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.

([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).

(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 services de fourniture électronique, ainsi que pour la mise 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 [1], 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 [2] 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 [3] 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 [4]. 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.

[1] JO C 50 E du 21.2.2012, p. 1.
[2] 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).
[3] 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).
[4] 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).

(13) Les États membres devraient rester libres, aux fins de l'identification électronique, d'utiliser ou d'introduire des moyens d'accès aux services en ligne. Ils devraient également pouvoir décider d'impliquer ou non le secteur privé dans la fourniture de ces moyens. Les États membres 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.

(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 d'utiliser de tels moyens d'identification électronique permettrait au secteur privé de s'appuyer sur des fonctions d'identification et d'authentification électroniques déjà largement utilisées dans de nombreux États membres, au moins pour les services publics, et de faciliter l'accès des entreprises et des particuliers à leurs services en ligne transfrontaliers. Afin de faciliter l'utilisation transfrontalière de tels moyens d'identification électronique par le secteur privé, la possibilité d'authentification prévue par un État membre devrait être accessible aux parties utilisatrices du 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.

(23) Dans la mesure où le présent règlement rend obligatoire la reconnaissance d'un service de confiance, un tel service ne peut être rejeté que si le destinataire de l'obligation est incapable de le lire ou de le vérifier pour des 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 [1], 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.

(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.

(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.

[1] 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).

(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.

(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.

(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).

(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.

(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 correcte de dispositions relatives aux plans d'arrêt d'activité dans les cas où des prestataires de services de confiance qualifiés cessent leurs activités.

(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.

(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.

(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) n° 765/2008 du Parlement européen et du Conseil ([1]), qui fixe les exigences relatives à l'accréditation d'organismes d'évaluation de la conformité et à la surveillance du marché de produits.

([1]) Règlement (CE) n° 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) n° 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30).

(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.

(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.

(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.

(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 [1], des signatures électroniques offrant une garantie de sécurité moindre devraient également être acceptées.

(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 une forme électronique ou qu'elle ne satisfait pas à toutes les exigences de la signature électronique qualifiée. Toutefois, il appartient au droit national de définir l'effet juridique produit par les signatures électroniques, à 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.

[1] 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).

(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.

(55) Une certification de sécurité informatique fondée sur des normes internationales, tels que la norme ISO 15408 et les méthodes d'évaluation et accords de reconnaissance mutuelle qui y sont liés, est un outil important pour vérifier la sécurité de dispositifs de création de signature électronique qualifiés et devrait être encouragée. Cependant, des solutions et des services innovants, comme 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.

(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.

(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.

(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.

(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.

(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.

(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.

(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 niveau de sécurité équivalent et satisfait aux obligations 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 ([1]).

(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.

([1]) 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).

(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 les critères que doivent remplir les organismes responsables de la certification des dispositifs de création de signature électronique qualifiés. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts. Il 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.

(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) n° 182/2011 du Parlement européen et du Conseil ([1]).

(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.

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

(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.

(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.

(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.

(77) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001 du Parlement européen et du Conseil ([2]) et a émis un avis, le 27 septembre 2012 ([3]),

([1]) Règlement (UE) n° 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).

([2]) Règlement (CE) n° 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).

([3]) JO C 28 du 30.1.2013, p. 6.

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet

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:

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;

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

c) instaure un cadre juridique pour les services de signatures électroniques, de cachets électroniques, d'horodatages électroniques, de documents électroniques, 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 ([1]);

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;

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;

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;

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;

17. «service de confiance qualifié», un service de confiance qui satisfait aux exigences du présent règlement;

([1]) 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).

18. «organisme d'évaluation de la conformité», un organisme défini à l'article 2, point 13), du règlement (CE) n° 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;

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;

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;

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;

22. «dispositif de création de signature électronique», un dispositif logiciel ou matériel configuré servant à créer une signature électronique;

23. «dispositif de création de signature électronique qualifié», un dispositif de création de signature électronique qui satisfait aux exigences énoncées à l'annexe II;

24. «créateur de cachet», une personne morale qui crée un cachet électronique;

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;

26. «cachet électronique avancé», un cachet électronique qui satisfait aux exigences énoncées à l'article 36;

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;

28. «données de création de cachet électronique», des données uniques qui sont utilisées par le créateur du cachet électronique pour créer un cachet électronique;

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;

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 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;

d) l'État membre notifiant veille à ce que les données d'identification personnelle représentant de manière univoque la personne en question soient attribuées 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, 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;

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;

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.

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;

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.

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

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);

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 est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les 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.

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 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.

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;

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.

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 reposent sur un certificat qualifié de signature électronique et les signatures électroniques qualifiées au moins dans les 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 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

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

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. 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

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

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.

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

Article 46

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.

CHAPITRE V

DÉLÉGATIONS DE POUVOIR ET DISPOSITIONS D'EXÉCUTION

Article 47

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.

Article 48

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

CHAPITRE VI

DISPOSITIONS FINALES

Article 49

Réexamen

La Commission procède à un réexamen de l'application du présent règlement et rend compte au Parlement européen et au Conseil, au plus tard le 1er juillet 2020. La Commission 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*.

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	*Par le Conseil*
Le président	*Le président*
M. SCHULZ	S. GOZI

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;

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

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 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.