28.8.2014 | FR | Journal officiel de l'Union européenne | L 257/73

RÈGLEMENT (UE) No 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 23 juillet 2014

sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen (1),

statuant conformément à la procédure législative ordinaire (2),

considérant ce qui suit:

(1) | Instaurer un climat de confiance dans l'environnement en ligne est essentiel au développement économique et social. En effet, si les consommateurs, les entreprises et les autorités publiques n'ont pas confiance, notamment en raison d'un sentiment d'insécurité juridique, ils hésiteront à effectuer des transactions par voie électronique et à adopter de nouveaux services.

(2) | Le présent règlement vise à susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur en fournissant un socle commun pour des interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques et en accroissant ainsi l'efficacité des services en ligne publics et privés, ainsi que de l'activité économique et du commerce électronique dans l'Union.

(3) | La directive 1999/93/CE du Parlement européen et du Conseil (3) régissait les signatures électroniques sans fournir de cadre transfrontalier et intersectoriel complet pour des transactions électroniques sécurisées, fiables et aisées à utiliser. Le présent règlement renforce et développe l'acquis que représente ladite directive.

(4) | Dans sa communication du 26 août 2010 intitulée «Une stratégie numérique pour l'Europe», la Commission a identifié la fragmentation du marché numérique, le manque d'interopérabilité et l'augmentation de la cybercriminalité comme les principaux obstacles au cercle vertueux de l'économie numérique. Dans son rapport 2010 sur la citoyenneté de l'Union, intitulé «Lever les obstacles à l'exercice des droits des citoyens de l'Union», la Commission a également souligné la nécessité de résoudre les principaux problèmes empêchant les citoyens de l'Union de profiter des avantages d'un marché unique numérique et des services numériques transfrontaliers.

(5) | Dans ses conclusions du 4 février 2011 et du 23 octobre 2011, le Conseil européen a invité la Commission à créer un marché unique numérique d'ici à 2015, à progresser rapidement dans les domaines clés de l'économie numérique et à favoriser la mise en place d'un marché unique numérique pleinement intégré en facilitant l'utilisation transfrontalière de services en ligne et, en particulier, l'identification et l'authentification électroniques sécurisées.

(6) | Dans ses conclusions du 27 mai 2011, le Conseil a invité la Commission à contribuer à la mise en place du marché unique numérique en créant les conditions appropriées pour la reconnaissance mutuelle des outils clés entre les pays, tels que l'identification électronique, les documents électroniques, les signatures électroniques et les

28.8.2014 | NL | Publicatieblad van de Europese Unie | L 257/73

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

van 23 juli 2014

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

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

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

Gezien het voorstel van de Europese Commissie,

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

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

Handelend volgens de gewone wetgevingsprocedure (2),

Overwegende hetgeen volgt:

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

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

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

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

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

(6) | In zijn conclusies van 27 mei 2011 heeft de Raad de Commissie verzocht bij te dragen tot de digitale interne markt door de juiste voorwaarden te scheppen voor de wederzijdse erkenning van cruciale mogelijkheden scheppende voorzieningen over de grenzen heen, zoals elektronische identificatie, elektronische documenten,

au point de services interopérables d'administration en ligne dans toute l'Union européenne.

(7) | Le Parlement européen, dans sa résolution du 21 septembre 2010 sur l'achèvement du marché intérieur pour ce qui concerne le commerce en ligne (4), a souligné l'importance de la sécurité des services électroniques, en particulier des signatures électroniques, et la nécessité de créer une infrastructure clé publique au niveau paneuropéen, et il a invité la Commission à mettre en place un portail des autorités européennes de validation afin d'assurer l'interopérabilité transfrontalière des signatures électroniques et d'accroître la sécurité des transactions réalisées au moyen de l'internet.

(8) | La directive 2006/123/CE du Parlement européen et du Conseil (5) exige des États membres qu'ils créent des guichets uniques pour que toutes les procédures et formalités relatives à l'accès à une activité de service et à son exercice puissent être effectuées facilement, à distance et par voie électronique, par l'intermédiaire du guichet unique approprié, auprès des autorités compétentes. Or, de nombreux services en ligne accessibles par guichet unique exigent une identification, une authentification et une signature électroniques.

(9) | Dans la plupart des cas, les citoyens ne peuvent pas utiliser leur identification électronique pour s'authentifier dans un autre État membre parce que les schémas nationaux d'identification électronique de leur pays ne sont pas reconnus dans d'autres États membres. Cet obstacle numérique empêche les prestataires de services de tirer tous les bénéfices du marché intérieur. La reconnaissance mutuelle des moyens d'identification électronique facilitera la fourniture transfrontalière de nombreux services dans le marché intérieur et permettra aux entreprises de mener des activités transfrontalières sans faire face à de nombreux obstacles dans leurs relations avec les pouvoirs publics.

(10) | La directive 2011/24/UE du Parlement européen et du Conseil (6) instaure un réseau d'autorités nationales chargées de la santé en ligne. Pour assurer la sécurité et la continuité des soins de santé transfrontaliers, ce réseau est tenu d'établir des orientations concernant l'accès transfrontalier aux données et services électroniques de santé, y compris en soutenant des «mesures communes d'identification et d'authentification, afin de faciliter la transférabilité des données dans le cadre de soins de santé transfrontaliers». La reconnaissance mutuelle de l'identification et de l'authentification électroniques est essentielle pour que les soins de santé transfrontaliers deviennent une réalité pour les citoyens européens. Lorsque ces derniers se déplacent pour subir un traitement, il faut que leurs données médicales soient accessibles dans le pays où les soins sont dispensés. Cela exige un cadre solide, sûr et fiable en matière d'identification électronique.

(11) | Le présent règlement devrait être appliqué dans le respect total des principes relatifs à la protection des données à caractère personnel prévus dans la directive 95/46/CE du Parlement européen et du Conseil (7). À cet égard, compte tenu du principe de la reconnaissance mutuelle établi par le présent règlement, l'authentification pour un service en ligne ne devrait concerner que le traitement des données d'identification qui sont adéquates, pertinentes et non excessives afin de permettre l'accès audit service en ligne. En outre, il y a lieu que les prestataires de services de confiance et les organes de contrôle satisfassent aux exigences de confidentialité et de sécurité des traitements imposées par la directive 95/46/CE.

(12) | Un des objectifs du présent règlement est de lever les obstacles existants à l'utilisation transfrontalière des moyens d'identification électronique employés dans les États membres pour s'identifier, au moins pour les services publics. Le présent règlement ne vise pas à intervenir en ce qui concerne les systèmes de gestion de l'identité électronique et les infrastructures associées établis dans les États membres. Le présent règlement a pour but de s'assurer que, concernant l'accès aux services en ligne transfrontaliers proposés par les États membres, l'identification et l'authentification électroniques sécurisées sont possibles.

leveringsdiensten en voor interoperabele e-overheidsdiensten in de gehele EU.

(7) | In zijn resolutie van 21 september 2010 over de voltooiing van de interne markt voor e-handel (4) heeft het Europees Parlement het belang onderstreept van de veiligheid van elektronische diensten, vooral van elektronische handtekeningen, en van de noodzaak om een publieke sleutelinfrastructuur op pan-Europees niveau te creëren, en heeft de Commissie verzocht een toegangspoort voor Europese valideringsinstanties op te zetten om de grensoverschrijdende interoperabiliteit van elektronische handtekeningen te waarborgen en de veiligheid van transacties via internet te verhogen.

(8) | Bij Richtlijn 2006/123/EG van het Europees Parlement en de Raad (5) wordt van de lidstaten vereist dat zij „één-loketten" opzetten zodat alle procedures en formaliteiten betreffende de toegang tot en de uitoefening van een dienstenactiviteit eenvoudig, op afstand en met elektronische middelen, via het juiste één-loket en met de juiste instanties kunnen worden afgewikkeld. Veel onlinediensten die via één-loketten toegankelijk zijn, vergen elektronische identificatie, authenticatie en een elektronische handtekening.

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

(10) | In Richtlijn 2011/24/EU van het Europees Parlement en de Raad (6) wordt een netwerk van voor e-gezondheid verantwoordelijke nationale autoriteiten opgezet. Om de veiligheid en de continuïteit van grensoverschrijdende gezondheidszorg te verbeteren, moet het netwerk richtsnoeren opstellen voor de grensoverschrijdende toegang tot elektronische gezondheidsgegevens en -diensten, ook door het ondersteunen van „gemeenschappelijke identificatie- en authenticatiemaatregelen, teneinde de overdraagbaarheid van gegevens bij grensoverschrijdende gezondheidszorg te bevorderen". De wederzijdse erkenning van elektronische identificatie en authenticatie is essentieel om voor de Europese burger grensoverschrijdende gezondheidszorg realiteit te maken. Wanneer mensen voor een behandeling naar het buitenland reizen, moeten hun medische gegevens in het land van behandeling toegankelijk zijn. Dat vergt een degelijk, veilig en betrouwbaar kader voor elektronische identificatie.

(11) | Deze verordening dient te worden toegepast in volledige overeenstemming met de beginselen inzake de bescherming van persoonsgegevens overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad (7). In dit verband en met inachtneming van het bij deze verordening vastgelegde beginsel inzake wederzijdse erkenning, mag authenticatie voor een onlinedienst alleen betrekking hebben op de verwerking van die identificatiegegevens die toereikend, ter zake dienend en niet bovenmatig zijn om toegang tot die onlinedienst te verlenen. Voorts moeten de in Richtlijn 95/46/EG gestelde eisen inzake vertrouwelijkheid en beveiliging van de verwerking worden geëerbiedigd door de verleners van vertrouwensdiensten en het toezichthoudend orgaan.

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

ne devraient pas être tenus de notifier leurs schémas d'identification électronique à la Commission. Il appartient aux États membres de choisir de notifier à la Commission la totalité ou une partie, ou de ne notifier aucun des schémas d'identification électronique utilisés au niveau national pour accéder, au moins, aux services publics en ligne ou à des services spécifiques.

(14) | Il convient de fixer dans le présent règlement certaines conditions, en ce qui concerne les moyens d'identification électronique qui doivent être reconnus et la façon dont les schémas d'identification électronique devraient être notifiés. Ces conditions devraient permettre aux États membres de susciter la confiance nécessaire dans leurs schémas d'identification électronique respectifs et faciliter la reconnaissance mutuelle des moyens d'identification électronique relevant de leurs schémas notifiés. Le principe de la reconnaissance mutuelle devrait s'appliquer si le schéma d'identification électronique de l'État membre notifiant remplit les conditions de notification et si la notification a été publiée au Journal officiel de l'Union européenne. Toutefois, le principe de la reconnaissance mutuelle ne devrait concerner que l'authentification pour un service en ligne. L'accès à ces services en ligne et leur fourniture finale au demandeur devraient être étroitement liés au droit de recevoir de tels services dans les conditions fixées par la législation nationale.

(15) | L'obligation de reconnaître des moyens d'identification électronique devrait se rapporter uniquement aux moyens dont le niveau de garantie de l'identité correspond à un niveau égal ou supérieur au niveau requis pour le service en ligne en question. En outre, cette obligation ne devrait s'appliquer que lorsque l'organisme du secteur public en question utilise le niveau de garantie «substantiel» ou «élevé» en rapport avec l'accès audit service en ligne. Les États membres devraient demeurer libres, conformément au droit de l'Union, de reconnaître des moyens d'identification électronique disposant d'un niveau inférieur de garantie de l'identité.

(16) | Les niveaux de garantie devraient caractériser le niveau de fiabilité d'un moyen d'identification électronique pour établir l'identité d'une personne, garantissant ainsi que la personne revendiquant une identité particulière est bien la personne à laquelle cette identité a été attribuée. Le niveau de garantie dépend du niveau de fiabilité que le moyen d'identification électronique accorde à l'identité revendiquée ou prétendue d'une personne en tenant compte des processus (par exemple, preuve et vérification d'identité, et authentification), des activités de gestion (par exemple, l'entité délivrant les moyens d'identification et la procédure de délivrance de ces moyens) et contrôles techniques mis en œuvres. Il existe diverses définitions techniques et des descriptions des niveaux de garantie à la suite de projets pilotes à grande échelle financés au niveau de l'Union, d'activités internationales et de normalisation. En particulier, le projet pilote à grande échelle STORK et la norme ISO 29115 mentionnent, entre autres, les niveaux 2, 3 et 4 qui devraient être pris scrupuleusement en compte pour établir les exigences techniques, les normes et les procédures minimales pour les niveaux de garantie faible, substantiel et élevé au sens du présent règlement, tout en garantissant une application cohérente du présent règlement, en particulier en ce qui concerne le niveau élevé de garantie pour la preuve de l'identité en vue de la délivrance de certificats qualifiés. Les exigences établies devraient être neutres du point de vue de la technologie. Il devrait être possible de répondre aux exigences de sécurité au moyen de différentes technologies.

betrekken. De lidstaten dienen niet te worden verplicht hun stelsels voor elektronische identificatie aan de Commissie te melden. Het staat de lidstaten vrij om alle, sommige dan wel geen van de stelsels voor elektronische identificatie die op nationaal niveau worden gebruikt om ten minste toegang te krijgen tot publieke onlinediensten of specifieke diensten, aan de Commissie te melden.

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

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

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

(17) | Les États membres devraient encourager le secteur privé à utiliser, sur une base volontaire, aux fins de l'identification exigée par des services en ligne ou des transactions électroniques, les moyens d'identification électronique relevant d'un schéma notifié. La possibilité

(17) | De lidstaten dienen de private sector aan te moedigen vrijwillig gebruik te maken van elektronische identificatiemiddelen die onder een aangemeld stelsel vallen, indien identificatie bij onlinediensten of elektronische transacties nodig is. De mogelijkheid om

secteur privé établies en dehors du territoire de cet État membre aux mêmes conditions que celles qui sont appliquées aux parties utilisatrices du secteur privé établies sur le territoire dudit État membre. Dès lors, en ce qui concerne les parties utilisatrices du secteur privé, l'État membre notifiant peut définir des conditions d'accès aux moyens d'authentification. Ces conditions d'accès peuvent indiquer si le moyen d'authentification relatif au schéma notifié est actuellement accessible aux parties utilisatrices du secteur privé.

(18) | Le présent règlement devrait prévoir la responsabilité de l'État membre notifiant, de la partie qui délivre le moyen d'identification électronique et de la partie qui gère la procédure d'authentification en cas de manquement aux obligations pertinentes au titre du présent règlement. Le présent règlement devrait cependant s'appliquer conformément aux dispositions nationales en matière de responsabilité. Il n'affecte donc pas ces règles nationales, par exemple, celles relatives à la définition des dommages ou aux règles procédurales applicables en la matière, y compris à la charge de la preuve.

(19) | La sécurité des schémas d'identification électronique est la clé pour assurer la fiabilité de la reconnaissance mutuelle transfrontalière des moyens d'identification électronique. Dans ce cadre, les États membres devraient coopérer pour ce qui est de la sécurité et de l'interopérabilité des schémas d'identification électronique au niveau de l'Union. Chaque fois qu'un schéma d'identification électronique exige des parties utilisatrices qu'elles utilisent un matériel ou un logiciel particulier au niveau national, l'interopérabilité transfrontalière requiert que ces États membres n'imposent pas cette exigence et les coûts qui y sont associés aux parties utilisatrices établies en dehors de leur territoire. Dans ce cas, il y a lieu d'envisager et d'élaborer des solutions appropriées dans les limites du cadre d'interopérabilité. Néanmoins, des exigences techniques découlant des spécifications inhérentes aux moyens nationaux d'identification électronique et susceptibles d'affecter les détenteurs de tels moyens électroniques (les cartes à puce, par exemple) sont inévitables.

(20) | La coopération des États membres devrait faciliter l'interopérabilité technique des schémas d'identification électronique notifiés en vue de promouvoir un niveau élevé de confiance et de sécurité, adapté au degré de risque. L'échange d'informations et le partage des bonnes pratiques entre les États membres en vue de leur reconnaissance mutuelle devraient faciliter une telle coopération.

(21) | Le présent règlement devrait aussi instaurer un cadre juridique général concernant l'utilisation de services de confiance. Toutefois, il ne devrait pas imposer d'obligation générale d'y recourir ou d'installer un point d'accès pour tous les services de confiance existants. En particulier, il ne devrait pas couvrir la fourniture de services utilisés exclusivement dans des systèmes fermés au sein d'un ensemble défini de participants, qui n'ont pas d'effets sur des tiers. Par exemple, les systèmes institués par des entreprises ou des administrations publiques pour gérer les procédures internes et utilisant des services de confiance ne devraient pas être soumis aux exigences du présent règlement. Seuls les services de confiance fournis au public ayant des effets sur les tiers devraient remplir les exigences du présent règlement. Le présent règlement ne devrait pas couvrir non plus les aspects relatifs à la conclusion et à la validité des contrats ou autres obligations juridiques lorsque des exigences d'ordre formel sont posées par le droit national ou de l'Union. En outre, il ne devrait pas porter atteinte à des exigences d'ordre formel imposées au niveau national aux registres publics, notamment les registres du commerce et les registres fonciers.

(22) | Afin de contribuer à l'utilisation transfrontalière généralisée des services de confiance, il devrait être possible de les utiliser comme moyen de preuve en justice dans tous les États membres. Il appartient au droit national de préciser les effets juridiques des services de confiance, sauf disposition contraire dans le présent règlement.

biedt, beschikbaar zijn voor buiten het grondgebied van die lidstaat gevestigde vertrouwende partijen uit de private sector, en wel onder dezelfde voorwaarden als in die lidstaat gevestigde vertrouwende partijen. Bijgevolg mag de aanmeldende lidstaat ten aanzien van vertrouwende partijen uit de private sector voorwaarden voor toegang tot de authenticatiemiddelen bepalen. Die voorwaarden voor toegang kunnen vermelden of de authenticatiemiddelen voor het aangemelde stelsel voor elektronische identificatie op dat moment beschikbaar zijn voor vertrouwende partijen uit de private sector.

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

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

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

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

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

raisons techniques qui échappent au contrôle immédiat du destinataire. Toutefois, cette obligation de reconnaissance ne devrait pas imposer, par elle-même, à un organisme public qu'il se dote du matériel ou du logiciel nécessaire afin d'assurer la lisibilité technique de tous les services de confiance existants.

(24) | Les États membres peuvent conserver ou instaurer des dispositions nationales, conformes au droit de l'Union, ayant trait aux services de confiance, pour autant que ces services ne soient pas complètement harmonisés par le présent règlement. Cependant, les services de confiance qui sont conformes au présent règlement devraient pouvoir circuler librement au sein du marché intérieur.

(25) | Les États membres devraient rester libres de définir d'autres types de services de confiance, en plus de ceux qui figurent sur la liste fermée des services de confiance prévus par le présent règlement, aux fins de leur reconnaissance au niveau national comme des services de confiance qualifiés.

(26) | Vu la rapidité de l'évolution technologique, le présent règlement devrait consacrer une approche qui soit ouverte aux innovations.

(27) | Le présent règlement devrait être neutre du point de vue de la technologie. Les effets juridiques qu'il confère devraient pouvoir être obtenus par tout moyen technique, pour autant que les exigences posées par le présent règlement soient satisfaites.

(28) | Pour accroître, en particulier, la confiance des petites et moyennes entreprises (PME) et des consommateurs dans le marché intérieur et pour promouvoir l'utilisation des services et produits de confiance, les notions de service de confiance qualifié et de prestataire de services de confiance qualifié devraient être introduites en vue de définir les exigences et obligations qui assurent un niveau élevé de sécurité de tous les services et produits de confiance qualifiés qui sont utilisés ou fournis.

(29) | Conformément aux obligations découlant de la convention des Nations unies relative aux droits des personnes handicapées, qui a été approuvée par la décision 2010/48/CE du Conseil (8), et notamment à l'article 9 de la convention, les personnes handicapées devraient pouvoir utiliser les services de confiance, ainsi que les produits destinés à l'utilisateur final qui servent à fournir ces services, dans les mêmes conditions que les autres consommateurs. Les services de confiance fournis, ainsi que les produits destinés à l'utilisateur final qui servent à fournir ces services, devraient donc être rendus accessibles aux personnes handicapées, dans la mesure du possible. L'évaluation de la faisabilité devrait inclure, entre autres, des considérations d'ordre technique et économique.

(30) | Il convient que les États membres désignent un ou des organes de contrôle chargés d'exécuter les activités de contrôle en application du présent règlement. Les États membres devraient également pouvoir décider, d'un commun accord avec un autre État membre, de désigner un organe de contrôle sur le territoire de cet autre État membre.

(31) | Les organes de contrôle devraient coopérer avec les autorités chargées de la protection des données, par exemple en les informant des résultats des audits des prestataires de services de confiance qualifiés, lorsqu'il apparaît que des règles en matière de protection des données à caractère personnel ont été violées. Cette fourniture d'informations devrait, notamment, porter sur les incidents liés à la sécurité et aux atteintes aux données à caractère personnel.

(32) | Il devrait incomber à tous les prestataires de services de confiance d'appliquer de bonnes pratiques de sécurité, adaptées aux risques inhérents à leurs activités, afin d'accroître la confiance des utilisateurs dans le marché unique.

(33) | Les dispositions relatives à l'utilisation de pseudonymes dans des certificats ne devraient pas empêcher les États membres d'exiger l'identification des personnes en vertu du droit national ou du droit de l'Union.

(34) | Tous les États membres devraient satisfaire à des exigences essentielles communes de contrôle afin d'assurer un niveau de sécurité comparable en matière de services de confiance qualifiés. Pour faciliter l'application cohérente de ces exigences dans l'Union, les États membres devraient adopter des procédures comparables et échanger des informations sur leurs activités de contrôle et les meilleures pratiques dans ce domaine.

technische redenen, waarop hij geen rechtstreekse invloed kan uitoefenen, niet kan lezen of verifiëren. Die verplichting hoeft evenwel op zich niet te betekenen dat een openbare instantie de voor de technische leesbaarheid van alle bestaande vertrouwensdiensten benodigde hardware en software moet verwerven.

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

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

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

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

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

(29) | In overeenstemming met de verplichtingen van het Verdrag van de Verenigde Naties inzake de rechten van personen met een handicap, goedgekeurd door Besluit 2010/48/EG van de Raad (8), in het bijzonder artikel 9 van dat verdrag, moeten personen met een handicap in staat zijn de geleverde vertrouwensdiensten en de producten voor de eindgebruiker die bij het leveren van deze diensten gebruikt worden, op gelijke voet als andere consumenten te gebruiken. Daarom moeten, waar dat haalbaar is, vertrouwensdiensten en eindgebruikersproducten die worden gebruikt bij de verlening van deze diensten toegankelijk worden gemaakt voor personen met een handicap. De haalbaarheidsbeoordeling moet onder andere op technische en economische overwegingen gebaseerd zijn.

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

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

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

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

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

(35) | Tous les prestataires de services de confiance devraient être soumis aux exigences du présent règlement, notamment en matière de sécurité et de responsabilité, pour assurer une diligence appropriée, la transparence et la responsabilité quant à leurs activités et à leurs services. Toutefois, eu égard au type de services fournis par les prestataires de services de confiance, il y a lieu de faire une distinction, au niveau de ces exigences, entre, d'une part, les prestataires de services de confiance qualifiés et, d'autre part, les prestataires de services de confiance non qualifiés.

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

(36) | La mise en place d'un régime de contrôle pour tous les prestataires de services de confiance devrait assurer des conditions de concurrence équitables pour ce qui est de la sécurité et de la responsabilité quant à leurs activités et à leurs services et contribuer ainsi à la protection des utilisateurs et au fonctionnement du marché intérieur. Les prestataires de services de confiance non qualifiés devraient être soumis à un contrôle a posteriori allégé et réactif justifié par la nature de leurs services et activités. L'organe de contrôle devrait dès lors ne pas avoir d'obligation générale de contrôler des prestataires de services non qualifiés. L'organe de contrôle ne devrait intervenir que lorsqu'il est informé (par exemple, par le prestataire de services de confiance non qualifié lui-même, par un autre organe de contrôle, par une notification émanant d'un utilisateur ou d'un partenaire économique ou sur la base de ses propres investigations) qu'un prestataire de services de confiance non qualifié ne satisfait pas aux exigences du présent règlement.

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

(37) | Le présent règlement devrait prévoir que tous les prestataires de services de confiance engagent leur responsabilité. Il établit notamment le régime de responsabilité en vertu duquel tous les prestataires de services de confiance devraient être responsables des dommages causés à toute personne physique ou morale en raison d'un manquement aux obligations prévues par le présent règlement. Afin de faciliter l'évaluation du risque financier que les prestataires de services de confiance pourraient devoir supporter ou qu'ils devraient couvrir au moyen d'une police d'assurance, le présent règlement les autorise à fixer des limites, sous certaines conditions, à l'utilisation des services qu'ils proposent et à ne pas être tenus pour responsables des dommages résultant de l'utilisation de services allant au-delà de ces limites. Les clients devraient être dûment informés à l'avance des limites fixées. Ces limites devraient être reconnaissables par un tiers, par exemple par l'insertion d'une notice relative à ces limites dans les conditions applicables au service fourni ou par d'autres moyens reconnaissables. Afin de donner effet à ces principes, il convient que le présent règlement s'applique conformément aux règles nationales en matière de responsabilité. Le présent règlement n'affecte donc pas ces règles nationales, par exemple celles relatives à la définition des dommages, au caractère intentionnel ou à la négligence, ou les règles procédurales applicables en la matière.

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

(38) | La notification des atteintes à la sécurité et des analyses des risques en matière de sécurité sont essentielles pour que des informations adéquates puissent être fournies aux parties concernées en cas d'atteinte à la sécurité ou de perte d'intégrité.

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

(39) | Pour permettre à la Commission et aux États membres d'évaluer l'efficacité du mécanisme de notification des atteintes à la sécurité instauré par le présent règlement, il devrait être demandé aux organes de contrôle de fournir des informations succinctes à la Commission et à l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA).

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

(40) | Pour permettre à la Commission et aux États membres d'évaluer l'efficacité du mécanisme de contrôle renforcé instauré par le présent règlement, il devrait être demandé aux organes de contrôle de rendre compte de leurs activités. Cela serait déterminant pour faciliter l'échange de bonnes pratiques entre les organes de contrôle et permettrait de vérifier la mise en œuvre cohérente et efficace des exigences de contrôle essentielles dans tous les États membres.

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

(41) | Pour assurer la pérennité et la durabilité des services de confiance qualifiés et pour accroître la confiance des utilisateurs dans la continuité de ces services, les organes de contrôle devraient vérifier l'existence et l'application

(41) | Om de duurzaamheid van gekwalificeerde vertrouwensdiensten te waarborgen en het vertrouwen van de gebruikers in de continuïteit van gekwalificeerde vertrouwensdiensten te stimuleren, moeten de

qualifiés cessent leurs activités.

activiteiten beëindigen, nagaan of er maatregelen betreffende beëindigingsplannen bestaan en of die correct worden toegepast.

(42) | Pour faciliter le contrôle des prestataires de services de confiance qualifiés, par exemple lorsqu'un prestataire fournit ses services sur le territoire d'un autre État membre dans lequel il n'est soumis à aucun contrôle ou lorsque les ordinateurs d'un prestataire sont situés sur le territoire d'un État membre autre que celui où il est établi, il convient que soit instauré un système d'assistance mutuelle entre les organes de contrôle des États membres.

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

(43) | Afin d'assurer le respect des exigences énoncées dans le présent règlement par les prestataires de services de confiance qualifiés et les services qu'ils fournissent, une évaluation de la conformité devrait être effectuée par un organisme d'évaluation de la conformité, et les rapports d'évaluation de la conformité qui en résultent devraient être soumis par les prestataires de services de confiance qualifiés à l'organisme de contrôle. Lorsqu'il exige qu'un prestataire de services de confiance qualifié lui soumette un rapport spécifique d'évaluation de la conformité, il convient que l'organe de contrôle applique, notamment, les principes de bonne administration, y compris l'obligation de motiver ses décisions, ainsi que le principe de proportionnalité. Par conséquent, l'organe de contrôle devrait dûment justifier sa décision d'exiger une évaluation spécifique de la conformité.

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

(44) | Le présent règlement vise à établir un cadre cohérent en vue de fournir des services de confiance d'un niveau de sécurité et de sécurité juridique élevé. À cet égard, lorsqu'elle aborde la question de l'évaluation de la conformité de produits et de services, la Commission devrait, le cas échéant, rechercher des synergies avec des schémas européens et internationaux pertinents existants, tels que le règlement (CE) no 765/2008 du Parlement européen et du Conseil (9), qui fixe les exigences relatives à l'accréditation d'organismes d'évaluation de la conformité et à la surveillance du marché de produits.

(44) | Deze verordening heeft tot doel te zorgen voor een samenhangend kader dat met betrekking tot vertrouwensdiensten in een hoog niveau van veiligheid en rechtszekerheid voorziet. In dit verband moet de Commissie, met betrekking tot de conformiteitsbeoordeling van producten en diensten, in voorkomend geval streven naar synergie met bestaande toepasselijke Europese en internationale systemen zoals Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad (9) waarin de eisen inzake accreditatie van conformiteitsbeoordelingsorganen en markttoezicht op producten worden opgesomd.

(45) | Afin de permettre un processus de lancement efficace, qui devrait conduire à l'inscription de prestataires de services de confiance qualifiés et des services de confiance qualifiés qu'ils fournissent sur des listes de confiance, il faudrait encourager des échanges préliminaires entre des prestataires de services de confiance qualifiés potentiels et l'organe de contrôle compétent en vue de faciliter les vérifications préalables à la fourniture de services de confiance qualifiés.

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

(46) | Les listes de confiance sont des éléments essentiels pour fonder la confiance des opérateurs économiques, car elles indiquent le statut qualifié du prestataire de service au moment du contrôle.

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

(47) | La confiance dans les services en ligne et leur commodité sont essentiels pour que les utilisateurs tirent pleinement avantage des services électroniques et qu'ils s'y fient en connaissance de cause. À cet effet, un label de confiance de l'Union devrait être créé pour identifier les services de confiance qualifiés fournis par des prestataires de services de confiance qualifiés. Un tel label de confiance de l'Union distinguerait clairement les services de confiance qualifiés d'autres services de confiance, contribuant ainsi à la transparence du marché. L'utilisation d'un label de confiance de l'Union par les prestataires de services de confiance qualifiés devrait se faire sur une base volontaire et ne devrait pas entraîner d'autres exigences que celles prévues dans le présent règlement.

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

(48) | Un niveau de sécurité élevé est nécessaire pour garantir la reconnaissance mutuelle des signatures électroniques, mais, dans certains cas particuliers, comme dans le contexte de la décision 2009/767/CE de la Commission (10), des signatures électroniques offrant une garantie de sécurité moindre devraient également être acceptées.

(48) | Hoewel een hoog beveiligingsniveau nodig is om de wederzijdse erkenning van elektronische handtekeningen te waarborgen, moeten in specifieke gevallen, zoals in het kader van Beschikking 2009/767/EG van de Commissie (10), elektronische handtekeningen met een lagere veiligheidsgarantie ook aanvaard worden.

(49) | Le présent règlement devrait établir le principe selon lequel une signature électronique ne devrait pas se voir refuser un effet juridique au motif qu'elle se présente sous

(49) | In deze verordening moet als beginsel worden gesteld dat het rechtsgevolg van een elektronische handtekening niet moet worden ontkend op grond van het feit dat de

l'exception de l'exigence prévue dans le présent règlement selon laquelle l'effet juridique d'une signature électronique qualifiée devrait être équivalent à celui d'une signature manuscrite.

(50) | Comme les autorités compétentes dans les États membres utilisent actuellement différents formats de signature électronique avancée pour signer électroniquement leurs documents, il est nécessaire de faire en sorte que les États membres, lorsqu'ils reçoivent des documents signés électroniquement, puissent prendre en charge techniquement au moins un certain nombre de formats de signature électronique avancée. De même, lorsque les autorités compétentes dans les États membres utilisent des cachets électroniques avancés, il faudrait veiller à ce qu'elles prennent en charge au moins un certain nombre de formats de cachet électronique avancé.

(51) | Le signataire devrait pouvoir confier les dispositifs de création de signature électronique qualifiés aux soins d'un tiers, pour autant que des mécanismes et procédures appropriés soient mis en œuvre pour garantir que le signataire a le contrôle exclusif de l'utilisation de ses données de création de signature électronique, et que l'utilisation du dispositif satisfait aux exigences en matière de signature électronique qualifiée.

(52) | La création de signatures électroniques à distance, système dans lequel l'environnement de création de signatures électroniques est géré par un prestataire de services de confiance au nom du signataire, est appelée à se développer en raison de ses multiples avantages économiques. Toutefois, afin que ces signatures électroniques reçoivent la même reconnaissance juridique que les signatures électroniques créées avec un environnement entièrement géré par l'utilisateur, les prestataires offrant des services de signature électronique à distance devraient appliquer des procédures de sécurité spécifiques en matière de gestion et d'administration et utiliser des systèmes et des produits fiables, notamment des canaux de communication électronique sécurisés, afin de garantir que l'environnement de création de signatures électroniques est fiable et qu'il est utilisé sous le contrôle exclusif du signataire. Dans le cas de la création d'une signature électronique qualifiée à l'aide d'un dispositif de création de signature électronique à distance, les exigences applicables aux prestataires de services de confiance qualifiés énoncées dans le présent règlement devraient s'appliquer.

(53) | La suspension de certificats qualifiés est, dans un certain nombre d'États membres, une pratique opérationnelle établie des prestataires de services de confiance qui est différente de la révocation et entraîne une perte temporaire de validité d'un certificat. La sécurité juridique impose que le statut de suspension d'un certificat soit toujours clairement indiqué. À cet effet, les prestataires de services de confiance devraient avoir la responsabilité de clairement indiquer le statut du certificat et, s'il est suspendu, la période précise de temps durant laquelle le certificat est suspendu. Le présent règlement ne devrait pas imposer aux prestataires de services de confiance ou aux États membres de recourir à la suspension, mais devrait prévoir des règles en matière de transparence, dans les cas où cette pratique est disponible.

(54) | L'interopérabilité et la reconnaissance transfrontalières des certificats qualifiés sont une condition préalable en vue de la reconnaissance transfrontalière des signatures électroniques qualifiées. Dès lors, les certificats qualifiés ne devraient faire l'objet d'aucune exigence allant au-delà des exigences énoncées dans le présent règlement. Cependant, il devrait être permis, au niveau national, d'inclure dans les certificats qualifiés des attributs spécifiques, tels que des identifiants uniques, pour autant que ces attributs spécifiques n'entravent pas l'interopérabilité et la reconnaissance transfrontalières des certificats et des signatures électroniques qualifiés.

van de in deze verordening vastgestelde voorschriften dat een gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg dient te hebben als een handgeschreven handtekening.

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

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

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

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

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

la signature mobile et la signature en mode informatique en nuage, nécessitent une solution technique et organisationnelle pour les dispositifs de création de signature électronique qualifiés pour lesquels des normes de sécurité peuvent ne pas encore exister ou pour lesquels la première certification de sécurité informatique est en cours d'examen. Le niveau de sécurité de ces dispositifs de création de signature électronique qualifiés ne pourrait être évalué en utilisant d'autres processus que lorsque ces normes de sécurité n'existent pas ou que la première certification de sécurité informatique est en cours d'examen. Ces processus devraient être comparables aux normes de certification de sécurité informatique, dans la mesure où leurs niveaux de sécurité sont équivalents. Ces processus pourraient être facilités grâce à un examen par les pairs.

mobiel ondertekenen en ondertekenen in de cloud berusten echter op technische en organisatorische oplossingen voor gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen waarvoor nog geen beveiligingsstandaarden voorhanden zijn of waarvoor de eerste IT-veiligheidscertificeringsprocedure nog loopt. Het beveiligingsniveau van dergelijke gekwalificeerde apparatuur voor het aanmaken van elektronische handtekeningen kan worden geëvalueerd door gebruik te maken van alternatieve processen, maar enkel indien dergelijke veiligheidsnormen niet beschikbaar zijn of indien de eerste IT-veiligheidsbeoordeling aan de gang is. Deze processen dienen vergelijkbaar te zijn met de standaarden voor IT-veiligheidscertificering, voor zover het om gelijke beveiligingsniveaus gaat. Deze processen zouden baat kunnen hebben bij onderlinge evaluatie.

(56) | Le présent règlement devrait énoncer les exigences applicables aux dispositifs de création de signature électronique qualifiés pour garantir les fonctionnalités des signatures électroniques avancées. Le présent règlement ne devrait pas couvrir l'intégralité de l'environnement de système d'exploitation de ces dispositifs. Dès lors, la certification des dispositifs de création de signature électronique qualifiés ne devrait pas s'étendre au-delà du matériel et du logiciel système utilisés pour gérer et protéger les données de création de signatures électroniques créées, stockées ou traitées dans le dispositif de création de signature électronique. Comme précisé dans les normes pertinentes, les applications de création de signatures électroniques ne devraient pas être soumises à l'obligation de certification.

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

(57) | Pour garantir la sécurité juridique concernant la validité de la signature, il est essentiel de préciser les éléments de la signature électronique qualifiée que devrait vérifier la partie utilisatrice effectuant la validation. En outre, le fait de définir les exigences applicables aux prestataires de services de confiance qualifiés qui peuvent fournir un service de validation qualifié aux parties utilisatrices ne voulant ou ne pouvant pas effectuer elles-mêmes la validation de signatures électroniques qualifiées devrait inciter les secteurs privé et public à investir dans de tels services. Les deux éléments devraient faire de la validation de signatures électroniques qualifiées une procédure aisée et adaptée à toutes les parties au niveau de l'Union.

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

(58) | Lorsqu'une transaction exige d'une personne morale un cachet électronique qualifié, une signature électronique qualifiée du représentant autorisé de la personne morale devrait être également recevable.

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

(59) | Les cachets électroniques devraient servir à prouver qu'un document électronique a été délivré par une personne morale en garantissant l'origine et l'intégrité du document.

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

(60) | Les prestataires de services de confiance délivrant des certificats qualifiés de cachet électronique devraient mettre en œuvre les mesures nécessaires afin de pouvoir établir l'identité de la personne physique représentant la personne morale à laquelle le certificat qualifié de cachet électronique est fourni, lorsque cette identification est nécessaire au niveau national dans le cadre d'une procédure judiciaire ou administrative.

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

(61) | Le présent règlement devrait prévoir la conservation à long terme des informations, afin d'assurer la validité juridique des signatures et cachets électroniques sur de longues périodes de temps, et de garantir qu'elles pourront être validées indépendamment de l'évolution technologique.

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

(62) | Afin d'assurer la sécurité des horodatages électroniques qualifiés, le présent règlement devrait imposer l'utilisation d'un cachet électronique avancé, d'une signature électronique avancée ou d'autres méthodes équivalentes. Il est à prévoir que l'innovation pourrait déboucher sur de nouvelles technologies susceptibles d'assurer un niveau de sécurité équivalent pour les horodatages. En cas de recours à une méthode autre que le cachet électronique avancé ou la signature électronique avancée, il devrait revenir au prestataire de services de confiance qualifié de démontrer, dans le rapport d'évaluation de la conformité, que ladite méthode assure un

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

énoncées dans le présent règlement.

(63) | Les documents électroniques sont importants pour la suite du développement des transactions électroniques transfrontalières au sein du marché intérieur. Le présent règlement devrait établir le principe selon lequel un document électronique ne pourrait se voir refuser un effet juridique au motif qu'il se présente sous une forme électronique afin de garantir qu'une transaction électronique ne sera pas rejetée au seul motif qu'un document se présente sous une forme électronique.

(64) | Lorsqu'elle traite la question du format des signatures et des cachets électroniques avancés, la Commission devrait s'appuyer sur les pratiques, normes et dispositions législatives en vigueur, en particulier la décision 2011/130/UE de la Commission (11).

(65) | Outre le document délivré par une personne morale, les cachets électroniques peuvent servir à authentifier tout bien numérique de ladite personne, tel un code logiciel ou des serveurs.

(66) | Il est essentiel de prévoir un cadre juridique en vue de faciliter la reconnaissance transfrontalière entre les systèmes juridiques nationaux existants en matière de services d'envoi recommandé électronique. Ce cadre pourrait également ouvrir de nouvelles possibilités de commercialisation permettant aux prestataires de services de confiance de l'Union d'offrir de nouveaux services d'envoi recommandé électronique paneuropéens.

(67) | Les services d'authentification de site internet sont un moyen permettant au visiteur d'un site internet de s'assurer que celui-ci est tenu par une entité véritable et légitime. Ces services contribuent à instaurer un climat de confiance pour la réalisation de transactions commerciales en ligne, les utilisateurs tendant à se fier à un site internet qui a été authentifié. La fourniture et l'utilisation de services d'authentification de site internet se font entièrement sur une base volontaire. Cependant, pour que l'authentification de site internet s'affirme comme un moyen de renforcer la confiance, de fournir à l'utilisateur davantage d'expériences positives et de favoriser la croissance sur le marché intérieur, il convient que le présent règlement impose des obligations minimales de sécurité et de responsabilité aux prestataires et à leurs services. À cette fin, il a été tenu compte des résultats des initiatives en cours menées par le secteur, par exemple le «Certification Authorities/Browser Forum – CA/B Forum» (Forum des autorités de certification/navigateurs internet). En outre, le présent règlement ne devrait pas entraver l'utilisation d'autres moyens ou méthodes permettant d'authentifier un site internet ne relevant pas du présent règlement, ni empêcher des prestataires de services d'authentification de site internet de pays tiers de fournir leurs services à des clients dans l'Union. Toutefois, les services d'authentification de site internet d'un prestataire d'un pays tiers ne devraient être reconnus comme étant qualifiés conformément au présent règlement que si une convention internationale a été conclue entre l'Union et le pays où ce prestataire est établi.

(68) | La notion de «personne morale», d'après les dispositions du traité sur le fonctionnement de l'Union européenne relatives à l'établissement, laisse aux opérateurs le choix de la forme juridique qu'ils jugent appropriée pour l'exercice de leur activité. Par conséquent, on entend par «personne morale», au sens du traité sur le fonctionnement de l'Union européenne, toute entité constituée en vertu du droit d'un État membre ou régie par celui-ci, quelle que soit sa forme juridique.

(69) | Les institutions, organes et organismes de l'Union sont encouragés à reconnaître l'identification électronique et les services de confiance couverts par le présent règlement aux fins de la coopération administrative en tirant parti, notamment, des bonnes pratiques existantes et des résultats de projets en cours dans les domaines couverts par le présent règlement.

(70) | Afin de compléter, de façon souple et rapide, certains aspects techniques précis du présent règlement, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne en ce qui concerne

garandeert en voldoet aan de in deze verordening vastgestelde verplichtingen.

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

(64) | Met betrekking tot de formats van geavanceerde elektronische handtekeningen en zegels moet de Commissie voortbouwen op bestaande praktijken, standaarden en wetgeving, in het bijzonder Besluit 2011/130/EU van de Commissie (11).

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

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

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

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

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

(70) | Om bepaalde uitvoerige technische aspecten van deze verordening op een flexibele en snelle manier aan te vullen, moet de bevoegdheid om handelingen vast te stellen overeenkomstig artikel 290 VWEU aan de Commissie worden overgedragen wat betreft de criteria waaraan de

convient que lorsqu'elle prépare et élabore des actes délégués, la Commission veille à ce que les documents pertinents soient transmis simultanément, en temps utile et de façon appropriée, au Parlement européen et au Conseil.

meer op deskundigenniveau. De Commissie moet er bij de voorbereiding en opstelling van gedelegeerde handelingen voor zorgen dat de desbetreffende documenten tijdig en op gepaste wijze gelijktijdig worden toegezonden aan het Europees Parlement en de Raad.

(71) | Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission, notamment pour ce qui est de spécifier les numéros de référence des normes dont l'utilisation donnerait lieu à une présomption de conformité à certaines exigences fixées par le présent règlement. Ces compétences devraient être exercées en conformité avec le règlement (UE) no 182/2011 du Parlement européen et du Conseil (12).

(71) | Om eenvormige voorwaarden te waarborgen voor de uitvoering van deze verordening, moeten uitvoeringsbevoegdheden worden toegekend aan de Commissie, in het bijzonder voor het specificeren van referentienummers voor standaarden waarvan het gebruik aanleiding zou zijn voor een vermoeden van overeenstemming met bepaalde vereisten die zijn vastgesteld in deze verordening. Die bevoegdheden moeten in overeenstemming met Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad worden uitgeoefend (12).

(72) | Lorsqu'elle adopte des actes délégués ou d'exécution, la Commission devrait tenir dûment compte des normes et des spécifications techniques établies par des instances et organismes européens et internationaux de normalisation, notamment le Comité européen de normalisation (CEN), l'Institut européen de normalisation des télécommunications (IENT), l'Organisation internationale de normalisation (ISO) et l'Union internationale des télécommunications (UIT), en vue de garantir un niveau élevé de sécurité et d'interopérabilité pour l'identification électronique et les services de confiance.

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

(73) | Par souci de sécurité juridique et de clarté, la directive 1999/93/CE devrait être abrogée.

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

(74) | Pour garantir la sécurité juridique aux opérateurs économiques qui utilisent déjà des certificats qualifiés délivrés à des personnes physiques conformément à la directive 1999/93/CE, il est nécessaire de prévoir un délai suffisant à des fins transitoires. De même, il convient de prévoir des mesures transitoires pour les dispositifs sécurisés de création de signature dont la conformité a été déterminée conformément à la directive 1999/93/CE, ainsi que pour les prestataires de service de certification qui délivrent des certificats qualifiés avant le 1er juillet 2016. Enfin, il est également nécessaire de doter la Commission des moyens d'adopter les actes d'exécution et les actes délégués avant cette date.

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

(75) | Les dates d'application établies dans le présent règlement n'affectent pas les obligations existantes incombant déjà aux États membres en vertu du droit de l'Union, notamment de la directive 2006/123/CE.

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

(76) | Étant donné que les objectifs du présent règlement ne peuvent être atteints de manière suffisante par les États membres mais peuvent, en raison de l'ampleur de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

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

(77) | Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) no 45/2001 du Parlement européen et du Conseil (13) et a émis un avis, le 27 septembre 2012 (14),

(77) | De Europese Toezichthouder voor gegevensbescherming werd geraadpleegd in overeenstemming met artikel 28, lid 2, van Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad (13) en heeft op 27 september 2012 advies uitgebracht (14),

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

CHAPITRE I

HOOFDSTUK I

DISPOSITIONS GÉNÉRALES

ALGEMENE BEPALINGEN

Article premier

Artikel 1

Objet

Onderwerp

En vue d'assurer le bon fonctionnement du marché intérieur tout en visant à atteindre un niveau adéquat de sécurité des moyens d'identification électronique et des services de confiance, le présent règlement:

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

a) | fixe les conditions dans lesquelles un État membre reconnaît les moyens d'identification électronique des personnes physiques et morales qui relèvent d'un schéma d'identification électronique notifié d'un autre État membre;

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

b) | établit des règles applicables aux services de confiance, en particulier pour les transactions électroniques; et

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

c) | instaure un cadre juridique pour les services de signatures électroniques, de cachets électroniques,

c) | een juridisch kader vastgesteld voor elektronische handtekeningen, elektronische zegels, elektronische

d'envoi recommandé électronique et les services de certificats pour l'authentification de site internet.

Article 2

Champ d'application

1. Le présent règlement s'applique aux schémas d'identification électronique qui ont été notifiés par un État membre et aux prestataires de services de confiance établis dans l'Union.

2. Le présent règlement ne s'applique pas à la fourniture de services de confiance utilisés exclusivement dans des systèmes fermés résultant du droit national ou d'accords au sein d'un ensemble défini de participants.

3. Le présent règlement n'affecte pas le droit national ou de l'Union relatif à la conclusion et à la validité des contrats ou d'autres obligations juridiques ou procédurales d'ordre formel.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

1. | «identification électronique», le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale;

2. | «moyen d'identification électronique», un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne;

3. | «données d'identification personnelle», un ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale;

4. | «schéma d'identification électronique», un système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales, ou à des personnes physiques représentant des personnes morales;

5. | «authentification», un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique;

6. | «partie utilisatrice», une personne physique ou morale qui se fie à une identification électronique ou à un service de confiance;

7. | «organismes du secteur public», un État, une autorité régionale ou locale, un organisme de droit public ou une association constituée d'une ou de plusieurs de ces autorités ou d'un ou de plusieurs de ces organismes de droit public, ou une entité privée mandatée par au moins un ou une de ces autorités, organismes, ou associations pour fournir des services publics lorsqu'elle agit en vertu de ce mandat;

8. | «organisme de droit public», un organisme au sens de l'article 2, paragraphe 1, point 4), de la directive 2014/24/UE du Parlement européen et du Conseil (15);

9. | «signataire», une personne physique qui crée une signature électronique;

10. | «signature électronique», des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer;

11. | «signature électronique avancée», une signature électronique qui satisfait aux exigences énoncées à l'article 26:

12. | «signature électronique qualifiée», une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique;

13. | «données de création de signature électronique», des données uniques qui sont utilisées par le signataire pour créer une signature électronique;

elektronisch aangetekende bezorging en certificatendiensten voor websiteauthenticatie.

Artikel 2

Toepassingsgebied

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

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

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

Artikel 3

Definities

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

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

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

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

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

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

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

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

8. „publiekrechtelijke instelling": een instelling volgens de definitie in punt 4 van artikel 2, lid 1, van Richtlijn 2014/24/EU van het Europees Parlement en de Raad (15);

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

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

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

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

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

14. | «certificat de signature électronique», une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne;	14. „certificaat voor elektronische handtekeningen": een elektronische attestering die valideringsgegevens voor elektronische handtekeningen aan een natuurlijke persoon koppelt en ten minste de naam of het pseudoniem van die persoon bevestigt;
15. | «certificat qualifié de signature électronique», un certificat de signature électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe I;	15. „gekwalificeerd certificaat voor elektronische handtekeningen": een certificaat voor elektronische handtekeningen, dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage I;
16. | «service de confiance», un service électronique normalement fourni contre rémunération qui consiste: | a) | en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services; ou | b) | en la création, en la vérification et en la validation de certificats pour l'authentification de site internet; ou | c) | en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services;	16. „vertrouwensdienst": een elektronische dienst die gewoonlijk tegen betaling wordt verricht en het onderstaande inhoudt:
17. | «service de confiance qualifié», un service de confiance qui satisfait aux exigences du présent règlement;	a) | het aanmaken, verifiëren en valideren van elektronische handtekeningen, elektronische zegels of elektronische tijdstempels, diensten voor elektronisch aangetekende bezorging en op deze diensten betrekking hebbende certificaten of
18. | «organisme d'évaluation de la conformité», un organisme défini à l'article 2, point 13), du règlement (CE) no 765/2008, qui est accrédité conformément audit règlement comme étant compétent pour effectuer l'évaluation de la conformité d'un prestataire de services de confiance qualifié et des services de confiance qualifiés qu'il fournit;	b) | het aanmaken, verifiëren en valideren van certificaten voor authenticatie van websites, of
19. | «prestataire de services de confiance», une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié;	c) | het bewaren van elektronische handtekeningen, zegels of certificaten die op deze diensten betrekking hebben;
20. | «prestataire de services de confiance qualifié», un prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut qualifié;	17. „gekwalificeerde vertrouwensdienst": een vertrouwensdienst die voldoet aan de toepasselijke eisen zoals vastgelegd in deze verordening;
21. | «produit», un dispositif matériel ou logiciel, ou les composants correspondants du dispositif matériel ou logiciel, qui sont destinés à être utilisés pour la fourniture de services de confiance;	18. „conformiteitsbeoordelingsinstantie": een instantie omschreven in artikel 2, punt 13, van Verordening (EG) nr. 765/2008, die in overeenstemming met die verordening geaccrediteerd is om een conformiteitsbeoordeling te verrichten van een gekwalificeerde verlener van vertrouwensdiensten en van de door hem verleende vertrouwensdiensten;
22. | «dispositif de création de signature électronique», un dispositif logiciel ou matériel configuré servant à créer une signature électronique;	19. „verlener van vertrouwensdiensten": een natuurlijke persoon of rechtspersoon die een of meer vertrouwensdiensten verleent als een gekwalificeerde of als een niet-gekwalificeerde verlener van vertrouwensdiensten;
23. | «dispositif de création de signature électronique qualifié», un dispositif de création de signature électronique qui satisfait aux exigences énoncées à l'annexe II;	20. „gekwalificeerde verlener van vertrouwensdiensten": een verlener van vertrouwensdiensten die één of meerdere gekwalificeerde vertrouwensdiensten verleent en van het toezichthoudende orgaan de status van gekwalificeerde heeft gekregen;
24. | «créateur de cachet», une personne morale qui crée un cachet électronique;	21. „product": software of hardware, of relevante componenten van hardware of software, die bedoeld zijn om te worden gebruikt voor de verlening van vertrouwensdiensten;
25. | «cachet électronique», des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières;	22. „middel voor het aanmaken van elektronische handtekeningen": geconfigureerde software of hardware die wordt gebruikt om een elektronische handtekening aan te maken;
26. | «cachet électronique avancé», un cachet électronique qui satisfait aux exigences énoncées à l'article 36;	23. „gekwalificeerd middel voor het aanmaken van elektronische handtekeningen": een middel voor het aanmaken van elektronische handtekeningen dat voldoet aan de eisen van bijlage II;
27. | «cachet électronique qualifié», un cachet électronique avancé qui est créé à l'aide d'un dispositif de création de cachet électronique qualifié et qui repose sur un certificat qualifié de cachet électronique;	24. „aanmaker van een zegel": een rechtspersoon die een elektronisch zegel aanmaakt;
28. | «données de création de cachet électronique», des données uniques qui sont utilisées par le créateur du cachet électronique pour créer un cachet électronique;	25. „elektronisch zegel": gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die worden gebruikt om de oorsprong en integriteit daarvan te waarborgen;
29. | «certificat de cachet électronique», une attestation électronique qui associe les données de validation d'un cachet électronique à une personne morale et confirme le nom de cette personne;	26. „geavanceerd elektronisch zegel": een elektronisch zegel dat voldoet aan de eisen in artikel 36;

30. | «certificat qualifié de cachet électronique», un certificat de cachet électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe III;

31. | «dispositif de création de cachet électronique», un dispositif logiciel ou matériel configuré utilisé pour créer un cachet électronique;

32. | «dispositif de création de cachet électronique qualifié», un dispositif de création de cachet électronique qui satisfait mutatis mutandis aux exigences fixées à l'annexe II;

33. | «horodatage électronique», des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant;

34. | «horodatage électronique qualifié», un horodatage électronique qui satisfait aux exigences fixées à l'article 42;

35. | «document électronique», tout contenu conservé sous forme électronique, notamment un texte ou un enregistrement sonore, visuel ou audiovisuel;

36. | «service d'envoi recommandé électronique», un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée;

37. | «service d'envoi recommandé électronique qualifié», un service d'envoi recommandé électronique qui satisfait aux exigences fixées à l'article 44;

38. | «certificat d'authentification de site internet«, une attestation qui permet d'authentifier un site internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré;

39. | «certificat qualifié d'authentification de site internet«, un certificat d'authentification de site internet, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe IV;

40. | «données de validation», des données qui servent à valider une signature électronique ou un cachet électronique;

41. | «validation», le processus de vérification et de confirmation de la validité d'une signature ou d'un cachet électronique.

Article 4

Principe du marché intérieur

1. Il n'y a pas de restriction à la fourniture de services de confiance, sur le territoire d'un État membre, par un prestataire de services de confiance établi dans un autre État membre pour des raisons qui relèvent des domaines couverts par le présent règlement.

2. Les produits et les services de confiance qui sont conformes au présent règlement sont autorisés à circuler librement au sein du marché intérieur.

Article 5

Protection et traitement des données à caractère personnel

1. Le traitement de données à caractère personnel est effectué conformément à la directive 95/46/CE.

2. Sans préjudice de l'effet juridique donné aux pseudonymes au titre du droit national, l'utilisation de pseudonymes dans les transactions électroniques n'est pas

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artikel 4

Internemarktbeginsel

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

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

Artikel 5

interdite.

CHAPITRE II

IDENTIFICATION ÉLECTRONIQUE

Article 6

Reconnaissance mutuelle

1. Lorsqu'une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification est exigée en vertu du droit national ou de pratiques administratives nationales pour accéder à un service en ligne fourni par un organisme du secteur public dans un État membre, le moyen d'identification électronique délivré dans un autre État membre est reconnu dans le premier État membre aux fins de l'authentification transfrontalière pour ce service en ligne, à condition que les conditions suivantes soient remplies:

a) | la délivrance de ce moyen d'identification électronique relève d'un schéma d'identification électronique qui figure sur la liste publiée par la Commission en vertu de l'article 9;

b) | le niveau de garantie de ce moyen d'identification électronique correspond à un niveau de garantie égal ou supérieur à celui requis par l'organisme du secteur public concerné pour accéder à ce service en ligne dans le premier État membre, à condition que le niveau de garantie de ce moyen d'identification électronique corresponde au niveau de garantie substantiel ou élevé;

c) | l'organisme du secteur public concerné utilise le niveau de garantie substantiel ou élevé pour ce qui concerne l'accès à ce service en ligne.

Cette reconnaissance intervient au plus tard douze mois après la publication par la Commission de la liste visée au point a) du premier alinéa.

2. Un moyen d'identification électronique dont la délivrance relève d'un schéma d'identification électronique figurant sur la liste publiée par la Commission en vertu de l'article 9 et qui correspond au niveau de garantie faible peut être reconnu par des organismes du secteur public aux fins de l'authentification transfrontalière du service fourni en ligne par ces organismes.

Article 7

Éligibilité pour la notification des schémas d'identification électronique

Un schéma d'identification électronique est éligible aux fins de notification en vertu de l'article 9, paragraphe 1, si toutes les conditions suivantes sont remplies:

a) | les moyens d'identification électronique relevant du schéma d'identification électronique sont délivrés: | i) | par l'État membre notifiant; | ii) | dans le cadre d'un mandat de l'État membre notifiant; ou | iii) | indépendamment de l'État membre notifiant et sont reconnus par cet État membre;

b) | les moyens d'identification électronique relevant du schéma d'identification électronique peuvent être utilisés pour accéder au moins à un service qui est fourni par un organisme du secteur public et qui exige l'identification électronique dans l'État membre notifiant;

c) | le schéma d'identification électronique et les moyens d'identification électronique délivrés dans ce cadre répondent aux exigences d'au moins un des niveaux de garantie prévus dans l'acte d'exécution visé à l'article 8, paragraphe 3;

Gegevensverwerking en -bescherming

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

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

HOOFDSTUK II

ELEKTRONISCHE IDENTIFICATIE

Artikel 6

Wederzijdse erkenning

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

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

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

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

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

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

Artikel 7

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

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

aux procédures pour le niveau de garantie concerné prévues dans l'acte d'exécution visé à l'article 8, paragraphe 3, à la personne physique ou morale visée à l'article 3, point 1), au moment de la délivrance du moyen d'identification électronique relevant de ce schéma;

e) | la partie délivrant le moyen d'identification électronique relevant de ce schéma veille à ce que le moyen d'identification électronique soit attribué à la personne visée au point d) du présent article conformément aux spécifications techniques, aux normes et aux procédures pour le niveau de garantie concerné prévues dans l'acte d'exécution visé à l'article 8, paragraphe 3;

f) | l'État membre notifiant veille à ce qu'une authentification en ligne soit disponible afin de permettre à toute partie utilisatrice établie sur le territoire d'un autre État membre de confirmer les données d'identification personnelle reçues sous forme électronique. | Pour les parties utilisatrices autres que des organismes du secteur public, l'État membre notifiant peut définir les conditions d'accès à cette authentification. Cette authentification transfrontalière est fournie gratuitement lorsqu'elle est effectuée en liaison avec un service en ligne fourni par un organisme du secteur public. | Les États membres n'imposent aucune exigence technique disproportionnée aux parties utilisatrices qui envisagent de procéder à cette authentification, lorsque de telles exigences empêchent ou entravent sensiblement l'interopérabilité des schémas d'identification électronique notifiés;

g) | six mois au moins avant la notification en vertu de l'article 9, paragraphe 1, l'État membre notifiant fournit aux autres États membres aux fins de l'obligation au titre de l'article 12, paragraphe 5, une description de ce schéma conformément aux modalités de procédure établies par les actes d'exécution visés à l'article 12, paragraphe 7.

h) | le schéma d'identification électronique satisfait aux exigences de l'acte d'exécution visé à l'article 12, paragraphe 8.

Article 8

Niveaux de garantie des schémas d'identification électronique

1. Un schéma d'identification électronique notifié en vertu de l'article 9, paragraphe 1, détermine les spécifications des niveaux de garantie faible, substantiel et/ou élevé des moyens d'identification électronique délivrés dans le cadre dudit schéma.

2. Les niveaux de garantie faible, substantiel et élevé satisfont, respectivement, aux critères suivants:

a) | le niveau de garantie faible renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un degré limité de fiabilité à l'identité revendiquée ou prétendue d'une personne, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire le risque d'utilisation abusive ou d'altération de l'identité;

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

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

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

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

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

f) | de aanmeldende lidstaat zorgt voor de beschikbaarheid van onlineauthenticatie, zodat iedere vertrouwende partij die op het grondgebied van een andere lidstaat gevestigd is, de mogelijkheid heeft de ontvangen persoonsidentificatiegegevens in elektronische vorm te bevestigen. | Voor andere vertrouwende partijen dan openbare instanties mag de aanmeldende lidstaat voorwaarden stellen voor toegang tot die authenticatie. Grensoverschrijdende authenticatie is kosteloos wanneer zij wordt uitgevoerd voor een door een openbare instantie verleende onlinedienst. | De lidstaten leggen geen specifieke onevenredige technische eisen op aan vertrouwende partijen die voornemens zijn een dergelijke authenticatie uit te voeren indien dergelijke eisen de interoperabiliteit van de aangemelde stelsels voor elektronische identificatie tegenhouden of in aanzienlijke mate belemmeren;

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

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

Artikel 8

Betrouwbaarheidsniveaus van stelsels voor elektronische identificatie

b) | le niveau de garantie substantiel renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un degré substantiel de fiabilité à l'identité revendiquée ou prétendue d'une personne, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité;

c) | le niveau de garantie élevé renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un niveau de fiabilité à l'identité revendiquée ou prétendue d'une personne plus élevé qu'un moyen d'identification électronique ayant le niveau de garantie substantiel, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité.

3. Au plus tard le 18 septembre 2015, compte tenu des normes internationales pertinentes et sous réserve du paragraphe 2, la Commission fixe, au moyen d'actes d'exécution, les spécifications techniques, normes et procédures minimales sur la base desquelles les niveaux de garantie faible, substantiel et élevé sont spécifiés pour les moyens d'identification électronique aux fins du paragraphe 1.

Ces spécifications techniques, normes et procédures minimales sont fixées par référence à la fiabilité et à la qualité des éléments suivants:

a) | la procédure visant à prouver et vérifier l'identité des personnes physiques ou morales demandant la délivrance de moyens d'identification électronique;

b) | la procédure de délivrance des moyens d'identification électronique demandés;

c) | le mécanisme d'authentification au moyen duquel la personne physique ou morale utilise le moyen d'identification électronique pour confirmer son identité à une partie utilisatrice;

d) | l'entité délivrant les moyens d'identification électronique;

e) | tout autre organisme associé à la demande de délivrance de moyens d'identification électronique; et

f) | les spécifications techniques et de sécurité des moyens d'identification électronique délivrés.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 9

Notification

1. L'État membre notifiant notifie les informations suivantes à la Commission et lui communique toute modification ultérieure qui leur est apportée dans les meilleurs délais:

a) | une description du schéma d'identification électronique, y compris ses niveaux de garantie et l'entité ou les entités qui délivrent les moyens d'identification électronique relevant de ce schéma;

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

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

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

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

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

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

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

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

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

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

d) | de entiteit die het elektronische identificatiemiddel uitgeeft;

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

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

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

Artikel 9

b) | le régime de contrôle applicable et des informations sur la responsabilité en ce qui concerne les aspects suivants: | i) | la partie qui délivre le moyen d'identification électronique; et | ii) | la partie qui gère la procédure d'authentification;

c) | l'autorité ou les autorités responsables du schéma d'identification électronique;

d) | des informations sur l'entité ou les entités qui gèrent l'enregistrement des données d'identification personnelle uniques;

e) | une description de la façon dont il est satisfait aux exigences énoncées dans l'acte d'exécution visé à l'article 12, paragraphe 8;

f) | une description de l'authentification visée à l'article 7, point f);

g) | les dispositions concernant la suspension ou la révocation du schéma d'identification électronique notifié, de l'authentification ou des parties compromises concernées.

2. Un an à compter de la date d'application des actes d'exécution visés à l'article 8, paragraphe 3, et à l'article 12, paragraphe 8, la Commission publie au Journal officiel de l'Union européenne la liste des schémas d'identification électronique qui ont été notifiés en vertu du paragraphe 1, et les informations essentielles à leur sujet.

3. Si la Commission reçoit une notification après expiration du délai visé au paragraphe 2, elle publie au Journal officiel de l'Union européenne les modifications apportées à la liste visée au paragraphe 2 dans les deux mois à compter de la date de réception de cette notification.

4. Un État membre peut soumettre à la Commission une demande visant à retirer de la liste visée au paragraphe 2 le schéma d'identification électronique qu'il a notifié. La Commission publie au Journal officiel de l'Union européenne les modifications correspondantes apportées à la liste dans un délai d'un mois à compter de la date de réception de la demande de l'État membre.

5. La Commission peut définir, au moyen d'actes d'exécution, les circonstances, les formats et les procédures pour les notifications au titre du paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 10

Atteinte à la sécurité

1. En cas d'atteinte ou d'altération partielle du schéma d'identification électronique notifié en application de l'article 9, paragraphe 1, ou de l'authentification visée à l'article 7, point f), telle qu'elle affecte la fiabilité de l'authentification transfrontalière de ce schéma, l'État membre notifiant suspend ou révoque, immédiatement, cette authentification transfrontalière ou les éléments altérés en cause, et en informe les autres États membres et la Commission.

2. Lorsqu'il a été remédié à l'atteinte ou à l'altération visée au paragraphe 1, l'État membre notifiant rétablit l'authentification transfrontalière et en informe les autres États membres et la Commission dans les meilleurs délais.

3. S'il n'est pas remédié à l'atteinte ou à l'altération visée au paragraphe 1 dans un délai de trois mois à compter de la suspension ou de la révocation, l'État membre notifiant notifie le retrait du schéma d'identification électronique aux autres États membres et à la Commission.

La Commission publie, dans les meilleurs délais, au Journal officiel de l'Union européenne, les modifications correspondantes apportées à la liste visée à l'article 9, paragraphe 2.

Aanmelding

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

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

b) | de toepasselijke toezichtregeling en informatie over de aansprakelijkheidsregeling met betrekking tot onderstaande: | i) | de partij die het elektronische identificatiemiddel uitgeeft, en | ii) | de partij die de authenticatieprocedure uitvoert;

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

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

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

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

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

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

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

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

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

Artikel 10

Inbreuk op de beveiliging

1. Wanneer er inbreuk wordt gepleegd op het overeenkomstig artikel 9, lid 1, aangemelde stelsel voor elektronische identificatie of op de in artikel 7, onder f), bedoelde authenticatie of wanneer de integriteit ervan deels wordt geschonden zodat de betrouwbaarheid van de

grensoverschrijdende authenticatie of de delen waarvan de integriteit geschonden is, opschorten of intrekken, en de andere lidstaten en de Commissie hiervan op de hoogte stellen.

Article 11

Responsabilité

1. L'État membre notifiant est responsable du dommage causé intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations qui lui incombent en vertu de l'article 7, points d) et f), dans le cas d'une transaction transfrontalière.

2. La partie qui délivre le moyen d'identification électronique est responsable du dommage causé intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations qui lui incombent en vertu de l'article 7, point e), dans le cas d'une transaction transfrontalière.

3. La partie qui gère la procédure d'authentification est responsable du dommage causé intentionnellement ou par négligence à toute personne physique ou morale pour ne pas avoir assuré la gestion correcte de l'authentification visée à l'article 7, point f), dans le cas d'une transaction transfrontalière.

4. Les paragraphes 1, 2 et 3 s'appliquent conformément aux dispositions nationales en matière de responsabilité.

5. Les paragraphes 1, 2 et 3 sont sans préjudice de la responsabilité incombant, au titre du droit national, aux parties à une transaction effectuée à l'aide de moyens d'identification électronique relevant du schéma d'identification électronique notifié en vertu de l'article 9, paragraphe 1.

Article 12

Coopération et interopérabilité

1. Les schémas nationaux d'identification électronique notifiés en vertu de l'article 9, paragraphe 1, sont interopérables.

2. Aux fins du paragraphe 1, un cadre d'interopérabilité est établi.

3. Le cadre d'interopérabilité satisfait aux critères suivants:

a) | il vise à être neutre du point de vue technologique et n'opère pas de discrimination entre l'une ou l'autre des solutions techniques nationales particulières destinées à l'identification électronique au sein d'un État membre;

b) | il suit les normes européennes et internationales, dans la mesure du possible;

c) | il facilite la mise en œuvre du principe du respect de la vie privée dès la conception; et

d) | il garantit que les données à caractère personnel sont traitées conformément à la directive 95/46/CE.

4. Le cadre d'interopérabilité est composé:

a) | d'une référence aux exigences techniques minimales liées aux niveaux de garantie prévus à l'article 8;

b) | d'une table de correspondance entre les niveaux de garantie nationaux des schémas d'identification électronique notifiés et les niveaux de garantie au titre de l'article 8;

c) | d'une référence aux exigences techniques minimales en matière d'interopérabilité;

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

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

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

Artikel 11

Aansprakelijkheid

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

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

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

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

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

Artikel 12

Samenwerking en interoperabiliteit

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

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

3. Het interoperabiliteitskader voldoet aan de volgende criteria:

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

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

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

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

4. Het interoperabiliteitskader bestaat uit:

d) | d'une référence à un ensemble minimal de données d'identification personnelle représentant de manière univoque une personne physique ou morale, qui est disponible dans les schémas d'identification électronique;

e) | de règles de procédure;

f) | de dispositions pour le règlement des litiges; et

g) | de normes opérationnelles communes de sécurité.

5. Les États membres coopèrent en ce qui concerne:

a) | l'interopérabilité des schémas d'identification électronique notifiés en application de l'article 9, paragraphe 1, et des schémas d'identification électronique que les États membres entendent notifier; et

b) | la sécurité des schémas d'identification électronique.

6. La coopération entre les États membres consiste:

a) | en un échange d'informations, d'expériences et de bonnes pratiques en ce qui concerne les schémas d'identification électronique, notamment les exigences techniques liées à l'interopérabilité et aux niveaux de garantie;

b) | en un échange d'informations, d'expériences et de bonnes pratiques en ce qui concerne l'utilisation des niveaux de garantie des schémas d'identification électronique prévus à l'article 8;

c) | en une évaluation par les pairs des schémas d'identification électronique relevant du présent règlement; et

d) | en un examen des évolutions pertinentes dans le secteur de l'identification électronique.

7. Au plus tard le 18 mars 2015, la Commission fixe, au moyen d'actes d'exécution, les modalités de procédure nécessaires pour faciliter la coopération entre les États membres visée aux paragraphes 5 et 6, en vue de favoriser un niveau élevé de confiance et de sécurité approprié au degré de risque.

8. Au plus tard le 18 septembre 2015, aux fins de fixer des conditions uniformes d'exécution de l'obligation prévue au paragraphe 1, la Commission adopte, sous réserve des critères énoncés au paragraphe 3 et compte tenu des résultats de la coopération entre les États membres, des actes d'exécution sur le cadre d'interopérabilité énoncé au paragraphe 4.

9. Les actes d'exécution visés aux paragraphes 7 et 8 du présent article sont adoptés en conformité avec la procédure d'examen visés à l'article 48, paragraphe 2.

CHAPITRE III

SERVICES DE CONFIANCE

SECTION 1

Dispositions générales

Article 13

Responsabilité et charge de la preuve

1. Sans préjudice du paragraphe 2, les prestataires de services de confiance sont responsables des dommages causés intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations prévues par le présent règlement.

Il incombe à la personne physique ou morale qui invoque les dommages visés au premier alinéa de prouver que le prestataire de services de confiance non qualifié a agi intentionnellement ou par négligence.

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

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

c) | een verwijzing naar technische minimumeisen voor interoperabiliteit;

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

e) | procedureregels;

f) | regelingen voor geschillenbeslechting; en

g) | gemeenschappelijke operationele veiligheidsnormen.

5. De lidstaten werken op onderstaande gebieden samen:

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

b) | de veiligheid van de stelsels voor elektronische identificatie.

6. De samenwerking tussen de lidstaten bestaat uit:

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

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

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

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

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

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

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

HOOFDSTUK III

VERTROUWENSDIENSTEN

AFDELING 1

Algemene bepalingen

Artikel 13

Un prestataire de services de confiance qualifié est présumé avoir agi intentionnellement ou par négligence, à moins qu'il ne prouve que les dommages visés au premier alinéa ont été causés sans intention ni négligence de sa part.

2. Lorsque les prestataires de services de confiance informent dûment leurs clients au préalable des limites qui existent à l'utilisation des services qu'ils fournissent et que ces limites peuvent être reconnues par des tiers, les prestataires de services de confiance ne peuvent être tenus responsables des dommages découlant de l'utilisation des services au-delà des limites indiquées.

3. Les paragraphes 1 et 2 s'appliquent conformément aux règles nationales en matière de responsabilité.

Article 14

Aspects internationaux

1. Les services de confiance fournis par des prestataires de services de confiance établis dans un pays tiers sont reconnus comme équivalents, sur le plan juridique, à des services de confiance qualifiés fournis par des prestataires de services de confiance qualifiés établis dans l'Union lorsque les services de confiance provenant du pays tiers sont reconnus en vertu d'un accord conclu entre l'Union et le pays tiers concerné ou une organisation internationale conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne.

2. Les accords visés au paragraphe 1 garantissent, en particulier, que:

a) | les exigences applicables aux prestataires de services de confiance qualifiés établis dans l'Union et les services de confiance qualifiés qu'ils fournissent sont respectés par les prestataires de services de confiance dans le pays tiers ou par les organisations internationales avec lesquels l'accord est conclu, et par les services de confiance qu'ils fournissent;

b) | les services de confiance qualifiés fournis par des prestataires de services de confiance qualifiés établis dans l'Union sont reconnus comme équivalents, sur le plan juridique, à des services de confiance fournis par des prestataires de services de confiance dans le pays tiers ou par l'organisation internationale avec lequels l'accord est conclu.

Article 15

Accessibilité aux personnes handicapées

Dans la mesure du possible, les services de confiance fournis, ainsi que les produits destinés à un utilisateur final qui servent à fournir ces services, sont accessibles aux personnes handicapées.

Article 16

Sanctions

Les États membres fixent le régime des sanctions applicables aux violations du présent règlement. Les sanctions prévues sont effectives, proportionnées et dissuasives.

SECTION 2

Contrôle

Aansprakelijkheid en bewijslast

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

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

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

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

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

Artikel 14

Internationale aspecten

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

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

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

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

Artikel 15

Toegankelijkheid voor personen met een handicap

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

Artikel 16

Sancties

Article 17

Organe de contrôle

1. Les États membres désignent un organe de contrôle établi sur leur territoire ou, d'un commun accord avec un autre État membre, un organe de contrôle établi dans cet autre État membre. Cet organe est chargé des tâches de contrôle dans l'État membre qui a procédé à la désignation.

Les organes de contrôle sont investis des pouvoirs nécessaires et dotés des ressources adéquates pour l'exercice de leurs tâches.

2. Les États membres notifient à la Commission le nom et l'adresse de l'organe de contrôle qu'ils ont désigné.

3. Le rôle de l'organe de contrôle est le suivant:

a) | contrôler les prestataires de services de confiance qualifiés établis sur le territoire de l'État membre qui a procédé à la désignation afin de s'assurer, par des activités de contrôle a priori et a posteriori, que ces prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent satisfont aux exigences fixées dans le présent règlement;

b) | prendre des mesures, si nécessaire, en ce qui concerne les prestataires de services de confiance non qualifiés établis sur le territoire de l'État membre qui a procédé à la désignation, par des activités de contrôle a posteriori, lorsqu'il est informé que ces prestataires de services de confiance non qualifiés ou les services de confiance qu'ils fournissent ne satisferaient pas aux exigences fixées dans le présent règlement.

4. Aux fins du paragraphe 3 et sous réserve des limites qu'il prévoit, les tâches de l'organe de contrôle consistent notamment:

a) | à coopérer avec d'autres organes de contrôle et à leur apporter assistance conformément à l'article 18;

b) | à analyser les rapports d'évaluation de la conformité visés à l'article 20, paragraphe 1, et à l'article 21, paragraphe 1;

c) | à informer d'autres organes de contrôle et le public d'atteintes à la sécurité ou de pertes d'intégrité conformément à l'article 19, paragraphe 2;

d) | à présenter un rapport à la Commission sur ses principales activités conformément au paragraphe 6 du présent article;

e) | à procéder à des audits ou à demander à un organisme d'évaluation de la conformité d'effectuer une évaluation de la conformité des prestataires de services de confiance qualifiés conformément à l'article 20, paragraphe 2;

f) | à coopérer avec les autorités chargées de la protection des données, en particulier en les informant, dans les meilleurs délais, des résultats des audits des prestataires de services de confiance qualifiés lorsqu'il apparaît que des règles en matière de protection des données à caractère personnel ont été violées;

g) | à accorder le statut qualifié aux prestataires de services de confiance et aux services qu'ils fournissent et à retirer ce statut conformément aux articles 20 et 21;

h) | à informer l'organisme chargé de la liste nationale de confiance visée à l'article 22, paragraphe 3, de ses décisions d'accorder ou de retirer le statut qualifié, à moins que cet organisme ne soit également l'organe de contrôle;

i) | à vérifier l'existence et l'application correcte de dispositions relatives aux plans d'arrêt d'activité lorsque le prestataire de services de confiance qualifié cesse son activité, y compris la façon dont les informations restent accessibles conformément à l'article 24, paragraphe 2, point h);

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

AFDELING 2

Toezicht

Artikel 17

Toezichthoudend orgaan

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

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

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

3. De rol van het toezichthoudend orgaan is:

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

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

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

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

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

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

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

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

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

j) | à exiger que les prestataires de services de confiance corrigent tout manquement aux obligations fixées par le présent règlement.

5. Les États membres peuvent exiger de l'organe de contrôle qu'il établisse, gère et actualise une infrastructure de confiance conformément aux conditions prévues par le droit national.

6. Au plus tard le 31 mars de chaque année, chaque organe de contrôle soumet à la Commission un rapport sur ses principales activités de l'année civile précédente, accompagné d'un résumé des notifications d'atteinte à la sécurité reçues de prestataires de services de confiance conformément à l'article 19, paragraphe 2.

7. La Commission met le rapport annuel visé au paragraphe 6 à la disposition des États membres.

8. La Commission peut définir, au moyen d'actes d'exécution, les formats et procédures applicables aux fins du rapport visé au paragraphe 6. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 18

Assistance mutuelle

1. Les organes de contrôle coopèrent en vue d'échanger des bonnes pratiques.

Un organe de contrôle fournit, après réception d'une demande justifiée d'un autre organe de contrôle, à cet organe une assistance afin que les activités des organes de contrôle puissent être exécutées de façon cohérente. L'assistance mutuelle peut notamment couvrir des demandes d'informations et des mesures de contrôle, telles que des demandes de procéder à des inspections liées aux rapports d'évaluation de la conformité visés aux articles 20 et 21.

2. Un organe de contrôle saisi d'une demande d'assistance peut refuser cette demande sur la base de l'un ou l'autre des motifs suivants:

a) | l'organe de contrôle n'est pas compétent pour fournir l'assistance demandée;

b) | l'assistance demandée n'est pas proportionnée aux activités de contrôle de l'organe de contrôle effectuées conformément à l'article 17;

c) | la fourniture de l'assistance demandée serait incompatible avec le présent règlement.

3. Le cas échéant, les États membres peuvent autoriser leurs organes de contrôle respectifs à mener des enquêtes conjointes faisant intervenir des membres des organes de contrôle d'autres États membres. Les modalités et procédures concernant ces actions conjointes sont approuvées et établies par les États membres concernés conformément à leur droit national.

Article 19

Exigences de sécurité applicables aux prestataires de services de confiance

1. Les prestataires de services de confiance qualifiés et non qualifiés prennent les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité

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

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

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

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

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

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

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

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

Artikel 18

Wederzijdse bijstand

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

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

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

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

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

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

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

conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents.

2. Les prestataires de services de confiance qualifiés et non qualifiés notifient, dans les meilleurs délais et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, à l'organe de contrôle et, le cas échéant, à d'autres organismes concernés, tels que l'organisme national compétent en matière de sécurité de l'information ou l'autorité chargée de la protection des données, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.

Lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible de porter préjudice à une personne physique ou morale à laquelle le service de confiance a été fourni, le prestataire de services de confiance notifie aussi, dans les meilleurs délais, à la personne physique ou morale l'atteinte à la sécurité ou la perte d'intégrité.

Le cas échéant, notamment lorsqu'une atteinte à la sécurité ou une perte d'intégrité concerne deux États membres ou plus, l'organe de contrôle notifié informe les organes de contrôle des autres États membres concernés ainsi que l'ENISA.

L'organe de contrôle notifié informe le public ou exige du prestataire de services de confiance qu'il le fasse, dès lors qu'il constate qu'il est dans l'intérêt public de divulguer l'atteinte à la sécurité ou la perte d'intégrité.

3. Une fois par an, l'organe de contrôle fournit à l'ENISA un résumé des notifications d'atteinte à la sécurité et de perte d'intégrité reçues de prestataires de services de confiance.

4. La Commission peut, au moyen d'actes d'exécution:

a) | préciser davantage les mesures visées au paragraphe 1; et

b) | définir les formats et procédures, y compris les délais, applicables aux fins du paragraphe 2.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

SECTION 3

Services de confiance qualifiés

Article 20

Contrôle des prestataires de services de confiance qualifiés

1. Les prestataires de services de confiance qualifiés font l'objet, au moins tous les vingt-quatre mois, d'un audit effectué à leurs frais par un organisme d'évaluation de la conformité. Le but de l'audit est de confirmer que les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent remplissent les exigences fixées par le présent règlement. Les prestataires de services de confiance qualifiés transmettent le rapport d'évaluation de la conformité à l'organe de contrôle dans un délai de trois jours ouvrables qui suivent sa réception.

Artikel 19

Veiligheidseisen die van toepassing zijn op verleners van vertrouwensdiensten

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

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

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

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

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

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

4. De Commissie kan middels uitvoeringshandelingen:

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

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

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

AFDELING 3

Vertrouwensdiensten

2. Sans préjudice du paragraphe 1, l'organe de contrôle peut à tout moment, soumettre les prestataires de services de confiance qualifiés à un audit ou demander à un organisme d'évaluation de la conformité de procéder à une évaluation de la conformité des prestataires de services de confiance qualifiés, aux frais de ces prestataires de services de confiance, afin de confirmer que les prestataires et les services de confiance qualifiés qu'ils fournissent remplissent les exigences fixées par le présent règlement. L'organe de contrôle informe les autorités chargées de la protection des données des résultats de ses audits lorsqu'il apparaît que les règles en matière de protection des données à caractère personnel ont été violées.

3. Lorsque l'organe de contrôle exige du prestataire de services de confiance qualifié qu'il corrige un manquement aux exigences prévues par le présent règlement et que le prestataire n'agit pas en conséquence, et le cas échéant dans un délai fixé par l'organe de contrôle, l'organe de contrôle, tenant compte, en particulier, de l'ampleur, de la durée et des conséquences de ce manquement, peut retirer à ce prestataire ou au service affecté le statut qualifié et informe l'organisme visé à l'article 22, paragraphe 3, aux fins de la mise à jour des listes de confiance visées à l'article 22, paragraphe 1. L'organe de contrôle informe le prestataire de services de confiance qualifié du retrait de son statut qualifié ou du retrait du statut qualifié du service concerné.

4. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes suivantes:

a) | accréditation des organismes d'évaluation de la conformité et rapports d'évaluation de la conformité visés au paragraphe 1;

b) | règles d'audit en fonction desquelles les organismes d'évaluation de la conformité procéderont à leur évaluation de la conformité des prestataires de services de confiance qualifiés visés au paragraphe 1.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 21

Lancement d'un service de confiance qualifié

1. Lorsque des prestataires de services de confiance, sans statut qualifié, ont l'intention de commencer à offrir des services de confiance qualifiés, ils soumettent à l'organe de contrôle une notification de leur intention accompagnée d'un rapport d'évaluation de la conformité délivré par un

Artikel 20

Toezicht op gekwalificeerde verleners van vertrouwensdiensten

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

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

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

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

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

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

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

organisme d'évaluation de la conformité.

2. L'organe de contrôle vérifie que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences fixées par le présent règlement, en particulier les exigences en ce qui concerne les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent.

Si l'organe de contrôle conclut que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences visées au premier alinéa, l'organe de contrôle accorde le statut qualifié au prestataire de services de confiance et aux services de confiance qu'il fournit et informe l'organisme visé à l'article 22, paragraphe 3, aux fins de la mise à jour des listes de confiance visées à l'article 22, paragraphe 1, au plus tard trois mois suivant la notification conformément au paragraphe 1 du présent article.

Si la vérification n'est pas terminée dans un délai de trois mois à compter de la notification, l'organe de contrôle en informe le prestataire de services de confiance en précisant les raisons du retard et le délai nécessaire pour terminer la vérification.

3. Les prestataires de services de confiance qualifiés peuvent commencer à fournir le service de confiance qualifié une fois que le statut qualifié est indiqué sur les listes de confiance visées à l'article 22, paragraphe 1.

4. La Commission peut définir, au moyen d'actes d'exécution, les formats et les procédures applicables aux fins des paragraphes 1 et 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 22

Listes de confiance

1. Chaque État membre établit, tient à jour et publie des listes de confiance, y compris des informations relatives aux prestataires de services de confiance qualifiés dont il est responsable, ainsi que des informations relatives aux services de confiance qualifiés qu'ils fournissent.

2. Les États membres établissent, tiennent à jour et publient, de façon sécurisée et sous une forme adaptée au traitement automatisé, les listes de confiance visées au paragraphe 1 portant une signature électronique ou un cachet électronique.

3. Les États membres communiquent à la Commission, dans les meilleurs délais, des informations relatives à l'organisme chargé d'établir, de tenir à jour et de publier les listes nationales de confiance, ainsi que des détails précisant où ces listes sont publiées, indiquant les certificats utilisés pour apposer une signature électronique ou un cachet électronique sur ces listes et signalant les modifications apportées à ces listes.

4. La Commission met à la disposition du public, par l'intermédiaire d'un canal sécurisé, les informations visées au paragraphe 3 sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé.

5. Au plus tard le 18 septembre 2015, la Commission précise, au moyen d'actes d'exécution, les informations visées au paragraphe 1 et définit les spécifications techniques et les formats des listes de confiance applicables aux fins des paragraphes 1 à 4. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Artikel 21

Aanvang voor het aanbieden van een gekwalificeerde vertrouwensdienst

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

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

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

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

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

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

Artikel 22

Vertrouwenslijsten

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

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

Article 23

Label de confiance de l'Union pour les services de confiance qualifiés

1. Une fois que le statut qualifié visé à l'article 21, paragraphe 2, deuxième alinéa, a été indiqué sur la liste de confiance visée à l'article 22, paragraphe 1, les prestataires de service de confiance qualifiés peuvent utiliser le label de confiance de l'Union pour indiquer d'une manière simple, claire et reconnaissable les services de confiance qualifiés qu'ils fournissent.

2. Lorsqu'ils utilisent le label de confiance de l'Union pour les services de confiance qualifiés visé au paragraphe 1, les prestataires de services de confiance qualifiés veillent à ce qu'un lien vers la liste de confiance concernée soit disponible sur leur site internet.

3. Au plus tard le 1er juillet 2015, la Commission prévoit, au moyen d'actes d'exécution, les spécifications relatives à la forme et notamment à la présentation, à la composition, à la taille et à la conception du label de confiance de l'Union pour les services de confiance qualifiés. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 24

Exigences applicables aux prestataires de services de confiance qualifiés

1. Lorsqu'un prestataire de services de confiance qualifié délivre un certificat qualifié pour un service de confiance, il vérifie, par des moyens appropriés et conformément au droit national, l'identité et, le cas échéant, tous les attributs spécifiques de la personne physique ou morale à laquelle il délivre le certificat qualifié.

Les informations visées au premier alinéa sont vérifiées par le prestataire de services de confiance qualifié directement ou en en ayant recours à un tiers conformément au droit national:

a) | par la présence en personne de la personne physique ou du représentant autorisé de la personne morale; ou

b) | à distance, à l'aide de moyens d'identification électronique pour lesquels, avant la délivrance du certificat qualifié, la personne physique ou un représentant autorisé de la personne morale s'est présenté en personne et qui satisfont aux exigences énoncées à l'article 8 en ce qui concerne les niveaux de garantie substantiel et élevé; ou

c) | au moyen d'un certificat de signature électronique qualifié ou d'un cachet électronique qualifié délivré conformément au point a) ou b); ou

d) | à l'aide d'autres méthodes d'identification reconnues au niveau national qui fournissent une garantie équivalente en termes de fiabilité à la présence en personne. La garantie équivalente est confirmée par un organisme d'évaluation de la conformité.

2. Un prestataire de services de confiance qualifié qui fournit des services de confiance qualifiés:

a) | informe l'organe de contrôle de toute modification dans la fourniture de ses services de confiance qualifiés et de son intention éventuelle de cesser ces activités;

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

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

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

Artikel 23

Vertrouwensmerk van de EU voor gekwalificeerde vertrouwensdiensten

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

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

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

Artikel 24

Eisen aan gekwalificeerde verleners van vertrouwensdiensten

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

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

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

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

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

b) | emploie du personnel et, le cas échéant, des sous-traitants qui possèdent l'expertise, la fiabilité, l'expérience et les qualifications nécessaires, qui ont reçu une formation appropriée en ce qui concerne les règles en matière de sécurité et de protection des données à caractère personnel et appliquent des procédures administratives et de gestion correspondant à des normes européennes ou internationales;

c) | en ce qui concerne le risque de responsabilité pour dommages conformément à l'article 13, maintient des ressources financières suffisantes et/ou contracte une assurance responsabilité appropriée, conformément au droit national;

d) | avant d'établir une relation contractuelle, informe, de manière claire et exhaustive, toute personne désireuse d'utiliser un service de confiance qualifié des conditions précises relatives à l'utilisation de ce service, y compris toute limite quant à son utilisation;

e) | utilise des systèmes et des produits fiables qui sont protégés contre les modifications et assure la sécurité technique et la fiabilité des processus qu'ils prennent en charge;

f) | utilise des systèmes fiables pour stocker les données qui lui sont fournies, sous une forme vérifiable de manière que: | i) | les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée par ces données; | ii) | seules des personnes autorisées puissent introduire des données et modifier les données conservées; | iii) | l'authenticité des données puisse être vérifiée;

g) | prend des mesures appropriées contre la falsification et le vol de données;

h) | enregistre et maintient accessibles pour une durée appropriée, y compris après que les activités du prestataire de services de confiance qualifié ont cessé, toutes les informations pertinentes concernant les données délivrées et reçues par le prestataire de services de confiance qualifié, aux fins notamment de pouvoir fournir des preuves en justice et aux fins d'assurer la continuité du service. Ces enregistrements peuvent être effectués par voie électronique;

i) | a un plan actualisé d'arrêt d'activité afin d'assurer la continuité du service conformément aux dispositions vérifiées par l'organe de contrôle au titre de l'article 17, paragraphe 4, point i);

j) | assure le traitement licite de données à caractère personnel conformément à la directive 95/46/CE;

k) | au cas où le prestataire de services de confiance qualifié délivre des certificats qualifiés, établit et tient à jour une base de données relative aux certificats.

3. Lorsqu'un prestataire de services de confiance qualifié qui délivre des certificats qualifiés décide de révoquer un certificat, il enregistre cette révocation dans sa base de données relative aux certificats et publie le statut de révocation du certificat en temps utile, et en tout état de cause dans les vingt-quatre heures suivant la réception de la demande. Cette révocation devient effective immédiatement dès sa publication.

4. En ce qui concerne le paragraphe 3, les prestataires de services de confiance qualifiés qui délivrent des certificats qualifiés fournissent à toute partie utilisatrice des informations sur la validité ou le statut de révocation des certificats qualifiés qu'ils ont délivrés. Ces informations sont disponibles, au moins par certificat, à tout moment et au-delà de la période de validité du certificat, sous une forme automatisée qui est fiable, gratuite et efficace.

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

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

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

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

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

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

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

f) | maakt gebruik van betrouwbare systemen voor de opslag van aan hem verstrekte gegevens in verifieerbare vorm, zodat: | i) | de gegevens uitsluitend publiek beschikbaar zijn indien de persoon op wie de gegevens betrekking hebben, hiervoor toestemming heeft gegeven, | ii) | alleen bevoegde personen de opgeslagen gegevens kunnen invoeren en wijzigen, | iii) | de authenticiteit van de gegevens kan worden gecontroleerd;

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

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

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

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

5. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux systèmes et produits fiables, qui satisfont aux exigences du paragraphe 2, points e) et f), du présent article. Les systèmes et les produits fiables sont présumés satisfaire aux exigences fixées au présent article lorsqu'ils respectent ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

SECTION 4

Signatures électroniques

Article 25

Effets juridiques des signatures électroniques

1. L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée.

2. L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite.

3. Une signature électronique qualifiée qui repose sur un certificat qualifié délivré dans un État membre est reconnue en tant que signature électronique qualifiée dans tous les autres États membres.

Article 26

Exigences relatives à une signature électronique avancée

Une signature électronique avancée satisfait aux exigences suivantes:

a) | être liée au signataire de manière univoque;

b) | permettre d'identifier le signataire;

c) | avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif; et

d) | être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Article 27

Signatures électroniques dans les services publics

1. Si un État membre exige une signature électronique avancée pour utiliser un service en ligne offert par un organisme du secteur public ou pour l'utiliser au nom de cet organisme, il reconnaît les signatures électroniques avancées, les signatures électroniques avancées qui

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

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

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

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

AFDELING 4

Elektronische handtekeningen

Artikel 25

Rechtsgevolgen van elektronische handtekeningen

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

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

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

Artikel 26

Eisen voor geavanceerde elektronische handtekeningen

Een geavanceerde elektronische handtekening voldoet aan de volgende eisen:

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

b) | zij maakt het mogelijk de ondertekenaar te identificeren;

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

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

formats ou utilisant les méthodes définis dans les actes d'exécution visés au paragraphe 5.

2. Si un État membre exige une signature électronique avancée qui repose sur un certificat qualifié pour utiliser un service en ligne proposé par un organisme du secteur public ou pour l'utiliser au nom de cet organisme, il reconnaît les signatures électroniques avancées qui reposent sur un certificat qualifié et les signatures électroniques qualifiées au moins dans les formats ou utilisant les méthodes définis dans les actes d'exécution visés au paragraphe 5.

3. Les États membres n'exigent pas, pour une utilisation transfrontalière dans un service en ligne offert par un organisme du secteur public, de signature électronique présentant un niveau de sécurité supérieur à celui de la signature électronique qualifiée.

4. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux signatures électroniques avancées. Une signature électronique avancée est présumée satisfaire aux exigences applicables aux signatures électroniques avancées visées aux paragraphes 1 et 2 du présent article et à l'article 26 lorsqu'elle respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

5. Au plus tard le 18 septembre 2015, et compte tenu des pratiques et des normes ainsi que des actes juridiques de l'Union en vigueur, la Commission définit, au moyen d'actes d'exécution, les formats de référence des signatures électroniques avancées ou les méthodes de référence lorsque d'autres formats sont utilisés. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 28

Certificats qualifiés de signature électronique

1. Les certificats qualifiés de signature électronique satisfont aux exigences fixées à l'annexe I.

2. Les certificats qualifiés de signature électronique ne font l'objet d'aucune exigence obligatoire allant au-delà des exigences fixées à l'annexe I.

3. Les certificats qualifiés de signature électronique peuvent comprendre des attributs spécifiques supplémentaires non obligatoires. Ces attributs n'affectent pas l'interopérabilité et la reconnaissance des signatures électroniques qualifiées.

4. Si un certificat qualifié de signature électronique a été révoqué après la première activation, il perd sa validité à compter du moment de sa révocation et il ne peut en aucun cas recouvrer son statut antérieur.

5. Sous réserve des conditions suivantes, les États membres peuvent établir des règles nationales relatives à la suspension temporaire d'un certificat qualifié de signature électronique:

a) | si un certificat qualifié de signature électronique a été temporairement suspendu, ce certificat perd sa validité pendant la période de suspension.

b) | la période de suspension est clairement indiquée dans la base de données relative aux certificats et le statut de suspension est visible, pendant la période de suspension, auprès du service fournissant les informations sur le statut

Artikel 27

Elektronische handtekeningen in openbare diensten

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

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

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

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

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

Artikel 28

Gekwalificeerde certificaten voor elektronische handtekeningen

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

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

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

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

du certificat.

6. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux certificats qualifiés de signature électronique. Un certificat qualifié de signature électronique est présumé satisfaire aux exigences fixées à l'annexe I lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 29

Exigences applicables aux dispositifs de création de signature électronique qualifiés

1. Les dispositifs de création de signature électronique qualifiés respectent les exigences fixées à l'annexe II.

2. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux dispositifs de création de signature électronique qualifiés. Un dispositif de création de signature électronique qualifié est présumé satisfaire aux exigences fixées à l'annexe II lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 30

Certification des dispositifs de création de signature électronique qualifiés

1. La conformité des dispositifs de création de signature électronique qualifiés avec les exigences fixées à l'annexe II est certifiée par les organismes publics ou privés compétents désignés par les États membres.

2. Les États membres notifient à la Commission le nom et l'adresse de l'organisme public ou privé visé au paragraphe 1. La Commission met ces informations à la disposition des États membres.

3. La certification visée au paragraphe 1 est fondée sur l'un des éléments suivants:

a) | un processus d'évaluation de la sécurité mis en œuvre conformément à l'une des normes relatives à l'évaluation de la sécurité des produits informatiques figurant sur la liste établie conformément au deuxième alinéa; ou

b) | un processus autre que le processus visé au point a), à condition qu'il recoure à des niveaux de sécurité comparables et que l'organisme public ou privé visé au paragraphe 1 notifie ce processus à la Commission. Ledit processus ne peut être utilisé qu'en l'absence des normes visées au point a) ou lorsqu'un processus d'évaluation de la sécurité visé au point a) est en cours.

La Commission établit, au moyen d'actes d'exécution, une liste de normes relatives à l'évaluation de la sécurité des produits informatiques visés au point a). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

4. La Commission est habilitée à adopter des actes délégués, en conformité avec l'article 47, en ce qui concerne la définition de critères spécifiques que doivent respecter les organismes désignés visés au paragraphe 1 du présent article.

Article 31

hersteld.

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

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

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

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

Artikel 29

Eisen voor gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen

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

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

Artikel 30

Certificering van gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen

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

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

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

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

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

veiligheidsbeoordeling gaande is.

Publication d'une liste des dispositifs de création de signature électronique qualifiés certifiés

1. Les États membres notifient à la Commission, dans les meilleurs délais et au plus tard un mois après la conclusion de la certification, des informations sur les dispositifs de création de signature électronique qualifiés qui ont été certifiés par les organismes visés à l'article 30, paragraphe 1. Ils notifient également à la Commission, dans les meilleurs délais et au plus tard un mois après l'annulation de la certification, des informations sur les dispositifs de création de signature électronique qui ne sont plus certifiés.

2. Sur la base des informations reçues, la Commission établit, publie et met à jour une liste des dispositifs de création de signature électronique qualifiés certifiés.

3. La Commission peut définir, au moyen d'actes d'exécution, les formats et les procédures applicables aux fins du paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 32

Exigences applicables à la validation des signatures électroniques qualifiées

1. Le processus de validation d'une signature électronique qualifiée confirme la validité d'une signature électronique qualifiée à condition que:

a) | le certificat sur lequel repose la signature ait été, au moment de la signature, un certificat qualifié de signature électronique conforme à l'annexe I;

b) | le certificat qualifié ait été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature;

c) | les données de validation de la signature correspondent aux données communiquées à la partie utilisatrice;

d) | l'ensemble unique de données représentant le signataire dans le certificat soit correctement fourni à la partie utilisatrice;

e) | l'utilisation d'un pseudonyme soit clairement indiquée à la partie utilisatrice, si un pseudonyme a été utilisé au moment de la signature;

f) | la signature électronique ait été créée par un dispositif de création de signature électronique qualifié;

g) | l'intégrité des données signées n'ait pas été compromise;

h) | les exigences prévues à l'article 26 aient été satisfaites au moment de la signature.

2. Le système utilisé pour valider la signature électronique qualifiée fournit à la partie utilisatrice le résultat correct du processus de validation et permet à celle-ci de détecter tout problème pertinent relatif à la sécurité.

3. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables à la validation des signatures électroniques qualifiées. La validation des signatures électroniques qualifiées est présumée satisfaire aux exigences fixées au paragraphe 1 lorsqu'elle respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 33

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

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

Artikel 31

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

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

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

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

Artikel 32

Eisen voor de validering van gekwalificeerde elektronische handtekeningen

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

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

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

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

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

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

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

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

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

Service de validation qualifié des signatures électroniques qualifiées

1. Un service de validation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui:

a) | fournit une validation en conformité avec l'article 32, paragraphe 1; et

b) | permet aux parties utilisatrices de recevoir le résultat du processus de validation d'une manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire qui fournit le service de validation qualifié.

2. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables au service de validation qualifié visé au paragraphe 1. Le service de validation de signatures électroniques qualifiées est présumé satisfaire aux exigences fixées au paragraphe 1 lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 34

Service de conservation qualifié des signatures électroniques qualifiées

1. Un service de conservation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique.

2. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables au service de conservation qualifié des signatures électroniques qualifiées. Le service de conservation qualifié des signatures électroniques qualifiées est présumé satisfaire aux exigences fixées au paragraphe 1 lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

SECTION 5

Cachets électroniques

Article 35

Effets juridiques des cachets électroniques

1. L'effet juridique et la recevabilité d'un cachet électronique comme preuve en justice ne peuvent être refusés au seul motif que ce cachet se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du cachet électronique qualifié.

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

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

Artikel 33

Gekwalificeerde valideringsdienst voor gekwalificeerde elektronische handtekeningen

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

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

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

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

Artikel 34

Gekwalificeerde bewaringsdienst voor gekwalificeerde elektronische handtekeningen

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

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

AFDELING 5

Elektronische zegels

2. Un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié.

3. Un cachet électronique qualifié qui repose sur un certificat qualifié délivré dans un État membre est reconnu en tant que cachet électronique qualifié dans tous les autres États membres.

Article 36

Exigences du cachet électronique avancé

Un cachet électronique avancé satisfait aux exigences suivantes:

a) | être lié au créateur du cachet de manière univoque;

b) | permettre d'identifier le créateur du cachet;

c) | avoir été créé à l'aide de données de création de cachet électronique que le créateur du cachet peut, avec un niveau de confiance élevé, utiliser sous son contrôle pour créer un cachet électronique; et

d) | être lié aux données auxquelles il est associé de telle sorte que toute modification ultérieure des données soit détectable.

Article 37

Cachets électroniques dans les services publics

1. Si un État membre exige un cachet électronique avancé pour utiliser un service en ligne offert par un organisme du secteur public ou pour l'utiliser au nom de cet organisme, il reconnaît les cachets électroniques avancés, les cachets électroniques avancés qui reposent sur un certificat qualifié de cachet électronique et les cachets électroniques qualifiés au moins dans les formats ou utilisant les méthodes définis dans les actes d'exécutions visés au paragraphe 5.

2. Si un État membre exige un cachet électronique avancé qui repose sur un certificat qualifié pour utiliser un service en ligne proposé par un organisme du secteur public ou pour l'utiliser au nom de cet organisme, il reconnaît les cachets électroniques avancés qui reposent sur un certificat qualifié et les cachets électroniques qualifiés au moins dans les formats ou utilisant les méthodes définis dans les actes d'exécution visés au paragraphe 5.

3. Les États membres n'exigent pas, pour l'utilisation transfrontalière dans un service en ligne offert par un organisme du secteur public, de cachet électronique présentant un niveau de sécurité supérieur à celui du cachet électronique qualifié.

4. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux cachets électroniques avancés. Un cachet électronique avancé est présumé satisfaire aux exigences applicables aux cachets électroniques avancés visées aux paragraphes 1 et 2 du présent article et à l'article 36 lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

5. Au plus tard le 18 septembre 2015, et compte tenu des pratiques et des normes ainsi que des actes juridiques de l'Union en vigueur, la Commission définit, au moyen d'actes d'exécution, les formats de référence des cachets électroniques avancés ou les méthodes de référence lorsque d'autres formats sont utilisés. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 38

Artikel 35

Rechtsgevolgen van elektronische zegels

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

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

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

Artikel 36

Eisen voor geavanceerde elektronische zegels

Een geavanceerd elektronisch zegel voldoet aan de volgende eisen:

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

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

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

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

Artikel 37

Elektronische zegels in openbare diensten

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

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

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

Certificats qualifiés de cachet électronique

1. Les certificats qualifiés de cachet électronique satisfont aux exigences fixées à l'annexe III.

2. Les certificats qualifiés de cachet électronique ne font l'objet d'aucune exigence obligatoire allant au-delà des exigences fixées à l'annexe III.

3. Les certificats qualifiés de cachet électronique peuvent comprendre des attributs spécifiques supplémentaires non obligatoires. Ces attributs n'affectent pas l'interopérabilité et la reconnaissance des cachets électroniques qualifiés.

4. Si un certificat qualifié de cachet électronique a été révoqué après la première activation, il perd sa validité à compter du moment de sa révocation et il ne peut en aucun cas recouvrer son statut antérieur.

5. Sous réserve des conditions suivantes, les États membres peuvent établir des règles nationales relatives à la suspension temporaire de certificats qualifiés de cachet électronique:

a) | si un certificat qualifié de cachet électronique a été temporairement suspendu, ce certificat perd sa validité pendant la période de suspension;

b) | la période de suspension est clairement indiquée dans la base de données relative aux certificats et le statut de suspension est visible, pendant la période de suspension, auprès du service fournissant les informations sur le statut du certificat.

6. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux certificats qualifiés de cachet électronique. Un certificat qualifié de cachet électronique est présumé satisfaire aux exigences fixées à l'annexe III lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

Article 39

Dispositifs de création de cachet électronique qualifiés

1. L'article 29 s'applique mutatis mutandis aux exigences applicables aux dispositifs de création de cachet électronique qualifiés.

2. L'article 30 s'applique mutatis mutandis à la certification des dispositifs de création de cachet électronique qualifiés.

3. L'article 31 s'applique mutatis mutandis à la publication d'une liste de dispositifs de création de cachet électronique qualifiés.

Article 40

Validation et conservation des cachets électroniques qualifiés

Les articles 32, 33 et 34 s'appliquent mutatis mutandis à la validation et à la conservation des cachets électroniques qualifiés.

SECTION 6

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

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

Artikel 38

Gekwalificeerde certificaten voor elektronische zegels

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

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

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

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

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

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

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

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

Artikel 39

Gekwalificeerde middelen voor het aanmaken van elektronische zegels

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

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

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

Artikel 40

Horodatage électronique

Article 41

Effet juridique des horodatages électroniques

1. L'effet juridique et la recevabilité d'un horodatage électronique comme preuve en justice ne peuvent être refusés au seul motif que cet horodatage se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences de l'horodatage électronique qualifié.

2. Un horodatage électronique qualifié bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure.

3. Un horodatage électronique qualifié délivré dans un État membre est reconnu en tant qu'horodatage électronique qualifié dans tous les États membres.

Article 42

Exigences applicables aux horodatages électroniques qualifiés

1. Un horodatage électronique qualifié satisfait aux exigences suivantes:

a) | il lie la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données;

b) | il est fondé sur une horloge exacte liée au temps universel coordonné; et

c) | il est signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié, ou par une méthode équivalente.

2. La Commission peut, au moyen d'actes d'exécution, établir les numéros de référence des normes en ce qui concerne l'établissement du lien entre la date et l'heure et les données, et les horloges exactes. L'établissement du lien entre la date et l'heure et les données et les horloges exactes sont présumés satisfaire aux exigences fixées au paragraphe 1 lorsqu'ils respectent ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

SECTION 7

Services d'envoi recommandé électronique

Article 43

Effet juridique d'un service d'envoi recommandé électronique

1. L'effet juridique et la recevabilité des données envoyées et reçues à l'aide d'un service d'envoi recommandé électronique comme preuves en justice ne peuvent être refusés au seul motif que ce service se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du service d'envoi recommandé électronique qualifié.

2. Les données envoyées et reçues au moyen d'un service d'envoi recommandé électronique qualifié bénéficient d'une présomption quant à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié et à leur réception par le destinataire identifié, et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées par le service d'envoi recommandé électronique qualifié.

Validering en bewaring van gekwalificeerde elektronische zegels

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

AFDELING 6

Elektronisch tijdstempel

Artikel 41

Rechtsgevolg van elektronische tijdstempels

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

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

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

Artikel 42

Eisen voor gekwalificeerde elektronische tijdstempels

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

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

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

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

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

AFDELING 7

Diensten voor elektronisch aangetekende bezorging

Artikel 43

Article 44

Exigences applicables aux services d'envoi recommandé électronique qualifiés

1. Les services d'envoi recommandé électronique qualifiés satisfont aux exigences suivantes:

a) | ils sont fournis par un ou plusieurs prestataires de services de confiance qualifiés;

b) | ils garantissent l'identification de l'expéditeur avec un degré de confiance élevé;

c) | ils garantissent l'identification du destinataire avant la fourniture des données;

d) | l'envoi et la réception de données sont sécurisés par une signature électronique avancée ou par un cachet électronique avancé d'un prestataire de services de confiance qualifié, de manière à exclure toute possibilité de modification indétectable des données;

e) | toute modification des données nécessaire pour l'envoi ou la réception de celles-ci est clairement signalée à l'expéditeur et au destinataire des données;

f) | la date et l'heure d'envoi, de réception et toute modification des données sont indiquées par un horodatage électronique qualifié.

Dans le cas où les données sont transférées entre deux prestataires de services de confiance qualifiés ou plus, les exigences fixées aux points a) à f) s'appliquent à tous les prestataires de services de confiance qualifiés.

2. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux processus d'envoi et de réception de données. Le processus d'envoi et de réception de données est présumé satisfaire aux exigences fixées au paragraphe 1 lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

SECTION 8

Authentification de site internet

Article 45

Exigences applicables aux certificats qualifiés d'authentification de site internet

1. Les certificats qualifiés d'authentification de site internet satisfont aux exigences fixées à l'annexe IV.

2. La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux certificats qualifiés d'authentification de site internet. Un certificat qualifié d'authentification de site internet est présumé satisfaire aux exigences fixées à l'annexe IV lorsqu'il respecte ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2.

CHAPITRE IV

DOCUMENTS ÉLECTRONIQUES

Rechtsgevolg van een dienst voor elektronisch aangetekende bezorging

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

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

Artikel 44

Eisen voor gekwalificeerde diensten voor elektronisch aangetekende bezorging

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

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

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

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

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

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

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

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

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

AFDELING 8

Authenticatie van websites

Artikel 45

Eisen voor gekwalificeerde certificaten voor websiteauthenticatie

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

Article 46

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

Effets juridiques des documents électroniques

L'effet juridique et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique.

HOOFDSTUK IV

ELEKTRONISCHE DOCUMENTEN

CHAPITRE V

DÉLÉGATIONS DE POUVOIR ET DISPOSITIONS D'EXÉCUTION

Article 47

Artikel 46

Rechtsgevolgen van elektronische documenten

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

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 30, paragraphe 4, est conféré à la Commission pour une durée indéterminée à compter du 17 septembre 2014.

3. La délégation de pouvoir visée à l'article 30, paragraphe 4, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

5. Un acte délégué adopté en vertu de l'article 30, paragraphe 4, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

HOOFDSTUK V

BEVOEGDHEIDSDELEGATIES EN UITVOERINGSBEPALINGEN

Artikel 47

Uitoefening van de bevoegdheidsdelegatie

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

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

Article 48

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) no 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) no 182/2011 s'applique.

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

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

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

Artikel 48

Comitéprocedure

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

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

CHAPITRE VI

DISPOSITIONS FINALES

Article 49

Réexamen

HOOFDSTUK VI

évalue, en particulier, s'il convient de modifier le champ d'application du présent règlement ou ses dispositions spécifiques, y compris l'article 6, l'article 7, point f) et les articles 34, 43, 44 et 45, compte tenu de l'expérience acquise dans l'application du présent règlement ainsi que de l'évolution des technologies, du marché et du contexte juridique.

Le rapport visé au premier alinéa est, au besoin, accompagné de propositions législatives.

En outre, la Commission présente au Parlement européen et au Conseil, tous les quatre ans après la présentation du rapport visé au premier alinéa, un rapport sur les progrès accomplis dans la réalisation des objectifs du présent règlement.

Article 50

Abrogation

1. La directive 1999/93/CE est abrogée avec effet au 1er juillet 2016.

2. Les références faites à la directive abrogée s'entendent comme faites au présent règlement.

Article 51

Mesures transitoires

1. Les dispositifs sécurisés de création de signature dont la conformité a été déterminée conformément à l'article 3, paragraphe 4, de la directive 1999/93/CE sont considérés comme des dispositifs de création de signature électronique qualifiés au titre du présent règlement.

2. Les certificats qualifiés délivrés aux personnes physiques au titre de la directive 1999/93/CE sont considérés comme des certificats qualifiés de signature électronique au titre du présent règlement jusqu'à leur expiration.

3. Un prestataire de services de certification qui délivre des certificats qualifiés au titre de la directive 1999/93/CE soumet un rapport d'évaluation de la conformité à l'organe de contrôle le plus rapidement possible, et au plus tard le 1er juillet 2017. Jusqu'à la présentation d'un tel rapport d'évaluation de la conformité et l'achèvement de l'évaluation par l'organe de contrôle, ce prestataire de services de certification est considéré comme un prestataire de services de confiance qualifié au titre du présent règlement.

4. Si un prestataire de services de certification qui délivre des certificats qualifiés au titre de la directive 1999/93/CE ne soumet pas de rapport d'évaluation de la conformité à l'organe de contrôle dans le délai visé au paragraphe 3, ce prestataire de services de certification n'est pas considéré comme un prestataire de services de confiance qualifié au titre du présent règlement à partir du 2 juillet 2017.

Article 52

Entrée en vigueur

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne.

Artikel 49

Evaluatie

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

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

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

Artikel 50

Intrekking

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

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

Artikel 51

Overgangsmaatregelen

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

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

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

4. Indien een certificatiedienstverlener die gekwalificeerde certificaten overeenkomstig Richtlijn 1999/93/EG afgeeft, niet binnen de in lid 3 bedoelde termijn een conformiteitsbeoordelingsverslag indient bij het

vanaf 2 juli 2017 niet beschouwd als gekwalificeerde verlener van vertrouwensdiensten in de zin van deze verordening.

2. Le présent règlement est applicable à partir du 1er juillet 2016, à l'exception des dispositions suivantes:

a) | l'article 8, paragraphe 3, l'article 9, paragraphe 5, l'article 12, paragraphes 2 à 9, l'article 17, paragraphe 8, l'article 19, paragraphe 4, l'article 20, paragraphe 4, l'article 21, paragraphe 4, l'article 22, paragraphe 5, l'article 23, paragraphe 3, l'article 24, paragraphe 5, l'article 27, paragraphes 4 et 5, l'article 28, paragraphe 6, l'article 29, paragraphe 2, l'article 30, paragraphes 3 et 4, l'article 31, paragraphe 3, l'article 32, paragraphe 3, l'article 33, paragraphe 2, l'article 34, paragraphe 2, l'article 37, paragraphes 4 et 5, l'article 38, paragraphe 6, l'article 42, paragraphe 2, l'article 44, paragraphe 2, l'article 45, paragraphe 2, et les articles 47 et 48 sont applicables à partir du 17 septembre 2014;

b) | l'article 7, l'article 8, paragraphes 1 et 2, les articles 9, 10, 11, et l'article 12, paragraphe 1, sont applicables à compter de la date d'application des actes d'exécution visés à l'article 8, paragraphe 3, et à l'article 12, paragraphe 8;

c) | l'article 6 s'applique après trois ans à compter de la date d'application des actes d'exécution visés à l'article 8, paragraphe 3 et à l'article 12, paragraphe 8.

3. Lorsque le schéma d'identification électronique notifié est inscrit sur la liste publiée par la Commission en application de l'article 9 avant la date visée au paragraphe 2, point c), du présent article, la reconnaissance des moyens d'identification électronique dans le cadre de ce schéma en application de l'article 6 a lieu au plus tard douze mois après la publication dudit schéma, mais pas avant la date visée au paragraphe 2, point c), du présent article.

4. Nonobstant le paragraphe 2, point c), du présent article, un État membre peut décider que des moyens d'identification électronique relevant d'un schéma d'identification électronique notifié en application de l'article 9, paragraphe 1, par un autre État membre sont reconnus dans le premier État membre à compter de la date d'application des actes d'exécution visés à l'article 8, paragraphe 3, et à l'article 12, paragraphe 8. Les États membres concernés informent la Commission. La Commission rend publiques ces informations.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 23 juillet 2014.

Par le Parlement européen

Le président

M. SCHULZ

Par le Conseil

Le président

S. GOZI

(1) JO C 351 du 15.11.2012, p. 73.

(2) Position du Parlement européen du 3 avril 2014 (non encore parue au Journal officiel) et décision du Conseil du 23 juillet 2014.

(3) Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (JO L 13 du 19.1.2000, p. 12).

(4) JO C 50 E du 21.2.2012, p. 1.

(5) Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur (JO L 376 du 27.12.2006, p. 36).

Artikel 52

Inwerkingtreding

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

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

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

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

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

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

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

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

Gedaan te Brussel, 23 juli 2014.

Voor het Parlement

De voorzitter

M. SCHULZ

Voor de Raad

De voorzitter

S. GOZI

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

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

(6) Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).

(7) Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

(8) Décision 2010/48/CE du Conseil du 26 novembre 2009 concernant la conclusion, par la Communauté européenne, de la convention des Nations unies relative aux droits des personnes handicapées (JO L 23 du 27.1.2010, p. 35).

(9) Règlement (CE) no 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) no 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30).

(10) Décision 2009/767/CE de la Commission du 16 octobre 2009 établissant des mesures destinées à faciliter l'exécution de procédures par voie électronique par l'intermédiaire des «guichets uniques» conformément à la directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur (JO L 274 du 20.10.2009, p. 36).

(11) Décision 2011/130/UE de la Commission du 25 février 2011 établissant des exigences minimales pour le traitement transfrontalier des documents signés électroniquement par les autorités compétentes conformément à la directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur (JO L 53 du 26.2.2011, p. 66).

(12) Règlement (UE) no 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

(13) Règlement (CE) no 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

(14) JO C 28 du 30.1.2013, p. 6.

(15) Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65).

ANNEXE I

EXIGENCES APPLICABLES AUX CERTIFICATS QUALIFIÉS DE SIGNATURE ÉLECTRONIQUE

Les certificats qualifiés de signature électronique contiennent:

a) | une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié de signature électronique;

b) | un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés, comprenant au moins l'État membre dans lequel ce prestataire est établi, et: | — | pour une personne morale: le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels, | — | pour une personne physique: le nom de la personne;

c) | au moins le nom du signataire ou un pseudonyme; si un pseudonyme est utilisé, cela est clairement indiqué;

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

(4) PB C 50 E van 21.2.2012, blz. 1.

(5) Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt (PB L 376 van 27.12.2006, blz. 36).

(6) Richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg (PB L 88 van 4.4.2011, blz. 45).

(7) Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB L 281 van 23.11.1995, blz. 31).

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

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

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

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

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

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

(14) PB C 28 van 30.1.2013, blz. 6.

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

BIJLAGE I

EISEN VOOR GEKWALIFICEERDE CERTIFICATEN VOOR ELEKTRONISCHE HANDTEKENINGEN

Gekwalificeerde certificaten voor elektronische handtekeningen bevatten:

d) | des données de validation de la signature électronique qui correspondent aux données de création de la signature électronique;

e) | des précisions sur le début et la fin de la période de validité du certificat;

f) | le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance qualifié;

g) | la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat;

h) | l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé mentionnés au point g);

i) | l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié;

j) | lorsque les données de création de la signature électronique associées aux données de validation de la signature électronique se trouvent dans un dispositif de création de signature électronique qualifié, une mention l'indiquant, au moins sous une forme adaptée au traitement automatisé.

ANNEXE II

EXIGENCES APPLICABLES AUX DISPOSITIFS DE CRÉATION DE SIGNATURE ÉLECTRONIQUE QUALIFIÉS

1. | Les dispositifs de création de signature électronique qualifiés garantissent au moins, par des moyens techniques et des procédures appropriés, que: | a) | la confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée; | b) | les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être pratiquement établies qu'une seule fois; | c) | l'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par les moyens techniques actuellement disponibles; | d) | les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

2. | Les dispositifs de création de signature électronique qualifiés ne modifient pas les données à signer et n'empêchent pas la présentation de ces données au signataire avant la signature.

3. | La génération ou la gestion de données de création de signature électronique pour le compte du signataire peut être seulement confiée à un prestataire de services de confiance qualifié.

4. | Sans préjudice du paragraphe 1, point d), un prestataire de services de confiance qualifié gérant des données de création de signature électronique pour le compte d'un signataire ne peut reproduire les données de création de signature électronique qu'à des fins de sauvegarde, sous réserve du respect des exigences suivantes: | a) | le niveau de sécurité des ensembles de données reproduits doit être équivalent à celui des ensembles de données d'origine; | b) | le nombre d'ensembles de données reproduits n'excède pas le minimum nécessaire pour assurer la continuité du service.

ANNEXE III

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

b) | een reeks gegevens die ondubbelzinnig verwijzen naar de gekwalificeerde verlener van vertrouwensdiensten die de gekwalificeerde certificaten afgeeft, met inbegrip van ten minste de lidstaat waarin de verlener is gevestigd en | — | voor een rechtspersoon: de naam en, indien van toepassing, het registratienummer zoals vermeld in de officiële registers, | — | voor een natuurlijke persoon: de naam van de persoon;

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

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

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

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

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

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

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

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

BIJLAGE II

EISEN VOOR GEKWALIFICEERDE MIDDELEN VOOR HET AANMAKEN VAN ELEKTRONISCHE HANDTEKENINGEN

1. | Gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen waarborgen via passende technieken en procedures dat ten minste: | a) | de vertrouwelijkheid van de gegevens die worden gebruikt om elektronische handtekeningen aan te maken redelijkerwijs gewaarborgd is; | b) | de gegevens voor het aanmaken van elektronische handtekeningen in de praktijk slechts één keer kunnen voorkomen; | c) | de gegevens voor het aanmaken van elektronische handtekeningen met redelijke zekerheid niet kunnen worden afgeleid en dat de elektronische handtekening op betrouwbare wijze beschermd is tegen vervalsing met de thans beschikbare technologie; | d) | de gegevens voor het aanmaken van elektronische handtekeningen door de legitieme ondertekenaar op betrouwbare wijze kunnen worden beschermd tegen gebruik door anderen.

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

EXIGENCES APPLICABLES AUX CERTIFICATS QUALIFIÉS DE CACHET ÉLECTRONIQUE

Les certificats qualifiés de cachet électronique contiennent:

a) | une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié de cachet électronique;

b) | un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés, comprenant au moins l'État membre dans lequel ce prestataire est établi et: | — | pour une personne morale: le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels, | — | pour une personne physique: le nom de la personne;

c) | au moins le nom du créateur du cachet et, le cas échéant, son numéro d'immatriculation tels qu'ils figurent dans les registres officiels;

d) | des données de validation du cachet électronique, qui correspondent aux données de création du cachet électronique;

e) | des précisions sur le début et la fin de la période de validité du certificat;

f) | le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance qualifié;

g) | la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat;

h) | l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé mentionnés au point g);

i) | l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié;

j) | lorsque les données de création du cachet électronique associées aux données de validation du cachet électronique se trouvent dans un dispositif de création de cachet électronique qualifié, une mention l'indiquant, au moins sous une forme adaptée au traitement automatisé.

ANNEXE IV

EXIGENCES APPLICABLES AUX CERTIFICATS QUALIFIÉS D'AUTHENTIFICATION DE SITE INTERNET

Les certificats qualifiés d'authentification de site internet contiennent:

a) | une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié d'authentification de site internet;

b) | un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés, comprenant au moins l'État membre dans lequel ce prestataire est établi et: | — | pour une personne morale: le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels, | — | pour une personne physique: le nom de la

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

4. | Onverminderd punt 1, onder d), mogen gekwalificeerde verleners van vertrouwensdiensten die namens de ondertekenaar gegevens voor het aanmaken van elektronische handtekeningen beheren, de gegevens voor het aanmaken van elektronische handtekeningen alleen dupliceren voor back-updoeleinden, op voorwaarde dat aan de volgende eisen wordt voldaan: | a) | de beveiliging van de gedupliceerde gegevensverzamelingen moet van hetzelfde niveau zijn als de beveiliging van de originele gegevensverzamelingen; | b) | het aantal gedupliceerde gegevensverzamelingen mag niet hoger zijn dan het minimum dat nodig is om de continuïteit van de dienst te waarborgen.

BIJLAGE III

EISEN VOOR GEKWALIFICEERDE CERTIFICATEN VOOR ELEKTRONISCHE ZEGELS

Gekwalificeerde certificaten voor elektronische zegels bevatten:

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

b) | een reeks gegevens die ondubbelzinnig verwijzen naar de gekwalificeerde verlener van vertrouwensdiensten die de gekwalificeerde certificaten afgeeft, met inbegrip van ten minste de lidstaat waar die dienstverlener is gevestigd en | — | voor een rechtspersoon: de naam en, indien van toepassing, het registratienummer zoals vermeld in de officiële registers, | — | voor een natuurlijke persoon: de naam van de persoon;

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

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

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

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

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

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

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

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

BIJLAGE IV

EISEN VOOR GEKWALIFICEERDE CERTIFICATEN VOOR WEBSITE-AUTHENTICATIE

personne;

c) | pour les personnes physiques: au moins le nom de la personne à qui le certificat a été délivré, ou un pseudonyme. Si un pseudonyme est utilisé, cela est clairement indiqué; | pour les personnes morales: au moins le nom de la personne morale à laquelle le certificat est délivré et, le cas échéant, son numéro d'immatriculation, tels qu'ils figurent dans les registres officiels;

d) | des éléments de l'adresse, dont au moins la ville et l'État, de la personne physique ou morale à laquelle le certificat est délivré et, le cas échéant, ces éléments tels qu'ils figurent dans les registres officiels;

e) | le(s) nom(s) de domaine exploité(s) par la personne physique ou morale à laquelle le certificat est délivré;

f) | des précisions sur le début et la fin de la période de validité du certificat;

g) | le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance qualifié;

h) | la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat;

i) | l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé visés au point h);

j) | l'emplacement des services de statut de validité des certificats qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié.

Gekwalificeerde certificaten voor websiteauthenticatie moeten het volgende bevatten:

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

b) | een reeks gegevens die ondubbelzinnig verwijzen naar de gekwalificeerde verlener van vertrouwensdiensten die de gekwalificeerde certificaten afgeeft, met inbegrip van ten minste de lidstaat waar die dienstverlener is gevestigd en | — | voor een rechtspersoon: de naam en, indien van toepassing, het registratienummer zoals vermeld in de officiële registers, | — | voor een natuurlijke persoon: de naam van de persoon;

c) | voor natuurlijke personen: op zijn minst de naam van de persoon aan wie het certificaat is afgegeven, of een pseudoniem. Indien een pseudoniem wordt gebruikt, wordt dat duidelijk aangegeven; | voor rechtspersonen: ten minste de naam van de rechtspersoon aan wie het certificaat is afgegeven en, indien van toepassing, het registratienummer zoals vermeld in de officiële registers;

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

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

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

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

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

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

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