VERORDENING (EU) Nr. 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 23 juli 2014

betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité ([1]),

Handelend volgens de gewone wetgevingsprocedure ([2]),

Overwegende hetgeen volgt:

(1) Het opbouwen van vertrouwen in de online-omgeving is essentieel voor economische en sociale ontwikkeling. Een gebrek aan vertrouwen, met name ten gevolge van een ogenschijnlijk gebrek aan rechtszekerheid, leidt ertoe dat consumenten, bedrijven en overheden aarzelen om transacties elektronisch uit te voeren en van nieuwe diensten gebruik te maken.

(2) Deze verordening heeft tot doel het vertrouwen in elektronische transacties in de interne markt te vergroten door te voorzien in een gemeenschappelijke grondslag voor veilige elektronische interactie tussen burgers, bedrijven en overheden, en bijgevolg ook de doeltreffendheid van publieke en private onlinediensten, e-business en elektronische handel in de Unie te verhogen.

(3) Richtlijn 1999/93/EG van het Europees Parlement en de Raad ([3]) had betrekking op elektronische handtekeningen zonder een uitgebreid grens- en sectoroverschrijdend kader te bieden voor veilige, betrouwbare en gebruiksvriendelijke elektronische transacties. Deze verordening voorziet in een versterking en uitbreiding van de verworvenheden van die richtlijn.

(4) In de mededeling van de Commissie van 26 augustus 2010 met de titel „Een digitale Agenda voor Europa" werden de fragmentatie van de digitale markt, het gebrek aan interoperabiliteit en de toename van cybercriminaliteit aangewezen als de grootste belemmeringen voor de opkomst van de digitale economie. In haar verslag over het EU-burgerschap 2010 „Het wegnemen van de belemmeringen voor de rechten van EU-burgers" benadrukt de Commissie verder de noodzaak van het oplossen van de belangrijkste problemen die de burgers van de Unie verhinderen ten volle gebruik te maken van de voordelen van een digitale eengemaakte markt en grensoverschrijdende digitale diensten.

(5) In zijn conclusies van 4 februari 2011 en 23 oktober 2011 heeft de Europese Raad de Commissie verzocht tegen 2015 een digitale eengemaakte markt te creëren om snelle vorderingen te maken op sleutelgebieden van de digitale economie en om een volledig geïntegreerde digitale eengemaakte markt te bevorderen door het grensoverschrijdend gebruik van onlinediensten te vergemakkelijken, met bijzondere aandacht voor de facilitering van veilige elektronische identificatie en authenticatie.

([1]) PB C 351 van 15.11.2012, blz. 73.

([2]) Standpunt van het Europees Parlement van 3 april 2014 (nog niet bekendgemaakt in het Publicatieblad) en besluit van de Raad van 23 juli 2014.

([3]) Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PB L 13 van 19.1.2000, blz. 12).

(6) In zijn conclusies van 27 mei 2011 heeft de Raad de Commissie verzocht bij te dragen tot de digitale interne markt door de juiste voorwaarden te scheppen voor de wederzijdse erkenning van cruciale mogelijkheden scheppende voorzieningen over de grenzen heen, zoals elektronische identificatie, elektronische documenten, elektronische handtekeningen en elektronische leveringsdiensten en voor interoperabele e-overheidsdiensten in de gehele EU.

(7) In zijn resolutie van 21 september 2010 over de voltooiing van de interne markt voor e-handel [1] heeft het Europees Parlement het belang onderstreept van de veiligheid van elektronische diensten, vooral van elektronische handtekeningen, en van de noodzaak om een publieke sleutelinfrastructuur op pan-Europees niveau te creëren, en heeft de Commissie verzocht een toegangspoort voor Europese valideringsinstanties op te zetten om de grensoverschrijdende interoperabiliteit van elektronische handtekeningen te waarborgen en de veiligheid van transacties via internet te verhogen.

(8) Bij Richtlijn 2006/123/EG van het Europees Parlement en de Raad [2] wordt van de lidstaten vereist dat zij „één-loketten" opzetten zodat alle procedures en formaliteiten betreffende de toegang tot en de uitoefening van een dienstenactiviteit eenvoudig, op afstand en met elektronische middelen, via het juiste één-loket en met de juiste instanties kunnen worden afgewikkeld. Veel onlinediensten die via één-loketten toegankelijk zijn, vergen elektronische identificatie, authenticatie en een elektronische handtekening.

(9) In de meeste gevallen kunnen burgers hun elektronische identificatie niet gebruiken om zich te authenticeren in een andere lidstaat omdat de nationale stelsels voor elektronische identificatie van hun land niet erkend worden in andere lidstaten. Door deze elektronische belemmering kunnen dienstverleners de voordelen van de interne markt niet ten volle benutten. Wederzijds erkende elektronische identificatiemiddelen zullen het grensoverschrijdend verlenen van talrijke diensten op de interne markt faciliteren en bedrijven in staat stellen op een grensoverschrijdende basis activiteiten te ondernemen zonder daarbij veel belemmeringen te ondervinden in hun contacten met overheidsinstanties.

(10) In Richtlijn 2011/24/EU van het Europees Parlement en de Raad [3] wordt een netwerk van voor e-gezondheid verantwoordelijke nationale autoriteiten opgezet. Om de veiligheid en de continuïteit van grensoverschrijdende gezondheidszorg te verbeteren, moet het netwerk richtsnoeren opstellen voor de grensoverschrijdende toegang tot elektronische gezondheidsgegevens en -diensten, ook door het ondersteunen van „gemeenschappelijke identificatie- en authenticatiemaatregelen, teneinde de overdraagbaarheid van gegevens bij grensoverschrijdende gezondheidszorg te bevorderen". De wederzijdse erkenning van elektronische identificatie en authenticatie is essentieel om voor de Europese burger grensoverschrijdende gezondheidszorg realiteit te maken. Wanneer mensen voor een behandeling naar het buitenland reizen, moeten hun medische gegevens in het land van behandeling toegankelijk zijn. Dat vergt een degelijk, veilig en betrouwbaar kader voor elektronische identificatie.

(11) Deze verordening dient te worden toegepast in volledige overeenstemming met de beginselen inzake de bescherming van persoonsgegevens overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad [4]. In dit verband en met inachtneming van het bij deze verordening vastgelegde beginsel inzake wederzijdse erkenning, mag authenticatie voor een onlinedienst alleen betrekking hebben op de verwerking van die identificatiegegevens die toereikend, ter zake dienend en niet bovenmatig zijn om toegang tot die onlinedienst te verlenen. Voorts moeten de in Richtlijn 95/46/EG gestelde eisen inzake vertrouwelijkheid en beveiliging van de verwerking worden geëerbiedigd door de verleners van vertrouwensdiensten en het toezichthoudend orgaan.

(12) Een van de doelstellingen van deze verordening is het wegnemen van bestaande belemmeringen voor het grensoverschrijdende gebruik van elektronische identificatiemiddelen die in de lidstaten worden gebruikt om daarmee ten minste ten behoeve van publieke diensten te authenticeren. Deze verordening heeft niet tot doel systemen voor elektronisch identiteitsbeheer en bijbehorende infrastructuren in de lidstaten te beïnvloeden. Het doel van deze verordening is te waarborgen dat veilige elektronische identificatie en authenticatie voor de toegang tot grensoverschrijdende onlinediensten van de lidstaten mogelijk is.

[1] PB C 50 E van 21.2.2012, blz. 1.
[2] Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt (PB L 376 van 27.12.2006, blz. 36).
[3] Richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg (PB L 88 van 4.4.2011, blz. 45).
[4] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB L 281 van 23.11.1995, blz. 31).

(13) De lidstaten moeten de vrijheid behouden om ten behoeve van elektronische identificatie middelen voor toegang tot onlinediensten te gebruiken of in te voeren. De lidstaten moeten ook kunnen beslissen of zij de private sector bij het aanbieden van deze middelen wensen te betrekken. De lidstaten dienen niet te worden verplicht hun stelsels voor elektronische identificatie aan de Commissie te melden. Het staat de lidstaten vrij om alle, sommige dan wel geen van de stelsels voor elektronische identificatie die op nationaal niveau worden gebruikt om ten minste toegang te krijgen tot publieke onlinediensten of specifieke diensten, aan de Commissie te melden.

(14) In deze verordening moet een aantal voorwaarden worden vastgesteld om te bepalen welke elektronische identificatiemiddelen moeten worden erkend en hoe de stelsels voor elektronische identificatie moeten worden aangemeld. Deze voorwaarden moeten de lidstaten helpen het noodzakelijke vertrouwen in elkaars stelsels voor elektronische identificatie op te bouwen en elektronische identificatiemiddelen die onder hun aangemelde stelsels vallen, wederzijds te erkennen. Het beginsel van wederzijdse erkenning moet worden toegepast als het stelsel voor elektronische identificatie van de aanmeldende lidstaat voldoet aan de voorwaarden voor aanmelding en de aanmelding is bekendgemaakt in het *Publicatieblad van de Europese Unie*. Het beginsel van wederzijdse erkenning dient echter alleen op authenticatie voor een onlinedienst betrekking te hebben. De toegang tot deze onlinediensten en de daadwerkelijke verlening ervan aan de aanvrager moeten nauw verbonden zijn aan het recht om dergelijke diensten af te nemen onder de in de nationale wetgeving gestelde voorwaarden.

(15) De verplichting tot erkenning van elektronische identificatiemiddelen moet alleen betrekking hebben op die middelen waarvan het identiteitsbetrouwbaarheidsniveau overeenstemt met het niveau dat gelijk is aan of hoger is dan het voor de bewuste onlinedienst vereiste niveau. Voorts dient deze verplichting alleen te gelden als de openbare instantie in kwestie het betrouwbaarheidsniveau „substantieel" of „hoog" gebruikt voor de toegang tot die onlinedienst. De lidstaten moeten overeenkomstig het Unierecht de vrijheid behouden om elektronische identificatiemiddelen met lagere identiteitsbetrouwbaarheidsniveaus te erkennen.

(16) Het betrouwbaarheidsniveau moet de mate van vertrouwen weergeven die in een elektronisch identificatiemiddel kan worden gesteld voor het vaststellen van de identiteit van een persoon, en moet zodoende zekerheid geven dat de persoon die beweert een bepaalde identiteit te hebben ook daadwerkelijk degene is aan wie deze identiteit is toegekend. Het betrouwbaarheidsniveau hangt af van de mate van vertrouwen die elektronische identificatiemiddelen bieden voor de opgegeven of beweerde identiteit van een persoon, rekening houdend met processen (bijvoorbeeld het bewijzen van de identiteit,verificatie, en authenticatie), beheersactiviteiten (bijvoorbeeld de entiteit die elektronische identificatiemiddelen uitgeeft en de procedure voor uitgifte van dergelijke middelen) en geïmplementeerde technische beheersmaatregelen. Diverse technische definities en beschrijvingen van betrouwbaarheidsniveaus danken hun bestaan aan door de Unie gefinancierde Grootschalige Proefprojecten, standaardisering en internationale activiteiten. In het bijzonder refereren het Grootschalige Proefproject STORK en ISO 29115 aan, onder meer, de niveaus 2, 3 en 4, met welke niveaus ten zeerste rekening moet worden gehouden bij het vaststellen van minimale technische vereisten, standaarden en procedures voor de betrouwbaarheidsniveaus laag, substantieel en hoog in de zin van deze verordening, terwijl gezorgd moet worden voor een consequente toepassing van deze verordening, met name wat betreft betrouwbaarheidniveau hoog voor het bewijzen van de identiteit voor het afgeven van gekwalificeerde certificaten. De vereisten moeten technologieneutraal zijn. Het moet mogelijk zijn aan de noodzakelijke veiligheidsvereisten te voldoen door middel van verschillende technologieën.

(17) De lidstaten dienen de private sector aan te moedigen vrijwillig gebruik te maken van elektronische identificatiemiddelen die onder een aangemeld stelsel vallen, indien identificatie bij onlinediensten of elektronische transacties nodig is. De mogelijkheid om zulke elektronische identificatiemiddelen te gebruiken stelt de particuliere sector in staat gebruik te maken van elektronische identificatie en authenticatie, waar in diverse lidstaten in ieder geval voor publieke diensten reeds vaak gebruik van gemaakt wordt, en maakt het voor bedrijven en burgers gemakkelijker om grensoverschrijdende toegang te krijgen tot hun onlinediensten. Om het gebruik van dergelijke elektronische identificatiemiddelen door de private sector over de grenzen heen te vergemakkelijken, moet de mogelijkheid tot authenticatie die elke lidstaat biedt, beschikbaar zijn voor buiten het grondgebied van die lidstaat gevestigde vertrouwende partijen uit de private sector, en wel onder dezelfde voorwaarden als in die lidstaat gevestigde vertrouwende partijen. Bijgevolg mag de aanmeldende lidstaat ten aanzien van vertrouwende partijen uit de private sector voorwaarden voor toegang tot de authenticatiemiddelen bepalen. Die voorwaarden voor toegang kunnen vermelden of de authenticatiemiddelen voor het aangemelde stelsel voor elektronische identificatie op dat moment beschikbaar zijn voor vertrouwende partijen uit de private sector.

(18) Deze verordening dient te voorzien in de aansprakelijkheid van de aanmeldende lidstaat, de partij die de elektronische identificatiemiddelen verstrekt en de partij die de authenticatieprocedure uitvoert, wanneer zij niet voldoen aan de verplichtingen ter zake in deze verordening. Deze verordening moet echter worden uitgevoerd volgens de nationale voorschriften inzake aansprakelijkheid. De verordening beïnvloedt derhalve niet deze nationale voorschriften inzake, bijvoorbeeld, de definitie van schade of het bepalen van de toepasselijke procedureregels, waaronder inzake de bewijslast.

(19) De veiligheid van stelsels voor elektronische identificatie is van cruciaal belang voor een betrouwbare grensoverschrijdende wederzijdse erkenning van elektronische identificatiemiddelen. In dit verband moeten de lidstaten samenwerken op het gebied van de veiligheid en interoperabiliteit van de stelsels voor elektronische identificatie op Unieniveau. Wanneer in stelsels voor elektronische identificatie wordt geëist dat de vertrouwende partijen specifieke hardware of software gebruiken op nationaal niveau, dan wordt de betrokken lidstaten in het kader van de grensoverschrijdende interoperabiliteit verzocht dergelijke vereisten en daarmee verband houdende kosten niet op te leggen aan vertrouwende partijen die buiten hun grondgebied gevestigd zijn. In dat geval moeten binnen de grenzen van het interoperabiliteitskader passende oplossingen worden besproken en ontwikkeld. Niettemin zijn technische vereisten die voortvloeien uit de inherente specificaties van nationale elektronische identificatiemiddelen en die waarschijnlijk gevolgen zullen hebben voor de houders van dergelijke elektronische middelen (bv. smartcards), onvermijdelijk.

(20) De samenwerking tussen lidstaten moet de technische interoperabiliteit van de aangemelde stelsels voor elektronische identificatie faciliteren teneinde een sterk vertrouwen en een op het risiconiveau afgestemde beveiliging te bevorderen. Het uitwisselen van informatie en het delen van goede praktijken tussen lidstaten met het oog op hun wederzijdse erkenning, is bevorderlijk voor een dergelijke samenwerking.

(21) Deze verordening dient ook te voorzien in een algemeen wetgevingskader voor het gebruik van vertrouwensdiensten. Zij mag echter geen algemene verplichting scheppen om elektronische vertrouwensdiensten te gebruiken of om een toegangspunt voor alle bestaande vertrouwensdiensten te installeren. De verordening mag met name niet voorzien in de verlening van diensten die uitsluitend binnen gesloten systemen gebruikt worden tussen een welbepaalde groep deelnemers, en die geen gevolgen hebben voor derden. Systemen die zijn opgezet bij bedrijven of overheden voor het beheer van interne procedures waarbij gebruik wordt gemaakt van vertrouwensdiensten, behoren bijvoorbeeld niet onder deze verordening te vallen. Alleen vertrouwensdiensten die aan het publiek verleend worden en gevolgen hebben voor derden moeten voldoen aan de vereisten van deze verordening. Ook mag deze verordening geen betrekking hebben op aspecten die verband houden met de totstandkoming en geldigheid van contracten of andere juridische verbintenissen waaraan in het nationale recht of het Unierecht vormvereisten worden gesteld. Daarenboven dient zij de nationale vormvereisten voor openbare registers, met name handelsregisters en kadasters onverlet te laten.

(22) Teneinde bij te dragen tot het algemene grensoverschrijdende gebruik van vertrouwensdiensten, moet het mogelijk zijn deze in alle lidstaten in gerechtelijke procedures als bewijsmiddel te gebruiken. De rechtsgevolgen van vertrouwensdiensten moeten worden vastgesteld door het nationale recht, tenzij in deze verordening anders wordt bepaald.

(23) Voor zover deze verordening een verplichting schept om een vertrouwensdienst te erkennen, is het alleen mogelijk een dergelijke vertrouwensdienst niet te erkennen als de geadresseerde van de verplichting deze om technische redenen, waarop hij geen rechtstreekse invloed kan uitoefenen, niet kan lezen of verifiëren. Die verplichting hoeft evenwel op zich niet te betekenen dat een openbare instantie de voor de technische leesbaarheid van alle bestaande vertrouwensdiensten benodigde hardware en software moet verwerven.

(24) De lidstaten mogen in overeenstemming met het Unierecht nationale bepalingen in verband met vertrouwensdiensten invoeren of handhaven, voor zover die diensten niet volledig worden geharmoniseerd door deze verordening. Het vrije verkeer in de interne markt van vertrouwensdiensten die aan deze verordening voldoen, moet evenwel gewaarborgd worden.

(25) De lidstaten moeten de vrijheid behouden om naast de vertrouwensdiensten die deel uitmaken van de gesloten lijst waarin deze verordening voorziet, andere soorten vertrouwensdiensten te definiëren om deze op nationaal niveau als gekwalificeerde vertrouwensdienst te erkennen.

(26) Vanwege het hoge tempo van de technologische veranderingen dient deze verordening te voorzien in een aanpak die open staat voor innovatie.

(27) De verordening moet technologieneutraal zijn. De rechtsgevolgen waarin de verordening voorziet, moeten bereikt kunnen worden met om het even welk technologisch middel, op voorwaarde dat voldaan is aan de vereisten van deze verordening.

(28) Om het vertrouwen van in het bijzonder kleine en middelgrote ondernemingen (kmo's) en de consumenten in de interne markt te bevorderen en het gebruik van vertrouwensdiensten en producten te stimuleren, dienen de noties van gekwalificeerde vertrouwensdiensten en gekwalificeerde verlener van vertrouwensdiensten te worden geïntroduceerd om eisen en verplichtingen aan te duiden die ertoe dienen de beveiliging van welke gebruikte of geleverde gekwalificeerde vertrouwensdiensten en producten dan ook op hoog niveau te waarborgen.

(29) In overeenstemming met de verplichtingen van het Verdrag van de Verenigde Naties inzake de rechten van personen met een handicap, goedgekeurd door Besluit 2010/48/EG van de Raad [1], in het bijzonder artikel 9 van dat verdrag, moeten personen met een handicap in staat zijn de geleverde vertrouwensdiensten en de producten voor de eindgebruiker die bij het leveren van deze diensten gebruikt worden, op gelijke voet als andere consumenten te gebruiken. Daarom moeten, waar dat haalbaar is, vertrouwensdiensten en eindgebruikersproducten die worden gebruikt bij de verlening van deze diensten toegankelijk worden gemaakt voor personen met een handicap. De haalbaarheidsbeoordeling moet onder andere op technische en economische overwegingen gebaseerd zijn.

(30) De lidstaten dienen een of meer toezichthoudende organen aan te wijzen voor het verrichten van de toezichtactiviteiten uit hoofde van deze verordening. De lidstaten moeten eveneens kunnen besluiten om, in onderlinge overeenstemming met een andere lidstaat, een toezichthoudend orgaan aan te wijzen op het grondgebied van die andere lidstaat.

(31) Toezichthoudende organen moeten samenwerken met gegevensbeschermingsinstanties, bijvoorbeeld door hen te informeren over de resultaten van audits van gekwalificeerde verleners van vertrouwensdiensten wanneer er aanwijzingen zijn dat inbreuk op voorschriften inzake de bescherming van persoonsgegevens is gepleegd. De verstrekking van informatie moet in het bijzonder betrekking hebben op beveiligingsincidenten en inbreuken op persoonsgegevens.

(32) Alle verleners van vertrouwensdiensten zijn ertoe gehouden goede praktijkervaringen op beveiligingsgebied toe te passen, aangepast aan de risico's die verbonden zijn aan hun activiteiten, om het vertrouwen van gebruikers in de eengemaakte markt te bevorderen.

(33) De bepalingen inzake het gebruik van pseudoniemen in certificaten dienen de lidstaten niet te beletten op grond van het Unierecht of het nationale recht te verlangen dat personen zich legitimeren.

(34) Alle lidstaten moeten zich houden aan gemeenschappelijke essentiële toezichtvereisten om een vergelijkbaar niveau van veiligheid van gekwalificeerde vertrouwensdiensten te verzekeren. Om de consequente toepassing van deze vereisten in de gehele Unie te vergemakkelijken, moeten de lidstaten vergelijkbare procedures invoeren en informatie over hun toezichtactiviteiten en de beste praktijken in het veld uitwisselen.

(35) Alle verleners van vertrouwensdiensten moeten zich houden aan de vereisten van deze verordening, in het bijzonder wat betreft veiligheid en betrouwbaarheid, zodat de zorgvuldigheid, transparantie en verantwoording van hun activiteiten worden gewaarborgd. Gelet op de soort diensten die verleners van vertrouwensdiensten verlenen, dient echter met betrekking tot deze vereisten onderscheid te worden gemaakt tussen gekwalificeerde en niet-gekwalificeerde verleners van vertrouwensdiensten.

(36) De instelling van een toezichtregeling voor alle verleners van vertrouwensdiensten moet zorgen voor een gelijk speelveld met betrekking tot de veiligheid en verantwoording van hun activiteiten en diensten, hetgeen bijdraagt aan de bescherming van de gebruikers en aan de werking van de interne markt. Niet-gekwalificeerde verleners van vertrouwensdiensten moeten worden onderworpen aan eenvoudige en reactieve toezichtactiviteiten achteraf die worden gerechtvaardigd door de aard van hun diensten en activiteiten. Het toezichthoudend orgaan mag daarom geen algemene verplichting hebben om toezicht te houden op niet-gekwalificeerde dienstverleners. Het toezichthoudend orgaan dient alleen op te treden wanneer het ervan in kennis wordt gesteld (bijvoorbeeld door de niet-gekwalificeerde verlener van vertrouwensdiensten zelf, door een ander toezichthoudend orgaan, door een kennisgeving van een gebruiker of een zakenpartner of op basis van zijn eigen onderzoek) dat een niet-gekwalificeerde verlener van vertrouwensdiensten niet voldoet aan de vereisten van deze verordening.

[1] Besluit 2010/48/EG van de Raad van 26 november 2009 betreffende de sluiting door de Europese Gemeenschap van het Verdrag van de Verenigde Naties inzake de rechten van personen met een handicap (PB L 23 van 27.1.2010, blz. 35).

(37) Deze verordening moet voorzien in de aansprakelijkheid van alle verleners van vertrouwensdiensten. De verordening voorziet meer bepaald in de aansprakelijkheidsregeling in het kader waarvan alle verleners van vertrouwensdiensten aansprakelijk moeten zijn voor schade die wordt toegebracht aan een natuurlijke persoon of rechtspersoon wegens niet-naleving van de verplichtingen uit hoofde van deze verordening. Teneinde de beoordeling te vergemakkelijken van het financiële risico dat verleners van vertrouwensdiensten misschien moeten dragen of dat zij zouden moeten dekken met verzekeringspolissen, laat deze richtlijn toe dat verleners van vertrouwensdiensten, onder bepaalde voorwaarden, beperkingen verbinden aan het gebruik van de door hen verleende diensten en dat zij niet aansprakelijk zijn voor schade die het gevolg is van het gebruik van diensten dat deze beperkingen te buiten gaat. De klanten moeten vooraf terdege worden geïnformeerd over de beperkingen. Deze beperkingen moeten herkenbaar zijn voor een derde partij, bijvoorbeeld doordat er informatie over de beperkingen wordt opgenomen in de voorwaarden met betrekking tot de verleende dienst, of via andere herkenbare middelen. Om uitvoering te geven aan deze beginselen, moet deze verordening overeenkomstig de nationale aansprakelijkheidsregels worden toegepast. Daarom laat deze verordening die nationale regels inzake bijvoorbeeld de definitie van schade, opzet, nalatigheid, of de toepasselijke procedurele regels, onverlet.

(38) Het is van essentieel belang dat inbreuken op de veiligheid en beoordelingen van de veiligheidsrisico's worden gemeld zodat in het geval van een inbreuk of verlies van integriteit de juiste informatie aan de betrokken partijen kan worden verstrekt.

(39) Om de Commissie en de lidstaten in staat te stellen de doeltreffendheid van het bij deze verordening ingevoerde aanmeldingsmechanisme voor inbreuken te beoordelen, moet de toezichthoudende organen worden verzocht beknopte informatie te verstrekken aan de Commissie en aan het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa).

(40) Om de Commissie en de lidstaten in staat te stellen de doeltreffendheid te beoordelen van het versterkte toezichtmechanisme waarin deze verordening voorziet, moet de toezichtorganen worden verzocht verslag uit te brengen over hun activiteiten. Dit zou bevorderlijk zijn voor de uitwisseling van goede praktijken tussen toezichtorganen en zou de garantie bieden dat de essentiële toezichtvereisten in alle lidstaten consequent en efficiënt worden vervuld.

(41) Om de duurzaamheid van gekwalificeerde vertrouwensdiensten te waarborgen en het vertrouwen van de gebruikers in de continuïteit van gekwalificeerde vertrouwensdiensten te stimuleren, moeten de toezichthoudende organen, voor het geval dat gekwalificeerde verleners van vertrouwensdiensten hun activiteiten beëindigen, nagaan of er maatregelen betreffende beëindigingsplannen bestaan en of die correct worden toegepast.

(42) Om het toezicht op gekwalificeerde verleners van vertrouwensdiensten te vergemakkelijken, bijvoorbeeld wanneer een verlener zijn diensten aanbiedt op het grondgebied van een andere lidstaat en daar niet aan toezicht onderworpen is, of wanneer de computers van een verlener zich bevinden op het grondgebied van een andere lidstaat dan die waar hij gevestigd is, moet een systeem voor wederzijdse bijstand tussen de toezichtorganen in de lidstaten worden opgezet.

(43) Om te waarborgen dat de gekwalificeerde verleners van vertrouwensdiensten alsook de door hen verleende diensten voldoen aan de voorschriften van deze verordening, moet een conformiteitsbeoordeling worden verricht door een conformiteitsbeoordelingsorgaan en moeten de daaruit resulterende conformiteitsbeoordelingsrapporten door de gekwalificeerde verleners van vertrouwensdiensten aan het toezichthoudende orgaan worden voorgelegd. Telkens wanneer het toezichthoudende orgaan verlangt dat een gekwalificeerde verlener van vertrouwensdiensten een ad-hocconformiteitsbeoordelingsrapport indient, dient het in het bijzonder het beginsel van behoorlijk bestuur te eerbiedigen, mede omvattende de verplichting tot motivering van zijn besluiten, alsook het evenredigheidsbeginsel. Het toezichthoudende orgaan moet derhalve zijn besluit waarbij het een ad-hocconformiteitsbeoordeling vereist, naar behoren met redenen omkleden.

(44) Deze verordening heeft tot doel te zorgen voor een samenhangend kader dat met betrekking tot vertrouwensdiensten in een hoog niveau van veiligheid en rechtszekerheid voorziet. In dit verband moet de Commissie, met betrekking tot de conformiteitsbeoordeling van producten en diensten, in voorkomend geval streven naar synergie met bestaande toepasselijke Europese en internationale systemen zoals Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad [1] waarin de eisen inzake accreditatie van conformiteitsbeoordelingsorganen en markttoezicht op producten worden opgesomd.

[1] Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 (PB L 218 van 13.8.2008, blz. 30).

(45) Omwille van een doelmatig initiatieproces dat ertoe strekt gekwalificeerde verleners van vertrouwensdiensten en de door hen verleende gekwalificeerde vertrouwensdiensten in vertrouwenslijsten op te nemen, moeten voorbereidende interacties tussen kandidaat-gekwalificeerde verleners van vertrouwensdiensten en het bevoegde toezichthoudende orgaan worden bevorderd teneinde de zorgvuldigheid die tot het verlenen van gekwalificeerde vertrouwensdiensten moet leiden, te faciliteren.

(46) Vertrouwenslijsten zijn essentieel voor het opbouwen van vertrouwen tussen marktdeelnemers, aangezien zij informatie bevatten over de gekwalificeerde status van de dienstverlener op het moment van het toezicht.

(47) Vertrouwen in en gebruiksgemak van onlinediensten zijn voor gebruikers van wezenlijk belang om maximaal te kunnen profiteren van en bewust te vertrouwen op elektronische diensten. Daartoe moet een EU-vertrouwensmerk worden ingevoerd ter aanduiding van de door gekwalificeerde verleners van vertrouwensdiensten verleende gekwalificeerde vertrouwensdiensten. Dankzij dat EU-vertrouwensmerk voor gekwalificeerde vertrouwensdiensten zouden gekwalificeerde vertrouwensdiensten duidelijk kunnen worden onderscheiden van andere vertrouwensdiensten, wat tot transparantie in de markt zou bijdragen. Het gebruik van een EU-vertrouwensmerk door gekwalificeerde verleners van vertrouwensdiensten zou vrijwillig moeten zijn en geen aanleiding mogen geven tot andere vereisten dan die welke in deze verordening vastgelegd zijn.

(48) Hoewel een hoog beveiligingsniveau nodig is om de wederzijdse erkenning van elektronische handtekeningen te waarborgen, moeten in specifieke gevallen, zoals in het kader van Beschikking 2009/767/EG van de Commissie [1], elektronische handtekeningen met een lagere veiligheidsgarantie ook aanvaard worden.

(49) In deze verordening moet als beginsel worden gesteld dat het rechtsgevolg van een elektronische handtekening niet moet worden ontkend op grond van het feit dat de handtekening elektronisch is of niet aan de eisen voor gekwalificeerde elektronische handtekeningen voldoet. Het nationaal recht moet echter bepalen welk rechtsgevolg elektronische handtekeningen hebben, met uitzondering van de in deze verordening vastgestelde voorschriften dat een gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg dient te hebben als een handgeschreven handtekening.

(50) Aangezien bevoegde autoriteiten in de lidstaten momenteel verschillende formats voor geavanceerde elektronische handtekeningen gebruiken om hun documenten elektronisch te ondertekenen, moet worden gewaarborgd dat ten minste een aantal formats voor geavanceerde elektronische handtekeningen technisch ondersteund kunnen worden door de lidstaten wanneer zij elektronisch ondertekende documenten ontvangen. Evenzo is het nodig om, wanneer bevoegde autoriteiten in de lidstaten gebruikmaken van geavanceerde elektronische zegels, te waarborgen dat zij ten minste een aantal formats voor geavanceerde elektronische zegels ondersteunen.

(51) Het zou voor de ondertekenaar mogelijk moeten zijn om middelen voor het aanmaken van een gekwalificeerde elektronische handtekening toe te vertrouwen aan een derde, mits passende mechanismen en procedures worden toegepast om te waarborgen dat uitsluitend de ondertekenaar controle heeft over het gebruik van de aanmaakgegevens van zijn elektronische handtekening, en mits door gebruik te maken van dit middel de vereisten inzake gekwalificeerde elektronische handtekeningen worden nageleefd.

(52) Het aanmaken van elektronische handtekeningen op afstand, waarbij de omgeving waarin de elektronische handtekening wordt aangemaakt, door een verlener van vertrouwensdiensten namens de ondertekenaar wordt beheerd, zal wellicht toenemen gezien de talrijke economische voordelen ervan. Om er evenwel voor te zorgen dat die elektronische handtekeningen dezelfde juridische erkenning krijgen als elektronische handtekeningen die zijn aangemaakt in een volledig door de gebruiker beheerde omgeving, dienen de verleners van diensten voor elektronische handtekeningen op afstand specifieke veiligheidsprocedures toe te passen wat betreft beheer en administratie, en gebruik te maken van betrouwbare systemen en producten, met inbegrip van beveiligde elektronische communicatiekanalen, om te waarborgen dat de omgeving waarin de elektronische handtekening wordt aangemaakt betrouwbaar is en dat uitsluitend de ondertekenaar controle heeft over het gebruik ervan. Indien een gekwalificeerde elektronische handtekening is aangemaakt door gebruik te maken van een middel voor het aanmaken van elektronische handtekeningen op afstand, dienen de in deze verordening vastgelegde vereisten voor gekwalificeerde verleners van vertrouwensdiensten van toepassing te zijn.

[1] Beschikking 2009/767/EG van de Commissie van 16 oktober 2009 inzake maatregelen voor een gemakkelijker gebruik van elektronische procedures via het „één-loket" in het kader van Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt (PB L 274 van 20.10.2009, blz. 36).

(53) De schorsing van gekwalificeerde certificaten is een ingeburgerde operationele praktijk van verleners van vertrouwensdiensten in een aantal lidstaten en heeft het tijdelijk verlies van geldigheid van een certificaat tot gevolg, hetgeen is te onderscheiden van de intrekking van certificaten. Ten behoeve van de rechtszekerheid moet de geschorste status van een certificaat steeds duidelijk worden aangegeven. Daarom moeten verleners van vertrouwensdiensten de verantwoordelijkheid hebben om de status van het certificaat en, in geval van schorsing, de precieze tijdsduur van de schorsing, duidelijk aan te geven. Deze verordening dient het gebruik van schorsing niet aan de lidstaten of aan de verleners van vertrouwensdiensten op te leggen; de verordening dient evenwel te voorzien in transparantieregels in de gevallen waarin die praktijk gangbaar is.

(54) De grensoverschrijdende interoperabiliteit en erkenning van gekwalificeerde certificaten vormt een noodzakelijke voorwaarde voor grensoverschrijdende erkenning van gekwalificeerde elektronische handtekeningen. Derhalve dienen voor gekwalificeerde certificaten geen dwingende vereisten te gelden die strenger zijn dan de in deze verordening vastgestelde vereisten. Op nationaal niveau moet het evenwel mogelijk zijn specifieke kenmerken, zoals unieke identificatiegegevens, in gekwalificeerde certificaten te doen opnemen, mits die specifieke kenmerken de grensoverschrijdende interoperabiliteit en erkenning van gekwalificeerde certificaten en elektronische handtekeningen niet hinderen.

(55) Een op internationale normen gebaseerde IT-veiligheidscertificering, zoals ISO 15408 en verwante evaluatiemethoden en regelingen voor wederzijdse erkenning, is een belangrijk instrument voor de verificatie van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen, en dient te worden gestimuleerd. Innovatieve oplossingen en diensten zoals mobiel ondertekenen en ondertekenen in de cloud berusten echter op technische en organisatorische oplossingen voor gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen waarvoor nog geen beveiligingsstandaarden voorhanden zijn of waarvoor de eerste IT-veiligheidscertificeringsprocedure nog loopt. Het beveiligingsniveau van dergelijke gekwalificeerde apparatuur voor het aanmaken van elektronische handtekeningen kan worden geëvalueerd door gebruik te maken van alternatieve processen, maar enkel indien dergelijke veiligheidsnormen niet beschikbaar zijn of indien de eerste IT-veiligheidsbeoordeling aan de gang is. Deze processen dienen vergelijkbaar te zijn met de standaarden voor IT-veiligheidscertificering, voor zover het om gelijke beveiligingsniveaus gaat. Deze processen zouden baat kunnen hebben bij onderlinge evaluatie.

(56) In deze verordening moeten vereisten worden vastgesteld voor gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen vastgelegd om de functionaliteit van geavanceerde elektronische handtekeningen te waarborgen. Deze verordening hoeft niet de hele systeemomgeving waarbinnen dergelijke middelen functioneren te bestrijken. De werkingssfeer van de certificering van gekwalificeerde middelen voor het aanmaken van handtekeningen dient derhalve te worden beperkt tot de hardware en de systeemprogrammatuur die worden gebruikt voor het beheer en de bescherming van de voor het aanmaken van de handtekening in dat middel aangemaakte, opgeslagen of verwerkte gegevens. Als aangegeven in de toepasselijke standaarden moeten toepassingen voor het aanmaken van handtekeningen buiten de werkingssfeer van de verplichte certificering vallen.

(57) Om de rechtszekerheid wat betreft de geldigheid van de handtekening te zeker te stellen, is het van essentieel belang de componenten van een gekwalificeerde elektronische handtekening te specificeren, die moeten worden beoordeeld door de vertrouwende partij die de validering uitvoert. Bovendien moet het specificeren van de eisen aan gekwalificeerde verleners van vertrouwensdiensten die een gekwalificeerde valideringsdienst kunnen leveren aan vertrouwende partijen die niet bereid of in staat zijn om de validering van gekwalificeerde elektronische handtekeningen zelf uit te voeren, de private en de publieke sector stimuleren om in dergelijke diensten te investeren. Beide elementen moeten de validering van gekwalificeerde elektronische handtekeningen eenvoudig en handzaam maken voor alle partijen op het niveau van de Unie.

(58) Wanneer voor een transactie een gekwalificeerd elektronisch zegel van een rechtspersoon vereist is, moet een gekwalificeerde elektronische handtekening van de gemachtigd vertegenwoordiger van de rechtspersoon gelijkelijk aanvaardbaar zijn.

(59) Elektronische zegels moeten dienen als bewijs dat een elektronisch document door een rechtspersoon is afgegeven, door zekerheid omtrent de oorsprong en integriteit van het document te garanderen.

(60) Verleners van vertrouwensdiensten die gekwalificeerde certificaten voor elektronische zegels afgeven, dienen de maatregelen toe te passen die nodig zijn om de identiteit te kunnen vaststellen van de natuurlijke persoon die optreedt als vertegenwoordiger van de rechtspersoon waaraan het gekwalificeerd certificaat voor het elektronische zegel wordt uitgereikt, indien dat op nationaal niveau in het kader van een gerechtelijke of administratieve procedure noodzakelijk is.

(61) Deze verordening moet ervoor zorgen dat informatie langdurig bewaard blijft teneinde zeker te stellen dat elektronische handtekeningen en elektronische zegels gedurende lange tijd rechtsgeldig blijven en te garanderen dat zij gevalideerd kunnen worden ongeacht toekomstige technologische veranderingen.

(62) Omwille van de veiligheid van gekwalificeerde elektronische tijdstempels moet deze verordening het gebruik van een geavanceerd elektronisch zegel, een geavanceerde elektronische handtekening of andere, gelijkwaardige methoden voorschrijven. Verwacht kan worden dat door innovatie nieuwe technologieën ontstaan die een gelijkwaardig beveiligingsniveau bieden voor tijdstempels. Telkens wanneer gebruik wordt gemaakt van een andere methode dan een geavanceerd elektronisch zegel of een geavanceerde elektronische handtekening, moet de gekwalificeerde verlener van vertrouwensdiensten in het conformiteitsbeoordelingsrapport aantonen dat die andere methode een gelijkwaardig beveiligingsniveau garandeert en voldoet aan de in deze verordening vastgestelde verplichtingen.

(63) Elektronische documenten zijn van belang voor de verdere ontwikkeling van grensoverschrijdende elektronische transacties op de interne markt. In deze verordening moet als beginsel worden vastgelegd dat het rechtsgevolg van een elektronisch document niet moet worden ontkend op grond van het feit het elektronisch is, zodat een elektronische transactie niet zal worden geweigerd alleen omdat een document een document in elektronische vorm is.

(64) Met betrekking tot de formats van geavanceerde elektronische handtekeningen en zegels moet de Commissie voortbouwen op bestaande praktijken, standaarden en wetgeving, in het bijzonder Besluit 2011/130/EU van de Commissie ([1]).

(65) Behalve voor de authenticatie van het door de rechtspersoon afgegeven document, kunnen elektronische zegels worden gebruikt voor de authenticatie van alle digitale activa van de rechtspersoon, zoals softwarecode of servers.

(66) Het is van essentieel belang dat wordt voorzien in een juridisch kader ter facilitering van de grensoverschrijdende erkenning van bestaande nationale juridische regelingen met betrekking tot diensten voor elektronisch aangetekende bezorging. Dat kader zou voor verleners van vertrouwensdiensten in de Unie ook nieuwe afzetmogelijkheden kunnen openen voor het aanbieden van nieuwe pan-Europese diensten voor elektronisch aangetekende bezorging.

(67) Diensten voor authenticatie van websites vormen een middel waarmee websitebezoekers er zeker van kunnen zijn dat het om de website van een werkelijk bestaande, legitieme entiteit gaat. Die diensten dragen bij tot toenemend vertrouwen in online zaken doen, aangezien een geauthentiseerde website het vertrouwen van de gebruikers zal genieten. Het verlenen en gebruikmaken van diensten voor authenticatie van websites gebeurt volledig op vrijwillige basis. Echter, om van authenticatie van websites een middel te maken om het vertrouwen te bevorderen, de gebruikers betere ervaringen te bezorgen en de groei in de interne markt te bevorderen, moet deze verordening evenwel voorzien in minimumverplichtingen inzake veiligheid en aansprakelijkheid voor dienstverleners en voor de door hen verleende diensten. Daartoe is rekening gehouden met de resultaten van bestaande initiatieven van de sector, zoals Certification Authorities/Browsers Forum — CA/B Forum. Daarnaast dient deze verordening geen beletsel te vormen voor het gebruik van andere, niet onder deze verordening vallende middelen of methoden voor authenticatie van een website, noch te voorkomen dat verleners van diensten voor websiteauthenticatie uit derde landen hun diensten aanbieden aan afnemers in de Unie. Door dienstverleners uit derde landen aangeboden diensten voor authenticatie van websites dienen evenwel enkel te worden erkend als overeenkomstig deze verordening gekwalificeerde diensten als de Unie en het vestigingsland van de dienverlener een internationale overeenkomst hebben gesloten.

(68) Overeenkomstig de bepalingen van het Verdrag betreffende de werking van de Europese Unie (VWEU) inzake vestiging laat het begrip „rechtspersonen" de marktdeelnemers vrij in de keuze van de rechtsvorm die zij voor hun activiteiten geschikt achten. Bijgevolg slaat „rechtspersonen" in de zin van het VWEU op alle entiteiten die zijn opgericht naar of worden beheerst door het recht van een lidstaat, ongeacht hun rechtsvorm.

(69) De instellingen, organen, bureaus en agentschappen van de Unie worden aangemoedigd onder deze verordening vallende elektronische identificatie en vertrouwensdiensten te erkennen met als doel administratieve samenwerking, en daarbij vooral te profiteren van bestaande goede werkwijzen en de resultaten van lopende projecten op onder deze verordening vallende gebieden.

([1]) Besluit 2011/130/EU van de Commissie van 25 februari 2011 tot vaststelling van minimumvoorschriften voor de grensoverschrijdende verwerking van documenten die door de bevoegde autoriteiten elektronisch zijn ondertekend krachtens Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt (PB L 53 van 26.2.2011, blz. 66).

(70) Om bepaalde uitvoerige technische aspecten van deze verordening op een flexibele en snelle manier aan te vullen, moet de bevoegdheid om handelingen vast te stellen overeenkomstig artikel 290 VWEU aan de Commissie worden overgedragen wat betreft de criteria waaraan de organen die verantwoordelijk zijn voor de certificering van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen moeten voldoen. Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadpleging overgaat, onder meer op deskundigenniveau. De Commissie moet er bij de voorbereiding en opstelling van gedelegeerde handelingen voor zorgen dat de desbetreffende documenten tijdig en op gepaste wijze gelijktijdig worden toegezonden aan het Europees Parlement en de Raad.

(71) Om eenvormige voorwaarden te waarborgen voor de uitvoering van deze verordening, moeten uitvoeringsbevoegdheden worden toegekend aan de Commissie, in het bijzonder voor het specificeren van referentienummers voor standaarden waarvan het gebruik aanleiding zou zijn voor een vermoeden van overeenstemming met bepaalde vereisten die zijn vastgesteld in deze verordening. Die bevoegdheden moeten in overeenstemming met Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad worden uitgeoefend ([1]).

(72) Bij de vaststelling van gedelegeerde of uitvoeringshandelingen dient de Commissie terdege rekening te houden met de standaarden en technische specificaties als opgesteld door Europese en internationale organisaties en organen voor normalisatie, in het bijzonder het Europees Comité voor Normalisatie (CEN), het Europees Instituut voor telecommunicatienormen (ETSI), de Internationale Organisatie voor normalisatie (ISO), en de Internationale Telecommunicatie-unie (ITU), met het oog op het waarborgen van een hoog niveau van veiligheid en interoperabiliteit van elektronische identificatie en vertrouwensdiensten.

(73) Omwille van de rechtszekerheid en duidelijkheid moet Richtlijn 1999/93/EG worden ingetrokken.

(74) Om rechtszekerheid te waarborgen voor marktdeelnemers die reeds van aan natuurlijke personen afgegeven gekwalificeerde certificaten gebruikmaken in overeenstemming met Richtlijn 1999/93/EG, moet een voldoende ruime overgangsperiode worden vastgesteld. Ook moeten overgangsmaatregelen worden vastgesteld voor middelen voor het veilig aanmaken van handtekeningen waarvan de overeenstemming overeenkomstig Richtlijn 1999/93/EG is vastgesteld, evenals voor certificatiedienstverleners die voor 1 juli 2016 gekwalificeerde certificaten afgeven. Ook moet de Commissie tot slot voorzien worden van de middelen die nodig zijn om de uitvoeringshandelingen en gedelegeerde handelingen vóór die datum vast te stellen.

(75) De toepassingsdata in deze verordening veranderen niets aan bestaande verplichtingen die lidstaten reeds krachtens het Unierecht, en in het bijzonder Richtlijn 2006/123/EG, hebben.

(76) Daar de doelstellingen van deze verordening niet voldoende door de lidstaten kunnen worden verwezenlijkt maar, vanwege de omvang van het optreden, beter door de Unie kunnen worden verwezenlijkt, kan de Unie maatregelen vaststellen, overeenkomstig het subsidiariteitsbeginsel als bedoeld in artikel 5 van het Verdrag betreffende de Europese Unie. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om deze doelstellingen te verwezenlijken.

(77) De Europese Toezichthouder voor gegevensbescherming werd geraadpleegd in overeenstemming met artikel 28, lid 2, van Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad ([2]) en heeft op 27 september 2012 advies uitgebracht ([3]),

([1]) Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren (PB L 55 van 28.2.2011, blz. 13).

([2]) Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB L 8 van 12.1.2001, blz. 1).

([3]) PB C 28 van 30.1.2013, blz. 6.

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp

Met het oog op het goede functioneren van de interne markt, en daarbij strevend naar een adequaat niveau van veiligheid van elektronische identificatiemiddelen en vertrouwensdiensten, worden bij deze verordening:

a) de voorwaarden vastgesteld waaronder lidstaten elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen erkennen die onder een aangemeld stelsel voor elektronische identificatie van een andere lidstaat vallen,

b) regels vastgesteld voor vertrouwensdiensten, met name voor elektronische transacties, en

c) een juridisch kader vastgesteld voor elektronische handtekeningen, elektronische zegels, elektronische tijdstempels, elektronische documenten, diensten voor elektronisch aangetekende bezorging en certificatendiensten voor websiteauthenticatie.

Artikel 2

Toepassingsgebied

1. Deze verordening is van toepassing op stelsels voor elektronische identificatie die zijn aangemeld door een lidstaat en op verleners van vertrouwensdiensten die in de Unie zijn gevestigd.

2. Deze verordening is niet van toepassing op de verlening van vertrouwensdiensten die uitsluitend in systemen die gesloten zijn als gevolg van nationaal recht of overeenkomsten tussen een welbepaalde groep deelnemers.

3. Deze verordening doet geen afbreuk aan nationaal of Unierecht dat betrekking heeft op de totstandkoming en geldigheid van contracten of andere wettelijke of procedurele verplichtingen inzake vormvereisten.

Artikel 3

Definities

Voor de doelstellingen van deze verordening, zijn de volgende definities van toepassing:

1. „elektronische identificatie”: het proces van het gebruiken van persoonsidentificatiegegevens in elektronische vorm die op unieke wijze een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, aanduiden;

2. „elektronisch identificatiemiddel”: een materiële en/of immateriële eenheid die persoonsidentificatiegegevens bevat en die gebruikt wordt voor authenticatie bij een onlinedienst;

3. „persoonsidentificatiegegevens”: een reeks gegevens aan de hand waarvan de identiteit van een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, kan worden vastgesteld;

4. „stelsel voor elektronische identificatie”: een stelsel voor elektronische identificatie waarbinnen elektronische identificatiemiddelen worden uitgegeven aan natuurlijke personen, rechtspersonen of natuurlijke personen die rechtspersonen vertegenwoordigen;

5. „authenticatie": een elektronisch proces dat de bevestiging van de elektronische identificatie van een natuurlijke persoon of rechtspersoon, of van de oorsprong en integriteit van gegevens in elektronische vorm mogelijk maakt;

6. „vertrouwende partij": een natuurlijke persoon of een rechtspersoon die vertrouwt op een elektronische identificatie of een vertrouwensdienst;

7. „openbare instantie": een staat, regionale of lokale overheden, publiekrechtelijke instellingen en samenwerkingsverbanden bestaand uit één of meer van deze overheidsinstanties of een of meer van deze publiekrechtelijke instellingen, of een private entiteit die door ten minste een van deze autoriteiten, publiekrechtelijke instellingen of verenigingen is gemachtigd tot het verlenen van openbare diensten, wanneer zij in die hoedanigheid optreden;

8. „publiekrechtelijke instelling": een instelling volgens de definitie in punt 4 van artikel 2, lid 1, van Richtlijn 2014/24/EU van het Europees Parlement en de Raad ([1]);

9. „ondertekenaar": een natuurlijke persoon die een elektronische handtekening aanmaakt;

10. „elektronische handtekening": gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen;

11. „geavanceerde elektronische handtekening": een elektronische handtekening die voldoet aan de eisen in artikel 26;

12. „gekwalificeerde elektronische handtekening": een geavanceerde elektronische handtekening die is aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en die gebaseerd is op een gekwalificeerd certificaat voor elektronische handtekeningen;

13. „gegevens voor het aanmaken van elektronische handtekeningen": unieke gegevens die door de ondertekenaar worden gebruikt om een elektronische handtekening aan te maken;

14. „certificaat voor elektronische handtekeningen": een elektronische attestering die valideringsgegevens voor elektronische handtekeningen aan een natuurlijke persoon koppelt en ten minste de naam of het pseudoniem van die persoon bevestigt;

15. „gekwalificeerd certificaat voor elektronische handtekeningen": een certificaat voor elektronische handtekeningen, dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage I;

16. „vertrouwensdienst": een elektronische dienst die gewoonlijk tegen betaling wordt verricht en het onderstaande inhoudt:

    a) het aanmaken, verifiëren en valideren van elektronische handtekeningen, elektronische zegels of elektronische tijdstempels, diensten voor elektronisch aangetekende bezorging en op deze diensten betrekking hebbende certificaten of

    b) het aanmaken, verifiëren en valideren van certificaten voor authenticatie van websites, of

    c) het bewaren van elektronische handtekeningen, zegels of certificaten die op deze diensten betrekking hebben;

17. „gekwalificeerde vertrouwensdienst": een vertrouwensdienst die voldoet aan de toepasselijke eisen zoals vastgelegd in deze verordening;

([1]) Richtlijn 2014/24/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten en tot intrekking van Richtlijn 2004/18/EG (PB L 94 van 28.3.2014, blz. 65).

18. „conformiteitsbeoordelingsinstantie": een instantie omschreven in artikel 2, punt 13, van Verordening (EG) nr. 765/2008, die in overeenstemming met die verordening geaccrediteerd is om een conformiteitsbeoordeling te verrichten van een gekwalificeerde verlener van vertrouwensdiensten en van de door hem verleende vertrouwensdiensten;

19. „verlener van vertrouwensdiensten": een natuurlijke persoon of rechtspersoon die een of meer vertrouwensdiensten verleent als een gekwalificeerde of als een niet-gekwalificeerde verlener van vertrouwensdiensten;

20. „gekwalificeerde verlener van vertrouwensdiensten": een verlener van vertrouwensdiensten die één of meerdere gekwalificeerde vertrouwensdiensten verleent en van het toezichthoudende orgaan de status van gekwalificeerde heeft gekregen;

21. „product": software of hardware, of relevante componenten van hardware of software, die bedoeld zijn om te worden gebruikt voor de verlening van vertrouwensdiensten;

22. „middel voor het aanmaken van elektronische handtekeningen": geconfigureerde software of hardware die wordt gebruikt om een elektronische handtekening aan te maken;

23. „gekwalificeerd middel voor het aanmaken van elektronische handtekeningen": een middel voor het aanmaken van elektronische handtekeningen dat voldoet aan de eisen van bijlage II;

24. „aanmaker van een zegel": een rechtspersoon die een elektronisch zegel aanmaakt;

25. „elektronisch zegel": gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die worden gebruikt om de oorsprong en integriteit daarvan te waarborgen;

26. „geavanceerd elektronisch zegel": een elektronisch zegel dat voldoet aan de eisen in artikel 36;

27. „gekwalificeerd elektronisch zegel": een geavanceerd elektronisch zegel dat aangemaakt is door een gekwalificeerd middel voor het aanmaken van elektronische zegels en dat gebaseerd is op een gekwalificeerd certificaat voor elektronische zegels;

28. „gegevens voor het aanmaken van elektronische zegels": unieke gegevens die door de aanmaker van het elektronische zegel worden gebruikt om een elektronisch zegel aan te maken;

29. „certificaat voor elektronische zegels": een elektronische attestering die valideringsgegevens van elektronische zegels aan een rechtspersoon verbindt en de naam van die rechtspersoon bevestigt;

30. „gekwalificeerd certificaat voor elektronische zegels": een certificaat voor een elektronische zegel dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage III;

31. „middel voor het aanmaken van elektronische zegels": geconfigureerde software of hardware die wordt gebruikt om een elektronisch zegel aan te maken;

32. „gekwalificeerd middel voor het aanmaken van elektronische zegels": een middel voor het aanmaken van elektronische zegels dat mutatis mutandis voldoet aan de eisen van bijlage II;

33. „elektronische tijdstempel": gegevens in elektronische vorm die andere gegevens in elektronische vorm verbinden aan een bepaald tijdstip en die bewijzen dat die laatstgenoemde gegevens op dat tijdstip bestonden;

34. „gekwalificeerde elektronische tijdstempel": een elektronische tijdstempel die voldoet aan de in artikel 42 vastgelegde eisen;

35. „elektronisch document": elke inhoud die is opgeslagen in elektronische vorm, in het bijzonder tekst of geluid, beeld of audiovisuele opname;

36. „dienst voor elektronisch aangetekende bezorging": een dienst die het mogelijk maakt gegevens via elektronische middelen tussen derden te verzenden en die bewijs verschaft ten aanzien van het hanteren van de verzonden gegevens, met inbegrip van bewijs van het verzenden en ontvangen van de gegevens, en die de verzonden gegevens beschermt tegen het risico van verlies, diefstal, beschadiging of onbevoegde wijzigingen;

37. „gekwalificeerde dienst voor elektronisch aangetekende bezorging": een dienst voor elektronisch aangetekende bezorging die voldoet aan de in artikel 44 vastgestelde eisen;

38. „certificaat voor websiteauthenticatie": attestering die het mogelijk maakt de authenticiteit van een website vast te stellen en die de website verbindt aan de natuurlijke of rechtspersoon aan wie het certificaat is afgegeven;

39. „gekwalificeerd certificaat voor websiteauthenticatie": certificaat voor websiteauthenticatie dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage IV;

40. „valideringsgegevens": gegevens die worden gebruikt om een elektronische handtekening of elektronisch zegel te valideren;

41. „validering": proces waarmee wordt nagegaan of en bevestigd dat een elektronische handtekening of een elektronisch zegel geldig is.

Artikel 4

Internemarktbeginsel

1. Aan de verlening van vertrouwensdiensten op het grondgebied van een lidstaat door een verlener van vertrouwensdiensten die in een andere lidstaat gevestigd is mogen geen beperkingen worden opgelegd om redenen die behoren tot de gebieden waarop deze verordening betrekking heeft.

2. Producten en vertrouwensdiensten die aan deze verordening voldoen, kunnen in de interne markt in het vrije verkeer worden gebracht.

Artikel 5

Gegevensverwerking en -bescherming

1. De verwerking van persoonsgegevens geschiedt in overeenstemming met Richtlijn 95/46/EG.

2. Onverminderd het rechtsgevolg dat dat aan het gebruik van pseudoniemen op grond van het nationaal recht wordt toegekend, wordt het gebruik ervan in elektronische transacties niet verboden.

HOOFDSTUK II

ELEKTRONISCHE IDENTIFICATIE

Artikel 6

Wederzijdse erkenning

1. Wanneer een elektronische identificatie met gebruikmaking van een elektronisch identificatiemiddel en authenticatie vereist is op grond van nationaal recht of door gangbare bestuursrechtelijke praktijk om toegang te krijgen tot een onlinedienst aangeboden door een openbare instantie in een lidstaat, moet het elektronisch identificatiemiddel dat uitgegeven is in een andere lidstaat worden erkend in de eerste lidstaat ten behoeve van de grensoverschrijdende onlineauthenticatie van die dienst, mits aan de volgende voorwaarden is voldaan:

a) het elektronisch identificatiemiddel is uitgegeven op grond van een stelsel voor elektronische identificatie dat is opgenomen in de lijst die de Commissie uit hoofde van artikel 9 heeft bekendgemaakt;

b) het betrouwbaarheidsniveau van het elektronisch identificatiemiddel is gelijk aan of hoger dan het betrouwbaarheidsniveau dat de bevoegde openbare instantie als voorwaarde stelt voor onlinetoegang tot die dienst in de eerste lidstaat, mits het betrouwbaarheidsniveau van dat elektronisch identificatiemiddel in overeenstemming is met het betrouwbaarheidsniveau substantieel of hoog;

c) de openbare instantie in kwestie gebruikt het betrouwbaarheidsniveau substantieel of hoog voor de toegang tot die onlinedienst.

Die erkenning vindt plaats uiterlijk twaalf maanden nadat de Commissie de lijst als bedoeld in de eerste alinea, onder a), heeft bekendgemaakt.

2. Een elektronisch identificatiemiddel dat is uitgegeven op grond van een stelsel voor elektronische identificatie opgenomen in de lijst die op grond van artikel 9 door de Commissie is gepubliceerd en het betrouwbaarheidsniveau laag heeft, kan door openbare instanties worden erkend ten behoeve van de grensoverschrijdende authenticatie voor de onlinediensten die door die instanties worden geleverd.

Artikel 7

Voorwaarden voor het in aanmerking komen voor de aanmelding van stelsels voor elektronische identificatie

Een stelsel voor elektronische identificatie komt in aanmerking voor aanmelding overeenkomstig artikel 9, lid 1, indien aan alle onderstaande voorwaarden is voldaan:

a) het elektronische identificatiemiddel dat onder het stelsel voor elektronische identificatie valt wordt uitgegeven:

i) door de aanmeldende lidstaat;

ii) op grond van een mandaat van de aanmeldende lidstaat; of

iii) onafhankelijk van de aanmeldende lidstaat, en wordt door die lidstaat erkend;

b) de elektronische identificatiemiddelen uit hoofde van het stelsel voor elektronische identificatie kunnen worden gebruikt om toegang te verkrijgen tot ten minste één door een openbare instantie geleverde dienst waarvoor elektronische identificatie vereist is in de aanmeldende lidstaat;

c) het stelsel voor elektronische identificatie en de uit hoofde ervan uitgegeven elektronische identificatiemiddelen voldoen aan de eisen van op zijn minst één van de betrouwbaarheidsniveaus, opgenomen in de in artikel 8, lid 3, vermelde uitvoeringshandeling;

d) de aanmeldende lidstaat waarborgt dat de persoonsidentificatiegegevens die de persoon in kwestie op unieke wijze kenmerken op het moment van uitgifte van het elektronische identificatiemiddel op grond van dat stelsel, conform de technische specificaties, normen en procedures voor het respectieve betrouwbaarheidsniveau zoals neergelegd in de uitvoeringshandeling bedoeld in artikel 8, lid 3, worden gekoppeld aan de natuurlijke persoon of rechtspersoon als bedoeld in artikel 3, punt 1;

e) de partij die het elektronische identificatiemiddel uitgeeft op grond van dat stelsel, zorgt ervoor dat het elektronische identificatiemiddel wordt gekoppeld aan de persoon bedoeld in punt d) van dat artikel, in overeenstemming met de technische specificaties, normen en procedures voor het respectieve betrouwbaarheidsniveau zoals neergelegd in de uitvoeringshandeling bedoeld in artikel 8, lid 3;

f) de aanmeldende lidstaat zorgt voor de beschikbaarheid van onlineauthenticatie, zodat iedere vertrouwende partij die op het grondgebied van een andere lidstaat gevestigd is, de mogelijkheid heeft de ontvangen persoonsidentificatiegegevens in elektronische vorm te bevestigen.

Voor andere vertrouwende partijen dan openbare instanties mag de aanmeldende lidstaat voorwaarden stellen voor toegang tot die authenticatie. Grensoverschrijdende authenticatie is kosteloos wanneer zij wordt uitgevoerd voor een door een openbare instantie verleende onlinedienst.

De lidstaten leggen geen specifieke onevenredige technische eisen op aan vertrouwende partijen die voornemens zijn een dergelijke authenticatie uit te voeren indien dergelijke eisen de interoperabiliteit van de aangemelde stelsels voor elektronische identificatie tegenhouden of in aanzienlijke mate belemmeren;

g) ten minste zes maanden voor de aanmelding bedoeld in artikel 9, lid 1, verstrekt de aanmeldende lidstaat met het oog op de verplichting van artikel 12, lid 5, de andere lidstaten een beschrijving van dat stelsel, in overeenstemming met de procedurele voorschriften die zijn vastgesteld bij de in artikel 12, lid 7, bedoelde uitvoeringshandelingen;

h) het stelsel voor elektronische identificatie voldoet aan de eisen van de uitvoeringshandeling bedoeld in artikel 12, lid 8.

Artikel 8

Betrouwbaarheidsniveaus van stelsels voor elektronische identificatie

1. Een stelsel voor elektronische identificatie dat is aangemeld krachtens artikel 9, lid 1, omschrijft betrouwbaarheidsniveaus laag, substantieel en/of hoog voor op grond van dat stelsel uitgegeven elektronische identificatiemiddelen.

2. De betrouwbaarheidsniveaus laag, substantieel en hoog voldoen respectievelijk aan de volgende criteria:

a) het betrouwbaarheidsniveau laag betreft een elektronisch identificatiemiddel in het kader van een stelsel voor elektronische identificatie, dat een beperkte mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te verkleinen;

b) het betrouwbaarheidsniveau substantieel betreft een elektronisch identificatiemiddel in het kader van een stelsel voor elektronische identificatie, dat een substantiële mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te verkleinen;

c) het betrouwbaarheidsniveau hoog betreft een elektronisch identificatiemiddel in het kader van een stelsel voor elektronische identificatie, dat een hogere mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt dan een elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te voorkomen.

3. Uiterlijk op 18 september 2015, rekening houdend met de geldende internationale normen en behoudens lid 2, stelt de Commissie bij uitvoeringshandeling minimale technische specificaties, normen en procedures vast aan de hand waarvan de betrouwbaarheidsniveaus laag, substantieel en hoog worden bepaald voor de elektronische identificatiemiddelen als bedoeld in lid 1.

Deze minimale technische specificaties, normen en procedures worden vastgesteld onder verwijzing naar de betrouwbaarheid en kwaliteit van de volgende elementen:

a) de procedure om de identiteit van de natuurlijke of rechtspersoon die om uitgifte van het elektronisch identificatiemiddel verzoekt, te bewijzen en te verifiëren;

b) de procedure voor de uitgifte van het aangevraagde elektronische identificatiemiddel;

c) het authenticatiemechanisme, door middel waarvan de natuurlijke of rechtspersoon het elektronische identificatiemiddel gebruikt om zijn identiteit te bevestigen tegenover een vertrouwende partij;

d) de entiteit die het elektronische identificatiemiddel uitgeeft;

e) ieder ander orgaan dat betrokken is bij de uitgifte van het elektronische identificatiemiddel en

f) de technische en veiligheidsspecificaties van het uitgegeven elektronische identificatiemiddel.

Die uitvoeringsbesluiten worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 9

Aanmelding

1. De aanmeldende lidstaat geeft de Commissie onverwijld kennis van de volgende informatie en van eventuele latere wijzigingen daarvan:

a) een beschrijving van het stelsel voor elektronische identificatie, met inbegrip van de betrouwbaarheidsniveaus daarvan en de uitgever of de uitgevers van elektronische identificatiemiddelen in het kader van het stelsel;

b) de toepasselijke toezichtregeling en informatie over de aansprakelijkheidsregeling met betrekking tot onderstaande:

i) de partij die het elektronische identificatiemiddel uitgeeft, en

ii) de partij die de authenticatieprocedure uitvoert;

c) de autoriteit of autoriteiten die verantwoordelijk is/zijn voor het stelsel voor elektronische identificatie;

d) informatie over de entiteit of entiteiten die de registratie van de unieke persoonsidentificatiegegevens beheert/beheren;

e) een beschrijving van de manier waarop aan de vereisten van de in artikel 12, lid 8, bedoelde uitvoeringshandelingen wordt voldaan;

f) een beschrijving van de authenticatie bedoeld in artikel 7, onder f);

g) regelingen voor de opschorting of intrekking van het aangemelde stelsel voor elektronische identificatie of de authenticatie of de delen waarvan de integriteit is geschonden.

2. Eén jaar na de datum van toepassing van de in artikel 8, lid 3, en artikel 12, lid 8, bedoelde uitvoeringshandelingen maakt de Commissie in het *Publicatieblad van de Europese Unie* een lijst bekend van de stelsels voor elektronische identificatie die zijn aangemeld overeenkomstig lid 1 van dit artikel alsmede de basisinformatie in verband hiermee.

3. Indien de Commissie een aanmelding ontvangt nadat de periode als bedoeld in lid 2 verstreken is, maakt zij binnen twee maanden na de datum van ontvangst van die aanmelding in het *Publicatieblad van de Europese Unie* de wijzigingen van de in lid 2 bedoelde lijst bekend.

4. Een lidstaat kan bij de Commissie een verzoek indienen om een door die lidstaat aangemelde stelsel voor elektronische identificatie van de in lid 2 bedoelde lijst te verwijderen. De Commissie zal de desbetreffende wijzigingen binnen een maand na de datum van ontvangst van het verzoek van de lidstaat in het *Publicatieblad van de Europese Unie* bekendmaken.

5. De Commissie kan door middel van uitvoeringshandelingen de omstandigheden, formaten en procedures voor aanmeldingen in het kader van lid 1 definiëren. Deze uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 10

Inbreuk op de beveiliging

1. Wanneer er inbreuk wordt gepleegd op het overeenkomstig artikel 9, lid 1, aangemelde stelsel voor elektronische identificatie of op de in artikel 7, onder f), bedoelde authenticatie of wanneer de integriteit ervan deels wordt geschonden zodat de betrouwbaarheid van de grensoverschrijdende authenticatie van dat stelsel in gevaar komt, moet de aanmeldende lidstaat onverwijld de grensoverschrijdende authenticatie of de delen waarvan de integriteit geschonden is, opschorten of intrekken, en de andere lidstaten en de Commissie hiervan op de hoogte stellen.

2. Wanneer de in lid 1 bedoelde inbreuk of schending hersteld is, herstelt de aanmeldende lidstaat de grensoverschrijdende authenticatie en stelt hij de andere lidstaten en de Commissie daarvan onverwijld op de hoogte.

3. Indien de in lid 1 bedoelde inbreuk of schending niet binnen drie maanden na de opschorting of intrekking is verholpen, stelt de aanmeldende lidstaat de andere lidstaten en de Commissie op de hoogte van de intrekking van het stelsel voor elektronische identificatie.

De Commissie maakt de overeenkomstige wijzigingen aan de in artikel 9, lid 2, bedoelde lijst zonder onnodige vertraging bekend in het *Publicatieblad van de Europese Unie*.

Artikel 11

Aansprakelijkheid

1. De aanmeldende lidstaat is aansprakelijk voor aan een natuurlijke persoon of rechtspersoon met opzet of door nalatigheid toegebrachte schade die is te wijten aan een verzuim zijn verplichtingen uit hoofde van artikel 7, onder d) en f), in een grensoverschrijdende transactie na te leven.

2. De partij die de elektronische identificatiemiddelen verstrekt, is aansprakelijk voor aan een natuurlijke persoon of rechtspersoon met opzet of door nalatigheid toegebrachte schade die te wijten is aan een verzuim de verplichting bedoeld in artikel 7, onder e), in een grensoverschrijdende transactie na te leven.

3. De partij die de authenticatieprocedure uitvoert, is aansprakelijk voor aan een natuurlijke persoon of een rechtspersoon met opzet of door nalatigheid toegebrachte schade die te wijten is aan een verzuim de verplichting bedoeld in artikel 7, onder f), in een grensoverschrijdende transactie na te leven.

4. De leden 1, 2 en 3 worden toegepast in overeenstemming met de nationale rechtsregels aangaande aansprakelijkheid.

5. De leden 1, 2 en 3 doen niet af aan de aansprakelijkheid uit hoofde van nationale wetgeving van partijen bij een transactie waarin elektronische identificatiemiddelen worden gebruikt die onder het krachtens artikel 9, lid 1, aangemelde stelsel voor elektronische identificatie vallen.

Artikel 12

Samenwerking en interoperabiliteit

1. De krachtens artikel 9, lid 1, aangemelde nationale stelsels voor elektronische identificatie zijn interoperabel.

2. Voor de toepassing van lid 1 wordt een interoperabiliteitskader opgezet.

3. Het interoperabiliteitskader voldoet aan de volgende criteria:

a) het is erop gericht technologieneutraal te zijn en discrimineert niet tussen specifieke nationale technische oplossingen voor elektronische identificatie binnen de lidstaat;

b) het volgt, zo mogelijk, Europese en internationale normen;

c) het bevordert de toepassing van het beginsel van privacy by design; en

d) het waarborgt dat persoonsgegevens overeenkomstig Richtlijn 95/46/EG worden verwerkt.

4. Het interoperabiliteitskader bestaat uit:

a) een vermelding van de technische minimumeisen met betrekking tot de betrouwbaarheidsniveaus van artikel 8;

b) het relateren van nationale betrouwbaarheidsniveaus van aangemelde stelsels voor elektronische identificatie aan de betrouwbaarheidsniveaus volgens artikel 8;

c) een verwijzing naar technische minimumeisen voor interoperabiliteit;

d) een verwijzing naar een minimaal pakket persoonsidentificatiegegevens die een natuurlijke of rechtspersoon op unieke wijze vertegenwoordigen, beschikbaar vanaf stelsels voor elektronische identificatie;

e) procedureregels;

f) regelingen voor geschillenbeslechting; en

g) gemeenschappelijke operationele veiligheidsnormen.

5. De lidstaten werken op onderstaande gebieden samen:

a) de interoperabiliteit van de uit hoofde van artikel 9, lid 1, aangemelde stelsels voor elektronische identificatie en de stelsels voor elektronische identificatie die de lidstaten voornemens zijn aan te melden; en

b) de veiligheid van de stelsels voor elektronische identificatie.

6. De samenwerking tussen de lidstaten bestaat uit:

a) de uitwisseling van informatie, ervaring en goede werkwijzen wat betreft stelsels voor elektronische identificatie en in het bijzonder wat betreft de technische vereisten inzake het niveau van interoperabiliteit en betrouwbaarheid;

b) de uitwisseling van informatie, ervaring en goede werkwijzen wat betreft het werken met betrouwbaarheidsniveaus van stelsels voor elektronische identificatie volgens artikel 8;

c) onderlinge evaluatie van stelsels voor elektronische identificatie die onder deze verordening vallen; en

d) onderzoek naar ontwikkelingen ter zake in de sector van de elektronische identificatie.

7. De Commissie stelt uiterlijk op 18 maart 2015, door middel van uitvoeringshandelingen, de nodige procedurele voorschriften vast om de in lid 5 en lid 6 bedoelde samenwerking tussen de lidstaten te vergemakkelijken teneinde een hoog op het risiconiveau afgestemde niveau van vertrouwen en veiligheid te waarborgen.

8. De Commissie stelt uiterlijk op 18 september 2015, volgens de criteria in lid 3 en met inachtneming van de resultaten van de samenwerking tussen de lidstaten, uitvoeringshandelingen vast aangaande het lid 4 uitgewerkte interoperabiliteitskader ten behoeve van de vaststelling van eenduidige voorwaarden ter uitvoering van de in lid 1 bedoelde verplichting.

9. De in de leden 7 en 8 van dit artikel bedoelde uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

HOOFDSTUK III

VERTROUWENSDIENSTEN

AFDELING 1

Algemene bepalingen

Artikel 13

Aansprakelijkheid en bewijslast

1. Onverminderd lid 2 zijn verleners van vertrouwensdiensten aansprakelijk voor opzettelijk of uit onachtzaamheid toegebrachte schade aan een natuurlijke persoon of rechtspersoon die is te wijten aan een verzuim de verplichtingen uit hoofde van deze verordening na te leven.

De bewijslast voor het aantonen van opzet of nalatigheid van een niet gekwalificeerde verlener van vertrouwensdiensten ligt bij de natuurlijke persoon of de rechtspersoon die zich op de in de eerste alinea 1 bedoelde schade beroept.

De opzet of nalatigheid van een gekwalificeerde verlener van vertrouwensdiensten wordt vermoed tenzij die gekwalificeerde verlener van vertrouwensdiensten bewijst dat in de eerste alinea bedoelde schade is ontstaan zonder dat er sprake was van opzet of nalatigheid van die gekwalificeerde verlener van vertrouwensdiensten.

2. Indien verleners van vertrouwensdiensten hun klanten van te voren goed informeren over de beperkingen bij het gebruik van de aangeboden diensten en als deze beperkingen voor derden herkenbaar zijn, zijn verleners van vertrouwensdiensten niet aansprakelijk voor schade die ontstaat door gebruikmaking van diensten die de aangegeven beperkingen overschrijden.

3. De leden 1 en 2 worden toegepast volgens de nationale voorschriften inzake aansprakelijkheid.

Artikel 14

Internationale aspecten

1. Vertrouwensdiensten verstrekt door in een derde land gevestigde verleners van vertrouwensdiensten worden rechtens erkend als gelijkwaardig aan gekwalificeerde vertrouwensdiensten verstrekt door gekwalificeerde, in de Unie gevestigde verleners van vertrouwensdiensten, indien de vertrouwensdiensten die afkomstig zijn uit het derde land worden erkend op grond van een overeenkomst, gesloten tussen de Unie en het betrokken derde land of een internationale organisatie overeenkomstig artikel 218 VWEU.

2. In lid 1 bedoelde overeenkomsten regelen in het bijzonder dat:

a) de voorschriften die gelden voor in de Unie gevestigde gekwalificeerde verleners van vertrouwensdiensten en de door hen geleverde gekwalificeerde vertrouwensdiensten worden nageleefd door verleners van vertrouwensdiensten in het derde land of de internationale organisaties waarmee de overeenkomst is gesloten, en door de vertrouwensdiensten die zij verlenen;

b) de door in de Unie gevestigde, gekwalificeerde verleners van vertrouwensdiensten geleverde gekwalificeerde vertrouwensdiensten worden erkend als wettelijk gelijkwaardig aan vertrouwensdiensten van verleners van vertrouwensdiensten in het derde land of de internationale organisatie waarmee de overeenkomst is gesloten.

Artikel 15

Toegankelijkheid voor personen met een handicap

Waar dat haalbaar is, zullen vertrouwensdiensten en eindgebruikersproducten die worden gebruikt bij de verlening van deze diensten toegankelijk worden gemaakt voor personen met een handicap.

Artikel 16

Sancties

De lidstaten stellen de voorschriften vast inzake de sancties die van toepassing zijn op inbreuken op deze verordening. De vastgestelde sancties moeten doeltreffend, evenredig en afschrikkend zijn.

AFDELING 2

Toezicht

Artikel 17

Toezichthoudend orgaan

1. De lidstaten wijzen een toezichthoudend orgaan aan dat gevestigd is op hun grondgebied of, in overeenstemming met een andere lidstaat, een in die andere lidstaat gevestigd toezichthoudend orgaan. Dat orgaanis verantwoordelijk voor toezichthoudende taken in de aanwijzende lidstaat.

Toezichthoudende organen krijgen de noodzakelijke bevoegdheden en toereikende middelen voor de uitvoering van hun opdrachten.

2. De lidstaten delen de Commissie de namen en adressen mee van de door hen aangewezen toezichthoudende organen.

3. De rol van het toezichthoudend orgaan is:

a) toezicht te houden op gekwalificeerde verleners van vertrouwensdiensten die gevestigd zijn in de aanwijzende lidstaat om door middel van toezichthoudende activiteiten vooraf en achteraf te waarborgen dat deze gekwalificeerde verleners van vertrouwensdiensten en de door hen verleende gekwalificeerde vertrouwensdiensten voldoen aan de eisen in deze verordening;

b) indien nodig tegen niet-gekwalificeerde verleners van vertrouwensdiensten die gevestigd zijn in de aanwijzende lidstaat op te treden door middel van toezichthoudende activiteiten achteraf, wanneer het orgaan verneemt dat deze niet-gekwalificeerde verleners van vertrouwensdiensten of de door hen verleende vertrouwensdiensten niet zouden voldoen aan de vereisten van deze verordening.

4. Met het oog op de doeleinden van lid 3 en behoudens de aldaar aangegeven beperkingen bestaan de taken van het toezichthoudend orgaan in het bijzonder in:

a) samenwerking met andere toezichthoudende organen en bijstandsverlening aan deze organen overeenkomstig artikel 18;

b) analyse van de conformiteitsbeoordelingsverslagen bedoeld in artikel 20, lid 1, en artikel 21, lid 1;

c) andere toezichthoudende organen en het publiek overeenkomstig artikel 19, lid 2, op de hoogte brengen van veiligheidsinbreuken of integriteitsverlies;

d) aan de Commissie verslag uitbrengen over zijn hoofdactiviteiten, overeenkomstig lid 6;

e) audits uitvoeren of een conformiteitsbeoordelingsinstantie verzoeken een conformiteitsbeoordeling te doen van de gekwalificeerde verleners van vertrouwensdiensten overeenkomstig artikel 20, lid 2;

f) samenwerken met de gegevensbeschermingsinstanties en in het bijzonder deze instanties zonder onnodige vertraging informeren over de resultaten van de audits van gekwalificeerde verleners van vertrouwensdiensten indien er aanwijzingen zijn dat er regels inzake bescherming van persoonsgegevens zijn overtreden;

g) de status van gekwalificeerde toekennen aan verleners van vertrouwensdiensten en aan de door hen verleende diensten, en deze status intrekken, overeenkomstig de artikelen 20 en 21;

h) het voor de nationale vertrouwenslijst verantwoordelijke orgaan, bedoeld in artikel 22, lid 3, op de hoogte brengen van zijn besluiten om de status van gekwalificeerde toe te kennen of in te trekken, tenzij dit orgaan ook het toezichthoudend orgaan is;

i) indien de gekwalificeerde verlener van vertrouwensdiensten zijn activiteiten beëindigt, nagaan of er bepalingen bestaan over beëindigingsplannen en of deze correct worden toegepast, ook inzake de vraag hoe informatie toegankelijk wordt gehouden overeenkomstig artikel 24, lid 2, onder h);

j) eisen dat verleners van vertrouwensdiensten iedere niet-naleving van de in deze verordening vastgestelde voorschriften rechtzetten.

5. De lidstaten mogen vereisen dat het toezichthoudende orgaan een vertrouwensinfrastructuur opzet, onderhoudt en geregeld aanpast in overeenstemming met de voorwaarden uit hoofde van het nationale recht.

6. Elk toezichthoudend orgaan legt de Commissie jaarlijks uiterlijk op 31 maart een verslag voor over zijn hoofdactiviteiten in het voorgaande kalenderjaar, evenals een samenvatting van inbreukmeldingen die van verleners van vertrouwensdiensten ontvangen zijn overeenkomstig artikel 19, lid 2.

7. De Commissie stelt het in lid 6 bedoelde jaarverslag voor de lidstaten beschikbaar.

8. De Commissie kan door middel van uitvoeringshandelingen de formaten en procedures voor het in lid 6 bedoelde verslag definiëren. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 48, lid 2, bedoelde onderzoeksprocedure.

Artikel 18

Wederzijdse bijstand

1. Toezichthoudende organen moeten samenwerken met het oog op de uitwisseling van goede praktijken.

Een toezichthoudend orgaan verleent een ander toezichthoudend orgaan bij ontvangst van diens gemotiveerd verzoek bijstand, zodat de activiteiten van toezichthoudende organen op consistente wijze kunnen worden uitgevoerd. Wederzijdse bijstand kan in het bijzonder betrekking hebben op informatieverzoeken en toezichthoudende maatregelen, zoals verzoeken om inspecties uit te voeren in verband met de conformiteitsbeoordelingsverslagen bedoeld in de artikelen 20 en 21.

2. Een toezichthoudend orgaan tot welk een verzoek om bijstand wordt gericht, mag dat verzoek om alle onderstaande redenen weigeren:

a) het toezichthoudend orgaan is niet bevoegd om de gevraagde bijstand te leveren;

b) de gevraagde bijstand staat niet in verhouding tot de toezichthoudende activiteiten van het toezichthoudend orgaan, uitgevoerd overeenkomstig artikel 17;

c) het aanbieden van de gevraagde bijstand zou onverenigbaar zijn met deze verordening.

3. Indien van toepassing kunnen lidstaten hun toezichthoudende organen toestaan gezamenlijke onderzoeken uit te voeren waarbij personeelsleden van toezichthoudende organen van andere lidstaten betrokken zijn. De regelingen en procedures voor dergelijke gezamenlijke acties worden door de betrokken lidstaten overeenkomstig hun wetgeving overeengekomen en vastgelegd.

Artikel 19

Veiligheidseisen die van toepassing zijn op verleners van vertrouwensdiensten

1. Gekwalificeerde en niet gekwalificeerde verleners van vertrouwensdiensten treffen passende technische en organisatorische maatregelen om de risico's te beheren in verband met de veiligheid van de door hen verleende vertrouwensdiensten. Deze maatregelen waarborgen, rekening houdend met de meest recente technologische ontwikkelingen, een veiligheidsniveau dat in verhouding staat tot de mate van risico. In het bijzonder worden maatregelen getroffen om de gevolgen van veiligheidsincidenten te voorkomen en tot een minimum te beperken alsmede om belanghebbenden op de hoogte te stellen van de negatieve gevolgen van dergelijke incidenten.

2. Gekwalificeerde en niet gekwalificeerde verleners van vertrouwensdiensten stellen, zonder onnodige vertragingen maar in ieder geval binnen 24 uur nadat zij hiervan op de hoogte zijn geraakt, het toezichthoudende orgaan, en, waar passend, andere relevante organen zoals het bevoegde nationale orgaan voor informatieveiligheid of de gegevensbeschermingsautoriteit op de hoogte van iedere veiligheidsinbreuk of ieder integriteitsverlies met aanzienlijke gevolgen voor de verleende vertrouwensdienst of voor de persoonsgegevens die daarmee worden beheerd.

Indien de veiligheidsinbreuk of het integriteitsverlies naar verwachting negatieve gevolgen zal hebben voor een natuurlijke persoon of een rechtspersoon aan wie een vertrouwensdienst is verleend, stelt de verlener van de vertrouwensdienst ook de natuurlijke persoon of de rechtspersoon onmiddellijk in kennis van de veiligheidsinbreuk of het integriteitsverlies.

Indien van toepassing, in het bijzonder indien een veiligheidsinbreuk of integriteitsverlies twee of meer lidstaten treft, stelt het op de hoogte gestelde toezichthoudende orgaan de toezichthoudende organen in andere betrokken lidstaten en Enisa op de hoogte.

Het op de hoogte gestelde toezichthoudende orgaan informeert het publiek, of eist dat de verlener van vertrouwensdiensten dat doet, indien het van oordeel is dat bekendmaking van de veiligheidsinbreuk of het integriteitsverlies in het algemene belang is.

3. Het toezichthoudende orgaan bezorgt het Enisa eenmaal per jaar een samenvatting van meldingen van inbreuken op beveiliging en integriteitsverlies die zijn ontvangen van verleners van vertrouwensdiensten.

4. De Commissie kan middels uitvoeringshandelingen:

a) de in lid 1 bedoelde maatregelen nader specificeren, en

b) de formaten en procedures, met inbegrip van termijnen, definiëren die van toepassing zijn voor de doeleinden van lid 2.

Die uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

AFDELING 3

Vertrouwensdiensten

Artikel 20

Toezicht op gekwalificeerde verleners van vertrouwensdiensten

1. Gekwalificeerde verleners van vertrouwensdiensten worden minstens eens in de 24 maanden op hun kosten onderworpen aan een audit door een conformiteitsbeoordelingsorgaan. Het doel van deze audit is te bevestigen dat de gekwalificeerde verleners van vertrouwensdiensten en de gekwalificeerde vertrouwensdiensten die door hen worden verleend, voldoen aan de in deze verordening vastgestelde eisen. De gekwalificeerde verleners van vertrouwensdiensten dienen het conformiteitsbeoordelingsverslag binnen de termijn van drie werkdagen na ontvangst in bij het toezichthoudend orgaan.

2. Onverminderd het bepaalde in lid 1 kan het toezichthoudend orgaan op elk tijdstip een audit houden van, of een conformiteitsbeoordelingsorgaan verzoeken een conformiteitsbeoordeling uit te voeren ten aanzien van de gekwalificeerde verleners van vertrouwensdiensten, en wel op kosten van deze verleners van vertrouwensdiensten, om te bevestigen dat zij en de gekwalificeerde vertrouwensdiensten die door hen verleend worden, voldoen aan de in deze verordening vastgestelde vereisten. Indien er sprake blijkt te zijn van een inbreuk op de regels voor de bescherming van persoonsgegevens brengt het toezichthoudend orgaan de instanties voor gegevensbescherming op de hoogte van de resultaten van de audits.

3. Indien het toezichthoudend orgaan van de gekwalificeerde verlener van vertrouwensdiensten vereist dat deze het niet naleven van de eisen uit hoofde van deze verordening rechtzet en indien deze verlener niet aan dat verzoek tegemoet komt, en indien van toepassing binnen een door het toezichthoudend orgaan bepaalde tijdspanne, kan het toezichthoudend orgaan, gelet op in het bijzonder de mate, de duur en de gevolgen van die niet-naleving, de status van gekwalificeerde van die verlener of van de door hem verleende betrokken dienst intrekken en het in artikel 22, lid 3, bedoelde orgaan daarvan op de hoogte brengen met als doel de actualisering van de in artikel 22, lid 1, bedoelde vertrouwenslijsten. Het toezichthoudend orgaan stelt de gekwalificeerde verlener van vertrouwensdiensten in kennis van het feit dat zijn status van gekwalificeerde of de status van gekwalificeerde van de betrokken dienst is ingetrokken.

4. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor onderstaande normen:

a) accreditering van de conformiteitsbeoordelingsinstanties en voor het conformiteitsbeoordelingsverslag bedoeld in lid 1;

b) auditregels volgens welke conformiteitsbeoordelingsinstanties hun conformiteitsbeoordeling van de gekwalificeerde verleners van vertrouwensdiensten, bedoeld in lid 1, uitvoeren.

Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 48, lid 2, bedoelde onderzoeksprocedure.

Artikel 21

Aanvang voor het aanbieden van een gekwalificeerde vertrouwensdienst

1. Indien verleners van vertrouwensdiensten die niet over de status gekwalificeerd beschikken de intentie hebben gekwalificeerde vertrouwensdiensten te gaan leveren, dienen zij bij het toezichthoudend orgaan een kennisgeving van hun voornemen in, evenals een door een conformiteitsbeoordelingsorgaan afgegeven conformiteitsbeoordelingsverslag.

2. Het toezichthoudend orgaan verifieert of de verlener van vertrouwensdiensten en de door hem verleende vertrouwensdiensten in overeenstemming met de in deze verordening vastgestelde eisen zijn, en in het bijzonder met de eisen die worden gesteld aan gekwalificeerde verleners van vertrouwensdiensten en aan de gekwalificeerde vertrouwensdiensten die zij verlenen.

Indien het toezichthoudend orgaan tot het oordeel komt dat de verlener van vertrouwensdiensten en de door hem verleende vertrouwensdiensten in overeenstemming met de in de eerste alinea bedoelde eisen zijn, kent het toezichthoudend orgaan de status van gekwalificeerde toe aan de verlener van vertrouwensdiensten en aan de door hem verleende vertrouwensdiensten en stelt het het in artikel 22, lid 3, bedoelde orgaan in kennis zodatde in artikel 22, lid 1, bedoelde vertrouwenslijsten bijgewerkt worden, en wel binnen drie maanden na kennisgeving overeenkomstig lid 1 van dit artikel.

Indien de verificatie niet binnen drie maanden na de kennisgeving is afgerond, brengt het toezichthoudend orgaan de verlener van vertrouwensdiensten op de hoogte van de redenen voor de vertraging en van de termijn waarbinnen de verificatie zal zijn afgerond.

3. Gekwalificeerde verleners van vertrouwensdiensten mogen beginnen met het verlenen van de gekwalificeerde vertrouwensdienst nadat de status van gekwalificeerde is opgenomen in de in artikel 22, lid 1, bedoelde vertrouwenslijsten.

4. De Commissie kan door middel van uitvoeringshandelingen de formaten en procedures omschrijven voor de doeleinden van de leden 1 en 2. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 48, lid 2, bedoelde onderzoeksprocedure.

Artikel 22

Vertrouwenslijsten

1. Elke lidstaat stelt vertrouwenslijsten op met onder meer informatie over de gekwalificeerde verleners van vertrouwensdiensten waarvoor hij verantwoordelijk is, samen met informatie over de gekwalificeerde vertrouwensdiensten die door hen verleend worden, en hij houdt deze lijsten bij en maakt deze bekend.

2. De lidstaten dragen zorg voor het op een veilige manier opstellen, bijhouden en publiceren van elektronisch ondertekende of verzegelde vertrouwenslijsten, als bedoeld in lid 1, in een vorm die geschikt is voor automatische verwerking.

3. De lidstaten verschaffen de Commissie onverwijld informatie over het orgaan dat verantwoordelijk is voor het opstellen, onderhouden en publiceren van nationale vertrouwenslijsten en gegevens over waar deze lijsten gepubliceerd zijn, over het certificaat dat gebruikt wordt om de vertrouwenslijsten te ondertekenen of te verzegelen, en over alle wijzigingen daarin.

4. De Commissie maakt via een beveiligd kanaal de in lid 3 bedoelde informatie in elektronisch ondertekende of verzegelde en voor automatische verwerking geschikte vorm publiek beschikbaar.

5. Uiterlijk op 18 september 2015 specificeert de Commissie door middel van uitvoeringshandelingen de in lid 1 bedoelde informatie en omschrijft zij de technische specificaties en formaten van vertrouwenslijsten die gelden voor de toepassing van lid 1 tot en met 4. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 48, lid 2, bedoelde onderzoeksprocedure.

Artikel 23

Vertrouwensmerk van de EU voor gekwalificeerde vertrouwensdiensten

1. Nadat de in artikel 21, lid 2, tweede alinea, bedoelde status van gekwalificeerde is aangegeven op de in artikel 22, lid 1, bedoelde vertrouwenslijst, kunnen gekwalificeerde verleners van vertrouwensdiensten het vertrouwensmerk van de EU gebruiken om de gekwalificeerde vertrouwensdiensten die zij leveren op een eenvoudige, herkenbare en duidelijke manier aan te geven.

2. Wanneer gekwalificeerde dienstverleners gebruikmaken van het vertrouwensmerk van de EU voor de in lid 1 bedoelde gekwalificeerde vertrouwensdiensten, zorgen zij ervoor dat op hun website een koppeling naar de desbetreffende vertrouwenslijst beschikbaar is.

3. De Commissie bepaalt uiterlijk op 1 juli 2015, via uitvoeringshandelingen, de specificaties van het formulier, en in het bijzonder de presentatie, samenstelling, omvang en vormgeving van het vertrouwensmerk van de EU voor gekwalificeerde vertrouwensdiensten. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 48, lid 2, bedoelde onderzoeksprocedure.

Artikel 24

Eisen aan gekwalificeerde verleners van vertrouwensdiensten

1. Wanneer een gekwalificeerde verlener van vertrouwensdiensten een gekwalificeerd certificaat voor een vertrouwensdienst afgeeft, moet hij met daartoe geschikte middelen en overeenkomstig de nationale wetgeving de identiteit en in voorkomend geval de specifieke attributen verifiëren van de natuurlijke persoon of de rechtspersoon aan wie het gekwalificeerde certificaat wordt afgegeven.

De in de eerste alinea bedoelde informatie wordt door de gekwalificeerde verlener van vertrouwensdiensten geverifieerd, hetzij rechtstreeks, hetzij door een beroep te doen op een derde partij, overeenkomstig de nationale wetgeving:

a) door de fysieke aanwezigheid van de natuurlijke persoon of een gemachtigde afgevaardigde van de rechtspersoon, of

b) op afstand, door middel van elektronische identificatiemiddelen, waarbij voorafgaand aan de afgifte van het gekwalificeerd certificaat de fysieke aanwezigheid van de natuurlijke persoon of de gemachtigde afgevaardigde van de rechtspersoon werd gewaarborgd, en die voldoen aan de vereisten van artikel 8 wat betreft de betrouwbaarheidsniveaus „substantieel" of „hoog", of

c) door middel van een certificaat van een gekwalificeerde elektronische handtekening of van een gekwalificeerd elektronisch zegel afgegeven overeenkomstig punt a) of b), of

d) door middel van andere op nationaal niveau erkende identificatiemethoden die een mate van betrouwbaarheid verschaffen die gelijkwaardig is als fysieke aanwezigheid. Dat gelijkwaardige betrouwbaarheidsniveau wordt bevestigd door een conformiteitsbeoordelingsinstantie.

2. Een gekwalificeerde verlener van vertrouwensdiensten die gekwalificeerde vertrouwensdiensten verleent:

a) stelt het toezichthoudende orgaan in kennis van veranderingen in de verlening van gekwalificeerde vertrouwensdiensten en een intentie om deze activiteiten te staken;

b) neemt personeelsleden, en, waar van toepassing, onderaannemers in dienst die over de noodzakelijke deskundigheid, betrouwbaarheid, ervaring, en kwalificaties beschikken, en die een passende opleiding hebben genoten met betrekking tot regels inzake beveiliging en bescherming van persoonsgegevens, en past administratieve en managementprocedures toe die voldoen aan Europese of internationale normen;

c) zorgt ervoor dat hij, in verband met het risico op de in artikel 13 bedoelde aansprakelijkheid voor schade, voldoende financiële middelen ter beschikking heeft en/of sluit, overeenkomstig het nationale recht, een toereikende aansprakelijkheidsverzekering af;

d) verstrekt aan personen die gebruik wensen te maken van een gekwalificeerde vertrouwensdienst duidelijke en volledige informatie over de precieze voorwaarden betreffende het gebruik van die dienst, met inbegrip van eventuele beperkingen op het gebruik ervan, alvorens een contractuele verbintenis aan te gaan;

e) maakt gebruik van betrouwbare systemen en producten die beschermd zijn tegen wijziging en die de technische veiligheid en betrouwbaarheid waarborgen van de processen die zij ondersteunen;

f) maakt gebruik van betrouwbare systemen voor de opslag van aan hem verstrekte gegevens in verifieerbare vorm, zodat:

i) de gegevens uitsluitend publiek beschikbaar zijn indien de persoon op wie de gegevens betrekking hebben, hiervoor toestemming heeft gegeven,

ii) alleen bevoegde personen de opgeslagen gegevens kunnen invoeren en wijzigen,

iii) de authenticiteit van de gegevens kan worden gecontroleerd;

g) neemt passende maatregelen tegen vervalsing en diefstal van gegevens;

h) legt gedurende een passende periode, ook nadat de gekwalificeerde verlener van vertrouwensdiensten zijn activiteiten heeft gestaakt, alle relevante informatie vast met betrekking tot de gegevens die de gekwalificeerde verlener van vertrouwensdiensten heeft afgegeven en ontvangen, en houdt deze informatie toegankelijk, met name om ten behoeve van gerechtelijke procedures bewijzen te kunnen leveren en om de continuïteit van de dienst te waarborgen. Dit vastleggen mag elektronisch plaatsvinden;

i) heeft een geactualiseerd beëindigingsplan om de continuïteit van de dienst te verzekeren in overeenstemming met de door het toezichthoudende orgaan op grond van artikel 17, lid 4, onder i), geverifieerde bepalingen;

j) zorgt voor wettelijke verwerking van persoonsgegevens in overeenstemming met Richtlijn 95/46/EG;

k) legt, indien het gaat om gekwalificeerde verleners van vertrouwensdiensten die gekwalificeerde certificaten afgeven, een certificatendatabank aan en houdt deze actueel.

3. Indien een gekwalificeerde verlener van vertrouwensdiensten die gekwalificeerde certificaten afgeeft, beslist een certificaat in te trekken, dan registreert hij deze intrekking in zijn certificatendatabank en maakt hij de ingetrokken status van het certificaat tijdig, en in elk geval binnen 24 uur na ontvangst van het verzoek, bekend. De intrekking wordt onmiddellijk na de bekendmaking ervan van kracht.

4. Wat lid 3 betreft, verstrekken gekwalificeerde verleners van vertrouwensdiensten die gekwalificeerde certificaten afgeven, aan elke vertrouwende partij informatie over de geldigheid of ingetrokken status van door hen afgegeven gekwalificeerde certificaten. Deze informatie is op elk moment, en ook na de geldigheidsduur van het certificaat, in ieder geval per certificaat beschikbaar in een geautomatiseerde vorm die betrouwbaar, kosteloos en efficiënt is.

5. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake betrouwbare systemen en producten, die voldoen aan de vereisten uit hoofde van lid 2, onder e) en f). Indien betrouwbare systemen en producten aan dergelijke normen voldoen, wordt aangenomen dat er overeenstemming is met de in dit artikel bepaalde eisen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 48, lid 2, bedoelde onderzoeksprocedure.

AFDELING 4

Elektronische handtekeningen

Artikel 25

Rechtsgevolgen van elektronische handtekeningen

1. Het rechtsgevolg van een elektronische handtekening en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures mogen niet worden ontkend louter op grond van het feit dat de handtekening elektronisch is of niet aan de eisen voor gekwalificeerde elektronische handtekeningen voldoet.

2. Een gekwalificeerde elektronische handtekening heeft hetzelfde rechtsgevolg als een handgeschreven handtekening.

3. Een gekwalificeerde elektronische handtekening die op een in een lidstaat afgegeven gekwalificeerd certificaat is gebaseerd, wordt in alle andere lidstaten als een gekwalificeerde elektronische handtekening erkend.

Artikel 26

Eisen voor geavanceerde elektronische handtekeningen

Een geavanceerde elektronische handtekening voldoet aan de volgende eisen:

a) zij is op unieke wijze aan de ondertekenaar verbonden;

b) zij maakt het mogelijk de ondertekenaar te identificeren;

c) zij komt tot stand met gegevens voor het aanmaken van elektronische handtekeningen die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitende controle kan gebruiken, en

d) zij is op zodanige wijze aan de daarmee ondertekende gegevens verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.

Artikel 27

Elektronische handtekeningen in openbare diensten

1. Indien een lidstaat een geavanceerde elektronische handtekening vereist voor het gebruik van een door of namens een openbare instantie aangeboden onlinedienst, erkent die lidstaat geavanceerde elektronische handtekeningen, geavanceerde elektronische handtekeningen gebaseerd op een gekwalificeerd certificaat voor elektronische handtekeningen, en gekwalificeerde elektronische handtekeningen, op zijn minst in de formaten of gebruikmakend van methoden die zijn gedefinieerd in de in lid 5 bedoelde uitvoeringshandelingen.

2. Indien een lidstaat een op een gekwalificeerd certificaat gebaseerde geavanceerde elektronische handtekening vereist voor het gebruik van een door of namens een openbare instantie aangeboden onlinedienst, erkent die lidstaat geavanceerde elektronische handtekeningen gebaseerd op een gekwalificeerd certificaat en gekwalificeerde elektronische handtekeningen, op zijn minst in de formaten of gebruikmakend van de methoden die zijn gedefinieerd in de in lid 5 bedoelde uitvoeringshandelingen.

3. De lidstaten vereisen voor grensoverschrijdend gebruik bij een door een openbare instantie aangeboden onlinedienst geen elektronische handtekening van een hoger betrouwbaarheidsniveau dan een gekwalificeerde elektronische handtekening.

4. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake geavanceerde elektronische handtekeningen. Indien een geavanceerde elektronische handtekening aan die normen voldoet, wordt zij geacht in overeenstemming te zijn met de in de leden 1 en 2 van dit artikel en in artikel 26, bedoelde vereisten voor geavanceerde elektronische handtekeningen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 48, lid 2, bedoelde onderzoeksprocedure.

5. Uiterlijk op 18 september 2015, rekening houdend met bestaande praktijken, normen en rechtshandelingen van de Unie, definieert de Commissie door middel van uitvoeringshandelingen referentieformaten van geavanceerde elektronische handtekeningen of referentiemethoden wanneer alternatieve formaten worden gebruikt. Deze uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 28

Gekwalificeerde certificaten voor elektronische handtekeningen

1. Gekwalificeerde certificaten voor elektronische handtekeningen voldoen aan de in bijlage I vastgestelde eisen.

2. Voor gekwalificeerde certificaten voor elektronische handtekeningen gelden geen dwingende eisen die strenger zijn dan de in bijlage I vastgestelde eisen.

3. Gekwalificeerde certificaten voor elektronische handtekeningen kunnen facultatieve aanvullende specifieke attributen hebben. Die attributen hebben geen invloed op de interoperabiliteit en de erkenning van gekwalificeerde elektronische handtekeningen.

4. Indien een gekwalificeerd certificaat voor elektronische handtekeningen na initiële activering wordt ingetrokken, verliest het zijn geldigheid vanaf het moment van de intrekking en kan de status ervan in geen geval worden hersteld.

5. Behoudens de hierna volgende voorwaarden kunnen lidstaten nationale regels vaststellen inzake de tijdelijke schorsing van een gekwalificeerd certificaat voor elektronische handtekeningen:

a) indien een gekwalificeerd certificaat voor elektronische handtekeningen tijdelijk is geschorst, verliest dit certificaat gedurende de periode van de schorsing zijn geldigheid;

b) de periode van schorsing wordt duidelijk aangegeven in de certificatendatabank en de schorsingsstatus is, gedurende de schorsingsperiode, zichtbaar vanuit de dienst die informatie over de status van het certificaat geeft.

6. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake gekwalificeerde certificaten voor elektronische handtekeningen. Indien een gekwalificeerd certificaat voor elektronische handtekeningen aan dergelijke normen voldoet, wordt aangenomen dat er overeenstemming is met de in bijlage I vastgestelde eisen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 48, lid 2, bedoelde onderzoeksprocedure.

Artikel 29

Eisen voor gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen

1. Gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen dienen te voldoen aan de in bijlage II vastgestelde eisen.

2. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen. Indien een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen aan dergelijke normen voldoet, wordt aangenomen dat er overeenstemming is met de in bijlage II vastgestelde eisen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 48, lid 2, bedoelde onderzoeksprocedure.

Artikel 30

Certificering van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen

1. De overeenstemming van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen met de in bijlage II vastgestelde eisen wordt gecertificeerd door geschikte, daartoe door de lidstaten aangewezen openbare of private organen.

2. De lidstaten verstrekken aan de Commissie de namen en adressen van de in lid 1 bedoelde openbare of private organen. De Commissie stelt deze informatie beschikbaar aan de lidstaten.

3. De in lid 1 bedoelde certificering is gebaseerd op een van de volgende elementen:

a) een veiligheidsbeoordeling uitgevoerd in overeenstemming met een van de normen inzake de veiligheidsbeoordeling van producten op het gebied van informatietechnologie die zijn opgenomen in de overeenkomstig de tweede alinea vastgestelde lijst, of

b) een ander proces dan het in punt a) vermelde, op voorwaarde dat dit proces vergelijkbare beveiligingsniveaus hanteert, en dat het in lid 1 bedoelde openbare of private orgaan de Commissie van het proces in kennis stelt. Dat proces mag alleen worden gebruikt als er geen in punt a) bedoelde normen zijn of wanneer een in punt a) bedoelde veiligheidsbeoordeling gaande is.

De Commissie stelt door middel van uitvoeringshandelingen een lijst vast voor de veiligheidsbeoordeling van producten op het gebied van onder a) bedoelde informatietechnologie. Deze uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

4. De Commissie is bevoegd overeenkomstig artikel 47 gedelegeerde handelingen vast te stellen met betrekking tot het opstellen van specifieke criteria waaraan de aangewezen organen zoals bedoeld in lid 1 van dit artikel moeten voldoen.

Artikel 31

Publicatie van een lijst van gecertificeerde gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen

1. De lidstaten verstrekken de Commissie onverwijld, en uiterlijk één maand na het voltooien van de certificering, informatie over gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen die zijn gecertificeerd door de organen zoals bedoeld in artikel 30, lid 1. Zij bezorgen de Commissie ook onverwijld, en uiterlijk één maand na het annuleren van de certificering, informatie over middelen voor het aanmaken van elektronische handtekeningen die niet meer gecertificeerd zijn.

2. De Commissie stelt op basis van de ontvangen informatie een lijst op van gecertificeerde gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen, publiceert deze lijst en houdt haar bij.

3. De Commissie kan door middel van uitvoeringshandelingen formaten en procedures omschrijven die gelden voor de toepassing van lid 1. Deze uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 32

Eisen voor de validering van gekwalificeerde elektronische handtekeningen

1. Het valideringsproces voor een gekwalificeerde elektronische handtekening bevestigt de geldigheid van een gekwalificeerde elektronische handtekening, op voorwaarde dat:

a) het certificaat dat de handtekening ondersteunt op het tijdstip van ondertekening een gekwalificeerd certificaat voor elektronische handtekeningen was overeenkomstig bijlage I;

b) het gekwalificeerd certificaat werd afgegeven door een gekwalificeerd verlener van vertrouwensdiensten en op het tijdstip van ondertekening geldig was;

c) de gegevens voor het valideren van de handtekening overeenstemmen met de gegevens die aan de vertrouwende partij zijn verstrekt;

d) de unieke reeks gegevens die in het certificaat verwijst naar de ondertekenaar, correct wordt doorgegeven aan de vertrouwende partij;

e) de vertrouwende partij duidelijk wordt gewezen op het eventuele gebruik van een pseudoniem op het tijdstip van ondertekening;

f) de elektronische handtekening werd aangemaakt met behulp van een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen;

g) de integriteit van de ondertekende gegevens niet is aangetast;

h) op het tijdstip van ondertekening voldaan was aan de in artikel 26, bedoelde eisen.

2. Het systeem dat is gebruikt voor het valideren van de gekwalificeerde elektronische handtekening verstrekt het juiste resultaat van het valideringsproces aan de vertrouwende partij en stelt deze in de gelegenheid om veiligheidsproblemen te identificeren.

3. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake de validering van gekwalificeerde elektronische handtekeningen. Indien de validering van gekwalificeerde elektronische handtekeningen aan dergelijke normen voldoet, wordt aangenomen dat er overeenstemming is met de in lid 1 vastgestelde eisen. Deze uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 33

Gekwalificeerde valideringsdienst voor gekwalificeerde elektronische handtekeningen

1. Een gekwalificeerde valideringsdienst voor gekwalificeerde elektronische handtekeningen kan uitsluitend worden verleend door een gekwalificeerde verlener van vertrouwensdiensten die:

a) validering verstrekt overeenkomstig artikel 32, lid 1, en

b) de vertrouwende partijen in staat stelt om het resultaat van het valideringsproces op een geautomatiseerde, betrouwbare en efficiënte manier, voorzien van de geavanceerde elektronische handtekening of het geavanceerde elektronische zegel van de verlener van de gekwalificeerde valideringsdienst, te ontvangen.

2. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake de in lid 1 bedoelde gekwalificeerde valideringsdienst. Indien de dienst voor de validering van gekwalificeerde elektronische handtekeningen aan dergelijke normen voldoet, wordt aangenomen dat er overeenstemming is met de in lid 1 vastgestelde eisen. Deze uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 34

Gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische handtekeningen

1. Een gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische handtekeningen kan uitsluitend worden verleend door een gekwalificeerde verlener van vertrouwensdiensten die procedures en technologieën hanteert welke het mogelijk maken de betrouwbaarheid van de gekwalificeerde elektronische handtekeningen te verlengen tot na de technologische geldigheidsduur.

2. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake de gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische handtekeningen. Indien de voorzieningen voor de gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische handtekeningen aan dergelijke normen voldoen, wordt aangenomen dat er overeenstemming is met de in lid 1 vastgestelde eisen. Deze uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

AFDELING 5

Elektronische zegels

Artikel 35

Rechtsgevolgen van elektronische zegels

1. Het rechtsgevolg van een elektronisch zegel en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures mogen niet worden ontkend louter op grond van het feit dat het zegel elektronisch is of niet aan de eisen voor gekwalificeerde elektronische zegels voldoet.

2. Voor een gekwalificeerd elektronisch zegel geldt het vermoeden van integriteit van de gegevens en van juistheid van de oorsprong van de gegevens waaraan het gekwalificeerd elektronisch zegel is verbonden.

3. Een gekwalificeerd elektronisch zegel dat op een in een lidstaat afgegeven gekwalificeerd certificaat is gebaseerd, wordt in alle andere lidstaten als een gekwalificeerd elektronisch zegel erkend.

Artikel 36

Eisen voor geavanceerde elektronische zegels

Een geavanceerd elektronisch zegel voldoet aan de volgende eisen:

a) het is op unieke wijze aan de aanmaker van het zegel verbonden;

b) het maakt het mogelijk de aanmaker van het zegel te identificeren;

c) het komt tot stand met gebruikmaking van gegevens voor het aanmaken van elektronische zegels die de aanmaker van het zegel met een hoog vertrouwensniveau onder zijn controle kan gebruiken voor het aanmaken van elektronische zegels;

d) het is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.

Artikel 37

Elektronische zegels in openbare diensten

1. Indien een lidstaat een geavanceerd elektronisch zegel vereist voor het gebruik van een door of namens een openbare instantie aangeboden onlinedienst, erkent die lidstaat geavanceerde elektronische zegels, geavanceerde elektronische zegels gebaseerd op een gekwalificeerd certificaat voor elektronische zegels en gekwalificeerde elektronische zegels, op zijn minst in de formaten of gebruikmakend van methoden die zijn gedefinieerd in de in lid 5 bedoelde uitvoeringshandelingen.

2. Indien een lidstaat een op een gekwalificeerd certificaat gebaseerd geavanceerd elektronisch zegel vereist voor het gebruik van een door of namens een openbare instantie aangeboden onlinedienst, erkent die lidstaat geavanceerde elektronische zegels gebaseerd op een gekwalificeerd certificaat en gekwalificeerde elektronische zegels, op zijn minst in de formaten of gebruikmakend van methoden die zijn gedefinieerd in de in lid 5 bedoelde uitvoeringshandelingen.

3. De lidstaten vragen voor grensoverschrijdend gebruik bij een door een openbare instantie aangeboden onlinedienst geen elektronisch zegel van een hoger betrouwbaarheidsniveau dan het gekwalificeerde elektronische zegel.

4. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake geavanceerde elektronische zegels. Indien een geavanceerd elektronisch zegel aan die normen voldoet, wordt het geacht in overeenstemming te zijn met de in de leden 1 en 2 van dit artikel, en in artikel 36, bedoelde vereisten voor geavanceerde elektronische zegels. Deze uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

5. Uiterlijk op 18 september 2015, en rekening houdend met bestaande praktijken, normen en rechtshandelingen van de Unie, definieert de Commissie door middel van uitvoeringshandelingen referentieformaten van geavanceerde elektronische zegels of referentiemethoden indien alternatieve formaten worden gebruikt. Deze uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 38

Gekwalificeerde certificaten voor elektronische zegels

1. Gekwalificeerde certificaten voor elektronische zegels voldoen aan de in bijlage III vastgestelde eisen.

2. Voor gekwalificeerde certificaten voor elektronische zegels gelden geen dwingende eisen die strenger zijn dan de in bijlage III vastgestelde eisen.

3. Gekwalificeerde certificaten voor elektronische zegels kunnen facultatieve aanvullende specifieke attributen hebben. Die attributen hebben geen invloed op de interoperabiliteit en de erkenning van gekwalificeerde elektronische zegels.

4. Indien een gekwalificeerd certificaat voor elektronische zegels na initiële activering wordt ingetrokken, verliest het zijn geldigheid vanaf het moment van de intrekking en kan de status ervan in geen geval worden hersteld.

5. Behoudens de hierna volgende voorwaarden kunnen lidstaten nationale regels vaststellen inzake de tijdelijke schorsing van gekwalificeerde certificaten voor elektronische zegels:

a) indien een gekwalificeerd certificaat voor elektronische zegels tijdelijk is geschorst, verliest dit certificaat gedurende de periode van de schorsing zijn geldigheid;

b) de periode van schorsing wordt duidelijk aangegeven in de certificatendatabank en de schorsingsstatus is, gedurende de schorsingsperiode, zichtbaar vanuit de dienst die informatie geeft over de status van het certificaat.

6. De Commissie kan door middel van uitvoeringshandelingen referentienummers opstellen voor normen inzake gekwalificeerde certificaten voor elektronische zegels. Indien een gekwalificeerd certificaat voor elektronisch zegels aan dergelijke normen voldoet, wordt aangenomen dat er overeenstemming is met de in bijlage III vastgestelde eisen. Deze uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 39

Gekwalificeerde middelen voor het aanmaken van elektronische zegels

1. Artikel 29 is van overeenkomstige toepassing op eisen voor gekwalificeerde middelen voor het aanmaken van elektronische zegels.

2. Artikel 30 is van overeenkomstige toepassing op de certificatie van gekwalificeerde middelen voor het aanmaken van elektronische zegels.

3. Artikel 31 is van overeenkomstige toepassing op de publicatie van een lijst van gecertificeerde gekwalificeerde middelen voor het aanmaken van elektronische zegels.

Artikel 40

Validering en bewaring van gekwalificeerde elektronische zegels

De artikelen 32, 33 en 34 zijn van overeenkomstige toepassing op de validering en bewaring van gekwalificeerde elektronische zegels.

AFDELING 6

Elektronisch tijdstempel

Artikel 41

Rechtsgevolg van elektronische tijdstempels

1. Het rechtsgevolg van een elektronisch tijdstempel en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures mogen niet worden ontkend louter op grond van het feit dat het stempel elektronisch is of niet aan de eisen voor gekwalificeerde elektronische tijdstempels voldoet.

2. Voor een gekwalificeerd elektronisch tijdstempel geldt het vermoeden van de juistheid van de aangegeven datum en het aangegeven tijdstip, en van de integriteit van de gegevens waaraan de datum en het tijdstip zijn gekoppeld.

3. Een gekwalificeerd elektronisch tijdstempel, afgegeven in een lidstaat, wordt in alle lidstaten als een gekwalificeerd elektronisch tijdstempel erkend.

Artikel 42

Eisen voor gekwalificeerde elektronische tijdstempels

1. Een gekwalificeerd elektronisch tijdstempel voldoet aan de volgende eisen:

a) het tijdstempel koppelt de datum en het tijdstip op zodanige wijze aan gegevens dat onmerkbare wijziging van de gegevens redelijkerwijs kan worden uitgesloten;

b) het stempel is gebaseerd op een nauwkeurige tijdsbron die aan de gecoördineerde universele tijd gekoppeld is; en

c) het stempel wordt ondertekend met behulp van een geavanceerde elektronische handtekening of verzegeld met een geavanceerd elektronisch zegel van de gekwalificeerde verlener van vertrouwensdiensten, of met behulp van een andere gelijkwaardige methode.

2. De Commissie kan door middel van uitvoeringshandelingen referentienummers opstellen voor normen inzake de koppeling van datum en tijdstip aan gegevens en voor nauwkeurige tijdsbronnen. Indien de koppeling van datum en tijdstip aan gegevens en de nauwkeurige tijdsbron aan dergelijke normen voldoen, wordt aangenomen dat er overeenstemming is met de in lid 1 vastgestelde eisen.Deze uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

AFDELING 7

Diensten voor elektronisch aangetekende bezorging

Artikel 43

Rechtsgevolg van een dienst voor elektronisch aangetekende bezorging

1. Het rechtsgevolg en toelaatbaarheid als bewijsmiddel in gerechtelijke procedures van gegevens die via een dienst voor elektronisch aangetekende bezorging verstuurd en ontvangen worden, mogen niet worden ontkend louter op grond van het feit dat de dienst elektronisch is of niet aan de eisen voor de gekwalificeerde dienst voor elektronisch aangetekende bezorging voldoet.

2. Voor gegevens die via een gekwalificeerde dienst voor elektronisch aangetekende bezorging worden verstuurd en ontvangen, geldt het vermoeden van integriteit van de gegevens, van de verzending van die gegevens door de geïdentificeerde afzender, van de ontvangst daarvan door de geïdentificeerde geadresseerde, en van de nauwkeurigheid van de datum en het tijdstip van verzending en van ontvangst, zoals aangegeven door de gekwalificeerde dienst voor elektronisch aangetekende bezorging.

Artikel 44

Eisen voor gekwalificeerde diensten voor elektronisch aangetekende bezorging

1. Gekwalificeerde diensten voor elektronisch aangetekende bezorging voldoen aan de volgende eisen:

a) zij worden verleend door een of meer gekwalificeerde verleners van vertrouwensdiensten;

b) zij bevestigen op een hoog vertrouwensniveau de identiteit van de zender;

c) zij bevestigen de identiteit van de geadresseerde, alvorens de gegevens te bezorgen;

d) het verzenden en ontvangen van gegevens wordt beveiligd door een geavanceerde elektronische handtekening of een geavanceerd elektronisch zegel van een gekwalificeerde verlener van vertrouwensdiensten, en wel op zodanige wijze dat onmerkbare wijziging van gegevens kan worden uitgesloten;

e) de verzender en de geadresseerde van de gegevens worden op duidelijke wijze in kennis gesteld van eventuele wijzigingen van de gegevens die nodig zijn voor het verzenden of ontvangen van de gegevens;

f) de datum en het tijdstip van verzenden, ontvangen en wijzigen van gegevens worden aangegeven met een gekwalificeerd elektronisch tijdstempel.

Wanneer gegevens overgedragen worden tussen twee of meer gekwalificeerde verleners van vertrouwensdiensten, zijn de eisen onder a) tot en met f) van toepassing op alle gekwalificeerde verleners van vertrouwensdiensten.

2. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake processen voor het verzenden en ontvangen van gegevens. Indien het proces voor het verzenden en ontvangen van gegevens aan dergelijke normen voldoet, wordt aangenomen dat er overeenstemming is met de in lid 1 vastgestelde eisen. Deze uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

AFDELING 8

Authenticatie van websites

Artikel 45

Eisen voor gekwalificeerde certificaten voor websiteauthenticatie

1. Gekwalificeerde certificaten voor authenticatie van websites voldoen aan de in bijlage IV vastgestelde eisen.

2. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake gekwalificeerde certificaten voor de authenticatie van websites. Indien een gekwalificeerd certificaat voor de authenticatie van websites aan dergelijke normen voldoet, wordt aangenomen dat er overeenstemming is met de in bijlage IV vastgestelde eisen. Deze uitvoeringshandelingen worden volgens de in artikel 48, lid 2, bedoelde onderzoeksprocedure vastgesteld.

HOOFDSTUK IV

ELEKTRONISCHE DOCUMENTEN

Artikel 46

Rechtsgevolgen van elektronische documenten

Het rechtsgevolg van een elektronisch document en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures mogen niet worden ontkend louter op grond van het feit dat het document elektronisch is.

HOOFDSTUK V

BEVOEGDHEIDSDELEGATIES EN UITVOERINGSBEPALINGEN

Artikel 47

Uitoefening van de bevoegdheidsdelegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend onder de in dit artikel neergelegde voorwaarden.

2. De in artikel 30, lid 4, bedoelde bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend voor onbepaalde duur met ingang van 17 september 2014.

3. Het Europees Parlement of de Raad kan de in artikel 30, lid 4, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie* of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.

4. Zodra de Commissie een gedelegeerde handeling vaststelt, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.

5. Een overeenkomstig artikel 30, lid 4, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van twee maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad daartegen bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben medegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met twee maanden verlengd.

Artikel 48

Comitéprocedure

1. De Commissie wordt bijgestaan door een comité. Dat comité is een comité in de zin van Verordening (EU) nr. 182/2011.

2. Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening (EU) nr. 182/2011 van toepassing.

HOOFDSTUK VI

SLOTBEPALINGEN

Artikel 49

Evaluatie

De Commissie evalueert de toepassing van deze verordening en brengt daarover uiterlijk op 1 juli 2020 verslag uit bij het Europees Parlement en de Raad. De Commissie evalueert met name of het gepast is het toepassingsgebied van deze verordening dan wel de specifieke bepalingen ervan, met inbegrip van artikel 6, artikel 7, onder f), en de artikelen 34, 43, 44 en 45 te wijzigen, rekening houdend met de ervaring met de toepassing van deze verordening, alsook met technologische, marktgebonden en juridische ontwikkelingen.

Het in de eerste alinea bedoelde verslag gaat, in voorkomend geval, vergezeld van wetgevingsvoorstellen.

Daarnaast dient de Commissie elke vier jaar na het in de eerste alinea bedoelde verslag een verslag over de vooruitgang bij de verwezenlijking van de doelstellingen van deze verordening in bij het Europees Parlement en de Raad.

Artikel 50

Intrekking

1. Richtlijn 1999/93/EG wordt ingetrokken met ingang van 1 juli 2016.

2. Verwijzingen naar de ingetrokken richtlijn gelden als verwijzingen naar de onderhavige verordening.

Artikel 51

Overgangsmaatregelen

1. Veilige middelen voor het aanmaken van handtekeningen waarvan de overeenstemming bepaald is overeenkomstig artikel 3, lid 4, van Richtlijn 1999/93/EG, worden beschouwd als gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen in de zin van de onderhavige verordening.

2. Gekwalificeerde certificaten voor natuurlijke personen in de zin van Richtlijn 1999/93/EG worden, totdat zij verlopen, beschouwd als gekwalificeerde certificaten voor elektronische handtekeningen in de zin van onderhavige verordening.

3. Een certificatiedienstverlener die gekwalificeerde certificaten overeenkomstig Richtlijn 1999/93/EG afgeeft, dient zo spoedig mogelijk, maar niet later dan 1 juli 2017, een conformiteitsbeoordelingsverslag in bij het toezichthoudend orgaan. Tot de indiening van dat conformiteitsbeoordelingsverslag en de voltooiing van de beoordeling ervan door het toezichthoudend orgaan wordt die certificatiedienstverlener beschouwd als een gekwalificeerde verlener van vertrouwensdiensten in de zin van deze verordening.

4. Indien een certificatiedienstverlener die gekwalificeerde certificaten overeenkomstig Richtlijn 1999/93/EG afgeeft, niet binnen de in lid 3 bedoelde termijn een conformiteitsbeoordelingsverslag indient bij het toezichthoudend orgaan, wordt die certificatiedienstverlener vanaf 2 juli 2017 niet beschouwd als gekwalificeerde verlener van vertrouwensdiensten in de zin van deze verordening.

Artikel 52

Inwerkingtreding

1. Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

2. Deze verordening is van toepassing vanaf 1 juli 2016, met uitzondering van onderstaande:

a) artikel 8, lid 3, artikel 9, lid 5, artikel 12, lid 2 tot en met 9, artikel 17, lid 8, artikel 19, lid 4, artikel 20, lid 4, artikel 21, lid 4, artikel 22, lid 5, artikel 23, lid 3, artikel 24, lid 5, artikel 27, lid 4 en lid 5, artikel 28, lid 6, artikel 29, lid 2, artikel 30, lid 3 en lid 4, artikel 31, lid 3, artikel 32, lid 3, artikel 33, lid 2, artikel 34, lid 2, artikel 37, lid 4 en lid 5, artikel 38, lid 6, artikel 42, lid 2, artikel 44, lid 2, artikel 45, lid 2, en artikelen 47 en 48 zijn van toepassing met ingang van 17 september 2014;

b) artikel 7, artikel 8, leden 1 en 2, de artikelen 9, 10, 11 en artikel 12, lid 1, zijn van toepassing vanaf de datum van toepassing van de in artikel 8, lid 3, en artikel 12, lid 8, bedoelde uitvoeringshandelingen;

c) artikel 6 is van toepassing vanaf drie jaar na de datum van toepassing van de in artikel 8, lid 3, en artikel 12, lid 8, bedoelde uitvoeringshandelingen.

3. Indien het aangemelde stelsel voor elektronische identificatie voorkomt in de lijst die de Commissie krachtens artikel 9 bekendmaakt, en wel vóór de datum in lid 2, onder c), van dit artikel, wordt het elektronische identificatiemiddel in het kader van dat stelsel krachtens artikel 6 erkend binnen twaalf maanden na de bekendmaking van dat stelsel, maar niet vóór de datum in lid 2, onder c), van dit artikel.

4. Niettegenstaande lid 2, onder c), van dit artikel kan een lidstaat besluiten dat elektronische identificatiemiddelen in het kader van een stelsel voor elektronische identificatie, krachtens artikel 9, lid 1, door een andere lidstaat aangemeld, in de eerste lidstaat worden erkend met ingang van de datum van toepassing van de in artikel 8, lid 3, en artikel 12, lid 8, bedoelde uitvoeringshandelingen. De betrokken lidstaten stellen de Commissie daarvan in kennis. De Commissie maakt deze informatie openbaar.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 23 juli 2014.

Voor het Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*
M. SCHULZ	S. GOZI

BIJLAGE I

EISEN VOOR GEKWALIFICEERDE CERTIFICATEN VOOR ELEKTRONISCHE HANDTEKENINGEN

Gekwalificeerde certificaten voor elektronische handtekeningen bevatten:

a) een vermelding, ten minste in een vorm die geschikt is voor automatische verwerking, dat het certificaat afgegeven is als een gekwalificeerd certificaat voor elektronische handtekeningen;

b) een reeks gegevens die ondubbelzinnig verwijzen naar de gekwalificeerde verlener van vertrouwensdiensten die de gekwalificeerde certificaten afgeeft, met inbegrip van ten minste de lidstaat waarin de verlener is gevestigd en

— voor een rechtspersoon: de naam en, indien van toepassing, het registratienummer zoals vermeld in de officiële registers,

— voor een natuurlijke persoon: de naam van de persoon;

c) op zijn minst de naam van de ondertekenaar of een pseudoniem; als er een pseudoniem wordt gebruikt, wordt dat duidelijk aangegeven;

d) gegevens voor de validering van elektronische handtekeningen, die overeenkomen met de gegevens voor het aanmaken van de elektronische handtekening;

e) informatie over begin en einde van de geldigheidsduur van het certificaat;

f) de identiteitscode van het certificaat, die uniek moet zijn voor de gekwalificeerde verlener van vertrouwensdiensten;

g) de geavanceerde elektronische handtekening of het geavanceerde elektronische zegel van de afgevende gekwalificeerde verlener van vertrouwensdiensten;

h) de locatie waar het certificaat ter ondersteuning van de geavanceerde elektronische handtekening of het geavanceerde elektronische zegel als bedoeld onder g) gratis beschikbaar is;

i) de locatie van de diensten waar informatie kan worden opgevraagd over de geldigheidsstatus van het gekwalificeerde certificaat;

j) indien de gegevens voor het aanmaken van een elektronische handtekening die gekoppeld zijn aan de gegevens voor de validering van de elektronische handtekening zich bevinden in een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen, een passende vermelding hiervan, ten minste in een vorm die geschikt is voor automatische verwerking.

BIJLAGE II

EISEN VOOR GEKWALIFICEERDE MIDDELEN VOOR HET AANMAKEN VAN ELEKTRONISCHE HANDTEKENINGEN

1. Gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen waarborgen via passende technieken en procedures dat ten minste:

   a) de vertrouwelijkheid van de gegevens die worden gebruikt om elektronische handtekeningen aan te maken redelijkerwijs gewaarborgd is;

   b) de gegevens voor het aanmaken van elektronische handtekeningen in de praktijk slechts één keer kunnen voorkomen;

   c) de gegevens voor het aanmaken van elektronische handtekeningen met redelijke zekerheid niet kunnen worden afgeleid en dat de elektronische handtekening op betrouwbare wijze beschermd is tegen vervalsing met de thans beschikbare technologie;

   d) de gegevens voor het aanmaken van elektronische handtekeningen door de legitieme ondertekenaar op betrouwbare wijze kunnen worden beschermd tegen gebruik door anderen.

2. Gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen laten de te ondertekenen gegevens ongewijzigd en beletten niet dat die gegevens vóór ondertekening aan de ondertekenaar worden voorgelegd.

3. Het genereren of beheren van de gegevens voor het aanmaken van elektronische handtekeningen namens de ondertekenaar kan alleen worden uitgevoerd door een gekwalificeerde verlener van vertrouwensdiensten.

4. Onverminderd punt 1, onder d), mogen gekwalificeerde verleners van vertrouwensdiensten die namens de ondertekenaar gegevens voor het aanmaken van elektronische handtekeningen beheren, de gegevens voor het aanmaken van elektronische handtekeningen alleen dupliceren voor back-updoeleinden, op voorwaarde dat aan de volgende eisen wordt voldaan:

   a) de beveiliging van de gedupliceerde gegevensverzamelingen moet van hetzelfde niveau zijn als de beveiliging van de originele gegevensverzamelingen;

   b) het aantal gedupliceerde gegevensverzamelingen mag niet hoger zijn dan het minimum dat nodig is om de continuïteit van de dienst te waarborgen.

BIJLAGE III

EISEN VOOR GEKWALIFICEERDE CERTIFICATEN VOOR ELEKTRONISCHE ZEGELS

Gekwalificeerde certificaten voor elektronische zegels bevatten:

a) een vermelding, ten minste in een vorm die geschikt is voor automatische verwerking, dat het certificaat is afgegeven als een gekwalificeerd certificaat voor elektronische zegels;

b) een reeks gegevens die ondubbelzinnig verwijzen naar de gekwalificeerde verlener van vertrouwensdiensten die de gekwalificeerde certificaten afgeeft, met inbegrip van ten minste de lidstaat waar die dienstverlener is gevestigd en

— voor een rechtspersoon: de naam en, indien van toepassing, het registratienummer zoals vermeld in de officiële registers,

— voor een natuurlijke persoon: de naam van de persoon;

c) ten minste de naam van de aanmaker van het zegel en, indien van toepassing, het registratienummer zoals vermeld in de officiële registers;

d) gegevens voor de validering van elektronische zegels, die overeenkomen met de gegevens voor het aanmaken van elektronische zegels;

e) informatie over begin en einde van de geldigheidsduur van het certificaat;

f) de identiteitscode van het certificaat, die uniek moet zijn voor de gekwalificeerde verlener van vertrouwensdiensten;

g) de geavanceerde elektronische handtekening of het geavanceerde elektronische zegel van de afgevende gekwalificeerde verlener van vertrouwensdiensten;

h) de locatie waar het certificaat ter ondersteuning van de geavanceerde elektronische handtekening of het geavanceerde elektronische zegel als bedoeld onder g) gratis beschikbaar is;

i) de locatie van de diensten waar informatie kan worden opgevraagd over de geldigheidsstatus van het gekwalificeerde certificaat;

j) indien de gegevens voor het aanmaken van elektronische zegels die gekoppeld zijn aan de gegevens voor de validering voor elektronische zegels zich bevinden in een gekwalificeerd middel voor het aanmaken van elektronische zegels, een passende vermelding hiervan, ten minste in een vorm die geschikt is voor automatische verwerking.

BIJLAGE IV

EISEN VOOR GEKWALIFICEERDE CERTIFICATEN VOOR WEBSITE-AUTHENTICATIE

Gekwalificeerde certificaten voor websiteauthenticatie moeten het volgende bevatten:

a) een vermelding, ten minste in een vorm die geschikt is voor automatische verwerking, dat het certificaat afgegeven is als een gekwalificeerd certificaat voor websiteauthenticatie;

b) een reeks gegevens die ondubbelzinnig verwijzen naar de gekwalificeerde verlener van vertrouwensdiensten die de gekwalificeerde certificaten afgeeft, met inbegrip van ten minste de lidstaat waar die dienstverlener is gevestigd en

— voor een rechtspersoon: de naam en, indien van toepassing, het registratienummer zoals vermeld in de officiële registers,

— voor een natuurlijke persoon: de naam van de persoon;

c) voor natuurlijke personen: op zijn minst de naam van de persoon aan wie het certificaat is afgegeven, of een pseudoniem. Indien een pseudoniem wordt gebruikt, wordt dat duidelijk aangegeven;

voor rechtspersonen: ten minste de naam van de rechtspersoon aan wie het certificaat is afgegeven en, indien van toepassing, het registratienummer zoals vermeld in de officiële registers;

d) elementen van het adres, met inbegrip van ten minste de plaats en de staat, van de natuurlijke of rechtspersoon aan wie het certificaat is afgegeven en, indien van toepassing, zoals vermeld in de officiële registers;

e) de domeinnaam/-namen die wordt/worden geëxploiteerd door de natuurlijke of rechtspersoon aan wie het certificaat is afgegeven;

f) informatie over begin en einde van de geldigheidsduur van het certificaat;

g) de identiteitscode van het certificaat, die uniek moet zijn voor de gekwalificeerde verlener van vertrouwensdiensten;

h) de geavanceerde elektronische handtekening of het geavanceerde elektronische zegel van de afgevende gekwalificeerde verlener van vertrouwensdiensten;

i) de locatie waar het certificaat ter ondersteuning van de geavanceerde elektronische handtekening of het geavanceerde elektronische zegel als bedoeld onder h) gratis beschikbaar is;

j) de locatie van de valideringsstatusdiensten voor certificaten die gebruikt kunnen worden om informatie over de geldigheidsstatus van het gekwalificeerde certificaat te raadplegen.