifikatet skal anerkendes og accepteres i alle medlemsstater.

3.5 Delegerede retsakter (kapitel IV)
Med henblik på at sikre, at forslaget til forordning kan suppleres fleksibelt og hurtigt delegerer forslaget i udstrakt grad beføjelser til Kommissionen til at vedtage retsakter om visse detaljerede tekniske aspekter, der er nødvendige at regulere mere detaljeret for at opnå formålet med forordningen.

Det understreges i præamblen, at Kommissionen i denne forbindelse bør gennemføre relevante høringer under sit forberedende arbejde, herunder på ekspertniveau.

3.6 Gennemførelsesretsakter (forordningens kapitel V)
Med henblik på at sikre ensartede betingelser for gennemførelsen af forslaget til forordning tillægges Kommissionen ifølge forslaget gennemførelsesbeføjelser, navnlig beføjelse til at opstille referencenumre på standarder, hvis brug giver formodning om overensstemmelse med bestemte krav, der er fastlagt i denne forordning eller i delegerede retsakter. Disse beføjelser udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser.

3.7 Afsluttende bestemmelser (kapitel VI)
Der fastlægges bestemmelser vedr. Kommissionens afrapportering til Europa-Parlamentet og Rådet om anvendelsen af forordningen.

Ved sin ikrafttræden ophæver forordningen det eksisterende direktiv 1999/93/EF og fastlægger, at henvisninger til det ophævede direktiv betragtes som henvisninger til nærværende forordning.

Desuden fastlægger forslaget overgangsregler for kvalificerede certifikater udstedt i overensstemmelse med gældende regler, hvorefter de vil være gyldige indtil ordinært udløb, dog højst i fem år regnet fra forordningens ikrafttræden. Der fastlægges ligeledes overgangsregler for sikre signaturgenereringssystemer.

Forordningen skal træde i kraft på tyvendedagen efter offentliggørelsen i Den Europæiske Unions Tidende og er herefter bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

4. Europa-Parlamentets udtalelser

Europa-Parlamentet har endnu ikke udtalt sig.

5. Nærhedsprincippet

Kommissionen har vurderet, at forslaget er i overensstemmelse med nærhedsprincippet.

Det er Kommissionens opfattelse, at forordningsforslagets bestemmelser er nødvendige af hensyn til at sikre en effektiv anvendelse af identifikationsmidler og elektroniske tillidstjenester på EU-plan. Det er Kommissionens vurdering, at man i øjeblikket ikke når disse mål ved hjælp af frivillig koordinering mellem medlemsstaterne, og det er heller ikke sandsynligt, at dette vil ske i fremtiden.

Regeringen er umiddelbart enig med Kommissionen i, at elektronisk identifikation, autentifikation og e-signatur tjenesters grænseoverskridende karakter kræver handling på EU-niveau. Det er på den baggrund regeringens foreløbige holdning, at forslaget er i overensstemmelse med nærhedsprincippet.

6. Gældende dansk ret

Lov om elektroniske signaturer (Lov nr. 417 af 31. maj 2000).

Bekendtgørelser udstedt i medfør af loven:

- Bekendtgørelse nr. 922 af 5. oktober 2000 om nøglecentres og systemrevisionens indberetning af oplysninger til Telestyrelsen
- Bekendtgørelse nr. 923 af 5. oktober 2000 om sikkerhedskrav m.v. til nøglecentre.

7. Lovgivningsmæssige og statsfinansielle konsekvenser

Lovgivningsmæssige konsekvenser

Det følger af EUF-traktatens artikel 288, at en forordning er almengyldig, samt at den binder i alle enkeltheder og gælder umiddelbart i hver medlemsstat. Hertil kommer, at forordningsforslaget efter sit indhold bl.a. har til formål at erstatte det eksisterende direktiv om elektroniske signaturer (direktiv 1999/EF). En konsekvens af forslaget vil derfor være, at regulering som følger af lov nr. 417 af 31. maj 2000 om elektroniske signaturer samt tilhørende be-

kendtgørelser vil skulle ophæves. Idet lov om elektroniske signaturer alene implementerer EU-direktivet og ikke har en selvstændig regulering herudover vurderes det på nuværende tidspunkt relevant at foretage ændringer heri.

I en række danske love er der krav om anvendelse af digital signatur. Den gældende anbefaling fra Digitaliseringsstyrelsen (og tidligere IT- og Telestyrelsen) er, at sådanne krav indføres i lovgivningen med følgende ordlyd: "..digital signatur med et sikkerhedsniveau svarende til OCES-standarden eller højere".

Det skal analyseres nærmere, om krav om anvendelse af digital signatur i lyset af forordningsforslagets bestemmelser om gensidig anerkendelse og accept af elektroniske identifikationsmekanismer og elektroniske tillidstjenester vil kunne opretholdes, men i det omfang den angivne terminologi er anvendt i lovgivningen vil der formentlig ikke være behov for ændringer.

Forslagets bestemmelser vedr. retsvirkninger af elektroniske signaturer og fuld anerkendelse af elektroniske dokumenter vurderes at være i overensstemmelse med gældende dansk ret, herunder som følge af lov om elektroniske signaturer. Det skal dog analyseres nærmere, om der er behov for yderligere regulering som følge af forordningen.

Det skal endvidere analyseres nærmere, om forordningens bestemmelser om fuld anerkendelse af elektroniske dokumenter og underskrifter har betydning for gældende dansk ret.

Statsfinansielle konsekvenser

Forslagets statsfinansielle konsekvenser skal analyseres nærmere, men umiddelbart vurderes det, at forslaget vil kunne have statsfinansielle konsekvenser.

Forslaget medfører et behov for at gennemføre ændringer i den tekniske infrastruktur, der understøtter anvendelse af OCES digital signatur (udmøntet i NemID løsningen). Ændringerne skal bl.a. gennemføres med henblik på at kunne sikre, at der gives adgang til danske offentlige tjenester ved anvendelse af udenlandske identifikationsmekanismer og elektroniske signaturer.

Kravet om gratis valideringsmulighed for såvel elektroniske identifikationsordninger som kvalificerede elektroniske signaturer udfordrer dels den nuværende finansieringsmodel for NemID, der baserer sig på, at validering i professionelle forhold udløser betaling af vederlag til Nets DanID, dels kan det være forbundet med omkostninger at tilvejebringe den tekniske understøttelse af gratis validering.

Endeligt kan de skærpede krav til tilsynsmyndigheden, der ligger hos Digitaliseringsstyrelsen under Finansministeriet, have statsfinansielle konsekvenser.

8. Samfundsøkonomiske konsekvenser

Kommissionen vurderer, at forslaget vil give øget vækst på baggrund af mulighederne for administrative lettelser, øget mulighed for samhandel og højere grad af konkurrence. Regeringen er i vidt omfang enig i heri, idet forslaget forventes at kunne skabe større interoperabilitet i det indre marked til gavn for borgere, virksomheder og myndigheder, hvilket i høj grad vil understøtte et digitalt indre marked.

9. Administrative konsekvenser for erhvervslivet

Kommissionens forslag vurderes at medføre administrative lettelser for erhvervslivet.

En øget anvendelse af elektroniske identifikationsmidler og elektroniske signaturer vil muliggøre reduktion i de administrative byrder ved kommunikation med offentlige myndigheder, herunder offentlige myndigheder i udlandet.

10. Høring

Forslaget har været sendt i høring i EU-Specialudvalg for Konkurrenceevne, Vækst og Forbrugerspørgsmål med frist den 1. august 2012.

Der er modtaget høringssvar fra

- Lønmodtagernes Dyrtidsfond
- Foreningen af Statsautoriserede Revisorer
- IT-Branchen
- Nationalbanken
- Finansrådet
- Signaturgruppen
- ATP
- Dansk Aktionærforening

Lønmodtagernes Dyrtidsfond er positive over for en europæisk løsning, der vil lette elektronisk kommunikationen med en lang række af fondens medlemmer, der er bosat i udlandet, forudsat at den elektroniske løsning har samme retsvirkninger som en håndskrevet underskrift.

Lønmodtagernes Dyrtidsfond påpeger behovet for, at der skal findes en national løsning, der letter den tekniske modtagelse af elektroniske ID fra andre medlemsstater.

Foreningen af Statsautoriserede Revisorer mener, at kravene til uafhængighed for det organ, der årligt skal føre kontrol med de tjenesteydere, der udsteder kvalificerede tillidstjenester, bør svare til tilsvarende krav ved revision af årsregnskaber for børsnoterede virksomheder, og at der bør stilles kompetencemæssige krav om revisionsfaglig og teknisk indsigt i løsningerne. Det uafhængige organ bør endvidere være omfattet af passende forsikringsordninger, der dækker den udførte kontrol, hvilket kan opfyldes, hvis kontrollen udføres af en godkendt revisor.

Desuden anbefaler Foreningen af Statsautoriserede Revisorer indførelse af krav til, at sikkerhedskontrol rapporterne omfatter såvel generelle it-kontroller som kontroller i systemer, der anvendes til generering af nøgler, nøglekomponenter samt registrering, udstedelse, verifikation, opbevaring og spærring af certifikater eller til udveksling af data med andre parter.

IT-Branchen udtrykker støtte til forslagets formål, men finder, at der bør være større fokus på at fremme tillidsbaseret samhandel mellem virksomheder og private. IT-Branchen ønsker, at forslaget udvides med regler om private virksomheders gensidige anerkendelse af medarbejdercertifikater samt til sikring af elektroniske dokumenter over tid.

IT-Branchen understreger, at der er et stort potentiale for tillidsbaseret samhandel i det private erhvervsliv på tværs af grænser, hvilket bør understøttes af forordningen ved specifikke reguleringer, der sikrer en ensartet anvendelse i medlemslandende samt understøtter en positiv business case for det private erhvervsliv.

Nationalbanken er positiv over for forslaget og vurderer, at det kan øge anvendelsen af elektronisk identifikation på tværs af landegrænser.

Finansrådet udtrykker principiel støtte til forslaget. Finansrådet konstaterer, at forslaget ikke regulerer NemID til netbankerne og således ikke direkte vil regulere banksektoren. Idet Danmark i vidt omfang opererer med én fælles identifikations-/sikkerhedsløsning, vil forslaget dog få en afledt effekt for bankerne.

Det anføres af Finansrådet, at det må forventes, at en kommende forordning vil medføre betydelige investeringer, hvis Danmark skal understøtte udenlandske eID samt omkostninger til en evt. ændring af de eksisterende danske signaturer baseret på den nationale OCES-standard til kvalificerede certifikater efter europæisk standard, idet dette vil kræve et fysisk fremmøde for indehaverne af certifikater.

Finansrådet ønsker en afklaring af grænsen mellem forslaget til forordning og de eksisterende regler om hvidvask (krav til identifikation af en bruger/kunde).

Endeligt anfører Finansrådet, at det er positivt, at konkrete sikkerhedsstandarder og formater ikke er fastlagt i forordningen, idet dette bl.a. vil kunne hindre innovation. Det samlede sikkerhedsniveau for elektroniske løsninger er en væsentligt faktor for anvendelse af nye teknologier og for overblikket over de samlede økonomiske omkostninger, hvorfor sikkerhedsniveauet for konkrete løsninger bør behandles inden vedtagelsen af forordningen.

Signaturgruppen anfører, at forslaget i den eksisterende form udgør et godt udgangspunkt for det videre arbejde, idet standardisering og koordinering på området er stærkt nødvendigt. Det er i denne forbindelse Signaturgruppens vurdering, at forordningen særligt fokuserer på identitetsløsninger, der er ejet eller finansieret af det offentlige og derfor ikke understøtter en dynamisk markedsudvikling.

Det anføres af Signaturgruppen, at kravene til udbydere af kvalificerede tillidstjenester synes unødigt byrdefulde, idet forslaget forudsætter et meget bredt sortiment af ydelser fra alle kvalificerede tillidstjenester, hvilket potentielt vil hindre en naturlig specialisering mellem markedsdeltagere. Signaturgruppen anfører ligeledes, at kravene til tilsyn kan betyde øgede omkostninger til kvalificerede tjenesteydere, og at det i den forbindelse er vigtigt at sikre, at disse tjenesteydere skal stilles ens uanset hvilket medlemsland, de opererer fra.

Endelig har Signaturgruppen afgivet en række specifikke tekniske bemærkninger til forordningens enkeltbestemmelser.

ATP og Dansk Aktionærforening har meddelt, at de ikke har bemærkninger til forslaget.

11. Forhandlingssituationen

Der er ikke på nuværende tidspunkt kendskab til medlemslandenes holdninger til forslaget.

12. Regeringens generelle holdning

Regeringen er overordnet set positiv over for Kommissionens forslag.

Regeringen støtter Kommissionens intention om at fremme anvendeligheden af elektroniske identifikationsordninger og elektroniske signaturer på tværs af EU's medlemsstater og finder det hensigtsmæssigt at udvide lovgivningens virkefelt som foreslået.

Regeringens nærmere holdning til forslaget vil blive fastlagt på baggrund af en nærmere analyse af forslagets konsekvenser, herunder statsfinansielle konsekvenser. Regeringen vil arbejde for, at forslagets økonomiske konsekvenser minimeres.

13. Tidligere forelæggelse for Folketingets Europaudvalg

Sagen har ikke tidligere været forelagt for Folketingets Europaudvalg.