



EUROPESE COMMISSIE

Brussel, 4.6.2012
COM(2012) 238 final

2012/0146 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

**betreffende elektronische identificatie en vertrouwensdiensten voor elektronische
transacties in de interne markt**

(Voor de EER relevante tekst)

{SWD(2012) 135 final}
{SWD(2012) 136 final}

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

In deze toelichting wordt een voorstel voor een wetgevingskader uiteengezet dat bedoeld is om het vertrouwen in elektronische transacties in de interne markt te bevorderen.

Het opbouwen van vertrouwen in een online-omgeving is essentieel voor economische ontwikkeling. Een gebrek aan vertrouwen leidt ertoe dat consumenten, bedrijven en overheidsdiensten aarzelen om transacties elektronisch uit te voeren en nieuwe diensten te gebruiken.

In de *Digitale Agenda voor Europa*¹ worden de bestaande hinderpalen voor de digitale ontwikkeling van Europa genoemd en wordt een voorstel gedaan voor wetgeving inzake de e-handtekening (kernactie 3) en de wederzijdse erkenning van e-identificatie en e-authenticatie (kernactie 16). Zo wordt een duidelijk rechtskader gecreëerd om fragmentatie en een gebrek aan interoperabiliteit te vermijden, digitaal burgerschap te stimuleren en cybercriminaliteit te voorkomen. Wetgeving gericht op wederzijdse erkenning van elektronische identificatie en authenticatie in de EU en herziening van de richtlijn inzake de elektronische handtekening zijn eveneens een kernactie in de *Single Market Act* (wetgevingspakket eengemaakte markt)², bedoeld om de eengemaakte digitale markt tot stand te brengen. De *routekaart voor stabiliteit en groei*³ benadrukt dat het toekomstige gemeenschappelijke wetgevingskader voor wederzijdse erkenning en aanvaarding van grensoverschrijdende elektronische identificatie en authenticatie een cruciale rol speelt in de ontwikkeling van de digitale economie.

Het voorgestelde wetgevingskader, dat bestaat uit een "*verordening van het Europees Parlement en de Raad inzake elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt*", heeft tot doel veilige en ongehinderde elektronische interactie tussen bedrijven, burgers en overheden mogelijk te maken en zo de effectiviteit van publieke en particuliere onlinediensten, e-business en elektronische handel in de EU te vergroten.

De bestaande EU-wetgeving, met name Richtlijn 1999/93/EG betreffende een "*gemeenschappelijk kader voor elektronische handtekeningen*"⁴ betreft feitelijk alleen elektronische handtekeningen. Er is geen uitgebreid grens- en sectoroverschrijdend EU-kader voor veilige, betrouwbare en gebruiksvriendelijke elektronische transacties dat elektronische identificatie, authenticatie en handtekeningen omvat.

Het doel is de bestaande wetgeving te versterken en zodanig uit te breiden dat zij op EU-niveau ook de wederzijdse erkenning en aanvaarding van aangemelde regelingen voor elektronische identificatie en andere essentiële verwante elektronische vertrouwensdiensten omvat.

¹ COM(2010) 245 van 19.5.2010.

² COM(2011) 206 definitief van 13.4.2011.

³ COM (2011) 669 van 12.10.2011.

⁴ PB L 13 van 19.1.2000, blz. 12.

2. RESULTATEN VAN DE RAADPLEGING VAN BELANGHEBBENDE PARTIJEN EN EFFECTBEOORDELINGEN

Dit initiatief vloeit voort uit een uitgebreide raadpleging over een herziening van het huidige wetgevingskader voor elektronische handtekeningen waarbij de Commissie feedback kreeg van de lidstaten, het Europees Parlement en andere belanghebbenden⁵. Een "mkb-testpanel" hield online een openbare raadpleging om de specifieke meningen en behoeften van het mkb vast te stellen; daarnaast werden ook andere doelgerichte raadplegingen van belanghebbenden georganiseerd^{6,7}. De Commissie gaf eveneens opdracht tot een aantal studies in verband met elektronische identificatie, authenticatie, handtekeningen en verwante vertrouwensdiensten (eIAS).

Het overleg maakte duidelijk dat een grote meerderheid van de belanghebbenden het erover eens was dat er behoefte was aan een herziening van het huidige kader om de leemten te vullen die er in de richtlijn inzake elektronische handtekeningen nog zijn. Men was van mening dat op deze manier beter zou kunnen worden ingespeeld op de uitdagingen die de snelle ontwikkeling van nieuwe technologieën (met name online- en mobiele toegang) en de toenemende mondialisering met zich meebrengen, terwijl de technologische onpartijdigheid van het wetgevingskader behouden blijft.

In overeenstemming met haar beleid voor een betere regelgeving, heeft de Commissie een effectbeoordeling uitgevoerd voor beleidsalternatieven. Er werden drie reeksen beleidsopties beoordeeld op het gebied van respectievelijk (1) de reikwijdte van het nieuwe kader, (2) het rechtsinstrument en (3) het vereiste niveau van toezicht⁸. De beleidsoptie die de voorkeur genoot, bleek te leiden tot grotere rechtszekerheid, betere coördinatie van nationaal toezicht, waarborging van de wederzijdse erkenning en aanvaarding van elektronische identificatieregelingen en omvatte tevens essentiële verwante vertrouwensdiensten. De conclusie van de effectbeoordeling was dat dit leidt tot een aanzienlijke verbetering van de rechtszekerheid, de veiligheid van en het vertrouwen in grensoverschrijdende elektronische transacties, met als gevolg minder fragmentering van de markt.

⁵ Voor meer informatie over de raadpleging, zie http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision

⁶ Op 10.3.2011 werd een workshop voor belanghebbenden georganiseerd met vertegenwoordigers uit de openbare en particuliere sector en de academische wereld om de wetgevingsmaatregelen te bespreken die nodig zijn om de uitdagingen van de toekomst aan te pakken. Tijdens een interactief forum werd van gedachten gewisseld en werden de verschillende standpunten betreffende de vraagstukken die in de openbare raadpleging aan de orde kwamen nader toegelicht. Verschillende organisaties zonden spontaan standpuntnota's in.

⁷ Met name het Poolse Voorzitterschap van de EU organiseerde een bijeenkomst met de lidstaten betreffende elektronische handtekeningen in Warschau op 9.11.2011 en over elektronische identificatie in Poznan op 17.11.2011. Op 25.1.2012 organiseerde de Commissie een workshop met de lidstaten om de resterende vraagstukken betreffende elektronische identificatie, authenticatie en handtekeningen te bespreken.

⁸ In de eerste reeks werden vier mogelijkheden onderzocht: het intrekken van de richtlijn betreffende e-handtekeningen; geen beleidswijziging; het verhogen van de rechtszekerheid, het stimuleren van de coördinatie van nationaal toezicht en het waarborgen van wederzijdse erkenning en aanvaarding van elektronische identificatie in de hele EU; en ten vierde uitbreiding zodat ook bepaalde verwante vertrouwensdiensten worden opgenomen. De tweede reeks bestond uit een beoordeling van de voordelen van regulering door middel van één instrument ten opzichte van twee instrumenten en door middel van een richtlijn ten opzichte van een verordening. De derde reeks was bedoeld om de mogelijkheden te onderzoeken die voortvloeien uit de toepassing van nationale toezichtsregelingen op basis van gemeenschappelijke essentiële toezichtseisen tegenover een toezichtstelsel op EU-basis. Met de hulp van een groep bestaande uit alle betrokken directoraten-generaal van de Commissie werden alle beleidsalternatieven beoordeeld op de doeltreffendheid ervan bij het halen van de beleidsdoelstellingen, op de economische gevolgen voor belanghebbenden (met inbegrip van de begroting van de EU-instellingen), op de sociale en milieugevolgen, en op de gevolgen ervan voor de administratieve last.

3. JURIDISCHE ASPECTEN VAN HET VOORSTEL

3.1 Rechtsgrondslag

Dit voorstel is gebaseerd op artikel 114 VWEU, dat handelt over het goedkeuren van regels om hinderpalen weg te nemen die het functioneren van de interne markt onnodig belemmeren. Burgers, bedrijven en overheidsdiensten hebben baat bij de wederzijdse erkenning en aanvaarding van grensoverschrijdende elektronische identificatie, authenticatie, handtekeningen en andere vertrouwensdiensten met het oog op de toegang tot en afwikkeling van elektronische procedures of transacties.

Een verordening wordt beschouwd als het meest geschikte rechtsinstrument. Door de rechtstreekse toepasselijkheid krachtens artikel 288 VWEU zal een verordening de juridische fragmentatie verminderen en de rechtszekerheid bevorderen door een geharmoniseerd pakket basisregels in te voeren dat bijdraagt tot de werking van de eengemaakte markt.

3.2 Subsidiariteit en evenredigheid

Om Europese maatregelen te rechtvaardigen moet het subsidiariteitsbeginsel worden gerespecteerd:

a) Grensoverschrijdende aard van het probleem (noodzakelijkheidstoets)

De grensoverschrijdende aard van eIAS vergt maatregelen van de Unie. Nationale maatregelen alleen volstaan niet om de doelstellingen te behalen die zijn vastgesteld in het kader van de *Europa 2020-strategie*⁹. Anderzijds heeft de ervaring geleerd dat nationale maatregelen *de facto* de interoperabiliteit van elektronische handtekeningen in de EU hebben belemmerd, en dat zij momenteel hetzelfde effect hebben op elektronische identificatie, elektronische authenticatie en verwante vertrouwensdiensten. Daarom is het noodzakelijk dat de EU een kader schept dat zich richt op de grensoverschrijdende interoperabiliteit en dat de regelingen voor toezicht verbetert. Elektronische identificatie kan in de voorgestelde verordening echter niet op dezelfde generieke manier worden behandeld als de andere elektronische vertrouwensdiensten, omdat het uitreiken van identificatiemiddelen een nationale aangelegenheid is. Daarom wordt in het voorstel enkel ingegaan op de grensoverschrijdende aspecten van elektronische identificatie.

De voorgestelde verordening creëert gelijke concurrentievoorwaarden voor bedrijven die vertrouwensdiensten aanbieden en die door de bestaande verschillende in de nationale wetgeving vaak met rechtsonzekerheid en extra lasten worden geconfronteerd. De rechtszekerheid wordt met name verhoogd door de duidelijke verplichtingen voor de lidstaten tot wederzijdse aanvaarding van gekwalificeerde vertrouwensdiensten, die voor bedrijven een extra stimulans vormen om zich op de buitenlandse markt te begeven. Een onderneming zal bijvoorbeeld via elektronische weg aan een door een overheid in een andere lidstaat uitgeschreven openbare aanbesteding kunnen deelnemen zonder dat haar elektronische handtekening wordt geblokkeerd door specifieke nationale eisen en interoperabiliteitsproblemen. Voorts zal een bedrijf een contract met een in een andere lidstaat gevestigde tegenpartij elektronisch kunnen ondertekenen zonder zich zorgen te maken over verschillende juridische vereisten op het gebied van vertrouwensdiensten zoals elektronische zegels, elektronische documenten of tijdsstempels. Bij de verzending van een

⁹ Mededeling van de Commissie: *Europa 2020. Een strategie voor slimme, duurzame en inclusieve groei*, COM(2010) 2020 van 3.3.2010.

ingebrekestelling van de ene lidstaat naar een andere wordt de rechtsgeldigheid in beide lidstaten gewaarborgd. Ten slotte wordt de handel via het internet betrouwbaarder wanneer kopers over de middelen beschikken om na te gaan dat of zij daadwerkelijk toegang hebben tot de website van de verkoper bevinden en niet tot een namaaksite.

Instrumenten voor wederzijdse erkende elektronische identificatie en algemeen aanvaarde elektronische handtekeningen zullen de grensoverschrijdende levering van talrijke diensten op de interne markt faciliteren en bedrijven in staat stellen zich zonder belemmeringen in hun contacten met overheden op de buitenlandse markt te begeven. In de praktijk leidt dit voor zowel ondernemingen als burgers tot aanzienlijke efficiëntiewinsten bij de afhandeling van administratieve formaliteiten: studenten zullen zich bijvoorbeeld elektronisch aan een buitenlandse universiteit kunnen inschrijven, burgers kunnen hun belastingaangifte online in een andere lidstaat indienen of een patiënt kan zijn medisch dossier online raadplegen. Zonder wederzijds erkende elektronische identificatie kan een dokter de medische gegevens die hij nodig heeft om een patiënt te behandelen niet raadplegen en moeten de medische en laboratoriumonderzoeken die de patiënt reeds heeft doorlopen opnieuw worden uitgevoerd.

b) Toegevoegde waarde (doelmatigheidstest)

De doelstellingen die hierboven worden geschetst, worden op basis van vrijwillige coördinatie tussen de lidstaten momenteel niet gehaald. Het is onwaarschijnlijk dat dit in de toekomst wel zal gebeuren. Dit leidt tot dubbele inspanningen, het opstellen van verschillende normen, de grensoverschrijdende aard van door ICT gegenereerde overloopeffecten en de administratieve complexiteit die een dergelijke coördinatie door middel van bilaterale of multilaterale overeenkomsten met zich meebrengt.

De aanpak van problemen zoals (a) een gebrek aan rechtszekerheid als gevolg van heterogene nationale bepalingen die hun oorsprong vinden in verschillende interpretaties van de richtlijn inzake elektronische handtekeningen en (b) een gebrek aan interoperabiliteit van de systemen voor elektronische handtekening op nationaal niveau als gevolg van een niet-uniforme toepassing van technische standaarden, vergt bovendien coördinatie tussen EU-lidstaten die van dien aard is dat deze op doeltreffender wijze op EU-niveau plaatsvindt.

3.3 Nadere uitleg van het voorstel

3.3.1 HOOFDSTUK I – ALGEMENE BEPALINGEN

In artikel 1 wordt het onderwerp van de verordening bepaald.

In artikel 2 wordt de materiële werkingssfeer van de verordening bepaald.

Artikel 3 bevat definities van de begrippen die in de verordening worden gebruikt. Hoewel sommige definities volledig zijn overgenomen uit Richtlijn 1999/93/EG, zijn andere verduidelijkt, aangevuld met extra elementen of geheel nieuw.

In artikel 4 worden de beginselen van de interne markt met betrekking tot de territoriale toepassing van de verordening bepaald. Er wordt uitdrukkelijk melding gemaakt van een verbod op belemmering van het vrije verkeer van goederen en diensten.

3.3.2 HOOFDSTUK II – ELEKTRONISCHE IDENTIFICATIE

In artikel 5 wordt bepaald dat de wederzijdse erkenning en aanvaarding van elektronische identificatiemiddelen onder een regeling vallen die bij de Commissie aangemeld wordt op basis van de voorwaarden die in de verordening worden vastgesteld. De meeste EU-lidstaten hebben een vorm van elektronische identificatiesystemen ingevoerd. Deze zijn echter in vele opzichten verschillend. Het gebrek aan een gemeenschappelijke rechtsgrondslag die elke lidstaat ertoe verplicht om elektronische identificatiemiddelen uit andere lidstaten te erkennen en als toegangsmiddel voor onlinediensten te aanvaarden en de ontoereikende grensoverschrijdende interoperabiliteit van nationale elektronische identificatie zijn hinderpalen die burgers en bedrijven ervan weerhouden ten volle gebruik te maken van de digitale eengemaakte markt. De wederzijdse erkenning en aanvaarding van alle elektronische identificatiemiddelen die onder een volgens deze verordening aangemelde regeling vallen, neemt deze wettelijke hinderpalen weg.

De verordening verplicht lidstaten niet om elektronische identificatieregelingen in te voeren of aan te melden, maar wel om de aangemelde elektronische identificatie te erkennen en te aanvaarden voor de onlinediensten waarbij elektronische identificatie vereist is om toegang te krijgen op nationaal niveau. De potentiële toename van de schaalvoordelen die dankzij het grensoverschrijdend gebruik van aangemelde elektronische identificatiemiddelen en authenticatiesystemen ontstaan, kunnen lidstaten ertoe aansporen hun elektronische identificatieregelingen aan te melden. In artikel 6 worden de vijf voorwaarden voor de aanmelding van elektronische identificatieregelingen bepaald:

Lidstaten kunnen de elektronische identificatieregelingen aanmelden die zij onder hun jurisdictie aanvaarden waarbij elektronische identificatie voor publieke diensten vereist is. Een verdere vereiste is dat het respectieve elektronische identificatiemiddel uitgereikt moet worden door, in naam van of ten minste onder de verantwoordelijkheid van de lidstaat die een regeling aanmeldt.

De lidstaten moeten een ondubbelzinnig verband kunnen waarborgen tussen de elektronische identificatiegegevens en de betrokken persoon. Deze verplichting betekent niet dat een persoon geen verschillende elektronische identificatiemiddelen kan hebben, maar ze moeten alle naar dezelfde persoon verwijzen.

De betrouwbaarheid van elektronische identificatie is afhankelijk van de beschikbaarheid van authenticatiemiddelen (d.w.z. de mogelijkheid om de geldigheid van de elektronische identificatiegegevens te controleren). De aanmeldende lidstaten zijn op grond van de verordening verplicht om kosteloos online-authenticatie te verstrekken aan betrokken partijen. Die mogelijkheid tot authenticatie moet ononderbroken beschikbaar zijn. Er kunnen geen specifieke technische vereisten zoals hardware of software opgelegd worden aan de partijen die afhankelijk zijn van een dergelijke authenticatie. Deze bepaling is niet van toepassing op vereisten voor de gebruikers (houders) van de elektronische identificatiemiddelen die om technische redenen noodzakelijk zijn voor het gebruik ervan, zoals kaartlezers.

De lidstaten moeten de aansprakelijkheid aanvaarden voor de ondubbelzinnigheid van het verband (d.w.z. dat de identificatiegegevens van een persoon niet verwijzen naar een andere persoon) en de mogelijkheid van authenticatie (d.w.z. de mogelijkheid om de geldigheid van elektronische identificatiegegevens te controleren). De aansprakelijkheid van de lidstaten geldt niet voor andere aspecten van het identificatieproces of voor andere transacties waarvoor identificatie vereist is.

Artikel 7 bevat regels voor het aanmelden van elektronische identificatieregelingen bij de Commissie.

Artikel 8 heeft tot doel de technische interoperabiliteit van de aangemelde identificatieregelingen te waarborgen door middel van coördinatie, met inbegrip van gedelegeerde handelingen.

3.3.3 *HOOFDSTUK III – VERTROUWENSDIENSTEN*

3.3.3.1 Afdeling 1 – Algemene bepalingen

Artikel 9 voorziet in de beginselen voor aansprakelijkheid van zowel niet-gekwaliceerde als gekwalificeerde verleners van vertrouwensdiensten. Het bouwt voort op artikel 6 van Richtlijn 1999/93/EG en breidt het recht op compensatie uit tot schade veroorzaakt door een nalatige verlener van vertrouwensdiensten die de goede praktijken voor veiligheid niet heeft nageleefd, met als gevolg een inbreuk op de veiligheid die een aanzienlijk effect op de dienst heeft.

In artikel 10 wordt het mechanisme beschreven voor de erkenning en aanvaarding van gekwalificeerde vertrouwensdiensten die worden verleend door een in een derde land gevestigde aanbieder. Het bouwt voort op artikel 7 van Richtlijn 1999/93/EG maar alleen de enige praktisch haalbare optie, namelijk het toestaan van een dergelijke erkenning volgens een internationale overeenkomst tussen de Europese Unie en derde landen of internationale organisaties, wordt gehandhaafd.

Artikel 11 voorziet in de beginselen inzake gegevensbescherming en -minimalisering. Het bouwt voort op artikel 8 van Richtlijn 1999/93/EG.

Artikel 12 maakt vertrouwensdiensten toegankelijk voor mensen met een handicap.

3.3.3.2 Afdeling 2 – Toezicht

Artikel 13 verplicht de lidstaten om toezichtsorganen op te richten, op basis van artikel 3, lid 3, van Richtlijn 1999/93/EG, en zorgt voor verduidelijking en uitbreiding van hun bevoegdheid met betrekking tot zowel niet-gekwaliceerde als gekwalificeerde verleners van vertrouwensdiensten.

Artikel 14 voorziet in een expliciet mechanisme voor wederzijdse ondersteuning tussen toezichtsorganen in lidstaten om het grensoverschrijdende toezicht op verleners van vertrouwensdiensten te vergemakkelijken. Het artikel bevat regels voor gezamenlijke operaties en biedt toezichthoudende overheden het recht om aan dergelijke operaties deel te nemen.

Artikel 15 voorziet in een verplichting voor zowel gekwalificeerde als niet-gekwaliceerde verleners van vertrouwensdiensten om passende technische en organisatorische maatregelen in te stellen voor de beveiliging van hun activiteiten. Bovendien moeten de bevoegde toezichtsorganen en andere relevante autoriteiten op de hoogte gebracht worden van inbreuken op de veiligheid. Indien nodig brengen zij op hun beurt de toezichtsorganen in andere lidstaten op de hoogte en informeren zij de burgers, rechtstreeks of via de betrokken verlener van vertrouwensdiensten.

Artikel 16 voorziet in de voorwaarden voor het toezicht op gekwalificeerde verleners van vertrouwensdiensten en de gekwalificeerde vertrouwensdiensten die zij verstrekken. Gekwalificeerde verleners van vertrouwensdiensten zijn op grond van het artikel verplicht tot een jaarlijkse audit door een erkend onafhankelijk orgaan, om aan het toezichtsorgaan te kunnen bevestigen dat zij voldoen aan de in de verordening vastgelegde verplichtingen. Bovendien geeft artikel 16, lid 2, het toezichtsorgaan het recht om ter plaatse op elk moment audits van de gekwalificeerde verleners van vertrouwensdiensten uit te voeren. Het toezichtsorgaan is ook bevoegd om aan gekwalificeerde verleners van vertrouwensdiensten die blijkens een veiligheidsaudit een verplichting niet naleven, bindende instructies op te leggen om de tekortkoming op evenredige wijze recht te zetten.

Artikel 17 betreft de activiteit van het toezichtsorgaan wanneer een verlener van vertrouwensdiensten voornemens is een gekwalificeerde vertrouwensdienst te starten.

Artikel 18 voorziet in de opstelling van vertrouwenslijsten¹⁰ die informatie bevatten over de gekwalificeerde dienstverleners van vertrouwensdiensten die aan toezicht onderhevig zijn en over de gekwalificeerde diensten die zij bieden. Deze informatie moet volgens een gemeenschappelijk model openbaar worden gemaakt om het automatisch gebruik ervan te vereenvoudigen en te waarborgen dat er voldoende bijzonderheden worden opgenomen.

Artikel 19 voorziet in de vereisten waaraan gekwalificeerde verleners van vertrouwensdiensten moeten voldoen om als dusdanig erkend te worden. Het artikel is gebaseerd op bijlage II bij Richtlijn 1999/93/EG.

3.3.3.3 Afdeling 3 – Elektronische handtekening

Artikel 20 omvat de regelgeving in verband met de rechtsgevolgen van elektronische handtekeningen van natuurlijke personen. Het is een verduidelijking en uitbreiding van artikel 5 van Richtlijn 1999/93/EG, die voorziet in een expliciete verplichting om aan gekwalificeerde elektronische handtekeningen dezelfde rechtsgevolgen te verbinden als aan handgeschreven handtekeningen. Bovendien moeten de lidstaten de grensoverschrijdende aanvaarding van gekwalificeerde elektronische handtekeningen waarborgen in verband met de levering van publieke diensten en mogen zij geen bijkomende vereisten invoeren die belemmering van het gebruik van dergelijke handtekeningen in de hand werken.

Artikel 21 bevat de vereisten voor gekwalificeerde certificaten voor handtekeningen. Het bevat een verduidelijking van bijlage I bij Richtlijn 1999/93/EG en voorziet in de intrekking van bepalingen die in de praktijk niet werkten (bijvoorbeeld grenzen met betrekking tot de waarde van transacties).

Artikel 22 bevat de eisen voor gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen. Het bevat een verduidelijking van de eisen voor veilige middelen voor het aanmaken van handtekeningen zoals bepaald in artikel 3, lid 5, van Richtlijn 1999/93/EG, die volgens deze verordening beschouwd moeten worden als gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen. In het artikel wordt ook duidelijk gemaakt dat onder een middel voor het aanmaken van handtekeningen veel meer kan worden verstaan dan slechts een middel dat gegevens voor het aanmaken van

¹⁰

De vertrouwenslijst zoals vastgesteld bij Beschikking 2009/767/EG van de Commissie, als gewijzigd bij Besluit 2010/425/EU van de Commissie, zal de basis vormen van een nieuw Besluit van de Commissie inzake lijsten betreffende vertrouwenslijsten krachtens deze verordening.

handtekeningen bevat. De Commissie kan ook een lijst maken van referentienummers voor normen inzake veiligheidseisen voor middelen.

Artikel 23 bouwt voort op artikel 3, lid 4, van Richtlijn 1999/93/EG en bevat een omschrijving van het concept certificatie van gekwalificeerde middelen voor elektronische handtekeningen bedoeld om vast te stellen of deze in overeenstemming zijn met de veiligheidseisen van bijlage II. Alle lidstaten moeten bevestigen dat deze middelen in overeenstemming zijn met de eisen wanneer een certificatieprocedure geleid wordt door een door een lidstaat aangewezen certificatieorgaan. De Commissie publiceert een positieve lijst van dergelijke gecertificeerde middelen op grond van artikel 24. De Commissie kan ook een lijst vaststellen met referentienummers van normen voor de veiligheidsbeoordeling van producten op het gebied van informatietechnologie zoals genoemd in artikel 23, lid 1.

Artikel 24 betreft de publicatie van een door de Commissie opgestelde lijst van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen na kennisgeving van conformiteit door de lidstaten.

Artikel 25 bouwt voort op aanbevelingen van bijlage IV bij Richtlijn 1999/93/EG om bindende eisen vast te leggen voor het valideren van gekwalificeerde elektronische handtekeningen om de rechtszekerheid van een dergelijke validering te verhogen.

Artikel 26 voorziet in de voorwaarden voor gekwalificeerde validatiediensten.

Artikel 27 bevat de voorwaarde voor de duurzame bewaring van gekwalificeerde elektronische handtekeningen. Dit is mogelijk door het gebruik van procedures en technologieën die de betrouwbaarheid van de validatiegegevens van gekwalificeerde elektronische handtekeningen verlengen tot na de technologische houdbaarheid ervan, wanneer cybercriminelen eenvoudig vervalsing zouden kunnen plegen.

3.3.3.4 Afdeling 4 – Elektronische zegels

Artikel 28 betreft de rechtsgevolgen van elektronische zegels voor rechtspersonen. Er kan een specifiek gewettigd vermoeden worden toegekend aan een gekwalificeerd elektronisch zegel als waarborg van de oorsprong en de echtheid van de elektronische documenten waarop het betrekking heeft.

Artikel 29 bevat de eisen voor gekwalificeerde certificaten voor elektronische zegels.

Artikel 30 bevat de eisen voor de certificatie en publicatie van de lijst van de gekwalificeerde middelen voor het aanmaken van elektronische zegels.

Artikel 31 bevat de voorwaarde voor validatie en bewaring van gekwalificeerde elektronische zegels.

3.3.3.5 Afdeling 5 – Elektronische tijdstempel

Artikel 32 betreft de rechtsgevolgen van elektronische tijdstempels. Er kan een specifiek gewettigd vermoeden aan gekwalificeerde elektronische tijdstempels worden toegekend met betrekking tot de zekerheid van het tijdstip.

Artikel 33 bevat de eisen voor gekwalificeerde elektronische tijdstempels.

3.3.3.6 Afdeling 6 – Elektronische documenten

Artikel 34 betreft de rechtsgevolgen en de voorwaarden voor aanvaarding van elektronische documenten. Er is sprake van een specifiek gewettigd vermoeden van authenticiteit en echtheid ingeval een elektronisch document is ondertekend met een gekwalificeerde elektronische handtekening of een gekwalificeerd elektronisch zegel draagt. Met betrekking tot de aanvaarding van elektronische documenten geldt dat, wanneer een origineel document of een gecertificeerd afschrift vereist is voor het verlenen van een publieke dienst, zonder bijkomende eisen in andere lidstaten in ieder geval elektronische documenten zullen worden aanvaard wanneer deze zijn afgegeven door de personen die bevoegd zijn om de desbetreffende documenten af te geven en wanneer zij in overeenstemming met de nationale wetgeving van de lidstaat van herkomst beschouwd worden als originelen of gecertificeerde kopieën.

3.3.3.7 Afdeling 7 – Elektronische bezorgingsdiensten

Artikel 35 betreft de rechtsgevolgen van gegevens die door middel van een elektronische bezorgingsdienst verstuurd of ontvangen worden. Een specifiek gewettigd vermoeden over de echtheid van de gegevens die verstuurd of ontvangen worden en de juistheid van het tijdstip waarop de gegevens verstuurd of ontvangen worden is gewaarborgd voor gekwalificeerde elektronische bezorgingsdiensten. De wederzijdse erkenning van gekwalificeerde elektronische bezorgingsdiensten op EU-niveau is ook gewaarborgd.

Artikel 36 bevat de eisen voor gekwalificeerde elektronische bezorgingsdiensten.

3.3.3.8 Afdeling 8 – Authenticatie van websites

Deze afdeling heeft als doel de authenticiteit van websites en de eigenaars ervan te waarborgen.

Artikel 37 voorziet in de eisen voor gekwalificeerde certificaten voor authenticatie van websites die gebruikt kunnen worden als waarborg voor de authenticiteit van een website. Een gekwalificeerd certificaat voor authenticatie van websites biedt een minimale reeks betrouwbare gegevens over de website en de juridische status van de eigenaar.

3.3.4 HOOFDSTUK IV – GEDELEGEERDE HANDELINGEN

Artikel 38 bevat de standaardbepalingen voor het uitoefenen van de delegaties overeenkomstig artikel 290 VWEU (gedelegeerde handelingen). Hierdoor is de wetgever in staat de bevoegdheid om niet-wetgevingshandelingen van algemene strekking vast te stellen ter aanvulling of wijziging van bepaalde niet-essentiële onderdelen van een wetgevingshandeling te delegeren aan de Commissie.

3.3.5 HOOFDSTUK V – UITVOERINGSHANDELINGEN

Artikel 39 bevat de bepaling over de comitéprocedure die nodig is om de bevoegdheid voor tenuitvoerlegging bij de Commissie te leggen wanneer overeenkomstig artikel 291 VWEU uniforme voorwaarden voor het uitvoeren van wettelijk bindende handelingen van de Unie nodig zijn. De onderzoeksprocedure is van toepassing.

3.3.6 HOOFDSTUK VI – SLOTBEPALINGEN

Artikel 40 verplicht de Commissie om de verordening te beoordelen en verslag uit te brengen over haar bevindingen.

Artikel 41 voorziet in intrekking van Richtlijn 1999/93/EG en zorgt voor de vlotte overgang van de bestaande infrastructuur voor elektronische handtekeningen naar de nieuwe vereisten van de verordening.

Artikel 42 voorziet in de datum voor de inwerkingtreding van de verordening.

4. GEVOLGEN VOOR DE BEGROTING

De specifieke gevolgen van het voorstel voor de begroting hebben betrekking op de taken die aan de Europese Commissie zijn toegekend, zoals gespecificeerd in het financieel memorandum bij dit voorstel.

Het voorstel heeft geen gevolgen voor de beleidsuitgaven.

Het financieel memorandum bij dit voorstel voor een verordening behandelt de budgettaire gevolgen van de verordening zelf.

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt

(Voor de EER relevante tekst)

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 Comité¹¹,

Na raadpleging van de Europese Toezichthouder voor gegevensbescherming¹²,

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

- (1) Het opbouwen van vertrouwen in een online-omgeving is essentieel voor economische ontwikkeling. Een gebrek aan vertrouwen leidt ertoe dat consumenten, bedrijven en overheidsdiensten aarzelen om transacties elektronisch uit te voeren en van nieuwe diensten gebruik te maken.
- (2) Deze verordening heeft als doel het vertrouwen in elektronische transacties in de interne markt te vergroten door veilige en ongehinderde elektronische interactie mogelijk te maken tussen bedrijven, burgers en publieke overheidsdiensten, en bijgevolg ook de doeltreffendheid van publieke en particuliere onlinediensten, e-business en elektronische handel in de Unie te verhogen.
- (3) Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen¹³, had hoofdzakelijk betrekking op elektronische handtekeningen zonder een algemeen grens- en sectoroverschrijdend kader te bieden voor veilige, betrouwbare en gebruiksvriendelijke elektronische transacties. Deze verordening voorziet in een versterking en uitbreiding van het *acquis* van de richtlijn.

¹¹ PB C [...] van [...], blz. [...].

¹² PB C [...] van [...], blz. [...].

¹³ PB L 13 van 19.1.2000, blz. 12.

- (4) In de Digitale Agenda voor Europa van de Commissie¹⁴ 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 van 2010 benadrukt de Commissie verder de noodzaak van het oplossen van de belangrijkste problemen die de Europese burger verhinderen ten volle gebruik te maken van de voordelen van een digitale eengemaakte markt en grensoverschrijdende digitale diensten¹⁵.
- (5) De Europese Raad nodigde de Commissie uit om tegen 2015 een digitale eengemaakte markt te creëren¹⁶ om snel vooruitgang te boeken op belangrijke onderdelen van de digitale economie en om een volledig geïntegreerde digitale eengemaakte markt te bevorderen¹⁷ door het grensoverschrijdend gebruik van onlinediensten te vergemakkelijken, met bijzondere aandacht voor de vereenvoudiging van veilige elektronische identificatie en authenticatie.
- (6) De Raad nodigde de Commissie uit om bij te dragen aan de digitale eengemaakte markt door toereikende voorwaarden te creëren voor de wederzijdse erkenning van grensoverschrijdende essentiële elementen, zoals elektronische identificatie, elektronische documenten, elektronische handtekeningen en elektronische leveringsdiensten, en voor interoperabele e-overheidsdiensten in de Unie¹⁸.
- (7) Het Europees Parlement onderstreept het belang 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 verzoekt de Commissie 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 verhogen¹⁹.
- (8) Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt²⁰ verzoekt de lidstaten om één-loketten op te zetten 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. Voor veel onlinediensten die via één-loketten toegankelijk zijn, zijn elektronische identificatie, authenticatie en handtekeningen vereist.
- (9) In de meeste gevallen kunnen dienstverleners uit andere lidstaten hun elektronische identificatie niet gebruiken om toegang te krijgen tot deze diensten, omdat de nationale elektronische identificatieregelingen uit hun land niet erkend en aanvaard worden in andere lidstaten. Deze elektronische drempel verhindert dat dienstverleners ten volle gebruik kunnen maken van de interne markt. Wederzijds erkende en aanvaarde elektronische identificatiemiddelen zullen de grensoverschrijdende

¹⁴ COM(2010) 245 definitief/2.

¹⁵ Verslag over het burgerschap van de EU 2010: Het wegnemen van de belemmeringen voor de rechten van EU-burgers, COM(2010) 603 definitief, punt 2.2.2, blz. 13.

¹⁶ 4.2.2011: EUCO 2/1/11.

¹⁷ 23.10.2011: EUCO 52/1/11.

¹⁸ Conclusies van de Raad over het Europese actieplan inzake e-overheid 2011-2015, 3093^{ste} bijeenkomst van de Raad Vervoer, Telecommunicatie en Energie, Brussel, 27 mei 2011.

¹⁹ Resolutie van het Europees Parlement van 21 september 2010 over de voltooiing van de interne markt voor e-handel, P7_TA(2010)0320, en Resolutie van het Europees Parlement van 15 juni 2010 over internetgovernance: de volgende stappen, P7_TA(2010)0208.

²⁰ PB L 376 van 27.12.2006, blz. 36.

verstrekking van talrijke diensten op de interne markt faciliteren en bedrijven in staat stellen zich op de buitenlandse markt te begeven zonder daarbij veel belemmeringen te ondervinden in hun contacten met de overheid.

- (10) 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 gezondheidszorg²¹ voorziet in de vorming van een netwerk van nationale overheden die verantwoordelijk zijn voor e-gezondheidsdiensten. Om de veiligheid en de voorzetting van grensoverschrijdende gezondheidszorg te waarborgen, is het netwerk genoodzaakt om richtsnoeren op te stellen voor de grensoverschrijdende toegang tot elektronische gezondheidsgegevens en -diensten, ook door het ondersteunen van *"gemeenschappelijke identificatie- en authenticatiemaatregelen die erop gericht zijn de overdraagbaarheid van gegevens bij grensoverschrijdende gezondheidszorg te bevorderen"*. De wederzijdse erkenning en aanvaarding van elektronische identificatie en authenticatie is essentieel om de Europese burger een grensoverschrijdende gezondheidszorg te bieden. Wanneer mensen voor een behandeling naar het buitenland reizen, moeten hun medische gegevens in het land van behandeling raadpleegbaar zijn. Dit vergt een stabiel, veilig en betrouwbaar kader voor elektronisch identificatie.
- (11) Een van de doelstellingen van deze verordening is het afschaffen van bestaande hinderpalen voor het grensoverschrijdende gebruik van elektronische identificatiemiddelen die in de lidstaten worden gebruikt om in ieder geval toegang te hebben tot publieke diensten. Deze verordening heeft niet tot doel om beheersystemen voor elektronische identiteit en verwante infrastructuren in de lidstaten te beïnvloeden. Het doel van deze verordening is veilige elektronische identificatie en authenticatie voor de toegang tot grensoverschrijdende onlinediensten van de lidstaten te waarborgen.
- (12) Het staat de lidstaten vrij om middelen voor elektronische identificatie of toegang tot onlinediensten te gebruiken of in te voeren. De lidstaten blijven ook bevoegd om te beslissen of de particuliere sector betrokken wordt bij het leveren van deze middelen. Zij zijn niet verplicht om hun elektronische identificatieregelingen aan te melden. De keuze om alle, sommige of geen elektronische identificatieregelingen die onder de regeling vallen en die op nationaal niveau worden gebruikt om in ieder geval toegang te krijgen tot publieke onlinediensten of specifieke diensten, aan te melden blijft bij de lidstaten.
- (13) In de verordening worden bepaalde voorwaarden opgenomen aan de hand waarvan moet worden bepaald welke elektronische identificatiemiddelen aanvaard worden en hoe de regelingen worden aangemeld. Deze helpen de lidstaten om het noodzakelijke vertrouwen in elkaars elektronische identificatieregelingen op te bouwen en om elektronische identificatiemiddelen die onder hun aangemelde regelingen vallen, wederzijds te erkennen en aanvaarden. Het beginsel van wederzijdse erkenning en aanvaarding is van toepassing als de aanmeldende lidstaat voldoet aan de voorwaarden voor aanmelding en de aanmelding verschenen is in het Publicatieblad van de Europese Unie. De toegang tot deze onlinediensten en de definitieve bezorging ervan bij de aanvrager moeten echter nauw in verband staan met het recht om zulke diensten

²¹

PB L 88 van 4.4.2011, blz. 45.

te ontvangen onder de voorwaarden die worden gesteld op grond van nationale wetgeving.

- (14) De lidstaten zijn bevoegd om te beslissen of de particuliere sector betrokken wordt bij het afgeven van elektronische identificatiemiddelen en of de particuliere sector in staat gesteld moet worden elektronische identificatiemiddelen te gebruiken op grond van een aangemelde regeling voor de identificatie voor onlinediensten of elektronische transacties. De mogelijkheid om zulke elektronische identificatiemiddelen te gebruiken stelt de particuliere sector in staat om 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 grensoverschrijdende elektronische identificatiemiddelen door de particuliere sector te vergemakkelijken, moet de mogelijkheid tot authenticatie die de lidstaten bieden, beschikbaar zijn voor daarvan afhankelijke partijen zonder onderscheid te maken tussen de publieke en de particuliere sector.
- (15) Het grensoverschrijdende gebruik van elektronische identificatiemiddelen onder een aangemelde regeling maakt het noodzakelijk dat lidstaten samenwerken om technische interoperabiliteit te verzekeren. Hierdoor worden specifieke nationale technische regels uitgesloten, waardoor niet-nationale partijen bijvoorbeeld specifieke hardware of software zouden moeten kopen om de aangemelde elektronische identificatie te verifiëren en valideren. Anderzijds is het onvermijdelijk dat aan de gebruikers technische eisen worden gesteld die voortkomen uit de inherente specificaties van het gebruikte hulpmiddel (bijvoorbeeld smartcards).
- (16) De samenwerking tussen lidstaten moet ten dienste staan van de technische interoperabiliteit van de aangemelde elektronische identificatieregelingen 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, bevordert een dergelijke samenwerking.
- (17) Deze verordening dient ook te voorzien in een algemeen wetgevingskader voor het gebruik van elektronische vertrouwensdiensten. Het schept echter geen algemene verplichting om ze te gebruiken. De verordening mag met name niet voorzien in de verlening van diensten die berusten op vrijwillige privaatrechtelijke overeenkomsten. Ook mag ze geen betrekking hebben op aspecten die verband houden met de totstandkoming of geldigheid van contracten of andere wettelijke verbintenissen waarvoor het nationale recht of het Gemeenschapsrecht vormvereisten voorschrijven.
- (18) Teneinde bij te dragen tot het algemene grensoverschrijdende gebruik van elektronische vertrouwensdiensten, moet het mogelijk zijn deze in alle lidstaten in gerechtelijke procedures als bewijsmiddel te gebruiken.
- (19) Het staat de lidstaten vrij om naast de vertrouwensdiensten die deel uitmaken van de gesloten lijst waarin deze verordening voorziet, andere vormen van vertrouwensdiensten te definiëren als het doel een nationale erkenning als gekwalificeerde vertrouwensdienst is.

- (20) Vanwege van het hoge tempo van de technologische veranderingen dient deze verordening de mogelijkheid tot innovatie te bieden.
- (21) De verordening is technologieneutraal. De rechtsgevolgen waarin de verordening voorziet, moeten bereikt kunnen worden door willekeurige technologische middelen, op voorwaarde dat voldaan is aan de eisen van deze verordening.
- (22) Om het vertrouwen van de mensen in de interne markt te bevorderen en het gebruik van vertrouwensdiensten en producten te stimuleren, worden de begrippen gekwalificeerde vertrouwensdiensten en gekwalificeerde verlener van vertrouwensdiensten gehanteerd om eisen en verplichtingen aan te duiden die ertoe dienen de beveiliging van gebruikte of geleverde gekwalificeerde vertrouwensdiensten en producten op hoog niveau te waarborgen.
- (23) In overeenstemming met de verplichtingen van het Verdrag van de Verenigde Naties inzake de rechten van personen met een handicap dat in de EU in werking is getreden, 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 dezelfde basis als andere consumenten te gebruiken.
- (24) Een verlener van vertrouwensdiensten is verantwoordelijk voor de verwerking van persoonsgegevens en moet voldoen aan de verplichtingen waarin 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 gegevens²². In het bijzonder moet het verzamelen van gegevens zo beperkt mogelijk blijven, rekening houdend met het doel van de verstrekte dienst.
- (25) Toezichtsorganen moeten samenwerken en informatie uitwisselen met overheidsdiensten voor gegevensbescherming om te waarborgen dat de dienstverleners de wetgeving voor gegevensbescherming op de juiste wijze toepassen. De uitwisseling van informatie moet in het bijzonder veiligheidsproblemen en inbreuken op persoonsgegevens bestrijken.
- (26) Het is een taak van de verlener van vertrouwensdiensten om goede praktijken voor veiligheid 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.
- (27) De bepalingen inzake het gebruik van pseudoniemen in certificaten beletten de lidstaten niet op grond van de communautaire of de nationale wetgeving de identificatie van personen te eisen.
- (28) Alle lidstaten moeten zich houden aan gemeenschappelijke essentiële toezichtsvereisten om een vergelijkbaar niveau van veiligheid van gekwalificeerde vertrouwensdiensten te verzekeren. Om de consistente toepassing van deze vereisten in de gehele EU te vergemakkelijken, moeten de lidstaten vergelijkbare procedures invoeren en informatie over hun toezichtsactiviteiten en de beste praktijken in het veld uitwisselen.

²²

PB L 281 van 23.11.1995, blz. 31.

- (29) Het is van essentieel belang dat inbreuken op de veiligheid en beoordelingen van de veiligheidsrisico's worden gemeld zodat in het geval van een dergelijke inbreuk of verlies van integriteit de juiste informatie aan de betrokken partijen kan worden verstrekt.
- (30) Om de Commissie en de lidstaten in staat te stellen de doeltreffendheid van het in deze verordening voorziene meldingsmechanisme voor inbreuken te beoordelen, worden de toezichtsorganen verzocht beknopte informatie te verstrekken aan de Commissie en het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA).
- (31) Om de Commissie en de lidstaten in staat te stellen het effect van deze verordening te beoordelen, worden de toezichtsorganen verzocht statistieken over het gebruik van gekwalificeerde vertrouwensdiensten te verstrekken.
- (32) Om de Commissie en de lidstaten in staat te stellen de doeltreffendheid van het versterkte toezichtsmechanisme waarin deze verordening voorziet, te beoordelen, worden de toezichtsorganen verzocht verslag uit te brengen over hun activiteiten. Dit is bevorderlijk voor de uitwisseling van goede praktijken tussen toezichtsorganen en biedt de garantie dat de essentiële eisen voor toezicht in de lidstaten op consistente en efficiënte wijze worden uitgevoerd.
- (33) Om de duurzaamheid van gekwalificeerde vertrouwensdiensten te waarborgen en het vertrouwen van de gebruikers in de continuïteit van gekwalificeerde vertrouwensdiensten te stimuleren, moeten de toezichtsorganen ervoor zorgen dat de gegevens van gekwalificeerde verleners van vertrouwensdiensten gedurende een passende periode bewaard worden en toegankelijk blijven, ook nadat een gekwalificeerde verlener van vertrouwensdiensten zijn werkzaamheden heeft beëindigd.
- (34) 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 onderhevig is, of wanneer de computers van een verlener zich bevinden op het grondgebied van een andere lidstaat dan waar hij gevestigd is, moet een systeem voor wederzijdse hulp tussen de toezichtsorganen in de lidstaten worden opgezet.
- (35) Verleners van vertrouwensdiensten zijn verantwoordelijk voor de naleving van de voorschriften die in deze verordening worden vastgesteld voor de verlening van vertrouwensdiensten, met name voor gekwalificeerde vertrouwensdiensten. Toezichtsorganen zijn verantwoordelijk voor het toezicht op de manier waarop de verleners van vertrouwensdiensten deze voorschriften naleven.
- (36) Om een doeltreffende initiatie mogelijk te maken, die dient te leiden tot de opname van gekwalificeerde verleners van vertrouwensdiensten en de gekwalificeerde vertrouwensdiensten die zij verlenen in vertrouwenslijsten, moeten voorbereidende uitwisselingen tussen kandidaat-gekwilificeerde verleners van vertrouwensdiensten en het bevoegde toezichtsorgaan worden aangemoedigd met het oog op de vergemakkelijking van het zorgvuldige onderzoek dat uitmondt in de verlening van gekwalificeerde vertrouwensdiensten.
- (37) Vertrouwenslijsten zijn essentiële elementen om vertrouwen op te bouwen bij de marktdeelnemers, aangezien zij aangeven dat de dienstverlener op het ogenblik van

toezicht beschikt over een gekwalificeerde status; anderzijds vormen zij geen voorwaarde om de gekwalificeerde status te bereiken en gekwalificeerde vertrouwensdiensten te kunnen verlenen die het gevolg is van de naleving van de voorschriften van deze verordening.

- (38) Zodra een gekwalificeerde vertrouwensdienst is aangemeld, kan zij niet worden geweigerd voor het vervullen van een administratieve procedure of formaliteit door de betrokken openbare instantie, omdat zij niet is opgenomen in de door de lidstaten opgestelde vertrouwenslijsten. Een openbare instantie verwijst in dit verband naar een overheid of andere entiteit die e-overheidsdiensten verleent zoals onlinebelastingaangiften, het aanvragen van geboorteakten, de deelname aan procedures voor elektronische overheidsopdrachten enz.
- (39) Hoewel een hoog veiligheidsniveau 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 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 markt²³, elektronische handtekeningen met een lagere veiligheidsgarantie ook worden aanvaard.
- (40) Het moet voor de ondertekenaar mogelijk zijn om middelen voor het aanmaken van gekwalificeerde elektronische handtekeningen toe te vertrouwen aan een derde partij, op voorwaarde dat passende mechanismen en procedures worden ingevoerd om te waarborgen dat uitsluitend de ondertekenaar controle heeft over het gebruik van de aanmaakgegevens van zijn elektronische handtekening, en op voorwaarde dat door het gebruik van dit middel wordt voldaan aan de eisen voor gekwalificeerde handtekeningen.
- (41) Om rechtszekerheid wat betreft de geldigheid van de handtekening te waarborgen, is het van essentieel belang vast te leggen welke componenten van een gekwalificeerde elektronische handtekening moeten worden beoordeeld door de afhankelijke partij die de validering uitvoert. Bovendien moet het definiëren van de eisen aan gekwalificeerde verleners van vertrouwensdiensten die een gekwalificeerde valideringsdienst kunnen leveren aan afhankelijke partijen die niet bereid of in staat zijn om de validering van gekwalificeerde elektronische handtekeningen zelf uit te voeren, de particuliere of publieke sector stimuleren om in dergelijke diensten te investeren. Beide elementen moeten de validering van gekwalificeerde elektronische handtekeningen eenvoudig en gemakkelijk maken voor alle partijen op het niveau van de Unie.
- (42) Wanneer voor een transactie een gekwalificeerd elektronisch zegel van een rechtspersoon vereist is, moet een gekwalificeerde elektronische handtekening van de gemachtigde vertegenwoordiger van de rechtspersoon op gelijke voet aanvaard worden.
- (43) 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.

²³

PB L 274 van 20.10.2009, blz. 36.

- (44) Deze verordening is bedoeld om de bewaring van informatie op de lange termijn te waarborgen, dat wil zeggen de rechtsgeldigheid van elektronische handtekeningen en elektronische zegels gedurende lange perioden, waarbij gegarandeerd wordt dat zij gevalideerd kunnen worden ongeacht toekomstige technologische veranderingen.
- (45) Om het grensoverschrijdende gebruik van elektronische documenten te verhogen moet deze verordening de rechtsgevolgen vaststellen van elektronische documenten die beschouwd moeten worden als gelijkwaardig aan papieren documenten, afhankelijk van de risicobeoordeling en op voorwaarde dat de authenticiteit en integriteit van de documenten gewaarborgd zijn. Voor de verdere ontwikkeling van grensoverschrijdende elektronische transacties binnen de interne markt is het ook van belang dat originele elektronische documenten of gecertificeerde kopieën die worden afgegeven door terzake bevoegde organen in een lidstaat in overeenstemming met hun nationale wetgeving, ook als zodanig in andere lidstaten worden aanvaard. Deze verordening moet het recht van lidstaten om te bepalen wat een origineel of kopie inhoudt op nationaal niveau onverlet laten, maar waarborgt dat deze als zodanig ook grensoverschrijdend kunnen worden gebruikt.
- (46) Aangezien bevoegde autoriteiten in de lidstaten momenteel verschillende formaten voor geavanceerde elektronische handtekeningen gebruiken om hun documenten elektronisch te ondertekenen, moet worden gewaarborgd dat ten minste een aantal formaten voor geavanceerde elektronische handtekeningen technisch ondersteund kunnen worden door de lidstaten, wanneer zij elektronisch ondertekende documenten ontvangen. Op vergelijkbare wijze is het nodig om, wanneer bevoegde autoriteiten in de lidstaten gebruikmaken van geavanceerde elektronische zegels, te waarborgen dat zij ten minste een aantal formaten voor geavanceerde elektronische zegels ondersteunen.
- (47) Aanvullend op het controleren van de authenticiteit van het door de rechtspersoon afgegeven document, kunnen elektronische zegels worden gebruikt om de authenticiteit van ieder digitaal bedrijfsmiddel van de rechtspersoon, bijvoorbeeld softwarecode of servers, te controleren.
- (48) Door de controle op de authenticiteit van websites en de eigenaar ervan mogelijk te maken, wordt het moeilijker om websites te vervalsen en wordt fraude derhalve teruggedrongen.
- (49) Om bepaalde 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 van het Verdrag betreffende de werking van de Europese Unie aan de Commissie worden gedelegeerd ten aanzien van de interoperabiliteit van elektronische identificatie; eisen die aan verleners van vertrouwensdiensten worden gesteld met betrekking tot veiligheidsmaatregelen; erkende onafhankelijke organen die verantwoordelijk zijn voor het houden van audits van dienstverleners; vertrouwenslijsten; eisen met betrekking tot de veiligheidsniveaus van elektronische handtekeningen; eisen met betrekking tot de validering en bewaring van gekwalificeerde certificaten voor elektronische handtekeningen; de organen die verantwoordelijk zijn voor de certificering van middelen voor het aanmaken van gekwalificeerde elektronische handtekeningen; de eisen met betrekking tot de veiligheidsniveaus van elektronische zegels en met betrekking tot gekwalificeerde certificaten voor elektronische zegels; en de interoperabiliteit tussen

bezorgingsdiensten. Het is van bijzonder belang dat de Commissie tijdens de voorbereiding passend overleg pleegt, onder meer met deskundigen.

- (50) Bij het voorbereiden en opstellen van gedelegeerde handelingen dient de Commissie erop toe te zien dat de desbetreffende documenten gelijktijdig, tijdig en op passende wijze bij het Europees Parlement en de Raad worden ingediend.
- (51) Om uniforme voorwaarden te waarborgen voor de uitvoering van deze verordening, moeten uitvoeringsbevoegdheden worden verleend 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 eisen die zijn vastgesteld in deze verordening of gedefinieerd in gedelegeerde handelingen. Deze bevoegdheden moeten worden uitgeoefend overeenkomstig 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 controleren²⁴.
- (52) Omwille van de rechtszekerheid en duidelijkheid moet Richtlijn 1999/93/EG worden ingetrokken.
- (53) Om rechtszekerheid te waarborgen voor de marktdeelnemers die reeds van gekwalificeerde certificaten gebruikmaken in overeenstemming met Richtlijn 1999/93/EG, moet een voldoende ruime overgangsperiode worden vastgesteld. Ook moet de Commissie voorzien worden van de middelen die nodig zijn om de uitvoeringshandelingen en gedelegeerde handelingen voor die datum vast te stellen.
- (54) Aangezien de doelstellingen van deze verordening niet voldoende door de lidstaten kunnen worden verwezenlijkt en derhalve, 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 evenredigheidsbeginsel als bedoeld in genoemd artikel gaat deze verordening niet verder dan hetgeen noodzakelijk is om deze doelstellingen te bereiken, in het bijzonder wat betreft de rol van de Commissie als coördinator van nationale activiteiten,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp

1. Deze verordening stelt regels vast voor elektronische identificatie en elektronische vertrouwensdiensten voor elektronische transacties met het oog op het waarborgen van de goede werking van de interne markt.

²⁴

PB L 55 van 28.2.2011, blz. 13.

2. Deze verordening stelt de voorwaarden vast waaronder lidstaten elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen die vallen onder een aangemeld stelsel voor elektronische identificatie erkennen en aanvaarden.
3. Deze verordening stelt een rechtskader vast voor elektronische handtekeningen, elektronische zegels, elektronische tijdstempels, elektronische documenten, diensten voor elektronische bezorging en website-authenticatie.
4. Deze verordening waarborgt het vrije verkeer in de interne markt van vertrouwensdiensten en -producten die aan deze verordening voldoen.

Artikel 2

Toepassingsgebied

1. Deze verordening is van toepassing op elektronische identificatie die wordt verstrekt door, namens of onder de verantwoordelijkheid van de lidstaten en op verleners van vertrouwensdiensten die in de Unie zijn gevestigd.
2. Deze verordening is niet van toepassing op de verlening van elektronische vertrouwensdiensten op basis van vrijwillige overeenkomsten op grond van het privaatrecht.
3. Deze verordening heeft geen betrekking op aspecten die verband houden met de totstandkoming of geldigheid van contracten of andere wettelijke verbintenissen waarvoor het nationale recht of het recht van de Unie vormvereisten voorschrijven.

Artikel 3

Definities

Voor de toepassing van deze verordening gelden de volgende definities:

- (1) "elektronische identificatie": het gebruik van persoonsidentificatiegegevens in elektronische vorm die op ondubbelzinnige wijze een natuurlijk persoon of rechtspersoon aanduiden;
- (2) "elektronisch identificatiemiddel": een materiële of immateriële eenheid die gegevens bevat als bedoeld in punt 1 van dit artikel en die gebruikt wordt voor de onlinetoegang tot diensten als bedoeld in artikel 5;
- (3) "stelsel voor elektronische identificatie": een systeem voor elektronische identificatie waarbinnen elektronische identificatiemiddelen worden uitgegeven aan de in punt 1 van dit artikel bedoelde personen;
- (4) "authenticatie": een elektronisch proces dat de validering van de elektronische identificatie van een natuurlijk persoon of rechtspersoon mogelijk maakt; of van de oorsprong en integriteit van elektronische gegevens;
- (5) "ondertekenaar": een natuurlijk persoon die een elektronische handtekening aanmaakt;
- (6) "elektronische handtekening": elektronische gegevens die gehecht zijn aan of logisch verbonden zijn met andere elektronische gegevens en die worden gebruikt door de ondertekenaar om te ondertekenen;

- (7) "geavanceerde elektronische handtekening": een elektronische handtekening die 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 gegevens waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;
- (8) "gekwaliceerde elektronische handtekening": een geavanceerde elektronische handtekening die wordt aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en die gebaseerd is op een gekwalificeerd certificaat voor elektronische handtekeningen;
- (9) "gegevens voor het aanmaken van elektronische handtekeningen": unieke gegevens die door de ondertekenaar worden gebruikt om een elektronische handtekening aan te maken;
- (10) "certificaat": een elektronische attestering die elektronische handtekeningen- of zegelvalideringsgegevens van een natuurlijk persoon of rechtspersoon koppelt aan het certificaat en bevestigt dat die gegevens en die persoon bij elkaar horen;
- (11) "gekwaliceerd certificaat voor elektronische handtekeningen": een attestering die wordt gebruikt om elektronische handtekeningen te ondersteunen, is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage I;
- (12) "vertrouwensdienst": iedere elektronische dienst bestaande uit het aanmaken, verifiëren, valideren, hanteren en bewaren van elektronische handtekeningen, elektronische zegels, elektronische tijdstempels, elektronische documenten, elektronische bezorgingsdiensten, website-authenticatie en elektronische certificaten, met inbegrip van certificaten voor elektronische handtekeningen en voor elektronische zegels;
- (13) "gekwaliceerde vertrouwensdienst": een vertrouwensdienst die voldoet aan de toepasselijke eisen in deze verordening;
- (14) "verlener van vertrouwensdiensten": een natuurlijke persoon of rechtspersoon die een of meer vertrouwensdiensten verleent;
- (15) "gekwaliceerde verlener van vertrouwensdiensten": een verlener van vertrouwensdiensten die voldoet aan de in deze verordening vastgestelde eisen;
- (16) "product": software of hardware, of relevante componenten daarvan, die bedoeld zijn om te worden gebruikt voor de verlening van vertrouwensdiensten;
- (17) "middel voor het aanmaken van elektronische handtekeningen": geconfigureerde software of hardware die wordt gebruikt om een elektronische handtekening aan te maken;
- (18) "gekwaliceerd middel voor het aanmaken van elektronische handtekeningen": een middel voor het aanmaken van elektronische handtekeningen dat voldoet aan de eisen van bijlage II;
- (19) "aanmaker van een zegel": een rechtspersoon die een elektronisch zegel aanmaakt;

(20) "elektronisch zegel": elektronische gegevens die gehecht zijn aan of logisch verbonden zijn met andere elektronische gegevens en die worden gebruikt om de oorsprong en integriteit van de ermee verbonden gegevens te waarborgen;

(21) "geavanceerd elektronisch zegel": een elektronisch zegel dat 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; en
- (d) het is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;

(22) "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;

(23) "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;

(24) "gekwalificeerd certificaat voor elektronische zegels": een attestering die wordt gebruikt om een elektronisch zegel te ondersteunen, is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage III;

(25) "elektronische tijdstempel": gegevens in elektronische vorm die andere elektronische gegevens verbinden aan een bepaald tijdstip en die bewijzen dat deze gegevens op dit tijdstip bestonden;

(26) "gekwalificeerde elektronische tijdstempel": een elektronische tijdstempel die voldoet aan de artikel 33 vastgestelde eisen;

(27) "elektronisch document": ieder document in elektronische vorm;

(28) "dienst voor elektronische bezorging": een dienst die het mogelijk maakt om gegevens via elektronische middelen te verzenden en die bewijs verstrekt ten aanzien van het hanteren van de verzonden gegevens, met inbegrip van bewijs van het verzenden of ontvangen van de gegevens, en die de verzonden gegevens beschermt tegen het risico van verlies, diefstal, beschadiging of eventuele onbevoegde wijzigingen;

(29) "gekwalificeerde dienst voor elektronische bezorging": een dienst voor elektronische bezorging die voldoet aan de in artikel 36 vastgestelde eisen;

(30) "gekwalificeerd certificaat voor website-authenticatie": een attestering die het mogelijk maakt om de authenticiteit van een website vast te stellen en die de website verbindt aan de persoon aan wie het certificaat is afgegeven, dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen in bijlage IV;

(31) "valideringsgegevens": gegevens die worden gebruikt om een elektronische handtekening of elektronisch zegel te valideren.

Artikel 4

Beginselen betreffende de interne markt

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

2. Het vrije verkeer van producten die aan deze verordening voldoen moet gewaarborgd worden.

HOOFDSTUK II

ELEKTRONISCHE IDENTIFICATIE

Artikel 5

Wederzijdse erkenning en aanvaarding

Wanneer een elektronische identificatie met gebruikmaking van een elektronisch identificatiemiddel en authenticatie vereist is op grond van nationale wetgeving of gangbare bestuursrechterlijke praktijk om onlinetoegang te krijgen tot een dienst, moet ieder elektronisch identificatiemiddel dat afgegeven is in een andere lidstaat en dat valt onder een stelsel dat is opgenomen in de door de Commissie gepubliceerde lijst overeenkomstig de procedure als bedoeld in artikel 7 worden erkend en aanvaard ten behoeve van het verkrijgen van toegang tot deze dienst.

Artikel 6

Voorwaarden voor de aanmelding van stelsels voor elektronische identificatie

1. Stelsels voor elektronische identificatie komen in aanmerking voor aanmelding overeenkomstig artikel 7, indien aan alle onderstaande voorwaarden is voldaan:

- (a) de elektronische identificatiemiddelen zijn afgegeven door, namens of onder de verantwoordelijkheid van de aanmeldende lidstaat;
- (b) de elektronische identificatiemiddelen kunnen worden gebruikt om toegang te verkrijgen tot ten minste overheidsdiensten waarvoor elektronische identificatie vereist is in de aanmeldende lidstaat;
- (c) de aanmeldende lidstaat waarborgt dat de persoonsidentificatiegegevens op ondubbelzinnige wijze worden gekoppeld aan de natuurlijke persoon of rechtspersoon als bedoeld in artikel 3, punt 1;
- (d) de aanmeldende lidstaat waarborgt de beschikbaarheid van een online-authenticatiemogelijkheid, op ieder moment en gratis, zodat iedere afhankelijke partij de ontvangen elektronische persoonsidentificatiegegevens kan valideren; de lidstaten

mogen geen specifieke technische eisen opleggen aan afhankelijke partijen die buiten hun grondgebied gevestigd zijn en die een dergelijke authenticatie willen uitvoeren. Wanneer er inbreuk wordt gepleegd op het aangemelde stelsel voor identificatie of de authenticatiemogelijkheid of wanneer de integriteit ervan deels wordt geschonden, moeten de lidstaten onverwijld het aangemelde stelsel of de authenticatiemogelijkheid of de delen waarvan de integriteit geschonden is opschorten of intrekken en de andere lidstaten en de Commissie overeenkomstig artikel 7 op de hoogte stellen;

- (e) de aanmeldende lidstaat stelt zich aansprakelijk voor:
- (i) de ondubbelzinnige koppeling van de persoonsidentificatiegegevens als bedoeld onder c), en
 - (ii) de onder d) beschreven authenticatiemogelijkheid.

2. Punt e) van lid 1 laat de aansprakelijkheid onverlet van partijen bij een transactie waarin elektronische identificatiemiddelen worden gebruikt die onder het aangemelde stelsel vallen.

Artikel 7

Aanmelding

1. Lidstaten die een stelsel voor elektronische identificatie aanmelden, doen de Commissie onverwijld de volgende informatie en eventuele latere wijzigingen daarvan toekomen:

- (a) een beschrijving van het aangemelde stelsel voor elektronische identificatie;
- (b) de autoriteiten die verantwoordelijk zijn voor het aangemelde stelsel voor elektronische identificatie;
- (c) informatie over wie de registratie van de ondubbelzinnige persoonsidentificatiegegevens beheert;
- (d) een beschrijving van de authenticatiemogelijkheid;
- (e) regelingen voor de opschorting of intrekking van het aangemelde identificatiestelsel of de authenticatiemogelijkheid of de delen waarvan de integriteit is geschonden in kwestie.

2. Zes maanden na de inwerkingtreding van deze verordening maakt de Commissie in het *Publicatieblad van de Europese Unie* de lijst bekend van de stelsels voor elektronische identificatie die zijn aangemeld overeenkomstig lid 1 alsmede de basisinformatie in verband hiermee.

3. Als de Commissie een aanmelding ontvangt nadat de periode als bedoeld in lid 2 verstreken is, wijzigt zij de lijst binnen drie maanden.

4. De Commissie kan door middel van uitvoeringshandelingen de omstandigheden, formaten en procedures van de aanmelding als bedoeld in lid 1 en 3 definiëren. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure.

Artikel 8

Coördinatie

1. De lidstaten werken samen om de interoperabiliteit te waarborgen van middelen voor elektronische identificatie die vallen onder een aangemeld stelsel en om de veiligheid ervan te verhogen.
2. De Commissie stelt door middel van uitvoeringshandelingen de nodige modaliteiten vast om de in lid 1 bedoelde samenwerking tussen de lidstaten te vergemakkelijken teneinde een hoog op het risiconiveau afgestemde niveau van vertrouwen en veiligheid te waarborgen. De uitvoeringshandelingen betreffen met name de uitwisseling van informatie, ervaringen en goede praktijken met betrekking tot stelsels voor elektronische identificatie, de collegiale toetsing van stelsels voor elektronische identificatie en het onderzoek van relevante ontwikkelingen in de sector voor elektronische identificatie door de bevoegde overheden van de lidstaten. De uitvoeringshandelingen worden goedgekeurd overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure.
3. De Commissie heeft de bevoegdheid om overeenkomstig artikel 38 betreffende het mogelijk maken van grensoverschrijdende interoperabiliteit van elektronische identificatiemiddelen gedelegeerde handelingen vast te stellen door de vaststelling van technische minimumeisen.

HOOFDSTUK III

VERTROUWENDIENSTEN

Afdeling 1

Algemene bepalingen

Artikel 9

Aansprakelijkheid

1. Een verlener van vertrouwensdiensten is aansprakelijk voor iedere rechtstreekse schade toegebracht aan iedere natuurlijk persoon of rechtspersoon wegens verzuim om te voldoen aan de in artikel 15, lid 1 vastgestelde verplichtingen, tenzij de verlener van vertrouwensdiensten kan bewijzen dat hij niet nalatig heeft gehandeld.
2. Een gekwalificeerde verlener van vertrouwensdiensten is aansprakelijk voor iedere rechtstreekse schade toegebracht aan ieder natuurlijk persoon of rechtspersoon wegens verzuim om te voldoen aan de in deze verordening vastgestelde eisen, in het bijzonder in artikel 19, tenzij de gekwalificeerde verlener van vertrouwensdiensten kan bewijzen dat hij niet nalatig heeft gehandeld.

Artikel 10

Verleners van vertrouwensdiensten uit derde landen

1. Gekwalificeerde vertrouwensdiensten en gekwalificeerde certificaten die zijn verstrekt door in een derde land gevestigde gekwalificeerde verleners van vertrouwensdiensten worden

aanvaard als gekwalificeerde vertrouwensdiensten en gekwalificeerde certificaten die zijn afgegeven door een gekwalificeerde, op het grondgebied van de Unie gevestigde verlener van vertrouwensdiensten, indien de gekwalificeerde vertrouwensdiensten of gekwalificeerde certificaten die afkomstig zijn uit het derde land erkend worden op grond van een overeenkomst tussen de Unie en derde landen of internationale organisaties overeenkomstig artikel 218 VWEU.

2. Met verwijzing naar lid 1 zorgen die overeenkomsten ervoor dat de voorschriften die gelden voor gekwalificeerde vertrouwensdiensten en gekwalificeerde certificaten die zijn verstrekt door op het grondgebied van de Unie gevestigde gekwalificeerde verlener van vertrouwensdiensten zijn nageleefd door de in derde landen gevestigde verlener van vertrouwensdiensten of door internationale organisaties, vooral met betrekking tot de bescherming van persoonsgegevens, veiligheid en toezicht.

Artikel 11

Gegevensverwerking- en bescherming

1. Verleners van vertrouwensdiensten en toezichthoudende organen waarborgen bij het verwerken van persoonsgegevens de eerlijke en rechtmatige verwerking overeenkomstig Richtlijn 95/46/EG.

2. Verleners van vertrouwensdiensten verwerken persoonsgegevens overeenkomstig Richtlijn 95/46/EG. Dergelijke verwerking is strikt beperkt tot het minimum aan gegevens dat nodig is om een certificaat af te geven of te beheren of om een gerelateerde vertrouwensdienst te verlenen.

3. Verleners van vertrouwensdiensten garanderen de geheimhouding en integriteit van gegevens die verbonden zijn aan een persoon aan wie de vertrouwensdienst wordt verleend.

4. Onverminderd de rechtsgevolgen van pseudoniemen in het nationale recht, mogen de lidstaten niet verhinderen dat verlener van vertrouwensdiensten op certificaten voor elektronische handtekeningen een pseudoniem vermelden in plaats van de werkelijke naam van de ondertekenaar.

Artikel 12

Toegankelijkheid voor personen met een handicap

Vertrouwensdiensten en eindgebruikersproducten die worden gebruikt bij de verlening van deze diensten worden zo veel mogelijk beschikbaar gemaakt voor personen met een handicap.

Afdeling 2

Toezicht

Artikel 13

Toe-zichthoudend orgaan

1. De lidstaten wijzen een passend orgaan aan dat gevestigd is op hun grondgebied of, onder voorwaarde van wederzijdse toestemming, in een andere lidstaat onder de verantwoordelijkheid van de aanwijzende lidstaat. Toezichthoudende organen krijgen alle toezichthoudende en onderzoeksbevoegdheden die nodig zijn voor de uitvoering van hun opdrachten.

2. Het toezichthoudende orgaan is verantwoordelijk voor de uitvoering van de volgende taken:

- (a) controle uitoefenen op verleners van vertrouwensdiensten die gevestigd zijn op het grondgebied van de aanwijzende lidstaat om te waarborgen dat zij voldoen aan de in artikel 15 vastgestelde eisen;
- (b) toezicht houden op gekwalificeerde verleners van vertrouwensdiensten die gevestigd zijn in de aanwijzende lidstaat en op de gekwalificeerde diensten die zij verlenen om te waarborgen dat zij en de door hen verleende gekwalificeerde vertrouwensdiensten voldoen aan de toepasselijke eisen in deze verordening;
- (c) waarborgen dat relevante informatie en gegevens als bedoeld onder g) van artikel 19, lid 2, en die vastgelegd zijn door gekwalificeerde verleners van vertrouwensdiensten, bewaard worden en toegankelijk blijven nadat een gekwalificeerde verlener van vertrouwensdiensten zijn activiteiten heeft gestaakt, gedurende een passende periode met het oog op het waarborgen van de continuïteit van de dienst.

3. Ieder toezichthoudend orgaan doet de Commissie en de lidstaten een jaarlijks verslag toekomen over de in het afgelopen kalenderjaar uitgevoerde toezichthoudende activiteiten voor het einde van het eerste kwartaal van het volgende jaar. Dit verslag bevat ten minste:

- (a) informatie over uitgevoerde toezichthoudende activiteiten;
- (b) een samenvatting van inbreukmeldingen die van verleners van vertrouwensdiensten ontvangen zijn overeenkomstig artikel 15, lid 2;
- (c) statistieken over de markt en het gebruik van gekwalificeerde vertrouwensdiensten, met inbegrip van informatie over gekwalificeerde verleners van vertrouwensdiensten zelf, de gekwalificeerde diensten die zij verlenen, de producten die zij gebruiken en de algemene beschrijving van hun klanten.

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

5. De Commissie wordt gemachtigd om overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen met betrekking tot de definitie van de in lid 2 bedoelde taken.

6. De Commissie kan door middel van uitvoeringshandelingen de omstandigheden, formaten en procedures voor het in lid 3 bedoelde verslag definiëren. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure.

Artikel 14

Onderlinge bijstand

1. Toezichthoudende organen moeten samenwerken met het oog op de uitwisseling van goede praktijken en elkaar zo snel mogelijk voorzien van relevante informatie en onderlinge bijstand, zodat de activiteiten op consequente wijze kunnen worden uitgevoerd. Onderlinge bijstand heeft in het bijzonder betrekking op informatieverzoeken en toezichthoudende maatregelen, zoals verzoeken om inspecties uit te voeren in verband met de veiligheidsaudits als bedoeld in de artikelen 15, 16 en 17.

2. Een toezichthoudend orgaan waartoe een verzoek om bijstand wordt gericht, mag niet weigeren het verzoek in te willigen, tenzij:

- (a) het niet bevoegd is om het verzoek te behandelen; of
- (b) de inwilliging van het verzoek onverenigbaar zou zijn met deze verordening.

3. Indien van toepassing kunnen toezichthoudende organen gezamenlijke onderzoeken uitvoeren waarbij personeelsleden van de toezichthoudende organen van andere lidstaten betrokken zijn.

Het toezichthoudende orgaan van de lidstaat waar het onderzoek plaatsvindt, mag in overeenstemming met het eigen nationale recht, onderzoekstaken delegeren aan de personeelsleden van het bijstand verlenende orgaan. Dergelijke bevoegdheden mogen uitsluitend worden uitgeoefend onder begeleiding en tijdens de aanwezigheid van personeel van het toezichthoudende orgaan dat om bijstand verzoekt. Het personeel van het bijstand verlenende orgaan is onderworpen aan het nationale recht van het toezichthoudende orgaan dat om bijstand verzoekt. Het toezichthoudende orgaan dat om bijstand verzoekt, is verantwoordelijk voor de handelingen van het personeel van het bijstand verlenende toezichthoudende orgaan.

4. De Commissie kan door middel van uitvoeringshandelingen de formaten en procedures voor de in dit artikel bedoelde onderlinge bijstand definiëren. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure.

Artikel 15

Veiligheidseisen die van toepassing zijn op verleners van vertrouwensdiensten

1. Verleners van vertrouwensdiensten die gevestigd zijn op het grondgebied van de Unie 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 technische mogelijkheden, 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 negatieve gevolgen van eventuele incidenten.

Onverminderd het bepaalde in artikel 16, lid 1, kan iedere verlener van vertrouwensdiensten het verslag van een door een erkend onafhankelijk orgaan uitgevoerde veiligheidsaudit indienen bij het toezichthoudende orgaan om te bevestigen dat passende veiligheidsmaatregelen zijn getroffen.

2. Verleners van vertrouwensdiensten stellen, zonder onnodige vertragingen en waar mogelijk binnen 24 uur nadat zij hiervan op de hoogte zijn, het bevoegde toezichthoudende orgaan, het bevoegde nationale orgaan voor informatieveiligheid en andere relevante derde partijen zoals gegevensbeschermingsautoriteiten op de hoogte van iedere veiligheidsinbreuk of ieder integriteitsverlies met aanzienlijke gevolgen voor de verleende vertrouwensdienst en voor de persoonsgegevens die daarmee worden beheerd.

Indien van toepassing, in het bijzonder indien een veiligheidsinbreuk of integriteitsverlies twee of meer lidstaten treft, stelt het toezichthoudende orgaan in kwestie toezichthoudende organen in andere lidstaten en het Europees Agentschap voor netwerk- en informatiebeveiliging (Enisa) op de hoogte.

Het toezichthoudende orgaan in kwestie kan ook het publiek op de hoogte stellen of dit eisen van de verlener van vertrouwensdiensten, indien het van oordeel is dat bekendmaking van de inbreuk in het algemene belang is.

3. Het toezichthoudende orgaan doet het Enisa en de Commissie eenmaal per jaar een samenvatting toekomen van inbreukmeldingen die zijn ontvangen van verleners van vertrouwensdiensten.

4. Ten behoeve van de uitvoering van lid 1 en 2 heeft het bevoegde toezichthoudende orgaan de bevoegdheid om bindende instructies op te leggen aan verleners van vertrouwensdiensten.

5. De Commissie wordt gemachtigd om overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen met betrekking tot de nadere omschrijving van de in lid 1 bedoelde maatregelen.

6. De Commissie kan door middel van uitvoeringshandelingen de omstandigheden, formaten en procedures, met inbegrip van termijnen, definiëren die van toepassing zijn voor de doeleinden van lid 1 tot en met lid 3. Deze uitvoeringshandelingen worden vastgelegd overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure.

Artikel 16

Toezicht op gekwalificeerde verleners van vertrouwensdiensten

1. Gekwalificeerde verleners van vertrouwensdiensten worden jaarlijks onderworpen aan een audit door een erkend onafhankelijk orgaan om te bevestigen dat zij en de gekwalificeerde vertrouwensdiensten die door hen worden verleend, voldoen aan de eisen waarin deze verordening voorziet, en zij dienen het verslag van de veiligheidsaudit in bij het toezichtsorgaan.

2. Onverminderd het bepaalde in lid 1, kan het toezichtsorgaan op elk tijdstip een audit houden van de gekwalificeerde verleners van vertrouwensdiensten om te bevestigen dat zij en de gekwalificeerde vertrouwensdiensten die door hen verleend worden, nog steeds voldoen aan de eisen waarin deze verordening voorziet, ofwel op eigen initiatief ofwel ten gevolge van een verzoek van de Commissie. Het toezichtsorgaan brengt de overheden voor gegevensbescherming op de hoogte van de resultaten van de audits wanneer er sprake blijkt te zijn van een inbreuk op de regels voor de bescherming van persoonsgegevens.

3. Het toezichtsorgaan is bevoegd om bindende instructies op te leggen aan gekwalificeerde dienstverleners om niet-naleving van de voorschriften die uit het verslag van de veiligheidsaudit blijkt, recht te zetten.

4. Wat punt 3 betreft: als de gekwalificeerde verlener van vertrouwensdiensten een dergelijke niet-naleving niet binnen een door het toezichtsorgaan bepaalde tijdspanne rechtzet, verliest hij zijn gekwalificeerde status en wordt hem door het toezichtsorgaan medegedeeld dat zijn status dienovereenkomstig aangepast zal worden in de in artikel 18 bedoelde vertrouwenslijsten.

5. De Commissie is gemachtigd om overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen met betrekking tot de specificatie van de voorwaarden voor erkenning van het onafhankelijke orgaan dat de in lid 1 van dit artikel en in artikel 15, lid 1, en artikel 17, lid 1, bedoelde audit uitvoert.

6. De Commissie kan door middel van uitvoeringshandelingen de omstandigheden, procedures en formaten omschrijven die gelden voor de toepassing van lid 1, 2 en 4. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure.

Artikel 17

Initiatie van een gekwalificeerde vertrouwensdienst

1. Gekwalificeerde verlener van vertrouwensdiensten melden bij het toezichtsorgaan hun voornemen om een gekwalificeerde vertrouwensdienst op te starten en dienen bij het toezichtsorgaan een verslag in van een door een erkend onafhankelijk orgaan uitgevoerde veiligheidsaudit, zoals bepaald in artikel 16, lid 1. Gekwalificeerde verlener van vertrouwensdiensten kunnen een aanvang maken met de verlening van de vertrouwensdienst zodra zij de melding en het verslag van de veiligheidsaudit bij het toezichtsorgaan hebben ingediend.

2. Zodra de desbetreffende documenten overeenkomstig lid 1 bij het toezichtsorgaan zijn ingediend, worden de gekwalificeerde dienstverleners opgenomen in de vertrouwenslijsten als bedoeld in artikel 18, met de vermelding dat de aanmelding is ingediend.

3. Het toezichtsorgaan verifieert of de gekwalificeerde verlener van vertrouwensdiensten en de door hem verleende vertrouwensdiensten in overeenstemming met de eisen van de verordening zijn.

Het toezichtsorgaan geeft de gekwalificeerde status van de gekwalificeerde dienstverleners evenals van de door hem verleende diensten aan in de vertrouwenslijsten na een positieve evaluatie van de naleving, ten laatste een maand nadat de melding in overeenstemming met lid 1 heeft plaatsgevonden.

Indien de evaluatie van de naleving niet binnen een maand is afgerond, brengt het toezichtsorgaan de gekwalificeerde verlener van vertrouwensdiensten op de hoogte met opgave van redenen van de vertraging en de termijn waarbinnen de naleving geëvalueerd zal zijn.

4. Een gekwalificeerde vertrouwensdienst waarvoor een aanmelding is gebeurd conform lid 1 kan niet worden geweigerd voor de vervulling van een administratieve procedure of formaliteit door de betrokken openbare instantie omdat zij niet is opgenomen in de in lid 3 bedoelde lijsten.

5. De Commissie kan door middel van uitvoeringshandelingen de omstandigheden, formaten en procedures omschrijven die gelden voor de toepassing van de leden 1, 2 en 3. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure.

Artikel 18

Vertrouwenslijsten

1. Elke lidstaat stelt vertrouwenslijsten op met informatie over de gekwalificeerde verleners van vertrouwensdiensten waarvoor hij bevoegd is, samen met informatie over de gekwalificeerde vertrouwensdiensten die door hen verleend worden; hij houdt deze lijst bij en publiceert ze.

2. De lidstaten dragen zorg voor het op een veilige manier opstellen, bijhouden en publiceren van elektronisch ondertekende of verzegelde vertrouwenslijsten, als vastgesteld 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 verzegelen, en alle wijzigingen daaraan.

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

5. De Commissie is bevoegd om overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen met betrekking tot de omschrijving van de in lid 1 bedoelde informatie.

6. De Commissie kan door middel van uitvoeringshandelingen de technische specificaties en formaten van vertrouwenslijsten omschrijven die gelden voor de toepassing van lid 1 tot en met 4. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure.

Artikel 19

Eisen voor gekwalificeerde verleners van vertrouwensdiensten

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

Dergelijke informatie wordt geverifieerd door de gekwalificeerde verlener van vertrouwensdiensten of door een gemachtigde derde partij die handelt onder de verantwoordelijkheid van de gekwalificeerde dienstverlener:

- (a) door de fysieke aanwezigheid van de natuurlijk persoon of een gemachtigde afgevaardigde van de rechtspersoon, of
- (b) op afstand, door middel van elektronische identificatiemiddelen onder een aangemeld schema dat is afgegeven in overeenstemming met het onder a) bepaalde.

2. Gekwalificeerde verlener van vertrouwensdiensten die gekwalificeerde vertrouwensdiensten verlenen:

- (a) hebben personeel in dienst dat beschikt over de nodige deskundigheid, ervaring en kwalificaties, dat administratieve en managementprocedures toepast die in overeenstemming zijn met Europese of internationale normen, en dat een toereikende scholing heeft ontvangen op het gebied van voorschriften inzake veiligheid en bescherming van persoonsgegevens;
- (b) dragen het risico van aansprakelijkheid voor schade door ervoor te zorgen dat zij voldoende financiële middelen tot hun beschikking hebben of door middel van een toereikende aansprakelijkheidsverzekering;
- (c) informeren personen die gebruik wensen te maken van een gekwalificeerde vertrouwensdienst over de precieze voorwaarden betreffende het gebruik van die dienst alvorens een contractuele verbintenis aan te gaan;
- (d) maken gebruik van betrouwbare systemen en producten die beschermd zijn tegen wijziging en die de technische veiligheid en betrouwbaarheid garanderen van de processen die zij ondersteunen;
- (e) maken gebruik van betrouwbare systemen voor de opslag van aan hen verstrekte gegevens in een vorm die verifieerbaar is, zodat
 - de gegevens uitsluitend publiek beschikbaar zijn wanneer de persoon aan wie de gegevens afgegeven werden, hiervoor toestemming heeft gegeven,
 - alleen bevoegde personen gegevens kunnen invoeren en wijzigen,
 - de authenticiteit van de informatie kan worden gecontroleerd;
- (f) nemen maatregelen tegen vervalsing en diefstal van gegevens;
- (g) leggen gedurende een gepaste periode alle relevante informatie vast met betrekking tot de gegevens die de gekwalificeerde verlener van vertrouwensdiensten heeft afgegeven en ontvangen, met name om ten behoeve van gerechtelijke procedures bewijzen te kunnen leveren. Dit vastleggen mag elektronisch plaatsvinden;
- (h) hebben een geactualiseerd beëindigingsplan om de continuïteit van de dienst te verzekeren in overeenstemming met wat door het toezichtsorgaan op grond van artikel 13, lid 2, onder c), is bepaald;

- (i) zorgen voor wettelijke verwerking van persoonsgegevens in overeenstemming met artikel 11.

3. Gekwalificeerde verleners van vertrouwensdiensten die gekwalificeerde certificaten afgeven, registreren in hun certificatendatabase de intrekking van een certificaat ten laatste tien minuten nadat de intrekking ingegaan is.

4. Betreffende het bepaalde onder lid 3 verstrekken gekwalificeerde verleners van vertrouwensdiensten die gekwalificeerde certificaten afgeven aan elke afhankelijke partij informatie over de geldigheid of ingetrokken status van door hen afgegeven gekwalificeerde certificaten. Deze informatie is op elk moment in ieder geval op certificaatbasis 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. Wanneer betrouwbare systemen en producten aan dergelijke normen voldoen, wordt aangenomen dat er sprake is van overeenstemming met de in artikel 19 bepaalde eisen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure. De Commissie maakt deze handelingen bekend in het *Publicatieblad van de Europese Unie*.

Afdeling 3

Elektronische handtekening

Artikel 20

Rechtsgevolgen en aanvaarding van elektronische handtekeningen

1. De rechtsgeldigheid 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.

2. Een gekwalificeerde elektronische handtekening heeft dezelfde rechtsgeldigheid als een handgeschreven handtekening.

3. Gekwalificeerde elektronische handtekeningen worden erkend en aanvaard in alle lidstaten.

4. Als een elektronische handtekening met een veiligheidsniveau lager dan een gekwalificeerde elektronische handtekening vereist is, met name door een lidstaat voor toegang tot een onlinedienst aangeboden door een openbare instantie op grond van een toereikende beoordeling van de bij een dergelijke dienst betrokken risico's, worden alle elektronische handtekeningen die ten minste hetzelfde veiligheidsniveau hebben, erkend en aanvaard.

5. De lidstaten vereisen voor grensoverschrijdende toegang tot een onlinedienst die door een openbare instantie wordt aangeboden, geen elektronische handtekening van een hoger veiligheidsniveau dan een gekwalificeerde elektronische handtekening.

6. De Commissie is gemachtigd om overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen met betrekking tot de omschrijving van de in lid 4 bedoelde verschillende veiligheidsniveaus van elektronische handtekeningen.

7. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake de veiligheidsniveaus van elektronische handtekeningen. Wanneer een elektronische handtekening aan dergelijke normen voldoet, wordt aangenomen dat er sprake is van overeenstemming met het veiligheidsniveau dat in een gedelegeerde handeling op grond van lid 6 omschreven is. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure. De Commissie maakt deze handelingen bekend in het *Publicatieblad van de Europese Unie*.

Artikel 21

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. Als een gekwalificeerd certificaat voor elektronische handtekeningen na initiële activering wordt ingetrokken, verliest het zijn geldigheid en kan de status ervan in geen geval worden hersteld door de geldigheid ervan te vernieuwen.
4. De Commissie is gemachtigd om overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen betreffende de nadere specificatie van de in bijlage I vastgestelde eisen.
5. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake gekwalificeerde certificaten voor elektronische handtekeningen. Wanneer een gekwalificeerd certificaat voor elektronische handtekeningen aan dergelijke normen voldoet, wordt aangenomen dat er sprake is van overeenstemming met de in bijlage I vastgestelde eisen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure. De Commissie maakt deze handelingen bekend in het *Publicatieblad van de Europese Unie*.

Artikel 22

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. Wanneer een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen aan dergelijke normen voldoet, wordt aangenomen dat er sprake is van overeenstemming met de in bijlage II bepaalde eisen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure. De Commissie maakt deze handelingen bekend in het *Publicatieblad van de Europese Unie*.

Artikel 23

Certificatie van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen

1. Gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen kunnen worden gecertificeerd door geschikte, daartoe door de lidstaten aangewezen publieke of particuliere organen, op voorwaarde dat zij daarvoor zijn onderworpen aan een veiligheidsbeoordeling uitgevoerd in overeenstemming met een van de normen inzake de veiligheidsbeoordeling van producten op het gebied van informatietechnologie die zijn opgenomen in een lijst welke door de Commissie door middel van uitvoeringshandelingen wordt vastgesteld. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure. De Commissie maakt deze handelingen bekend in het *Publicatieblad van de Europese Unie*.
2. De lidstaten verstrekken aan de Commissie en de andere lidstaten de namen en adressen van de door hen aangewezen publieke of particuliere organen zoals bedoeld in lid 1.
3. De Commissie is gemachtigd om overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen met betrekking tot het opstellen van specifieke criteria waaraan de aangewezen organen zoals bedoeld in lid 1, moeten voldoen.

Artikel 24

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

1. De lidstaten verstrekken de Commissie onverwijld informatie over gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen die zijn gecertificeerd door de organen zoals bedoeld in artikel 23. Zij bezorgen de Commissie ook onverwijld informatie over middelen voor het aanmaken van elektronische handtekeningen die niet langer 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, en publiceert en onderhoudt deze lijst.
3. De Commissie kan door middel van uitvoeringshandelingen omstandigheden, formaten en procedures omschrijven die gelden voor de toepassing van lid 1. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure.

Artikel 25

Eisen voor de validering van gekwalificeerde elektronische handtekeningen

1. Een gekwalificeerde elektronische handtekening wordt als geldig beschouwd indien de geldigheid ervan met een hoog niveau van zekerheid vastgesteld kan worden en indien op het moment van ondertekenen:

- (a) het certificaat dat de handtekening ondersteunt een gekwalificeerd certificaat voor elektronische handtekeningen is overeenkomstig het bepaalde in bijlage I;
- (b) het vereiste gekwalificeerde certificaat authentiek en geldig is;
- (c) de gegevens voor het valideren van de handtekening overeenstemmen met de gegevens die aan de afhankelijke partij verstrekt werden;
- (d) de reeks gegevens die ondubbelzinnig verwijst naar de ondertekenaar, correct werd doorgegeven aan de afhankelijke partij;
- (e) de afhankelijke partij duidelijk wordt gewezen op het eventuele gebruik van een pseudoniem;
- (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) voldaan is aan de in artikel 3, punt 7, bedoelde eisen;
- (i) het juiste resultaat van het valideringsproces dat door het systeem is gebruikt voor het valideren van de handtekening wordt doorgegeven aan de afhankelijke partij en de afhankelijke partij in de gelegenheid wordt gesteld om relevante veiligheidsproblemen op te merken.

2. De Commissie is gemachtigd om overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen betreffende de nadere specificatie van de in lid 1 vastgestelde eisen.

3. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake de validering van gekwalificeerde elektronische handtekeningen. Wanneer de validering van gekwalificeerde elektronische handtekeningen aan dergelijke normen voldoet, wordt aangenomen dat er sprake is van overeenstemming met de in lid 1 vastgestelde eisen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure. De Commissie maakt deze handelingen bekend in het *Publicatieblad van de Europese Unie*.

Artikel 26

Gekwalificeerde valideringsdienst voor gekwalificeerde elektronische handtekeningen

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

- (a) validering verstrekt overeenkomstig artikel 25, lid 1, en
- (b) de daarvan afhankelijke 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. Wanneer de valideringsdienst voor gekwalificeerde elektronische handtekeningen aan dergelijke normen voldoet, wordt aangenomen dat er sprake is van overeenstemming met de in lid 1, onder b), bepaalde eisen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure. De Commissie maakt deze handelingen bekend in het *Publicatieblad van de Europese Unie*.

Artikel 27

Bewaring van gekwalificeerde elektronische handtekeningen

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

2. De Commissie is gemachtigd om overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen betreffende de nadere specificatie van de in lid 1 bepaalde eisen.

3. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake de bewaring van gekwalificeerde elektronische handtekeningen. Wanneer de voorzieningen voor de bewaring van gekwalificeerde elektronische handtekeningen aan dergelijke normen voldoen, wordt aangenomen dat er sprake is van overeenstemming met de in lid 1 vastgestelde eisen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure. De Commissie maakt deze handelingen bekend in het *Publicatieblad van de Europese Unie*.

Afdeling 4

Elektronische zegels

Artikel 28

Rechtsgevolgen van elektronische zegels

1. De rechtsgeldigheid 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.

2. Voor een gekwalificeerd elektronisch zegel geldt het wettelijk vermoeden dat het de oorsprong en integriteit van de gegevens waaraan het verbonden is, waarborgt.

3. Een gekwalificeerd elektronisch zegel wordt erkend en aanvaard in alle lidstaten.

4. Als voor elektronische zegels een veiligheidsniveau lager dan een gekwalificeerd elektronisch zegel vereist is, met name door een lidstaat voor toegang tot een onlinedienst aangeboden door een openbare instantie op grond van een toereikende beoordeling van de aan

een dergelijke dienst verbonden risico's, worden alle elektronische zegels met ten minste hetzelfde veiligheidsniveau aanvaard.

5. De lidstaten vereisen voor de toegang tot een door een overheidsinstantie aangeboden onlinedienst geen elektronisch zegel met een hoger veiligheidsniveau dan gekwalificeerde elektronische zegels.

6. De Commissie is gemachtigd om overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen met betrekking tot de omschrijving van de in lid 4 bedoelde verschillende veiligheidsniveaus voor elektronische zegels.

7. De Commissie kan door middel van uitvoeringshandelingen referentienummers opstellen voor normen inzake de veiligheidsniveaus van elektronische zegels. Wanneer een elektronisch zegel aan dergelijke normen voldoet, wordt aangenomen dat er sprake is van overeenstemming met het veiligheidsniveau dat overeenkomstig lid 6 in een gedelegeerde handeling is vastgesteld. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure. De Commissie maakt deze handelingen bekend in het *Publicatieblad van de Europese Unie*.

Artikel 29

Eisen voor 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. Als een gekwalificeerd certificaat voor een elektronisch zegel na initiële activering wordt ingetrokken, verliest het zijn geldigheid en kan de status ervan in geen geval worden hersteld door de geldigheid ervan te vernieuwen.

4. De Commissie is gemachtigd om overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen met betrekking tot de nadere specificatie van de in bijlage III bepaalde eisen.

5. De Commissie kan door middel van uitvoeringshandelingen referentienummers opstellen voor normen inzake gekwalificeerde certificaten voor elektronische zegels. Wanneer een elektronisch zegel aan dergelijke normen voldoet, wordt aangenomen dat er sprake is van overeenstemming met de in bijlage III bepaalde eisen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure. De Commissie maakt deze handelingen bekend in het *Publicatieblad van de Europese Unie*.

Artikel 30

Gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen

1. Artikel 22 is *mutatis mutandis* van toepassing op eisen voor gekwalificeerde middelen voor het aanmaken van elektronische zegels.

2. Artikel 23 is *mutatis mutandis* van toepassing op de certificatie van gekwalificeerde middelen voor het aanmaken van elektronische zegels.
3. Artikel 24 is *mutatis mutandis* van toepassing op de publicatie van een lijst van gecertificeerde gekwalificeerde middelen voor het aanmaken van elektronische zegels.

Artikel 31

Validering en bewaring van gekwalificeerde elektronische zegels

De artikelen 25, 26 en 27 zijn *mutatis mutandis* van toepassing op de validering en bewaring van gekwalificeerde elektronische zegels.

Afdeling 5

Elektronisch tijdstempel

Artikel 32

Rechtsgevolg van elektronische tijdstempels

1. De rechtsgeldigheid 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.
2. Voor een gekwalificeerd elektronisch tijdstempel geldt het wettelijk vermoeden dat het aangeduide tijdstip en de integriteit van de gegevens die aan het tijdstip zijn gekoppeld, zijn gewaarborgd.
3. Een gekwalificeerd elektronisch tijdstempel wordt erkend en aanvaard in alle lidstaten.

Artikel 33

Eisen voor gekwalificeerde elektronische tijdstempels

1. Een gekwalificeerd elektronisch tijdstempel voldoet aan de volgende eisen:
 - (a) het tijdstempel wordt op correcte wijze gekoppeld aan de gecoördineerde universele tijd (UTC) en wel op zodanige wijze dat onmerkbare wijziging van de gegevens kan worden uitgesloten;
 - (b) het stempel is gebaseerd op een betrouwbare tijdsbron;
 - (c) het stempel wordt afgegeven door een gekwalificeerd verlener van vertrouwensdiensten;
 - (d) het stempel wordt ondertekend met behulp van een geavanceerde elektronische handtekening of 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 juiste koppeling van tijd aan gegevens en aan een betrouwbare tijdsbron. Wanneer een juiste koppeling van tijd aan gegevens en aan een betrouwbare tijdsbron aan dergelijke normen voldoet, wordt aangenomen dat er sprake is van overeenstemming met de in lid 1 vastgestelde eisen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure. De Commissie maakt deze handelingen bekend in het *Publicatieblad van de Europese Unie*.

Afdeling 6

Elektronische documenten

Artikel 34

Rechtsgevolgen en aanvaarding van de elektronische documenten

1. Een elektronisch document wordt beschouwd als gelijkwaardig aan een papieren document en is toelaatbaar als bewijsmiddel in gerechtelijke procedures, gelet op het gegarandeerde niveau van authenticiteit en integriteit van het document.
2. Voor een document met een gekwalificeerde elektronische handtekening of een gekwalificeerd elektronisch zegel van de persoon die bevoegd is om het betreffende document af te geven, geldt het wettelijk vermoeden van authenticiteit en integriteit op voorwaarde dat het document geen dynamische kenmerken heeft die automatische wijziging van het document tot gevolg kunnen hebben.
3. Als een origineel document of een gecertificeerd afschrift vereist is voor het verlenen van een door een overheidsinstantie aangeboden onlinedienst, worden in andere lidstaten zonder verdere eisen in ieder geval elektronische documenten aanvaard die zijn afgegeven door de personen welke bevoegd zijn om de betreffende documenten af te geven en die op grond van de nationale wetgeving van de lidstaat van herkomst worden beschouwd als originelen of gecertificeerde afschriften.
4. De Commissie kan door middel van uitvoeringshandelingen formaten van elektronische handtekeningen en van zegels vaststellen die worden aanvaard wanneer een ondertekenend of bezegeld document door een lidstaat vereist is voor het leveren van een in lid 2 bedoelde, door een overheidsinstantie aangeboden onlinedienst. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure.

Afdeling 7

Gekwalificeerde dienst voor elektronische bezorging

Artikel 35

Rechtsgevolg van een dienst voor elektronische bezorging

1. Gegevens die door middel van een dienst voor elektronische bezorging ontvangen of verstuurd worden zijn toelaatbaar als bewijsmiddel in gerechtelijke procedures wat betreft de integriteit van de gegevens en de betrouwbaarheid van de datum en het tijdstip waarop de gegevens werden verstuurd naar of ontvangen door een specifieke geadresseerde.

2. Voor gegevens die door middel van een gekwalificeerde dienst voor elektronische bezorging worden verstuurd of ontvangen, geldt het wettelijk vermoeden dat de gegevens correct zijn en dat de datum en het tijdstip van verzending of ontvangst van de gegevens zoals aangeduid door het gekwalificeerde systeem voor elektronische bezorging, betrouwbaar zijn.

3. De Commissie is gemachtigd om in overeenstemming met artikel 38 gedelegeerde handelingen vast te stellen met betrekking tot de specificatie van mechanismen voor het zenden of ontvangen van gegevens door middel van elektronische bezorgingsdiensten, met als doel de interoperabiliteit tussen elektronische bezorgingsdiensten te bevorderen.

Artikel 36

Eisen voor gekwalificeerde elektronische bezorgingsdiensten

1. Gekwalificeerde elektronische bezorgingsdiensten voldoen aan de volgende eisen:

- (a) zij worden verleend door een of meerdere gekwalificeerde verleners van vertrouwensdiensten;
- (b) het is mogelijk de identiteit van de zender en, indien van toepassing, de geadresseerde ondubbelzinnig vast te stellen;
- (c) het proces van versturen of 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 onmerkbaar wijziging van gegevens kan worden uitgesloten;
- (d) de verzender en de geadresseerde van de gegevens worden in kennis gesteld van eventuele wijzigingen van de gegevens die nodig zijn voor het verzenden of ontvangen van de gegevens;
- (e) het tijdstip van verzenden, ontvangen en wijzigen van gegevens wordt aangeduid door een gekwalificeerd elektronisch tijdstempel;
- (f) wanneer gegevens overgedragen worden tussen twee of meerdere gekwalificeerde verleners van vertrouwensdiensten, zijn de eisen onder a) tot en met e) 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. Wanneer het proces voor het verzenden en ontvangen van gegevens aan dergelijke normen voldoet, wordt aangenomen dat er sprake is van overeenstemming met de in lid 1 vastgelegde eisen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure. De Commissie maakt deze handelingen bekend in het *Publicatieblad van de Europese Unie*.

Afdeling 8

Authenticatie van websites

Eisen voor gekwalificeerde certificaten voor authenticatie van websites

1. Gekwalificeerde certificaten voor authenticatie van websites voldoen aan de in bijlage IV bepaalde eisen.
2. Gekwalificeerde certificaten voor authenticatie van websites worden erkend en aanvaard in alle lidstaten.
3. De Commissie is gemachtigd om in overeenstemming met artikel 38 gedelegeerde handelingen vast te stellen met betrekking tot de nadere specificatie van de in bijlage IV vastgestelde eisen.
4. De Commissie kan door middel van uitvoeringshandelingen referentienummers vaststellen voor normen inzake gekwalificeerde certificaten voor de authenticatie van websites. Wanneer een gekwalificeerd certificaat voor de authenticatie van websites aan dergelijke normen voldoet, wordt overeenstemming met de in bijlage IV vastgestelde eisen aangenomen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure. De Commissie maakt deze handelingen bekend in het *Publicatieblad van de Europese Unie*.

HOOFDSTUK IV

GEDELEGEERDE HANDELINGEN

Uitoefening van de delegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt volgens de voorwaarden van dit artikel aan de Commissie toegekend.
2. De Commissie wordt voor een onbepaalde periode vanaf het in werking treden van de verordening gemachtigd om de in artikel 8, lid 3, artikel 13, lid 5, artikel 15, lid 5, artikel 16, lid 5, artikel 18, lid 5, artikel 20, lid 6, artikel 21, lid 4, artikel 23, lid 3, artikel 25, lid 2, artikel 27, lid 2, artikel 28, lid 6, artikel 29, lid 4, artikel 30, lid 2, artikel 31, artikel 35, lid 3 en artikel 37, lid 3, bedoelde gedelegeerde handelingen vast te stellen.
3. De in artikel 8, lid 3, artikel 13, lid 5, artikel 15, lid 5, artikel 16, lid 5, artikel 18, lid 5, artikel 20, lid 6, artikel 21, lid 4, artikel 23, lid 3, artikel 25, lid 2, artikel 27, lid 2, artikel 28, lid 6, artikel 29, lid 4, artikel 30, lid 2, artikel 31, artikel 35, lid 3, en artikel 37, lid 3, bedoelde bevoegdheidsdelegatie kan op elk tijdstip door het Europees Parlement of de Raad worden ingetrokken. Een besluit tot intrekking maakt een einde aan de delegatie van de in dat besluit genoemde bevoegdheid. Dit treedt in werking op de dag volgend op de publicatie van de beschikking in het Publicatieblad van de Europese Unie of een latere datum die daarin nader wordt bepaald. Het laat de geldigheid van alle reeds in werking zijnde gedelegeerde handelingen onverlet.
4. Zodra de Commissie een gedelegeerde handeling vaststelt, stelt zij het Europees Parlement en de Raad daar op hetzelfde moment van in kennis.

5. Een overeenkomstig artikel 8, lid 3, artikel 13, lid 5, artikel 15, lid 5, artikel 16, lid 5, artikel 18, lid 5, artikel 20, lid 6, artikel 21, lid 4, artikel 23, lid 3, artikel 25, lid 2, artikel 27, lid 2, artikel 28, lid 6, artikel 29, lid 4, artikel 30, lid 2, artikel 31, artikel 35, lid 3, en artikel 37, lid 3 vastgestelde gedelegeerde handeling treedt alleen in werking wanneer noch het Europees Parlement, noch de Raad binnen een termijn van twee maanden na de kennisgeving van die handeling aan het Europees Parlement en de Raad bezwaar tegen de handeling heeft gemaakt of wanneer zowel het Europees Parlement als de Raad vóór het verstrijken van die termijn aan de Commissie hebben meegedeeld geen bezwaar te zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met twee maanden verlengd.

HOOFDSTUK V

UITVOERINGSHANDELINGEN

Artikel 39

Comitéprocedure

1. De Commissie wordt bijgestaan door een comité. Dat comité is een comité in de betekenis van Verordening (EU) nr. 182/2011.
2. Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening 182/2011 van toepassing.

HOOFDSTUK IV

SLOTBEPALINGEN

Artikel 40

Verslag

De Commissie dient bij het Europees Parlement en de Raad een verslag in over de toepassing van deze verordening. Het eerste verslag wordt uiterlijk vier jaar na de inwerkingtreding van deze verordening ingediend. Daarna worden de volgende verslagen om de vier jaar ingediend.

Artikel 41

Intrekking

1. Richtlijn 1999/93/EG wordt ingetrokken.
2. Verwijzingen naar de ingetrokken richtlijn gelden als verwijzingen naar de onderhavige verordening.
3. 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 handtekeningen volgens de onderhavige verordening.

4. Gekwalificeerde certificaten die overeenkomstig Richtlijn 1999/93/EG werden afgegeven, worden beschouwd als gekwalificeerde certificaten voor elektronische handtekeningen volgens de onderhavige verordening totdat de geldigheidsduur ervan is verstreken, maar ten laatste vijf jaar na het in werking treden van de onderhavige verordening.

Artikel 42

Inwerkingtreding

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

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

Gedaan te Brussel,

Voor het Europees Parlement
De voorzitter

Voor de Raad
De voorzitter

BIJLAGE I

Eisen voor gekwalificeerde certificaten voor elektronische handtekeningen

Gekwalificeerde certificaten voor elektronische handtekeningen bevatten:

- (a) een aanduiding, ten minste in een voor automatische verwerking geschikte vorm, 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 aflevert, waarin ten minste de lidstaat vermeld is waarin de verlener gevestigd is en
 - voor een rechtspersoon: de naam en het registratienummer zoals deze voorkomen in de officiële administratie,
 - voor een natuurlijk persoon: de naam van de persoon;
- (c) een reeks gegevens die ondubbelzinnig verwijzen naar de ondertekenaar aan wie het certificaat is afgegeven, met ten minste de naam van de ondertekenaar of een pseudoniem, dat als dusdanig geïdentificeerd wordt;
- (d) valideringsgegevens voor elektronische handtekeningen die overeenstemmen met de gegevens voor het aanmaken van de elektronische handtekening;
- (e) informatie over het begin en einde van de geldigheidsduur van het certificaat;
- (f) de identificatiecode van het certificaat, die uniek is voor de gekwalificeerde verlener van de vertrouwensdienst;
- (g) de geavanceerde elektronische handtekening of het geavanceerde elektronische zegel van de afgevende gekwalificeerde verlener van vertrouwensdiensten;
- (h) de locatie waar het certificaat dat de geavanceerde elektronische handtekening of geavanceerde elektronische zegel zoals bedoeld onder g) ondersteunt, kosteloos beschikbaar is;
- (i) de locatie van de diensten in verband met de geldigheidsstatus van een certificaat waar informatie kan worden opgevraagd over de geldigheidsstatus van het gekwalificeerde certificaat;
- (j) indien de gegevens voor het aanmaken van een elektronische handtekening met betrekking tot de valideringsgegevens van de elektronische handtekening bewaard worden in een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen, een toereikende aanduiding hiervan, ten minste in een voor automatische verwerking geschikte vorm.

BIJLAGE II

Eisen voor gekwalificeerde middelen voor het aanmaken van handtekeningen

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

- (a) de geheimhouding van de gegevens die worden gebruikt om elektronische handtekeningen aan te maken gewaarborgd is;
- (b) de gegevens voor het aanmaken van elektronische handtekeningen 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 beschermd is tegen vervalsing met de thans beschikbare technieken;
- (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 de ondertekening aan de ondertekenaar worden voorgelegd.

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

4. Gekwalificeerde verlener van vertrouwensdiensten die gegevens voor het aanmaken van elektronische handtekeningen beheren namens de ondertekenaar mogen de gegevens voor het aanmaken van elektronische handtekening 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 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 moeten het navolgende bevatten:

- (a) een vermelding, minimaal 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 op ondubbelzinnige wijze de gekwalificeerde verlener van vertrouwensdiensten aanduidt die de gekwalificeerde certificaten afgeeft, met inbegrip van ten minste de lidstaat waar die dienstverlener is gevestigd en
 - voor een rechtspersoon: naam en registratienummer zoals vermeld in de officiële registers,
 - voor een natuurlijk persoon: naam van de persoon;
- (c) een reeks gegevens die op ondubbelzinnige wijze de rechtspersoon aanduidt aan wie het certificaat is afgegeven, met inbegrip van ten minste de naam en 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) nadere informatie ten aanzien van het 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 valideringsstatusdiensten voor certificaten die gebruikt kunnen worden om informatie over de valideringsstatus van het gekwalificeerde certificaat te raadplegen;
- (j) in gevallen waarin de gegevens voor het aanmaken van elektronische zegels die gekoppeld zijn aan de valideringsgegevens voor elektronische zegels zich bevinden in een gekwalificeerd middel voor het aanmaken van elektronische zegels, een passende vermelding hiervan, minimaal in een vorm die geschikt is voor automatische verwerking.

BIJLAGE IV

Eisen voor gekwalificeerde certificaten voor website-authenticatie

Gekwalificeerde certificaten voor website-authenticatie moeten het navolgende bevatten:

- (a) een vermelding, minimaal in een vorm die geschikt is voor automatische verwerking, dat het certificaat is afgegeven als een gekwalificeerd certificaat voor website-authenticatie;
- (b) een reeks gegevens die op ondubbelzinnige wijze de gekwalificeerde verlener van vertrouwensdiensten aanduidt die de gekwalificeerde certificaten afgeeft, met inbegrip van ten minste de lidstaat waar die dienstverlener is gevestigd en
 - voor een rechtspersoon: naam en registratienummer zoals vermeld in de officiële registers,
 - voor een natuurlijk persoon: naam van de persoon;
- (c) een reeks gegevens die op ondubbelzinnige wijze de rechtspersoon aanduidt aan wie het certificaat is afgegeven, met inbegrip van ten minste de naam en het registratienummer zoals vermeld in de officiële registers;
- (d) elementen van het adres, met inbegrip van ten minste de plaats en de lidstaat, van de rechtspersoon aan wie het certificaat is afgegeven zoals vermeld in de officiële registers;
- (e) de domeinnaam/-namen die worden geëxploiteerd door de rechtspersoon aan wie het certificaat is afgegeven;
- (f) nadere informatie ten aanzien van het 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 valideringsstatus van het gekwalificeerde certificaat te raadplegen.

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

Dit financieel memorandum beschrijft de eisen met betrekking tot administratieve uitgaven voor de uitvoering van de voorgestelde verordening inzake *elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt*.

Aansluitend op de wetgevingsprocedure en het debat voor de goedkeuring door het Europees Parlement en de Raad van de voorgestelde verordening, heeft de Commissie twaalf VTE nodig om de daarmee verbonden gedelegeerde en uitvoeringshandelingen uit te werken, de beschikbaarheid van organisatorische en technische normen te waarborgen, de door de lidstaten gemelde informatie te verwerken, in het bijzonder de informatie met betrekking tot vertrouwenslijsten te beheren, ervoor te zorgen dat belanghebbenden – in het bijzonder burgers en kleine en middelgrote ondernemingen – zich bewust zijn van de voordelen van het gebruik van elektronische identificatie, authenticatie, handtekeningen en gerelateerde vertrouwensdiensten (eIAS) en om in gesprek te gaan met derde landen met het oog op het bereiken van eIAS-interoperabiliteit op mondiaal niveau.

1.1. Benaming van het voorstel/initiatief

Voorstel van de Commissie voor een verordening inzake elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt

1.2. Betrokken beleidsterrein(en) in de ABM/ABB-structuur²⁵

09 INFORMATIEMAATSCHAPPIJ

1.3. Aard van het voorstel/initiatief

- ☐ Het voorstel/initiatief betreft **een nieuwe actie**
- ☐ Het voorstel/initiatief betreft **een nieuwe actie na een proefproject/een voorbereidende actie**²⁶
- ☐ Het voorstel/initiatief betreft de **verlenging van een bestaande actie**
- ☒ Het voorstel/initiatief betreft **een actie die wordt omgebogen naar een nieuwe actie**

²⁵ ABM: activiteitsgestuurd management (Activity-Based Management) – ABB: activiteitsgestuurde begroting (Activity-Based Budgeting).

²⁶ Als bedoeld in artikel 49, lid 6, onder a) of b), van het Financieel Reglement.

1.4. Doelstellingen

1.4.1. *De met het voorstel/initiatief beoogde strategische meerjarendoelstelling(en) van de Commissie*

De algemene doelstellingen van het voorstel zijn die van de algemene EU-beleidsmaatregelen waarin het voorstel past, zoals de Europa 2020-strategie. Het heeft als doel van Europa "een slimme, duurzame en inclusieve economie [te maken] met een hoog niveau van werkgelegenheid, productiviteit en sociale cohesie."

1.4.2. *Specifieke doelstelling(en) en betrokken ABM/ABB-activiteit(en)*

Zorgen voor meer vertrouwen in pan-Europese elektronische transacties en het waarborgen van de grensoverschrijdende wettelijke erkenning van elektronische identificatie, authenticatie, handtekeningen en daarmee verband houdende vertrouwensdiensten, alsmede van een hoog niveau van gegevensbescherming en gebruikersbevoegdheden in de interne markt (zie de Digitale Agenda voor Europa, kernacties 3 en 16).

Betrokken ABM/ABB-activiteit(en)

09 02 - Regelgevingskader voor de digitale agenda voor Europa

1.4.3. *Verwachte resulta(a)t(en) en gevolg(en)*

Vermeld de gevolgen die het voorstel/initiatief zou moeten hebben op de beoogde begunstigden/doelgroepen.

Duidelijke regelgeving vaststellen voor eIAS-diensten die moeten leiden tot een aanzienlijke vergroting van het gebruiksgemak en vertrouwen in de digitale wereld.

1.4.4. *Resultaat- en effectindicatoren*

Vermeld de indicatoren aan de hand waarvan kan worden nagegaan in hoeverre het voorstel/initiatief is uitgevoerd.

1. Het bestaan van verleners van eIAS-diensten die activiteiten hebben in meerdere EU-lidstaten.
2. Mate waarin middelen interoperatieel worden (bijv. smartcard-lezers) tussen sectoren en landen.
3. Gebruik van eIAS door alle categorieën van de bevolking.
4. Mate waarin eIAS wordt gebruikt door eindgebruikers voor nationale en internationale (grensoverschrijdende) transacties.
5. Mate van harmonisatie van de eIAS-wetgeving tussen lidstaten.
6. Elektronische identificatieregelingen aangemeld bij de Commissie.
7. Diensten die beschikbaar zijn met aangemelde middelen voor elektronische identificatie in de overheidssector (bv. e-overheid, e-gezondheid, e-justitie, e-aanbesteding).

8. Diensten die beschikbaar zijn met aangemelde middelen voor elektronische identificatie in de particuliere sector (bv. onlinebankieren, e-handel, e-kansspelen, aanmelden bij websites, veiligere internetdiensten).

1.5. Motivering van het voorstel/initiatief

1.5.1. Behoeft(e)n waarin op korte of lange termijn moet worden voorzien

De uiteenlopende manieren waarop de lidstaten op nationaal niveau de richtlijnen inzake elektronische handtekeningen hebben uitgevoerd op grond van een verschillende interpretatie daarvan door de lidstaten leiden tot problemen voor de grensoverschrijdende interoperabiliteit en daardoor tot een gesegmenteerd EU-landschap en verstoringen van de interne markt. Dit gaat gepaard met een gebrek aan vertrouwen in elektronische systemen dat Europese burgers erin belemmert in de digitale wereld hun voordeel te doen met dezelfde soorten diensten als in de fysieke wereld.

1.5.2. Toegevoegde waarde van de betrokkenheid van de EU

Maatregelen op EU-niveau leveren duidelijke voordelen op in vergelijking met maatregelen op het niveau van de lidstaten. De ervaring heeft aangetoond dat nationale maatregelen niet alleen ontoereikend zijn om elektronische transacties over de grenzen heen mogelijk te maken, maar ze hebben zelfs barrières opgeworpen voor de EU-brede interoperabiliteit van elektronische handtekeningen, en de ervaring leert tevens dat ze momenteel hetzelfde effect hebben voor elektronische identificatie, elektronische authenticatie en daarmee verband houdende vertrouwensdiensten.

1.5.3. Lering getrokken uit soortgelijke ervaringen in het verleden

Het voorstel bouwt voort op de ervaringen die zijn opgedaan met de richtlijn inzake elektronische handtekeningen en de problemen die optraden vanwege de gefragmenteerde omzetting en uitvoering ervan, waardoor de doelstellingen van de richtlijn niet zijn bereikt.

1.5.4. Verenigbaarheid en eventuele synergie met andere relevante instrumenten

De richtlijn inzake elektronische handtekeningen houdt verband met verscheidene andere EU-initiatieven die zijn genomen om een einde te maken aan interoperabiliteitsproblemen, alsmede met kwesties op het gebied van grensoverschrijdende erkenning en aanvaarding voor bepaalde typen elektronische interacties, bijvoorbeeld de dienstenrichtlijn, de richtlijnen inzake overheidsopdrachten, de herziene btw-richtlijn (richtlijn inzake e-facturering) of de verordening over het burgerinitiatief.

Ook zorgt de voorgestelde verordening voor een rechtskader dat bevorderlijk is voor het ruime gebruik van de grootschalige proefprojecten (Large Scale Pilots - LSP's) die op EU-niveau zijn opgezet ter ondersteuning van de ontwikkeling van interoperabele en betrouwbare middelen voor elektronische communicatie (met inbegrip van SPOCS, ter ondersteuning van de uitvoering van de dienstenrichtlijn; STORK, ter ondersteuning van de ontwikkeling en het gebruik van interoperabele e-ID's; PEPPOL, ter ondersteuning van de ontwikkeling en het gebruik van

interoperabele oplossingen voor e-overheidsopdrachten; epSOS, ter ondersteuning van de ontwikkeling en het gebruik van interoperabele oplossingen voor e-gezondheidsdiensten; eCodex, ter ondersteuning van de ontwikkeling en het gebruik van interoperabele oplossingen voor e-justitie).

1.6. Duur en financiële gevolgen

- ☐ Voorstel/initiatief met een **beperkte geldigheidsduur**
 - ☐ Voorstel/initiatief is van kracht vanaf [DD/MM]JJJJ tot en met [DD/MM]JJJJ
 - ☐ Financiële gevolgen vanaf JJJJ tot en met JJJJ
- ☒ Voorstel/initiatief met een **onbeperkte geldigheidsduur**

1.7. Beoogde beheersvorm(en)²⁷

- ☒ **Direct gecentraliseerd beheer** door de Commissie
- ☐ **Gecentraliseerd indirect beheer** door delegatie van uitvoeringstaken aan:
 - ☐ uitvoerende agentschappen
 - ☐ door de Gemeenschappen opgerichte organen²⁸
 - ☐ nationale openbare organen of organen met een openbare dienstverleningstaak
 - ☐ personen aan wie de uitvoering van specifieke acties in het kader van titel V van het Verdrag betreffende de Europese Unie is toevertrouwd en die worden genoemd in het betrokken basisbesluit in de zin van artikel 49 van het Financieel Reglement
- ☐ **Gedeeld beheer** met lidstaten
- ☐ **Gedecentraliseerd beheer** met derde landen
- ☐ **Gezamenlijk beheer** met internationale organisaties (*geef aan welke*)

Verstrek, indien meer dan een beheersvorm is aangekruist, extra informatie onder "Opmerkingen".

Opmerkingen

[//]

²⁷ Nadere informatie over beheerswijzen en verwijzingen naar het Financieel Reglement zijn te vinden op de BudgWeb-site: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

²⁸ In de zin van artikel 185 van het Financieel Reglement.

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

Vermeld frequentie en voorwaarden.

De eerste evaluatie vindt plaats vier jaar na de inwerkingtreding van de verordening. De verordening bevat een uitdrukkelijke clausule over verslaglegging, op grond waarvan de Commissie verslag uit zal brengen aan het Europees Parlement en de Raad over de toepassing ervan. Hierna worden de verslagen eenmaal per vier jaar ingediend. De methodologie voor evaluaties van de Commissie zal worden toegepast. Deze evaluaties zullen worden uitgevoerd met behulp van gerichte onderzoeken naar de uitvoering van de rechtshandelingen, vragenlijsten voor nationale instanties, discussies met deskundigen, workshops, Eurobarometer-onderzoeken enz.

2.2. Beheers- en controlesysteem

2.2.1. Geconstateerde risico's

Een effectbeoordeling is uitgevoerd en aan het voorstel voor de verordening toegevoegd. De nieuwe rechtshandeling zal voorzien in wederzijdse erkenning en aanvaarding van elektronische identificatie over de grenzen heen, zorgen voor verbetering van het huidige kader voor elektronische handtekeningen, in het bijzonder door het nationale toezicht op verleners van vertrouwensdiensten te versterken, en voorzien in rechtsgevolgen en erkenning van gerelateerde vertrouwensdiensten. Hiermee wordt tevens het gebruik van gedelegeerde en uitvoeringshandelingen ingevoerd als een mechanisme om flexibiliteit ten aanzien van technologische ontwikkelingen te waarborgen.

2.2.2. Beoogde controlemiddel(en)

Bestaande door de Commissie toegepaste controlemethoden zullen voldoende zijn voor de controle van de aanvullende kredieten.

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

Vermeld de bestaande of geplande preventie- en beschermingsmaatregelen.

Bestaande door de Commissie toegepaste maatregelen ter voorkoming van fraude zullen voldoende zijn voor de controle van de aanvullende kredieten.

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarig financieel kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

- Bestaande begrotingsonderdelen voor uitgaven

In volgorde van de rubrieken van het meerjarig financieel kader en de begrotingsonderdelen.

Rubriek van het meerjarig financieel kader	Begrotingsonderdeel	Soort krediet	Bijdrage			
	Aantal [Beschrijving.....]	GK/ NGK ²⁹	van EVA-landen ³⁰	van kandidaat-lidstaten ³¹	van derde landen	in de zin van artikel 18, lid 1, onder a bis), van het Financieel Reglement
5	09. 01 01 01 Uitgaven voor personeel in actieve dienst in het DG "Informatiemaatschappij en media"	NGK	NEE	NEE	NEE	NEE
5	09. 01 02 01 Extern personeel	NGK	NEE	NEE	NEE	NEE

²⁹ GK = gesplitste kredieten/NGK = niet-gesplitste kredieten.

³⁰ EVA: Europese Vrijhandelsassociatie.

³¹ Kandidaat-lidstaten en, in voorkomend geval, potentiële kandidaat-lidstaten uit de Westelijke Balkan.

3.2. Geraamde gevolgen voor de uitgaven

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

Rubriek van het meerjarig financieel kader	Aantal	[Rubriek 1 Slimme en inclusieve groei]
---	--------	---

DG: INFSO			Jaar 2014	Jaar 2015	Jaar 2016	Jaar 2017	Jaar 2018	Jaar 2019	Jaar 2020	TOTAAL
• Beleidskredieten										
Nummer begrotingsonderdeel - nvt	Vastleggingen	(1)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
	Betalingen	(2)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Nummer begrotingsonderdeel - nvt	Vastleggingen	(1a)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
	Betalingen	(2a)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Administratieve kredieten gefinancierd uit het budget van specifieke programma's ³²			0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Nummer begrotingsonderdeel		(3)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
TOTAAL kredieten voor DG INFSO	Vastleggingen	=1+1a +3	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
	Betalingen	=2+2a +3	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000

³²

Technische en/of administratieve bijstand en uitgaven ter ondersteuning van de uitvoering van programma's en/of acties van de EU (vroegere "BA"-onderdelen), onderzoek door derden, eigen onderzoek.

Rubriek van het meerjarig financieel kader:	5	"Administratieve uitgaven"
--	----------	----------------------------

in miljoen euro (tot op 3 decimalen)

		Jaar 2014	Jaar 2015	Jaar 2016	Jaar 2017	Jaar 2018	Jaar 2019	Jaar 2020	TOTAAL
DG: INFSO									
• Personele middelen		1,344	1,344	1,344	1,344	1,344	1,344	1,344	9,408
• Andere administratieve uitgaven									
TOTAAL DG INFSO	Kredieten	1,344	1,344	1,344	1,344	1,344	1,344	1,344	9,408

TOTAAL kredieten voor RUBRIEK 5 van het meerjarig financieel kader	(Totaal vastleggingen = totaal betalingen)	1,344	1,344	1,344	1,344	1,344	1,344	1,344	9,408
---	---	-------	-------	-------	-------	-------	-------	-------	-------

in miljoen euro (tot op 3 decimalen)

		Jaar 2014	Jaar 2015	Jaar 2016	Jaar 2017	Jaar 2018	Jaar 2019	Jaar 2020	TOTAAL
TOTAAL kredieten voor RUBRIEK 1 tot en met 5 van het meerjarig financieel kader	Vastleggingen	1,344	1,344	1,344	1,344	1,344	1,344	1,344	9,408
	Betalingen	1,344	1,344	1,344	1,344	1,344	1,344	1,344	9,408

3.2.2. *Geraamde gevolgen voor de beleidskredieten*

- ☒ Voor het voorstel/initiatief zijn geen beleidskredieten nodig
- ☐ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

3.2.3. Geraamde gevolgen voor de administratieve kredieten

3.2.3.1. Samenvatting:

- ☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig
- ☒ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

in miljoen euro (tot op 3 decimalen)

	Jaar N 2014	Jaar 2015	Jaar 2016	Jaar 2017	Jaar 2018	Jaar 2019	Jaar 2020	TOTAAL
--	----------------	--------------	--------------	--------------	--------------	--------------	--------------	--------

RUBRIEK 5 van het meerjarig financieel kader								
Personele middelen	1,344	1,344	1,344	1,344	1,344	1,344	1,344	9,408
Andere administratieve uitgaven								
Subtotaal RUBRIEK 5 van het meerjarig financieel kader	1,344	1,344	1,344	1,344	1,344	1,344	1,344	9,408

Buiten RUBRIEK 5³³ van het meerjarig financieel kader								
Personele middelen								
Andere administratieve uitgaven								
Subtotaal buiten RUBRIEK 5 van het meerjarig financieel kader								

TOTAAL	1,344	1,344	1,344	1,344	1,344	1,344	1,344	9,408
---------------	-------	-------	-------	-------	-------	-------	-------	--------------

³³

Technische en/of administratieve bijstand en uitgaven ter ondersteuning van de uitvoering van programma's en/of acties van de EU (vroegere "BA"-onderdelen), onderzoek door derden, eigen onderzoek.

3.2.3.2. Geraamde personeelsbehoeften

- ☐ Voor het voorstel/initiatief zijn geen personele middelen nodig
- ☒ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader wordt beschreven:

Raming in een geheel getal (of met hoogstens 1 decimaal)

	Jaar 2014	Jaar 2015	Jaar 2016	Jaar 2017	Jaar 2018	Jaar 2019	Jaar 2020
• Formatieplaatsen (ambtenaren en tijdelijke functionarissen)							
09 01 01 01 (zetel en vertegenwoordigingen van de Commissie)	9	9	9	9	9	9	9
XX 01 01 02 (delegaties)							
XX 01 05 01 (onderzoek door derden)							
10 01 05 01 (eigen onderzoek)							
• Extern personeel (in voltijds equivalent: VTE)³⁴							
09 01 02 01 (AC, END, INT van de "totale financiële middelen")	3	3	3	3	3	3	3
XX 01 02 02 (AC, AL, END, INT en JED in de delegaties)							
XX 01 04 <i>jj</i> ³⁵	- zetel ³⁶						
	- in delegaties						
XX 01 05 02 (AC, END, INT - onderzoek door derden)							
10 01 05 02 (AC, END, INT – eigen onderzoek)							
Andere begrotingsonderdelen (te vermelden)							
TOTAAL	12	12	12	12	12	12	12

De benodigde personele middelen zullen worden gefinancierd uit de middelen die reeds voor het beheer van deze actie zijn toegewezen en/of binnen het DG zijn herverdeeld, eventueel aangevuld met middelen die in het kader van de jaarlijkse toewijzingsprocedure met inachtneming van de budgettaire beperkingen aan het beherende DG kunnen worden toegewezen.

Beschrijving van de uit te voeren taken:

Ambtenaren en tijdelijke functionarissen	Beheer van de wetgevingsprocedures voor de goedkeuring door het Europees Parlement en de Raad van de geplande verordening en daarmee verband houdende gedelegeerde en uitvoeringshandelingen. Prioritaire gebieden: 1. Vaststelling van een nieuw regelgevingskader inzake elektronische vertrouwensdiensten. 2. Bevordering van het gebruik van elektronische vertrouwensdiensten door het
--	--

³⁴ AC = arbeidscontractant; INT= uitzendkracht; JED= "Jeune Expert en Délégation" (jonge deskundige in delegatie); LA= plaatselijke functionaris; END = gedetacheerd nationaal deskundige.

³⁵ Onder het maximum voor extern personeel uit beleidskredieten (vroegere "BA"-onderdelen).

³⁶ Vooral voor structuurfondsen, Europees Landbouwfonds voor plattelandontwikkeling (ELFPO) en Europees Visserijfonds (EVF).

	bewustzijn van kmo's/mkb-bedrijven en burgers omtrent de mogelijkheden ervan te vergroten. 3. Follow-up van Richtlijn 1999/93/EG, onder meer wat betreft internationale aspecten. 4. Benutting van de ervaringen met de grootschalige proefprojecten met het oog op een snellere concrete totstandbrenging van het doel van het nieuwe regelgevingskader.
Extern personeel	Zie hierboven

3.2.4. *Verenigbaarheid met het huidige meerjarig financieel kader*

- ☒ Het voorstel/initiatief is verenigbaar met het huidige meerjarig financieel kader.
- ☐ Het voorstel/initiatief vergt herprogrammering van de betrokken rubriek van het meerjarig financieel kader.

Zet uiteen welke herprogrammering nodig is, onder vermelding van de betrokken begrotingsonderdelen en de desbetreffende bedragen.

- ☐ Het voorstel/initiatief vergt toepassing van het flexibiliteitsinstrument of herziening van het meerjarig financieel kader³⁷.

Zet uiteen wat nodig is, onder vermelding van de betrokken rubrieken en begrotingsonderdelen en de desbetreffende bedragen.

3.2.5. *Bijdragen van derden*

- ☒ Het voorstel/initiatief voorziet niet in medefinanciering door derden.
- ☐ Het voorstel/initiatief voorziet in medefinanciering, zoals hieronder wordt geraamd:

3.3. **Geraamde gevolgen voor de ontvangsten**

- ☒ Het voorstel/initiatief heeft geen financiële gevolgen voor de ontvangsten.
- ☐ Het voorstel/initiatief heeft de hieronder beschreven financiële gevolgen:
 - ☐ voor de eigen middelen
 - ☐ voor de diverse ontvangsten

³⁷

Zie de punten 19 en 24 van het Interinstitutioneel Akkoord.