



EUROPEISKA KOMMISSIONEN

Bryssel den 4.6.2012
COM(2012) 238 final

2012/0146 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

(Text av betydelse för EES)

{SWD(2012) 135 final}

{SWD(2012) 136 final}

SAMMANFATTNING

1. BAKGRUND TILL FÖRSLAGET

I denna sammanfattning beskrivs ett förslag till regelverk som är utformat för att öka förtroendet för elektroniska transaktioner på den inre marknaden.

Att bygga upp förtroendet för nätmiljön är avgörande för den ekonomiska utvecklingen. Bristande förtroende gör att konsumenter, företag och myndigheter tvekar att utföra transaktioner på elektronisk väg och att använda nya tjänster.

I *En digital agenda för Europa*¹ identifieras befintliga hinder för Europas digitala utveckling. Dessutom föreslås lagstiftning om e-signaturer (nyckelåtgärd 3) och om ömsesidigt erkännande av e-identifiering och e-autentisering (nyckelåtgärd 16), där ett tydligt regelverk fastställs för att undanröja fragmentering och brist på interoperabilitet, främja det digitala medborgarskapet och förebygga it-brottslighet. Lagstiftning som säkerställer ömsesidigt erkännande av e-identifiering och e-autentisering inom hela EU samt en översyn av direktivet om elektroniska signaturer är även i *Inremarknadsakten*² en nyckelåtgärd för att den digitala inre marknaden ska kunna förverkligas. I *En färdplan för stabilitet och tillväxt*³ betonas den centrala betydelse som en framtida gemensam rättslig ram för gränsöverskridande ömsesidigt erkännande och godtagande av e-identifiering och e-autentisering har för utvecklingen av den digitala ekonomin.

Regelverket som föreslås består av *Europaparlamentets och rådets förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden*. Det syftar till att möjliggöra ett säkert och sömlöst elektroniskt samspel mellan företag, medborgare och offentliga myndigheter, för att därigenom öka effektiviteten hos offentliga och privata nättjänster, e-affärer och e-handel i EU.

Den nuvarande EU-lagstiftningen, dvs. direktiv 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer⁴, gäller i huvudsak endast elektroniska signaturer. Det finns inget heltäckande, gräns- och sektorsöverskridande regelverk i EU för säkra, pålitliga och lättanvända elektroniska transaktioner som omfattar elektronisk identifiering, elektronisk autentisering och elektroniska signaturer.

Syftet är att förbättra den befintliga lagstiftningen och utvidga den till att omfatta ömsesidigt erkännande och godtagande på EU-nivå av anmälda system för elektronisk identifiering och andra viktiga närliggande betrodda e-tjänster.

2. RESULTAT AV SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

Detta initiativ är resultatet av omfattande samråd om en översyn av den nuvarande rättsliga ramen för elektroniska signaturer, där kommissionen fått återkoppling från medlemsstaterna, Europaparlamentet och andra berörda parter⁵. Ett offentligt samråd på internet kompletterades av en testpanel för små och medelstora företag för att identifiera deras särskilda synpunkter

¹ KOM(2010) 245, 19.5.2010.

² KOM(2011) 206 slutlig, 13.4.2011.

³ KOM(2011) 669, 12.10.2011.

⁴ EGT L 13, 19.1.2000, s. 12.

⁵ Ytterligare information om samråden finns på webbplatsen http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision

och behov samt andra riktade samråd med berörda parter^{6,7}. Kommissionen genomförde även ett antal undersökningar med avseende på e-identifiering, e-autentisering, e-signaturer och närliggande betrodda tjänster.

Av samråden framgick att en stor majoritet av de berörda parterna var överens om att det behövs en översyn av det nuvarande regelverket för att överbrygga bristerna i direktivet om e-signaturer. Man ansåg att regelverket på ett bättre sätt måste möta de utmaningar som följer av den nya teknikens snabba utveckling (särskilt i fråga om tillgången till internet och mobila tjänster) och den ökande globaliseringen, samtidigt som den rättsliga ramens tekniska neutralitet vidmakthålls.

I enlighet med sin politik för bättre lagstiftning genomförde kommissionen en konsekvensbedömning av de politiska alternativen. Tre politiska alternativ bedömdes, vilka behandlade 1) tillämpningsområdet för det nya regelverket, 2) det rättsliga instrumentet och 3) den tillsynsnivå som krävs⁸. Det alternativ som föredrogs visade sig omfatta ökad rättssäkerhet, bättre samordning av nationell tillsyn, säkerställande av ömsesidigt erkännande och godtagande av system för e-identifiering samt integrering av viktiga närliggande betrodda tjänster. Konsekvensbedömningen ledde till slutsatsen att detta skulle leda till en avsevärd förbättring av rättssäkerheten, säkerheten och förtroendet i fråga om gränsöverskridande elektroniska transaktioner, vilket i sin tur innebär en minskning av marknadens fragmentering.

3. FÖRSLAGETS RÄTTSLIGA ASPEKTER

3.1 Rättslig grund

Detta förslag grundar sig på artikel 114 i EUF-fördraget, som gäller antagandet av bestämmelser för att undanröja befintliga hinder för den inre marknadens funktion. Medborgare, företag och myndigheter kommer att kunna dra nytta av ett ömsesidigt erkännande och godtagande av e-identifiering, e-autentisering, e-signaturer och andra gränsöverskridande betrodda tjänster när sådana behövs för att få åtkomst till och genomföra elektroniska förfaranden eller transaktioner.

En förordning anses vara det lämpligaste rättsliga instrumentet. Eftersom en förordning enligt artikel 288 i EUF-fördraget är direkt tillämplig kommer den att minska den rättsliga fragmenteringen och ge större rättssäkerhet genom att införa en harmoniserad uppsättning kärnbestämmelser och bidra till den inre marknadens funktion.

3.2 Subsidiaritet och proportionalitet

För att EU-åtgärder ska vara berättigade måste subsidiaritetsprincipen följas.

⁶ Den 10 mars 2011 anordnades en workshop för berörda parter med företrädare från offentlig och privat sektor samt den akademiska världen i syftet att diskutera vilka lagstiftningsåtgärder som behövs för att hantera de framtida utmaningarna. Workshopen fungerade som ett interaktivt forum för att utbyta idéer och peka på de olika synpunkter som framkommit om de frågor som tagits upp i det offentliga samrådet. Flera organisationer inkom spontant med ståndpunkter.

⁷ Det polska EU-ordförandeskapet anordnade ett möte med medlemsstaterna om elektroniska signaturer i Warszawa den 9 november 2011 och om elektronisk identifiering i Poznan den 17 november 2011. Den 25 januari 2012 samlade kommissionen medlemsstaterna i en workshop för att diskutera återstående frågor rörande e-identifiering, e-autentisering och e-signaturer.

⁸ Inom ramen för den första omgången undersöktes fyra alternativ, dvs. upphävande av direktivet om e-signaturer, ingen ändring av politiken, ökad rättssäkerhet, bättre samordning av nationell övervakning samt säkerställande av ömsesidigt erkännande och godtagande av e-identifiering i hela EU, samt slutligen en utvidgning för att integrera vissa närliggande betrodda tjänster. I den andra omgången bedömdes fördelarna med reglering genom ett respektive två instrument, och genom ett direktiv respektive en förordning. I den tredje omgången undersöktes möjligheterna med ett genomförande av nationella tillsynssystem baserade på gemensamma väsentliga tillsynskrav jämfört med ett EU-baserat tillsynssystem. Med hjälp av en grupp som samlade alla berörda generaldirektorat vid kommissionen bedömdes varje enskilt alternativ med hänsyn till hur effektivt det var i fråga om att uppnå de politiska målen, dess ekonomiska konsekvenser för berörda parter (inbegripet konsekvenserna för EU-institutionernas budget), dess sociala och miljömässiga konsekvenser samt dess inverkan på administrativa bördor.

a) Problemets gränsöverskridande natur (nödvändighetstestet)

E-identifiering, e-autentisering, e-signaturer och närliggande betrodda tjänster är av en gränsöverskridande natur, vilket gör EU-åtgärder nödvändiga. Enbart inhemska (dvs. nationella) åtgärder skulle inte vara tillräckligt för att uppfylla de syften och uppnå de mål som fastställs i *Europa 2020-strategin*⁹. Tidigare erfarenheter har tvärtom visat att nationella åtgärder faktiskt har skapat hinder för EU-täckande interoperabilitet för elektroniska signaturer och att de för närvarande har samma inverkan på e-identifiering, e-autentisering och närliggande betrodda tjänster. Därför är det nödvändigt att EU skapar en ram som främjar gränsöverskridande interoperabilitet och förbättrar samordningen av de nationella tillsynssystemen. Elektronisk identifiering är dock inte en fråga som kan behandlas på samma allmänna sätt som de andra betrodda elektroniska tjänsterna i den föreslagna förordningen, eftersom utfärdande av identifieringsmetoder är ett nationellt privilegium. Förslaget är därför strikt fokuserat på gränsöverskridande aspekter av elektronisk identifiering.

Den föreslagna förordningen skapar jämlika förhållanden för företag som erbjuder betrodda tjänster och som med dagens mångfaldiga lagstiftning ofta står inför rättslig osäkerhet och extra administrativa bördor. Den rättsliga säkerheten ökar kraftigt genom att medlemsstaterna tydligt åläggs att godkänna kvalificerade betrodda tjänster, vilket ytterligare kommer att uppmuntra företagen att erbjuda sina tjänster över gränserna. Företagen kommer exempelvis att kunna delta elektroniskt i anbudsförfaranden som publiceras av förvaltningen i en annan medlemsstat, utan att företagets e-signatur blockeras till följd av specifika nationella krav eller interoperabilitetsproblem. Likaså kommer företag att kunna teckna kontrakt elektroniskt med parter i andra EU-länder utan att behöva frukta olika rättsliga bestämmelser om betrodda tjänster som e-elektroniska sigill, elektroniska dokument eller tidsmärkning. Meddelanden om utebliven betalning kan sändas från en medlemsstat till en annan utan att man behöver vara osäker på om de är rättsligt giltiga i båda länder. Och slutligen kommer näthandeln att vara säkrare om köparna kan kontrollera att de verkligen befinner sig på säljarens webbplats och inte på någon falsk sida.

Ömsesidigt erkännande av e-identifiering och allmänt godkännande av e-signaturer förenklar tillhandahållandet av många olika typer av tjänster över gränserna på den inre marknaden och ger företagen möjlighet att verka över gränserna utan att stöta på hinder i sina kontakter med myndigheter. I praktiken innebär detta betydande effektivitetsvinster både för företagen och allmänheten i samband med administrativa formaliteter. Exempelvis blir det möjligt för studenter att elektroniskt anmäla sig på ett utländskt universitet, för enskilda att lämna in skattedeklarationer i andra medlemsstater online, eller för patienter att komma åt de egna hälsouppgifterna via nätet. Utan ömsesidigt erkända elektroniska identifieringsmöjligheter kan läkare inte komma åt patienternas uppgifter, som kanske behövs för en behandling, eller de laboratorieresultat som redan föreligger kan behöva upprepas.

b) Utökat värde (effektivitetstestet)

De syften som beskrivs ovan uppnås för närvarande inte genom frivillig samordning mellan medlemsstaterna och det är heller inte sannolikt att detta kommer att inträffa i framtiden. Det leder till dubbelarbete, fastställandet av olika standarder och gränsöverskridande egenskaper hos de spridningseffekter som informations- och kommunikationstekniken ger upphov till, och det är förenat med administrativa svårigheter att upprätta en sådan samordning genom bilaterala eller multilaterala avtal.

⁹

Meddelande från kommissionen: *Europa 2020. En strategi för smart och hållbar tillväxt för alla*, KOM(2010) 2020, 3.3.2010.

För att kunna lösa problem som t.ex. a) en avsaknad av rättssäkerhet på grund av olikartade nationella bestämmelser som har sin grund i skiljaktiga tolkningar av direktivet om elektroniska signaturer och b) en bristfällig interoperabilitet för de system för elektroniska signaturer som inrättats på nationell nivå på grund av den inkonsekventa tillämpningen av tekniska standarder, krävs dessutom en typ av samordning mellan EU:s medlemsstater som kan genomföras effektivare på EU-nivå.

3.3 Närmare redogörelse för förslaget

3.3.1 KAPITEL I – ALLMÄNNA BESTÄMMELSER

I artikel 1 definieras förordningens syfte.

I artikel 2 definieras förordningens materiella tillämpningsområde.

Artikel 3 innehåller definitioner av de begrepp som används i förordningen. Vissa definitioner har övertagits från direktiv 1999/93/EG, medan andra har förtydligats, kompletterats med ytterligare element eller är helt nya.

Genom artikel 4 fastställs principerna om den inre marknaden med avseende på förordningens territoriella tillämpningsområde. Att inga begränsningar av friheten att tillhandahålla tjänster och den fria rörligheten för varor får införas nämns uttryckligen.

3.3.2 KAPITEL II – ELEKTRONISK IDENTIFIERING

Genom artikel 5 föreskrivs ömsesidigt erkännande och godtagande av medel för elektronisk identifiering som omfattas av ett system som ska anmälas till kommissionen enligt de villkor som anges i förordningen. De flesta av EU:s medlemsstater har infört någon form av system för e-identifiering. De skiljer sig dock i många avseenden från varandra. Det finns ingen gemensam rättslig grund enligt vilken alla medlemsstater är skyldiga att erkänna och godta medel för elektronisk identifiering som andra medlemsstater utfärdar för åtkomst till nättjänster. Den gränsöverskridande interoperabiliteten för nationella e-identifieringar är dessutom otillräcklig. Detta skapar hinder som gör att medborgare och företag inte fullt ut kan utnyttja fördelarna med den digitala inre marknaden. Genom det ömsesidiga erkännandet och godtagandet av alla medel för elektronisk identifiering som omfattas av ett anmält system enligt denna förordning undanröjs dessa rättsliga hinder.

Förordningen medför ingen skyldighet för medlemsstaterna att införa eller anmäla system för e-identifiering, utan en skyldighet att erkänna och godta anmälda e-identifieringar för de nättjänster där e-identifiering krävs för att få åtkomst på nationell nivå. De potentiella stordriftsfördelarna om elektronisk identifiering och autentisering används över gränserna kan uppmuntra medlemsstaterna att anmäla sina system för elektronisk identifiering. I artikel 6 fastställs följande fem villkor som ska uppfyllas vid anmälan av system för e-identifiering:

Medlemsstaterna kan anmäla de system för elektronisk identifiering som de godtar under sin jurisdiktion i de fall där sådan identifiering krävs för offentliga tjänster. Ett ytterligare krav är att respektive medel för elektronisk identifiering måste utfärdas av den medlemsstat som anmäler ett system, alternativt för dess räkning eller åtminstone på dess ansvar.

Medlemsstaterna måste se till att det finns ett otvetydigt samband mellan uppgifterna i e-identifieringen och den berörda personen. Den här förpliktelsen innebär inte att en person inte

kan ha flera olika typer av e-identifieringsmedel, men de måste alla vara kopplade till samma person.

En e-identifierings tillförlitlighet är beroende av tillgången till autentiseringsmedel (dvs. möjligheten att kontrollera giltigheten hos de elektroniska identifieringsuppgifterna). Genom förordningen förpliktigas de medlemsstater som anmäler ett system för e-identifiering att tillhandahålla autentiseringstjänster på internet som är kostnadsfria för tredje parter. Denna autentiseringsmöjlighet måste vara tillgänglig utan avbrott. Parter som är beroende av sådan autentisering får inte åläggas några särskilda tekniska krav rörande t.ex. maskinvara, eller programvara. Bestämmelsen gäller inte eventuella krav på e-identifieringsmedlens användare (innehavare) när det gäller sådant som är tekniskt nödvändigt för att använda medel för elektronisk identifiering, som t.ex. kortläsare.

Medlemsstaterna måste ta på sig skadeståndsansvaret för sambandets otvetydighet (dvs. att de identifieringsuppgifter som tilldelas personen inte är kopplade till någon annan person) och autentiseringsmöjligheten (dvs. möjligheten att kontrollera att uppgifterna i e-identifieringen är giltiga). Medlemsstaternas skadeståndsansvar gäller inte andra aspekter av identifieringsförfarandet eller andra transaktioner som kräver identifiering.

Artikel 7 innehåller regler om anmälan till kommissionen av system för elektronisk identifiering.

Artikel 8 syftar till att säkerställa den tekniska interoperabiliteten för anmälda system för elektronisk identifiering genom en samordningsstrategi, inklusive delegerade akter.

3.3.3 KAPITEL III – BETRODDA TJÄNSTER

3.3.3.1 Avsnitt 1 – Allmänna bestämmelser

I artikel 9 fastställs principerna avseende både icke kvalificerade tillhandahållare av betrodda tjänster och kvalificerade tillhandahållare av betrodda tjänster. Artikeln bygger på artikel 6 i direktiv 1999/93/EG och utvidgar rätten till ersättning till skador som orsakas av en försumlig tillhandahållare av betrodda tjänster genom underlåtenhet att uppfylla god säkerhetspraxis som leder till en överträdelse av säkerheten som har betydande effekter på tjänsten.

I artikel 10 beskrivs mekanismen för erkännande och godtagande av kvalificerade betrodda tjänster som tillhandahålls av tillhandahållare som är etablerade i ett tredjeland. Den bygger på artikel 7 i direktiv 1999/93/EG men det är bara det enda praktiskt genomförbara alternativet som behålls, vilket är att tillåta sådana erkännanden som omfattas ett internationellt avtal mellan Europeiska unionen och tredjeländer eller internationella organisationer.

I artikel 11 fastställs principerna för dataskydd och dataminimering. Den bygger på artikel 8 i direktiv 1999/93/EG.

Genom artikel 12 görs betrodda tjänster tillgängliga för personer med funktionsnedsättning.

3.3.3.2 Avsnitt 2 – Tillsyn

Genom artikel 13 förpliktigas medlemsstaterna att inrätta tillsynsorgan, baserade på artikel 3.3 i direktiv 1999/93/EG. Dessutom förtydligas och utvidgas deras ansvarsområde med avseende

på både tillhandahållare av betrodda tjänster och kvalificerade tillhandahållare av betrodda tjänster.

Genom artikel 14 införs en konkret mekanism för ömsesidigt bistånd mellan medlemsstaternas tillsynsorgan som ska underlätta den gränsöverskridande tillsynen av tillhandahållare av betrodda tjänster. Genom artikeln införs regler om gemensamma åtgärder och tillsynsmyndigheternas rätt att delta i sådana åtgärder.

Genom artikel 15 införs en förpliktelse för både kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster att vidta lämpliga tekniska och organisatoriska åtgärder för att se till att deras verksamhet är säker. Dessutom måste behöriga tillsynsorgan och andra relevanta myndigheter informeras om eventuella säkerhetsöverträdelser. I tillämpliga fall ska dessa tillsynsorgan i sin tur informera övriga medlemsstaters tillsynsorgan samt direkt eller via den berörda tillhandahållaren av betrodda tjänster även informera allmänheten.

I artikel 16 fastställs villkoren för tillsynen av kvalificerade tillhandahållare av betrodda tjänster och kvalificerade betrodda tjänster som tillhandahålls av dessa. Dessa tillhandahållare ska årligen granskas av ett erkänt oberoende organ för att bekräfta för tillsynsorganet att de uppfyller de förpliktelser som anges i förordningen. Genom artikel 16.2 tilldelas tillsynsorganet dessutom rätten att när som helst utföra kontroller på plats av de kvalificerade tillhandahållarna av betrodda tjänster. Tillsynsorganet har även befogenheter att utfärda bindande instruktioner till tillhandahållare av betrodda tjänster om att på ett proportionerligt sätt åtgärda en eventuell underlåtenhet att uppfylla förpliktelser som upptäckts genom en säkerhetsgranskning.

Artikel 17 gäller den åtgärd som tillsynsorganet utför på begäran av en tillhandahållare av betrodda tjänster som vill inleda verksamhet som omfattar kvalificerade betrodda tjänster.

I artikel 18 föreskrivs att förteckningar över betrodda tjänsteleverantörer¹⁰ ska upprättas, med information om de kvalificerade tillhandahållare av betrodda tjänster som omfattas av tillsyn och om de kvalificerade tjänster som dessa erbjuder. Informationen måste göras allmänt tillgänglig med hjälp av en gemensam mall för att underlätta dess automatiserade användning och se till att en lämplig detaljnivå upprätthålls.

I artikel 19 fastställs de krav som kvalificerade tillhandahållare av betrodda tjänster måste uppfylla för att erkännas som en sådan tillhandahållare. Den bygger på bilaga II till direktiv 1999/93/EG.

3.3.3.3 Avsnitt 3 – Elektroniska signaturer

Artikel 20 innehåller regler om den rättsliga verkan av fysiska personers elektroniska signaturer. Artikel 5 i direktiv 1999/93/EG förtydligas och utvidgas genom en uttrycklig förpliktelse att ge kvalificerade e-signaturer samma rättsliga verkan som handskrivna signaturer. Medlemsstaterna måste dessutom säkerställa ett gränsöverskridande godtagande av kvalificerade e-signaturer, inom ramen för tillhandahållande av allmännyttiga tjänster, och de får inte införa några ytterliga krav som kan leda till hinder för användningen av sådana signaturer.

¹⁰ Den tillförlitliga förteckningen enligt kommissionens beslut 2009/767/EG, ändrat genom kommissionens beslut 2010/425/EU ska ligga till grund för ett nytt kommissionsbeslut om förteckningar över kvalificerad status, enligt denna förordning.

I artikel 21 fastställs kraven på kvalificerade certifikat för elektroniska signaturer. Genom artikeln förtydligas bilaga I till direktiv 1999/93/EG samtidigt som bestämmelser som inte fungerade i praktiken upphävs (t.ex. begränsningar av transaktionsvärden).

I artikel 22 fastställs kraven på kvalificerade anordningar för skapande av elektroniska signaturer. De krav på säkra anordningar för skapande av signaturer som fastställs i artikel 3.5 i direktiv 1999/93/EG förtydligas och dessa anordningar ska nu betraktas som kvalificerade anordningar för skapande av elektroniska signaturer i den mening som avses i denna förordning. I artikeln görs det också tydligt att en anordning för skapande av e-signaturer kan ha ett mycket vidare tillämpningsområde än att enbart innehålla uppgifter för att skapa e-signaturer. Kommissionen får även upprätta en förteckning över referensnummer till standarder för säkerhetskrav på anordningar.

Genom artikel 23, som bygger på artikel 3.4 i direktiv 1999/93/EG, införs även begreppet certifiering av kvalificerade anordningar för skapande av elektroniska signaturer i syfte att fastställa deras överensstämmelse med de säkerhetskrav som anges i bilaga II. Anordningarna måste erkännas av alla medlemsstater såsom motsvarande kraven när ett certifieringsförfarande utförs av ett certifieringsorgan som utsetts av en medlemsstat. Kommissionen ska offentliggöra en s.k. positivlista över sådana certifierade anordningar enligt artikel 24. Kommissionen får även upprätta en förteckning över referensnummer till standarder för säkerhetsbedömningen av IT-produkter som anges i artikel 23.1.

Artikel 24 gäller kommissionens offentliggörande av en förteckning över kvalificerade anordningar för skapande av elektroniska signaturer efter anmälan av överensstämmelse från medlemsstaterna.

Artikel 25 bygger på rekommendationerna i bilaga IV till direktiv 1999/93/EG om att fastställa bindande krav för valideringar av kvalificerade elektroniska signaturer i syfte att öka rättssäkerheten för sådana valideringar.

I artikel 26 fastställs villkoren för kvalificerade valideringstjänster.

I artikel 27 fastställs villkoret för långsiktigt bevarande av kvalificerade elektroniska signaturer. Detta är möjligt genom att man använder förfaranden och tekniker som gör det möjligt att utöka tillförlitligheten hos valideringsuppgifter för kvalificerade elektroniska signaturer bortom tidpunkten för deras tekniska giltighet när det kan bli enkelt för it-brottslingar att göra förfalskningar.

3.3.3.4 Avsnitt 4 – Elektroniska sigill

Artikel 28 gäller den rättsliga verkan av juridiska personers elektroniska sigill. En särskild rättslig presumtion tilldelas kvalificerade elektroniska sigill som garanterar ursprunget och integriteten hos de elektroniska dokument som de är kopplade till.

I artikel 29 fastställs kraven på kvalificerade certifikat för elektroniska sigill.

I artikel 30 fastställs krav på, certifiering av och offentliggörande av en förteckning över kvalificerade anordningar för skapande av elektroniska sigill.

I artikel 31 fastställs villkor för validering och bevarande av kvalificerade elektroniska sigill.

3.3.3.5 Avsnitt 5 – Elektronisk tidsmärkning

Artikel 32 gäller den rättsliga verkan av elektroniska tidsmärknings. En särskild rättslig presumtion tilldelas kvalificerade elektroniska tidsmärknings med avseende på vissheten om den berörda tidpunkten.

I artikel 33 fastställs kraven på kvalificerade elektroniska tidsmärknings.

3.3.3.6 Avsnitt 6 – Elektroniska dokument

Artikel 34 avser den rättsliga verkan och villkoren för godtagande av elektroniska dokument. Det finns en särskild rättslig presumtion om äktheten och integriteten hos elektroniska dokument som undertecknats med en kvalificerad elektronisk signatur eller som bär ett kvalificerat elektroniskt sigill. När det gäller godtagandet av elektroniska dokument ska, när ett originaldokument eller en bestyrkt kopia krävs för tillhandahållandet av en offentlig tjänst, åtminstone elektroniska dokument som utfärdats av personer med behörighet att utfärda dokumenten i fråga och som anses utgöra original eller bestyrkta kopior i enlighet med ursprungsmedlemsstatens nationella lagstiftning godtas i övriga medlemsstater utan ytterligare krav.

3.3.3.7 Avsnitt 7 – Elektroniska leveranstjänster

Artikel 35 gäller den rättsliga verkan av uppgifter som sänds eller tas emot med hjälp av en elektronisk leveranstjänst. En särskild rättslig presumtion rörande integriteten hos uppgifter som sänds eller tas emot samt i fråga om den tidpunkt vid vilken uppgifterna sänds eller tas emot är garanterad för kvalificerade elektroniska leveranstjänster. Genom artikeln garanteras även det ömsesidiga erkännandet av kvalificerade elektroniska leveranstjänster på unionsnivå.

I artikel 36 fastställs kraven på kvalificerade elektroniska leveranstjänster.

3.3.3.8 Avsnitt 8 – Autentisering av webbplatser

Detta avsnitt syftar till att se till att en webbplats äkthet med avseende på dess ägare kan garanteras.

I artikel 37 fastställs kraven för kvalificerade certifikat för autentisering av webbplatser, vilka kan användas för att garantera en webbplats äkthet. Ett kvalificerat certifikat för autentisering av webbplatser kommer att ge en minimiuppsättning tillförlitliga uppgifter om webbplatsen och om dess ägares rättsliga existens.

3.3.4 KAPITEL IV – DELEGERADE AKTER

Artikel 38 innehåller standardbestämmelser för utövandet av delegering i överensstämmelse med artikel 290 i EUF-fördraget (delegerade akter). Enligt denna artikel kan lagstiftaren till kommissionen delegera befogenheten att anta akter med allmän räckvidd som inte är lagstiftningsakter och som kompletterar eller ändrar vissa icke väsentliga delar av en lagstiftningsakt.

3.3.5 KAPITEL V – GENOMFÖRANDEAKTER

Artikel 39 innehåller bestämmelserna för kommittéförfarandet då kommissionen tilldelas genomförandebefogenheter när enhetliga villkor för genomförandet av unionens rättsligt bindande akter i enlighet med artikel 291 i EUF-fördraget behövs. Granskningsförfarandet är tillämpligt.

3.3.6 KAPITEL VI – SLUTBESTÄMMELSER

Genom artikel 40 förpliktigas kommissionen att utvärdera förordningen och rapportera om resultaten av denna utvärdering.

Genom artikel 41 upphävs direktiv 1999/93/EG och grunden läggs för en smidig övergång från den befintliga infrastrukturen för elektroniska signaturer till de nya kraven i denna förordning.

Genom artikel 42 fastställs dagen för förordningens ikraftträdande.

4. BUDGETEFFEKTER

Förslagets specifika budgeteffekter omfattar de uppgifter som tilldelas Europeiska kommissionen i enlighet med den finansieringsöversikt för rättsakter som medföljer förslaget.

Förslaget har ingen inverkan på driftskostnaderna.

Den finansieringsöversikt för rättsakt som medföljer detta förslag till förordning omfattar själva förordningens budgeteffekter.

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande¹¹,

efter samråd med Europeiska datatillsynsmannen¹²,

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

- (1) Att bygga upp förtroendet för nätmiljön är avgörande för den ekonomiska utvecklingen. Bristande förtroende gör att konsumenter, företag och myndigheter tvekar att utföra transaktioner på elektronisk väg och att använda nya tjänster.
- (2) Syftet med denna förordning är att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att möjliggöra ett säkert och sömlöst samspel mellan företag, medborgare och offentliga myndigheter, och därigenom öka effektiviteten hos offentliga och privata nättjänster, elektronisk affärsverksamhet och e-handel i unionen.
- (3) Europaparlamentet och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer¹³ gällde i huvudsak elektroniska signaturer. Det är inget heltäckande, gräns- och sektorsöverskridande regelverk för säkra, pålitliga och lättanvända elektroniska transaktioner. Genom denna förordning stärks och utvidgas direktivets regelverk.

¹¹ EUT C , , s . .

¹² EUT C , , s . .

¹³ EGT L 13, 19.1.2000, s. 12.

- (4) I kommissionens digitala agenda för Europa¹⁴ identifieras fragmenteringen av den digitala marknaden, bristen på interoperabilitet och den ökande it-brottsligheten som viktiga hinder för den digitala ekonomins positiva cykel. I sin Rapport om EU-medborgarskapet 2010 betonade kommissionen ytterligare vikten av att undanröja de största hindren för att EU-medborgarna ska kunna utnyttja fördelarna med en digital inre marknad och gränsöverskridande digitala tjänster¹⁵.
- (5) Europeiska rådet har uppmanat kommissionen att se till att en digital inre marknad skapas senast 2015, att göra snabba framsteg på centrala områden inom den digitala ekonomin¹⁶ och att främja en fullständigt integrerad digital inre marknad¹⁷ genom att underlätta gränsöverskridande användning av internetjänster, i synnerhet för att underlätta säker elektronisk identifiering och autentisering.
- (6) Rådet har uppmanat kommissionen att bidra till den digitala marknaden genom att skapa lämpliga förhållanden för ömsesidigt gränsöverskridande erkännande av grundläggande funktioner såsom elektronisk identifiering, elektroniska dokument, elektroniska signaturer och elektroniska leveranstjänster samt för interoperabla e-förvaltningstjänster i hela EU¹⁸.
- (7) Europaparlamentet har betonat betydelsen av säkerhet i elektroniska tjänster, särskilt i elektroniska signaturer, och behovet av att skapa en infrastruktur för kryptering med öppen nyckel (PKI) i hela Europa samt uppmanat kommissionen att inrätta en europeisk nätport för valideringsmyndigheter för att garantera gränsöverskridande interoperabilitet för elektroniska signaturer och öka säkerheten i samband med transaktioner som görs via internet¹⁹.
- (8) I Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden²⁰ uppmanas medlemsstaterna att inrätta gemensamma kontaktpunkter för att se till att alla förfaranden och formaliteter som är nödvändiga för tillträde till en tjänsteverksamhet och för att utöva den kan fullgöras enkelt, på distans och på elektronisk väg, via lämplig gemensam kontaktpunkt och med lämpliga myndigheter. Många nättjänster som är tillgängliga via gemensamma kontaktpunkter kräver e-identifiering, e-autentisering och e-signaturer.
- (9) I de flesta fall kan tillhandahållare av tjänster från en annan medlemsstat inte använda sin elektroniska identifiering för att få åtkomst till dessa tjänster därför att de nationella systemen för elektronisk identifiering i deras land inte är erkända och godtagna i andra medlemsstater. Detta elektroniska hinder utestänger tillhandahållare av tjänster från möjligheten att fullt ut utnyttja fördelarna med den inre marknaden. Ömsesidigt erkända och accepterade medel för elektronisk identifiering kommer att underlätta tillhandahållandet av en rad olika tjänster över gränserna på den inre

¹⁴ KOM(2010) 245 slutlig/2.

¹⁵ Rapport om EU-medborgarskapet 2010: Att undanröja hindren för EU-medborgarnas möjligheter att utöva sina rättigheter, KOM(2010) 603 slutlig, punkt 2.2.2, s. 13.

¹⁶ Europeiska rådets möte den 4 februari 2011: EUCO 2/1/11.

¹⁷ Europeiska rådets möte den 23 oktober 2011: EUCO 52/1/11.

¹⁸ Rådets slutsatser om EU:s handlingsplan för e-förvaltning 2011–2015, 3093:e mötet i rådet (transport, telekommunikation och energi), Bryssel den 27 maj 2011.

¹⁹ Europaparlamentets resolution av den 21 september 2010 om fullbordandet av den inre marknaden för e-handel, P7_TA(2010)0320, och Europaparlamentets resolution av den 15 juni 2010 om förvaltning av Internet – framtida åtgärder, P7_TA(2010)0208.

²⁰ EUT L 376, 27.12.2006, s. 36.

marknaden och ge företagen möjlighet att verka över gränserna utan att stöta på en mängd hinder i sina kontakter med myndigheter.

- (10) Genom Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård²¹ inrättas ett nätverk för nationella myndigheter som är ansvariga för e-hälsa. I syfte att öka säkerheten och kontinuiteten i gränsöverskridande hälso- och sjukvård ska nätverket utarbeta riktlinjer om tillgång till elektroniska hälso- och sjukvårdsuppgifter samt tjänster, inklusive genom att stödja ”*gemensamma åtgärder för identifiering och autentisering för att underlätta överförbara uppgifter i gränsöverskridande hälso- och sjukvård*”. Ömsesidigt erkännande av e-identifiering och –autentisering är en förutsättning för att gränsöverskridande sjukvård ska kunna bli en verklighet för Europas befolkning. OM personer reser för att söka vård måste deras sjukjournaler vara tillgängliga i behandlingslandet. Detta förutsätter robusta, säkra och tillförlitliga ramar för elektronisk identifiering.
- (11) Ett av målen för denna förordning är att undanröja befintliga hinder för den gränsöverskridande användningen av medel för elektronisk identifiering som används i medlemsstaterna för att få åtkomst till åtminstone offentliga tjänster. Förordningen syftar inte till att ingripa i elektroniska identitetshanteringssystem och tillhörande infrastrukturer som inrättats i medlemsstaterna. Syftet med denna förordning är att se till att säker elektronisk identifiering och autentisering för åtkomst till gränsöverskridande nättjänster som erbjuds av medlemsstaterna är möjlig.
- (12) Medlemsstaterna bör fortsätta att ha rätt att för elektronisk identifiering använda eller införa medel för åtkomst till nättjänster. De bör även ha möjlighet att själva bestämma om de vill engagera den privata sektorn i tillhandahållandet av dessa medel. Medlemsstaterna bör inte vara skyldiga att anmäla sina system för elektronisk identifiering. Det är upp till medlemsstaterna att välja om de vill anmäla alla, några eller inga av de elektroniska identifieringssystem som används på nationell nivå för att få åtkomst till åtminstone offentliga nättjänster eller särskilda nättjänster.
- (13) I förordningen bör vissa villkor fastställas rörande vilka medel för elektronisk identifiering som måste godtas och hur systemen bör anmälas. Dessa villkor bör hjälpa medlemsstaterna att bygga upp det förtroende som krävs för varandras system för elektronisk identifiering samt att ömsesidigt erkänna och godta medel för elektronisk identifiering som ingår i deras anmälda system. Principen om ömsesidigt erkännande och godtagande bör gälla om den anmälande medlemsstaten uppfyller villkoren för anmälan och om anmälan har offentliggjorts i *Europeiska unionens officiella tidning*. Åtkomsten till dessa nättjänster och deras slutliga leverans till den sökande bör dock vara nära kopplad till rätten att motta sådana tjänster enligt villkoren i nationell lagstiftning.
- (14) Medlemsstaterna bör ha möjlighet att besluta om den privata sektorn ska engageras i utfärdandet av medel för elektronisk identifiering och om den privata sektorn ska få använda medel för elektronisk identifiering inom ramen för ett anmält system för identifieringsändamål när detta behövs för nättjänster eller elektroniska transaktioner. Genom möjligheten att använda sådana medel för elektronisk identifiering kan den privata sektorn förlita sig på elektronisk identifiering och autentisering som redan i

²¹ EUT L 88, 4.4.2011, s. 45.

stor utsträckning används i många medlemsstater för åtminstone offentliga tjänster, samtidigt som det blir lättare för företag och medborgare att få åtkomst till sina gränsöverskridande nättjänster. För att göra det lättare för den privata sektorn att använda sådana gränsöverskridande medel för elektronisk identifiering bör den autentiseringsmöjlighet som tillhandahålls av medlemsstaterna vara tillgänglig för beroende parter utan diskriminering mellan den offentliga och den privata sektorn.

- (15) Gränsöverskridande användning av medel för elektronisk identifiering inom ramen för ett anmält system kräver att medlemsstaterna samarbetar när det gäller att tillhandahålla teknisk interoperabilitet. Detta innebär att det inte får finnas några särskilda nationella tekniska regler enligt vilka utländska parter måste skaffa sig t.ex. särskild maskinvara eller programvara för att kontrollera och validera den anmälda elektroniska identifieringen. Tekniska krav på användare som har sin grund i de inneboende specifikationerna för det igenkänningstecken som används (t.ex. smartkort) är däremot oundvikliga.
- (16) Medlemsstaternas samarbete bör gagna den tekniska interoperabiliteten för de anmälda systemen för elektronisk identifiering i syfte att främja förtroende och en hög skyddsnivå som är anpassad till risknivån. Ett utbyte av information och bästa praxis mellan medlemsstaterna med sikte på ömsesidigt erkännande bör bidra till detta samarbete.
- (17) Genom denna förordning bör även ett allmänt regelverk för användningen av elektroniska betrodda tjänster upprättas. Någon allmän förpliktelse att använda dem bör dock inte skapas. Den bör inte gälla tillhandahållande av tjänster som grundar sig på frivilliga civilrättsliga avtal. Den bör heller inte gälla frågor som avser ingående eller giltighet av avtal eller andra rättsliga förpliktelser om den nationella lagstiftningen eller unionslagstiftningen föreskriver vissa formkrav.
- (18) För att bidra till den allmänna gränsöverskridande användningen av elektroniska betrodda tjänster bör det vara möjligt att använda dem som bevis vid rättsliga förfaranden i alla medlemsstater.
- (19) Utöver de tjänster som ingår i den fasta förteckning över betrodda tjänster som avses i denna förordning bör medlemsstaterna ha frihet att fastställa andra typer av betrodda tjänster för erkännande på nationell nivå som kvalificerade betrodda tjänster.
- (20) På grund av den snabba tekniska utvecklingen bör denna förordning omfatta en strategi som är öppen för innovationer.
- (21) Denna förordning bör vara teknikneutral. Den rättsliga verkan som den medför bör vara möjlig att uppnå med alla typer av tekniska medel, förutsatt att kraven i denna förordning är uppfyllda.
- (22) För att öka människors förtroende för den inre marknaden och för att främja användningen av betrodda tjänster och produkter, bör begreppen kvalificerade betrodda tjänster och kvalificerad tillhandahållare av betrodda tjänster införas i syfte att ange krav och förpliktelser som garanterar en hög grad av säkerhet oavsett vilken typ av kvalificerad betrodd tjänst eller produkt som används eller tillhandahålls.
- (23) I linje med de förpliktelser som följer av Förenta nationernas konvention om rättigheter för personer med funktionsnedsättning, som har trätt i kraft i EU, bör

personer med funktionsnedsättning kunna använda betrodda tjänster och slutanvändarprodukter som används vid tillhandahållandet av dessa tjänster på samma villkor som andra konsumenter.

- (24) En tillhandahållare av betrodda tjänster är registeransvarig för personuppgifter och måste därför uppfylla de förpliktelser som anges i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter²². Särskilt insamling av uppgifter ska begränsas så mycket som möjligt med hänsyn till ändamålet med den tjänst som tillhandahålls.
- (25) Tillsynsorganen bör samarbeta och utbyta information med dataskyddsmyndigheter för att säkerställa att tjänstetillhandahållare genomför dataskyddslagstiftningen på ett korrekt sätt. Informationsutbytet bör särskilt gälla säkerhetstillbud och personuppgiftsöverträdelser.
- (26) För att öka användarnas förtroende för den inre marknaden bör det åligga alla tillhandahållare av betrodda tjänster att tillämpa goda säkerhetsförfaranden som är lämpliga i förhållande till de risker som deras verksamhet är förenad med.
- (27) Bestämmelser om användningen av pseudonymer i certifikat bör inte hindra medlemsstaterna från att kräva identifiering av personer i enlighet med unionslagstiftningen eller nationell lagstiftning.
- (28) För att säkerställa en jämförbar säkerhetsnivå i fråga om kvalificerade betrodda tjänster bör alla medlemsstater införa gemensamma grundläggande tillsynskrav. För att underlätta en enhetlig tillämpning av dessa krav i hela unionen bör medlemsstaterna införa jämförbara förfaranden och utbyta information om sin tillsynsverksamhet och bästa praxis på området.
- (29) Det är mycket viktigt att säkerhetsöverträdelser och bedömningar av säkerhetsrisker anmäls så att berörda parter kan förses med tillräcklig information i händelse av en säkerhetsöverträdelse eller en integritetsförlust.
- (30) För att kommissionen och medlemsstaterna ska kunna bedöma hur effektiv den mekanism för anmälan av överträdelser som införs genom denna förordning är, bör tillsynsorganen vara skyldiga att överlämna sammanfattande information till kommissionen och till Europeiska byrån för nät- och informationssäkerhet (Enisa).
- (31) För att kommissionen och medlemsstaterna ska kunna bedöma effekterna av denna förordning bör tillsynsorganen vara skyldiga att överlämna statistik om marknaden för och användningen av kvalificerade betrodda tjänster.
- (32) För att kommissionen och medlemsstaterna ska kunna bedöma hur effektiv den förstärkta tillsynsmekanism som införs genom denna förordning är, bör tillsynsorganen vara skyldiga att rapportera om sin verksamhet. Detta skulle kraftigt bidra till att underlätta utbytet av god praxis mellan tillsynsorganen och säkerställa kontrollen av att väsentliga tillsynskrav genomförs på ett enhetligt och verkningfullt sätt i alla medlemsstater.

²²

EUT L 281, 23.11.1995, s. 31.

- (33) För att säkerställa att kvalificerade betrodda tjänster är hållbara och varaktiga samt för att öka användarnas förtroende för kontinuiteten i dessa tjänster, bör tillsynsorganen se till att uppgifterna hos kvalificerade tillhandahållare av betrodda tjänster bevaras och förblir tillgängliga under en lämplig tidsperiod även i de fall en sådan tillhandahållare upphör att existera.
- (34) För att underlätta tillsynen av kvalificerade tillhandahållare av betrodda tjänster, t.ex. när en sådan tillhandahåller sina tjänster i en annan medlemsstat och inte omfattas av tillsyn där, eller när en tillhandahållares datorer är placerade i en annan medlemsstat än den där tillhandahållaren är etablerad, bör ett system för ömsesidigt bistånd mellan medlemsstaternas tillsynsorgan inrättas.
- (35) Tillhandahållare av betrodda tjänster ansvarar för att uppfylla de krav som anges i denna förordning för tillhandahållande av betrodda tjänster och särskilt för kvalificerade betrodda tjänster. Tillsynsorgan ansvarar för tillsynen av huruvida tillhandahållarna av betrodda tjänster uppfyller dessa krav.
- (36) För att få till stånd en effektiv initieringsprocess, som bör leda till att kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster de tillhandahåller införs i förteckningar över betrodda tjänsteleverantörer, bör man uppmuntra inledande kontakter mellan potentiella kvalificerade tillhandahållare av betrodda tjänster och behöriga tillsynsorgan, i syfte att underlätta den omsorgsfulla granskning som ska leda fram till tillhandahållandet av kvalificerade betrodda tjänster.
- (37) Förteckningar över betrodda tjänsteleverantörer kan vara viktiga för att hjälpa till att bygga upp förtroendet bland aktörer på marknaden, eftersom de visar att tjänstetillhandahållaren vid tidpunkten för tillsynen hade status som kvalificerad. Å andra sidan är sådana förteckningar inte obligatoriska, eftersom huruvida en aktör ges status som kvalificerad och får tillhandahålla kvalificerade betrodda tjänster endast är avhängigt att kraven i denna förordning respekteras.
- (38) Så snart en kvalificerad betrodd tjänst har anmälts får den inte avvisas för utförande av ett administrativt förfarande eller formalitet av det berörda offentliga organet av det skälet att den inte ingår i den betrodda förteckning som upprättats av medlemsstaterna. För detta syfte avses med offentligt organ en offentlig myndighet eller annan enhet som tillhandahåller e-förvaltningstjänster som skattedeklaration via internet, begäran om personbevis, deltagande i elektroniska offentliga upphandlingar etc.
- (39) Det krävs en hög säkerhetsnivå för att säkerställa ömsesidigt erkännande av elektroniska signaturer, men i vissa fall, som t.ex. i den mening som avses i kommissionens beslut 2009/767/EG av den 16 oktober 2009 om åtgärder som underlättar användningen av förfaranden på elektronisk väg genom gemensamma kontaktpunkter i enlighet med Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden²³, bör även elektroniska signaturer med en lägre säkerhetsgrad godtas.
- (40) Det bör vara möjligt för undertecknare att anförtro anordningar för skapande av kvalificerade elektroniska signaturer till en tredje part, förutsatt att lämpliga mekanismer och förfaranden tillämpas för att se till att undertecknaren har användningen av sina uppgifter för skapande av elektroniska signaturer uteslutande

²³

EUT L 274, 20.10.2009, s. 36.

under sin egen kontroll och att kraven för kvalificerade elektroniska signaturer uppfylls genom anordningens användning.

- (41) För att kunna garantera rättssäkerheten avseende en signaturs giltighet är det nödvändigt att i närmare detalj ange vilka komponenter i en kvalificerad elektronisk signatur som måste bedömas av den beroende part som utför valideringen. Genom att fastställa krav på kvalificerade tillhandahållare av betrodda tjänster som kan tillhandahålla en kvalificerad valideringstjänst till beroende parter som inte själva vill eller kan utföra valideringen av kvalificerade elektroniska signaturer bör dessutom den privata eller den offentliga sektorn stimuleras att investera i sådana tjänster. Sammantaget bör dessa krav göra kvalificerad validering av elektroniska signaturer enkelt och bekvämt för alla parter på unionsnivå.
- (42) När en transaktion kräver ett kvalificerat elektroniskt sigill från en juridisk person bör en kvalificerad elektronisk signatur från ett behörigt ombud för den juridiska personen vara lika godtagbar.
- (43) Elektroniska sigill bör utgöra bevis för att ett elektroniskt dokument har utfärdats av en juridisk person och med säkerhet garantera dokumentets ursprung och integritet.
- (44) Genom denna förordning bör långsiktigt bevarande av uppgifter säkerställas, dvs. den rättsliga giltigheten hos elektroniska signaturer och elektroniska sigill över längre tidsperioder, i syfte att garantera att de kan valideras oavsett kommande tekniska förändringar.
- (45) För att öka den gränsöverskridande användningen av elektroniska dokument bör denna förordning innehålla bestämmelser om den rättsliga verkan av elektroniska dokument, vilken bör anses vara densamma som för pappersdokument beroende på en riskbedömning och förutsatt att dokumentens äkthet och integritet har säkerställts. För att ytterligare utveckling av gränsöverskridande elektroniska transaktioner på den inre marknaden ska vara möjlig är det också viktigt att elektroniska dokument i original eller bestyrkta kopior utfärdade enligt den nationella lagstiftningen av relevanta behöriga organ i en medlemsstat godtas som sådana även i andra medlemsstater. Denna förordning bör inte påverka medlemsstaternas rätt att avgöra vad som utgör ett original eller en kopia på nationell nivå, utan den ska se till att dessa kan användas som sådana även över gränserna.
- (46) Eftersom behöriga myndigheter i medlemsstaterna för närvarande använder olika avancerade elektroniska signaturer av olika format för att underteckna sina dokument elektroniskt är det nödvändigt att se till att åtminstone ett visst antal format av avancerade elektroniska signaturer kan stödjas tekniskt av medlemsstaterna när de erhåller dokument som undertecknats elektroniskt. På samma sätt skulle det när behöriga myndigheter i medlemsstaterna använder avancerade elektroniska sigill vara nödvändigt att se till att de stödjer åtminstone ett visst antal format av avancerade elektroniska sigill.
- (47) Elektroniska sigill kan användas för att autentisera ett dokument som utfärdats av en juridisk person men även för att autentisera en juridisk persons digitala tillgångar, t.ex. programvarukoder och servrar.

- (48) Genom att göra det möjligt att autentisera webbplatser och den person som äger dem skulle det bli svårare att förfalska webbplatser och därmed även bli möjligt att minska bedrägerierna.
- (49) För att på ett flexibelt och snabbt sätt kunna komplettera vissa detaljerade tekniska aspekter av denna förordning bör befogenhet att anta akter i enlighet med artikel 290 i fördraget om Europeiska unionens funktionssätt delegeras till kommissionen med avseende på följande: interoperabilitet för elektronisk identifiering; krav på säkerhetsåtgärder som ska vidtas av tillhandahållare av betrodda tjänster; erkända oberoende organ med ansvar för att granska tjänstetillhandahållarna; förteckningar över betrodda tjänsteleverantörer; krav som avser säkerhetsnivåer för elektroniska signaturer; krav på kvalificerade certifikat för elektroniska signaturer, deras validering och deras bevarande; organ med ansvar för certifieringen av kvalificerade anordningar för skapande av elektroniska signaturer; krav som avser säkerhetsnivåer för elektroniska sigill och kvalificerade certifikat för elektroniska sigill; interoperabilitet mellan leveranstjänster. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, även på expertnivå.
- (50) Kommissionen bör, då den förbereder och utarbetar delegerade akter, se till att relevanta handlingar översänds samtidigt till Europaparlamentet och till rådet samt att detta sker så snabbt som möjligt och på lämpligt sätt.
- (51) För att säkerställa enhetliga villkor för genomförandet av denna förordning bör genomförandebefogenheter tilldelas kommissionen, särskilt för att ange referensnummer till standarder vilkas användning skulle förutsätta en överensstämmelse med vissa krav i denna förordning eller i delegerade akter. Befogenheterna bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter²⁴.
- (52) Av rättssäkerhets- och tydlighetsskäl bör direktiv 1999/93/EG upphävas.
- (53) För att garantera rättssäkerheten för marknadsoperatörer som redan använder kvalificerade certifikat som utfärdas i enlighet med direktiv 1999/93/EG är det nödvändigt att medge tillräckligt med tid för en övergångsperiod. Det är också nödvändigt att göra det möjligt för kommissionen att anta genomförandekter och delegerade akter före det datumet.
- (54) Eftersom denna förordnings mål inte i tillräcklig utsträckning kan uppnås av medlemsstaterna och därför på grund av åtgärdens omfattning bättre kan uppnås på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål, särskilt när det gäller kommissionens roll som samordnare av nationell verksamhet.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

²⁴ EUT L 55, 28.2.2011, s. 13.

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte

1. I denna förordning fastställs regler för elektronisk identifiering och elektroniska betrodda tjänster för elektroniska transaktioner i syfte att säkerställa en väl fungerande inre marknad.
2. I förordningen fastställs de villkor under vilka medlemsstaterna ska erkänna och godta medel för elektronisk identifiering av fysiska och juridiska personer som omfattas av ett anmält system för elektronisk identifiering från en annan medlemsstat.
3. I förordningen fastställs en rättslig ram för elektroniska signaturer, elektroniska sigill, elektronisk tidsmärkning, elektroniska dokument, elektroniska leveranstjänster och autentisering av webbplatser.
4. Genom förordningen säkerställs att betrodda tjänster och produkter som överensstämmer med denna förordning har fri rörlighet på den inre marknaden.

Artikel 2

Tillämpningsområde

1. Denna förordning gäller elektronisk identifiering som tillhandahålls av medlemsstaterna, alternativt för deras räkning eller på deras ansvar, och tillhandahållare av betrodda tjänster inom unionen.
2. Förordningen gäller inte tillhandahållande av elektroniska betrodda tjänster som grundar sig på frivilliga civilrättsliga avtal.
3. Den gäller inte frågor som avser ingående eller giltighet av avtal eller andra rättsliga förpliktelser om den nationella lagstiftningen eller unionslagstiftningen föreskriver vissa formkrav.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

- 1) *elektronisk identifiering*: en process inom vilken personidentifieringsuppgifter i elektronisk form som otvetydigt företräder en fysisk eller juridisk person används.
- 2) *medel för elektronisk identifiering*: en materiell eller immateriell enhet som innehåller de uppgifter som avses i punkt 1 i denna artikel och som används för att få åtkomst till de nättjänster som avses i artikel 5.
- 3) *system för elektronisk identifiering*: ett system för elektronisk identifiering genom vilket medel för elektronisk identifiering utfärdas till personer enligt punkt 1 i denna artikel.

4) *autentisering*: en elektronisk process som gör det möjligt att validera den elektroniska identifieringen av en fysisk eller juridisk person, eller en elektronisk uppgifts ursprung och integritet.

5) *undertecknare*: en fysisk person som skapar en elektronisk signatur.

6) *elektronisk signatur*: uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska uppgifter och som används av undertecknaren för att underteckna.

7) *avancerad elektronisk signatur*: en elektronisk signatur som uppfyller följande krav:

(a) Den ska vara knuten uteslutande till undertecknaren.

(b) Undertecknaren ska kunna identifieras genom den.

(c) Den ska vara skapad med uppgifter för skapande av en elektronisk signatur som undertecknaren med en hög grad av förtroende kan använda under uteslutande sin egen kontroll.

(d) Den ska vara kopplad till de uppgifter den avser på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

8) *kvalificerad elektronisk signatur*: en avancerad elektronisk signatur som skapas med en kvalificerad anordning för skapande av elektroniska signaturer och som är baserad på ett kvalificerat certifikat för elektroniska signaturer.

9) *uppgifter för skapande av elektroniska signaturer*: unika uppgifter som undertecknaren använder för att skapa en elektronisk signatur.

10) *certifikat*: ett elektroniskt intyg som kopplar valideringsuppgifter för en elektronisk signatur eller ett elektroniskt sigill till en fysisk respektive juridisk person och bekräftar uppgifterna om den personen.

11) *kvalificerat certifikat för elektroniska signaturer*: ett certifikat som används till stöd för elektroniska signaturer, utfärdas av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga I.

12) *betrodd tjänst*: en elektronisk tjänst som består av skapande, kontroll, validering, hantering och bevarande av elektroniska signaturer, elektroniska sigill, elektroniska tidsmärkingar, elektroniska dokument, elektroniska leveranstjänster, autentisering av webbplatser och elektroniska certifikat, inklusive certifikat för elektroniska signaturer och för elektroniska sigill.

13) *kvalificerad betrodd tjänst*: en betrodd tjänst som uppfyller tillämpliga krav i denna förordning.

14) *tillhandahållare av betrodda tjänster*: en fysisk eller en juridisk person som tillhandahåller en eller flera betrodda tjänster.

15) *kvalificerad tillhandahållare av betrodda tjänster*: en tillhandahållare av betrodda tjänster som uppfyller kraven i denna förordning.

16) *produkt*: maskinvara eller programvara, eller komponenter i sådana system, som är avsedda att användas för tillhandahållande av betrodda tjänster.

17) *anordning för skapande av elektroniska signaturer*: en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk signatur.

18) *kvalificerad anordning för skapande av elektroniska signaturer*: en anordning för skapande av elektroniska signaturer som uppfyller kraven i bilaga II.

19) *skapare av ett sigill*: en juridisk person som skapar ett elektroniskt sigill.

20) *elektroniskt sigill*: uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra elektroniska uppgifter för att garantera ursprung och integritet hos tillhörande uppgifter.

21) *avancerat elektroniskt sigill*: ett elektroniskt sigill som uppfyller följande krav:

- (a) Det ska vara knutet uteslutande till skaparen av sigillet.
- (b) Skaparen av sigillet ska kunna identifieras genom det.
- (c) Det ska vara skapat med uppgifter för skapande av ett elektroniskt sigill som sigillet skapare med en hög grad av förtroende under sin kontroll kan använda för skapande av elektroniska sigill.
- (d) Det ska vara kopplat till de uppgifter det avser på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

22) *kvalificerat elektroniskt sigill*: ett avancerat elektroniskt sigill som skapas med en kvalificerad anordning för skapande av elektroniska sigill och som är baserat på ett kvalificerat certifikat för elektroniska sigill.

23) *uppgifter för skapande av elektroniska sigill*: unika uppgifter som skaparen av det elektroniska sigillet använder för att skapa ett elektroniskt sigill.

24) *kvalificerat certifikat för elektroniska sigill*: ett intyg som används till stöd för ett elektroniskt sigill, utfärdas av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller de krav som fastställs i bilaga III.

25) *elektronisk tidsmärkning*: uppgifter i elektronisk form som binder andra elektroniska uppgifter till en viss tidpunkt och därmed utgör bevis om att de uppgifterna fanns vid den tidpunkten.

26) *kvalificerad elektronisk tidsmärkning*: en elektronisk tidsmärkning som uppfyller de krav som fastställs i artikel 33.

27) *elektroniskt dokument*: ett dokument i elektronisk format.

28) *elektronisk leveranstjänst*: en tjänst som gör det möjligt att överföra uppgifter på elektronisk väg och utgör bevis avseende de överförda uppgifternas hantering, inklusive bevis om uppgifternas sändning eller mottagande, och som skyddar överförda uppgifter mot risken för förlust, stöld, skada eller otillåtna ändringar.

29) *kvalificerad elektronisk leveranstjänst*: en elektronisk leveranstjänst som uppfyller de krav som fastställs i artikel 36.

30) *kvalificerat certifikat för autentisering av webbplatser*: ett intyg som gör det möjligt att autentisera en webbplats och koppla webbplatsen till den person som certifikatet utfärdats för, och som utfärdas av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga IV.

31) *valideringsuppgifter*: uppgifter som används för att validera en elektronisk signatur eller ett elektroniskt sigill.

Artikel 4

Inre marknadsprincipen

1. Tillhandahållande av betrodda tjänster i en medlemsstat som utförs av en tillhandahållare av sådana tjänster som är etablerad i en annan medlemsstat får inte begränsas av skäl som omfattas av de områden som regleras i denna förordning.
2. Produkter som överensstämmer med denna förordning ska omfattas av fri rörlighet på den inre marknaden.

KAPITEL II

ELEKTRONISK IDENTIFIERING

Artikel 5

Ömsesidigt erkännande och godtagande

När det enligt nationell lagstiftning eller administrativa förfaranden krävs en elektronisk identifiering där medel för elektronisk identifiering och autentisering används för att få åtkomst till en tjänst på internet, ska alla medel för elektronisk identifiering som utfärdats i en annan medlemsstat och som omfattas av ett system som ingår i den förteckning som offentliggjorts av kommissionen i enlighet med det förfarande som avses i artikel 7 erkännas och godtas för åtkomst till denna tjänst.

Artikel 6

Villkor för anmälan av system för elektronisk identifiering

1. System för elektronisk identifiering ska vara berättigade till anmälan enligt artikel 7 om samtliga följande villkor är uppfyllda:
 - (a) Medlet för elektronisk identifiering ska vara utfärdat av den anmälände medlemsstaten, alternativt för dess räkning eller på dess ansvar.
 - (b) Medlet för elektronisk identifiering ska kunna användas för att få åtkomst till åtminstone offentliga tjänster som kräver elektronisk identifiering i den anmälände medlemsstaten.
 - (c) Den anmälände medlemsstaten ska se till att personidentifieringsuppgifterna otvetydigt hänför sig till den fysiska eller juridiska person som avses i artikel 3.1.
 - (d) Den anmälände medlemsstaten ska se till att en autentiseringsmöjlighet är tillgänglig på internet när som helst och kostnadsfritt så att alla beroende parter kan validera de personliga identifieringsuppgifter som tas emot i elektronisk form. Medlemsstaterna får inte ålägga beroende parter som är etablerade utanför deras territorium och som vill utföra en sådan autentisering några särskilda tekniska krav. Vid överträdelse eller äventyrande av det anmälda systemet för identifiering eller autentiseringsmöjligheten ska medlemsstaterna utan dröjsmål upphäva eller återkalla det anmälda systemet för identifiering, autentiseringsmöjligheten eller de berörda äventyrade delarna och informera övriga medlemsstater och kommissionen i enlighet med artikel 7.

- (e) Den anmälade medlemsstaten tar på sig skadeståndsansvaret för
 - i) att de personliga identifieringsuppgifter som avses i punkt c otvetydigt hänför sig till den berörda personen, och
 - ii) den autentiseringsmöjlighet som anges i punkt d.

2. Punkt 1 e påverkar inte tillämpningen av det skadeståndsansvar som gäller för parter i en transaktion där medel för elektronisk identifiering som omfattas av det anmälda systemet används.

Artikel 7

Anmälan

1. Medlemsstater som anmäler ett system för elektronisk identifiering ska till kommissionen överlämna följande uppgifter samt utan onödigt dröjsmål meddela eventuella senare ändringar av dessa:

- (a) En beskrivning av det anmälda systemet för elektronisk identifiering.
- (b) De myndigheter som ansvarar för det anmälda systemet för elektronisk identifiering.
- (c) Information om den som hanterar registreringen av de otvetydiga personidentifieringsuppgifterna.
- (d) En beskrivning av autentiseringsmöjligheten.
- (e) System för upphävande eller återkallelse av det anmälda systemet för identifiering eller autentiseringsmöjligheten, eller de berörda äventyrade delarna.

2. Kommissionen ska sex månader efter förordningens ikraftträdande offentliggöra förteckningen över de system för elektronisk identifiering som anmälts enligt punkt 1 och de grundläggande uppgifterna om dessa i *Europeiska unionens officiella tidning*.

3. Om kommissionen mottar en anmälan efter den period som avses i punkt 2 ska den ändra förteckningen inom tre månader.

4. Kommissionen får genom genomförandeakter fastställa förutsättningar, format och förfaranden för den anmälan som avses i punkterna 1 och 3. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Artikel 8

Samordning

1. Medlemsstaterna ska samarbeta för att säkerställa interoperabiliteten för elektroniska identifieringsmedel som omfattas av ett anmält system och för att öka deras säkerhet.

2. Kommissionen ska genom genomförandeakter fastställa nödvändiga villkor för att underlätta det samarbete mellan medlemsstaterna som avses i punkt 1 i syfte att främja en hög nivå av förtroende och säkerhet som står i proportion till risknivån. Dessa genomförandeakter ska bland annat behandla utbyte av information, erfarenheter och bra metoder i fråga om

system för elektronisk identifiering, kollegial utvärdering av anmälda system för elektronisk identifiering samt undersökning av relevant utveckling inom sektorn för elektronisk identifiering. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

3. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 38 när det gäller att underlätta gränsöverskridande interoperabilitet för medel för elektronisk identifiering genom fastställande av tekniska minimikrav.

KAPITEL III

BETRODDA TJÄNSTER

Avsnitt 1

Allmänna bestämmelser

Artikel 9

Skadeståndsansvar

1. En tillhandahållare av betrodda tjänster ska vara ansvarig för all direkt skada som åsamkats en fysisk eller en juridisk person genom underlåtenhet att uppfylla de skyldigheter som anges i artikel 15.1, såvida inte tillhandahållaren i fråga kan bevisa att denne inte har handlat vårdslöst.

2. En kvalificerad tillhandahållare av betrodda tjänster ska vara ansvarig för all direkt skada som åsamkats en fysisk eller en juridisk person genom underlåtenhet att uppfylla de krav som anges i denna förordning, särskilt i artikel 19, såvida inte tillhandahållaren i fråga kan bevisa att denne inte har handlat vårdslöst.

Artikel 10

Tillhandahållare av betrodda tjänster från tredjeländer

1. Kvalificerade betrodda tjänster och kvalificerade certifikat som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster som är etablerade i ett tredjeland ska godtas som rättsligt likvärdiga med kvalificerade betrodda tjänster och kvalificerade certifikat som tillhandahålls av en kvalificerad tillhandahållare av betrodda tjänster som är etablerad inom unionen, under förutsättning att de kvalificerade betrodda tjänsterna eller kvalificerade certifikaten från tredjelandet är erkända enligt ett avtal mellan unionen och tredjeländer eller internationella organisationer i enlighet med artikel 218 i EUF-fördraget.

2. Med hänvisning till punkt 1 ska sådana avtal garantera att de krav som är tillämpliga på kvalificerade betrodda tjänster och kvalificerade certifikat som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster etablerade inom unionens territorium, uppfylls av tillhandahållarna av betrodda tjänster i tredjeländerna eller de internationella organisationerna, särskilt i fråga om skydd av personuppgifter, säkerhet och tillsyn.

Artikel 11

Databehandling och dataskydd

1. Tillhandahållare av betrodda tjänster och tillsynsorgan ska se till att personuppgifter behandlas på ett rättvist och lagligt sätt i enlighet med direktiv 95/46/EG.
2. Tillhandahållare av betrodda tjänster ska behandla personuppgifter i enlighet med direktiv 95/46/EG. Sådan behandling ska begränsas till de minimiuppgifter som krävs för att utfärda och bibehålla ett certifikat eller för att tillhandahålla en betrodd tjänst.
3. Tillhandahållare av betrodda tjänster ska garantera konfidentialiteten och integriteten hos uppgifter som gäller en person till vilken den betrodda tjänsten tillhandahålls.
4. Utan att det påverkar den rättsliga verkan som enligt nationell lagstiftning ges pseudonymer får inte medlemsstaterna hindra att tillhandahållare av betrodda tjänster anger en pseudonym i stället för undertecknarens namn i certifikat för elektroniska signaturer.

Artikel 12

Tillgänglighet för personer med funktionsnedsättning

Betrodda tjänster som tillhandahålls och slutanvändarprodukter som används i samband med tillhandahållandet av dessa tjänster ska då detta är möjligt göras tillgängliga för personer med funktionsnedsättning.

Avsnitt 2

Tillsyn

Artikel 13

Tillsynsorgan

1. Medlemsstaterna ska utse ett lämpligt organ som är etablerat inom deras territorium eller, efter ömsesidig överenskommelse, i en annan medlemsstat på ansvar av den medlemsstat som utsett organet. Tillsynsorgan ska tilldelas alla nödvändiga befogenheter för tillsyn och undersökning som krävs för utövande av deras uppgifter.
2. Tillsynsorganet ska ha ansvaret för att följande uppgifter utförs:
 - (a) Övervakning av tillhandahållare av betrodda tjänster som är etablerade i den medlemsstat där de har utsetts för att se till att de uppfyller kraven i artikel 15.
 - (b) Tillsyn av kvalificerade tillhandahållare av betrodda tjänster som är etablerade i den medlemsstat där de har utsetts och av de kvalificerade betrodda tjänster som de tillhandahåller för att se till att dessa och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller tillämpliga krav i denna förordning.
 - (c) Säkerställande av att den relevanta information och de relevanta uppgifter som avses i artikel 19.2 g och som registreras av kvalificerade tillhandahållare av betrodda

tjänster bevaras och är tillgängliga efter det att verksamheten hos en kvalificerad tillhandahållare av betrodda tjänster har upphört, under en lämplig tid och med sikte på att garantera tjänstens kontinuitet.

3. Varje tillsynsorgan ska till kommissionen och medlemsstaterna överlämna en årsrapport om det senaste kalenderårets tillsynsverksamhet före slutet av det första kvartalet på följande år. Denna rapport ska innehålla minst följande uppgifter:

- (a) Uppgifter om organets tillsynsverksamhet.
- (b) En sammanfattning av överträdelseanmälningar som har inkommit från tillhandahållare av betrodda tjänster i enlighet med artikel 15.2.
- (c) Statistik om marknaden för och användningen av kvalificerade betrodda tjänster, inklusive information om tillhandahållarna av betrodda tjänster själva, de kvalificerade betrodda tjänster som de tillhandahåller, de produkter som de använder och en allmän beskrivning av deras kunder.

4. Medlemsstaterna ska till kommissionen och övriga medlemsstater överlämna namn på och adress till deras respektive utsedda tillsynsorgan.

5. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 38 rörande fastställande av förfaranden för de uppgifter som avses i punkt 2.

6. Kommissionen får genom genomförandeakter fastställa förutsättningar, format och förfaranden för den rapport som avses i punkt 3. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Artikel 14

Ömsesidigt bistånd

1. Tillsynsorganen ska samarbeta med sikte på att utbyta god praxis och att snarast möjligt ge varandra relevant information och ömsesidigt bistånd så att åtgärder kan vidtas på ett enhetligt sätt. Det ömsesidiga biståndet ska bland annat omfatta möjligheten att kunna begära information från varandra och bistå varandra i tillsynsarbetet, t.ex. genom att utföra inspektioner avseende de säkerhetsgranskningar som avses i artiklarna 15, 16 och 17.

2. Ett tillsynsorgan som tar emot en begäran om bistånd får bara vägra att tillmötesgå begäran om

- (a) organet inte är behörigt att behandla den, eller
- (b) det skulle stå i strid med denna förordning att tillmötesgå begäran.

3. I tillämpliga fall får tillsynsorganen utföra gemensamma undersökningar där personal från andra medlemsstaters tillsynsorgan deltar.

Tillsynsorganet i den medlemsstat där undersökningen ska äga rum får inom ramen för sin nationella lagstiftning anförtro undersökande arbetsuppgifter åt personal från det biträdda tillsynsorganet. Sådana befogenheter får endast utövas under överinsyn av och i närvaro av personal från värdlandets tillsynsorgan. Personalen från det biträdda landets tillsynsorgan ska

lyda under den nationella lagstiftning som gäller för värdlandets tillsynsorgan. Vårdlandets tillsynsorgan ska ansvara för det biträdda tillsynsorganets personals handlingar.

4. Kommissionen får genom genomförandeakter ange format och förfaranden för det ömsesidiga bistånd som fastställs i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Artikel 15

Säkerhetskrav på tillhandahållare av betrodda tjänster

1. Tillhandahållare av betrodda tjänster som är etablerade inom unionens territorium ska vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster som de tillhandahåller. Dessa åtgärder ska utnyttja den senaste tekniken och säkerställa en lämplig säkerhetsnivå för graden av risk. I synnerhet ska åtgärder vidtas för att förhindra eller minimera säkerhetsincidenters inverkan samt för att informera berörda parter om negativa effekter av eventuella incidenter.

Tillhandahållare av betrodda tjänster får, utan att det påverkar tillämpningen av artikel 16.1, överlämna en rapport från en säkerhetsgranskning som utförts av ett erkänt oberoende organ till tillsynsorganet för att bekräfta att lämpliga säkerhetsåtgärder har vidtagits.

2. Tillhandahållare av betrodda tjänster ska, utan otillbörligt dröjsmål och om möjligt senast 24 timmar efter upptäckt, till det behöriga tillsynsorganet, det behöriga nationella organet för informationssäkerhet och övriga relevanta tredje parter, som t.ex. dataskyddsmyndigheter, anmäla alla säkerhetsöverträdelser eller integritetsförluster som har en betydande inverkan på den betrodda tjänst som tillhandahålls och på de personuppgifter som ingår i denna.

Det berörda tillsynsorganet ska vid behov, i synnerhet om säkerhetsöverträdelser eller integritetsförlusten gäller två eller flera medlemsstater, informera tillsynsorganen i övriga medlemsstater och Europeiska byrån för nät- och informationssäkerhet (Enisa).

Det berörda tillsynsorganet kan även informera allmänheten eller kräva att tillhandahållaren av betrodda tjänster gör det, om den slår fast att ett avslöjande av överträdelser ligger i allmänhetens intresse.

3. Tillsynsorganet ska en gång om året till Enisa och kommissionen överlämna en sammanfattning av de överträdelseanmälningar som inkommit från tillhandahållare av betrodda tjänster.

4. För att genomföra punkterna 1 och 2 ska det behöriga tillsynsorganet ha befogenhet att utfärda bindande instruktioner till tillhandahållare av betrodda tjänster.

5. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 38 rörande ytterligare specifikationer för de åtgärder som avses i punkt 1.

6. Kommissionen får genom genomförandeakter fastställa förutsättningar, format och förfaranden, inklusive tidsfrister, som ska vara tillämpliga för de ändamål som avses i punkterna 1–3. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Artikel 16

Tillsyn av kvalificerade tillhandahållare av betrodda tjänster

1. Kvalificerade tillhandahållare av betrodda tjänster ska en gång om året granskas av ett erkänt oberoende organ för att bekräfta att dessa och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning, samt lämna in rapporten om denna säkerhetsgranskning till tillsynsorganet.
2. Tillsynsorganet får, utan att det påverkar tillämpningen av punkt 1, när som helst granska de kvalificerade tillhandahållarna av betrodda tjänster för att bekräfta att dessa och de kvalificerade betrodda tjänster som de tillhandahåller fortfarande uppfyller kraven i denna förordning, på eget initiativ eller med anledning av en begäran från kommissionen. Vid misstänkta överträdelser av reglerna om skydd för personuppgifter ska tillsynsorganet informera dataskyddsmyndigheterna om sina granskningsresultat.
3. Tillsynsorganet ska även ha befogenhet att utfärda bindande instruktioner till kvalificerade tillhandahållare av betrodda tjänster om att åtgärda en eventuell underlåtenhet att uppfylla de krav som anges i rapporten från säkerhetsgranskningen.
4. Med hänvisning till punkt 3 ska den kvalificerade tillhandahållaren av betrodda tjänster, om denne inte åtgärdar underlåtenheten i fråga inom den tidsfrist som fastställts av tillsynsorganet, förlora sin status som kvalificerad och av tillsynsorganet informeras om att dess status kommer att ändras i enlighet med detta i de förteckningar över betrodda tjänsteleverantörer som avses i artikel 18.
5. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 38 rörande fastställandet av de villkor under vilka det oberoende organ som utför den granskning som avses i punkt i den här artikeln och i artiklarna 15.1 och 17.1 ska erkännas.
6. Kommissionen får genom genomförandeaakter fastställa förutsättningar, format och förfaranden som ska vara tillämpliga för de ändamål som avses i punkterna 1, 2 och 4. Dessa genomförandeaakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Artikel 17

Inledande av en kvalificerad betrodd tjänst

1. Kvalificerade tillhandahållare av betrodda tjänster ska anmäla sin avsikt att börja tillhandahålla en kvalificerad betrodd tjänst till tillsynsorganet och till detta även lämna in en rapport från en säkerhetsgranskning som utförts av ett erkänt oberoende organ i enlighet med artikel 16.1. Kvalificerade tillhandahållare av betrodda tjänster får börja tillhandahålla den kvalificerade betrodda tjänsten efter det att de lämnat in anmälan och rapporten från säkerhetsgranskningen till tillsynsorganet.
2. När de relevanta dokumenten har lämnats in till tillsynsorganet i enlighet med punkt 1 ska de kvalificerade tillhandahållarna av tjänster tas upp i de förteckningar över betrodda tjänsteleverantörer som avses i artikel 18 vilket visar att anmälan har lämnats in.

3. Tillsynsorganet ska kontrollera att den kvalificerade tillhandahållaren av betrodda tjänster och de kvalificerade betrodda tjänster som denne tillhandahåller uppfyller kraven i denna förordning.

Tillsynsorganet ska, efter kontroll med positivt utfall, ange kvalificerad status för kvalificerade tillhandahållare av tjänster och de kvalificerade betrodda tjänster som dessa tillhandahåller, i förteckningarna över betrodda tjänsteleverantörer, senast en månad efter att anmälan gjorts i enlighet med punkt 1.

Om kontrollen inte har slutförts inom en månad ska tillsynsorganet informera den kvalificerade tillhandahållaren av betrodda tjänster om detta och ange orsakerna till förseningen samt när kontrollen beräknas vara slutförd.

4. En kvalificerad betrodd tjänst som har anmälts i enlighet med punkt 1 får inte avvisas för utförande av ett administrativt förfarande eller formalitet av det berörda offentliga organet av det skälet att den inte ingår i de förteckningar som avses i punkt 3.

5. Kommissionen får genom genomförandeakter fastställa förutsättningar, format och förfaranden för de ändamål som avses i punkterna 1 och 2. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Artikel 18

Förteckningar över betrodda tjänsteleverantörer

1. Varje medlemsstat ska upprätta, underhålla och offentliggöra en förteckning över betrodda tjänsteleverantörer, med uppgifter om kvalificerade tillhandahållare av betrodda tjänster inom medlemsstatens behörighetsområde tillsammans med uppgifter om de kvalificerade betrodda tjänster som dessa tillhandahåller.

2. Medlemsstaterna ska på ett säkert sätt upprätta, underhålla och offentliggöra elektroniskt undertecknade eller förseglade förteckningar över betrodda tjänsteleverantörer enligt punkt 1 i en form som lämpar sig för automatiserad behandling.

3. Medlemsstaterna ska utan onödigt dröjsmål till kommissionen lämna information om det organ som ansvarar för att upprätta, underhålla och offentliggöra nationella förteckningar över betrodda tjänsteleverantörer, samt närmare uppgifter om var dessa förteckningar offentliggörs, det certifikat som används för att underteckna eller försegla förteckningarna över betrodda tjänsteleverantörer och eventuella ändringar i dem.

4. Kommissionen ska se till att den information som avses i punkt 3 genom en säker kanal görs tillgänglig för allmänheten i elektroniskt undertecknad eller förseglad form som lämpar sig för automatiserad behandling.

5. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 38 rörande fastställandet av den information som avses i punkt 1.

6. Kommissionen får genom genomförandeakter fastställa de tekniska specifikationer och format som ska gälla för förteckningar över betrodda tjänsteleverantörer för de ändamål som avses i punkterna 1–4. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Krav på kvalificerade tillhandahållare av betrodda tjänster

1. En kvalificerad tillhandahållare av betrodda tjänster ska när den utfärdar ett kvalificerat certifikat, på lämpligt sätt och i enlighet med nationell lagstiftning, kontrollera identiteten och i förekommande fall eventuella särskilda egenskaper avseende den fysiska eller juridiska person till vilken ett kvalificerat certifikat utfärdas.

Denna information ska kontrolleras av den kvalificerade tillhandahållaren av betrodda tjänster eller av en auktoriserad tredje part som agerar under ansvar av den kvalificerade tillhandahållaren av betrodda tjänster på något av följande sätt:

- (a) Genom fysisk inställelse av den fysiska personen eller av ett behörigt ombud för den juridiska personen.
- (b) På avstånd med hjälp av medel för elektronisk identifiering som omfattas av ett anmält system utfärdat i enlighet med punkt a.

2. Kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade betrodda tjänster ska uppfylla följande krav:

- (a) De ska ha personal som har de sakkunskaper, erfarenheter och kvalifikationer som behövs, som tillämpar förfaranden för administration och förvaltning som överensstämmer med europeiska eller internationella standarder, samt har genomgått lämplig utbildning om regler för säkerhet och skydd för personuppgifter.
- (b) De ska bära risken för skadeståndsskyldighet genom att förfoga över tillräckliga ekonomiska medel eller genom ett lämpligt ansvarsförsäkringssystem.
- (c) Innan de ingår ett avtalsförhållande ska de informera de personer som vill använda en kvalificerad betrodd tjänst om de exakta villkor som gäller för användning av den tjänsten.
- (d) De ska använda tillförlitliga system och produkter som är skyddade mot ändringar och garantera den tekniska säkerheten och tillförlitligheten hos de förfaranden som stöds av dessa.
- (e) De ska använda tillförlitliga system för att lagra uppgifter som har lämnats till dem, i en form som kan kontrolleras så att
 - de är offentligt tillgängliga för hämtning endast i de fall där samtycke från den person till vilken uppgifterna har utfärdats har erhållits,
 - endast behöriga personer kan föra in uppgifter och göra ändringar, och
 - uppgifters äkthet kan kontrolleras.
- (f) De ska vidta åtgärder mot förfalskning och stöld av uppgifter.
- (g) De ska under en lämplig tidsperiod registrera all relevant information om uppgifter som den kvalificerade tillhandahållaren av betrodda tjänster utfärdat och tagit emot, särskilt för att vid rättsliga förfaranden kunna lägga fram bevis. Registreringen får göras elektroniskt.

(h) De ska ha en uppdaterad plan för verksamhetens upphörande i syftet att kunna garantera tjänstens kontinuitet i enlighet med den ordning som fastställts av tillsynsorganet enligt artikel 13.2 c.

(i) De ska säkerställa en rättsligt korrekt behandling av personuppgifter i enlighet med artikel 11.

3. Kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat ska i sin certifierade databas registrera återkallandet av ett certifikat inom tio minuter efter det att återkallandet har fått verkan.

4. Med hänvisning till punkt 3 ska kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat informera eventuella beroende parter om giltigheten eller statusen som återkallad hos de kvalificerade certifikat som de utfärdat. Informationen ska på ett automatiskt sätt som är tillförlitligt, kostnadsfritt och effektivt göras tillgänglig när som helst åtminstone på certifikatnivå.

5. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för tillförlitliga system och produkter. Överensstämmelse med kraven i artikel 19 ska förutsättas när tillförlitliga system och produkter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2. Kommissionen ska offentliggöra akterna i *Europeiska unionens officiella tidning*.

Avsnitt 3

Elektroniska signaturer

Artikel 20

Rättslig verkan och godtagande av elektroniska signaturer

1. En elektronisk signatur ska inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att signaturen är i elektronisk form.

2. En kvalificerad elektronisk signatur ska ha samma rättsliga verkan som en handskriven signatur.

3. Kvalificerade elektroniska signaturer ska erkännas och godtas i alla medlemsstater.

4. Om en elektronisk signatur med en lägre säkerhetsnivå än den som gäller för kvalificerade elektroniska signaturer krävs, särskilt av en medlemsstat för tillgång till en nättjänst som erbjuds av ett offentligt organ på grundval av en lämplig bedömning av riskerna med en sådan tjänst, ska alla elektroniska signaturer som motsvarar minst samma säkerhetsnivå erkännas och godtas.

5. Medlemsstaterna får inte kräva en elektronisk signatur med en högre säkerhetsnivå än den som gäller för kvalificerade elektroniska signaturer, för gränsöverskridande tillgång till en nättjänst som erbjuds av ett offentligt organ.

6. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 38 rörande fastställandet av de olika säkerhetsnivåer för elektroniska signaturer som avses i punkt 4.

7. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för säkerhetsnivån hos elektroniska signaturer. Överensstämmelse med den säkerhetsnivå som fastställs i en delegerad akt antagen enligt punkt 6 ska förutsättas när en elektronisk signatur uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2. Kommissionen ska offentliggöra akterna i Europeiska unionens officiella tidning.

Artikel 21

Kvalificerade certifikat för elektroniska signaturer

1. Kvalificerade certifikat för elektroniska signaturer ska uppfylla kraven i bilaga I.
2. Kvalificerade certifikat för elektroniska signaturer ska inte omfattas av några obligatoriska krav som går utöver kraven i bilaga I.
3. Om ett kvalificerat certifikat för en elektronisk signatur har återkallats efter den ursprungliga aktiveringen, ska det förlora sin giltighet och dess status som kvalificerat ska inte under några omständigheter återgå genom att dess giltighet förnyas.
4. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 38 rörande ytterligare specifikationer av de krav som anges i bilaga I.
5. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för elektroniska signaturer. Överensstämmelse med kraven i bilaga I ska förutsättas när ett kvalificerat certifikat för elektroniska signaturer uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2. Kommissionen ska offentliggöra akterna i *Europeiska unionens officiella tidning*.

Artikel 22

Krav på kvalificerade anordningar för skapande av elektroniska signaturer

1. Kvalificerade anordningar för skapande av elektroniska signaturer ska uppfylla kraven i bilaga II.
2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade anordningar för skapande av elektroniska signaturer. Överensstämmelse med kraven i bilaga II ska förutsättas när en kvalificerad anordning för skapande av elektroniska signaturer uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2. Kommissionen ska offentliggöra akterna i *Europeiska unionens officiella tidning*.

Artikel 23

Certifiering av kvalificerade anordningar för skapande av elektroniska signaturer

1. Kvalificerade anordningar för skapande av elektroniska signaturer får certifieras av lämpliga offentliga eller privata organ som utsetts av medlemsstaterna, förutsatt att de har genomgått ett förfarande för säkerhetsutvärdering som utförts i enlighet med någon av de standarder för säkerhetsbedömning av informationsteknikprodukter som finns med i en förteckning som kommissionen ska upprätta genom genomförandeakter. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2. Kommissionen ska offentliggöra akterna i *Europeiska unionens officiella tidning*.
2. Medlemsstaterna ska underrätta kommissionen och övriga medlemsstater om namnet på och adressen till det av dem utsedda offentliga eller privata organet som avses i punkt 1.
3. Kommissionen ska ha befogenhet att anta delegerade akter i enligt med artikel 38 rörande fastställandet av särskilda kriterier som ska uppfyllas av de utsedda organ som avses i punkt 1.

Artikel 24

Offentliggörande av en förteckning över certifierade kvalificerade anordningar för skapande av elektroniska signaturer

1. Medlemsstaterna ska utan onödigt dröjsmål till kommissionen lämna information om kvalificerade anordningar för skapande av elektroniska signaturer som har certifierats av de organ som avses i artikel 23. De ska utan onödigt dröjsmål även informera kommissionen om anordningar för skapande av elektroniska signaturer som inte längre är certifierade.
2. Kommissionen ska på grundval av den information som inkommit upprätta, offentliggöra och underhålla en förteckning över certifierade kvalificerade anordningar för skapande av elektroniska signaturer.
3. Kommissionen får genom genomförandeakter fastställa förutsättningar, format och förfaranden som ska vara tillämpliga för de ändamål som avses i punkt 1. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Artikel 25

Krav på validering av kvalificerade elektroniska signaturer

1. En kvalificerad elektronisk signatur ska anses vara giltig om det med en hög grad av säkerhet kan fastställas att följande krav är uppfyllda vid tidpunkten för undertecknandet:
 - (a) Certifikatet som stöder signaturen ska vara ett kvalificerat certifikat för elektroniska signaturer som uppfyller kraven i bilaga I.
 - (b) Det kvalificerade certifikatet ska vara äkta och giltigt.

- (c) Valideringsuppgifterna för signaturen ska överensstämma med de uppgifter som lämnats till den beroende parten.
- (d) Den uppsättning uppgifter som otvetydigt företräder undertecknaren ska på rätt sätt ha tillhandahållits den beroende parten.
- (e) Användningen av en eventuell pseudonym ska tydligt ha angetts för den beroende parten om en pseudonym används.
- (f) Den elektroniska signaturen ska ha skapats med en kvalificerad anordning för skapande av elektroniska signaturer.
- (g) Integriteten hos de undertecknade uppgifterna ska inte ha äventyrats.
- (h) Kraven i artikel 3.7 ska vara uppfyllda.
- (i) Det system som används för att validera signaturen ska ge den beroende parten det korrekta resultatet av valideringsförfarandet och göra det möjligt för den beroende parten att upptäcka eventuella problem som är relevanta för säkerheten.

2. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 38 rörande ytterligare specifikationer av de krav som anges i punkt 1.

3. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för validering av kvalificerade elektroniska signaturer. Överensstämmelse med kraven i punkt 1 ska förutsättas när valideringen av kvalificerade elektroniska signaturer uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2. Kommissionen ska offentliggöra akterna i *Europeiska unionens officiella tidning*.

Artikel 26

Kvalificerad valideringstjänst för kvalificerade elektroniska signaturer

1. En kvalificerad valideringstjänst för kvalificerade elektroniska signaturer ska tillhandahållas av en kvalificerad tillhandahållare som

- (a) tillhandahåller validering i enlighet med artikel 25.1, och
- (b) gör det möjligt för betrodda parter att erhålla resultaten av valideringsförfarandet på ett automatiskt sätt som är tillförlitligt, effektivt och försett med en avancerad elektronisk signatur eller ett avancerat elektroniskt sigill från tillhandahållaren av den kvalificerade valideringstjänsten.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för den kvalificerade valideringstjänst som avses i punkt 1. Överensstämmelse med kraven i punkt 1 b ska förutsättas när valideringstjänsten för en kvalificerad elektronisk signatur uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2. Kommissionen ska offentliggöra akterna i *Europeiska unionens officiella tidning*.

Artikel 27

Bevarande av kvalificerade elektroniska signaturer

1. En kvalificerad tjänst för bevarande av elektroniska signaturer ska tillhandahållas av en kvalificerad tillhandahållare av betrodda tjänster som använder förfaranden och tekniker som gör det möjligt att utöka tillförlitligheten hos valideringsuppgifterna för kvalificerade elektroniska signaturer bortom tidpunkten för deras tekniska giltighet.
2. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 38 rörande ytterligare specifikationer av de krav som anges i punkt 1.
3. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för bevarande av kvalificerade elektroniska signaturer. Överensstämmelse med kraven i punkt 1 ska förutsättas när systemen för bevarandet av kvalificerade elektroniska signaturer uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2. Kommissionen ska offentliggöra akterna i *Europeiska unionens officiella tidning*.

Avsnitt 4

Elektroniska sigill

Artikel 28

Rättslig verkan av elektroniska sigill

1. Ett elektroniskt sigill ska inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att sigillet är i elektronisk form.
2. Ett kvalificerat elektroniskt sigill ska omfattas av en rättslig presumtion som garanterar ursprunget och integriteten hos de uppgifter som det är kopplat till.
3. Ett kvalificerat elektroniskt sigill ska erkännas och godtas i alla medlemsstater.
4. Om ett elektroniskt sigill med en lägre säkerhetsnivå än den som gäller för kvalificerade elektroniska sigill krävs, särskilt av en medlemsstat för tillgång till en nättjänst som erbjuds av ett offentligt organ på grundval av en lämplig bedömning av riskerna med en sådan tjänst, ska alla elektroniska sigill som motsvarar minst samma säkerhetsnivå erkännas och godtas.
5. Medlemsstaterna ska för tillgång till en tjänst online som tillhandahålls av ett organ i den offentliga förvaltningen inte kräva ett elektroniskt sigill med en högre säkerhetsnivå än den som gäller för kvalificerade elektroniska sigill.
6. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 38 rörande fastställandet av de olika säkerhetsnivåer för elektroniska sigill som avses i punkt 4.
7. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för säkerhetsnivån hos elektroniska sigill. Överensstämmelse med den säkerhetsnivå som fastställs i en delegerad akt antagen enligt punkt 6 ska förutsättas när ett elektroniskt sigill uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det

granskningsförfarande som avses i artikel 39.2. Kommissionen ska offentliggöra akterna i *Europeiska unionens officiella tidning*.

Artikel 29

Krav på kvalificerade certifikat för elektroniska sigill

1. Kvalificerade certifikat för elektroniska sigill ska uppfylla kraven i bilaga III.
2. Kvalificerade certifikat för elektroniska sigill ska inte omfattas av några obligatoriska krav som går utöver kraven i bilaga III.
3. Om ett kvalificerat certifikat för ett elektroniskt sigill har återkallats efter den ursprungliga aktiveringen ska det förlora sin giltighet och dess status som kvalificerat ska inte under några omständigheter återgå genom att dess giltighet förnyas.
4. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 38 rörande ytterligare specifikationer av de krav som anges i bilaga III.
5. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för elektroniska sigill. Överensstämmelse med kraven i bilaga III ska förutsättas när ett kvalificerat certifikat för elektroniska sigill uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2. Kommissionen ska offentliggöra akterna i *Europeiska unionens officiella tidning*.

Artikel 30

Kvalificerade anordningar för skapande av elektroniska sigill

1. Artikel 22 ska även gälla för kraven på kvalificerade anordningar för skapande av elektroniska sigill.
2. Artikel 23 ska även gälla för certifieringen av kvalificerade anordningar för skapande av elektroniska sigill.
3. Artikel 24 ska även gälla för offentliggörandet av en förteckning över certifierade kvalificerade anordningar för skapande av elektroniska sigill.

Artikel 31

Validering och bevarande av kvalificerade elektroniska sigill

Artiklarna 25, 26 och 27 ska även gälla för validering och bevarande av kvalificerade elektroniska sigill.

Avsnitt 5

Elektronisk tidsmärkning

Artikel 32

Rättslig verkan av elektroniska tidsmärknings

1. En elektronisk tidsmärkning ska inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att tidsmärkningen är i elektronisk form.
2. En kvalificerad elektronisk tidsmärkning ska omfattas av en rättslig presumtion som garanterar den tid som den anger och integriteten hos de uppgifter som tiden är kopplad till.
3. En kvalificerad elektronisk tidsmärkning ska erkännas och godtas i alla medlemsstater.

Artikel 33

Krav på kvalificerade elektroniska tidsmärknings

1. En kvalificerad elektronisk tidsmärkning ska uppfylla följande krav:
 - (a) Den ska vara korrekt kopplad till samordnad universaltid (UTC) så att det utesluter varje möjlighet till att uppgifterna ändras utan att det går att upptäcka.
 - (b) Den ska vara grundad på en korrekt tidskälla.
 - (c) Den ska vara utfärdad av en kvalificerad tillhandahållare av betrodda tjänster.
 - (d) Den ska vara undertecknad med hjälp av en avancerad elektronisk signatur eller ett avancerat elektroniskt sigill från den kvalificerade tillhandahållaren av betrodda tjänster eller genom en likvärdig metod.
2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för korrekt koppling av tidpunkt till uppgifter och korrekt tidskälla. Överensstämmelse med kraven i punkt 1 ska förutsättas när en korrekt koppling av tidpunkt till uppgifter och en korrekt tidskälla uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2. Kommissionen ska offentliggöra akterna i *Europeiska unionens officiella tidning*.

Avsnitt 6

Elektroniska dokument

Artikel 34

Rättslig verkan och godtagande av elektroniska dokument

1. Ett elektroniskt dokument ska anses vara likvärdigt med ett pappersdokument och vara giltigt som bevis vid rättsliga förfaranden med avseende på dess säkerhetsnivå i fråga om äkthet och integritet.
2. Ett dokument försett med en kvalificerad elektronisk signatur eller ett kvalificerat elektroniskt sigill från den person som har behörighet att utfärda dokumentet i fråga ska omfattas av en rättslig presumtion om dess äkthet och integritet, förutsatt att dokumentet inte innehåller några dynamiska egenskaper som automatiskt kan förändra dokumentet.
3. När ett originaldokument eller en bestyrkt kopia krävs för tillhandahållandet av en tjänst online av ett organ i den offentliga förvaltningen ska åtminstone elektroniska dokument som

utfärdats av personer med behörighet att utfärda dokumenten i fråga och som anses utgöra original eller bestyrkta kopior i enlighet med ursprungsmedlemsstatens nationella lagstiftning godtas i övriga medlemsstater utan ytterligare krav.

4. Kommissionen får genom genomförandeakter fastställa format för elektroniska signaturer och sigill som alltid ska godtas när ett signerat eller förseglat dokument krävs av en medlemsstat för tillhandahållandet av en tjänst online av ett organ i den offentliga förvaltningen enligt punkt 2. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Avsnitt 7

Kvalificerad elektronisk leveranstjänst

Artikel 35

Rättslig verkan av en elektronisk leveranstjänst

1. Uppgifter som sänds eller tas emot med hjälp av en elektronisk leveranstjänst ska kunna godtas som bevis vid rättsliga förfaranden med avseende på uppgifternas integritet och vissheten om det datum och den tidpunkt då uppgifterna sändes eller togs emot av en särskilt angiven adressat.

2. Uppgifter som sänds eller tas emot med hjälp av en elektronisk leveranstjänst ska omfattas av en rättslig presumtion om uppgifternas integritet samt om riktigheten i det datum och den tidpunkt för sändning eller mottagande av uppgifterna som anges av den kvalificerade elektroniska leveranstjänsten.

3. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 38 rörande fastställandet av mekanismer för att sända eller ta emot uppgifter med hjälp av elektroniska leveranstjänster, vilka ska användas med sikte på att främja interoperabilitet mellan elektroniska leveranstjänster.

Artikel 36

Krav på kvalificerade elektroniska leveranstjänster

1. Kvalificerade elektroniska leveranstjänster ska uppfylla följande krav:

- (a) De ska tillhandahållas av en eller flera kvalificerade tillhandahållare av betrodda tjänster.
- (b) De ska utformas så att man otvetydigt kan identifiera avsändaren och i tillämpliga fall adressaten.
- (c) Processen för att sända och ta emot uppgifter måste säkras genom en avancerad elektronisk signatur eller ett avancerat elektroniskt sigill från en kvalificerad tillhandahållare av betrodda tjänster på ett sätt som utesluter varje möjlighet till att uppgifterna ändras utan att det går att upptäcka.
- (d) Eventuella ändringar av de uppgifter som behövs för att sända eller ta emot uppgifterna måste tydligt anges för uppgifternas avsändare och adressat.

- (e) Datumet för sändning, mottagande och eventuella ändringar av uppgifter måste anges genom en kvalificerad elektronisk tidsmärkning.
- (f) Om uppgifterna överförs mellan två eller flera kvalificerade tillhandahållare av betrodda tjänster ska kraven i punkterna a till e gälla för alla kvalificerade tillhandahållare av betrodda tjänster.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för processer för att sända och ta emot uppgifter. Överensstämmelse med kraven i punkt 1 ska förutsättas när en process för att sända och ta emot uppgifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2. Kommissionen ska offentliggöra akterna i *Europeiska unionens officiella tidning*.

Avsnitt 8

Autentisering av webbplatser

Artikel 37

Krav på kvalificerade certifikat för autentisering av webbplatser

1. Kvalificerade certifikat för autentisering av webbplatser ska uppfylla kraven i bilaga IV.
2. Kvalificerade certifikat för autentisering av webbplatser ska erkännas och godtas i alla medlemsstater.
3. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 38 rörande ytterligare specifikationer av de krav som anges i bilaga IV.
4. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för autentisering av webbplatser. Överensstämmelse med kraven i bilaga IV ska förutsättas när ett kvalificerat certifikat för autentisering av webbplatser uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2. Kommissionen ska offentliggöra akterna i *Europeiska unionens officiella tidning*.

KAPITEL IV

DELEGERADE AKTER

Artikel 38

Utövande av delegering

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.
2. Befogenhet att anta de delegerade akter som avses i artiklarna 8.3, 13.5, 15.5, 16.5, 18.5, 20.6, 21.4, 23.3, 25.2, 27.2, 28.6, 29.4, 30.2, 31, 35.3 och 37.3 ska ges till kommissionen för en obegränsad tidsperiod från och med ikraftträdandet av denna förordning.

3. Den delegering av befogenhet som avses i artiklarna 8.3, 13.5, 15.5, 16.5, 18.5, 20.6, 21.4, 23.3, 25.2, 27.2, 28.6, 29.4, 30.2, 31, 35.3 och 37.3 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallande ska avsluta delegeringen av de befogenheter som anges i beslutet. Beslutet ska få verkan dagen efter det att beslutet har offentliggjorts i Europeiska unionens officiella tidning eller vid ett senare angivet datum. Det ska inte påverka giltigheten av delegerade akter som redan trätt i kraft.

4. När kommissionen antar en delegerad akt ska den samtidigt underrätta Europaparlamentet och rådet.

5. En delegerad akt som antas i enlighet med artiklarna 8.3, 13.5, 15.5, 16.5, 18.5, 20.6, 21.4, 23.3, 25.2, 27.2, 28.6, 29.4, 30.2, 31, 35.3 och 37.3 ska endast träda i kraft om varken Europaparlamentet eller rådet har motsatt sig detta inom två månader från det datum då akten delgetts Europaparlamentet och rådet, eller om både Europaparlamentet och rådet före utgången av denna period har informerat kommissionen om att de inte kommer att motsätta sig detta. Den tidsfristen ska på Europaparlamentets eller rådets initiativ förlängas med två månader.

KAPITEL V

GENOMFÖRANDEAKTER

Artikel 39

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Kommittén ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

KAPITEL VI

SLUTBESTÄMMELSER

Artikel 40

Rapport

Kommissionen ska rapportera till Europaparlamentet och rådet om tillämpningen av den här förordningen. Den första rapporten ska överlämnas senast fyra år efter det att denna förordning träder i kraft. Därefter ska rapporter överlämnas vart fjärde år.

Artikel 41

Upphävande

1. Direktiv 1999/93/EG ska upphöra att gälla.

2. Hänvisningar till det upphävda direktivet ska anses som hänvisningar till den här förordningen.

3. Säkra anordningar för skapande av signaturer vilkas överensstämmelse har fastställts i enlighet med artikel 3.4 i direktiv 1999/93/EG ska anses som kvalificerade anordningar för skapande av elektroniska signaturer enligt denna förordning.

4. Kvalificerade certifikat som utfärdats enligt direktiv 1999/93/EG ska anses som kvalificerade certifikat för elektroniska signaturer enligt denna förordning till dess att de löper ut, men högst fem år från denna förordnings ikraftträdande.

Artikel 42

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den

På Europaparlamentets vägnar
Ordförande

På rådets vägnar
Ordförande

BILAGA I

Krav på kvalificerade certifikat för elektroniska signaturer

Kvalificerade certifikat för elektroniska signaturer ska innehålla följande:

- (a) En uppgift i en form som åtminstone lämpar sig för automatiserad behandling om att certifikatet har utfärdats som ett kvalificerat certifikat för elektroniska signaturer.
- (b) En uppsättning uppgifter som otvetydigt företräder den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, inklusive minst uppgift om den medlemsstat i vilken tillhandahållaren är etablerad och
 - för en juridisk person: namn och registreringsnummer i enlighet med vad som uppgetts i de officiella handlingarna,
 - för en fysisk person: personens namn.
- (c) En uppsättning uppgifter som otvetydigt företräder den undertecknare till vilken certifikatet utfärdas, inklusive minst undertecknarens namn eller en pseudonym med uppgift om att det rör sig om en pseudonym.
- (d) Valideringsuppgifter för elektroniska signaturer som motsvarar uppgifterna för skapande av elektroniska signaturer.
- (e) Detaljerade uppgifter om giltighetstidens början och slut för certifikatet.
- (f) Certifikatets identifieringskod, som måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster.
- (g) Den avancerade elektroniska signaturen eller det avancerade elektroniska sigillet för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikatet.
- (h) Uppgift om var det certifikat som stödjer den avancerade elektroniska signatur eller det avancerade elektroniska sigill som avses i punkt g är tillgängligt kostnadsfritt.
- (i) Uppgift om var de tjänster för certifikats giltighet som kan användas för att göra förfrågningar angående det kvalificerade certifikatets giltighet är lokaliserade.
- (j) Om de uppgifter för skapande av elektroniska signaturer som avser valideringsuppgifterna för elektroniska signaturer är placerade i en kvalificerad anordning för skapande av elektroniska signaturer, en lämplig uppgift som anger detta i en form som åtminstone lämpar sig för automatiserad behandling.

BILAGA II

Krav på kvalificerade anordningar för skapande av elektroniska signaturer

1. Kvalificerade anordningar för skapande av elektroniska signaturer ska genom lämpliga tekniker och förfaranden säkerställa att åtminstone

- (a) sekretessen för de uppgifter för skapande av elektroniska signaturer som används för att generera elektroniska signaturer är säkerställd,
- (b) de uppgifter för skapande av elektroniska signaturer som används för att generera elektroniska signaturer endast kan förekomma en gång,
- (c) de uppgifter för skapande av elektroniska signaturer som används för att generera elektroniska signaturer inte med rimlig garanti kan härledas och att den elektroniska signaturen är skyddad mot förfälskning med den teknik som för närvarande finns tillgänglig,
- (d) de uppgifter skapande av elektroniska signaturer som används för att generera elektroniska signaturer kan skyddas på ett tillförlitligt sätt av den legitime undertecknaren så att andra inte kan använda dem.

2. Kvalificerade anordningar för skapande av elektroniska signaturer får inte förändra de uppgifter som ska undertecknas eller hindra att dessa uppgifter presenteras för undertecknaren före undertecknandet.

3. Generering eller hantering av uppgifter för skapande av elektroniska signaturer för undertecknarens räkning ska utföras av en kvalificerad tillhandahållare av betrodda tjänster.

4. Kvalificerade tillhandahållare av betrodda tjänster som för undertecknarens räkning hanterar uppgifter för skapande av elektroniska signaturer får kopiera dessa uppgifter för framställning av säkerhetskopior, förutsatt att följande krav uppfylls:

- (a) Säkerhetsnivån för de kopierade uppsättningarna av uppgifter måste vara densamma som för de ursprungliga uppsättningarna av uppgifter.
- (b) Antalet kopierade uppsättningar av uppgifter får inte överskrida det minimum som behövs för att garantera tjänstens kontinuitet.

BILAGA III

Krav på kvalificerade certifikat för elektroniska sigill

Kvalificerade certifikat för elektroniska sigill ska innehålla följande:

- (a) En uppgift i en form som åtminstone lämpar sig för automatiserad behandling om att certifikatet har utfärdats som ett kvalificerat certifikat för elektroniska sigill.
- (b) En uppsättning uppgifter som otvetydigt företräder den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, inklusive minst uppgift om den medlemsstat i vilken tillhandahållaren är etablerad och
 - för en juridisk person: namn och registreringsnummer i enlighet med vad som uppgetts i de officiella handlingarna,
 - för en fysisk person: personens namn.
- (c) En uppsättning uppgifter som otvetydigt företräder den juridiska person till vilken certifikatet utfärdas, inklusive minst namn och registreringsnummer i enlighet med vad som uppgetts i de officiella handlingarna.
- (d) Valideringsuppgifter för elektroniska sigill som motsvarar uppgifterna för skapande av elektroniska sigill.
- (e) Detaljerade uppgifter om giltighetstidens början och slut för certifikatet.
- (f) Certifikatets identifieringskod, som måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster.
- (g) Den avancerade elektroniska signaturen eller det avancerade elektroniska sigillet för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikatet.
- (h) Uppgift om var det certifikat som stödjer den avancerade elektroniska signatur eller det avancerade elektroniska sigill som avses i punkt g är tillgängligt kostnadsfritt.
- (i) Uppgift om var de tjänster för certifikats giltighet som kan användas för att göra förfrågningar angående det kvalificerade certifikatets giltighet är lokaliserade.
- (j) Om de uppgifter för skapande av elektroniska sigill är placerade i en kvalificerad anordning för skapande av elektroniska sigill, en lämplig uppgift som anger detta i en form som åtminstone lämpar sig för automatiserad behandling.

BILAGA IV

Krav på kvalificerade certifikat för autentisering av webbplatser

Kvalificerade certifikat för autentisering av webbplatser ska innehålla följande:

- (a) En uppgift i en form som åtminstone lämpar sig för automatiserad behandling om att certifikatet har utfärdats som ett kvalificerat certifikat för autentisering av webbplatser.
- (b) En uppsättning uppgifter som otvetydigt företräder den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, inklusive minst uppgift om den medlemsstat i vilken tillhandahållaren är etablerad och
 - för en juridisk person: namn och registreringsnummer i enlighet med vad som uppgetts i de officiella handlingarna,
 - för en fysisk person: personens namn.
- (c) En uppsättning uppgifter som otvetydigt företräder den juridiska person till vilken certifikatet utfärdas, inklusive minst namn och registreringsnummer i enlighet med vad som uppgetts i de officiella handlingarna.
- (d) Adressuppgifter, inklusive minst stad och medlemsstat, för den juridiska person till vilken certifikatet utfärdas i enlighet med vad som uppgetts i de officiella handlingarna.
- (e) Det eller de domännamn som drivs av den juridiska person till vilken certifikatet utfärdas.
- (f) Detaljerade uppgifter om giltighetstidens början och slut för certifikatet.
- (g) Certifikatets identifieringskod, som måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster.
- (h) Den avancerade elektroniska signaturen eller det avancerade elektroniska sigillet för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikatet.
- (i) Uppgift om var det certifikat som stödjer den avancerade elektroniska signatur eller det avancerade elektroniska sigill som avses i punkt h är tillgängligt kostnadsfritt.
- (j) Uppgift om var de tjänster för certifikats giltighet som kan användas för att göra förfrågningar angående det kvalificerade certifikatets giltighet är lokaliserade.

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

I denna finansieringsöversikt redogörs närmare för de behov räknat i administrativa utgifter som genomförandet av den föreslagna förordningen om *elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden* kommer att medföra.

Efter lagstiftningsförfarandet och diskussionen för Europaparlamentets och rådets antagande av den föreslagna förordningen kommer kommissionen att behöva tolv heltidsekvivalenter för att planera de tillhörande delegerade akterna och genomförandeakterna, se till att organisatoriska och tekniska förfaranden är tillgängliga, hantera den information som inkommer från medlemsstaterna, särskilt för att underhålla den information som avser förteckningar över kvalificerad status, se till att berörda parter – särskilt medborgare samt små och medelstora företag – är medvetna om fördelarna med att använda e-identifiering, e-autentisering, e-signaturer och närliggande betrodda tjänster, samt för att inleda diskussioner med tredjeländer med sikte på att uppnå interoperabilitet för e-identifiering, e-autentisering, e-signaturer och närliggande betrodda tjänster på global nivå.

1.1. Förslagets eller initiativets beteckning

| |
|--|
| Kommissionens förslag till förordning om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden |
|--|

1.2. Berörda politikområden i den verksamhetsbaserade förvaltningen och budgeteringen²⁵

| |
|---------------------------------|
| 09 INFORMATIONSSAMHÄLLET |
|---------------------------------|

1.3. Typ av förslag eller initiativ

- Ny åtgärd
- Ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd²⁶
- Befintlig åtgärd vars genomförande förlängs i tiden
- Tidigare åtgärd som omformas till eller ersätts av en ny

²⁵ Verksamhetsbaserad förvaltning och verksamhetsbaserad budgetering benämns ibland med de interna förkortningarna ABM respektive ABB.

²⁶ I den mening som avses i artikel 49.6 a respektive 49.6 b i budgetförordningen.

1.4. Mål

1.4.1. *Fleråriga strategiska mål för kommissionen som förslaget eller initiativet är avsett att bidra till*

De allmänna målen för förslaget är de mål inom den allmänna EU-politiken som det omfattas av, som t.ex. Europa 2020-strategin. Strategin syftar till att se till att Europa omvandlas till "en smart och hållbar för alla, med hög sysselsättning, produktivitet och social sammanhållning".

1.4.2. *Specifika mål eller verksamheter inom den verksamhetsbaserade förvaltningen och budgeteringen som berörs*

Att öka förtroendet för EU-täckande elektroniska transaktioner och att säkra gränsöverskridande rättsligt erkännande av e-identifiering, e-autentisering, e-signaturer och närliggande betrodda tjänster samt en hög nivå av dataskydd och av egenmakt för användare på den inre marknaden (se En digital agenda för Europa, nyckelåtgärderna 3 och 16).

Berörda verksamheter enligt den verksamhetsbaserade förvaltningen och budgeteringen

09 02 – Regelverk för En digital agenda för Europa

1.4.3. *Verkan eller resultat som förväntas*

Beskriv den verkan som förslaget eller initiativet förväntas få på de mottagare eller den del av befolkningen som berörs.

Genom att fastställa ett tydligt regelverk för e-identifiering, e-autentisering, e-signaturer och närliggande betrodda tjänster kan användarna få ökad tillgång till och ett ökat förtroende för den digitala världen.

1.4.4. *Indikatorer för bedömning av resultat eller verkan*

Ange vilka indikatorer som ska användas för att följa upp hur förslaget eller initiativet genomförs.

1. Förekomsten av tillhandahållare av e-identifiering, e-autentisering, e-signaturer och närliggande betrodda tjänster som bedriver verksamhet i flera av EU:s medlemsstater.
2. Graden av interoperabilitet för anordningar (t.ex. smartkortläsare) mellan olika sektorer och länder.
3. Användningen av e-identifiering, e-autentisering, e-signaturer och närliggande betrodda tjänster i alla befolkningskategorier.
4. Omfattningen av slutanvändares användning av e-identifiering, e-autentisering, e-signaturer och närliggande betrodda tjänster för nationella transaktioner och internationella (gränsöverskridande) transaktioner.
5. Graden av harmonisering mellan medlemsstaterna när det gäller lagstiftning om e-identifiering, e-autentisering, e-signaturer och närliggande betrodda tjänster.
6. System för elektronisk identifiering som anmälts till kommissionen.

7. Tjänster som är tillgängliga med anmälda medel för elektronisk identifiering inom den offentliga sektorn (t.ex. e-förvaltning, e-hälsa, e-juridik och e-upphandling).
8. Tjänster som är tillgängliga med anmälda medel för elektronisk identifiering inom den privata sektorn (t.ex. e-bankverksamhet, e-handel, e-spel, inloggning till webbplatser och säkra internetjänster).

1.5. Motivering till förslaget eller initiativet

1.5.1. *Behov som ska tillgodoses på kort eller lång sikt*

De skiljaktiga nationella genomförandena av direktivet om elektroniska signaturer, som beror på att medlemsstaterna har tolkat direktivet på olika sätt, leder till problem med den gränsöverskridande interoperabiliteten och därmed till ett splittrat EU-landskap och snedvridningar på den inre marknaden. Detta åtföljs av en brist på förtroende för elektroniska system som hindrar EU:s medborgare från att dra nytta av samma typ av tjänster i den digitala världen som i den fysiska världen.

1.5.2. *Mervärdet av en åtgärd på unionsnivå*

En åtgärd på EU-nivå skulle ge tydliga fördelar jämfört med en åtgärd på medlemsstatsnivå. Tidigare erfarenheter har tydligt visat att nationella åtgärder inte bara är otillräckliga för att göra elektroniska transaktioner möjliga över gränserna, utan de har tvärtom skapat hinder för EU-täckande interoperabilitet för elektroniska signaturer och att de för närvarande har samma inverkan på elektronisk identifiering och autentisering och närliggande betrodda tjänster.

1.5.3. *Huvudsakliga erfarenheter från liknande försök eller åtgärder*

Förslaget bygger på erfarenheterna från direktivet om e-signaturer och problemet med fragmentering vid införlivandet och genomförandet av direktivet. Detta problem har lett till att det inte har gått att uppfylla direktivs mål.

1.5.4. *Förenlighet med andra finansieringsformer och eventuella synergieffekter*

Direktivet om elektroniska signaturer nämns i flera andra EU-initiativ som har inrättats för att undanröja interoperabilitetsproblem samt problem med gränsöverskridande erkännande och godtagande som avser vissa typer av elektroniska utbyten, t.ex. tjänstedirektivet, direktiven om offentlig upphandling, det reviderade momsdirektivet (e-fakturerings) och förordningen om det europeiska medborgarinitiativet.

Den föreslagna förordningen kommer dessutom att ge ett regelverk som främjar en bred användning av de storskaliga pilotprojekt som har inrättats på EU-nivå för att stödja utvecklingen av interoperabla och tillförlitliga medel för elektronisk kommunikation (inbegripet enkla onlinieförfaranden för gränsöverskridande tjänster som stödjer genomförandet av tjänstedirektivet, det storskaliga pilotprojektet (STORK) som stödjer utvecklingen och användningen av interoperabla e-identifieringar, det storskaliga pilotprojektet för gränsöverskridande offentlig upphandling (Peppol) som stödjer utvecklingen och användningen av interoperabla e-upphandlingslösningar, det storskaliga pilotprojektet epSOS som stödjer

utvecklingen och användningen av interoperabla e-hälsalösningar samt eCodex som stödjer utvecklingen och användningen av interoperabla e-juridiklösningar.

1.6. Tid under vilken åtgärden kommer att pågå respektive påverka resursanvändningen

Förslag eller initiativ som pågår under **begränsad tid**

– Förslaget eller initiativet ska gälla från [den DD/MM]ÅÅÅÅ till [den DD/MM]ÅÅÅÅ

– Det påverkar resursanvändningen från ÅÅÅÅ till ÅÅÅÅ

Förslag eller initiativ som pågår under en **obegränsad tid**

1.7. Planerad metod för genomförandet²⁷

Direkt centraliserad förvaltning som sköts av kommissionen

Indirekt centraliserad förvaltning genom delegering till

– genomförandeorgan

– byråer/organ som inrättats av gemenskaperna²⁸

– nationella offentligrättsliga organ eller organ som anförtrotts uppgifter som faller inom offentlig förvaltning

– personer som anförtrotts ansvaret för genomförandet av särskilda åtgärder som följer av avdelning V i fördraget om Europeiska unionen och som anges i den grundläggande rättsakten i den mening som avses i artikel 49 i budgetförordningen

Delad förvaltning med medlemsstaterna

Decentraliserad förvaltning med tredjeländer

Gemensam förvaltning med internationella organisationer (*ange vilka*)

Vid fler än en metod, ange kompletterande uppgifter under "Anmärkningar".

Anmärkningar

[//]

²⁷ Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

²⁸ Organ som avses i artikel 185 i budgetförordningen.

2. FÖRVALTNING

2.1. Bestämmelser om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder.

Den första utvärderingen ska göras inom fyra år efter det att förordningen trätt i kraft. Förordningen innehåller uttryckliga bestämmelser om rapportering, enligt vilka kommissionen ska avlägga rapport till Europaparlamentet och rådet om dess tillämpning. Därefter ska rapporter överlämnas vart fjärde år. Kommissionen kommer att använda den utvärderingsmetod som den själv har utformat, och arbetet kommer att genomföras med hjälp av riktade studier av hur lagstiftningsakterna har genomförts, enkäter bland nationella myndigheter, expertdiskussioner, workshoppar, Eurobarometer-undersökningar m.m.

2.2. Administrations- och kontrollsystem

2.2.1. Risker som identifierats

En konsekvensbedömning har utförts, vilken åtföljer förslaget till förordning. Den nya lagstiftningsakten kommer att tillgodose behovet av ömsesidigt gränsöverskridande erkännande och godtagande av elektronisk identifiering, förbättra den nuvarande rättsliga ramen för elektroniska signaturer, stärka den nationella tillsynen av tillhandahållare av betrodda tjänster och ge rättslig verkan och erkännande för närliggande betrodda tjänster. Genom förordningen införs även användningen av delegerade akter och genomförandeakter som en mekanism för att säkerställa flexibilitet i förhållande till den tekniska utvecklingen.

2.2.2. Planerade kontrollmetoder

De befintliga kontrollmetoder som kommissionen tillämpar kommer att kunna användas även för de ytterligare anslagen.

2.3. Åtgärder för att förebygga bedrägeri och oegentligheter/oriktigheter

Beskriv förebyggande åtgärder (befintliga eller planerade).

De befintliga metoder för bedrägeriförebyggande som kommissionen tillämpar kommer att kunna användas även för de ytterligare anslagen.

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

- Befintliga budgetrubriker (även kallade ”budgetposter”)

Redovisa de berörda rubrikerna i budgetramen i nummerföljd och – inom varje sådan rubrik – de berörda budgetrubrikerna i den årliga budgeten i nummerföljd.

| Rubrik i den fleråriga budgetramen | Budgetrubrik i den årliga budgeten | Typ av anslag | Bidrag | | | |
|------------------------------------|--|----------------------------------|-------------------------------|-----------------------------------|--------------------|---|
| | Nummer [Beteckning.....] | Diff./Icke-diff. ⁽²⁹⁾ | från Eftaländer ³⁰ | från kandidatländer ³¹ | från tredje-länder | enligt artikel 18.1 aa i budgetförordningen |
| 5 | 09. 01 01 01 Utgifter för personal i aktiv tjänst inom GD Informationssamhället och media | Icke-diff. | NEJ | NEJ | NEJ | NEJ |
| 5 | 09. 01 02 01 Extern personal | Icke-diff. | NEJ | NEJ | NEJ | NEJ |

²⁹ Differentierade respektive icke-differentierade anslag.

³⁰ Efta: Europeiska frihandelssammanslutningen.

³¹ Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

3.2. Beräknad inverkan på utgifterna

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna

| | | |
|---|--------|---|
| Rubrik i den fleråriga budgetramen | Nummer | [Beteckning: Smart tillväxt för alla] |
|---|--------|---|

| GD: INFSO | | | År 2014 | År 2015 | År 2016 | År 2017 | År 2018 | År 2019 | År 2020 | TOTALT |
|---|-------------|-------------|------------|------------|------------|------------|------------|------------|------------|--------------|
| • Driftsanslag | | | | | | | | | | |
| Budgetrubrik (nr) | Åtaganden | (1) | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 |
| | Betalningar | (2) | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 |
| Budgetrubrik (nr) | Åtaganden | (1a) | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 |
| | Betalningar | (2a) | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 |
| Administrativa anslag som finansieras genom ramanslagen för vissa operativa program ³² | | | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 |
| Budgetrubrik (nr) | | (3) | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 |
| TOTALA anslag för GD INFSO | Åtaganden | =1+1a +3 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 |
| | Betalningar | =2+2a +3 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 | 0,000 |

| | | |
|---|----------|---------------------------|
| Rubrik i den fleråriga budgetramen | 5 | ”Administrativa utgifter” |
|---|----------|---------------------------|

Miljoner euro (avrundat till tre decimaler)

³²

Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

| | | År 2014 | År 2015 | År 2016 | År 2017 | År 2018 | År 2019 | År 2020 | TOTALT |
|----------------------------------|--------|------------|------------|------------|------------|------------|------------|------------|--------|
| GD: INFSO | | | | | | | | | |
| • Personalresurser | | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 9 408 |
| • Övriga administrativa utgifter | | | | | | | | | |
| TOTALT GD INFSO | Anslag | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 9 408 |

| | | | | | | | | | |
|--|--|-------|-------|-------|-------|-------|-------|-------|-------|
| TOTALA anslag för RUBRIK 5 i den fleråriga budgetramen | (summa åtaganden = summa betalningar) | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 9 408 |
|--|--|-------|-------|-------|-------|-------|-------|-------|-------|

Miljoner euro (avrundat till tre decimaler)

| | | År 2014 | År 2015 | År 2016 | År 2017 | År 2018 | År 2019 | År 2020 | TOTALT |
|--|-------------|------------|------------|------------|------------|------------|------------|------------|--------|
| TOTALA anslag för RUBRIK 1-5 i den fleråriga budgetramen | Åtaganden | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 9 408 |
| | Betalningar | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 9 408 |

3.2.2. *Beräknad inverkan på driftsanslagen*

- Förslaget/initiativet kräver inte att driftsanslag tas i anspråk
- Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

3.2.3. Beräknad inverkan på de administrativa anslagen

3.2.3.1. Sammanfattning

- Förslaget/initiativet kräver inte att administrativa anslag tas i anspråk
- Förslaget/initiativet kräver att administrativa anslag tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

| | År n 2014 | År 2015 | År 2016 | År 2017 | År 2018 | År 2019 | År 2020 | TOTALT |
|--|--------------|------------|------------|------------|------------|------------|------------|--------|
|--|--------------|------------|------------|------------|------------|------------|------------|--------|

| RUBRIK 5 i den fleråriga budgetramen | | | | | | | | |
|--|-------|-------|-------|-------|-------|-------|-------|--------------|
| Personalresurser | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 9 408 |
| Övriga administrativa utgifter | | | | | | | | |
| Delsumma RUBRIK 5 i den fleråriga budgetramen | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 9 408 |

| Belopp utanför RUBRIK 5³³ i den fleråriga budgetramen | | | | | | | | |
|---|--|--|--|--|--|--|--|--|
| Personalresurser | | | | | | | | |
| Övriga administrativa utgifter | | | | | | | | |
| Delsumma för belopp utanför RUBRIK 5 i den fleråriga budgetramen | | | | | | | | |

| | | | | | | | | |
|---------------|-------|-------|-------|-------|-------|-------|-------|--------------|
| TOTALT | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 1 344 | 9 408 |
|---------------|-------|-------|-------|-------|-------|-------|-------|--------------|

³³

Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

3.2.3.2. Beräknat personalbehov

- Förslaget/initiativet kräver inte att personalresurser tas i anspråk
- Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

Uppgifterna ska anges i heltal (eller med högst en decimal)

| | År 2014 | År 2015 | År 2016 | År 2017 | År 2018 | År 2019 | År 2020 |
|---|-----------------------------------|------------|------------|------------|------------|------------|------------|
| • Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda) Ange AD- eller AST-tjänst | | | | | | | |
| 09 01 01 01 (vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna) | 9 | 9 | 9 | 9 | 9 | 9 | 9 |
| XX 01 01 02 (vid delegationer) | | | | | | | |
| XX 01 05 01 (indirekta forskningsåtgärder) | | | | | | | |
| 10 01 05 01 (direkta forskningsåtgärder) | | | | | | | |
| • Extern personal (i heltidsekvivalenter)³⁴ | | | | | | | |
| 09 01 02 01 (kontraktsanställda, nationella experter och vikarier – totalt) | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| XX 01 02 02 (kontraktsanställda, lokalanställda, nationella experter, vikarier och unga experter vid delegationerna) | | | | | | | |
| XX 01 04 yy ³⁵ | - vid huvudkontoret ³⁶ | | | | | | |
| | - vid delegationer | | | | | | |
| XX 01 05 02 (kontraktsanställda, nationella experter och vikarier som arbetar med indirekta forskningsåtgärder) | | | | | | | |
| 10 01 05 02 (kontraktsanställda, nationella experter och vikarier som arbetar med direkta forskningsåtgärder) | | | | | | | |
| Annan budgetrubrik (ange vilken) | | | | | | | |
| TOTALT | 12 | 12 | 12 | 12 | 12 | 12 | 12 |

Personalbehoven ska täckas med personal inom generaldirektoratet som redan har avdelats för att förvalta åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

Beskrivning av arbetsuppgifter:

| | |
|--------------------------------------|--|
| Tjänstemän och tillfälligt anställda | Leda arbetet med lagstiftningsförfarandena för Europaparlamentets och rådets antagande av den planerade förordningen samt därtill hörande delegerade akter och genomförandeakter. Prioriterade områden: |
|--------------------------------------|--|

³⁴ [Denna fotnot förklarar vissa initialförkortningar som inte används i den svenska versionen].

³⁵ Särskilt tak för finansiering av extern personal genom driftsanslag (tidigare s.k. BA-poster).

³⁶ Inom förvaltningen av strukturfonderna, Europeiska jordbruksfonden för landsbygdsutveckling (EJFLU) samt Europeiska fiskerifonden (EFF).

| | |
|-----------------|--|
| | <ol style="list-style-type: none"> 1. Att upprätta en ny rättslig ram för elektroniska betrodda tjänster. 2. Att främja användningen av elektroniska betrodda tjänster genom att öka medvetenheten om dessa tjänsters potential bland små och medelstora företag samt medborgare. 3. Att göra en uppföljning av direktiv 1999/93/EG, inklusive internationella aspekter. 4. Att utnyttja hävstångseffekten av storskaliga pilotprojekt för att påskynda det konkreta förverkligandet av målet för den nya rättsliga ramen. |
| Extern personal | Detsamma som ovan. |

3.2.4. Förenlighet med den gällande fleråriga budgetramen

- Förslaget/initiativet är förenligt med den gällande fleråriga budgetramen
- Förslaget/initiativet kräver omfördelningar under den berörda rubriken i den fleråriga budgetramen

Förklara i förekommande fall vilka ändringar i planeringen som krävs, och ange berörda budgetrubriker och belopp.

- Förslaget/initiativet förutsätter att flexibilitetsmekanismen utnyttjas eller att den fleråriga budgetramen revideras³⁷

Beskriv behovet av sådana åtgärder, och ange berörda rubriker i budgetramen, budgetrubriker i den årliga budgeten samt belopp.

3.2.5. Bidrag från tredje part

- Det ingår inga bidrag från tredje part i det aktuella förslaget eller initiativet
- Förslaget eller initiativet kommer att medfinansieras enligt följande:

3.3. Beräknad inverkan på inkomsterna

- Förslaget/initiativet påverkar inte budgetens inkomstsida.
- Förslaget/initiativet påverkar inkomsterna på följande sätt:
 - Påverkan på egna medel
 - Påverkan på ”diverse inkomster”

³⁷

Se punkterna 19 och 24 i det interinstitutionella avtalet.