EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) nr 910/2014

av den 23 juli 2014

om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG

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 yttrande ([1]),

i enlighet med det ordinarie lagstiftningsförfarandet ([2]), och

av följande skäl:

(1) Att bygga upp förtroendet för nätmiljön är avgörande för den ekonomiska och sociala utvecklingen. Bristande förtroende, särskilt på grund av upplevd brist på rättssäkerhet, gör att konsumenter, företag och offentliga 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 tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan medborgare, företag 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 ([3]) gällde elektroniska underskrifter utan att skapa ett heltäckande, gräns- och sektorsöverskridande regelverk för säkra, pålitliga och lättanvända elektroniska transaktioner. Genom denna förordning stärks och utvidgas det direktivets regelverk.

(4) I kommissionens meddelande av den 26 augusti 2010 med titeln *En digital agenda för Europa* utpekades fragmenteringen av den digitala marknaden, bristen på interoperabilitet och den ökande it-brottsligheten som viktiga hinder för en positiv spiral för den digitala ekonomin. I sin rapport om EU-medborgarskapet 2010 med titeln *Att undanröja hindren för EU-medborgarnas möjligheter att utöva sina rättigheter* betonade kommissionen ytterligare vikten av att undanröja de största hindren för att unionsmedborgarna ska kunna utnyttja fördelarna med en digital inre marknad och gränsöverskridande digitala tjänster.

(5) I sina slutsatser av den 4 februari 2011 och den 23 oktober 2011 uppmanade Europeiska rådet kommissionen att se till att en digital inre marknad skapas senast 2015, att göra snabba framsteg på centrala områden inom den digitala ekonomin och att främja en fullständigt integrerad digital inre marknad genom att underlätta gränsöverskridande användning av nättjänster, med särskild fokus på att underlätta säker elektronisk identifiering och autentisering.

([1]) EUT C 351, 15.11.2012, s. 73.
([2]) Europaparlamentets ståndpunkt av den 3 april 2014 (ännu ej offentliggjord i EUT) och rådets beslut av den 23 juli 2014.
([3]) Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer (EGT L 13, 19.1.2000, s. 12).

(6) I sina slutsatser av den 27 maj 2011 uppmanade rådet 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 underskrifter och elektroniska leveranstjänster samt för interoperabla e-förvaltningstjänster i hela EU.

(7) Europaparlamentet betonade, i sin resolution av den 21 september 2010 om fullbordandet av den inre marknaden för e-handel ([1]), betydelsen av säkerhet i elektroniska tjänster, särskilt i elektroniska underskrifter, och behovet av att skapa en infrastruktur för kryptering med öppen nyckel (PKI) i hela Europa samt uppmanade kommissionen att inrätta en europeisk nätverksport för valideringsmyndigheter för att garantera gränsöverskridande interoperabilitet för elektroniska underskrifter och öka säkerheten i samband med transaktioner som görs via internet.

(8) Enligt Europaparlamentets och rådets direktiv 2006/123/EG ([2]) ska medlemsstaterna 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 den lämpliga gemensamma kontaktpunkten och med behöriga myndigheter. Många nättjänster som är tillgängliga via gemensamma kontaktpunkter kräver elektronisk identifiering, autentisering och underskrift.

(9) I de flesta fall kan medborgare inte använda sin elektroniska identifiering för att autentisera sig i en annan medlemsstat därför att de nationella systemen för elektronisk identifiering i deras land inte är erkända i andra medlemsstater. Detta elektroniska hinder utestänger tillhandahållare av tjänster från möjligheten att fullt ut utnyttja fördelarna med den inre marknaden. Ömsesidigt erkända medel för elektronisk identifiering kommer att underlätta tillhandahållandet av en rad olika tjänster över gränserna på den inre 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 ([3]) inrättades ett nätverk av 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 elektronisk identifiering och autentisering är en förutsättning för att gränsöverskridande sjukvård ska kunna bli 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) Denna förordning bör tillämpas i full överensstämmelse med de principer om skydd av personuppgifter som föreskrivs i Europaparlamentets och rådets direktiv 95/46/EG ([4]). Vad gäller principen om ömsesidigt erkännande som fastställs genom denna förordning bör autentisering för en nättjänst endast avse behandling av den identifieringsinformation som är adekvat, relevant och som inte går utöver vad som är nödvändigt för att få tillgång till den aktuella nättjänsten. Därtill bör kraven i direktiv 95/46/EG om sekretess och säkerhet vid behandling följas av tillhandahållaren av betrodda tjänster och tillsynsorgan.

(12) 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 autentisering för åtminstone offentliga tjänster. Denna förordning syftar inte till att ingripa i fråga om 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.

([1]) EUT C 50 E, 21.2.2012, s. 1.
([2]) Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden (EUT L 376, 27.12.2006, s. 36).
([3]) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).
([4]) 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 uppgifter (EGT L 281, 23.11.1995, s. 31).

(13) Medlemsstaterna bör även fortsättningsvis 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 till kommissionen. Det ankommer på medlemsstaterna att välja om de till kommissionen 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.

(14) I förordningen bör vissa villkor fastställas rörande vilka medel för elektronisk identifiering som måste erkännas och hur systemen för elektronisk identifiering bör anmälas. Dessa villkor bör hjälpa medlemsstaterna att bygga upp det förtroende som krävs för varandras system för elektronisk identifiering samt att ömsesidigt erkänna medel för elektronisk identifiering som ingår i deras anmälda system. Principen om ömsesidigt erkännande bör gälla om den anmälande medlemsstatens system för elektronisk identifiering uppfyller villkoren för anmälan och om anmälan har offentliggjorts i *Europeiska unionens officiella tidning*. Principen om ömsesidigt erkännande bör dock endast avse autentisering för en nättjänst. Åtkomsten till dessa nättjänster och deras slutliga leverans till den sökande bör vara nära kopplad till rätten att ta emot sådana tjänster enligt villkoren i nationell lagstiftning.

(15) Skyldigheten att erkänna medel för elektronisk identifiering bör enbart avse medel vars identifieringstillitsnivå motsvarar en nivå som är lika hög eller högre än den nivå som krävs för den aktuella nättjänsten. Den skyldigheten bör dessutom endast tillämpas när det offentliga organet i fråga använder tillitsnivån väsentlig eller hög i samband med åtkomst till den nättjänsten. Medlemsstaterna bör ha rätt att, i enlighet med unionsrätten, erkänna medel för elektronisk identifiering med lägre identifieringstillitsnivåer.

(16) Tillitsnivåerna bör återge graden av tillit till ett medel för elektronisk identifiering vid fastställande av en persons identitet och skapa visshet om att den person som gör anspråk på en viss identitet faktiskt är den person som har tilldelats denna identitet. Tillitsnivån beror på den grad av tillit detta medel för elektronisk identifiering ger i fråga om en persons påstådda eller styrkta identitet med beaktande av olika processer (t.ex. styrkande och kontroll av identitet, och autentisering), förvaltningsverksamhet (t.ex. den enhet som utfärdar medel för elektronisk identifiering och förfaranden för att utfärda sådana medel) och de tekniska kontroller som tillämpas. Det finns olika tekniska definitioner och beskrivningar av tillitsnivåer tack vare unionsfinansierade storskaliga pilotprojekt, standardiseringsarbete och internationell verksamhet. Det storskaliga pilotprojektet Stork och ISO 29115 avser, bland annat, nivåerna 2, 3 och 4, som bör tas under noggrant övervägande vid fastställandet av minsta tekniska krav, standarder och förfaranden för tillitsnivåerna låg, väsentlig och hög enligt denna förordning, samtidigt som en konsekvent tillämpning av denna förordning säkerställs med särskilt hänseende på tillitsnivån hög i samband med styrkande av identitet för utfärdande av kvalificerade certifikat. De fastställda kraven ska vara teknikneutrala. Det ska vara möjligt att uppnå de nödvändiga tekniska kraven med hjälp av olika tekniklösningar.

(17) Medlemsstaterna bör uppmana den privata sektorn att frivilligt 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 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 en medlemsstat vara tillgänglig för de förlitande parter i den privata sektorn som är etablerade utanför denna medlemsstats territorium på samma villkor som för de förlitande parter i den privata sektorn som är etablerade i denna medlemsstat. Med hänsyn till förlitande parter i den privata sektorn får den anmälande medlemsstaten fastställa villkor för åtkomst till medlen för autentisering. Sådana villkor för åtkomst kan innehålla uppgift om huruvida medlen för autentisering för det anmälda systemet för närvarande är tillgängliga för förlitande parter i den privata sektorn.

(18) I denna förordning bör det föreskrivas skadeståndsansvar för den anmälande medlemsstaten, den part som utfärdar medlet för elektronisk identifiering och den part som handhar autentiseringsförfarandet vid underlåtenhet att uppfylla relevanta skyldigheter enligt denna förordning. Denna förordning bör dock tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar. Den ska därför inte påverka tillämpningen av dessa nationella bestämmelser om t.ex. definition av skada eller relevanta tillämpliga förfaranderegler, inbegripet regler om bevisbörda.

(19) Säkerheten i system för elektronisk identifiering är avgörande för ett tillförlitligt gränsöverskridande ömsesidigt erkännande av medel för elektronisk identifiering. Mot denna bakgrund bör medlemsstaterna samarbeta med avseende på säkerheten och interoperabiliteten i systemen för elektronisk identifiering på unionsnivå. När system för elektronisk identifiering kräver att förlitande parter på nationell nivå använder särskild maskinvara eller programvara förutsätter den gränsöverskridande interoperabiliteten att dessa medlemsstater inte inför sådana krav och därtill hörande kostnader för förlitande parter som är etablerade utanför deras territorium. I så fall bör lämpliga lösningar diskuteras och utvecklas inom interoperabilitetsramverkets räckvidd. Tekniska krav som har sin grund i de inneboende specifikationerna för nationella medel för elektronisk identifiering som sannolikt berör innehavarna av sådana elektroniska medel (t.ex. smartkort) är däremot oundvikliga.

(20) Medlemsstaternas samarbete bör underlätta den tekniska interoperabiliteten för de anmälda systemen för elektronisk identifiering i syfte att främja en hög nivå av förtroende och en säkerhetsnivå som är anpassad till risknivån. Ett utbyte av information och bästa praxis mellan medlemsstaterna med sikte på ömsesidigt erkännande bör bidra till detta samarbete.

(21) Genom denna förordning bör även ett allmänt regelverk för användningen av betrodda tjänster upprättas. Någon allmän skyldighet att använda dem eller att installera en accesspunkt för alla befintliga betrodda tjänster bör dock inte skapas. I synnerhet bör den inte gälla tillhandahållande av tjänster som endast används inom slutna system mellan en avgränsad uppsättning deltagare, och som inte påverkar tredje man. Exempelvis system som inrättats i företag eller offentlig förvaltning för hantering av interna förfaranden där betrodda tjänster används bör inte omfattas av kraven i denna förordning. Endast betrodda tjänster som tillhandahålls för allmänheten och som påverkar tredje man bör uppfylla de krav som fastställs i denna förordning. Denna förordning bör inte heller gälla frågor som avser ingående eller giltighet av avtal eller andra rättsliga förpliktelser om nationell rätt eller unionsrätten föreskriver vissa formkrav. Den bör inte heller inverka på nationella formkrav avseende offentliga register, i synnerhet inte kommersiella register eller fastighetsregister.

(22) För att bidra till deras allmänna gränsöverskridande användning bör det vara möjligt att använda betrodda tjänster som bevis vid rättsliga förfaranden i alla medlemsstater. Rättsverkan av betrodda tjänster ska definieras i nationell rätt, om inte annat föreskrivs i denna förordning.

(23) I den mån denna förordning medför en skyldighet att erkänna en betrodd tjänst, får en sådan betrodd tjänst ogillas endast om skyldighetens adressat av tekniska skäl bortom adressatens direkta kontroll är oförmögen att läsa eller kontrollera den. Denna skyldighet bör dock inte i sig medföra att ett offentligt organ är tvunget att anskaffa den maskinvara och programvara som krävs för teknisk läsbarhet för alla befintliga betrodda tjänster.

(24) Medlemsstaterna får behålla eller införa nationella bestämmelser, i överensstämmelse med unionsrätten, avseende betrodda tjänster så länge dessa tjänster inte har harmoniserats fullständigt genom denna förordning. Betrodda tjänster som överensstämmer med denna förordning bör dock omfattas av fri rörlighet på den inre marknaden.

(25) 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.

(26) På grund av den snabba tekniska utvecklingen bör denna förordning omfatta en strategi som är öppen för innovation.

(27) 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.

(28) För att framför allt öka små och medelstora företags samt konsumenternas 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 skyldigheter som säkerställer hög grad av säkerhet oavsett vilken typ av kvalificerad betrodd tjänst eller produkt som används eller tillhandahålls.

(29) I linje med de skyldigheter som följer av Förenta nationernas konvention om rättigheter för personer med funktionsnedsättning, som godkändes genom rådets beslut 2010/48/EG ([1]), särskilt artikel 9 i konventionen, bör personer med funktionshinder kunna använda betrodda tjänster och slutanvändarprodukter som används vid tillhandahållandet av dessa tjänster på samma villkor som andra konsumenter. När det är genomförbart bör därför betrodda tjänster som tillhandahålls och slutanvändarprodukter som används i samband med tillhandahållandet av dessa tjänster göras tillgängliga för personer med funktionsnedsättning. Genomförbarhetsbedömningen bör inbegripa tekniska och ekonomiska överväganden.

(30) Medlemsstaterna bör utse ett eller flera tillsynsorgan för genomförandet av tillsynsverksamheten enligt denna förordning. Medlemsstaterna bör också kunna fatta beslut, efter ömsesidig överenskommelse med en annan medlemsstat, om att utse ett tillsynsorgan på den andra medlemsstatens territorium.

(31) Tillsynsorgan bör samarbeta med dataskyddsmyndigheter, t.ex. genom att informera dem om resultatet av granskningar av kvalificerade tillhandahållare av betrodda tjänster, när det förefaller ha skett en överträdelse av reglerna om skydd för personuppgifter. Bestämmelsen om information bör särskilt gälla säkerhetstillbud och personuppgiftsöverträdelser.

(32) 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.

(33) Bestämmelser om användningen av pseudonymer i certifikat bör inte hindra medlemsstaterna från att kräva identifiering av personer i enlighet med unionsrätten eller nationell rätt.

(34) För att säkerställa en jämförbar säkerhetsnivå i fråga om kvalificerade betrodda tjänster bör alla medlemsstater följa gemensamma grundläggande tillsynskrav. För att underlätta enhetlig tillämpning av dessa krav i hela unionen bör medlemsstaterna införa jämförbara förfaranden och utbyta information om sin tillsynsverksamhet och bästa praxis på området.

(35) Alla tillhandahållare av betrodda tjänster bör omfattas av kraven i denna förordning, särskilt de som gäller säkerhet och skadeståndsansvar, för att säkerställa vederbörlig noggrannhet, insyn och ansvarighet i sina verksamheter och tjänster. Med tanke på den typ av tjänster som de tillhandahåller bör det emellertid med avseende på dessa krav göras åtskillnad mellan kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster.

(36) Inrättandet av ett tillsynssystem för alla tillhandahållare av betrodda tjänster bör säkerställa lika villkor för säkerheten och tillförlitligheten i deras åtgärder och tjänster, och därigenom bidra till användarskyddet och till en fungerande inre marknad. Icke-kvalificerade tillhandahållare av betrodda tjänster bör omfattas av mindre omfattande, förebyggande tillsynsverksamhet i efterhand som är anpassad till arten av deras tjänster och åtgärder. Tillsynsorganet bör därför inte ha någon allmän skyldighet att utöva tillsyn av icke-kvalificerade tillhandahållare av betrodda tjänster. Tillsynsorganet bör endast vidta åtgärder när det har informerats (t.ex. av den icke-kvalificerade tillhandahållaren av betrodda tjänster själv, av ett annat tillsynsorgan, genom anmälan från en användare eller en affärspartner eller på grundval av en egen utredning) om att en icke-kvalificerad tillhandahållare av betrodda tjänster inte uppfyller kraven i denna förordning.

([1]) Rådets beslut 2010/48/EG av den 26 november 2009 om ingående från Europeiska gemenskapens sida av Förenta nationernas konvention om rättigheter för personer med funktionsnedsättning (EUT L 23, 27.1.2010, s. 35).

(37) Denna förordning bör föreskriva skadeståndsansvar för alla tillhandahållare av betrodda tjänster. Den fastställer särskilt det system för skadeståndsansvar enligt vilket alla tillhandahållare av betrodda tjänster bör ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person genom underlåtenhet att uppfylla kraven i denna förordning. För att underlätta bedömningen av den ekonomiska risk som tillhandahållare av betrodda tjänster kan vara tvungna att bära eller som de bör täcka genom försäkring, tillåts tillhandahållare av betrodda tjänster genom denna förordning att på vissa villkor fastställa begränsningar för användningen av de tjänster de tillhandahåller, varvid de inte ska hållas ansvariga för skada som uppkommit genom sådan användning av tjänster som överskrider dessa begränsningar. Kunder bör vederbörligen informeras i förväg om begränsningarna. Sådana begränsningar bör vara igenkännliga för tredje man, t.ex. genom att information om begränsningarna bifogas villkoren för den tillhandahållna tjänsten eller genom andra igenkännliga medel. För att dessa principer ska kunna genomföras bör denna förordning tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar. Denna förordning påverkar därför inte dessa nationella bestämmelser om t.ex. definitionen av skada, avsikt, oaktsamhet eller relevanta tillämpliga procedurregler.

(38) Det är mycket viktigt att säkerhetsincidenter och bedömningar av säkerhetsrisker anmäls så att berörda parter kan förses med tillräcklig information i händelse av en säkerhetsincident eller en integritetsförlust.

(39) 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).

(40) 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 verkningsfullt sätt i alla medlemsstater.

(41) För att säkerställa att kvalificerade betrodda tjänster är hållbara och varaktiga samt för att öka användarnas förtroende för kontinuiteten i dessa tjänster, bör tillsynsorganen kontrollera befintlighet och korrekt tillämpning av bestämmelser om planer för verksamhetens upphörande när kvalificerade tillhandahållare av betrodda tjänster upphör med sin verksamhet.

(42) 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.

(43) För att säkerställa att kvalificerade tillhandahållare av betrodda tjänster och de tjänster de tillhandahåller uppfyller de krav som fastställs i denna förordning bör en bedömning av överensstämmelse utföras av organ för bedömning av överensstämmelse, och de rapporter om överensstämmelsebedömning dessa resulterar i bör av den kvalificerade tillhandahållaren av betrodda tjänster lämnas in till tillsynsorganet. Om tillsynsorganet begär att en kvalificerad tillhandahållare av betrodda tjänster ska lämna in en särskild rapport om överensstämmelsebedömning, bör tillsynsorganet särskilt respektera principen om god förvaltning, inbegripet skyldigheten att motivera beslut, samt proportionalitetsprincipen. Tillsynsorganet bör därför vederbörligen motivera sitt beslut om krav på särskild överensstämmelsebedömning.

(44) Målet med denna förordning är att säkerställa ett konsekvent ramverk i syfte att tillhandahålla en hög nivå av säkerhet och rättssäkerhet för betrodda tjänster. I detta avseende bör kommissionen när den behandlar bedömning av överensstämmelse av produkter och tjänster i tillämpliga fall söka synergier med befintliga relevanta europeiska och internationella system så som Europaparlamentets och rådets förordning (EG) nr 765/2008 ([1]) om krav för ackreditering av organ för bedömning av överensstämmelse och marknadskontroll av produkter.

([1]) Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

(45) 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 *due diligence*-granskning som ska leda fram till tillhandahållandet av kvalificerade betrodda tjänster.

(46) Förteckningar över betrodda tjänsteleverantörer kan vara viktiga för att hjälpa till att bygga upp förtroendet bland aktörer på marknaden, eftersom de visar att tillhandahållaren av tjänster vid tidpunkten för tillsynen hade status som kvalificerad.

(47) För att användare ska kunna dra full nytta av och veta att de kan förlita sig på nättjänster är det nödvändigt att de har förtroende för nättjänsterna och att dessa är lättillgängliga. Det bör därför inrättas ett EU-förtroendemärke för att identifiera kvalificerade betrodda tjänster som tillhandhålls av kvalificerade tillhandahållare av betrodda tjänster. Ett sådant EU-förtroendemärke av kvalificerade betrodda tjänster skulle göra tydlig åtskillnad mellan kvalificerade betrodda tjänster och andra betrodda tjänster och på så sätt bidra till insynen på marknaden. Det bör vara frivilligt för kvalificerade tillhandahållare av betrodda tjänster att använda sig av ett EU-förtroendemärke och detta bör inte medföra några andra krav än de som föreskrivs i denna förordning.

(48) Det krävs en hög tillitsnivå för att säkerställa ömsesidigt erkännande av elektroniska underskrifter, men i vissa fall, som t.ex. inom ramen för kommissionens beslut 2009/767/EG ([1]) bör även elektroniska underskrifter med en lägre säkerhetsgrad godtas.

(49) Denna förordning bör fastställa principen om att en elektronisk underskrift inte bör förvägras rättslig verkan på grund av att den har elektronisk form eller inte uppfyller kraven för en kvalificerad elektronisk underskrift. Den rättsliga verkan av elektroniska underskrifter ska emellertid definieras i nationell rätt, med undantag för kraven i denna förordning på att en kvalificerad elektronisk underskrift ska ha samma rättsliga verkan som en handskriven underskrift.

(50) Eftersom behöriga myndigheter i medlemsstaterna för närvarande använder olika avancerade elektroniska underskrifter av olika format för att underteckna sina dokument elektroniskt är det nödvändigt att se till att åtminstone ett visst antal format av avancerade elektroniska underskrifter 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 stämplar vara nödvändigt att se till att de stöder åtminstone ett visst antal format av avancerade elektroniska stämplar.

(51) Det bör vara möjligt för undertecknare att anförtro anordningar för skapande av kvalificerade elektroniska underskrifter till tredje man, förutsatt att lämpliga mekanismer och förfaranden tillämpas för att se till att undertecknaren har användningen av sina uppgifter för skapande av elektroniska underskrifter uteslutande under sin egen kontroll och att kraven för kvalificerade elektroniska underskrifter uppfylls genom anordningens användning.

(52) Om miljön för skapande av elektroniska underskrifter styrs av en tillhandahållare av betrodda tjänster på uppdrag av undertecknaren, kommer elektroniska underskrifter på distans med säkerhet att utvecklas på grund av sina många ekonomiska fördelar. För att säkerställa att dessa elektroniska underskrifter får samma rättsliga erkännande som elektroniska underskrifter som skapas i en miljö som helt och hållet styrs av användaren bör emellertid tillhandahållare av tjänster för elektroniska underskrifter på distans tillämpa särskilda säkerhetsförfaranden för förvaltning och administration samt använda tillförlitliga system och produkter, bland annat säkra elektroniska kommunikationskanaler, för att säkerställa en tillförlitlig miljö för skapande av elektroniska underskrifter som undertecknaren använder uteslutande under sin egen kontroll. För en kvalificerad elektronisk underskrift som skapas med en anordning för skapande av elektroniska underskrifter på distans bör de krav som gäller för kvalificerade tillhandahållare av betrodda tjänster och som anges i denna förordning tillämpas.

([1]) 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 marknaden (EUT L 274, 20.10.2009, s. 36).

(53) Tillfälligt upphävande av kvalificerade certifikat är etablerad operativ praxis för tillhandahållare av betrodda tjänster i ett antal medlemsstater som skiljer sig från återkallande och medför en tillfällig förlust av giltighet för ett certifikat. Rättsäkerheten kräver att ett certifikats status som tillfälligt upphävt alltid ska anges klart och tydligt. Tillhandahållare av betrodda tjänster bör därför ansvara för att klart och tydligt ange ett certifikats status och, om detta upphävs, den exakta tidsperiod under vilket certifikatet har tillfälligt upphävts. Denna förordning bör inte ålägga tillhandahållare av betrodda tjänster eller medlemsstater att använda sig av tillfälligt upphävande men bör tillhandahålla transparensregler för när och hur en sådan möjlighet finns.

(54) Gränsöverskridande erkännande av kvalificerade elektroniska underskrifter förutsätter gränsöverskridande interoperabilitet och erkännande av kvalificerade certifikat. Därför bör inte kvalificerade certifikat omfattas av några obligatoriska krav som går utöver kraven i denna förordning. På nationell nivå bör man dock få inkludera särskilda egenskaper, t.ex. unika identifierare, i kvalificerade certifikat, under förutsättning att sådana särskilda egenskaper inte hindrar gränsöverskridande interoperabilitet och erkännande av kvalificerade certifikat och elektroniska underskrifter.

(55) It-säkerhetscertifiering som bygger på internationella standarder, såsom ISO 15408 och besläktade utvärderingsmetoder och arrangemang för ömsesidigt erkännande, utgör ett viktigt verktyg för att kontrollera säkerheten hos kvalificerade anordningar för skapande av elektroniska underskrifter och bör främjas. Innovativa lösningar och tjänster, såsom undertecknande via mobil och datamoln, förlitar sig emellertid på tekniska och organisatoriska lösningar för kvalificerade anordningar för skapande av elektroniska underskrifter, för vilka det eventuellt ännu inte finns tillgängliga säkerhetsstandarder eller för vilka den första it-säkerhetscertifieringen pågår. Säkerhetsnivån för sådana kvalificerade anordningar för skapande av elektroniska underskrifter skulle kunna utvärderas genom alternativa processer endast om sådana säkerhetsstandarder inte finns tillgängliga eller om den första it-säkerhetscertifieringen pågår. De processerna bör vara jämförbara med standarderna för it-säkerhetscertifiering i den mån deras säkerhetsnivåer är likvärdiga. Förfarandena skulle dessutom kunna underlättas av en sakkunnighetsbedömning.

(56) I denna förordning bör det fastställas krav på kvalificerade anordningar för skapande av elektroniska underskrifter för att säkerställa de avancerade elektroniska underskrifternas funktionalitet. Denna förordning bör inte omfatta hela den systemmiljö där sådana anordningar används. Därför bör omfattningen av certifieringen av kvalificerade anordningar för skapande av elektroniska underskrifter begränsas till den hårdvara och systemprogramvara som används för att hantera och skydda uppgifterna för skapande av underskrifter som skapas, lagras eller behandlas i anordningen för skapande av underskrifter. I enlighet med vad som fastställs i relevanta standarder bör certifieringsskyldigheterna inte omfatta tillämpningar för skapande av underskrifter.

(57) För att säkerställa rättssäkerheten avseende en underskrifts giltighet är det nödvändigt att specificera vilka komponenter i en kvalificerad elektronisk underskrift som bör bedömas av den förlitande part som utför valideringen. Genom att specificera kraven på kvalificerade tillhandahållare av betrodda tjänster som kan tillhandahålla en kvalificerad valideringstjänst till förlitande parter som inte själva vill eller kan utföra valideringen av kvalificerade elektroniska underskrifter bör dessutom privat och offentlig sektor stimuleras att investera i sådana tjänster. Sammantaget bör dessa krav göra kvalificerad validering av elektroniska underskrifter enkel och bekväm för alla parter på unionsnivå.

(58) När en transaktion kräver en kvalificerad elektronisk stämpel från en juridisk person bör en kvalificerad elektronisk underskrift från ett behörigt ombud för den juridiska personen vara lika godtagbar.

(59) Elektroniska stämplar bör utgöra bevis för att ett elektroniskt dokument har utfärdats av en juridisk person och säkerställa visshet om dokumentets ursprung och integritet.

(60) Tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat för elektroniska stämplar bör vidta de åtgärder som krävs för att kunna fastställa identiteten för den fysiska person som representerar den juridiska person som har fått ett kvalificerat certifikat för en elektronisk stämpel, om sådan identifiering krävs på nationell nivå inom ramen för juridiska eller administrativa förfaranden.

(61) Genom denna förordning bör långsiktigt bevarande av uppgifter säkerställas, för att säkerställa den rättsliga giltigheten hos elektroniska underskrifter och elektroniska stämplar över längre tidsperioder och garantera att de kan valideras oavsett kommande tekniska förändringar.

(62) I syfte att säkerställa säkerheten hos kvalificerad elektronisk tidsstämpling bör det i denna förordning krävas att man använder en avancerad elektronisk stämpel eller en avancerad elektronisk underskrift eller andra likvärdiga metoder. Sannolikt kan innovation leda till ny teknik som kan säkerställa en likvärdig säkerhetsnivå för tidsstämpling. Vid användning av någon annan metod än avancerade elektroniska stämplar eller avancerade elektroniska underskrifter bör det åligga tillhandahållaren av betrodda tjänster att i rapporten om bedömning av överensstämmelse visa att denna metod säkerställer en likvärdig säkerhetsnivå och att den är förenlig med skyldigheterna i denna förordning.

(63) Elektroniska dokument är viktiga för vidareutveckling av gränsöverskridande elektroniska transaktioner på den inre marknaden. Denna förordning bör fastställa principen om att ett elektroniskt dokument inte bör förvägras rättslig verkan på grund av att det har elektronisk form, för att säkerställa att elektroniska transaktioner inte kommer att ogillas enbart på grund av att ett dokument har elektronisk form.

(64) När kommissionen behandlar formaten för avancerade elektroniska underskrifter och stämplar ska den bygga vidare på den praxis, de standarder och den lagstiftning som redan finns, i synnerhet kommissionens beslut 2011/130/EU ([1]).

(65) Elektroniska stämplar 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 eller servrar.

(66) Det är av avgörande betydelse att det föreskrivs en rättslig ram för att främja gränsöverskridande erkännande mellan befintliga nationella rättssystem för elektroniska tjänster för rekommenderade leveranser. Den ramen skulle också kunna öppna nya marknadsmöjligheter för unionens tillhandahållare av betrodda tjänster att erbjuda nya paneuropeiska tjänster för elektroniska tjänster för rekommenderade leveranser.

(67) Tjänster för autentisering av webbplatser innebär möjlighet för en besökare på en webbplats att försäkra sig om att en verklig och legitim enhet står bakom webbplatsen. Dessa tjänster bidrar till att bygga upp förtroendet för näthandeln, eftersom användarna kommer att ha förtroende för en webbplats som har autentiserats. Tillhandahållande och användning av tjänster för autentisering av webbplatser är fullständigt frivilligt. För att autentiseringen av webbplatser ska kunna bli ett sätt att stärka förtroendet, ge användaren en bättre upplevelse och främja tillväxten på den inre marknaden bör man emellertid i denna förordning föreskriva minimiskyldigheter vad gäller säkerhet och skadeståndsansvar för tillhandahållarna och deras tjänster. Därför har hänsyn tagits till resultaten av befintliga initiativ ledda av industrin, t.ex. forumet för certifieringsinstanser och försäljare av webbläsare – CA/B Forum. Dessutom bör denna förordning inte hindra användning av andra sätt eller metoder för att autentisera webbplatser som inte omfattas av denna förordning och förordningen bör inte heller hindra tillhandahållare av autentiseringstjänster i tredjeland från att tillhandahålla sina tjänster till kunder i unionen. En tillhandahållare från ett tredjeland bör dock endast kunna få sina tjänster för autentisering av webbplatser erkända som kvalificerade i enlighet med denna förordning om ett internationellt avtal mellan unionen och det land i vilket tillhandahållaren är etablerad har ingåtts.

(68) Begreppet *juridisk person* enligt bestämmelserna om etablering i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) ger aktörer möjlighet att fritt välja den juridiska form de anser vara lämplig för att bedriva sin verksamhet. Följaktligen omfattar begreppet *juridisk person* enligt EUF-fördraget alla enheter, oberoende av juridisk form, som bildats i enlighet med eller som omfattas av rätten i en medlemsstat.

(69) Unionens institutioner, organ och byråer uppmanas att erkänna elektronisk identifiering och betrodda tjänster som omfattas av denna förordning för administrativt samarbete som drar nytta av framför allt befintlig god praxis och resultaten av pågående projekt på de områden som omfattas av denna förordning.

([1]) Kommissionens beslut 2011/130/EU av den 25 februari 2011 om fastställande av minimikrav för behandling över gränserna av dokument som signerats elektroniskt av behöriga myndigheter i enlighet med Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden (EUT L 53, 26.2.2011, s. 66).

(70) I syfte att på ett flexibelt och snabbt sätt kunna komplettera vissa detaljerade tekniska aspekter av denna förordning bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på de kriterier som ska uppfyllas av organ med ansvar för certifieringen av kvalificerade anordningar för skapande av elektroniska underskrifter. Det är av särskild betydelse att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå. När kommissionen förbereder och utarbetar delegerade akter bör den se till att relevanta handlingar översänds samtidigt till Europaparlamentet och rådet och att detta sker så snabbt som möjligt och på lämpligt sätt.

(71) För att säkerställa enhetliga villkor för genomförandet av denna förordning, bör kommissionen tilldelas genomförandebefogenheter, särskilt för att ange referensnummer till standarder vilkas användning skulle skapa presumtion för överensstämmelse med vissa krav i denna förordning. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([1]).

(72) När kommissionen antar delegerade akter eller genomförandeakter bör den ta vederbörlig hänsyn till de standarder och tekniska specifikationer som utarbetats av europeiska och internationella standardiseringsorgan, särskilt Europeiska standardiseringskommittén (CEN), Europeiska institutet för telekommunikationsstandarder (Etsi), Internationella standardiseringsorganisationen (ISO) och Internationella teleunionen (ITU), i syfte att säkerställa en hög nivå av säkerhet och interoperabilitet när det gäller elektronisk identifiering och betrodda tjänster.

(73) Av rättssäkerhets- och tydlighetsskäl bör direktiv 1999/93/EG upphävas.

(74) För att säkerställa rättssäkerheten för marknadsoperatörer som redan använder kvalificerade certifikat som utfärdas för fysiska personer i enlighet med direktiv 1999/93/EG är det nödvändigt att föreskriva en tillräckligt lång övergångsperiod. Övergångsåtgärder bör även fastställas för säkra anordningar för skapande av underskrifter vars överensstämmelse har fastställts i enlighet med direktiv 1999/93/EG samt för tillhandahållare av certifikattjänster som utfärdar kvalificerade certifikat före den 1 juli 2016. Slutligen är det också nödvändigt att göra det möjligt för kommissionen att anta genomförandeakter och delegerade akter före det datumet.

(75) De tillämpningsdagar som anges i denna förordning påverkar inte medlemsstaternas befintliga skyldigheter enligt unionsrätten, särskilt direktiv 2006/123/EG.

(76) Eftersom målen för denna förordning inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning, kan uppnås bättre 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 dessa mål.

(77) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i Europaparlamentets och rådets förordning (EG) nr 45/2001 ([2]) och avgav ett yttrande den 27 september 2012 ([3]).

([1]) 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 genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

([2]) Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).

([3]) EUT C 28, 30.1.2013, s. 6.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte

I syfte att säkerställa en väl fungerande inre marknad och uppnå en lämplig säkerhetsnivå för medel för elektronisk identifiering och betrodda tjänster fastställs i denna förordning

a) de villkor på vilka medlemsstaterna erkänner medel för elektronisk identifiering av fysiska och juridiska personer som omfattas av ett anmält system för elektronisk identifiering hos en annan medlemsstat,

b) regler för betrodda tjänster, i synnerhet för elektroniska transaktioner, och

c) en rättslig ram för elektroniska underskrifter, elektroniska stämplar, elektronisk tidsstämpling, elektroniska dokument, elektroniska tjänster för rekommenderade leveranser och certifikattjänster för autentisering av webbplatser.

Artikel 2

Tillämpningsområde

1. Denna förordning gäller system för elektronisk identifiering som har anmälts av en medlemsstat, och tillhandahållare av betrodda tjänster som är etablerade inom unionen.

2. Denna förordning gäller inte tillhandahållande av betrodda tjänster som till följd av nationell rätt eller avtal mellan en avgränsad uppsättning deltagare endast används inom slutna system.

3. Denna förordning påverkar inte nationell rätt eller unionsrätt som avser ingående av avtal och deras giltighet eller andra rättsliga eller förfarandemässiga skyldigheter avseende formkrav.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

1. *elektronisk identifiering:* en process inom vilken personidentifieringsuppgifter i elektronisk form, som unikt avser en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person, används.

2. *medel för elektronisk identifiering:* en materiell och/eller immateriell enhet som innehåller personidentifieringsuppgifter och som används för autentisering för nättjänster.

3. *personidentifieringsuppgifter:* en uppsättning uppgifter som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person.

4. *system för elektronisk identifiering:* ett system för elektronisk identifiering genom vilket medel för elektronisk identifiering utfärdas till en fysisk eller juridisk person eller en fysisk person som företräder en juridisk person.

5. *autentisering:* en elektronisk process som gör det möjligt att bekräfta den elektroniska identifieringen för en fysisk eller juridisk person, eller ursprunget för och integriteten hos uppgifter i elektronisk form.

6. *förlitande part:* en fysisk eller juridisk person som förlitar sig på en elektronisk identifiering eller betrodda tjänster.

7. *offentligt organ:* en statlig, regional eller lokal myndighet, ett organ som lyder under offentlig rätt eller en sammanslutning som bildats av en eller flera sådana myndigheter eller ett eller flera sådana offentligrättsliga organ, eller en privat enhet som av minst en av dessa myndigheter, enheter eller sammanslutningar har bemyndigats att tillhandahålla offentliga tjänster när de agerar i enlighet med ett sådant bemyndigande.

8. *offentligrättsligt organ:* ett organ enligt definitionen i artikel 2.1.4 i Europaparlamentets och rådets direktiv 2014/24/EU ([1]).

9. *undertecknare:* en fysisk person som skapar en elektronisk underskrift.

10. *elektronisk underskrift:* uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under.

11. *avancerad elektronisk underskrift:* en elektronisk underskrift som uppfyller kraven enligt artikel 26.

12. *kvalificerad elektronisk underskrift:* en avancerad elektronisk underskrift som skapas med hjälp av en kvalificerad anordning för underskriftframställning och som är baserad på ett kvalificerat certifikat för elektroniska underskrifter.

13. *uppgifter för skapande av elektroniska underskrifter:* unika uppgifter som undertecknaren använder för att skapa en elektronisk underskrift.

14. *certifikat för elektroniska underskrifter:* ett elektroniskt intyg som kopplar valideringsuppgifter för en elektronisk underskrift till en fysisk person och bekräftar åtminstone namnet eller pseudonymen på den personen.

15. *kvalificerat certifikat för elektroniska underskrifter:* ett certifikat för elektroniska underskrifter som utfärdas av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga I.

16. *betrodd tjänst:* en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som består av

    a) skapande, kontroll och validering av elektroniska underskrifter, elektroniska stämplar eller elektroniska tidsstämplingar, elektroniska tjänster för rekommenderade leveranser och certifikat med anknytning till dessa tjänster, eller

    b) skapande, kontroll och validering av certifikat för autentisering av webbplatser, eller

    c) bevarande av elektroniska underskrifter, stämplar eller certifikat med anknytning till dessa tjänster.

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

([1]) Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EU (EUT L 94, 28.3.2014, s. 65).

18. *organ för bedömning av överensstämmelse:* ett organ enligt definitionen i artikel 2.13 i förordning (EG) nr 765/2008 som i enlighet med den förordningen är ackrediterat för överensstämmelsebedömning av en kvalificerad tillhandahållare av en betrodd tjänst och den kvalificerade betrodda tjänst som denne tillhandahåller.

19. *tillhandahållare av betrodda tjänster:* en fysisk eller juridisk person som tillhandahåller en eller flera betrodda tjänster, antingen i egenskap av kvalificerade eller icke kvalificerade tillhandahållare av betrodda tjänster.

20. *kvalificerad tillhandahållare av betrodda tjänster:* en tillhandahållare av betrodda tjänster som tillhandahåller en eller flera kvalificerade betrodda tjänster och som beviljats status som kvalificerad av tillsynsorganet.

21. *produkt:* maskinvara eller programvara, eller relevanta komponenter i maskinvara eller programvara, som är avsedda att användas för tillhandahållande av betrodda tjänster.

22. *anordning för underskriftframställning:* en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk underskrift.

23. *kvalificerad anordning för underskriftframställning:* en anordning för skapande av elektroniska underskrifter som uppfyller kraven i bilaga II.

24. *skapare av en stämpel:* en juridisk person som skapar en elektronisk stämpel.

25. *elektronisk stämpel:* uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form för att säkerställa de senares ursprung och integritet.

26. *avancerad elektronisk stämpel:* en elektronisk stämpel som uppfyller kraven enligt artikel 36.

27. *kvalificerad elektronisk stämpel:* en avancerad elektronisk stämpel som skapas med hjälp av en kvalificerad anordning för skapande av elektroniska stämplar och som är baserat på ett kvalificerat certifikat för elektroniska stämplar.

28. *uppgifter för skapande av elektroniska stämplar:* unika uppgifter som skaparen av den elektroniska stämpeln använder för att skapa en elektronisk stämpel.

29. *certifikat för elektroniska stämplar:* ett elektroniskt intyg som kopplar valideringsuppgifter för en elektronisk stämpel till en juridisk person och bekräftar namnet på den personen.

30. *kvalificerat certifikat för elektroniska stämplar:* ett certifikat för en elektronisk stämpel som utfärdas av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga III.

31. *anordning för skapande av elektroniska stämplar:* en konfigurerad programvara eller maskinvara som används för att skapa en elektronisk stämpel.

32. *kvalificerad anordning för skapande av elektroniska stämplar:* en anordning för skapande av elektroniska stämplar som efter nödvändig anpassning uppfyller kraven i bilaga II.

33. *elektronisk tidsstämpling:* uppgifter i elektronisk form som binder andra uppgifter i elektronisk form till en viss tidpunkt och därmed utgör bevis för att de senare uppgifterna existerade vid den tidpunkten.

34. *kvalificerad elektronisk tidsstämpling:* en elektronisk tidsstämpling som uppfyller de krav som fastställs i artikel 42.

35. *elektroniskt dokument:* innehåll lagrat i elektronisk form, i synnerhet som ljud-, bild- eller audiovisuell inspelning.

36. *elektronisk tjänst för rekommenderad leverans:* en tjänst som gör det möjligt att överföra uppgifter mellan tredje män på elektronisk väg och tillhandahåller bevis avseende de överförda uppgifternas hantering, inklusive bevis för uppgifternas sändning och mottagande, och som skyddar överförda uppgifter mot risken för förlust, stöld, skada eller otillåtna ändringar.

37. *kvalificerad elektronisk tjänst för rekommenderad leverans:* en elektronisk tjänst för rekommenderad leverans som uppfyller de krav som fastställs i artikel 44.

38. *certifikat för autentisering av webbplatser:* ett intyg som gör det möjligt att autentisera en webbplats och koppla webbplatsen till den fysiska eller juridiska person som certifikatet utfärdats för.

39. *kvalificerat certifikat för autentisering av webbplatser:* ett certifikat för autentisering av webbplatser som utfärdas av en kvalificerad tillhandahållare av betrodda tjänster och uppfyller kraven i bilaga IV.

40. *valideringsuppgifter:* uppgifter som används för att validera en elektronisk underskrift eller en elektronisk stämpel.

41. *validering:* en process genom vilken en elektronisk underskrifts giltighet kontrolleras och bekräftas.

Artikel 4

Inremarknadsprincipen

1. Tillhandahållande av betrodda tjänster i en medlemsstat som utförs av en tillhandahållare av betrodda 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 och betrodda tjänster som överensstämmer med denna förordning ska omfattas av fri rörlighet på den inre marknaden.

Artikel 5

Behandling och skydd av uppgifter

1. Personuppgifter ska behandlas i enlighet med direktiv 95/46/EG.

2. Utan att det påverkar rättsverkan av pseudonymer enligt nationell rätt ska användningen av pseudonymer vid elektroniska transaktioner inte förbjudas.

KAPITEL II

ELEKTRONISK IDENTIFIERING

Artikel 6

Ömsesidigt erkännande

1. När det enligt nationell rätt eller enligt nationella administrativa förfaranden krävs en elektronisk identifiering där medel för elektronisk identifiering och autentisering används för att få åtkomst till en nättjänst som tillhandahålls av ett offentligt organ i en medlemsstat, ska de medel för elektronisk identifiering som utfärdats i en annan medlemsstat erkännas i den första medlemsstaten för gränsöverskridande autentisering för den tjänsten via internet, förutsatt att

a) medlet för elektronisk identifiering är utfärdat inom ramen för ett system för elektronisk identifiering som ingår i den förteckning som offentliggjorts av kommissionen enligt artikel 9,

b) tillitsnivån för medlet för elektronisk identifiering motsvarar en tillitsnivå som är lika hög som eller högre än den tillitsnivå som det berörda offentliga organet kräver för åtkomst till denna nättjänst i den första medlemsstaten, förutsatt att tillitsnivån för detta medel för elektronisk identifiering motsvarar tillitsnivån väsentlig eller hög,

c) det offentliga organet i fråga använder tillitsnivån väsentlig eller hög i samband med åtkomst till nättjänsten.

Ett sådant erkännande ska ske senast tolv månader efter det att kommissionen offentliggör den förteckning som avses i led a i första stycket.

2. Ett medel för elektronisk identifiering som utfärdats inom ramen för ett system för elektronisk identifiering som ingår i den förteckning som kommissionen offentliggjort enligt artikel 9 och som motsvarar tillitsnivån låg får erkännas av offentliga organ för gränsöverskridande autentisering för den tjänst som tillhandahålls via internet av dessa organ.

Artikel 7

Berättigande till anmälan av system för elektronisk identifiering

Ett system för elektronisk identifiering ska vara berättigat till anmälan enligt artikel 9.1 om samtliga följande villkor är uppfyllda:

a) Medlet för elektronisk identifiering inom ramen för systemet för elektronisk identifiering ska vara utfärdat

i) av den anmälande medlemsstaten,

ii) på uppdrag av den anmälande medlemsstaten, eller

iii) oberoende av den anmälande medlemsstaten och erkännas av den medlemsstaten.

b) Medlet för elektronisk identifiering inom systemet för elektronisk identifiering ska kunna användas för att få åtkomst till åtminstone en tjänst som tillhandahålls av ett offentligt organ och som kräver elektronisk identifiering i den anmälande medlemsstaten.

c) Systemet för elektronisk identifiering och det medel för elektronisk identifiering som utfärdats inom ramen för det ska uppfylla kraven för åtminstone en av de tillitsnivåer som anges i den genomförandeakt som avses i artikel 8.3.

d) Den anmälande medlemsstaten ska se till att de personidentifieringsuppgifter som unikt representerar personen i fråga, i enlighet med de tekniska specifikationer, standarder och förfaranden för den relevanta tillitsnivå som anges i den genomförandeakt som avses i artikel 8.3, tillskrivs den fysiska eller juridiska person som avses i artikel 3.1 vid tidpunkten för utfärdandet av medlet för elektronisk identifiering inom detta system.

e) Den part som utfärdar medlet för elektronisk identifiering inom detta system ska se till att medlet för elektronisk identifiering tilldelas den person som avses i led d i denna artikel i enlighet med de tekniska specifikationer, standarder och förfaranden för den relevanta tillitsnivå som anges i den genomförandeakt som avses i artikel 8.3.

f) Den anmälande medlemsstaten ska se till att autentisering är tillgänglig via internet så att alla förlitande parter som är etablerade på någon annan medlemsstats territorium kan bekräfta de personidentifieringsuppgifter som tas emot i elektronisk form.

För andra förlitande parter än offentliga organ får den anmälande medlemsstaten fastställa tillträdesvillkoren för autentiseringen. Sådan gränsöverskridande autentisering ska tillhandahållas kostnadsfritt när den utförs i samband med en nättjänst som tillhandahålls av ett offentligt organ.

Medlemsstaterna får inte ålägga förlitande parter som har för avsikt att utföra en sådan autentisering oproportionella tekniska krav om sådana krav skulle hindra eller avsevärt försvåra kompatibiliteten mellan anmälda system för elektronisk identifiering.

g) Minst sex månader före anmälan enligt artikel 9.1 ska den anmälande medlemsstaten när det gäller den skyldighet som anges i artikel 12.5 förse andra medlemsstater med en beskrivning av detta system i enlighet med de förfaranden som fastställts genom de genomförandeakter som avses i artikel 12.7.

h) System för elektronisk identifiering ska uppfylla kraven i den genomförandeakt som avses i artikel 12.8.

Artikel 8

Tillitsnivåer för system för elektronisk identifiering

1. I ett system för elektronisk identifiering som anmälts i enlighet med artikel 9.1 ska tillitsnivåerna låg, väsentlig och/eller hög specificeras för medel för elektronisk identifiering som har utfärdats inom det systemet.

2. Tillitsnivåerna låg, väsentlig och hög ska uppfylla följande kriterier för respektive nivå:

a) Tillitsnivå låg ska inom ramen för ett system för elektronisk identifiering avse ett medel för elektronisk identifiering som ger en begränsad grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet, och definieras med hänvisning till tekniska specifikationer, standarder och förfaranden som avser detta, inbegripet tekniska kontroller, vilkas syfte är att väsentligt minska risken för missbruk eller ändring av identiteten.

b) Tillitsnivå väsentlig ska inom ramen för ett system för elektronisk identifiering avse ett medel för elektronisk identifiering som ger en väsentlig grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet, och definieras med hänvisning till tekniska specifikationer, standarder och förfaranden som avser detta, inbegripet tekniska kontroller, vilkas syfte är att väsentligt minska risken för missbruk eller ändring av identiteten.

c) Tillitsnivå hög ska inom ramen för ett system för elektronisk identifiering avse ett medel för elektronisk identifiering som ger en högre grad av tillförlitlighet avseende en persons påstådda eller styrkta identitet än tillitsnivån väsentlig, och definieras med hänvisning till tekniska specifikationer, standarder och förfaranden som avser detta, inbegripet tekniska kontroller, vilkas syfte är att förhindra risken för missbruk eller ändring av identiteten.

3. Senast den 18 september 2015, med beaktande av relevanta internationella standarder, och om inte annat följer av punkt 2, ska kommissionen genom genomförandeakter fastställa tekniska minimispecifikationer, standarder och förfaranden genom vilka tillitsnivåerna låg, väsentlig och hög specificeras för medel för elektronisk identifiering för tillämpningen av punkt 1.

Dessa tekniska minimispecifikationer, standarder och förfaranden ska fastställas med hänvisning till tillförlitligheten och kvaliteten i följande delar:

a) Förfarandet för att styrka och kontrollera identiteten på fysiska eller juridiska personer som ansöker om utfärdande av medel för elektronisk identifiering.

b) Förfarandet för att utfärda det begärda medlet för elektronisk identifiering.

c) Den autentiseringsmekanism genom vilken den fysiska eller juridiska personen använder medlet för elektronisk identifiering för att bekräfta sin identitet för en förlitande part.

d) Den enhet som utfärdar medlen för elektronisk identifiering.

e) Varje annat organ som deltar i ansökningen om utfärdande av medel för elektronisk identifiering.

f) De tekniska och säkerhetsrelaterade specifikationerna för de utfärdade medlen för elektronisk identifiering.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 9

Anmälan

1. Den anmälande medlemsstaten ska till kommissionen anmäla följande uppgifter samt utan onödigt dröjsmål anmäla eventuella senare ändringar av dessa:

a) En beskrivning av systemet för elektronisk identifiering, inbegripet dess tillitsnivåer och av utfärdaren eller utfärdarna av medel för elektronisk identifiering inom systemet.

b) Det tillämpliga systemet för tillsyn och information om systemet för skadeståndsansvar med avseende på följande:

i) Den part som utfärdar medlet för elektronisk identifiering.

ii) Den part som handhar autentiseringsförfarandet.

c) Den myndighet eller de myndigheter som ansvarar för systemet för elektronisk identifiering.

d) Information om den enhet eller de enheter som hanterar registreringen av de unika personidentifieringsuppgifterna.

e) En beskrivning av hur kraven i den genomförandeakt som avses i artikel 12.8 har uppfyllts.

f) En beskrivning av den autentisering som avses i artikel 7 f.

g) System för tillfälligt upphävande eller återkallelse av det anmälda systemet för elektronisk identifiering eller autentisering eller av de berörda utsatta delarna.

2. Kommissionen ska ett år från dagen för tillämpning av de genomförandeakter som avses i artiklarna 8.3 och 12.8 offentliggöra en förteckning över de system för elektronisk identifiering som anmälts enligt punkt 1 i den här artikeln och de grundläggande uppgifterna om dessa i *Europeiska unionens officiella tidning*.

3. Om kommissionen tar emot en anmälan efter utgången av den period som avses i punkt 2 ska den i *Europeiska unionens officiella tidning* offentliggöra ändringarna i den förteckning som avses i punkt 2 inom två månader från den dag då anmälan mottogs.

4. En medlemsstat får lämna in en begäran till kommissionen om att ta bort ett system för elektronisk identifiering som anmälts av medlemsstaten från den förteckning som avses i punkt 2. Kommissionen ska offentliggöra motsvarande ändringar i förteckningen i *Europeiska unionens officiella tidning* inom en månad från den dag då medlemsstatens begäran mottogs.

5. Kommissionen får genom genomförandeakter fastställa förutsättningar, format och förfaranden för de anmälningar som avses i punkt 1. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 10

Säkerhetsincidenter

1. Om antingen det system för elektronisk identifiering som anmälts i enlighet med artikel 9.1 eller den autentisering som avses i artikel 7 f utsätts för intrång eller delvis äventyras på ett sätt som påverkar tillförlitligheten i systemets gränsöverskridande autentisering ska den anmälande medlemsstaten utan dröjsmål tillfälligt upphäva eller återkalla denna gränsöverskridande autentisering eller de berörda utsatta delarna och informera andra medlemsstater och kommissionen.

2. När en incident eller ett äventyrande som avses i punkt 1 har åtgärdats ska den anmälande medlemsstaten återinföra den gränsöverskridande autentiseringen och utan onödigt dröjsmål informera andra medlemsstater och kommissionen om detta.

3. Om en incident eller ett äventyrande som avses i punkt 1 inte åtgärdas inom tre månader från det tillfälliga upphävandet eller återkallelsen, ska den anmälande medlemsstaten till övriga medlemsstater och kommissionen anmäla att systemet för elektronisk identifiering har dragits tillbaka.

Kommissionen ska utan onödigt dröjsmål offentliggöra motsvarande ändringar i den förteckning som avses i artikel 9.2 i *Europeiska unionens officiella tidning*.

Artikel 11

Skadeståndsansvar

1. Den anmälande medlemsstaten ska ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom dess underlåtenhet att uppfylla sina skyldigheter enligt artikel 7 d och f vid en gränsöverskridande transaktion.

2. Den part som utfärdat medlet för elektronisk identifiering ska ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla den skyldighet som avses i artikel 7 e vid en gränsöverskridande transaktion.

3. Den part som handhar autentiseringsförfarandet ska ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att säkerställa korrekt handhavande av den autentisering som avses i artikel 7 f vid en gränsöverskridande transaktion.

4. Punkterna 1, 2 och 3 ska tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar.

5. Punkterna 1, 2 och 3 påverkar inte det skadeståndsansvar enligt nationell rätt som gäller för parter i en transaktion där de använda medlen för elektronisk identifiering omfattas av det system för elektronisk identifiering som anmälts i enlighet med artikel 9.1.

Artikel 12

Samarbete och interoperabilitet

1. De nationella system för elektronisk identifiering som anmälts i enlighet med artikel 9.1 ska vara interoperabla.

2. Med avseende på tillämpningen av punkt 1 ska ett interoperabilitetsramverk fastställas.

3. Interoperabilitetsramverket ska uppfylla följande kriterier:

a) Det ska ha som mål att vara teknikneutralt och ska inte diskriminera mellan särskilda nationella tekniska lösningar för elektronisk identifiering i en medlemsstat.

b) Det ska, när det är möjligt, följa europeiska och internationella standarder.

c) Det ska främja tillämpningen av principen om ett inbyggt integritetsskydd.

d) Det ska säkerställa att personuppgifter behandlas i enlighet med direktiv 95/46/EG.

4. Interoperabilitetsramverket ska bestå av följande:

a) Hänvisning till tekniska minimikrav avseende tillitsnivåerna i artikel 8.

b) Sammankoppling av nationella tillitsnivåer för anmälda system för elektronisk identifiering med tillitsnivåerna enligt artikel 8.

c) Hänvisning till tekniska minimikrav för interoperabilitet.

d) Hänvisning till en minimuppsättning personidentifieringsuppgifter som är unika för en fysisk eller juridisk person och som är tillgänglig via system för elektronisk identifiering.

e) Förfaranderegler.

f) Arrangemang för tvistlösning.

g) Gemensamma standarder för driftsäkerhet.

5. Medlemsstaterna ska samarbeta med avseende på följande:

a) Interoperabiliteten i de system för elektronisk identifiering som anmälts enligt artikel 9.1 och de system för elektronisk identifiering som medlemsstaterna avser att anmäla.

b) Säkerheten i systemen för elektronisk identifiering.

6. Samarbetet mellan medlemsstaterna ska bestå av följande:

a) Utbyte av information, erfarenhet och god praxis när det gäller system för elektronisk identifiering och särskilt i fråga om tekniska krav avseende interoperabilitet och tillitsnivåer.

b) Utbyte av information, erfarenheter och god praxis när det gäller arbete med tillitsnivåer för system för elektronisk identifiering enligt artikel 8.

c) Sakkunnigbedömning av system för elektronisk identifiering som omfattas av denna förordning.

d) Bedömning av relevant utveckling inom sektorn för elektronisk identifiering.

7. Senast den 18 mars 2015 ska kommissionen genom genomförandeakter fastställa nödvändiga förfaranden för att underlätta det samarbete mellan medlemsstaterna som avses i punkterna 5 och 6 i syfte att främja en hög nivå av förtroende och säkerhet som står i proportion till risknivån.

8. Senast den 18 september 2015 ska kommissionen, i enlighet med de kriterier som fastställs i punkt 3 och med beaktande av resultaten av samarbetet mellan medlemsstaterna, för att fastställa enhetliga villkor för tillämpningen av kraven i punkt 1 anta genomförandeakter om det interoperabilitetsramverk som anges i punkt 4.

9. De genomförandeakter som avses i punkterna 7 och 8 i denna artikel ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

KAPITEL III

BETRODDA TJÄNSTER

AVSNITT 1

Allmänna bestämmelser

Artikel 13

Skadeståndsansvar och bevisbörda

1. Utan att det påverkar tillämpningen av punkt 2 ska tillhandahållare av betrodda tjänster ha skadeståndsansvar för skada som åsamkats en fysisk eller juridisk person avsiktligt eller på grund av oaktsamhet genom underlåtenhet att uppfylla kraven i denna förordning.

Bevisbördan för avsikt eller oaktsamhet hos en icke-kvalificerad tillhandahållare av betrodda tjänster ska vila på den fysiska eller juridiska person som gör gällande sådan skada som avses i första stycket.

Avsikt eller oaktsamhet hos en kvalificerad tillhandahållare av betrodda tjänster ska anses föreligga såvida inte en kvalificerad tillhandahållare av betrodda tjänster bevisar att den skada som avses i första stycket har uppstått utan avsikt eller oaktsamhet hos den kvalificerade tillhandahållaren av betrodda tjänster.

2. Om en tillhandahållare av betrodda tjänster vederbörligen informerar sina kunder i förväg om de begränsningar som gäller för användningen av de tjänster de tillhandahåller och dessa begränsningar är möjliga för tredje man att ta del av, ska tillhandahållarna av betrodda tjänster inte ha skadeståndsansvar för skador som uppstår vid sådan användning av tjänster som överskrider de angivna begränsningarna.

3. Punkterna 1 och 2 ska tillämpas i enlighet med nationella bestämmelser om skadeståndsansvar.

Artikel 14

Internationella aspekter

1. Betrodda tjänster som tillhandahålls av tillhandahållare av betrodda tjänster som är etablerade i ett tredjeland ska erkännas som rättsligt likvärdiga med kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen, under förutsättning att de betrodda tjänsterna från tredjelandet är erkända enligt ett avtal som ingåtts mellan unionen och det berörda tredjelandet eller en internationell organisation i enlighet med artikel 218 i EUF-fördraget.

2. Avtal som avses i punkt 1 ska särskilt säkerställa att

a) de krav som är tillämpliga på kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen och de kvalificerade betrodda tjänster som de tillhandahåller uppfylls av tillhandahållarna av betrodda tjänster i det tredjeland eller den internationella organisation med vilket eller vilken avtalet ingås och av de betrodda tjänster som de tillhandahåller,

b) de kvalificerade betrodda tjänster som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster som är etablerade inom unionen erkänns som rättsligt likvärdiga med betrodda tjänster som tillhandahålls av tillhandahållare av betrodda tjänster i det tredjeland eller den internationella organisation med vilket eller vilken avtalet ingås.

Artikel 15

Tillgänglighet för personer med funktionshinder

När det är genomförbart ska betrodda tjänster som tillhandahålls och slutanvändarprodukter som används i samband med tillhandahållandet av dessa tjänster göras tillgängliga för personer med funktionshinder.

Artikel 16

Sanktioner

Medlemsstaterna ska fastställa bestämmelser om de sanktioner som ska tillämpas vid överträdelser av denna förordning. Sanktionerna ska vara effektiva, proportionella och avskräckande.

AVSNITT 2

Tillsyn

Artikel 17

Tillsynsorgan

1. Medlemsstaterna ska utse ett tillsynsorgan som är etablerat inom deras territorium eller, efter ömsesidig överenskommelse med en annan medlemsstat, ett tillsynsorgan som är etablerat i den andra medlemsstaten. Det organet ska ansvara för tillsynsuppgifter i den medlemsstat som utsett organet.

Tillsynsorgan ska tilldelas nödvändiga befogenheter och adekvata resurser för utövande av sina uppgifter.

2. Medlemsstaterna ska meddela kommissionen namn på och adress till sina respektive utsedda tillsynsorgan.

3. Tillsynsorganet ska ha följande roll:

a) Utöva tillsyn över kvalificerade tillhandahållare av betrodda tjänster som är etablerade i den medlemsstat där de har utsetts för att genom tillsynsverksamhet på förhand och i efterhand se till att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning.

b) Vid behov vidta åtgärder avseende icke-kvalificerade tillhandahållare av betrodda tjänster som är etablerade i den medlemsstat där de har utsetts genom tillsynsverksamhet i efterhand om de tar del av påståenden att dessa icke-kvalificerade tillhandahållare av betrodda tjänster eller de betrodda tjänster som de tillhandahåller inte uppfyller kraven i denna förordning.

4. Vid tillämpningen av punkt 3 och med förbehåll för de begränsningar som anges däri ska tillsynsorganets uppgifter särskilt innefatta följande:

a) Samarbete med andra tillsynsorgan och bistånd till dem i enlighet med artikel 18.

b) Analys av de rapporter om överensstämmelsebedömning som avses i artiklarna 20.1 och 21.1.

c) Information till andra tillsynsorgan samt allmänheten om säkerhetsincidenter eller integritetsförluster i enlighet med artikel 19.2.

d) Rapportering till kommissionen om sin huvudverksamhet i enlighet med punkt 6 i denna artikel.

e) Granskningsverksamhet eller framställningar till ett organ för bedömning av överensstämmelse om att detta ska göra en överensstämmelsebedömning av kvalificerade tillhandahållare av betrodda tjänster i enlighet med artikel 20.2.

f) Samarbete med dataskyddsmyndigheterna, främst genom att utan onödigt dröjsmål informera dem om resultatet av granskningar av kvalificerade tillhandahållare av betrodda tjänster, när det förefaller ha skett en överträdelse av reglerna för skydd för personuppgifter.

g) Beviljande av status som kvalificerad tillhandahållare av betrodda tjänster och till de tjänster som de tillhandahåller samt återkallande av denna status i enlighet med artiklarna 20 och 21.

h) Information till det organ som är ansvarigt för den nationella förteckning över betrodda tjänsteleverantörer som avses i artikel 22.3 om sina beslut om beviljande eller återkallande av status som kvalificerad, såvida inte det organet även är tillsynsorganet.

i) Kontroll av befintlighet och korrekt tillämpning av bestämmelser om planer för verksamhetens upphörande i sådana fall när den kvalificerade tillhandahållaren av betrodda tjänster upphör med sin verksamhet, inbegripet hur information hålls tillgänglig i enlighet med artikel 24.2 h.

j) Åläggande av krav på tillhandahållare av betrodda tjänster att åtgärda varje underlåtenhet att uppfylla kraven i denna förordning.

5. Medlemsstaterna får kräva att tillsynsorganet ska inrätta, underhålla och uppdatera en infrastruktur för betrodda tjänster i enlighet med villkoren i nationell rätt.

6. Senast den 31 mars varje år ska varje tillsynsorgan till kommissionen överlämna en rapport om det föregående kalenderårets huvudverksamhet tillsammans med en sammanfattning av överträdelseanmälningar som har inkommit från tillhandahållare av betrodda tjänster i enlighet med artikel 19.2.

7. Kommissionen ska göra den årsrapport som avses i punkt 6 tillgänglig för medlemsstaterna.

8. Kommissionen får genom genomförandeakter fastställa format och förfaranden för den rapport som avses i punkt 6. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 18

Ömsesidigt bistånd

1. Tillsynsorganen ska samarbeta med sikte på att utbyta god praxis.

Ett tillsynsorgan ska, efter att ha mottagit en motiverad begäran från ett annat tillsynsorgan, ge det organet bistånd så att deras åtgärder kan vidtas på ett enhetligt sätt. Det ömsesidiga biståndet kan bland annat omfatta begäranden om information och tillsynsåtgärder, t.ex. begäranden om att utföra inspektioner avseende de rapporter om överensstämmelsebedömning som avses i artiklarna 20 och 21.

2. Ett tillsynsorgan som tar emot en begäran om bistånd får vägra att tillmötesgå denna begäran på grundval av något av följande skäl:

a) Tillsynsorganet är inte behörigt att tillhandahålla det bistånd som begärs.

b) Det begärda biståndet står inte i proportion till den tillsynsverksamhet som tillsynsorganet utför i enlighet med artikel 17.

c) Det skulle stå i strid med denna förordning att tillhandahålla det begärda biståndet.

3. Där så är lämpligt får medlemsstaterna bemyndiga sina respektive tillsynsorgan att vidta gemensamma åtgärder där personal från andra medlemsstaters tillsynsorgan deltar. De berörda medlemsstaterna ska besluta om och inrätta arrangemangen och förfarandena för sådana gemensamma åtgärder i enlighet med sin nationella rätt.

Artikel 19

Säkerhetskrav på tillhandahållare av betrodda tjänster

1. Kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster som de tillhandahåller. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa att säkerhetsnivån står i proportion till graden av risk. I synnerhet ska åtgärder vidtas för att förhindra eller minimera säkerhetsincidenters inverkan samt för att informera berörda parter om de negativa effekterna av eventuella sådana incidenter.

2. Kvalificerade och icke kvalificerade tillhandahållare av betrodda tjänster ska, utan otillbörligt dröjsmål och under alla omständigheter inom 24 timmar efter upptäckt, underrätta tillsynsorganet och i förekommande fall andra relevanta organ, såsom det behöriga nationella organet för informationssäkerhet eller dataskyddsmyndigheten, om alla säkerhetsincidenter eller integritetsförluster som i betydande omfattning påverkar den betrodda tjänst som tillhandahålls eller på de personuppgifter som ingår i denna.

När det är troligt att säkerhetsincidenten eller integritetsförlusten kommer att ha negativ inverkan på en fysisk eller juridisk person till vilken den betrodda tjänsten har tillhandahållits, ska tillhandahållaren av betrodda tjänster utan onödigt dröjsmål även underrätta den fysiska eller juridiska personen om säkerhetsincidenten eller integritetsförlusten.

När så är lämpligt, särskilt om säkerhetsincidenten eller integritetsförlusten rör två eller flera medlemsstater, ska det underrättade tillsynsorganet informera tillsynsorganen i övriga berörda medlemsstater samt Enisa.

Det underrättade tillsynsorganet ska informera allmänheten eller kräva att tillhandahållaren av betrodda tjänster gör det, om den slår fast att ett avslöjande av säkerhetsincidenten eller integritetsförlusten ligger i allmänhetens intresse.

3. Tillsynsorganet ska en gång om året till Enisa överlämna en sammanfattning av de anmälningar om säkerhetsincidenter eller som inkommit från tillhandahållare av betrodda tjänster.

4. Kommissionen får, genom genomförandeakter,

a) ytterligare specificera de åtgärder som avses i punkt 1, och

b) fastställa format och förfaranden, inklusive tidsfrister, som ska vara tillämpliga för de ändamål som avses i punkt 2.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 3

Kvalificerade betrodda tjänster

Artikel 20

Tillsyn över kvalificerade tillhandahållare av betrodda tjänster

1. Kvalificerade tillhandahållare av betrodda tjänster ska minst en gång vartannat år och på egen bekostnad granskas av ett organ för bedömning av överensstämmelse. Syftet med denna granskning ska vara att bekräfta att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning. De kvalificerade tillhandahållarna av betrodda tjänster ska lämna in den resulterande rapporten om överensstämmelsebedömning till tillsynsorganet inom en period av tre arbetsdagar efter mottagande av denna.

2. Tillsynsorganet får, utan att det påverkar tillämpningen av punkt 1, när som helst granska eller begära att ett organ för bedömning av överensstämmelse gör en överensstämmelsebedömning av de kvalificerade tillhandahållarna av betrodda tjänster på dessa tillhandahållare av betrodda tjänsters egen bekostnad för att bekräfta att dessa och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i denna förordning. Vid misstänkta överträdelser av reglerna om skydd för personuppgifter ska tillsynsorganet informera dataskyddsmyndigheterna om sina granskningsresultat.

3. När tillsynsorganet begär att den kvalificerade tillhandahållaren av betrodda tjänster ska åtgärda en underlåtenhet att uppfylla kraven i denna förordning och när tillhandahållaren inte gör detta, och i tillämpliga fall inom den tidsfrist som fastställts av tillsynsorganet, får tillsynsorganet med beaktande av i synnerhet underlåtenhetens omfattning, varaktighet och följder återkalla den tillhandahållarens eller den berörda tillhandahållna tjänstens status som kvalificerad samt informera det organ som avses i artikel 22.3 för att de förteckningar över betrodda tjänsteleverantörer som avses i artikel 22.1 ska kunna uppdateras. Tillsynsorganet ska informera den kvalificerade tillhandahållaren av betrodda tjänster om återkallandet av dess eller den berörda tjänstens status som kvalificerad.

4. Kommissionen får genom genomförandeakter fastställa referensnummer till följande standarder:

a) Ackreditering av organ för bedömning av överensstämmelse och för den rapport om överensstämmelsebedömning som avses i punkt 1.

b) Granskningsregler som organen för bedömning av överensstämmelse ska följa vid sina överensstämmelsebedömningar av kvalificerade tillhandahållare av betrodda tjänster som avses i punkt 1.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 21

Igångsättande av en kvalificerad betrodd tjänst

1. När tillhandahållare av betrodda tjänster som inte har status som kvalificerade har för avsikt att börja tillhandahålla kvalificerade betrodda tjänster, ska de anmäla sin avsikt till tillsynsorganet och samtidigt lämna in en rapport om överensstämmelsebedömning som utfärdats av ett organ för bedömning av överensstämmelse.

2. Tillsynsorganet ska kontrollera huruvida tillhandahållaren av betrodda tjänster och de betrodda tjänster som denne tillhandahåller uppfyller kraven i denna förordning, och i synnerhet kraven för kvalificerade tillhandahållare av betrodda tjänster och för de kvalificerade betrodda tjänster som de tillhandahåller.

Om tillsynsorganet kommer fram till att tillhandahållaren av betrodda tjänster och de betrodda tjänster som denne tillhandahåller uppfyller de krav som avses i första stycket, ska det bevilja status som kvalificerad till tillhandahållare av betrodda tjänster och de betrodda tjänster som denne tillhandahåller samt informera det organ som avses i artikel 22.3 för att de förteckningar över betrodda tjänsteleverantörer som avses i artikel 22.1 ska kunna uppdateras, senast tre månader efter anmälan i enlighet med punkt 1 i denna artikel.

Om kontrollen inte har slutförts inom tre månader från anmälan, ska tillsynsorganet informera tillhandahållaren av betrodda tjänster om detta och ange orsakerna till förseningen samt när kontrollen beräknas vara slutförd.

3. Kvalificerade tillhandahållare av betrodda tjänster får börja tillhandahålla den kvalificerade betrodda tjänsten efter det att status som kvalificerad har angetts i de förteckningar över betrodda tjänsteleverantörer som avses i artikel 22.1.

4. Kommissionen får genom genomförandeakter fastställa 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 48.2.

Artikel 22

Förteckningar över betrodda tjänsteleverantörer

1. Varje medlemsstat ska upprätta, underhålla och offentliggöra förteckningar med uppgifter om kvalificerade tillhandahållare av betrodda tjänster som den ansvarar för, 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 som avses i 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, de 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. Senast den 18 september 2015 ska kommissionen genom genomförandeakter ange den information som avses i punkt 1 och 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 48.2.

Artikel 23

EU-förtroendemärke för kvalificerade betrodda tjänster

1. Efter det att den kvalificerade status som avses i artikel 21.2 andra stycket har angetts i den förteckning över betrodda tjänsteleverantörer som avses i artikel 22.1, får kvalificerade tillhandahållare av betrodda tjänster använda sig av EU-förtroendemärket för att på ett enkelt, igenkännligt och tydligt sätt ange de kvalificerade betrodda tjänster som de tillhandahåller.

2. Vid användning av det EU-förtroendemärke som avses i punkt 1 ska kvalificerade tillhandahållare av betrodda tjänster se till att en länk till den relevanta förteckningen över betrodda tjänsteleverantörer finns på deras webbplats.

3. Senast den 1 juli 2015 ska kommissionen genom genomförandeakter fastställa specifikationer med avseende på formatet för EU-förtroendemärket för kvalificerade betrodda tjänster och särskilt för dess presentation, sammansättning, storlek och utformning. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 24

Krav på kvalificerade tillhandahållare av betrodda tjänster

1. En kvalificerad tillhandahållare av betrodda tjänster ska, när den utfärdar ett kvalificerat certifikat för en betrodd tjänst, på lämpligt sätt och i enlighet med nationell rätt kontrollera identiteten och i förekommande fall eventuella särskilda attribut för den fysiska eller juridiska person till vilken det kvalificerade certifikatet utfärdas.

Den information som avses i första stycket ska kontrolleras av den kvalificerade tillhandahållaren av betrodda tjänster antingen direkt eller via tredje man i enlighet med nationell rätt på något av följande sätt:

a) Genom fysisk närvaro av den fysiska personen eller av en behörig företrädare för den juridiska personen.

b) På distans, med hjälp av medel för elektronisk identifiering, där en fysisk närvaro av den fysiska personen eller en behörig företrädare för den juridiska personen vid tidpunkt före utfärdandet av det kvalificerade certifikatet säkerställs och som uppfyller kraven i artikel 8 när det gäller tillitsnivåerna väsentlig eller hög.

c) Genom ett certifikat för en kvalificerad elektronisk underskrift eller en kvalificerad elektronisk stämpel som utfärdats i enlighet med led a eller b.

d) Med hjälp av andra identifieringsmetoder som erkänns på nationell nivå och som erbjuder garantier som är likvärdiga med fysisk närvaro. Likvärdiga garantier ska bekräftas av ett organ för bedömning av överensstämmelse.

2. En kvalificerad tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade betrodda tjänster ska

a) informera tillsynsorganet om alla ändringar av tillhandahållandet av dess kvalificerade betrodda tjänster, och om den har för avsikt att upphöra med denna verksamhet,

b) ha personal, och i förekommande fall underleverantörer, som har den sakkunskap, den tillförlitlighet samt de erfarenheter och kvalifikationer som behövs och som har genomgått lämplig utbildning om regler för säkerhet och skydd för personuppgifter och ska tillämpa förfaranden för administration och förvaltning som överensstämmer med europeiska eller internationella standarder,

c) när det gäller risken för ansvar vid skador i enlighet med artikel 13 förfoga över tillräckliga ekonomiska medel och/eller skaffa sig lämplig ansvarsförsäkring i enlighet med nationell rätt,

d) innan den ingår ett avtalsförhållande på ett tydligt och uttömmande sätt informera de personer som vill använda en kvalificerad betrodd tjänst om de exakta villkor som gäller för användning av den tjänsten, inbegripet om eventuella begränsningar av användningen,

e) använda tillförlitliga system och produkter som är skyddade mot ändringar och säkerställa den tekniska säkerheten och tillförlitligheten hos den process som stöds av dessa,

f) använda tillförlitliga system för att lagra uppgifter som har lämnats till den, i en form som kan kontrolleras så att

i) de är offentligt tillgängliga för hämtning endast i de fall där samtycke från den person som uppgifterna rör har erhållits,

ii) endast behöriga personer kan föra in uppgifter och göra ändringar i de lagrade uppgifterna, och

iii) uppgifternas äkthet kan kontrolleras,

g) vidta lämpliga åtgärder mot förfalskning och stöld av uppgifter,

h) under en lämplig tidsperiod registrera och hålla tillgänglig, även efter det att den kvalificerade tillhandahållaren av betrodda uppgifter har upphört med sin verksamhet, all relevant information om uppgifter som den kvalificerade tillhandahållaren av betrodda tjänster har utfärdat och tagit emot, särskilt för att vid rättsliga förfaranden kunna lägga fram bevis och för att säkerställa tjänstens kontinuitet; registreringen får göras elektroniskt,

i) ha en uppdaterad plan för verksamhetens upphörande i syfte att säkerställa tjänstens kontinuitet i enlighet med bestämmelser som kontrollerats av tillsynsorganet i enlighet med artikel 17.4 i,

j) säkerställa laglig behandling av personuppgifter i enlighet med direktiv 95/46/EG,

k) då det är fråga om kvalificerade tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat, upprätta och uppdatera en certifikatdatabas,

3. Om en kvalificerad tillhandahållare av betrodda tjänster som utfärdar kvalificerade certifikat beslutar att återkalla ett certifikat, ska den registrera ett sådant återkallande i sin certifikatdatabas och offentliggöra återkallandet av statusen för certifikatet i god tid och i alla händelser inom 24 timmar efter mottagandet av begäran. Återkallandet ska få verkan omedelbart efter offentliggörandet.

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

5. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för tillförlitliga system och produkter, vilka uppfyller kraven i punkt 2 e och f i denna artikel. Överensstämmelse med kraven i denna artikel ska förutsättas när tillförlitliga system och produkter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 4

Elektroniska underskrifter

Artikel 25

Rättslig verkan av elektroniska underskrifter

1. En elektronisk underskrift får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att underskriften har elektronisk form eller inte uppfyller kraven för kvalificerade elektroniska underskrifter.

2. En kvalificerad elektronisk underskrift ska ha motsvarande rättsliga verkan som en handskriven underskrift.

3. En kvalificerad elektronisk underskrift som är baserad på ett kvalificerat certifikat som utfärdats i en medlemsstat ska erkännas som en kvalificerad elektronisk underskrift i alla andra medlemsstater.

Artikel 26

Krav med avseende på avancerade elektroniska underskrifter

En avancerad elektronisk underskrift ska uppfylla följande krav:

a) Den ska vara unikt knuten till undertecknaren.

b) Undertecknaren ska kunna identifieras genom den.

c) Den ska vara skapad på grundval av uppgifter för skapande av elektroniska underskrifter som undertecknaren med hög grad av tillförlitlighet kan använda uteslutande under sin egen kontroll.

d) Den ska vara kopplad till de uppgifter som den används för att underteckna på ett sådant sätt att alla efterföljande ändringar av uppgifterna kan upptäckas.

Artikel 27

Elektroniska underskrifter i offentliga tjänster

1. Om en medlemsstat kräver en avancerad elektronisk underskrift för användningen av en nättjänst som erbjuds av ett offentligt organ eller på ett offentligt organs vägnar, ska medlemsstaten erkänna avancerade elektroniska underskrifter, avancerade elektroniska underskrifter som är baserade på ett kvalificerat certifikat för elektroniska underskrifter och kvalificerade elektroniska underskrifter i åtminstone de format eller med de metoder som anges i de genomförandeakter som avses i punkt 5.

2. Om en medlemsstat kräver en avancerad elektronisk underskrift som är baserad på ett kvalificerat certifikat för användningen av en nättjänst som erbjuds av ett offentligt organ eller på ett offentligt organs vägnar, ska medlemsstaten erkänna avancerade elektroniska underskrifter som är baserade på ett kvalificerat certifikat och kvalificerade elektroniska underskrifter i åtminstone de format eller med de metoder som anges i de genomförandeakter som avses i punkt 5.

3. Medlemsstaterna ska för gränsöverskridande användning av nättjänster som erbjuds av ett offentligt organ inte kräva en elektronisk underskrift med en högre säkerhetsnivå än den som gäller för kvalificerade elektroniska underskrifter.

4. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för avancerade elektroniska underskrifter. Överensstämmelse med de krav på avancerade elektroniska underskrifter som avses i punkterna 1 och 2 i denna artikel samt i artikel 26 ska förutsättas när en avancerad elektronisk underskrift uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

5. Kommissionen ska senast den 18 september 2015 och med beaktande av befintliga rutiner, standarder och unionsrättsakter, genom genomförandeakter, fastställa referensformat för avancerade elektroniska underskrifter eller referensmetoder i de fall alternativa format används. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 28

Kvalificerade certifikat för elektroniska underskrifter

1. Kvalificerade certifikat för elektroniska underskrifter ska uppfylla kraven i bilaga I.

2. Kvalificerade certifikat för elektroniska underskrifter ska inte omfattas av några obligatoriska krav som går utöver kraven i bilaga I.

3. Kvalificerade certifikat för elektroniska underskrifter får omfatta extra, icke-obligatoriska, särskilda attribut. Dessa attribut ska inte påverka kvalificerade elektroniska underskrifters kompatibilitet eller erkännande.

4. Om ett kvalificerat certifikat för elektroniska underskrifter har återkallats efter den ursprungliga aktiveringen, ska det förlora sin giltighet från och med tidpunkten för återkallandet, och dess status som giltigt ska inte under några omständigheter återgå.

5. På följande villkor får medlemsstaterna fastställa nationella bestämmelser för tillfälligt upphävande av ett kvalificerat certifikat för elektroniska underskrifter:

a) Om ett kvalificerat certifikat för en elektronisk underskrift tillfälligt har upphävts, ska certifikatet vara ogiltigt under tiden för det tillfälliga upphävandet.

b) Perioden för det tillfälliga upphävandet ska tydligt anges i certifikatdatabasen och certifikatets status som tillfälligt upphävt ska under perioden för det tillfälliga upphävandet vara synlig genom den tjänst som tillhandahåller information om certifikatets status.

6. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för elektroniska underskrifter. Överensstämmelse med kraven i bilaga I ska förutsättas när ett kvalificerat certifikat för elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 29

Krav på anordningar för skapande av kvalificerade elektroniska underskrifter

1. Anordningar för skapande av kvalificerade elektroniska underskrifter ska uppfylla kraven i bilaga II.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för anordningar för skapande av kvalificerade elektroniska underskrifter. Överensstämmelse med kraven i bilaga II ska förutsättas när en anordning för skapande av kvalificerade elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 30

Certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter

1. Lämpliga offentliga eller privata organ som utsetts av medlemsstaterna ska certifiera att anordningar för skapande av kvalificerade elektroniska underskrifter överensstämmer med kraven i bilaga II.

2. Medlemsstaterna ska underrätta kommissionen om namnet på och adressen till det offentliga eller privata organ som avses i punkt 1. Kommissionen ska göra den informationen tillgänglig för medlemsstaterna.

3. Den certifiering som avses i punkt 1 ska bygga på något av följande:

a) Ett förfarande för säkerhetsutvärdering som utförts i enlighet med någon av de standarder för säkerhetsutvärdering av informationsteknikprodukter som finns med i den förteckning som fastställts i enlighet med andra stycket.

b) Ett annat förfarande än det som avses i led a, förutsatt att det omfattar jämförbara säkerhetsnivåer och att det offentliga eller privata organ som avses i punkt 1 underrättar kommissionen om förfarandet. Detta förfarande får endast användas vid avsaknad av sådana standarder som avses i led a eller medan en sådan säkerhetsutvärdering som avses i led a pågår.

Kommissionen ska genom genomförandeakter upprätta en förteckning över standarder för den säkerhetsbedömning av informationsteknikprodukter som avses i led a. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

4. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 47 rörande fastställandet av särskilda kriterier som ska uppfyllas av de utsedda organ som avses i punkt 1 i den här artikeln.

Artikel 31

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

1. Medlemsstaterna ska utan onödigt dröjsmål och senast en månad efter det att certifieringen slutförts till kommissionen lämna information om anordningar för skapande av kvalificerade elektroniska underskrifter som har certifierats av de organ som avses i artikel 30.1. De ska utan onödigt dröjsmål och senast en månad efter det att en certifiering har upphört att gälla även informera kommissionen om anordningar för skapande av elektroniska underskrifter som inte längre är certifierade.

2. Kommissionen ska på grundval av den information som inkommit upprätta, offentliggöra och underhålla en förteckning över certifierade anordningar för skapande av kvalificerade elektroniska underskrifter.

3. Kommissionen får genom genomförandeakter fastställa 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 48.2.

Artikel 32

Krav på validering av kvalificerade elektroniska underskrifter

1. Genom valideringsförfarandet för en kvalificerad elektronisk underskrift ska den kvalificerade elektroniska underskriftens giltighet bekräftas under förutsättning att

a) det certifikat som stöder underskriften vid tidpunkten för undertecknandet var ett kvalificerat certifikat för elektroniska underskrifter som överensstämmer med bilaga I,

b) det kvalificerade certifikatet har utfärdats av en kvalificerad tillhandahållare av betrodda tjänster och var giltigt vid tidpunkten för undertecknandet,

c) valideringsuppgifterna för underskriften överensstämmer med de uppgifter som lämnats till den förlitande parten,

d) certifikatets unika uppsättning uppgifter som avser undertecknaren har tillhandahållits den förlitande parten på rätt sätt,

e) användningen av en eventuell pseudonym tydligt har angetts för den förlitande parten om en pseudonym användes vid tidpunkten för undertecknandet,

f) den elektroniska underskriften har skapats med hjälp av en anordning för skapande av kvalificerade elektroniska underskrifter,

g) integriteten hos de undertecknade uppgifterna inte har äventyrats,

h) kraven i artikel 26 var uppfyllda vid tidpunkten för undertecknandet.

2. Det system som används för att validera den kvalificerade elektroniska underskriften ska ge den förlitande parten det korrekta resultatet av valideringsförfarandet och ska göra det möjligt för den förlitande parten att upptäcka eventuella problem som är relevanta för säkerheten.

3. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för validering av kvalificerade elektroniska underskrifter. Överensstämmelse med kraven i punkt 1 ska förutsättas när valideringen av kvalificerade elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 33

Kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter

1. En kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter får endast tillhandahållas av en kvalificerad tillhandahållare av betrodda tjänster som

a) tillhandahåller validering i enlighet med artikel 32.1, och

b) gör det möjligt för förlitande parter att erhålla resultaten av valideringsförfarandet på ett automatiskt sätt som är tillförlitligt, effektivt och försett med en avancerad elektronisk underskrift eller en avancerad elektronisk stämpel 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 ska förutsättas när valideringstjänsten för kvalificerade elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 34

Kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter

1. En kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter får endast tillhandahållas av en kvalificerad tillhandahållare av betrodda tjänster som använder förfaranden och tekniker som gör det möjligt att förlänga den kvalificerade elektroniska underskriftens tillförlitlighet utöver perioden för teknisk giltighet.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter. Överensstämmelse med kraven i punkt 1 ska förutsättas när systemen för de kvalificerade tjänsterna för bevarande av kvalificerade elektroniska underskrifter uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 5

Elektroniska stämplar

Artikel 35

Rättslig verkan av elektroniska stämplar

1. En elektronisk stämpel får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att det har elektronisk form eller att det inte uppfyller kraven för kvalificerade elektroniska stämplar.

2. En kvalificerad elektronisk stämpel ska omfattas av en presumtion om integritet hos de uppgifter som den kvalificerade elektroniska stämpeln är kopplad till och om att de har korrekt ursprung.

3. En kvalificerad elektronisk stämpel som är baserat på ett kvalificerat certifikat som har utfärdats i en medlemsstat ska erkännas som en kvalificerad elektronisk stämpel i alla andra medlemsstater.

Artikel 36

Krav med avseende på avancerade elektroniska stämplar

En elektronisk stämpel ska uppfylla följande krav:

a) Den ska vara knuten uteslutande till skaparen av stämpeln.

b) Skaparen av stämpeln ska kunna identifieras genom det.

c) Det ska vara skapat på grundval av uppgifter för skapande av elektroniska stämplar som stämpelns skapare med hög grad av tillförlitlighet under sin kontroll kan använda för skapande av elektroniska stämplar.

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

Artikel 37

Elektroniska stämplar i offentliga tjänster

1. Om en medlemsstat kräver en avancerad elektronisk stämpel för användningen av en nättjänst som erbjuds av ett offentligt organ eller för organets räkning ska medlemsstaten erkänna avancerade elektroniska stämplar, avancerade elektroniska stämplar som är baserade på ett kvalificerat certifikat för elektroniska stämplar och kvalificerade elektroniska stämplar i åtminstone de format eller med användning av de metoder som anges i de genomförandeakter som avses i punkt 5.

2. Om en medlemsstat kräver en avancerad elektronisk stämpel som är baserad på ett kvalificerat certifikat för användningen av en nättjänst som erbjuds av ett offentligt organ eller för organets räkning, ska medlemsstaten erkänna avancerade elektroniska stämplar som är baserade på ett kvalificerat certifikat och kvalificerade elektroniska stämplar i åtminstone de format eller med användning av de metoder som anges i de genomförandeakter som avses i punkt 5.

3. Medlemsstaterna ska för gränsöverskridande användning av en nättjänst som erbjuds av ett offentligt organ inte kräva en elektronisk stämpel på en högre säkerhetsnivå än den som gäller för den kvalificerade elektroniska stämpeln.

4. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för avancerade elektroniska stämplar. Överensstämmelse med de krav på avancerade elektroniska stämplar som avses i punkterna 1 och 2 i denna artikel samt i artikel 36 ska förutsättas när en avancerad elektronisk stämpel uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

5. Kommissionen ska senast den 18 september 2015, och med beaktande av befintliga rutiner, standarder och unionsrättsakter genom genomförandeakter fastställa referensformat för avancerade elektroniska stämplar eller referensmetoder i de fall alternativa format används. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 38

Kvalificerade certifikat för elektroniska stämplar

1. Kvalificerade certifikat för elektroniska stämplar ska uppfylla kraven i bilaga III.

2. Kvalificerade certifikat för elektroniska stämplar ska inte omfattas av några obligatoriska krav som går utöver kraven i bilaga III.

3. Kvalificerade certifikat för elektroniska stämplar får omfatta extra, icke-obligatoriska, särskilda attribut. Dessa attribut ska inte påverka kvalificerade elektroniska stämplars interoperabilitet eller erkännande.

4. Om ett kvalificerat certifikat för en elektronisk stämpel har återkallats efter den ursprungliga aktiveringen ska det förlora sin giltighet från och med tidpunkten för återkallandet och dess status ska inte under några omständigheter återgå.

5. På följande villkor får medlemsstaterna fastställa nationella bestämmelser för tillfälligt upphävande av kvalificerade certifikat för elektroniska stämplar:

a) Om ett kvalificerat certifikat för elektroniska stämplar tillfälligt har upphävts ska certifikatet vara ogiltigt under perioden för det tillfälliga upphävandet.

b) Perioden för det tillfälliga upphävandet ska tydligt anges i certifikatdatabasen och certifikatets status som tillfälligt upphävt ska under perioden för det tillfälliga upphävandet vara synlig genom den tjänst som tillhandahåller information om certifikatets status.

6. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för kvalificerade certifikat för elektroniska stämplar. Överensstämmelse med kraven i bilaga III ska förutsättas när ett kvalificerat certifikat för elektroniska stämplar uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

Artikel 39

Kvalificerade anordningar för skapande av elektroniska stämplar

1. Artikel 29 ska på motsvarande sätt gälla för kraven på kvalificerade anordningar för skapande av elektroniska stämplar.

2. Artikel 30 ska på motsvarande sätt gälla för certifieringen av kvalificerade anordningar för skapande av elektroniska stämplar.

3. Artikel 31 ska på motsvarande sätt gälla för offentliggörandet av en förteckning över certifierade kvalificerade anordningar för skapande av elektroniska stämplar.

Artikel 40

Validering och bevarande av kvalificerade elektroniska stämplar

Artiklarna 32, 33 och 34 ska på motsvarande sätt gälla för validering och bevarande av kvalificerade elektroniska stämplar.

AVSNITT 6

Elektroniska tidsstämplingar

Artikel 41

Rättslig verkan av elektroniska tidsstämplingar

1. En elektronisk tidsstämpling ska inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att den har elektronisk form eller inte uppfyller kraven för en kvalificerad elektronisk tidsstämpling.

2. En kvalificerad elektronisk tidsstämpling ska omfattas av en presumtion om korrekthet hos det datum och den tid som den anger och integritet hos de uppgifter som datumet och tiden är kopplade till.

3. En kvalificerad elektronisk tidsstämpling som utfärdats i en medlemsstat ska erkännas som en kvalificerad elektronisk tidsstämpling i alla medlemsstater.

Artikel 42

Krav på kvalificerade elektroniska tidsstämplingar

1. En kvalificerad elektronisk tidsstämpling ska uppfylla följande krav:

a) Den ska binda datumet och tiden till uppgifter så att möjligheten att uppgifterna ändras utan att det går att upptäcka rimligtvis kan uteslutas.

b) Den ska vara grundad på en korrekt tidskälla som är kopplad till samordnad universaltid.

c) Den ska vara undertecknad med hjälp av en avancerad elektronisk underskrift eller förseglad med en avancerad elektronisk stämpel från den kvalificerade tillhandahållaren av betrodda tjänster eller genom en likvärdig metod.

2. Kommissionen får genom genomförandeakter fastställa referensnummer till standarder för bindning av datum och tidpunkt till uppgifter och för korrekta tidskällor. Överensstämmelse med kraven i punkt 1 ska förutsättas när bindningen av datum och tidpunkt till uppgifter och den korrekta tidskällan uppfyller dessa standarder. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 48.2.

AVSNITT 7

Elektroniska tjänster för rekommenderade leveranser

Artikel 43

Rättslig verkan av elektroniska tjänster för rekommenderade leveranser

1. Uppgifter som sänds och tas emot genom en elektronisk tjänst för rekommenderade leveranser får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att de har elektronisk form eller inte uppfyller kraven på den kvalificerade elektroniska tjänsten för rekommenderade leveranser.

2. Uppgifter som sänds och tas emot genom en kvalificerad elektronisk tjänst för rekommenderade leveranser ska omfattas av en presumtion om uppgifternas integritet, om uppgifternas avsändande av den identifierade avsändaren, uppgifternas mottagande av den identifierade adressaten samt om riktigheten i det datum och den tidpunkt för avsändande och mottagande som anges i den kvalificerade elektroniska tjänsten för rekommenderade leveranser.

Artikel 44

Krav på kvalificerade elektroniska tjänster för rekommenderade leveranser

1. Kvalificerade elektroniska tjänster för rekommenderade leveranser ska uppfylla följande krav:

a) De ska tillhandahållas av en eller flera kvalificerade tillhandahållare av betrodda tjänster.

b) De ska med hög grad av tillförlitlighet säkerställa avsändarens identitet.

c) De ska säkerställa adressatens identitet innan uppgifterna levereras.

d) Avsändandet och mottagandet av uppgifter ska säkerställas genom en avancerad elektronisk underskrift eller en avancerad elektronisk stämpel från en kvalificerad tillhandahållare av betrodda tjänster på ett sätt som utesluter möjligheten att uppgifterna ändras utan att det går att upptäcka.

e) Eventuella ändringar av de uppgifter som behövs för att sända eller ta emot uppgifterna ska tydligt anges för uppgifternas avsändare och adressat.

f) Datumet och tidpunkten för avsändande, mottagande och eventuella ändringar av uppgifter måste anges genom en kvalificerad elektronisk tidsstämpling.

Om uppgifterna överförs mellan två eller flera kvalificerade tillhandahållare av betrodda tjänster ska kraven i leden a–f 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 48.2.

AVSNITT 8

Autentisering av webbplatser

Artikel 45

Krav på kvalificerade certifikat för autentisering av webbplatser

1. Kvalificerade certifikat för autentisering av webbplatser ska uppfylla kraven i bilaga IV.

2. 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 48.2.

KAPITEL IV

ELEKTRONISKA DOKUMENT

Artikel 46

Rättslig verkan av elektroniska dokument

Ett elektroniskt dokument får inte förvägras rättslig verkan eller giltighet som bevis vid rättsliga förfaranden enbart på grund av att det har elektronisk form.

KAPITEL V

DELEGERING AV BEFOGENHETER OCH GENOMFÖRANDEBESTÄMMELSER

Artikel 47

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 30.4 ska ges till kommissionen tills vidare från och med den 17 september 2014.

3. Den delegering av befogenhet som avses i artikel 30.4 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

5. En delegerad akt som antas enligt artikel 30.4 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 48

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté 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 49

Översyn

Kommissionen ska göra en översyn över denna förordnings tillämpning och rapportera resultaten till Europaparlamentet och rådet senast den 1 juli 2020. Kommissionen ska särskilt utvärdera huruvida det är lämpligt att ändra denna förordnings tillämpningsområde eller dess särskilda bestämmelser, som artiklarna 6, 7 f, 34, 43, 44 eller 45, med beaktande av den erfarenhet som erhållits vid tillämpningen av denna förordning samt den tekniska och rättsliga utvecklingen och marknadsutvecklingen.

Den rapport som avses i första stycket ska vid behov åtföljas av lagstiftningsförslag.

Dessutom ska kommissionen vart fjärde år efter den rapport som avses i första stycket lämna en rapport till Europaparlamentet och rådet om framstegen med att uppfylla målen för denna förordning.

Artikel 50

Upphävande

1. Direktiv 1999/93/EG ska upphöra att gälla med verkan från och med den 1 juli 2016.

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

Artikel 51

Övergångsbestämmelser

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

2. Kvalificerade certifikat som utfärdats till fysiska personer enligt direktiv 1999/93/EG ska anses som kvalificerade certifikat för elektroniska underskrifter enligt denna förordning till dess att de löper ut.

3. Tillhandahållare av en certifieringstjänst som utfärdar certifikat enligt direktiv 1999/93/EG ska lämna in en rapport om bedömning av överensstämmelse till tillsynsorganet så snart som möjligt och senast den 1 juli 2017. Fram till dess att denna rapport har inlämnats och tillsynsorganet har slutfört sin bedömning av den ska tillhandahållaren av certifieringstjänsten anses vara en kvalificerad tillhandahållare av betrodda tjänster enligt denna förordning.

4. Om en tillhandahållare av certifieringstjänster som utfärdar kvalificerade certifikat enligt direktiv 1999/93/EG inte lämnar in någon rapport om bedömning av överensstämmelse till tillsynsorganet inom den tidsfrist som avses i punkt 3 ska denna tillhandahållare av certifieringstjänster inte anses vara en kvalificerad tillhandahållare av betrodda tjänster enligt denna förordning från och med den 2 juli 2017.

Artikel 52

Ikraftträdande

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

2. Den ska tillämpas från och med den 1 juli 2016, med undantag för följande:

a) Artiklarna 8.3, 9.5, 12.2–12.9, 17.8, 19.4, 20.4, 21.4, 22.5, 23.3, 24.5, 27.4, 27.5, 28.6, 29.2, 30.3, 30.4, 31.3, 32.3, 33.2, 34.2, 37.4, 37.5, 38.6, 42.2, 44.2, 45.2, 47 och 48 ska tillämpas från och med den 17 september 2014.

b) Artiklarna 7, 8.1, 8.2, 9, 10, 11 och 12.1 ska tillämpas från och med tillämpningsdagen för de genomförandeakter som avses i artiklarna 8.3 och 12.8.

c) Artikel 6 ska tillämpas från och med tre år efter tillämpningsdagen för de genomförandeakter som avses i artiklarna 8.3 och 12.8.

3. Om det anmälda systemet för elektronisk identifiering före det datum som avses i punkt 2 c i denna artikel finns upptaget i den förteckning som kommissionen offentliggjort enligt artikel 9, ska medlet för elektronisk identifiering inom ramen för detta system enligt artikel 6 erkännas senast 12 månader efter systemets offentliggörande, dock inte före det datum som avses i punkt 2 c i denna artikel.

4. Trots vad som sägs i punkt 2 c i denna artikel får en medlemsstat besluta att ett medel för elektronisk identifiering inom ramen för ett system för elektronisk identifiering som har anmälts i enlighet med artikel 9.1 av en annan medlemsstat ska erkännas i den första medlemsstaten från och med tillämpningsdagen för de genomförandeakter som avses i artiklarna 8.3 och 12.8. De berörda medlemsstaterna ska underrätta kommissionen. Kommissionen ska offentliggöra denna information.

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

Utfärdad i Bryssel 23 juli 2014.

På Europaparlamentets vägnar	*På rådets vägnar*
M. SCHULZ	S. GOZI
Ordförande	*Ordförande*

BILAGA I

KRAV PÅ KVALIFICERADE CERTIFIKAT FÖR ELEKTRONISKA UNDERSKRIFTER

Kvalificerade certifikat för elektroniska underskrifter ska innehålla följande:

a) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att certifikatet har utfärdats som ett kvalificerat certifikat för elektroniska underskrifter.

b) En uppsättning uppgifter som otvetydigt avser den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, inbegripet uppgift om åtminstone vilken medlemsstat tillhandahållaren är etablerad i, samt

— för juridiska personer: namn och, i tillämpliga fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar,

— för fysiska personer: personens namn.

c) Åtminstone undertecknarens namn eller en pseudonym. Om en pseudonym används ska detta tydligt anges.

d) Valideringsuppgifter för elektroniska underskrifter som stämmer överens med uppgifterna för skapande av elektroniska underskrifter.

e) Detaljerade uppgifter om när certifikatet börjar respektive upphör att gälla.

f) Certifikatets identifieringskod, som måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster.

g) Den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikatet.

h) Uppgift om var det certifikat som stöder den avancerade elektroniska underskrift eller den avancerade elektroniska stämpeln som avses i led g finns tillgängligt kostnadsfritt.

i) Uppgift om var de tjänster som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet är lokaliserade.

j) Om de uppgifter för skapande av elektroniska underskrifter som avser valideringsuppgifterna för elektroniska underskrifter är placerade i en kvalificerad anordning för skapande av elektroniska underskrifter, en lämplig uppgift som anger detta, åtminstone i en form som lämpar sig för automatiserad behandling.

BILAGA II

KRAV PÅ KVALIFICERADE ANORDNINGAR FÖR SKAPANDE AV ELEKTRONISKA UNDERSKRIFTER

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

   a) konfidentialiteten för de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter är säkerställd på rimligt sätt,

   b) de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter i praktiken endast kan förekomma en gång,

   c) de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter med rimlig säkerhet inte kan härledas och att den elektroniska underskriften på ett tillförlitligt sätt är skyddad mot förfalskning med den teknik som för närvarande finns tillgänglig,

   d) de uppgifter för skapande av elektroniska underskrifter som används för att skapa elektroniska underskrifter kan skyddas på ett tillförlitligt sätt av den legitime undertecknaren så att andra inte kan använda dem.

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

3. Generering eller hantering av uppgifter för skapande av elektroniska underskrifter för undertecknarens räkning får endast utföras av en kvalificerad tillhandahållare av betrodda tjänster.

4. Kvalificerade tillhandahållare av betrodda tjänster som för undertecknarens räkning hanterar uppgifter för skapande av elektroniska underskrifter får, utan att det påverkar tillämpningen av punkt 1 d, endast kopiera dessa uppgifter för framställning av säkerhetskopior om följande krav är uppfyllda:

   a) Tillitsnivån 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 minsta antal som krävs för att säkerställa tjänstens kontinuitet.

BILAGA III

KRAV PÅ KVALIFICERADE CERTIFIKAT FÖR ELEKTRONISKA STÄMPLAR

Kvalificerade certifikat för elektroniska stämplar ska innehålla följande:

a) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att certifikatet har utfärdats som ett kvalificerat certifikat för elektroniska stämplar.

b) En uppsättning uppgifter som otvetydigt avser den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, inbegripet uppgift om åtminstone vilken medlemsstat tillhandahållaren är etablerad i, samt

— för juridiska personer: namn och, i tillämpliga fall, registreringsnummer i enlighet med vad som uppgetts i de officiella handlingarna,

— för fysiska personer: personens namn.

c) Åtminstone namnet på skaparen av stämpeln och, i förekommande fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar.

d) Valideringsuppgifter för elektroniska stämplar som stämmer överens med uppgifterna för skapande av elektroniska stämplar.

e) Detaljerade uppgifter om när certifikatet börjar respektive upphör att gälla.

f) Certifikatets identifieringskod, som måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster.

g) Den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikatet.

h) Uppgift om var det certifikat som stöder den avancerade elektroniska underskrift eller den avancerade elektroniska stämpeln som avses i led g är tillgängligt kostnadsfritt.

i) Uppgift om var de tjänster som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet är lokaliserade.

j) Om de uppgifter för skapande av elektroniska stämplar som har koppling till uppgifterna för validering av elektroniska stämplar är placerade i en kvalificerad anordning för skapande av elektroniska stämplar, en lämplig uppgift om detta, åtminstone i en form som 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, åtminstone i en form som lämpar sig för automatiserad behandling, om att certifikatet har utfärdats som ett kvalificerat certifikat för autentisering av webbplatser.

b) En uppsättning uppgifter som otvetydigt avser den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, inbegripet uppgift om åtminstone vilken medlemsstat tillhandahållaren är etablerad i, samt

— för juridiska personer: namn och, i tillämpliga fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar,

— för fysiska personer: personens namn.

c) För fysiska personer: åtminstone namnet på den person som certifikatet utfärdats för eller en pseudonym. Om en pseudonym används ska detta tydligt anges.

För juridiska personer: åtminstone namnet på den juridiska person som certifikatet utfärdats för och, i förekommande fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar.

d) Adressuppgifter, inbegripet åtminstone stad och stat, för den fysiska eller juridiska person som certifikatet utfärdats för och, i förekommande fall, i enlighet med vad som uppgetts i officiella handlingar.

e) Det eller de domännamn som drivs av den fysiska eller juridiska person som certifikatet utfärdats för.

f) Detaljerade uppgifter om när certifikatet börjar respektive upphör att gälla.

g) Certifikatets identifieringskod, som måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster.

h) Den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikatet.

i) Uppgift om var det certifikat som stöder den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln som avses i led h finns tillgängligt kostnadsfritt.

j) Uppgift om var de tjänster är lokaliserade som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet.